

# スイッチング

概要・基本設定	10
レイヤー 3 スイッチとしての設定手順	10
ポート	12
ポートの指定方法	12
基本コマンド	12
ポートランキング	13
ポートミラーリング	15
基本設定	15
ポートセキュリティ	16
ループガード	19
MAC アドレススラッシングプロテクション	19
パケットストームプロテクション	21
ポート帯域制限機能	22
トリガー	22
LACP (IEEE 802.3ad)	25
基本設定	25
バーチャル LAN	28
概要	28
ポートと VLAN	28
デフォルト VLAN	29
ポート VLAN	29
タグ VLAN	31
VLAN タグ対応サーバーの共用	31
VLAN タグを利用したスイッチ間接続	32
IP サブネット VLAN	34
ARP パケットに関する注意事項	34
基本設定	34
プロトコル VLAN	36
マルチプル VLAN (Private VLAN)	37
基本ルール	38
設定例	39
ダブルタグ VLAN (Nested VLAN)	40
基本ルール	40
設定例	41

VLAN 間ルーティング . . . . .	43
スパンニングツリープロトコル (STP/RSTP) . . . . .	46
基本設定 . . . . .	46
マルチプル STP ドメイン . . . . .	47
スパンニングツリーパラメーターの設定変更 . . . . .	48
マルチプルスパンニングツリープロトコル (MSTP) . . . . .	51
概要 . . . . .	51
MST インスタンス . . . . .	51
MST リージョン . . . . .	52
CIST . . . . .	55
基本設定 . . . . .	55
マルチプルスパンニングツリーパラメーターの設定変更 . . . . .	60
イーサネットリングプロテクション (EPSR) . . . . .	64
概要 . . . . .	64
EPSR ドメイン . . . . .	65
マスターノードとトランジットノード . . . . .	65
プライマリーポートとセカンダリーポート . . . . .	65
コントロール VLAN とデータ VLAN . . . . .	65
制御メッセージ . . . . .	66
障害検出機能 . . . . .	66
基本動作 . . . . .	68
基本設定 . . . . .	70
フォワーディングデータベース . . . . .	74
FDB エントリー . . . . .	74
自動学習とダイナミックエントリー . . . . .	75
スタティックエントリー . . . . .	76
クラシファイア . . . . .	78
概要 . . . . .	78
基本設定 . . . . .	81
クラシファイアの作成 . . . . .	81
クラシファイアの使用 . . . . .	85
クラシファイアの変更・削除・確認 . . . . .	86
クラシファイアとルール領域消費量 . . . . .	87
ハードウェアパケットフィルタのみ使用時 . . . . .	88
ポリシーベース QoS のみ使用時 . . . . .	89
ハードウェアパケットフィルタとポリシーベース QoS 併用時 . . . . .	91
IPv6 ポリシーベース QoS 使用時 . . . . .	93
IPv6 ハードウェアパケットフィルタ使用時 . . . . .	94
QoS . . . . .	95
概要 . . . . .	95
基本的な用語 . . . . .	95
802.1p QoS の基本設定 . . . . .	99

設定手順例 . . . . .	99
ポリシーベース QoS の基本設定 . . . . .	100
設定の前に . . . . .	102
設定手順例 . . . . .	103
QoS ポリシー . . . . .	106
トラフィッククラス . . . . .	108
フローグループ . . . . .	109
クラシファイア . . . . .	110
QoS 処理フロー詳細 . . . . .	111
通常のパケット . . . . .	111
IPv6 ルーティングパケット . . . . .	113
パケット受信時の QoS 処理 . . . . .	116
ポリシーベースの QoS 処理 . . . . .	118
パケット送信時の QoS 処理 . . . . .	125
QoS ポリシーのフィルタリング機能 . . . . .	130
設定方法 . . . . .	130
具体例 . . . . .	131
設定例 . . . . .	131
最小帯域保証 . . . . .	132
DiffServ . . . . .	134
QoS ポリシーのルール領域消費量 . . . . .	141
ハードウェアパケットフィルター . . . . .	142
基本動作 . . . . .	142
フィルターの構成 . . . . .	142
フィルター処理の流れ . . . . .	143
設定手順 . . . . .	143
コマンド例 . . . . .	144
ハードウェアパケットフィルターのルール領域消費量 . . . . .	146
IPv6 ハードウェアパケットフィルター . . . . .	147
基本動作 . . . . .	147
フィルターの構成 . . . . .	147
フィルター処理の流れ . . . . .	147
設定手順 . . . . .	148
コマンド例 . . . . .	149
IPv6 ハードウェアパケットフィルターのルール領域消費量 . . . . .	150
ポート認証 . . . . .	151
概要 . . . . .	151
802.1X 認証方式 . . . . .	152
基本設定 . . . . .	152
Authenticator . . . . .	152
Authenticator (ダイナミック VLAN) . . . . .	153
Supplicant . . . . .	156

認証サーバー . . . . .	156
DHCP Snooping . . . . .	158
概要 . . . . .	158
登録できるクライアントの数 . . . . .	159
基本設定 . . . . .	159
コマンドリファレンス編 . . . . .	164
機能別コマンド索引 . . . . .	164
ACTIVATE PORTAUTH PORT REAUTHENTICATE . . . . .	170
ACTIVATE SWITCH PORT AUTONEGOTIATE . . . . .	171
ACTIVATE SWITCH PORT LOCK . . . . .	172
ADD DHCP Snooping BINDING . . . . .	173
ADD EPSR DATAVLAN . . . . .	175
ADD LACP PORT . . . . .	176
ADD MSTP MSTI VLAN . . . . .	178
ADD QOS FLOWGROUP . . . . .	179
ADD QOS POLICY . . . . .	180
ADD QOS TRAFFICCLASS . . . . .	181
ADD STP VLAN . . . . .	182
ADD SWITCH ACCELERATOR HWFILTER . . . . .	184
ADD SWITCH FILTER . . . . .	186
ADD SWITCH HWFILTER . . . . .	188
ADD SWITCH TRUNK . . . . .	190
ADD VLAN PORT . . . . .	191
ADD VLAN PROTOCOL . . . . .	194
ADD VLAN SUBNET . . . . .	197
CREATE CLASSIFIER . . . . .	198
CREATE EPSR . . . . .	205
CREATE MSTP MSTI . . . . .	208
CREATE QOS FLOWGROUP . . . . .	209
CREATE QOS POLICY . . . . .	212
CREATE QOS RED . . . . .	216
CREATE QOS TRAFFICCLASS . . . . .	218
CREATE STP . . . . .	222
CREATE SWITCH TRUNK . . . . .	223
CREATE VLAN . . . . .	225
DELETE DHCP Snooping BINDING . . . . .	227
DELETE EPSR DATAVLAN . . . . .	228
DELETE LACP PORT . . . . .	229
DELETE MSTP MSTI VLAN . . . . .	230
DELETE QOS FLOWGROUP . . . . .	231
DELETE QOS POLICY . . . . .	232
DELETE QOS TRAFFICCLASS . . . . .	233

DELETE STP VLAN . . . . .	234
DELETE SWITCH ACCELERATOR HWFILTER . . . . .	235
DELETE SWITCH FILTER . . . . .	236
DELETE SWITCH HWFILTER . . . . .	237
DELETE SWITCH TRUNK . . . . .	238
DELETE VLAN PORT . . . . .	239
DELETE VLAN PROTOCOL . . . . .	241
DELETE VLAN SUBNET . . . . .	242
DESTROY CLASSIFIER . . . . .	243
DESTROY EPSR . . . . .	244
DESTROY MSTP MSTI . . . . .	245
DESTROY QOS FLOWGROUP . . . . .	246
DESTROY QOS POLICY . . . . .	247
DESTROY QOS RED . . . . .	248
DESTROY QOS TRAFFICCLASS . . . . .	249
DESTROY STP . . . . .	250
DESTROY SWITCH TRUNK . . . . .	251
DESTROY VLAN . . . . .	252
DISABLE DHCP Snooping . . . . .	253
DISABLE DHCP Snooping ARPSECURITY . . . . .	254
DISABLE DHCP Snooping LOG . . . . .	255
DISABLE DHCP Snooping OPTION82 . . . . .	256
DISABLE EPSR . . . . .	257
DISABLE EPSR DEBUG . . . . .	258
DISABLE LACP . . . . .	259
DISABLE LACP DEBUG . . . . .	260
DISABLE MSTP . . . . .	261
DISABLE PORTAUTH . . . . .	262
DISABLE PORTAUTH DEBUG . . . . .	263
DISABLE PORTAUTH PORT . . . . .	264
DISABLE STP . . . . .	265
DISABLE STP DEBUG . . . . .	266
DISABLE STP PORT . . . . .	267
DISABLE STP PORT DEBUG . . . . .	268
DISABLE SWITCH AGEINGTIMER . . . . .	269
DISABLE SWITCH HASH . . . . .	270
DISABLE SWITCH LEARNING . . . . .	271
DISABLE SWITCH MCLIMITING . . . . .	272
DISABLE SWITCH MIRROR . . . . .	273
DISABLE SWITCH PORT . . . . .	274
DISABLE SWITCH PORT AUTOMDI . . . . .	275
DISABLE SWITCH PORT EGRESSQUEUE . . . . .	276

DISABLE SWITCH PORT FLOW . . . . .	277
DISABLE SWITCH PORT VLAN . . . . .	278
DISABLE SWITCH STPFORWARD . . . . .	279
ENABLE DHCP Snooping . . . . .	280
ENABLE DHCP Snooping ARPSECURITY . . . . .	281
ENABLE DHCP Snooping LOG . . . . .	282
ENABLE DHCP Snooping OPTION82 . . . . .	283
ENABLE EPSR . . . . .	284
ENABLE EPSR DEBUG . . . . .	285
ENABLE LACP . . . . .	286
ENABLE LACP DEBUG . . . . .	287
ENABLE MSTP . . . . .	288
ENABLE PORTAUTH . . . . .	289
ENABLE PORTAUTH DEBUG . . . . .	290
ENABLE PORTAUTH PORT . . . . .	291
ENABLE STP . . . . .	295
ENABLE STP DEBUG . . . . .	296
ENABLE STP PORT . . . . .	297
ENABLE STP PORT DEBUG . . . . .	298
ENABLE SWITCH AGEINGTIMER . . . . .	299
ENABLE SWITCH HASH . . . . .	300
ENABLE SWITCH LEARNING . . . . .	301
ENABLE SWITCH MCLIMITING . . . . .	302
ENABLE SWITCH MIRROR . . . . .	303
ENABLE SWITCH PORT . . . . .	304
ENABLE SWITCH PORT AUTOMDI . . . . .	305
ENABLE SWITCH PORT EGRESSQUEUE . . . . .	306
ENABLE SWITCH PORT FLOW . . . . .	307
ENABLE SWITCH PORT VLAN . . . . .	308
ENABLE SWITCH STPFORWARD . . . . .	309
PURGE EPSR . . . . .	310
PURGE LACP . . . . .	311
PURGE MSTP . . . . .	312
PURGE PORTAUTH PORT . . . . .	313
PURGE QOS . . . . .	314
PURGE STP . . . . .	315
RESET DHCP Snooping COUNTER . . . . .	316
RESET LACP PORT COUNTER . . . . .	317
RESET MSTP COUNTER PORT . . . . .	318
RESET PORTAUTH PORT . . . . .	319
RESET PORTAUTH PORT MULTIMIB . . . . .	320
RESET STP . . . . .	321

RESET SWITCH . . . . .	322
RESET SWITCH ACCELERATOR COUNTER . . . . .	323
RESET SWITCH PORT . . . . .	324
SET CLASSIFIER . . . . .	325
SET DHCP Snooping CHECKINTERVAL . . . . .	329
SET DHCP Snooping PORT . . . . .	330
SET EPSR . . . . .	332
SET EPSR PORT . . . . .	334
SET LACP PORT . . . . .	335
SET LACP . . . . .	336
SET MSTP . . . . .	338
SET MSTP CIST . . . . .	340
SET MSTP CIST PORT . . . . .	341
SET MSTP MSTI . . . . .	343
SET MSTP MSTI PORT . . . . .	344
SET PORTAUTH IDTOGGLE . . . . .	345
SET PORTAUTH PORT . . . . .	346
SET PORTAUTH PORT SUPPLICANTMAC . . . . .	350
SET PORTAUTH USERNAME . . . . .	353
SET QOS ACCELERATOR POLICY . . . . .	355
SET QOS DEFAULTPRIORITY . . . . .	356
SET QOS DSCP MAP . . . . .	357
SET QOS FLOWGROUP . . . . .	359
SET QOS POLICY . . . . .	361
SET QOS PORT . . . . .	365
SET QOS PORT EGRESSQUEUE . . . . .	367
SET QOS PRIO2QUEUE MAP . . . . .	369
SET QOS QUEUE2PRIOMAP . . . . .	370
SET QOS RED . . . . .	371
SET QOS TRAFFICCLASS . . . . .	373
SET STP . . . . .	377
SET STP PORT . . . . .	379
SET SWITCH AGEINGTIMER . . . . .	381
SET SWITCH CPUTXPRIORITY . . . . .	382
SET SWITCH CPUTXQUEUE . . . . .	383
SET SWITCH DLFLIMIT . . . . .	384
SET SWITCH MIRROR . . . . .	385
SET SWITCH NESTEDTPID . . . . .	386
SET SWITCH PORT . . . . .	387
SET SWITCH THRASHLIMIT . . . . .	391
SET SWITCH TRUNK . . . . .	392
SET VLAN PORT . . . . .	394

SHOW CLASSIFIER . . . . .	395
SHOW DHCP Snooping . . . . .	401
SHOW DHCP Snooping Counter . . . . .	403
SHOW DHCP Snooping Database . . . . .	405
SHOW DHCP Snooping Filter . . . . .	408
SHOW DHCP Snooping Port . . . . .	409
SHOW EPSR . . . . .	411
SHOW EPSR Counter . . . . .	414
SHOW EPSR Debug . . . . .	416
SHOW LACP . . . . .	417
SHOW LACP Port . . . . .	419
SHOW LACP Trunk . . . . .	423
SHOW MSTP . . . . .	425
SHOW MSTP CIST . . . . .	428
SHOW MSTP CIST Port . . . . .	431
SHOW MSTP Counter Port . . . . .	434
SHOW MSTP MSTI . . . . .	436
SHOW MSTP MSTI Port . . . . .	439
SHOW PortAuth . . . . .	441
SHOW PortAuth Counter . . . . .	444
SHOW PortAuth Multi-Subscriber Port . . . . .	447
SHOW PortAuth Port . . . . .	451
SHOW PortAuth Timer . . . . .	456
SHOW QoS Default Priority . . . . .	460
SHOW QoS DSCP Map . . . . .	461
SHOW QoS Flow Group . . . . .	463
SHOW QoS Policy . . . . .	465
SHOW QoS Port . . . . .	468
SHOW QoS Prio2Queue Map . . . . .	471
SHOW QoS Queue2Priomap . . . . .	472
SHOW QoS RED . . . . .	474
SHOW QoS Traffic Class . . . . .	477
SHOW STP . . . . .	480
SHOW STP Counter . . . . .	484
SHOW STP Debug . . . . .	486
SHOW STP Port . . . . .	487
SHOW Switch . . . . .	490
SHOW Switch Accelerator . . . . .	494
SHOW Switch Accelerator Counter . . . . .	496
SHOW Switch Accelerator HW Filter . . . . .	499
SHOW Switch Counter . . . . .	501
SHOW Switch FDB . . . . .	503



SHOW SWITCH FILTER . . . . .	505
SHOW SWITCH HWFILTER . . . . .	507
SHOW SWITCH PORT . . . . .	509
SHOW SWITCH PORT COUNTER . . . . .	513
SHOW SWITCH PORT INTRUSION . . . . .	516
SHOW SWITCH TRUNK . . . . .	517
SHOW VLAN . . . . .	519
SHOW VLAN PORT . . . . .	526

## 概要・基本設定

本製品はご購入時の状態でレイヤー 2 スイッチとして機能するように設定されています。単なるスイッチとして使用するだけであれば、特別な設定を行うことなく、設置・配線を行うだけで使用できます。しかし、レイヤー 3 スイッチとしての本製品の機能を十分に発揮するためには、レイヤー 3 スイッチとしての設定を施す必要があります。

## レイヤー 3 スイッチとしての設定手順

ここでは、レイヤー 3 スイッチとして使用するための基本的な設定手順について解説します。

### 1. VLAN の作成

ルーティング機能を有効にするには、最低でも 2 つの VLAN が必要です。ご購入時には 1 つしか VLAN が定義されていないので、新規に VLAN を作成する必要があります。

VLAN の作成は CREATE VLAN コマンド (225 ページ) で、ポートの割り当ては ADD VLAN PORT コマンド (191 ページ) で行います。

```
CREATE VLAN=white VID=10 ↵
CREATE VLAN=orange VID=20 ↵
ADD VLAN=white PORT=1-4 ↵
ADD VLAN=orange PORT=5-8 ↵
```

### 2. IP プロトコルモジュールの有効化

デフォルトでは IP モジュールは無効になっていますので、有効にしてください。これには、ENABLE IP コマンド (「IP」の 256 ページ) を使います。

```
ENABLE IP ↵
```

### 3. IP インターフェースの作成

VLAN に IP アドレスを割り当てることによって、VLAN 上に仮想的なルーターインターフェースが作成されます。

IP の場合は ADD IP INTERFACE コマンド (「IP」の 151 ページ) を使って VLAN インターフェースに IP アドレスとネットマスクを設定します。マルチホーミング機能を使用すれば、1 つの VLAN 上に最大 16 個までの論理インターフェースを作成できます。

```
ADD IP INT=vlan-white IP=172.20.1.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-orange IP=172.20.2.1 MASK=255.255.255.0 ↵
```

### 4. 経路設定

必要に応じて経路の設定を行います。

同一筐体上の VLAN だけで構成されたネットワークであれば、特別な経路設定は必要ありません。VLAN 上にレイヤー 3 インターフェースを作成した時点で、該当する VLAN へのダイレクト経路が

自動的に経路表に登録され、2つのインターフェースが作成された時点で VLAN 間ルーティングが有効になります。

これに対し、VLAN 上に本製品以外のルーターがあり、その先に別のネットワークが存在する場合は、それらのネットワークへの経路情報をなんらかの方法で登録する必要があります。経路情報の管理には手動で行う方法（スタティックルーティング）と半自動で行う方法（ダイナミックルーティング）があります。

- IP で経路を静的に登録するには、ADD IP ROUTE コマンド（「IP」の 160 ページ）を使います。外部への出口が 1 つしかないような場合は、デフォルトの経路を設定するのが一般的です。

```
ADD IP ROUTE=0.0.0.0 INT=vlan-white NEXTHOP=172.20.1.254 ↵
```

- IP で動的な経路制御を行うには、ダイナミックルーティングプロトコルの RIP（Routing Information Protocol）か OSPF（Open Shortest Path First）を使います。VLAN white と orange で RIP バージョン 2 を有効にするには次のようにします。

```
ADD IP RIP INT=vlan-white SEND=RIP2 RECEIVE=RIP2 ↵
```

```
ADD IP RIP INT=vlan-orange SEND=RIP2 RECEIVE=RIP2 ↵
```

基本設定は以上です。

## ポート

本製品のスイッチポートは、ご購入時の状態ですべてイネーブルに設定されており、互いに通信可能な状態にあります。スタンドアローンのレイヤー 2 スイッチとして使うのであれば、特別な設定は必要ありません。設置・配線を行うだけで使用できます。

## ポートの指定方法

スイッチポートに対する設定コマンドには、複数のポートを一度に指定できるものがあります。以下、指定するときの例を示します。

1 つのポートを指定

```
ENABLE SWITCH PORT=2 ↵
```

連続する複数のポートをハイフンで指定

```
ADD VLAN=black PORT=3-7 ↵
```

連続していない複数のポートをカンマで指定

```
SHOW SWITCH PORT=2,4,8 ↵
```

カンマとハイフンの組み合わせで指定

```
SHOW SWITCH PORT=2,4-7 ↵
```

すべてのポートを意味する特殊なキーワード ALL を指定

```
RESET SWITCH PORT=ALL COUNTER ↵
```

## 基本コマンド

スイッチポートに対して操作を行う基本的な設定コマンドを紹介します。詳細はコマンドリファレンスをご覧ください。

ポートをイネーブルにするには ENABLE SWITCH PORT コマンド (304 ページ) を使います。

```
ENABLE SWITCH PORT=8 ↵
```

ポートをディセーブルにするには DISABLE SWITCH PORT コマンド (274 ページ) を使います。

```
DISABLE SWITCH PORT=8 ↵
```

ポートの通信モード (通信速度とデュプレックスモード) を変更するには SET SWITCH PORT コマンド (387 ページ) の SPEED パラメーターを使います。デフォルトは AUTONEGOTIATE (オートネゴシエーション) です。

```
SET SWITCH PORT=2 SPEED=100MHALF ↵
```

- ☞ 通信モードを AUTONEGOTIATE 以外に設定すると、該当ポートでは MDI/MDI-X 自動切替が無効になります。その後、再度 AUTONEGOTIATE に設定すると、MDI/MDI-X 自動切替は有効になります。

強制的にオートネゴシエーションを行わせるには ACTIVATE SWITCH PORT AUTONEGOTIATE コマンド (171 ページ) を使います。通信モードが AUTONEGOTIATE のポートでのみ有効です。

```
ACTIVATE SWITCH PORT=8 AUTONEGOTIATE ↵
```

デフォルトでは、すべてのポートで MDI/MDI-X 自動切替が有効になっています。MDI/MDI-X 自動切替を無効にするには、DISABLE SWITCH PORT AUTOMDI コマンド (275 ページ) を実行します。

```
DISABLE SWITCH PORT=1 AUTOMDI ↵
```

MDI/MDI-X 自動切替を無効にした直後のポートは、MDI-X 固定になります。MDI/MDI-X 自動切替が無効なポートで MDI/MDI-X を変更するには、SET SWITCH PORT コマンド (387 ページ) の POLARITY パラメーターを使います。

```
SET SWITCH PORT=1 POLARITY=MDI ↵
```

ポートをハードウェア的にリセットするには RESET SWITCH PORT コマンド (324 ページ) を使います。

```
RESET SWITCH PORT=3,6 ↵
```

- ☞ 本コマンドは、SFP ポートに対しては機能しません。

ポートの状態を確認するには SHOW SWITCH PORT コマンド (509 ページ) を使います。

```
SHOW SWITCH PORT ↵
```

ポートの送受信統計を見るには SHOW SWITCH PORT COUNTER コマンド (513 ページ) を使います。

```
SHOW SWITCH PORT=12 COUNTER ↵
```

ポートの統計カウンターをクリアするには RESET SWITCH PORT コマンド (324 ページ) に COUNTER オプションをつけて実行します。COUNTER オプションをつけないと、ポートがハードウェア的にリセットされてしまうので注意してください (カウンターもクリアされる)。

```
RESET SWITCH PORT=ALL COUNTER ↵
```

## ポートランキング

ポートランキングは複数の物理ポートを束ねてスイッチ間の帯域幅を拡大する機能です。束ねたポートはトランクグループと呼ばれ、論理的に 1 本のポートとして扱われます。また、トランクグループ内のポート

に障害が発生しても残りのポートで通信が継続できるため、信頼性の向上にも貢献します。

- ✎ 本製品はトランクグループを動的に設定する LACP ( IEEE 802.3ad Link Aggregation Control Protocol ) にも対応しています。LACP については、「スイッチング」の「LACP ( IEEE 802.3ad )」をご覧ください。

作成できるトランクグループの数は最大 12 ( LACP により自動設定されたトランクグループを含む )、トランクグループの所属ポート数は最大 4 となります。グループ内のポートは隣接していなくてもかまいません。ポートトラッキングを使用するために最低限必要な設定について説明します。ここでは、ポート 1~4 を束ねて使用するものとします。

1. トランクグループ「aggr1」を作成します。グループ名は自由につけられますが、「LACP」で始まる名前は、LACP ( Link Aggregation Control Protocol ) によって自動生成されたトランクグループ用に予約されているため使用できません。

```
CREATE SWITCH TRUNK=aggr1 ↵
```

2. トランクグループにポートを追加します。束ねるポートはこの時点で同じ VLAN に所属していなくてはなりません。

```
ADD SWITCH TRUNK=aggr1 PORT=1-4 ↵
```

基本設定は以上です。

- ✎ トランクグループの所属ポートは、すべて同一の VLAN 設定である必要があります。すべての所属ポートは、同一 VLAN の所属で、同一のタグ設定 ( TAGGED か UNTAGGED ) にする必要があります。VLAN への追加・削除は、トランクグループの所属ポートすべてを一単位として行ってください。所属ポートのタグ設定を変更するときも同様です。
- ✎ トランクグループは、すべて同一メディアタイプのポートで構成してください。たとえば、トランクグループ内に 1000BASE-SX ポートと 1000BASE-LX ポートを混在させるような構成はサポート対象外です。
- ✎ ポートトラッキングの設定は、トランクポートによって接続される両方のスイッチで行う必要があります。
- ✎ ポートトラッキングとオーバーラップ STP、ポートトラッキングとポート認証は併用できません ( トランクポートでは、オーバーラップ STP、ポート認証を使用できません )。

トランクグループの情報は SHOW SWITCH TRUNK コマンド ( 517 ページ ) で確認できます。

```
SHOW SWITCH TRUNK=aggr1 ↵
```

トランクグループに追加されたポートの通信モードは、SPEED パラメーターで指定した速度のオートネゴシエーション ( AUTONEGOTIATE ) となります。個別ポートの設定はトランクグループに参加した時点で上書きされますが、内部的には保持されており、グループから抜けると元の設定に戻ります。

トランクグループ内のどのポートからパケットを送出するかは、L2、L3、L4 ヘッダーの情報に基づいて決定されます。ENABLE SWITCH HASH コマンド ( 300 ページ )、DISABLE SWITCH HASH コマンド ( 270 ページ ) を使うと、送出口決定に使うヘッダー情報を制御できます。

デフォルトでは、L2 と L3 のヘッダー情報を使って送出口を決定しますが、L4 のヘッダー情報も使う

ようにしたければ、次のようにします。

```
ENABLE SWITCH HASH=L4 ↵
```

- ルーター後トランクグループから送信される IP パケットの送出ポートは、ENABLE SWITCH HASH コマンド (300 ページ) \ DISABLE SWITCH HASH コマンド (270 ページ) の設定とは関係なく、L3 ヘッダー情報にのみ基づいて決定されます。その他のパケットには、同コマンドの設定が適用されます。

トランクグループからポートを削除するには DELETE SWITCH TRUNK コマンド (238 ページ) を使います。

```
DELETE SWITCH TRUNK=aggr1 PORT=4 ↵
```

トランクグループを削除するには DESTROY SWITCH TRUNK コマンド (251 ページ) を使います。所属ポートがあるときは削除できません。その場合は、先に DELETE SWITCH TRUNK コマンド (238 ページ) で所属ポートを削除してください。

```
DELETE SWITCH TRUNK=aggr1 PORT=ALL ↵
```

```
DESTROY SWITCH TRUNK=aggr1 ↵
```

## ポートミラーリング

ポートミラーリングは、特定のポートを通過するトラフィックをあらかじめ指定したミラーポートにコピーする機能です。パケットを必要なポートにだけ出力するスイッチではパケットキャプチャーなどが困難ですが、ポートミラーリングを利用すれば、任意のポートのトラフィックをミラーポートでキャプチャーすることができます。

なお、ポートミラーリング機能の仕様は以下のようになっています。

- パケットはすべてタグなし状態でミラーポートに出力されます。
- 不正なパケット (エラーパケットなど) はミラーされません。

### 基本設定

ここではポート 1 をミラーポートに設定し、ポート 5 から送受信されるトラフィックがミラーポートにコピーされるようにします。

- ミラーポートを指定します。指定できるのは VLAN default 所属のポートだけです。ミラーポートに指定したいポートが VLAN default 以外に所属している場合は、最初に現在所属の VLAN から削除し VLAN default の所属に戻した上で、SET SWITCH MIRROR コマンド (385 ページ) を実行します。

```
DELETE VLAN=somevlan PORT=1 ↵
```

SET SWITCH MIRROR コマンド (385 ページ) を実行すると、指定ポートはミラーポートとして設定され、どの VLAN にも属していない状態となります。

```
SET SWITCH MIRROR=1 ↵
```

すでにミラーポートとして設定されているポートがあった場合、本コマンド実行によりそのポートは VLAN default 所属のタグなしポートとなります。

✎ トランクグループに参加しているポートをミラーポートに設定することはできません。

✎ ミラーポートに設定されたポートは通常のスイッチポートとしては機能しません。

## 2. ポートミラーリング機能を有効にします。

```
ENABLE SWITCH MIRROR ↵
```

## 3. ソースポートとトラフィックの向きを指定します。ここではポート 5 から送受信されるトラフィックをミラーポートにコピーします。

```
SET SWITCH PORT=5 MIRROR=BOTH ↵
```

✎ 複数のポートをミラーしたいときは、SET SWITCH PORT コマンド (387 ページ) を複数回実行してください。ただし、ミラーリング対象ポートを増やすことはパフォーマンス低下につながりますのでご注意ください。

設定は以上です。

ポートミラーリングの設定を確認するには SHOW SWITCH コマンド (490 ページ) を実行します。ミラーポートは SHOW VLAN コマンド (519 ページ) の「Mirror Port」欄でも確認できます。また、ソースポートとミラー対象トラフィックは SHOW SWITCH PORT コマンド (509 ページ) の「Mirroring」欄でも確認できます。

ポートミラーリング機能を無効にするには DISABLE SWITCH MIRROR コマンド (273 ページ) を実行します。

```
DISABLE SWITCH MIRROR ↵
```

ミラーポートの設定を解除するには SET SWITCH MIRROR コマンド (385 ページ) に NONE を指定します。設定を解除されたポートは VLAN default 所属のタグなしポートに戻ります。

```
SET SWITCH MIRROR=NONE ↵
```

ソースポートでのミラーリングをやめるには SET SWITCH PORT コマンド (387 ページ) の MIRROR パラメーターに NONE を指定します。

```
SET SWITCH PORT=5 MIRROR=NONE ↵
```

ミラーポートに設定されたポートは通常のスイッチポートとしては機能しません。SET SWITCH MIRROR コマンド (385 ページ) を実行した時点で、ミラーポートはいずれの VLAN にも所属していない状態となります。



## ポートセキュリティ

ポートセキュリティは、MAC アドレスに基づき、ポートごとに通信を許可するデバイスを制限する機能です。許可していないデバイスからパケットを受信したときには、パケットを破棄する、SNMP トラップを上げるなどのアクションを実行させることができます。

本機能は、SET SWITCH PORT コマンド (387 ページ) の LEARN パラメーターで、ポートごとに学習可能な MAC アドレス数の上限 (1~256 個) を設定することによって有効になります。学習済みの MAC アドレスが制限値に達すると、それ以降に受信した未学習の送信元 MAC アドレスを持つパケットを不正なものとし、あらかじめ指定されたアクションを実行します。

アクションには次の種類があります (SET SWITCH PORT コマンド (387 ページ) の INTRUSIONACTION パラメーターで指定)

アクション名	動作
DISCARD	不正なパケットを破棄する。
TRAP	不正なパケットを破棄し、SNMP トラップを送信する (トラップは各 MAC アドレスに対して最初の一回だけ送信)。
DISABLE	不正なパケットを破棄し、SNMP トラップを送信した後、該当ポートをディセーブルにする。

表 1:

✎ ポートセキュリティが有効なポートでは、ポート認証を使用できません。

✎ ポートセキュリティと VRRP の併用は可能ですが、VRRP パケットを送受信するポートではポートセキュリティを有効にしないでください。有効にすると、VRRP が正しく動作しないことがあります。

ポートに学習可能な MAC アドレスの最大数と不正パケット受信時のアクションを設定するには、SET SWITCH PORT コマンド (387 ページ) を使います。たとえば、ポート 11 の MAC アドレス学習数の上限を 20 個、アクションを DISABLE に設定するには次のようにします。

```
SET SWITCH PORT=11 LEARN=20 INTRUSIONACTION=DISABLE ↵
```

SET SWITCH PORT コマンド (387 ページ) で LEARN パラメーターを設定すると、すでに同ポートで学習していたアドレスエントリ (ダイナミックエントリ) がフォワーディングデータベースから削除され、エントリなしの状態からアドレス学習が開始されます。

上限が設定されているときに学習した MAC アドレスの扱いは、SET SWITCH PORT コマンド (387 ページ) の RELEARN パラメーターの設定によって異なります。

- RELEARN パラメーターが ON のとき (ダイナミックポートセキュリティ)、学習した MAC アドレスはダイナミック MAC アドレスとして扱われ、エージングによって削除されます (Dynamic Limited モード)。
- RELEARN パラメーターが OFF のとき (通常のポートセキュリティ) は、学習した MAC アドレスはスタティック MAC アドレスとして扱われ、エージングによって削除されません (Limited モード)。

デフォルトでは、RELEARN パラメーターは OFF で、学習した MAC アドレスはスタティック MAC アド

レスとして扱われ、エージングによって削除されません。

学習アドレス数が上限に達すると、それ以降に受信した未知のアドレスからのパケットは「不正」なものとなされ、INTRUSIONACTION で指定したアクションが実行されます。

たとえば、アクションが「DISABLE」に設定されているときに不正パケットを受信すると、トラップ送信とポートのディセーブルが実行され、コンソール画面に次のように表示されます。

```
Manager >
Intrusion TRAP for 00-05-02-69-a0-49 port 11

Intrusion event.  Disabling port 11
```

学習済みのアドレスを確認するには、SHOW SWITCH FILTER コマンド (505 ページ) を使います。ポートセキュリティがオンのポートで学習されたアドレスは、Source 欄に「Learn」と表示されます。

```
SHOW SWITCH FILTER ↓
```

```
SHOW SWITCH FILTER PORT=11 ↓
```

ポートセキュリティの設定状況は SHOW SWITCH PORT コマンド (509 ページ) で確認できます。「Learn limit」欄には現在設定されている上限が、「Intrusion action」欄には不正パケット受信時のアクションが表示されます。また、「Current learned, lock state」欄には、現在までに学習したアドレスの数と、ポートがロック (これ以上学習しない状態のこと) されているかどうかが表示されます。「Relearn」欄には、LEARN パラメーターを設定した場合に、学習した MAC アドレスがエージングの対象であるかどうかが表示されます。

```
SHOW SWITCH PORT ↓
```

```
SHOW SWITCH PORT=11 ↓
```

不正とみなされた MAC アドレスは SHOW SWITCH PORT INTRUSION コマンド (516 ページ) で確認できます。

```
SHOW SWITCH PORT INTRUSION ↓
```

```
SHOW SWITCH PORT=11 INTRUSION ↓
```

学習済みアドレス数が上限に達する前に手動でポートをロックするには ACTIVATE SWITCH PORT LOCK コマンド (172 ページ) を使います。あらかじめ SET SWITCH PORT コマンド (387 ページ) で上限とアクションを設定した上で、ポートをロックします。

```
SET SWITCH PORT=ALL LEARN=256 INTRUSIONACTION=DISCARD ↓
```

```
ACTIVATE SWITCH PORT=ALL LOCK ↓
```

ポートセキュリティがオンのポート (学習可能アドレスに上限が設定されているポート) に対して、通信を許可するアドレスを手動登録するには、ADD SWITCH FILTER コマンド (186 ページ) に LEARN オ

プションを付けて実行します。すでに上限に達している場合であっても、本コマンドで手動追加した場合は上限値が引き上げられます。

```
ADD SWITCH FILTER DESTADDR=00-00-f4-88-88-88 PORT=11 ACTION=FORWARD
LEARN ↵
```

- ☞ LEARN オプションを付け忘れると通常のスタティックエントリとなり、ポートセキュリティ機能における「学習済みアドレス」としてはカウントされませんのでご注意ください。

スタティックエントリの削除は DELETE SWITCH FILTER コマンド (236 ページ) で行います。ENTRY 番号は SHOW SWITCH FILTER コマンド (505 ページ) で確認してください。

```
DELETE SWITCH FILTER ENTRY=3 PORT=11 ↵
```

ポートのロックを解除する、あるいはポートセキュリティ機能をオフにするには、SET SWITCH PORT コマンド (387 ページ) でアドレス学習の上限値 (LEARN パラメーター) に 0 (無制限) を設定します。ポートセキュリティがオンのときに学習されたエントリは、システムの再起動とともにデータベースから削除されます。

```
SET SWITCH PORT=11 LEARN=0 ↵
```

ポートセキュリティ機能のアクションによってディセーブルにされたポートは ENABLE SWITCH PORT コマンド (304 ページ) ではイネーブルに戻せません。この場合は、SET SWITCH PORT コマンド (387 ページ) の LEARN パラメーターに 0 を指定してポートセキュリティをオフにすると、イネーブルに戻ります。

```
Manager > enable switch port=11
```

```
Error (387312): Port 11 has been disabled by the Port Security feature.
```

- ☞ RELEARN パラメーターが ON のときは、学習アドレス数がいったん上限に達しても、エージングにより再度上限を下回ることがありますが、INTRUSIONACTION に DISABLE を指定した場合は、学習アドレス数が上限を下回っても、ポートが自動的にイネーブルになることはありません。

ポートセキュリティの状態 (学習済みアドレスやポートの状態) は CREATE CONFIG コマンド (「運用・管理」の 159 ページ) によって保存されます (SET SWITCH PORT コマンド (387 ページ) の RELEARN パラメーターが OFF の場合)。

## ループガード

本製品ではループガードとして以下の機能をサポートしています。

- MAC アドレススラッシングプロテクション
- パケットストームプロテクション

## MAC アドレススラッシングプロテクション

MAC アドレススラッシングプロテクションは、意図せぬループ構成などによって発生する MAC アドレススラッシング（同一 MAC アドレスの登録ポートが頻繁に変更される現象）を検出した場合に、関連するポートで MAC アドレスの学習やリンク状態を制御して、過負荷を回避するための機能です。MAC アドレススラッシングを検出した場合の動作や、検出後の対応動作の持続時間は、ポート、スタティックおよび LACP によって自動生成されたトランクグループ単位で設定します。

LEARNDISABLE	MAC アドレスの学習を停止する
PORTDISABLE	ポートまたはトランクグループをディセーブルにする
VLANDISABLE	該当する VLAN に対してのみポートまたはトランクグループをディセーブルにする
LINKDOWN	ポートまたはトランクグループ内の全ポートを物理的にリンクダウンさせる
NONE	なにもしない

表 2: MAC アドレススラッシング検出時の動作

ポート単位での動作設定は SET SWITCH PORT コマンド（387 ページ）で行います。ここでは、ポートグループ 1～8 に対して、MAC アドレススラッシング検出時に、スラッシングが発生した VLAN に対してのみポートをディセーブルにするよう設定します。

```
SET SWITCH PORT=1-8 THRASHACTION=VLANDISABLE ↵
```

MAC アドレススラッシングに対する動作の持続時間を 1～86400 秒の範囲または NONE（無期限）で指定します。ここでは持続時間を 5 秒に設定します。

```
SET SWITCH PORT=1-8 THRASHTIMEOUT=5 ↵
```

スタティックなトランクグループへの動作設定は、CREATE SWITCH TRUNK コマンド（223 ページ）か SET SWITCH TRUNK コマンド（392 ページ）で行います。次の例では、既存のトランクグループ「uplink」に対して設定を行っています。

```
SET SWITCH TRUNK=uplink THRASHACTION=LEARNDISABLE THRASHTIMEOUT=5 ↵
```

LACP によって自動生成されるトランクグループへの動作設定は、SET LACP コマンド（336 ページ）で行います。

```
SET LACP THRASHACTION=PORTDISABLE THRASHTIMEOUT=5 ↵
```

本製品全体に対する MAC アドレススラッシングの検出しきい値の設定は、SET SWITCH THRASHLIMIT コマンド（391 ページ）で行います。ここでは、1 秒間に 10 回以上の変更を検出した場合にスラッシングと見なすよう設定します。

```
SET SWITCH THRASHLIMIT=10 ↵
```

## パケットストームプロテクション

パケットストームプロテクションは、ブロードキャスト/マルチキャスト/未学習のユニキャストパケットの受信レートに上限を設定し、パケットストームを防止するための機能です。設定値を上回るレートでこれらのパケットを受信した場合、超過分のパケットは破棄されます。本機能はデフォルトではオフになっています。

ブロードキャスト・マルチキャストパケットに対しては、スイッチポートごとに上限値を設定できます（ブロードキャストとマルチキャストの上限値は共通）。一方、未学習のユニキャストパケットに対しては、システム全体で1つだけ上限値を設定できます。

各パケットの受信レートに上限値を設定するには、次のコマンド・パラメーターを使います。

- ブロードキャストパケット (SET SWITCH PORT コマンド (387 ページ) の BCLIMIT パラメーター)
- マルチキャストパケット (SET SWITCH PORT コマンド (387 ページ) の BCLIMIT パラメーター)
- 未学習ユニキャストパケット (SET SWITCH DLFLIMIT コマンド (384 ページ))

ブロードキャストパケットの受信レートを制限するには、SET SWITCH PORT コマンド (387 ページ) の BCLIMIT パラメーターを使います。たとえば、ポート 1 に対して、ブロードキャストパケットの受信レートを 1 秒あたり 1000Kbyte に制限するには、次のようにします。

```
SET SWITCH PORT=1 BCLIMIT=1000 ↵
```

マルチキャストパケットの受信レート上限値は、ブロードキャストパケットの受信レート上限値と同じになります。ただし、マルチキャストパケットの受信レート制限は、ENABLE SWITCH MCLIMITING コマンド (302 ページ) を実行するまで有効になりません。

```
ENABLE SWITCH MCLIMITING ↵
```

- ☞ SET SWITCH PORT コマンド (387 ページ) の BCLIMIT パラメーターで受信レートを指定しても、ENABLE SWITCH MCLIMITING コマンド (302 ページ) を実行するまでは、ブロードキャストパケットだけが制限され、マルチキャストパケットは制限されませんのでご注意ください。また、マルチキャストパケットだけを制限し、ブロードキャストパケットは制限しないという設定はできません。

ブロードキャスト・マルチキャストパケットの受信レート制限を解除するには、BCLIMIT パラメーターの値として NONE を指定します。

```
SET SWITCH PORT=1 BCLIMIT=NONE ↵
```

ブロードキャストパケットは制限するが、マルチキャストパケットは制限しないようにするには、DISABLE SWITCH MCLIMITING コマンド (272 ページ) を実行します。

```
DISABLE SWITCH MCLIMITING ↵
```

未学習ユニキャストパケットの受信レートを制限するには、SET SWITCH DLFLIMIT コマンド (384 ページ) を使います。たとえば、未学習ユニキャストパケットの受信レートを 1 秒あたり 1000Kbyte に制限するには、次のようにします。ブロードキャスト・マルチキャストパケットとは異なり、こちらはシステム全体に適用されます。

```
SET SWITCH DLFLIMIT=1000 ↓
```

未学習ユニキャストパケットの受信レート制限を解除するには、DLFLIMIT パラメーターの値として NONE を指定します。

```
SET SWITCH DLFLIMIT=NONE ↓
```

ブロードキャスト・マルチキャストパケットの受信レート上限値設定は、SHOW SWITCH PORT コマンド (509 ページ) で確認できます。「BCast & MCast rate limit」、「BCSC rate limiting」をご覧ください。

未学習ユニキャストパケットの受信レート上限値設定は、SHOW SWITCH コマンド (490 ページ) で確認できます。「DLF rate limit」をご覧ください。

## ポート帯域制限機能

本製品は、スイッチポートごとに送信レートを制限することができます。

帯域制限の設定は SET SWITCH PORT コマンド (387 ページ) の EGRESSLIMIT (送信レート) パラメーターで行います。

ポート 1 の送信レートを 50Mbps に制限するには、次のように指定します。EGRESSLIMIT の単位は Kbps です。

```
SET SWITCH PORT=1 EGRESSLIMIT=50000 ↓
```

- ✎ EGRESSLIMIT パラメーターに指定できる値の範囲は 0 ~ 2641248Kbps ですが、648 の倍数でない場合は倍数になるよう丸められるので注意してください。
- ✎ EGRESSLIMIT=0 は、EGRESSLIMIT=NONE (制限なし) と同じ意味になります。
- ✎ ポート帯域制限機能と QoS の重み付きラウンドロビン (WRR) スケジューリング (SET QOS PORT EGRESSQUEUE コマンド (367 ページ) の SCHEDULER パラメーターで設定) は併用できません。

ポートの帯域制限を解除するには値として NONE または 0 を指定します。

```
SET SWITCH PORT=1 EGRESSLIMIT=NONE ↓
```

ポート帯域制限機能の設定状況は SHOW SWITCH PORT コマンド (509 ページ) で確認できます。「Egress rate limit」をご覧ください。

## トリガー

トリガー機能を使用すると、スイッチポートのリンクアップ、リンクダウン時に任意のスクリプトを実行さ

せることができます。

スイッチポートのリンクアップ、リンクダウンは、スイッチングモジュール固有のモジュールトリガーを使って捕捉します。

CREATE TRIGGER MODULE コマンド（「運用・管理」の 174 ページ） SET TRIGGER MODULE コマンド（「運用・管理」の 334 ページ）に、スイッチングモジュール固有のパラメーターを加えたコマンド構文は次のようになります。

```
CREATE TRIGGER=trigger-id MODULE=SWITCH EVENT={LINKDOWN|LINKUP} PORT=port
  [AFTER=time] [BEFORE=time] [{DATE=date|DAYS=day-list}] [NAME=string]
  [REPEAT={YES|NO|ONCE|FOREVER|count}] [SCRIPT=filename...]
  [STATE={ENABLED|DISABLED}] [TEST={YES|NO|ON|OFF}]
```

```
SET TRIGGER=trigger-id PORT=port [AFTER=time] [BEFORE=time]
  [{DATE=date|DAYS=day-list}] [NAME=string]
  [REPEAT={YES|NO|ONCE|FOREVER|count}] [TEST={YES|NO|ON|OFF}]
```

PORT パラメーターにはスイッチポートの番号を、EVENT パラメーターには LINKDOWN（リンクダウン）か LINKUP（リンクアップ）のいずれかを指定します。

このトリガーは、PORT パラメーターで指定したスイッチポートがリンクアップするか（EVENT=LINKUP のとき）、リンクダウンするか（EVENT=LINKDOWN のとき）したときに起動されます。

トリガーから実行されるスクリプトには、特殊な引数として %D（日付）、%T（時刻）、%N（システム名）、%S（シリアル番号）が渡されます。また、引数 %1 としてスイッチポートの番号も渡されます。

次に例を示します。ここでは、スイッチポート 3 がリンクダウンしたら linkdown.scp を、リンクアップしたら linkup.scp を実行するように設定します。これらのスクリプトでは、MAIL コマンド（「運用・管理」の 266 ページ）を使って管理者にメールで通知するようにします。

なお、IP やメールの設定はすでにしているものと仮定します。IP の設定については「IP」の章をご覧ください。また、メールの設定については「運用・管理」の「メール送信」をご覧ください。

1. トリガー機能を有効にします。

```
ENABLE TRIGGER ↵
```

2. リンクダウン時に linkdown.scp を実行するトリガー「1」を作成します。

```
CREATE TRIGGER=1 MODULE=SWITCH EVENT=LINKDOWN PORT=3
  SCRIPT=linkdown.scp ↵
```

3. リンクアップ時に linkup.scp を実行するトリガー「2」を作成します。



```
CREATE TRIGGER=2 MODULE=SWITCH EVENT=LINKUP PORT=3  
SCRIPT=linkup.scp ↵
```

#### スクリプト「linkdown.scp」

```
MAIL TO=admin@is.example.com SUBJECT="%N #%1 linkdown" MES-  
SAGE="%D %T %N(SN:%S) Port %1 linkdown"
```

#### スクリプト「linkup.scp」

```
MAIL TO=admin@is.example.com SUBJECT="%N #%1 linkup" MES-  
SAGE="%D %T %N(SN:%S) Port %1 linkup"
```

ここではトリガースクリプト起動時に渡される特別な引数を使って、スイッチのシステム名（%N）やシリアル番号（%S）、日時（%D、%T）をメールのサブジェクトと本文に埋め込んでいます。次に、メールメッセージの例を示します。

```
Subject: ud-sw #3 linkdown  
From: manager@ud-sw.example.com  
To: <admin@is.example.com>  
Date: Thu, 23 May 2002 19:02:41  
  
23-May-2002 19:02:41 ud-sw(SN:40896093) Port 3 linkdown
```



## LACP (IEEE 802.3ad)

LACP (IEEE 802.3ad Link Aggregation Control Protocol) は、対向するポート間でネゴシエーションを行い、トランクグループを自動的に設定する機能です。

- ✎ LACP では、トランクグループを「リンクアグリゲーショングループ (LAG)」と呼びますが、本マニュアルでは原則的に「トランクグループ」を使用します。

- ✎ トランクグループの手動設定については、「スイッチング」の「ポート」をご覧ください(「ポートトランッキング」)。

LACP によって自動設定されたトランクグループは、手動設定したトランクグループと同じように、論理的に 1 本のポートとして扱われます。また、トランクグループ内のポートに障害が発生しても残りのポートで通信が継続できるため、信頼性の向上にも貢献します。

LACP では、次の条件をすべて満たすポート群が同一のトランクグループを構成する候補となります。

- 対向機器が同じ (同じ相手と接続されているポート群)
- 所属 VLAN が同じ (同じ VLAN に所属しているポート群)
- 通信速度が同じ (同じ通信速度で動作しているポート群)
- ポート鍵が同じ (同じポート鍵が設定されているポート群)

- ✎ トランクグループは、すべて同一メディアタイプのポートで構成してください。たとえば、トランクグループ内に 1000BASE-SX ポートと 1000BASE-LX ポートを混在させるような構成はサポート対象外です。

作成できるトランクグループの数は最大 12 (手動で設定したトランクグループを含む) トランクグループの所属ポート数は最大 4 となります。グループ内のポートは隣接していなくてもかまいません。

前記の条件を満たすポートが 5 ポート以上ある場合は、以下の基準にしたがってメンバーポートが 4 ポート選択されます。

1. ポートプライオリティーがもっとも小さいポート
2. ポートプライオリティーが等しい場合は、ポート番号の小さいポート

選択されなかったポートはスタンバイ状態となり、メンバーポートがリンクダウンしたときに備えて待機します。メンバーポートがリンクダウンしたときはスタンバイ状態のポートが自動的に昇格し、リンクダウンしていた旧メンバーポートが再度リンクアップしたときは、旧メンバーポートがメンバーに復帰します。

なお、以下のポートでは LACP を使用できません。これらのポートは、自動的に LACP の管理下から除外されます。

- 手動設定したトランクポート (CREATE SWITCH TRUNK コマンド (223 ページ) ADD SWITCH TRUNK コマンド (190 ページ))
- Half Duplex で動作しているポート

## 基本設定

LACP を使用するには、ENABLE LACP コマンド (286 ページ) を実行して LACP モジュールを有効にします (デフォルトは無効)。デフォルトでは、すべてのポートが LACP の管理下に置かれているため、

LACP モジュールを有効化すると、前述の条件を満たすポート群がトランクグループに束ねられます。

```
ENABLE LACP ↓
```

前述のとおり、デフォルトではすべてのポートで LACP が有効になっていますが、通常は特定のポートでのみ LACP を有効化して使います。たとえば、ポート 1~4 でのみ LACP を有効化するには、DELETE LACP PORT コマンド ( 229 ページ ) を使って、それ以外のポートを LACP の管理下から外します。

```
DELETE LACP PORT=5-24 ↓
```

あるいは、もう少し直感的な方法として、次のように指定することもできます。

```
DELETE LACP PORT=ALL ↓
```

```
ADD LACP PORT=1-4 ↓
```

1 つのトランクグループで同時に使用できるポート数は最大 4 ポートですが、より多くのポートで LACP を有効化しておくことにより、冗長性をさらに高めることが可能です。たとえば、ポート 1~6 で LACP を有効化するには次のようにします。

```
DELETE LACP PORT=ALL ↓
```

```
ADD LACP PORT=1-6 ↓
```

このように設定すると、通常時はポート 1~4 がメンバーポートに選択され、ポート 5、6 はスタンバイ状態となります。ここでポート 1 に障害が発生すると、ポート 5 がメンバーに選択されます。ポート 1 が復帰すると、再びポート 1 がメンバーに選択され、ポート 5 はスタンバイ状態に戻ります。

LACP モジュールの状態は、SHOW LACP コマンド ( 417 ページ ) で確認できます。

```
SHOW LACP ↓
```

LACP の管理下にあるポートの情報は、SHOW LACP PORT コマンド ( 419 ページ ) で確認できます。

```
SHOW LACP PORT ↓
```

```
SHOW LACP PORT=1 ↓
```

LACP によって自動生成されたトランクグループの情報は、SHOW LACP TRUNK コマンド ( 423 ページ ) で確認できます。また、SHOW SWITCH TRUNK コマンド ( 517 ページ ) でも確認できます。

```
SHOW LACP TRUNK ↓
```

```
SHOW SWITCH TRUNK ↓
```

✎ LACP の設定は、対向する両方のスイッチで行う必要があります。

✎ LACP とオーバーラップ STP、LACP とポート認証、LACP と IP マルチキャスト関連機能 ( DVMRP、PIM、IGMP/IGMP Snooping、MLD Snooping ) は併用できません ( LACP によって生成されたトランクポートでは、オーバーラップ STP、ポート認証、IP マルチキャスト関連機能を使用できません )。

トランクグループ内のどのポートからパケットを送出するかは、L2、L3、L4 ヘッダーの情報に基づいて決定されます。ENABLE SWITCH HASH コマンド ( 300 ページ )、DISABLE SWITCH HASH コマンド ( 270 ページ ) を使うと、送出ポート決定に使うヘッダー情報を制御できます。

デフォルトでは、L2 と L3 のヘッダー情報を使って送出ポートを決定しますが、L4 のヘッダー情報も使うようにしたければ、次のようにします。

ENABLE SWITCH HASH=L4 ↵

✎ ルーティング後トランクグループから送信される IP パケットの送出ポートは、ENABLE SWITCH HASH コマンド ( 300 ページ )、DISABLE SWITCH HASH コマンド ( 270 ページ ) の設定とは関係なく、L3 ヘッダー情報にのみ基づいて決定されます。その他のパケットには、同コマンドの設定が適用されます。

## バーチャル LAN

バーチャル LAN (VLAN) は、スイッチの設定によって論理的にブロードキャストドメインを分割する機能です。レイヤー 2 スイッチは、宛先 MAC アドレスとフォワーディングデータベースを用いて不要なトラフィックをフィルタリングする機能を持っていますが、未学習の宛先 MAC アドレスを持つユニキャストパケットと、マルチキャスト/ブロードキャストパケットは全ポートに出力します。VLAN を作成して、頻繁に通信を行うホスト同士をグループ化することにより、不要なトラフィックの影響を受ける範囲を限定し、帯域をより有効に活用できるようになります。


### 概要

本製品がサポートする基本的な VLAN は次の 3 種類です。

- ポート VLAN (タグ VLAN を含む)
- IP サブネット VLAN
- プロトコル VLAN

さらに、レイヤー 2 スイッチとしての動作を前提とした特殊な VLAN として次の 2 種類があります。

- マルチプル VLAN (Private VLAN)
- ダブルタグ VLAN (Nested VLAN)

 ダブルタグ VLAN (Nested VLAN) は別売のフィーチャーライセンス AT-FL-09 または AT-FL-09-B が必要です。

この章では、最初に基本的な VLAN について解説し、その後で特殊な VLAN について解説します。

### ポートと VLAN

スイッチポートは少なくとも 1 つのポート VLAN に所属していなくてはなりません (ミラーポートを除く)。また、ポートは複数の VLAN に所属できますが、所属先 VLAN の種類によって、いくつかの VLAN に所属できるかが異なります。基本ルールは次のとおりです。

- ポート VLAN (タグなしポート): 1 つの VLAN にだけ所属できます
- ポート VLAN (タグ付きポート): 複数の VLAN に所属できます
- IP サブネット VLAN (タグなしポート): 複数の VLAN に所属できます
- プロトコル VLAN (タグなしポート): 複数の VLAN に所属できます

ポートを IP サブネット VLAN、プロトコル VLAN に所属させる場合、該当ポートをあらかじめ任意のポート VLAN にタグなしポートとして参加させておく必要があります。

ポートが複数の VLAN に所属している場合、受信パケットの所属先は次の基準にしたがって決定されます。スイッチポートがどの VLAN に所属しているかは、SHOW VLAN PORT コマンド (526 ページ) で確認できます。

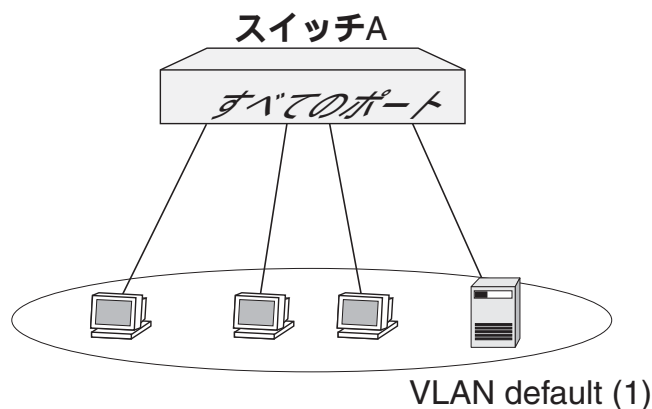
1. タグ付きパケットの VID と、ポートが所属しているタグ付きポート VLAN メンバーの VID が合致する場合、該当 VLAN の所属と判断します。

2. タグなしパケットの始点 IP アドレスが IP サブネット VLAN のサブネット範囲に合致する場合、IP サブネット VLAN の所属と判断します。
3. タグなしパケットの L3 プロトコルタイプがプロトコル VLAN の対象プロトコルに合致する場合、プロトコル VLAN の所属と判断します。
4. 上記の基準に当てはまらないタグなしパケットは、ポート VLAN の所属と判断します。

以下の各節では、上記をふまえ、最初にもっとも基本的な VLAN であるポート VLAN とタグ VLAN について説明したのち、その他の VLAN について簡単に説明します。

## デフォルト VLAN

ご購入時の状態ではすべてのポートが VLAN default ( VID=1 ) に所属しており、すべてのポートが相互に通信可能になっています。単なるレイヤー 2 スイッチとして本製品を使用する場合は、特別な設定を行うことなく、設置・配線を行うだけで使用できます。



VLAN default は特殊な VLAN であり、下記の特長があります。

- VLAN default は削除できません。
- ポートが VLAN default にしか所属していない場合、同ポートを VLAN default から削除することはできません。ただし同ポートを、ユーザー定義のポート VLAN にタグなしポートとして割り当てると、該当ポートは自動的に VLAN default から削除されます。
- ユーザー定義 VLAN のポート VLAN メンバーからタグなしポートを削除すると、該当ポートは自動的に VLAN default のタグなしポートに戻ります。
- VLAN default は「default STP」以外の STP ドメインに参加できません。
- VLAN default はマルチプル VLAN ( Private VLAN ) になれません。

## ポート VLAN

ポート VLAN は、ポート単位で VLAN の範囲を設定するもっとも基本的な VLAN です。ポート 1～4 は VLAN red、ポート 5～8 は VLAN white、といったように設定します。

1. 新規に VLAN を作成するには CREATE VLAN コマンド ( 225 ページ ) を使います。VLAN 作成時

には、VLAN 名と VLAN ID (VID) を割り当てる必要があります。VLAN 名は任意の文字列 (ただし、先頭文字は数字以外)、VID は 2~4094 の範囲の任意の数値です (1 は VLAN default に割り当てられているため使用できません)。3 つの VLAN、A (VID=10)、B (VID=20)、C (VID=30) を作成するには次のようにします。

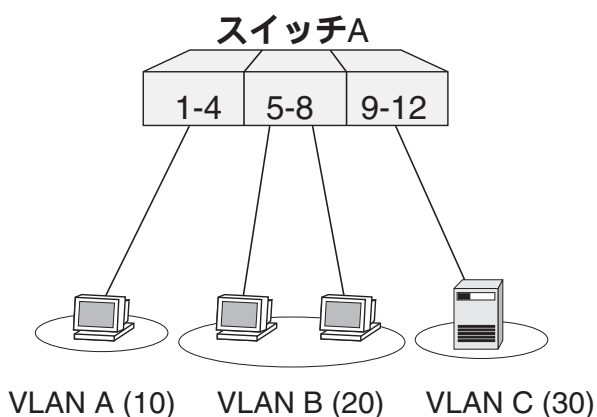
```
CREATE VLAN=A VID=10 ↵
CREATE VLAN=B VID=20 ↵
CREATE VLAN=C VID=30 ↵
```

これ以降、VLAN 名を指定するときは VLAN 名、VID のどちらを使ってもかまいません。ここではおもに VLAN 名を使います。

2. VLAN を作成したら、ADD VLAN PORT コマンド (191 ページ) で VLAN にポートを割り当てます。

```
ADD VLAN=A PORT=1-4 ↵
ADD VLAN=B PORT=5-8 ↵
ADD VLAN=C PORT=9-12 ↵
```

このようにしてポートを default 以外の VLAN に割り当てると、そのポートは自動的に VLAN default から削除されます。



これで、物理的には 1 台のスイッチでありながら、ネットワーク的には 3 台のスイッチに分割されたような状態となります。VLAN A、B、C は完全に独立しており、互いに通信することはできません。

VLAN の情報を確認するには、SHOW VLAN コマンド (519 ページ) を使います。

VLAN からポートを削除するには、DELETE VLAN PORT コマンド (239 ページ) を使います。たとえば、ポート 3 と 4 を VLAN A から削除するには、次のようにします。default 以外の VLAN から削除されたポートは、自動的に VLAN default の所属に戻ります。

```
DELETE VLAN=A PORT=3-4 ↵
```

VLAN を削除するには、DESTROY VLAN コマンド (252 ページ) を使います。VLAN の削除は、所属ポートをすべて削除してからでないと行えません。VLAN C を削除するには、次のようにします。

```
DELETE VLAN=C PORT=ALL ↵
DESTROY VLAN=C ↵
```

🔑 VLAN default は削除できません。

## タグ VLAN

タグ VLAN を使用すると、1 つのポートを複数の VLAN に所属させることができます。これは、イーサネットフレームに VLAN ID の情報を挿入し、各フレームが所属する VLAN を識別できるようにすることによって実現されます (802.1Q VLAN タギング)。タグ VLAN は、複数の VLAN を複数の筐体にまたがって作成したい場合や、802.1Q 対応サーバーを複数 VLAN から共用したい場合などに利用します。

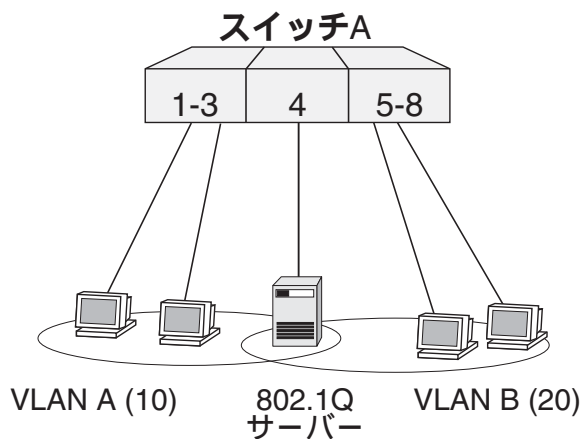
🔑 VLAN タグを使用する場合、接続先機器も VLAN タグ (802.1Q) に対応している必要があります。

🔑 802.1X 認証の Authenticator ポートと MAC ベース認証ポートをタグ付きに設定することはできません。

### VLAN タグ対応サーバーの共用

VLAN タグを利用して、ポート 4 を 2 つの VLAN に所属させ、どちらの VLAN からでも 802.1Q 対応サーバーにアクセスできるようにします。

ここでは次のようなネットワーク構成を例に説明します。



1. VLAN A、B を作成します。

```
CREATE VLAN=A VID=10 ↵
CREATE VLAN=B VID=20 ↵
```

2. VLAN A にポートを追加します。ポート 1～3 はタグを使わない通常のポートに設定し、ポート 4 はタグを使用するポートとして設定します。VLAN にタグ付きポートを追加するときは、ADD VLAN PORT コマンド (191 ページ) の FRAME パラメーターに TAGGED を指定します。FRAME パラメーターを付けなかったときはタグなし (UNTAGGED) となります。

```
ADD VLAN=A PORT=1-3 ↵
ADD VLAN=A PORT=4 FRAME=TAGGED ↵
```

3. VLAN B にポートを追加します。ポート 5～8 はタグを使わない通常のポートに設定し、ポート 4 はタグを使用するポートとして設定します。

```
ADD VLAN=B PORT=5-8 ↵
ADD VLAN=B PORT=4 FRAME=TAGGED ↵
```

以上で設定は完了です。

これにより、ポート 1～8 から送受信されるフレームは次のようになります。

ポート 1～3	送信	ポート 1～3 から送信するフレームは VLAN A 宛てのタグなしフレーム
	受信	ポート 1～3 で受信したタグなしフレームは VLAN A (VID=10) 所属とみなされる
ポート 4	送信	ポート 4 から送信するフレームは、VLAN A 宛てなら VID=10 のタグ付きで、VLAN B 宛てなら VID=20 のタグ付きで送信される
	受信	ポート 4 では VLAN A、B 両方のトラフィックを受信する。受信するフレームはタグ付き。タグの VID により、所属 VLAN を判断する
ポート 5～8	送信	ポート 5～8 から送信するフレームは VLAN B 宛てのタグなしフレーム
	受信	ポート 5～8 で受信したタグなしフレームは VLAN B (VID=20) 所属とみなされる

表 3:

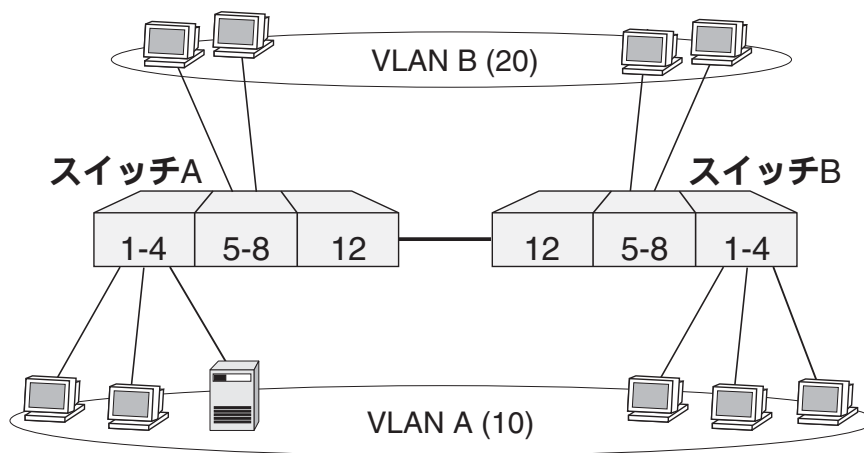
上記の設定では、ポート 4 は VLAN default にも (タグなしポートとして) 所属したままになっています。他にも VLAN default 所属のポートがあってトラフィックが流れている場合、ポート 4 にも VLAN default のブロードキャストパケットが送出されます。これが望ましくない場合は、DELETE VLAN PORT コマンド (239 ページ) を使って、ポート 4 を VLAN default から削除します。

```
DELETE VLAN=default PORT=4 ↵
```

## VLAN タグを利用したスイッチ間接続



VLAN タグを利用して、2 台のスイッチにまたがる VLAN を作成します。ここでは次のようなネットワーク構成を例に説明します。ポート 12 をタグ付きに設定し、VLAN A、B 両方のトラフィックがスイッチ間で流れるようにします。



#### スイッチの設定（A、B 共通）

1. VLAN A、B を作成します。

```
CREATE VLAN=A VID=10 ↵
```

```
CREATE VLAN=B VID=20 ↵
```

2. VLAN A にポートを追加します。ポート 1～4 はタグを使わない通常のポートに設定し、ポート 12 はタグを使用するポートとして設定します。VLAN にタグ付きポートを追加するときは、ADD VLAN PORT コマンド（191 ページ）の FRAME パラメーターに TAGGED を指定します。FRAME パラメーターを付けなかったときはタグなし（UNTAGGED）となります。

```
ADD VLAN=A PORT=1-4 ↵
```

```
ADD VLAN=A PORT=12 FRAME=TAGGED ↵
```

3. VLAN B にポートを追加します。ポート 5～8 はタグを使わない通常のポートに設定し、ポート 12 はタグを使用するポートとして設定します。

```
ADD VLAN=B PORT=5-8 ↵
```

```
ADD VLAN=B PORT=12 FRAME=TAGGED ↵
```

設定は以上です。

複数のスイッチにまたがる VLAN を作成する場合は、各筐体で同じ VLAN ID を設定するようにしてください。一方、VLAN 名は個々の筐体内でしか意味を持たないので、スイッチごとに異なってもかまいません。

ません（ただし、混乱を防ぐ意味では同じ名前を付けた方がよいでしょう）。

上記の設定では、ポート 12 は VLAN default にも（タグなしポートとして）所属したままになっています。他にも VLAN default 所属のポートがあってトラフィックが流れている場合、ポート 12 にも VLAN default のブロードキャストパケットが送出されます。これが望ましくない場合は、DELETE VLAN PORT コマンド（239 ページ）を使って、ポート 12 を VLAN default から削除します。

```
DELETE VLAN=default PORT=12 ↵
```

## IP サブネット VLAN

IP サブネット VLAN では、受信したタグなしパケットの始点 IP アドレスが特定のサブネットに属する場合、これを VLAN メンバーと見なします。

- ☞ IP サブネット VLAN の対象となるプロトコルは IP だけです。ARP パケットの扱いについては、次の「ARP パケットに関する注意事項」をご覧ください。

### ARP パケットに関する注意事項

IP サブネット VLAN の設定を行う場合は、下記のようなハードウェアパケットフィルタを適用して、ARP パケットが CPU に転送されるよう設定してください。この設定を行わない場合、IP サブネット VLAN の所属ポートで受信した ARP パケットが IP サブネット VLAN 所属として扱われず、ポート本来のタグなし VLAN 所属として扱われてしまいます。

```
CREATE CLASS=1 ETHF=ETHII-UNTAGGED PROT=0806 ↵
ADD SWITCH HWF=1 CLASS=1 ACTION=DISCARD,COPY ↵
```

- ☞ フィルター番号、クラシファイア番号は適宜変更してください。
- ☞ DISCARD,COPY アクションはサポート対象外のパラメーター値です。本現象を回避する以外の目的では使用しないでください。

### 基本設定

IP サブネット VLAN を作成するには、CREATE VLAN コマンド（225 ページ）の SUBNET、MASK パラメーターでサブネットの範囲を指定します。MASK パラメーターを省略した場合は、SUBNET パラメーターで指定したアドレスのクラス標準マスクが使用されます。

```
CREATE VLAN=net10 VID=10 SUBNET=192.168.10.0 MASK=255.255.255.0 ↵
```

また、サブネットの範囲は ADD VLAN SUBNET コマンド（197 ページ）を使って後から追加することもできます。

```
CREATE VLAN=net10 VID=10 ↓
```

```
ADD VLAN=net10 SUBNET=192.168.10.0 MASK=255.255.255.0 ↓
```

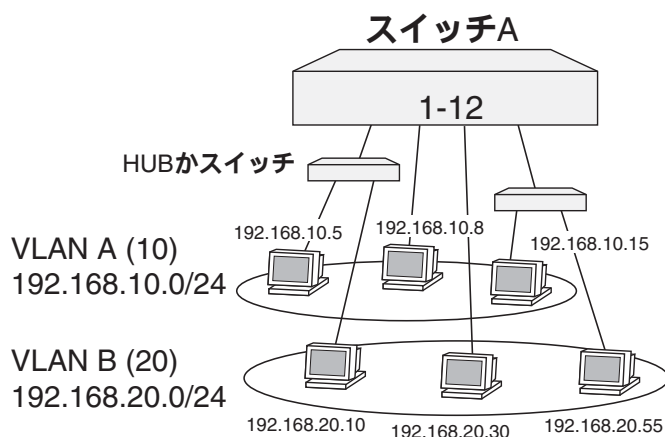
- ☞ IP サブネット VLAN にサブネット範囲を複数設定する場合、および、IP サブネット VLAN を複数作成する場合、サブネットのアドレス範囲が重複するような設定はできません。たとえば、VLAN A のサブネット範囲を「192.168.10.0/24」(192.168.10.0 ~ 192.168.10.255) に設定した場合、VLAN B のサブネット範囲として「192.168.0.0/16」(192.168.0.0 ~ 192.168.255.255) を指定することはできません。

IP サブネット VLAN を作成し、サブネットの範囲を指定したら、ADD VLAN PORT コマンド (191 ページ) でタグなしポートを IP サブネット VLAN に関連付けます。このとき、どのサブネットメンバーに所属させるかを、SUBNET パラメーターで必ず指定してください。

```
ADD VLAN=net10 PORT=1-6 SUBNET=192.168.10.0 ↓
```

これにより、ポート 1 ~ 6 で受信した IP パケットのうち、始点アドレスが 192.168.10.0/24 の範囲におさまるものが VLAN net10 の所属として扱われます。

同一のポート範囲 (ポート 1 ~ 12) に対して、2 つの IP サブネット VLAN を作成するには次のようにします。



```
CREATE VLAN=A VID=10 SUBNET=192.168.10.0 MASK=255.255.255.0 ↓
```

```
CREATE VLAN=B VID=20 SUBNET=192.168.20.0 MASK=255.255.255.0 ↓
```

```
ADD VLAN=A PORT=1-12 SUBNET=192.168.10.0 ↓
```

```
ADD VLAN=B PORT=1-12 SUBNET=192.168.20.0 ↓
```

これにより、ポート 1 ~ 12 で受信したパケットのうち、始点アドレスが 192.168.10.0/24 の範囲におさまるものは VLAN A、192.168.20.0/24 の範囲におさまるものは VLAN B の所属として扱われます。

また、その他のパケット (始点アドレスが上記以外、あるいは、IP でないパケット) は、受信ポートが所属

しているポート VLAN の所属になります。上記の例で VLAN A、B 以外にユーザー定義の VLAN がないと仮定すると、その他のパケットは VLAN default の所属として扱われます。

ポート 1～12 以外のポートにも機器が接続されている場合、それらの機器が送信したパケットは VLAN default 所属となるため、ポート 1～12 にもパケットが出力される可能性があります。これを避けるには、ポート 1～12 を VLAN default 以外のポート VLAN に所属させるか、ポート 1～12 以外を VLAN default 以外のポート VLAN に所属させます。前者の設定は次のとおりです。

```
CREATE VLAN=DUMMY VID=100 ↓
ADD VLAN=DUMMY PORT=1-12 ↓
```

前の例では、IP サブネット 192.168.10.0/24 と 192.168.20.0/24 は同一ポート上に混在していますが、それぞれのパケットが別の VLAN に所属するため、互いに通信することはできません。サブネット間で通信を可能にするには、両方の VLAN に IP アドレスを割り当て、VLAN 間ルーティングを有効にする必要があります。

```
ENABLE IP ↓
ADD IP INT=vlan-A IP=192.168.10.1 MASK=255.255.255.0 ↓
ADD IP INT=vlan-B IP=192.168.20.1 MASK=255.255.255.0 ↓
```

詳細は「VLAN 間ルーティング」をご覧ください。

☞ IP サブネット VLAN とダブルタグ VLAN (Nested VLAN) は併用できません。

## プロトコル VLAN

プロトコル VLAN では、受信したタグなしパケットの L3 プロトコルタイプフィールドに特定の値が格納されているパケットを VLAN メンバーと見なします。プロトコル VLAN は、他の種類の VLAN (ポート VLAN など) と組み合わせて使うケースがよくあります。

プロトコル VLAN を作成するには、CREATE VLAN コマンド (225 ページ) の PROTOCOL パラメーターでプロトコルを指定します。プロトコルは、定義済みのプロトコル名 (ADD VLAN PROTOCOL コマンド (194 ページ) の表を参照) か 16 進表記 (「0x」を前置) のプロトコル番号で指定します。

プロトコル名で指定する場合は次のようにします。

```
CREATE VLAN=nw VID=100 PROTOCOL="IPX 802.2" ↓
```

プロトコル番号で指定する場合は、フレームタイプ (エンキャプセレーション) に応じて、1 バイト (802.2 LLC DSAP)、2 バイト (Ethernet または 802.3 raw)、5 バイト (SNAP) の 16 進数 (「0x」を前置) で指定します。

```
CREATE VLAN=nw VID=100 PROTOCOL=0xe0 ↓
```

また、プロトコルは ADD VLAN PROTOCOL コマンド (194 ページ) を使って後から追加することもで

きます。

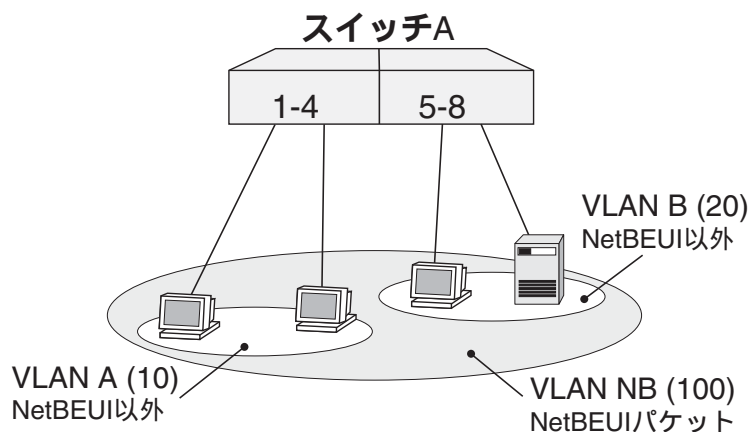
```
CREATE VLAN=nw VID=10 ↓
ADD VLAN=nw PROTOCOL="IPX 802.2" ↓
```

プロトコル VLAN を作成し、対象プロトコルを指定したら、ADD VLAN PORT コマンド (191 ページ) でタグなしポートをプロトコル VLAN に関連付けます。このとき、どのプロトコルメンバーに所属させるかを、PROTOCOL パラメーターで必ず指定してください。

```
ADD VLAN=nw PORT=1-6 PROTOCOL="IPX 802.2" ↓
```

これにより、ポート 1~6 で受信したパケットのうち、フレームタイプ 802.2 の IPX パケット (DSAP = 0xe0) が VLAN nw の所属として扱われます。

2 つのポート VLAN A と B を包含するプロトコル VLAN NB を作成します。ポート 1~8 で受信した NetBEUI パケットは VLAN NB 所属と見なされます。それ以外のパケットは、受信ポートが 1~4 なら VLAN A、4~8 なら VLAN B 所属として扱われます。



```
CREATE VLAN=A VID=10 ↓
CREATE VLAN=B VID=20 ↓
CREATE VLAN=NB VID=100 PROTOCOL=NetBEUI ↓
ADD VLAN=A PORT=1-4 ↓
ADD VLAN=B PORT=5-8 ↓
ADD VLAN=NB PORT=1-8 PROTOCOL=NetBEUI ↓
```

## マルチプル VLAN ( Private VLAN )

マルチプル VLAN ( Private VLAN。以下、Private VLAN で表記 ) は、アップリンクポートとプライベ

トポートという 2 種類のポートで構成される特殊な VLAN です。

プライベートポートとアップリンクポートは相互に通信可能ですが、プライベートポート間では一切通信ができません。この性質を利用すれば、各部屋にインターネットアクセスを提供しつつ、部屋同士の通信は遮断するような構成を組むことができます。

- ✎ DHCP サーバー機能とマルチプル VLAN (Private VLAN) は併用できません。
- ✎ マルチプル VLAN のプライベートポートでは ARP パケットの処理が行えないため、DHCP、SNMP、Telnet、IP ルーティングなど、本製品との通信が必要な機能は使用できません。

## 基本ルール

次に Private VLAN の基本ルールをまとめます。

Private VLAN には次のルールが適用されます。

- Private VLAN は、アップリンクポートとプライベートポートで構成される。
- Private VLAN には、アップリンクポート (トランクグループでもよい) が 1 つ必要。
- Private VLAN には、プライベートポートを複数割り当てられる。
- Private VLAN には、プライベートポートでもアップリンクポートでもないポートは所属できない。
- VLAN default は、Private VLAN になれない。
- 同一 Private VLAN のプライベートポート同士は通信できない。

アップリンクポートには次のルールが適用されます。

- アップリンクポートは、単一ポートか単一のトランクグループでなければならない。
- トランクグループをアップリンクポートとして指定してもよい。
- アップリンクポートは、複数の Private VLAN に所属できる。
- アップリンクポートは、Private VLAN でない通常の VLAN には所属できない。
- アップリンクポートは、ポート VLAN、タグ VLAN、IP サブネット VLAN、プロトコル VLAN との併用が可能。

プライベートポートには次のルールが適用されます。

- プライベートポートは、タグ VLAN や IP サブネット VLAN、プロトコル VLAN を併用することにより複数の Private VLAN に所属できるが、その場合すべての Private VLAN が同一のアップリンクポートを共有していなくてはならない。
- プライベートポートは、Private VLAN でない通常の VLAN には所属できない。
- プライベートポートは、他の Private VLAN のアップリンクポートになることはできない。
- プライベートポートは、ポート VLAN、タグ VLAN、IP サブネット VLAN、プロトコル VLAN との併用が可能。
- トランクポートをプライベートポートとして指定してもよい。
- プライベートポートでは ARP パケットの処理が行えないため、DHCP、SNMP、Telnet、IP ルーティングなど、本製品との通信が必要な機能は使用できない

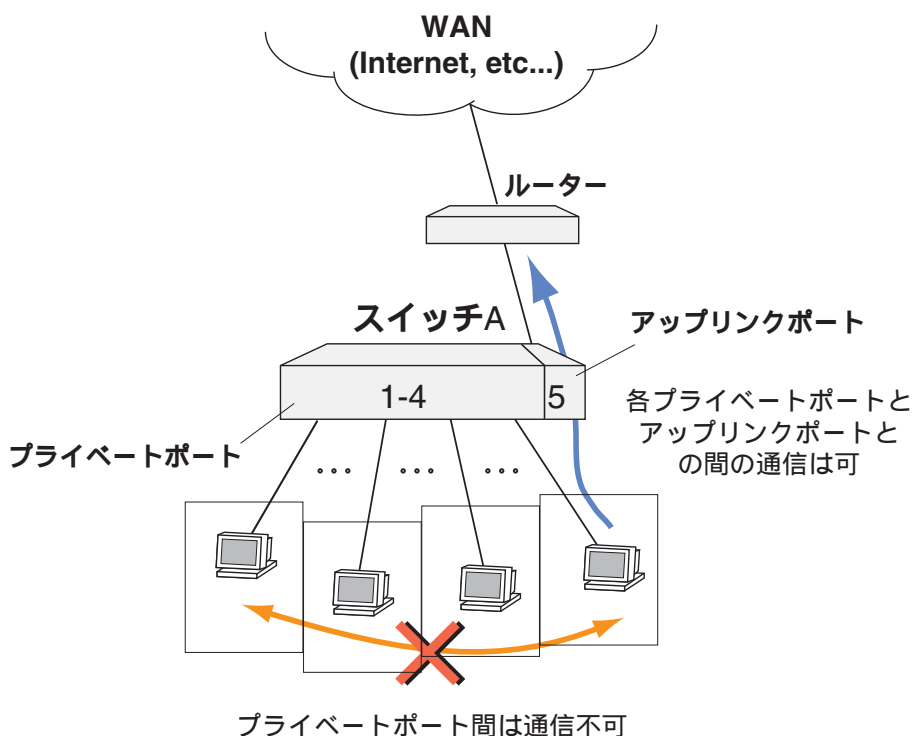
プライベートポートとアップリンクポートで受信したパケットは、それぞれ次のように処理されます。

- プライベートポートで受信したパケットは、VLAN ID や宛先 MAC アドレスに関わらず、すべてアップリンクポートに転送される。
- アップリンクポートで受信したパケットは、宛先 MAC アドレスの種類によって処理が異なる。
  - ユニキャストパケットは、宛先 MAC アドレスに応じて、適切なプライベートポートにだけ転送される。
  - ブロードキャスト・マルチキャストパケットは、すべてのプライベートポートに転送される。

### 設定例

次に Private VLAN の設定例を示します。

ここでは、ポート 5 をアップリンクポートとし、ポート 1~4 をプライベートポートとする Private VLAN 「pv」を作成します。インターネットマシジョンなどでの一般的な使用例です。この構成では、本製品をレイヤー 2 スイッチとして使用することになります。



1. Private VLAN 「pv」を作成します。Private VLAN を作成するには、CREATE VLAN コマンド（225 ページ）に PRIVATE オプションを付けます。

```
CREATE VLAN=pv VID=2 PRIVATE ㊟
```

🔑 VLAN default を Private VLAN にすることはできません。

2. アップリンクポートを割り当てます。アップリンクポートを追加するには、ADD VLAN PORT コマ

ンド (191 ページ) に UPLINK オプションを付けて実行します。

```
ADD VLAN=pv PORT=5 UPLINK ↵
```

✎ アップリンクポートは単一ポートか単一のトランクグループでなければなりません。1 つの Private VLAN にアップリンクポートを複数追加することはできません。

✎ アップリンクポートとして追加するポートは、VLAN default 以外の非 Private VLAN に所属していません。そのような場合は、最初に同ポートを非 Private VLAN から削除した上で、ADD VLAN PORT コマンド (191 ページ) を実行してください。

3. プライベートポートを割り当てます。プライベートポートを追加するには、ADD VLAN PORT コマンド (191 ページ) をオプションなしで実行します。

```
ADD VLAN=pv PORT=1-4 ↵
```

設定は以上です。

## ダブルタグ VLAN (Nested VLAN)

ダブルタグ VLAN (Nested VLAN。以下、Nested VLAN で表記) は、その名のとおり、VLAN タグを 2 重に付加する特殊な VLAN です。オリジナルパケットの VLAN タグ (内側タグ) をもう 1 つのタグ (外側タグ) でカプセル化する一種のトンネリング技術と言えます (802.1Q トンネリングなどとも呼ばれます)。Nested VLAN は、コアポートとカスタマーポートという 2 種類のポートで構成されます。

通常、コアポートはサービス事業者の広域網などに接続され、外側タグ (CID: カスタマー ID) のついたパケットを送受信します。コアポートでは、送信時に外側タグを挿入し、受信時には外側タグを削除します。一方、カスタマーポートは顧客のネットワークなどに接続され、内側タグだけの通常のタグ付きパケットおよびタグなしパケットを送受信します。カスタマーポートでは、送受信時にパケットの変更は行いません。

- ✎ ダブルタグ VLAN (Nested VLAN) は別売のフィーチャーライセンス AT-FL-09 または AT-FL-09-B が必要です。
- ✎ ダブルタグ VLAN (Nested VLAN) はレイヤー 2 を前提とした機能です。Nested VLAN 使用時のルーティングはサポート対象外となります。
- ✎ ダブルタグ VLAN (Nested VLAN) は、IP サブネット VLAN、IGMP Snooping、ハードウェアパケットフィルターの L3 以上の条件パラメーター (L2 は使用可) のいずれとも併用できません。

## 基本ルール

次に Nested VLAN の基本ルールをまとめます。

Nested VLAN には次のルールが適用されます。



- Nested VLAN は、コアポートとカスタマーポートで構成される。
- Nested VLAN の所属ポートは、コアポート、カスタマーポートのどちらかでなくてはならない。
- Nested VLAN の所属ポートは、コアポート、カスタマーポートのどちらか一方にしかねない。
- Nested VLAN の所属ポートは、Nested VLAN でない通常の VLAN には所属できない。
- VLAN default は、Nested VLAN になれない。
- Nested VLAN 内では、パケットの宛先 MAC アドレスと CID (Nested VLAN の VID) に基づいてレイヤー 2 スイッチングが行われる。内側タグの VID には関知しない。
- Nested VLAN と IGMP Snooping とは併用できない。
- Nested VLAN とルーティングの併用はサポート対象外。

コアポートには次のルールが適用されます。

- コアポートは、タグ付きポートであり、タグ付きパケットだけを送受信できる（ここでのタグとは、CID を格納する外側タグのこと）。
- コアポートは、タグ付き扱いなので、複数の Nested VLAN に所属できる。
- コアポートは、パケット送信前に外側タグを挿入する。
- コアポートは、パケット受信後に外側タグを削除する。

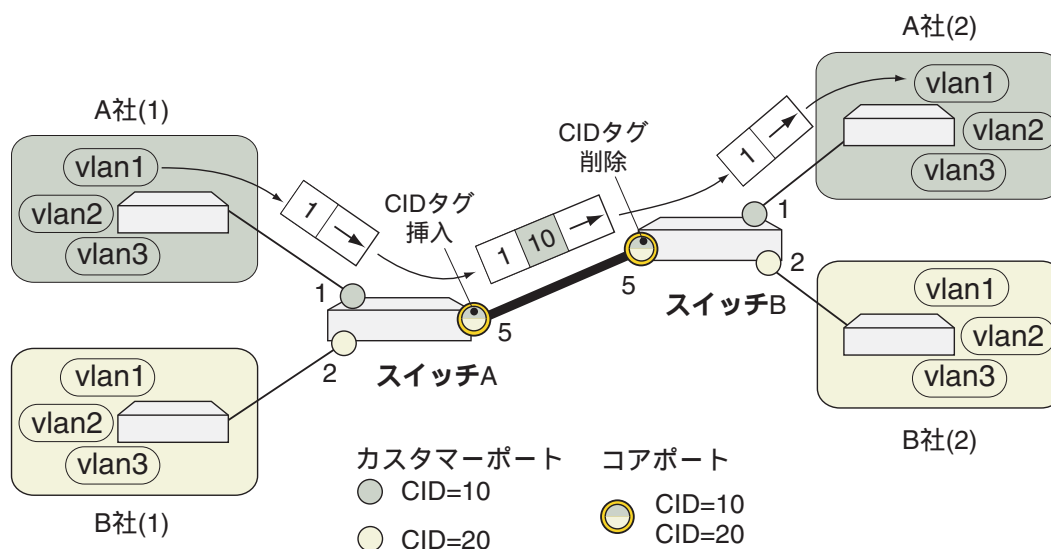
カスタマーポートには次のルールが適用されます。

- カスタマーポートは、タグなしポートであり、タグ付きパケット、タグなしパケットの両方を受信できる。また、送信時には、パケットがタグ付きかタグなしには関知しない。タグ付き、タグなし両方のパケットを送信できる（ここでのタグとは、VID を格納する内側タグのこと）。
- カスタマーポートは、タグなし扱いなので、通常 1 つの Nested VLAN にしか所属できないが、IP サブネット VLAN やプロトコル VLAN を併用すれば複数の Nested VLAN に所属することができる。
- カスタマーポートは、パケット送受信時にパケットの内容を変更しない（タグの挿入、削除などを行わない）。

## 設定例

次に Nested VLAN の設定例を示します。

ここでは、A 社と B 社をそれぞれ収容する Nested VLAN 「Acompany」と「Bcompany」を作成します。A 社のカスタマー ID (CID) は 10、B 社は 20 とします。スイッチ A、スイッチ B の設定は共通です。



1. Nested VLAN「Acompany」と「Bcompany」を作成します。Nested VLAN を作成するには、CREATE VLAN コマンド ( 225 ページ ) に NESTED オプションを付けます。VID パラメーターに指定するのは、外側タグに格納するカスタマー ID (CID) です。

```
CREATE VLAN=Acompany VID=10 NESTED ↵
CREATE VLAN=Bcompany VID=20 NESTED ↵
```

2. Nested VLAN「Acompany」と「Bcompany」に共通のコアポートを割り当てます。コアポートを追加するには、ADD VLAN PORT コマンド ( 191 ページ ) の NESTEDTYPE に CORE を指定します。

```
ADD VLAN=Acompany PORT=5 NESTEDTYPE=CORE ↵
ADD VLAN=Bcompany PORT=5 NESTEDTYPE=CORE ↵
```

📎 コアポートは複数の Nested VLAN に所属できます。

3. Nested VLAN「Acompany」と「Bcompany」のそれぞれにカスタマーポートを割り当てます。Nested VLAN にカスタマーポートを追加するには、ADD VLAN PORT コマンド ( 191 ページ ) の NESTEDTYPE に CUSTOMER を指定します。

```
ADD VLAN=Acompany PORT=1 NESTEDTYPE=CUSTOMER ↵
ADD VLAN=Bcompany PORT=2 NESTEDTYPE=CUSTOMER ↵
```

設定は以上です。

前の例を元に、Nested VLAN の動作を簡単に説明します。ここでは、A 社 (1) から A 社 (2) に送られる、vlan1 のパケットを例に取り上げます。

1. スイッチ A は、CID=10 のカスタマーポートで VID=1 のタグ付きパケットを受信します。
2. スイッチ A は、受信パケットの宛先 MAC アドレスと CID=10 をキーにフォワーディングデータベースを検索し、出力ポートを決定します。ここではポート 5 が出力ポートになったとします。
3. スイッチ A は、CID=10 と CID=20 のコアポートであるポート 5 において、パケットに外側タグを付加し、CID=10 を格納した上で送信します。
4. スイッチ B は、CID=10 と CID=20 のコアポートであるポート 5 において、CID=10 のタグ付きパケットを受信します。また、外側タグを削除します。
5. スイッチ B は、受信パケットの宛先 MAC アドレスと CID=10 をキーにフォワーディングデータベースを検索し、出力ポートを決定します。ここではポート 1 が出力ポートになったとします。
6. スイッチ B は、CID=10 のカスタマーポートであるポート 1 からパケットを送信します。すでに外側タグは削除されているので、送信されるパケットにはオリジナルの内側タグ (VID=1) だけが付いています。

外側タグのプロトコルタイプ (TPID) を変更するには、SET SWITCH NESTEDTPID コマンド (386 ページ) を使います。デフォルトは 0x8100 (802.1Q タグと同じ) です。

```
SET SWITCH NESTEDTPID=88ff ↵
```

## VLAN 間ルーティング

各 VLAN は独立したブロードキャストドメインになるため、互いに通信することはできません。しかし、各 VLAN にレイヤー 3 プロトコル (IP) のアドレスを割り当て、ルーティング機能を有効にすれば、ネットワーク層レベルでパケットがルーティングされ、VLAN 間通信が可能になります。ここでは IP を例に、VLAN 間ルーティングの基本設定について説明します。

1. VLAN を作成します。

```
CREATE VLAN=A VID=10 ↵
CREATE VLAN=B VID=20 ↵
CREATE VLAN=C VID=30 ↵
```

2. VLAN にポートを割り当てます。

```
ADD VLAN=A PORT=1-4 ↵
ADD VLAN=B PORT=5-8 ↵
ADD VLAN=C PORT=9-12 ↵
```

3. IP を使用するため、IP モジュールを有効にします。

```
ENABLE IP ↵
```

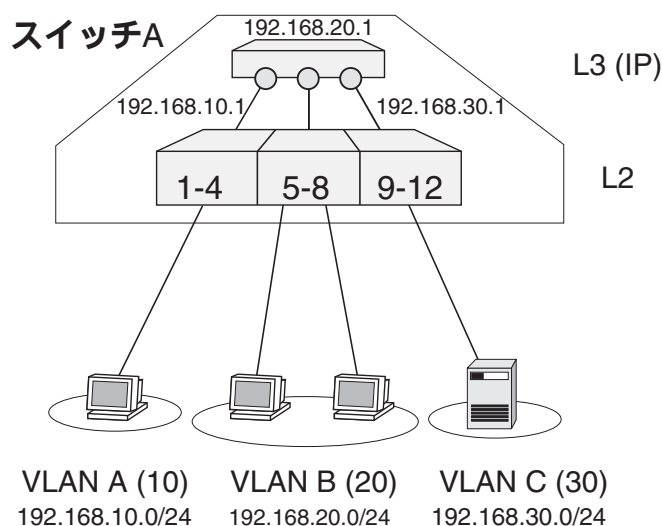
4. 各 VLAN (VLAN インターフェース) に IP アドレスを割り当てます。IP アドレスの設定は ADD IP INTERFACE コマンド ('IP' の 151 ページ) で行います。

```
ADD IP INTERFACE=vlan-A IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INTERFACE=vlan-B IP=192.168.20.1 MASK=255.255.255.0 ↵
ADD IP INTERFACE=vlan-C IP=192.168.30.1 MASK=255.255.255.0 ↵
```

設定は以上です。

これにより、VLAN 間で IP がルーティングされるようになります。VLAN 間ルーティングは、同じプロトコルのレイヤー 3 インターフェースを 2 つ作成した時点で自動的に有効になります。

次の図は、この状態を概念的に示したものです。VLAN 分けにより分割された仮想的なスイッチ 3 台の上位に、仮想的なルーターを設置したものと考えることができます。実際にはこれらのスイッチやルーターの機能は、1 台の筐体内で実現されています。



VLAN インターフェースの指定には次に示す 2 とおりの方法があります。レイヤー 3 (IP など) のコマンドで VLAN を指定するときは、どちらの方法を使ってもかまいません。詳細については、コマンドリファレンスの各コマンドの説明をご覧ください。

- VLAN 名による指定

VLAN 名が「myname」なら、vlan-myname のように「vlan-」+VLAN 名と指定します。次に例を示します。

```
ADD IP INT=vlan-myname IP=192.168.100.10 MASK=255.255.255.0 ↵
```

- VLAN ID (VID) による指定

VID が 10 ならば、vlan10 のように「vlan」+VID のように指定します。VLAN 名のとくとは異なり、ハイフンが入らないことに注意してください。

```
ADD IP INT=vlan10 IP=192.168.10.1 MASK=255.255.255.0 ↵
```

各 VLAN に割り当てられた IP アドレスは、SHOW IP INTERFACE コマンド（「IP」の 412 ページ）で確認できます。

デフォルトルートを設定するには、ADD IP ROUTE コマンド（「IP」の 160 ページ）を使います。

```
ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0 INT=vlan-A NEXTHOP=192.168.10.254 ↵
```

詳細は「IP」の章をご覧ください。

## スパニングツリープロトコル (STP/RSTP)

スパニングツリープロトコル (STP) は、スイッチ (ブリッジ) ネットワークにおいて、冗長経路 (複数経路) の設定を可能とし、ネットワークの耐障害性を高めるプロトコルです。

ネットワーク上に複数の経路を設定し、障害発生時に迂回路を使えるようにすることは自然な発想ですが、Ethernet ではループ状の経路がブロードキャストストームによるネットワーク停止を招くため、そのままでは複数経路の設定自体ができません。

スパニングツリープロトコルを使用すると、ブリッジ同士がメッセージを交換し合うことにより、すべてのブリッジを含むツリー状の論理経路 (スパニングツリー) が自立的に構築されます。物理的にループが存在しても、ツリーを構成しないポートは自動的にブロックされるため、パケットがループすることはありません。また、障害が発生して一部の経路が不通になったときは、ツリーの再計算が行われ、自動的に新しい経路に切り替わる冗長機能も備えています。

### 基本設定

本製品は、VLAN グループ (1 つ以上の VLAN で構成) ごとに個別のスパニングツリーを構成するマルチプル STP ドメインに対応していますが、デフォルトの設定では VLAN default、ユーザー定義の VLAN とも、すべての VLAN がデフォルトの STP ドメイン「default」所属となります。

以下、スパニングツリープロトコルの基本設定コマンドについて解説します。

- ✎ 802.1X 認証の Authenticator/Supplicant ポートと MAC ベース認証ポートでは、スパニングツリープロトコルを使用できません。
- ✎ スパニングツリープロトコルとタグ VLAN の併用時、スイッチポートのタグ設定に関わらず、BPDU にはタグを付加しません (オーバーラップ STP の場合を除く)。

スパニングツリープロトコルを有効にするには、ENABLE STP コマンド (295 ページ) を使います。各 STP ドメインのデフォルト設定は無効です。デフォルト STP ドメイン「default」でスパニングツリープロトコルを有効にするには、次のようにします。

```
ENABLE STP=default ↵
```

スパニングツリープロトコルを無効にするには、DISABLE STP コマンド (265 ページ) を使います。

```
DISABLE STP=default ↵
```

スパニングツリーの設定を確認するには、SHOW STP コマンド (480 ページ) を使います。

```
SHOW STP ↵
SHOW STP=default ↵
```

スパニングツリーのポート情報を確認するには、SHOW STP PORT コマンド (487 ページ) を使います。

```
SHOW STP PORT ↓
```

```
SHOW STP PORT=1 ↓
```

スパニングツリーの統計カウンターを確認するには、SHOW STP COUNTER コマンド (484 ページ) を使います。

```
SHOW STP COUNTER ↓
```

```
SHOW STP=default COUNTER ↓
```

## マルチプル STP ドメイン

本製品は、VLAN グループ (1 つ以上の VLAN で構成) ごとに個別のスパニングツリーを構成するマルチプル STP ドメインに対応しています。各 STP ドメインは、それぞれ個別のスパニングツリーパラメーターを持ち、別々にルートブリッジを選出してスパニングツリーを構成します。

複数の STP ドメインを設定するときは、以下の点に注意してください。

- 各 STP ドメインには複数の VLAN を所属させることができる
- 各 VLAN が所属できる STP ドメインは 1 つ
- スイッチポートが複数の VLAN に所属している場合、該当ポートは複数の STP ドメインに所属できる (オーバーラップ STP)。ただし、オーバーラップ STP は標準規格でないため、他製品との相互接続性は保証されない。

✎ トランクポートではオーバーラップ STP を使用できません。

なお、通常的环境では複数の STP ドメインを作成する必要はありません。

デフォルトの設定では、VLAN default、ユーザー定義の VLAN とともに、すべての VLAN がデフォルトの STP ドメイン「default」所属となります。

デフォルト以外の STP ドメインを作成するには、CREATE STP コマンド (222 ページ) を使います。

```
CREATE STP=mystp ↓
```

STP ドメインに VLAN を追加するには、ADD STP VLAN コマンド (182 ページ) を使います。

```
ADD STP=mystp VLAN=white ↓
```

✎ 本コマンドでは、デフォルト STP ドメインに VLAN を追加することはできません。DELETE STP VLAN コマンド (234 ページ) を使って VLAN をデフォルト以外の STP ドメインから削除すると、自動的にデフォルト STP の所属となります。

STP ドメインから VLAN を削除するには、DELETE STP VLAN コマンド (234 ページ) を使います。デフォルト以外の STP ドメインから削除された VLAN は、デフォルト STP ドメインの所属に戻ります。

```
DELETE STP=mystp VLAN=orange ↵
```

STP ドメインを削除するには、DESTROY STP コマンド (250 ページ) を使います。所属 VLAN がある STP ドメインは削除できないので、DELETE STP VLAN コマンド (234 ページ) で削除してから本コマンドを実行してください。所属 VLAN を削除後、STP ドメインを削除するには次のようにします。

```
DELETE STP=mystp VLAN=ALL ↵
DESTROY STP=mystp ↵
```

## スパンニングツリーパラメーターの設定変更

設定タイマーの変更方法など、より詳細な設定について解説します。

STP ドメインのスパンニングツリーパラメーター (各種タイマーとブリッジプライオリティー) を変更するには、SET STP コマンド (377 ページ) を使います。変更できるパラメーターは次のとおりです。

パラメーター	説明
FORWARDDELAY	ルートブリッジのポートがフォワーディング状態に移移するまでの時間を調整するためのパラメーター。MODE が STANDARD のときは、ルートブリッジ内のポートがリスニングからラーニング、ラーニングからフォワーディング状態に移移するまでの時間 (秒) を示す。MODE が RAPID のときは、ディスカードイングからラーニング、ラーニングからフォワーディング状態に移移するまでの最大時間 (秒) を示す。有効範囲は 4 ~ 30 秒。デフォルトは 15 秒。
HELLOTIME	ハロータイム。ルートブリッジが BPDU (Bridge Protocol Data Unit) を送信する間隔 (秒)。有効範囲は 1 ~ 10 秒。デフォルトは 2 秒。
MAXAGE	最大エージタイム。ルートブリッジから BPDU が届かなくなったことを認識するまでの時間 (秒)。この時間内に BPDU を受信できなかった場合、STPD 内の各ブリッジはスパンニングツリーの再構成を開始する。2 × (HELLOTIME + 1) 以上、かつ、2 × (FORWARDDELAY - 1) 以下でなくてはならない。有効範囲は 6 ~ 40 秒。デフォルトは 20 秒。
PRIORITY	ブリッジプライオリティー。小さいほど優先度が高く、ルートブリッジになる可能性が高くなる。MODE が RAPID のときは 4096 の倍数で指定する (4096 の倍数でない値を指定したときは、指定値より小さい直近の倍数に変換される)。有効範囲は 0 ~ 65535。デフォルトは 32768。
MODE	STP の動作モード。STANDARD (802.1d)、RAPID (802.1w) から選択する。動作モードを変更すると、STP のプロセスが初期化される。デフォルトは STANDARD。
RSTPTYPE	Rapid STP (MODE=RAPID) の動作モード。NORMAL (RSTP BPDU を使う)、STPCOMPATIBLE (標準の BPDU を使う) から選択する。デフォルトは NORMAL。



表 4:

STP ドメインのスパニングツリーパラメーター (MODE と RSTPTYPE を除く) をデフォルト値に戻したいときは、SET STP コマンド (377 ページ) の DEFAULT オプションを使います。

```
SET STP=default DEFAULT ↵
```

```
SET STP=ALL DEFAULT ↵
```

スイッチポートのスパニングツリーパラメーターを変更するには、SET STP PORT コマンド (379 ページ) を使います。変更できるパラメーターは次のとおりです。

パラメーター	説明
PATHCOST	パスコスト。該当ポートを通過する際のコストを示すもので、一般的にはポートの通信速度に応じて設定する。有効範囲は STP の動作モードによって異なり、STANDARD モードでは 1 ~ 1000000、RAPID モードでは 1 ~ 200000000。通信速度ごとのデフォルト値と推奨範囲は別表を参照のこと。
PORTPRIORITY	ポートプライオリティ。小さいほど優先度が高く、ルートポートになる可能性が高くなる。MODE が RAPID のときは 16 の倍数で指定する (16 の倍数でない値を指定したときは、指定値より小さい直近の倍数に変換される)。有効範囲は 0 ~ 255。デフォルトは 128。
EDGEPORT	MODE が RAPID のとき、該当ポートがエッジポートかどうかを指定する。エッジポートとは、他のブリッジが存在しない末端 (エッジ) の LAN に接続されているポートのこと。ただし、EDGEPORT=YES を指定した場合でも、同ポートで RSTP BPDU を受信した場合はエッジポートとしては扱われなくなる。デフォルトは NO。
PTP	MODE が RAPID のとき、該当ポートが他のブリッジとポイントツーポイントで接続されているかどうかを指定する。AUTO を指定した場合は、本製品が自動判別する。デフォルトは AUTO。

表 5:

通信速度	推奨範囲	デフォルト値
10Mbps	50 ~ 600	100
100Mbps	10 ~ 60	19
1000Mbps	3 ~ 10	4

表 6: STANDARD モードにおけるパスコストの推奨範囲とデフォルト値

通信速度	推奨範囲	デフォルト値
10Mbps	200000 ~ 2000000	2000000

100Mbps	20000 ~ 200000	200000
1000Mbps	2000 ~ 20000	20000

表 7: RAPID モードにおけるパスコストの推奨範囲とデフォルト値

スイッチポートのスパニングツリーパラメーター (EDGEPORT と PTP を除く) をデフォルト値に戻したいときは、SET STP PORT コマンド (379 ページ) の DEFAULT オプションを使います。

```
SET STP PORT=1 DEFAULT ↵
SET STP PORT=ALL DEFAULT ↵
```

特定ポートでスパニングツリープロトコルを無効にしたいときは、DISABLE STP PORT コマンド (267 ページ) を使います。

```
DISABLE STP PORT=2 ↵
```

特定ポートでスパニングツリープロトコルを再度有効にするには、ENABLE STP PORT コマンド (297 ページ) を使います。

```
ENABLE STP PORT=2 ↵
```

スパニングツリーの再初期化を行うには RESET STP コマンド (321 ページ) を実行します。

```
RESET STP=mystp ↵
```

スパニングツリープロトコルの設定をすべて消去するには、PURGE STP コマンド (315 ページ) を使います。デフォルト以外の STP ドメインはすべて削除され、パラメーターはすべてデフォルトに戻ります。

```
PURGE STP ↵
```

- ⚠ ランタイムメモリー上にあるスパニングツリープロトコル関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意してください。

## マルチプルスパニングツリープロトコル (MSTP)

マルチプルスパニングツリープロトコル (MSTP) は、既存のスパニングツリープロトコル (STP/RSTP) をもとに、VLAN 環境向けの機能拡張を施したレイヤー 2 のループ防止・冗長化プロトコルです。

この章では、MSTP の概要と使用方法について説明します。STP と RSTP については、「スイッチング」の「スパニングツリープロトコル (STP/RSTP)」をご覧ください。

- ✎ 本製品のマルチプルスパニングツリープロトコルは、IEEE802.1s Standard に準拠しています。IEEE802.1s ドラフトバージョンに準拠した装置とは接続できません。
- ✎ 既存のスパニングツリープロトコル (STP/RSTP) とマルチプルスパニングツリープロトコル (MSTP) を同時に有効化することはできません。なお、MSTP は、既存のスパニングツリープロトコル (STP/RSTP) を使用している機器との相互運用が可能です。
- ✎ マルチプルスパニングツリープロトコル (MSTP) とイーサネットリングプロテクション (EPSR) を同時に使用することはできません。

### 概要

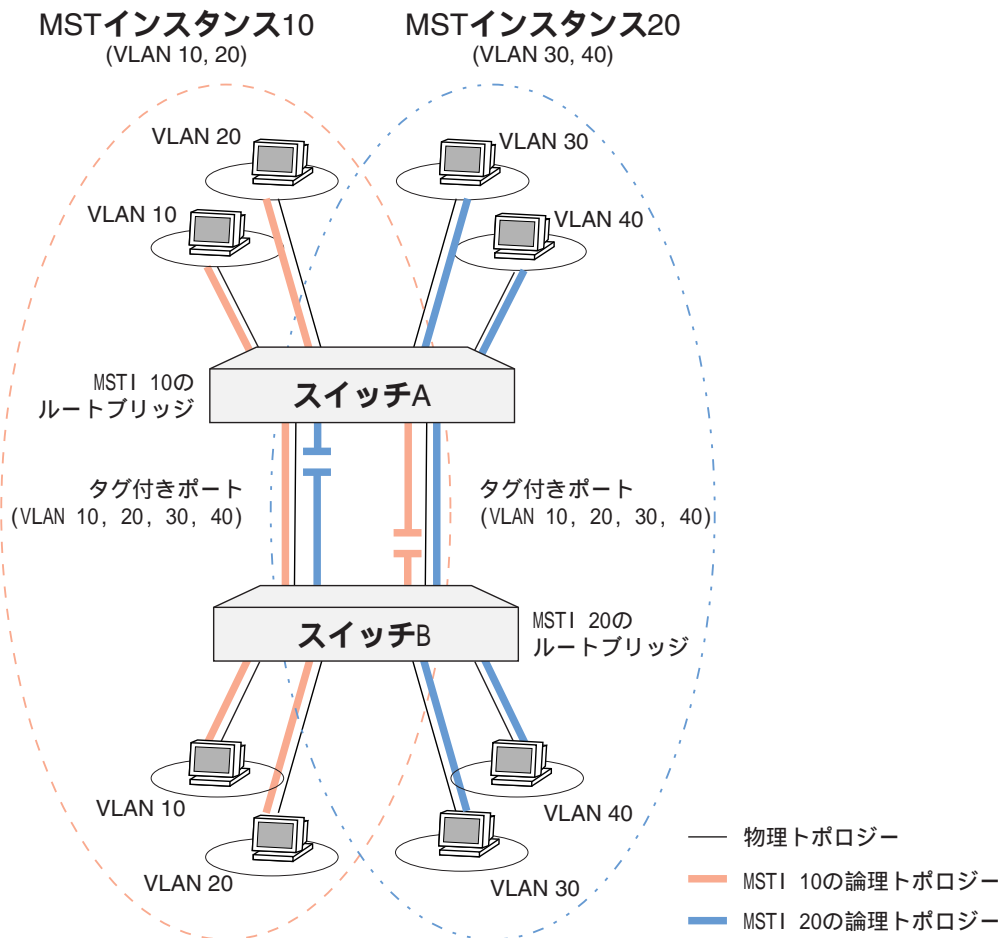
MSTP は、ツリー状の論理経路 (スパニングツリー) を自動的に形成してループを防止する点において、RSTP と同様の動作をします。

ただし、MSTP では、複数の VLAN を MST インスタンスと呼ばれるグループにまとめ、MST インスタンスごとにツリーを形成します。この特長をうまく利用すれば、タグ VLAN を利用したスイッチ間接続などにおいて、ネットワーク負荷を分散させることができます。また、VLAN ごとにツリーを形成する場合に比べて、VLAN 数の増加による CPU やネットワーク負荷の上昇を抑えることができます。

さらに、MSTP では、ネットワーク上のブリッジ (スイッチ) を MST リージョンと呼ばれるグループに分割し、MST リージョンごとに前述した MSTP の動作を行わせることができます。これは、大規模なネットワーク環境において、ネットワークの設計や管理を容易にする効果があります。

### MST インスタンス

MSTP では、複数の VLAN をまとめたものを MST インスタンス (MSTI) と呼び、MST インスタンスごとにスパニングツリーを形成します。MST インスタンスは、1 ~ 4094 のインスタンス ID で識別します。



MST インスタンスのルートブリッジは「リージョナルルート」と呼ばれ、MST インスタンスにおけるブリッジプライオリティーと MAC アドレスによって決定されます。

ブリッジプライオリティーは MST インスタンスごとに設定できるため、MST インスタンス「10」ではスイッチ A がルートブリッジ、MST インスタンス「20」ではスイッチ B がルートブリッジ、といった構成を組むことができます。また、ポートプライオリティーも MST インスタンスごとに設定できるため、MST インスタンスごとに最適なポートをルートポートにすることができます。これらの仕組みはトラフィックの負荷分散に有効です。

本製品の MST インスタンスの仕様は、次のとおりです。

- 最大 64 個の MST インスタンスを作成可能（これらとは別に、デフォルトで ID=0 の特殊なインスタンス (CIST) が存在する）
- MST インスタンスの範囲は、後述する MST リージョン内に限定される（インスタンス ID も MST リージョン内でのみ意味を持つ）
- 1 つの MST インスタンスに関連付ける VLAN 数に制限なし
- 1 つの VLAN は、1 つの MST インスタンス（または CIST）にのみ関連付けが可能

## MST リージョン

MSTP では、ネットワーク上のブリッジ (スイッチ) を MST リージョンと呼ばれるグループに分割することができます。MST リージョンは、他のリージョンからは 1 台の仮想ブリッジとして見えるため、MST リージョン内のトポロジーチェンジは MST リージョン内で完結し、リージョン外 (ネットワーク全体) には影響を与えません。

すなわち、MSTP の動作は、次の 2 つのレベルに分かれているということになります。

- MST リージョン内での動作  
MST リージョン内の MST インスタンスごとにツリーを形成。ある VLAN に所属するパケットは、その VLAN が関連付けられている MST インスタンスのツリーにしたがって転送される。
- MST リージョン間での動作  
MST リージョンを仮想ブリッジとみなしてネットワーク全体にわたるツリーを形成。個々のリージョン内のトポロジーには関知しない。

本製品の MST リージョンの仕様は、次のとおりです。

- 同一の MST リージョンに所属する装置では、以下の設定を同じにする。
  - MST リージョン名
  - MST リージョンのリビジョン
  - MST インスタンスと VLAN の関連付け (後述)
- 1 つの MST リージョンに所属するブリッジ数に制限なし
- 1 台のブリッジは、1 つの MST リージョンにのみ所属が可能

MSTP 対応ブリッジは、あるポートにおいて自身と異なる MST リージョン設定を持った MSTP BPDU を受信すると、該当ポートが MST リージョンの境界に位置するものと認識します。

また、旧バージョンの BPDU (STP BPDU、RSTP BPDU) を受信した場合も、受信ポートが MST リージョンの境界に位置するものと認識します。この場合、STP/RSTP ブリッジ (MSTP 非対応のブリッジ) は、1 つの MST リージョンとみなします。

#### MST インスタンスと VLAN の関連付けについて

本製品では、同一の MST リージョンに所属させたいすべての装置において、以下の設定内容を同じにしておく必要があります。

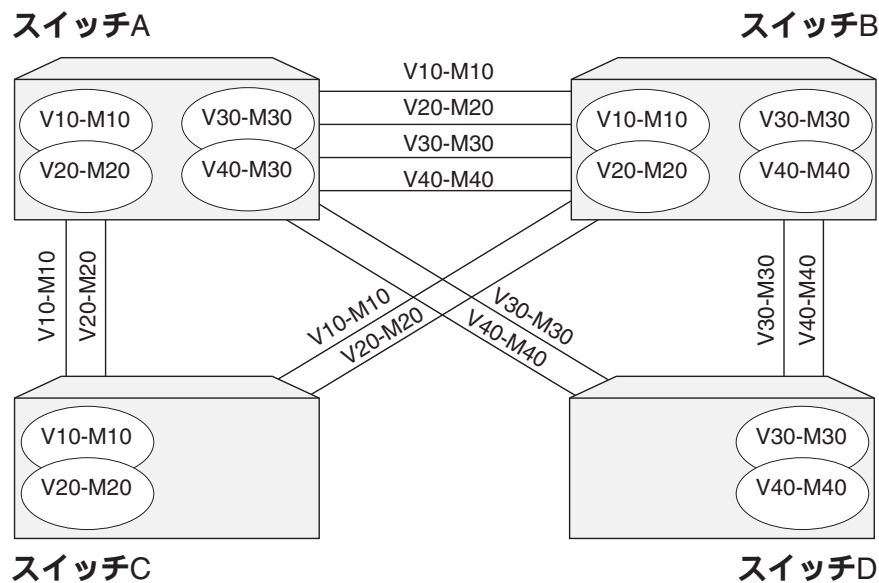
- MST リージョン名
- MST リージョンのリビジョン
- MST インスタンスと VLAN の関連付け (後述)

いずれか 1 つでも設定が他の装置と異なっていると、該当装置は同一リージョン所属とみなされず、結果的に意図した動作をしない可能性があるためご注意ください。

- 🔧 これらの設定が等しいことを確認するには、SHOW MSTP コマンド (425 ページ) を CONFIGID オプション付きで実行し、出力される情報がすべての装置で等しいことを確認してください。「MST インスタンスと VLAN の関連付け」に関しては、SHOW MSTP コマンド (425 ページ) の TABLE オプションで確認することもできます。

ここでは、「MST インスタンスと VLAN の関連付け」について、補足説明します。

例として、負荷分散のため本製品 4 台 (スイッチ A ~ D) で次の構成を組むと仮定とします。「V10-M10」のような表記は、MST インスタンス 10 に VLAN 10 が関連付けられていることを表しています。



ここでは、スイッチ A～D を同一 MST リージョンにするため、MST リージョン名とリビジョンをすべてのスイッチで同じに設定します。しかしそれだけでは、次表のように、各スイッチで「MST インスタンスと VLAN の関連付け」が異なっているため、実際には「スイッチ A と B」、「スイッチ C」、「スイッチ D」の 3 つのリージョンに分割されてしまいます。これでは、意図したとおりに負荷分散が行われません。

装置名		関連付け設定		
スイッチ A	V10-M10	V20-M20	V30-M30	V40-M40
スイッチ B	V10-M10	V20-M20	V30-M30	V40-M40
スイッチ C	V10-M10	V20-M20	-	-
スイッチ D	-	-	V30-M30	V40-M40

表 8: MST インスタンスと VLAN の関連付けが異なる例

意図どおりの動作をさせるには、次の追加設定が必要になります。

- スイッチ C 上で VLAN 30、40 および MST インスタンス 30、40 を定義し、VLAN 30 と MST インスタンス 30、VLAN 40 と MST インスタンス 40 を関連付ける。
- スイッチ D 上で VLAN 10、20 および MST インスタンス 10、20 を定義し、VLAN 10 と MST インスタンス 10、VLAN 20 と MST インスタンス 20 を関連付ける。

これにより、各スイッチの「MST インスタンスと VLAN の関連付け」設定が次のように同じになり、すべてのスイッチが同一リージョンとみなされるようになります。

装置名		関連付け設定		
スイッチ A	V10-M10	V20-M20	V30-M30	V40-M40
スイッチ B	V10-M10	V20-M20	V30-M30	V40-M40
スイッチ C	V10-M10	V20-M20	V30-M30	V40-M40

スイッチ D	V10-M10	V20-M20	V30-M30	V40-M40
--------	---------	---------	---------	---------

表 9: MST インスタンスと VLAN の関連付けが同一の例

## CIST

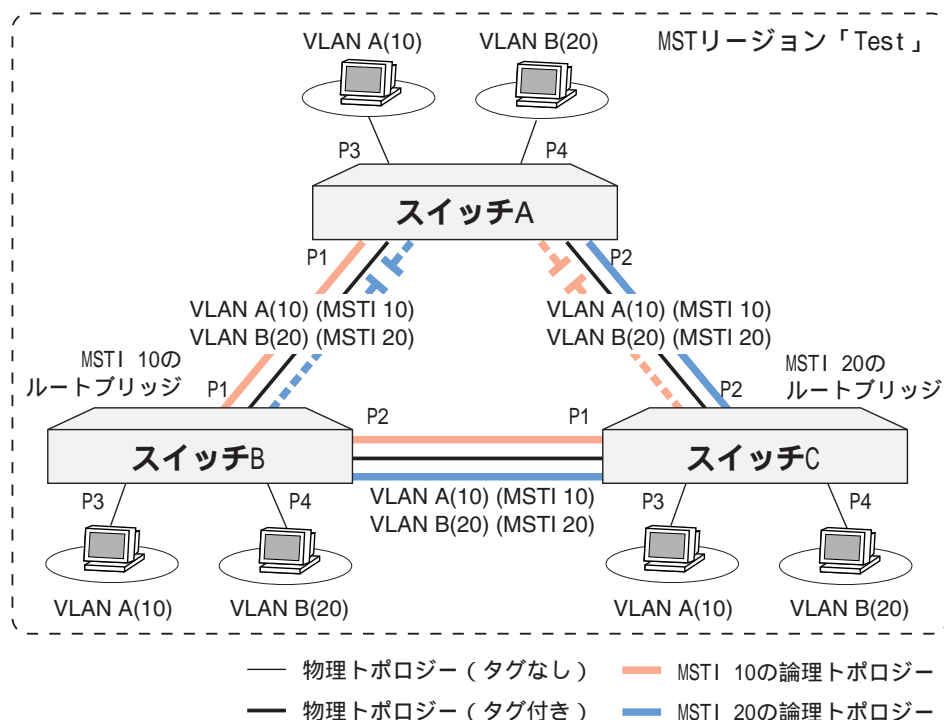
MSTP では、デフォルトで ID=0 の特殊なインスタンスが存在します。これは CIST (Common and Internal Spanning Tree) と呼ばれ、MST リージョン内のすべてのブリッジを接続し、さらには、MST リージョン同士を接続して、ネットワーク全体をカバーするスパニングツリーを形成します。

MST リージョン内における CIST ツリーのルートブリッジを「CIST リージョナルルート」、ネットワーク全体のルートブリッジ (CIST のルートブリッジ) を「CIST ルート」と呼びます。これらは CIST におけるブリッジプライオリティと MAC アドレスによって決定されます。

デフォルトでは、すべての VLAN が CIST に関連付けられています。VLAN を MST インスタンスに関連付けると、その VLAN は自動的に CIST との関連付けを解除されます。

## 基本設定

本製品で、マルチプルスパニングツリープロトコルを使用するための基本設定について説明します。ここでは、次のような構成を例に各スイッチの設定方法を説明します。



この例では、説明のため構成をシンプルにしていますので、各スイッチの設定はほとんど同じで、各 MST インスタンスのルートブリッジ（リージョナルルート）を決めるブリッジプライオリティの設定だけが異なります。

スイッチ A の設定

## 1. VLAN の設定を行います。

```
CREATE VLAN=A VID=10 ↵
CREATE VLAN=B VID=20 ↵
ADD VLAN=A PORT=1,2 FRAME=TAGGED ↵
ADD VLAN=B PORT=1,2 FRAME=TAGGED ↵
ADD VLAN=A PORT=3 ↵
ADD VLAN=B PORT=4 ↵
```

## 2. MST リージョンの識別情報を設定します。

この例では、すべてのスイッチを同一の MST リージョンに所属させるので、リージョン名 (CONFIGNAME) とリビジョン (REVISIONLEVEL) をすべてのスイッチで同じ値に設定します。ここではリージョン名を「Test」、リビジョンを 0 とします。さらに、続く手順 3~4 の設定内容 (MST インスタンスと VLAN の関連付け) もすべてのスイッチで同じになるようにします。

```
SET MSTP CONFIGNAME=Test REVISIONLEVEL=0 ↵
```

## 3. MST インスタンスを作成します。

```
CREATE MSTP MSTI=10 ↵
CREATE MSTP MSTI=20 ↵
```

## 4. MST インスタンスに VLAN を割り当てます。

```
ADD MSTP MSTI=10 VLAN=10 ↵
ADD MSTP MSTI=20 VLAN=20 ↵
```

## 5. 各 MST インスタンスにおけるブリッジプライオリティを設定します。スイッチ A はルートブリッジにするつもりがないので、どちらの MST インスタンスにおいても他のスイッチより低く (値が大きくなるよう、デフォルト値の 32768 のままで運用します (以下の 2 コマンドは実際には不要です)。

```
SET MSTP MSTI=10 PRIORITY=32768 ↵
SET MSTP MSTI=20 PRIORITY=32768 ↵
```

## 6. マルチプルスパニングツリープロトコルを有効にします。

```
ENABLE MSTP ↵
```

スイッチ B の設定 (MST インスタンス「10」のルートブリッジ)

## 1. VLAN の設定を行います。



```
CREATE VLAN=A VID=10 ↵
CREATE VLAN=B VID=20 ↵
ADD VLAN=A PORT=1,2 FRAME=TAGGED ↵
ADD VLAN=B PORT=1,2 FRAME=TAGGED ↵
ADD VLAN=A PORT=3 ↵
ADD VLAN=B PORT=4 ↵
```

2. MST リージョンの識別情報を設定します。

この例では、すべてのスイッチを同一の MST リージョンに所属させるので、リージョン名 (CONFIGNAME) とリビジョン (REVISIONLEVEL) をすべてのスイッチで同じ値に設定します。ここではリージョン名を「Test」、リビジョンを 0 とします。さらに、続く手順 3~4 の設定内容 (MST インスタンスと VLAN の関連付け) もすべてのスイッチで同じになるようにします。

```
SET MSTP CONFIGNAME=Test REVISIONLEVEL=0 ↵
```

3. MST インスタンスを作成します。

```
CREATE MSTP MSTI=10 ↵
CREATE MSTP MSTI=20 ↵
```

4. MST インスタンスに VLAN を割り当てます。

```
ADD MSTP MSTI=10 VLAN=10 ↵
ADD MSTP MSTI=20 VLAN=20 ↵
```

5. 各 MST インスタンスにおけるブリッジプライオリティーを設定します。スイッチ B は MST インスタンス「10」のルートブリッジにするので、MST インスタンス「10」におけるブリッジプライオリティーを他のスイッチより高く (値を小さく) 設定します。

```
SET MSTP MSTI=10 PRIORITY=4096 ↵
SET MSTP MSTI=20 PRIORITY=8192 ↵
```

6. マルチプルスパニングツリープロトコルを有効にします。

```
ENABLE MSTP ↵
```

スイッチ C の設定 (MST インスタンス「20」のルートブリッジ)

1. VLAN の設定を行います。

```
CREATE VLAN=A VID=10 ↵
CREATE VLAN=B VID=20 ↵
ADD VLAN=A PORT=1,2 FRAME=TAGGED ↵
ADD VLAN=B PORT=1,2 FRAME=TAGGED ↵
ADD VLAN=A PORT=3 ↵
ADD VLAN=B PORT=4 ↵
```

2. MST リージョンの識別情報を設定します。

この例では、すべてのスイッチを同一の MST リージョンに所属させるので、リージョン名 (CONFIGNAME) とリビジョン (REVISIONLEVEL) をすべてのスイッチで同じ値に設定します。ここではリージョン名を「Test」、リビジョンを 0 とします。さらに、続く手順 3~4 の設定内容 (MST インスタンスと VLAN の関連付け) もすべてのスイッチで同じになるようにします。

```
SET MSTP CONFIGNAME=Test REVISIONLEVEL=0 ↵
```

3. MST インスタンスを作成します。

```
CREATE MSTP MSTI=10 ↵
CREATE MSTP MSTI=20 ↵
```

4. MST インスタンスに VLAN を割り当てます。

```
ADD MSTP MSTI=10 VLAN=10 ↵
ADD MSTP MSTI=20 VLAN=20 ↵
```

5. 各 MST インスタンスにおけるブリッジプライオリティを設定します。スイッチ C は MST インスタンス「20」のルートブリッジにするので、MST インスタンス「20」におけるブリッジプライオリティを他のスイッチより高く (値を小さく) 設定します。

```
SET MSTP MSTI=10 PRIORITY=8192 ↵
SET MSTP MSTI=20 PRIORITY=4096 ↵
```

6. マルチプルスパニングツリープロトコルを有効にします。

```
ENABLE MSTP ↵
```

以上で設定は完了です。

マルチプルスパニングツリープロトコルを無効にするには、DISABLE MSTP コマンド (261 ページ) を使います。

DISABLE MSTP ↓

MST インスタンスと VLAN の関連付けを解除するには、DELETE MSTP MSTI VLAN コマンド (230 ページ) を使います。

DELETE MSTP MSTI=10 VLAN=10 ↓

MST インスタンスを削除するには、DESTROY MSTP MSTI コマンド (245 ページ) を使います。

DESTROY MSTP MSTI=10 ↓

- ✎ VLAN が関連付けられている MST インスタンスは削除できません。あらかじめ DELETE MSTP MSTI VLAN コマンド (230 ページ) を実行して、所属 VLAN をすべて削除しておいてください。

マルチブルスパニングツリープロトコルの全般的な設定を確認するには、SHOW MSTP コマンド (425 ページ) を使います。MST リージョンの識別情報を確認するときは CONFIGID オプションを、MST インスタンスと VLAN の関連付けを確認したいときは TABLE オプションを使用します。

SHOW MSTP ↓

SHOW MSTP CONFIGID ↓

SHOW MSTP TABLE ↓

- ✎ CONFIGID オプションで表示される情報が等しい装置は、同一の MST リージョンに所属していると見なされます。

MST インスタンスに関する情報を確認するには、SHOW MSTP MSTI コマンド (436 ページ) を使います。

SHOW MSTP MSTI ↓

SHOW MSTP MSTI=10 ↓

MST インスタンスにおけるポートの設定情報を確認するには、SHOW MSTP MSTI PORT コマンド (439 ページ) を使います。

SHOW MSTP MSTI=10 PORT=2 ↓

CIST に関する設定を確認するには、SHOW MSTP コマンド (425 ページ) で、CIST を指定します。

SHOW MSTP CIST ↓

CIST におけるポートの設定情報を確認するには、SHOW MSTP CIST PORT コマンド (431 ページ) を使います。

```
SHOW MSTP CIST PORT=4 ↵
```

## マルチプルスパニングツリーパラメーターの設定変更

設定パラメーターの変更方法など、より詳細な設定について解説します。

マルチプルスパニングツリーパラメーター（各種タイマーやリージョンの設定）を変更するには、SET MSTP コマンド（338 ページ）を使います。変更できるパラメーターは次のとおりです。

パラメーター	説明
CONFIGNAME	MST リージョン名。同一リージョンに所属させたい装置には、同じ名前を指定する。デフォルトは製品の MAC アドレス (xx-xx-xx-xx-xx-xx の型式)。
REVISIONLEVEL	MST リージョン設定のレビジョン。同一リージョンに所属させたい装置には、同じ数値を指定する。デフォルトは 0。
MAXHOPS	最大ホップ数。BPDU が MSTP ブリッジを抜けるごとにカウントダウンされる。BPDU の寿命カウンター。有効範囲は 1～40。デフォルトは 20。
MAXAGE	最大エージタイム。ルートブリッジから BPDU が届かなくなったことを認識するまでの時間 (秒)。この時間内に BPDU を受信できなかった場合、各ブリッジはスパニングツリーの再構成を開始する。2 × (HELLOTIME + 1) 以上、かつ、2 × (FORWARDDELAY - 1) 以下でなくてはならない。有効範囲は 6～40 秒。デフォルトは 20 秒。
HELLOTIME	ハロータイム。ルートブリッジが BPDU (Bridge Protocol Data Unit) を送信する間隔 (秒)。有効範囲は 1～10 秒。デフォルトは 2 秒。
FORWARDDELAY	フォワードディレイタイム。ネットワーク構成の変更後に、ルートブリッジ内のポートがディスカードイングからラーニング、ラーニングからフォワードイング状態に遷移するまでの最大時間 (秒) を示す。有効範囲は 4～30 秒。デフォルトは 15 秒。
PROTOCOLVERSION	MSTP の動作モード。MSTP (MSTP BPDU を使う)、RSP (RSTP BPDU を使う)、STP (STP BPDU を使う) から選択する。デフォルトは MSTP。
STATICVLANs	スパニングツリーのトポロジー計算時、MST インスタンスに所属している VLAN のポート構成を考慮するかどうか。YES を指定した場合は、VLAN のポート構成を考慮して計算を行う (MST インスタンスに所属している VLAN のメンバーポートだけを利用してトポロジーを計算する)。NO を指定した場合は、VLAN のポート構成を考慮せずに通常の MSTP の方法で計算を行う (MST インスタンスに所属している VLAN のメンバーポートだけでなく、すべての物理ポートを使用して計算を行う)。ブリッジ (スイッチ) 間を接続しているすべてのポートが同じ VLAN 設定であるなら OFF でよいが、そうでない場合は、特定の MST インスタンスにおいて、所属 VLAN のメンバーでないポートがルートポートになる可能性がある。このようなときは ON を指定するとよい (OFF のままでも、メンバーポートのポートプライオリティーやポートパスコストを調整すれば同じ効果を得られる)。デフォルトは OFF。

表 10:

MST インスタンスにおけるブリッジプライオリティーを変更するには、SET MSTP MSTI コマンド (343 ページ) を使います。設定できる値の範囲は 0～65535 ですが、実際に使用される値は 4096 の倍数に丸められます (指定値が 4096 の倍数でない場合、指定値よりも小さい直近の倍数が使われます)。デフォルトは 32768 です。

```
SET MSTP MSTI=10 PRIORITY=8192 ↵
```

CIST におけるブリッジプライオリティを変更するには、SET MSTP CIST コマンド (340 ページ) を使います。設定できる値の範囲は 0 ~ 65535 ですが、実際に使用される値は 4096 の倍数に丸められます (指定値が 4096 の倍数でない場合、指定値よりも小さい直近の倍数が使われます)。デフォルトは 32768 です。

```
SET MSTP CIST PRIORITY=4096 ↵
```

MST インスタンスにおけるスイッチポートのパラメーターを変更するには、SET MSTP MSTI PORT コマンド (344 ページ) を使います。変更できるパラメーターは次のとおりです。

パラメーター	説明
PRIORITY	MST インスタンス内でのトポロジー形成で使用するポートプライオリティ。小さいほど優先度が高く、ルートポートになる可能性が高くなる。設定できる値の範囲は 0 ~ 255 だが、実際に使用される値は 16 の倍数に丸められる (指定値が 16 の倍数でない場合、指定値よりも小さい直近の倍数が使われる)。デフォルトは 128。
PATHCOST	リージョナルルート (MST インスタンスのルートブリッジ) までのパスに対するポート通過コスト。有効範囲は 1 ~ 200000000。通信速度ごとのデフォルト値と推奨範囲は別表を参照のこと。

表 11:

通信速度	推奨範囲	デフォルト値
10Mbps	200000 ~ 2000000	2000000
100Mbps	20000 ~ 200000	200000
1000Mbps	2000 ~ 20000	20000

表 12: パスコストの推奨範囲とデフォルト値

CIST におけるスイッチポートのパラメーターを変更するには、SET MSTP CIST PORT コマンド (341 ページ) を使います。変更できるパラメーターは次のとおりです。

パラメーター	説明
PRIORITY	CIST 内のトポロジー形成で使用するポートプライオリティ。小さいほど優先度が高く、ルートポートになる可能性が高くなる。設定できる値の範囲は 0 ~ 255 だが、実際に使用される値は 16 の倍数に丸められる (指定値が 16 の倍数でない場合、指定値よりも小さい直近の倍数が使われる)。デフォルトは 128。

INTPATHCOST	CIST リージョナルルート (MST リージョン内における CIST ツリーのルートブリッジ) までのパスに対するポート通過コスト。有効範囲は 1 ~ 200000000。通信速度ごとのデフォルト値と推奨範囲は別表を参照のこと。なお、一度値を設定したあとでデフォルト状態に戻すときはキーワード DEFAULT を指定する
ETXPathCOST	CIST ルートブリッジが所属するリージョンまでのパスに対するポート通過コスト。有効範囲は 1 ~ 200000000。通信速度ごとのデフォルト値と推奨範囲は別表を参照のこと。なお、一度値を設定したあとでデフォルト状態に戻すときはキーワード DEFAULT を指定する
EDGEPORT	該当ポートがエッジポートかどうかを指定する。エッジポートとは、他のブリッジが存在しない末端 (エッジ) の LAN に接続されているポートのこと。ただし、EDGEPORT=YES を指定した場合でも、同ポートで MSTP BPDU を受信した場合はエッジポートとしては扱われなくなる。デフォルトは NO。
POINTTOPOINT	該当ポートが他のブリッジとポイントツーポイントで接続されているかどうかを指定する。AUTO を指定した場合は、本製品が自動判別する。デフォルトは AUTO。

表 13:

通信速度	推奨範囲	デフォルト値
10Mbps	200000 ~ 2000000	2000000
100Mbps	20000 ~ 200000	200000
1000Mbps	2000 ~ 20000	20000

表 14: パスコストの推奨範囲とデフォルト値

他のブリッジが存在していないことが確かなポート (PC などの端末接続用のポート) は、エッジポートに設定すると無駄な処理を減らすことができます。エッジポートの設定は、SET MSTP CIST PORT コマンド (341 ページ) の EDGEPORT パラメーターで行います。

```
SET MSTP CIST PORT=12-24 EDGEPORT=YES ↵
```

マルチブスパンニングツリープロトコルの設定をすべて消去するには、PURGE MSTP コマンド (312 ページ) を使います。パラメーターはすべてデフォルトに戻ります。

```
PURGE MSTP ↵
```

- ⚠ ランタイムメモリー上にあるマルチブスパンニングツリープロトコル関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意してください。

## イーサネットリングプロテクション (EPSR)

イーサネットリングプロテクション (EPSR = Ethernet Protected Switched Ring) は、リング構成の Ethernet ネットワークに特化したレイヤー 2 のループ防止・冗長化機能です。

EPSR は、スパニングツリープロトコル (STP/RSTP/MSTP) と同様な機能を提供するものですが、トポロジを限定し、各スイッチの役割をあらかじめ固定しておくことで、障害の検出と経路の切り替えをより高速に行います (最短 50 ミリ秒未満)。

この章では、EPSR の概要と使用方法について説明します。

- ☞ マルチプルスパニングツリープロトコル (MSTP) とイーサネットリングプロテクション (EPSR) を同時に使用することはできません。

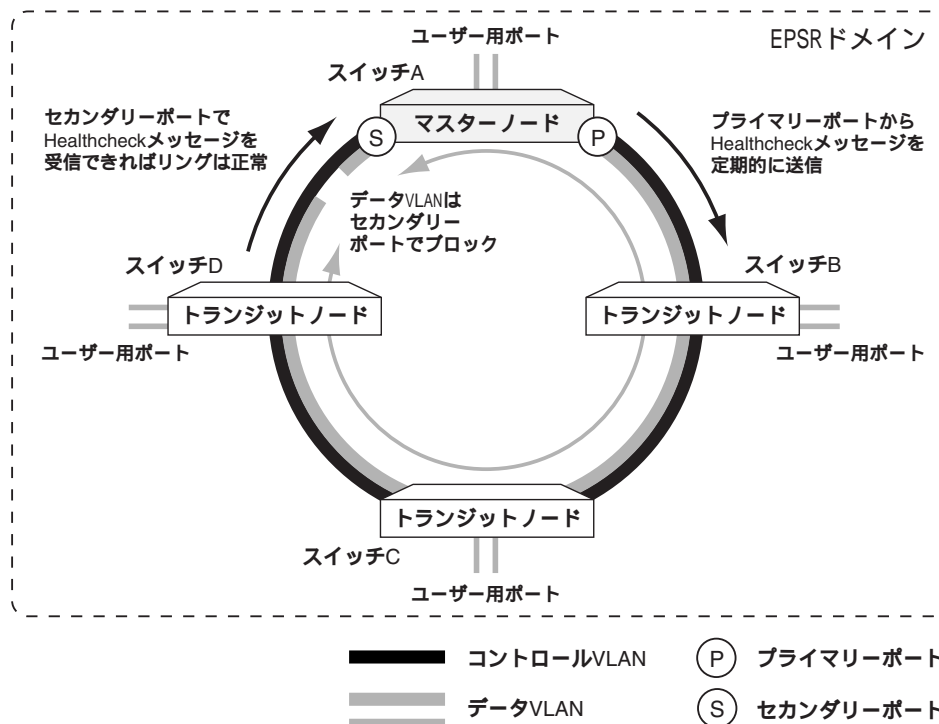
### 概要

EPSR は、リング構成の Ethernet ネットワークでのみ動作します。

EPSR リングは複数のスイッチ (ノード) で構成され、そのうちの 1 台はリングの動作を制御するマスターノードとして、他はトランジットノードとして設定します。

各スイッチは 2 つのポートで Ethernet リングに接続します。マスターノード上のポートは、一方をプライマリーポート、もう一方をセカンダリーポートとして設定します。データトラフィックに対し、プライマリーポートは常時フォワーディング状態ですが、セカンダリーポートは通常ブロック状態であり、リングに障害が発生したときだけフォワーディング状態に切り替わります。障害から復旧したときは再度ブロック状態に戻ります。

次にリングの基本的な構成を示します。





## EPSR ドメイン

EPSR の保護機能 (ループ防止・冗長化機能) は、EPSR ドメインと呼ばれる単位ごとに実行されます。EPSR ドメインで定義されるのはおもに次の情報です。

- EPSR ノード  
EPSR 対応スイッチのこと。それぞれ 2 つのポート (トランクグループは 1 ポート扱い) で Ethernet リングに接続する。役割上次の 2 つに分類される。
  - － マスターノード (1 台)
  - － トランジットノード (複数台)
- コントロール VLAN  
EPSR ドメインの動作を制御するための VLAN。制御メッセージだけがやりとりされる。各 EPSR ドメインに 1 つだけ設定。2 つのポート (タグ付き) で構成される。
- データ VLAN  
保護対象の VLAN。通常のトラフィックが運ばれる。各 EPSR ドメインには複数のデータ VLAN を指定可。リング上ではコントロール VLAN の 2 ポートを共有する。さらに、通常はユーザー接続用のメンバーポートを持つ

## マスターノードとトランジットノード

EPSR ドメインを構成するリング上の各スイッチは、役割上マスターノードとトランジットノードに分類されます。マスターノードは、該当 EPSR ドメインの動作を制御するスイッチで、各ドメインに 1 台だけ設定できます。その他のスイッチはトランジットノードとなります。

各ノードは 2 つのポート (トランクグループは 1 ポート扱い) で EPSR ドメインの Ethernet リングに接続します。リング上での通信は、制御トラフィック、データトラフィックともにこの 2 ポートを通じて行われるため、これらのリング接続用ポートはタグ付きに設定することとなります。

## プライマリーポートとセカンダリーポート

マスターノードでは、2 つのリング接続用ポートをプライマリーポートとセカンダリーポートに設定します。プライマリーポートは、コントロール VLAN、データ VLAN の両方に対して、つねにフォワーディング状態にある (送受信を行える) ポートです。

一方、セカンダリーポートは、コントロール VLAN に対してはつねにフォワーディング状態ですが、データ VLAN に対してはループを防ぐため通常はブロッキング状態になっています。リングに障害が発生した場合は、データ VLAN に対してもフォワーディング状態となり、送受信を行います。リングが障害から回復したときは、再びブロッキング状態となってループを防止します。

## コントロール VLAN とデータ VLAN

EPSR ドメインは、制御メッセージを運ぶコントロール VLAN と、通常データを運ぶデータ VLAN で構成されます。

コントロール VLAN は各ドメインに 1 つだけ設定でき、各スイッチ上においては純粹に 2 つのポート (トランクグループは 1 ポート扱い) で構成しなくてはなりません。

一方、データ VLAN は 1 つの EPSR ドメインに対して複数設定できます。データ VLAN は、リング上ではコントロール VLAN の 2 ポートを共有して通信を行います。また、通常データ VLAN は、リング接続ポート以外にユーザー接続用のメンバーポートを持ちます。

### 制御メッセージ

コントロール VLAN では、次の制御メッセージがやりとりされます。EPSR では、これらの制御メッセージを使って、リング障害の発生・回復を検出し、通信回復のための処置を行います。

メッセージ名	機能
Healthcheck	リング障害を検出するため、マスターノードが定期的にプライマリーポートから送出するメッセージ。マスターノードは、一定の時間内にセカンダリーポートで Healthcheck メッセージを受信できなかった場合、リングに障害が発生したと判断する。障害発生中もマスターノードは Healthcheck メッセージを送出し続け、セカンダリーポートで再び受信した場合にリングが障害から回復したと判断する
Ring Up	リングが障害から回復したと判断したマスターノードが、トランジットノードに対して FDB をクリアするよう指示するために送出するメッセージ
Ring Down	リングに障害が発生したと判断したマスターノードが、トランジットノードに対して FDB をクリアするよう指示するために送出するメッセージ
Link Down	自身のリング接続用ポートがリンクダウンしたことを検出したトランジットノードが、リング障害の発生をマスターノードに伝えるために送出するメッセージ。Link Down メッセージを受信したマスターノードは、リングに障害が発生したと判断して、Healthcheck メッセージがタイムアウトしたときと同様のアクションをとる

表 15: EPSR 制御メッセージ

### 障害検出機能

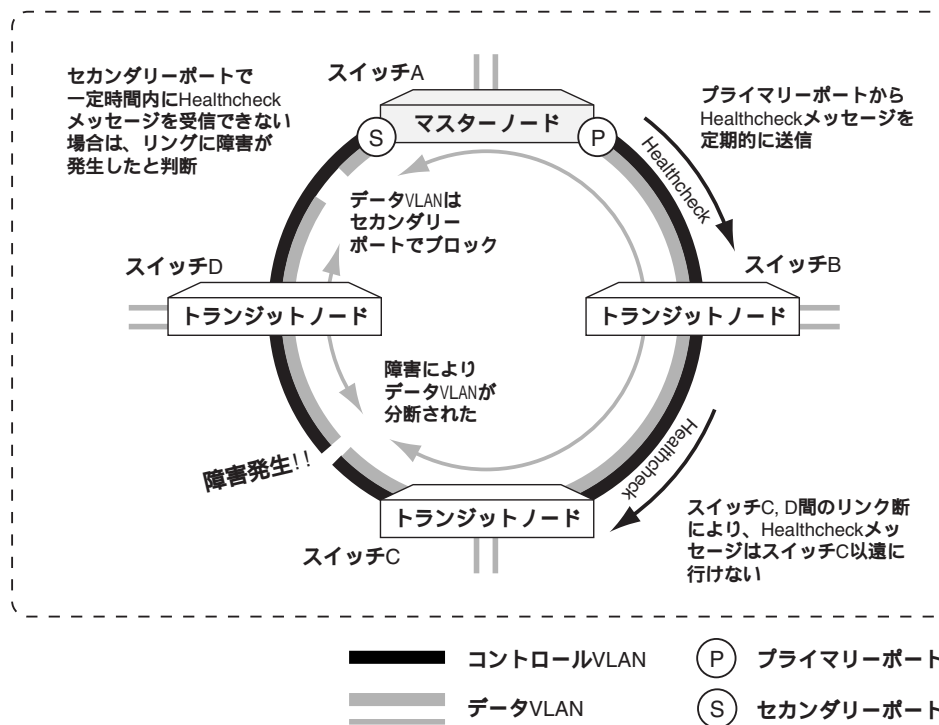
EPSR では、リング障害（ケーブルやスイッチの障害）を検出するために、次の 2 つの手段を用います。

- Healthcheck メッセージ（マスターノードによるポーリング）
- Link Down メッセージ（トランジットノードによる障害通知）

#### Healthcheck メッセージ

マスターノードは、コントロール VLAN 上において、プライマリーポートから Healthcheck メッセージを定期的に送出します。一定の時間内にセカンダリーポートで Healthcheck メッセージを受信できなかった場合は、リングに障害が発生したと判断します。

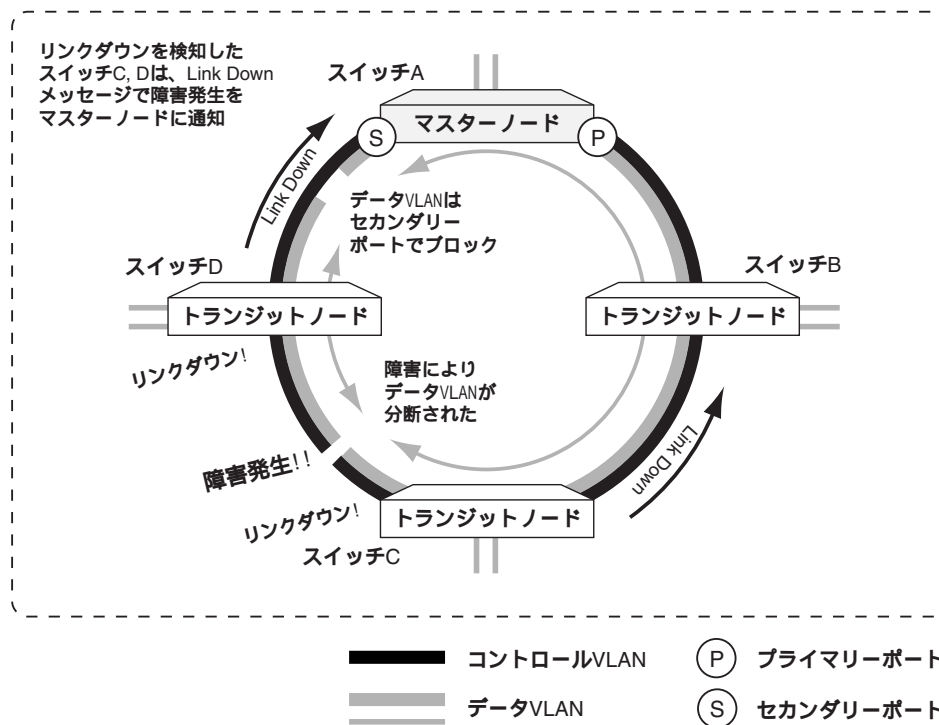
マスターノードは、障害発生中も Healthcheck メッセージを送出し続け、セカンダリーポートで再び受信できるようになると、リングが障害から回復したと判断します。



### Link Down メッセージ

トランジットノードは、リングに接続しているポートがリンクダウンしたことを検出すると、もう一方のポートから Link Down メッセージを送出して、障害発生をマスターノードに伝えます。

Link Down メッセージを受信したマスターノードは、リングに障害が発生したと判断して、Healthcheck メッセージがタイムアウトしたときと同様のアクションをとります。

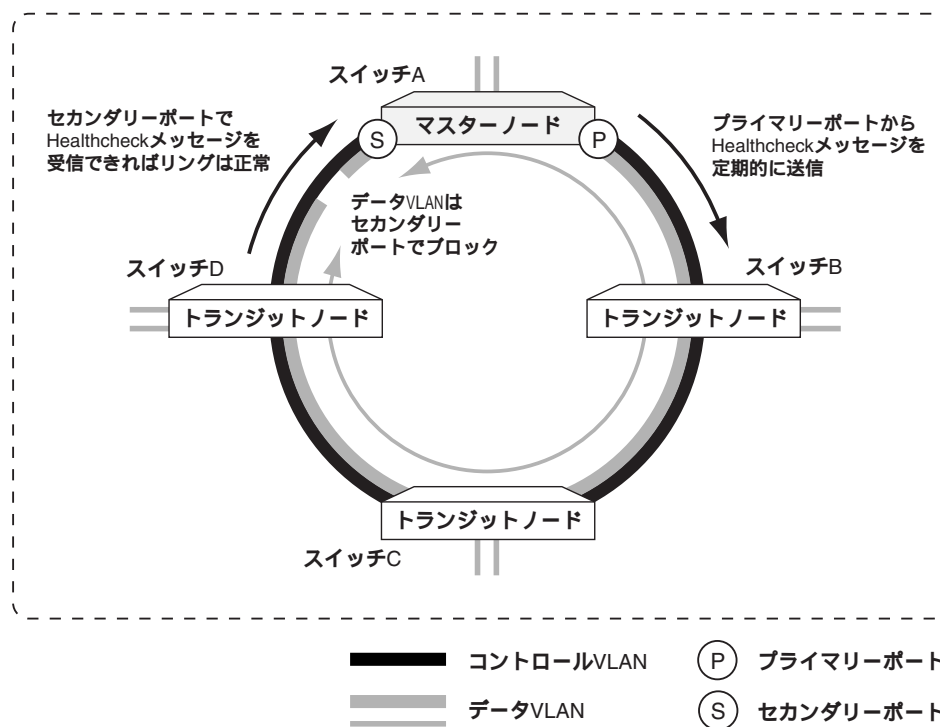


## 基本動作

次に、EPSR の基本的な動作について説明します。

### 正常動作時

EPSR ドメインを構成するリングに障害が発生していない場合、マスターノードがプライマリーポートから送出した Healthcheck メッセージは、一定時間内にセカンダリーポートに到着します。マスターノードはリングが「Complete」状態にあると見なし、データ VLAN に対してセカンダリーポートをブロックします。

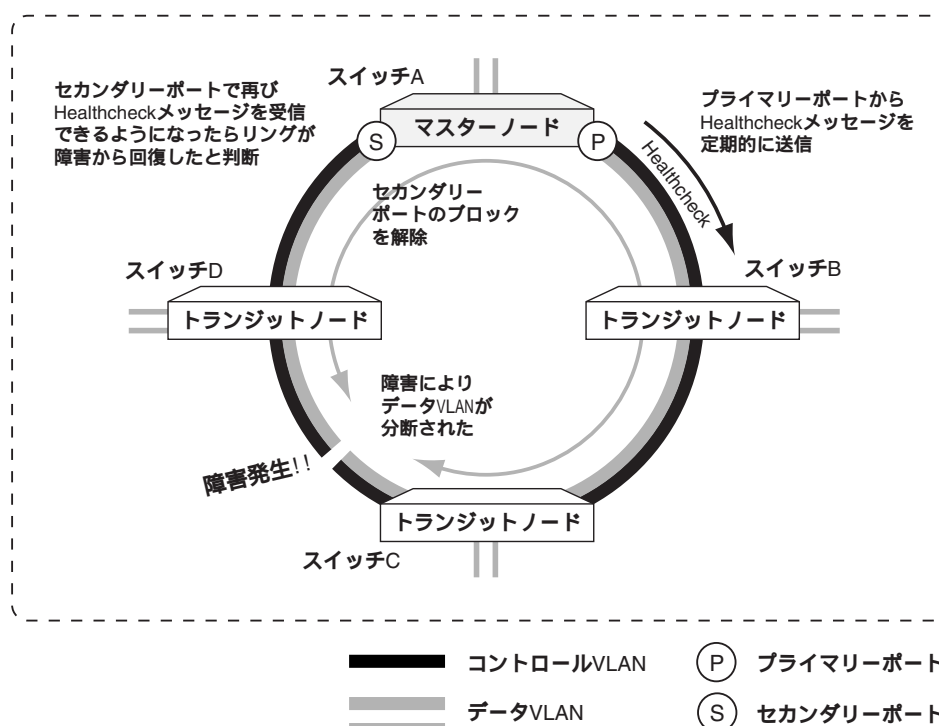


### 障害発生時

マスターノードは、一定時間内にセカンダリーポートで Healthcheck メッセージを受信できなかった場合、または、トランジットノードから Link Down メッセージを受信した場合、リングに障害が発生したと判断します。

マスターノードはリングを「Failed」状態に移行させ、データ VLAN に対してセカンダリーポートのブロックを解除します。また FDB をクリアして MAC アドレスを再学習します。

さらに、マスターノードは Ring Down メッセージをすべてのトランジットノードに送信して、FDB をクリアするよう指示します。これにより、リング上での通信が復旧します。



なお、マスターノードは、障害の回復を検出するため障害発生中も Healthcheck メッセージを通常どおり送出し続けます。

#### 障害回復時

障害が回復すると、マスターノードはセカンダリーポートで再び Healthcheck メッセージを受信できるようになります。

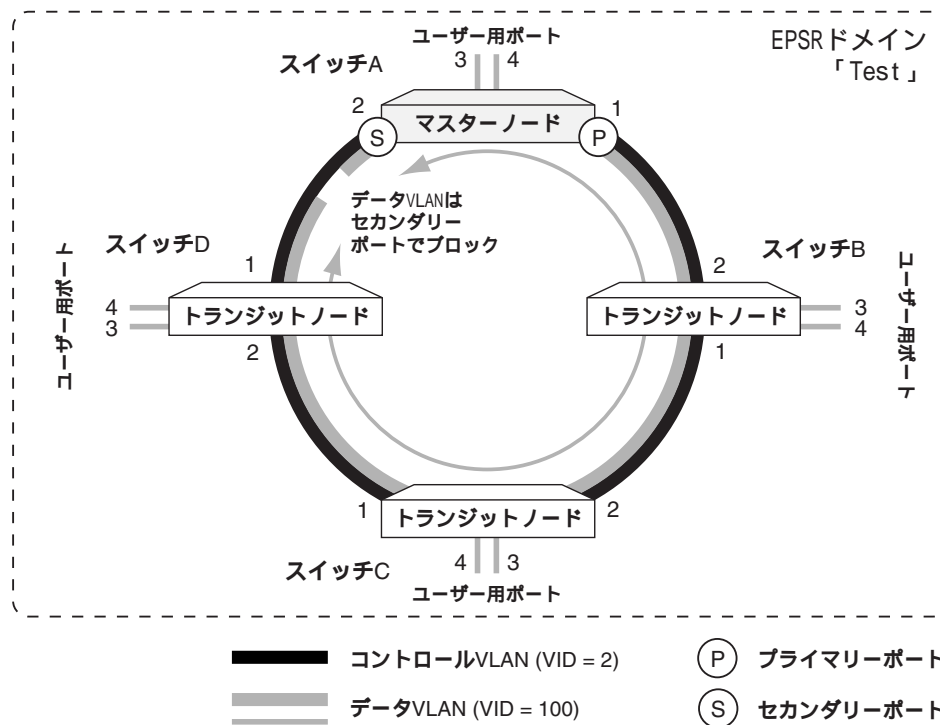
この場合、マスターノードはリングを「Complete」状態に復帰させ、データ VLAN に対してセカンダリーポートを再度ブロックします。また FDB をクリアして MAC アドレスを再学習します。

さらに、マスターノードは Ring Up メッセージをすべてのトランジットノードに送信して、FDB をクリアするよう指示します。これにより、リング上での通信が正常時の動作に復旧します。

なお、障害発生箇所に接続されているトランジットノードは、リング接続用ポートのリンクアップにより障害の回復を検知できますが、このとき、復旧したポートをデータ VLAN に対してただちにフォワーディング状態に戻すとループが起こる可能性があるため、該当ポートを一時的にプリフォワーディング状態に遷移させ、マスターノードから Ring Up メッセージが届くのを待って、FDB をクリアし、該当ポートをフォワーディング状態に戻します。

## 基本設定

EPSR を使用するための基本設定について説明します。ここでは次のような構成を例に各スイッチの設定方法を説明します。



この例では、説明のため構成をシンプルにしていますので、マスターノードとトランジットノードの設定の違いは、EPSRドメインを作成する箇所だけです。また、トランジットノード（スイッチB、C、D）の設定はどのスイッチも同じです。

スイッチA（マスターノード）の設定

1. コントロールVLANを作成します。

コントロールVLANはちょうど2ポートで構成しなくてはならず、さらに両ポートともタグ付きに設定する必要があります。

```
CREATE VLAN=ctrl VID=2 ↵
ADD VLAN=ctrl PORT=1,2 FRAME=TAGGED ↵
```

📎 コントロールVLANにはレイヤー3以上の設定（IPアドレスの設定など）を行わないでください。コントロールVLANはリングを構成・制御するためだけに存在するVLANです。

2. データVLANを作成します。

データVLANは、リング接続用のポート2つとユーザー接続用のポートで構成します。リング接続用のポートは、コントロールVLANのメンバーポートと同じポートで、同じくタグ付きに設定します。一方、ユーザー接続用のポートは通常タグなしに設定します。

```
CREATE VLAN=data VID=100 ↵
ADD VLAN=data PORT=1,2 FRAME=TAGGED ↵
ADD VLAN=data PORT=3,4 ↵
```

- ここまでの設定では、リング接続用のポート 1、2 がデフォルト VLAN に（タグなしポートとして）所属したままなので、これらのポートをデフォルト VLAN から明示的に削除します。

```
DELETE VLAN=default PORT=1,2 ↵
```

- EPSR ドメイン「Test」を作成します。動作モードは MASTER を指定します。マスターノードでは、コントロール VLAN とプライマリポートを指定してください。

```
CREATE EPSR=Test MODE=MASTER CONTROLVLAN=ctrl PRIMARYPORT=1 ↵
```

- EPSR ドメイン「Test」のデータ VLAN を指定します。

```
ADD EPSR=Test DATAVLAN=data ↵
```

- EPSR ドメイン「Test」を有効にします。

```
ENABLE EPSR=Test ↵
```

#### スイッチ B、C、D（トランジットノード）の設定

- コントロール VLAN を作成します。

コントロール VLAN はちょうど 2 ポートで構成しなくてはならず、さらに両ポートともタグ付きに設定する必要があります。

```
CREATE VLAN=ctrl VID=2 ↵
ADD VLAN=ctrl PORT=1,2 FRAME=TAGGED ↵
```

🔑 コントロール VLAN にはレイヤー 3 以上の設定（IP アドレスの設定など）を行わないでください。コントロール VLAN はリングを構成・制御するためだけに存在する VLAN です。

- データ VLAN を作成します。

データ VLAN は、リング接続用のポート 2 つとユーザー接続用のポートで構成します。リング接続用のポートは、コントロール VLAN のメンバーポートと同じポートで、同じくタグ付きに設定します。一方、ユーザー接続用のポートは通常タグなしに設定します。



```
CREATE VLAN=data VID=100 ↵  
ADD VLAN=data PORT=1,2 FRAME=TAGGED ↵  
ADD VLAN=data PORT=3,4 ↵
```

3. ここまでの設定では、リング接続用のポート 1、2 がデフォルト VLAN に（タグなしポートとして）所属したままなので、これらのポートをデフォルト VLAN から明示的に削除します。

```
DELETE VLAN=default PORT=1,2 ↵
```

4. EPSR ドメイン「Test」を作成します。動作モードは TRANSIT を指定します。トランジットノードでは、コントロール VLAN だけを指定してください。

```
CREATE EPSR=Test MODE=TRANSIT CONTROLVLAN=ctrl ↵
```

5. EPSR ドメイン「Test」のデータ VLAN を指定します。

```
ADD EPSR=Test DATAVLAN=data ↵
```

6. EPSR ドメイン「Test」を有効にします。

```
ENABLE EPSR=Test ↵
```

以上で設定は完了です。

# フォワーディングデータベース

フォワーディングデータベース（FDB）は、スイッチが受信フレームの転送先ポートを決定するために使用するデータベースです。

## FDB エントリー

FDB 内の各エントリーは次のようなフィールドで構成されています。

フィールド	内容
MAC アドレス	ステーションの MAC アドレス
ポート番号	ステーションが存在するポート
VLAN ID	ステーションが所属する VLAN
アクション	該当ステーション宛てフレームの処理方法。転送（FORWARD）と破棄（DISCARD）がある。

表 16:

スイッチは、フレームの宛先 MAC アドレスをキーに FDB を検索して出力ポートを決定します。宛先アドレスが FDB に登録されていない場合は、同一の VLAN に所属するすべてのポート（受信ポートを除く）からフレームを出力します（フラッドイング）。

FDB エントリーには、次のような種類があります。

種別	内容
ダイナミックエントリー	学習機能により自動的に登録されたエントリー。一定時間受信がなかったエントリーは削除される（エージング）。また、システムを再起動すると、すべてのエントリーが削除される
スタティックエントリー	管理者が手動で登録したエントリー。エージングによって削除されることはない。設定をファイルに保存すれば、再起動後にも使用できる。また、特定アドレス宛てのフレームを破棄するよう設定することもできる。ADD SWITCH FILTER コマンドで登録する
ポートセキュリティ（learn）エントリー	ポートセキュリティ機能の「学習済みアドレス」としてカウントされる特殊なエントリー。SET SWITCH PORT コマンドの RELEARN パラメーターで、エージアウトするかどうかを設定できる。ポートセキュリティ機能をオフにする、RELEARN の設定を変更する、またはシステムの再起動によって削除される。ポートセキュリティ機能が有効なポートで自動学習されるほか、ADD SWITCH FILTER コマンドに LEARN オプションを付けて手動登録することもできる。ポートセキュリティ機能は、SET SWITCH PORT コマンドの LEARN パラメーターで設定する

表 17:

FDB はスイッチの学習機能によって自動的に構築されていくため、通常管理者が設定すべきことはありませんが、FDB を参照したり、タイマー設定を変更したり、エントリーを手動で登録したりすることも可能です。

## 自動学習とダイナミックエントリー

スイッチは、その動作の過程において、受信フレームの送信元 MAC アドレスと受信ポートの情報に基づき FDB エントリーを動的に作成していきます。これを自動学習機能と呼びます。また、自動学習により登録されたエントリーをダイナミックエントリーと呼びます。

個々のダイナミックエントリーにはタイマーが用意されており、一定時間（エージングタイム）受信のなかったアドレスは FDB から削除されるようになっていきます。これは、電源が切られたり、移動したりして無効になったエントリーが、いつまでも残らないようにするためです。一方、時間内に再度受信があったときはタイマーがリセットされます。このようにして、常に最新の情報が保たれます。

FDB の内容を確認するには、SHOW SWITCH FDB コマンド（503 ページ）を実行します。

ダイナミックエントリーを削除するには、RESET SWITCH コマンド（322 ページ）を実行します。ただし、本コマンドを実行すると、ダイナミックエントリーがクリアされるだけでなく、ポートやカウンタもリセットされてしまうため注意が必要です。

自動学習機能はデフォルトでオンになっています。これをオフにするには DISABLE SWITCH LEARNING コマンド（271 ページ）を使います。また再度オンにするには、ENABLE SWITCH LEARNING コマンド（271 ページ）を使います。

マンド (301 ページ) を実行します。

- ✎ 学習機能をオフにすると、ほとんどのフレームが同一 VLAN 内の全ポートに出力されるようになるため、スイッチというよりも HUB に近い動作となります。

エージングタイム (MAC アドレス保持時間) を変更するには SET SWITCH AGEINGTIMER コマンド (381 ページ) を使用します。10 ~ 1000000 (11 日と 13 時間 46 分 40 秒) の範囲で指定できます。デフォルトは 300 秒 (5 分) です。

```
SET SWITCH AGEINGTIMER=600 ↵
```

エージングを無効にするには DISABLE SWITCH AGEINGTIMER コマンド (269 ページ) を実行します。これにより、ダイナミックエントリは登録されるだけで削除されなくなります。デフォルトではエージングは有効です。再度有効にするには ENABLE SWITCH AGEINGTIMER コマンド (299 ページ) を実行します。

自動学習とエージングの設定を確認するには SHOW SWITCH コマンド (490 ページ) を使います。「Learning」(自動学習機能)、「Ageing Timer」(エージング)、「AgeingTime」(エージングタイム) の表示をご覧ください。

## スタティックエントリ

手動で FDB エントリを追加するには ADD SWITCH FILTER コマンド (186 ページ) を使います。手動登録では、転送先ポートを指定する一般的なスタティックエントリだけでなく、特定アドレス宛てのフレームを破棄するためのエントリも作成できます。また、ポートセキュリティ機能の「学習済みアドレス」としてカウントされるエントリも登録できます。

FDB エントリは 1 ポートあたり 320 件まで登録可能です。

タグなしポートにスタティックエントリを追加します。

```
ADD SWITCH FILTER DEST=00-00-f4-12-34-56 PORT=10 ACTION=FORWARD ↵
```

タグ付きポートにスタティックエントリを追加するときは、VLAN 名または VLAN ID も指定します。指定しなかった場合は該当ポートのタグなし VLAN を指定したものと見なされます。そのため、ポートがタグ付き VLAN にしか所属していない場合は必ず指定する必要があります。

```
ADD SWITCH FILTER DEST=00-00-f4-99-88-76 PORT=1 VLAN=white  
ACTION=FORWARD ↵
```

特定アドレス宛てのフレームを破棄するには、ACTION に DISCARD を指定します。

```
ADD SWITCH FILTER DEST=00-00-f4-ab-cd-ef PORT=6 ACTION=DISCARD ↵
```

ポートセキュリティ機能が有効なポートに対して「学習済みアドレス」を追加するには、LEARN オプションを付けます。ポートセキュリティ機能は SET SWITCH PORT コマンド (387 ページ) の LEARN パラメーターで設定します。

```
ADD SWITCH FILTER DEST=00-00-f4-c9-73-ff PORT=2 ACTION=FORWARD LEARN ↵
```

- ✎ ポートセキュリティの学習済みアドレス（Learn エントリー）は、エージングにより削除されない点ではスタティックですが、ポートセキュリティ機能をオフにすると、システム再起動によって削除されます。

スタティックエントリーは SHOW SWITCH FILTER コマンド（505 ページ）で確認できます。

スタティックエントリーを削除するには、DELETE SWITCH FILTER コマンド（236 ページ）を使います。エントリー番号は可変なので、必ず SHOW SWITCH FILTER コマンド（505 ページ）で確認してから指定してください。例のように、ENTRY パラメーターには複数のエントリーを指定できます。

```
DELETE SWITCH FILTER PORT=2 ENTRY=1,3-7 ↵
```

- ✎ エントリーを削除すると、後続のエントリー番号が 1 つずつ前にずれます。

## クラシファイア

ヘッダー情報に基づいてパケットを分類するクラシファイア（汎用パケットフィルタ）について説明します。クラシファイアは単体で使用するのではなく、ハードウェアパケットフィルタやポリシーベース QoS と組み合わせて使用します。

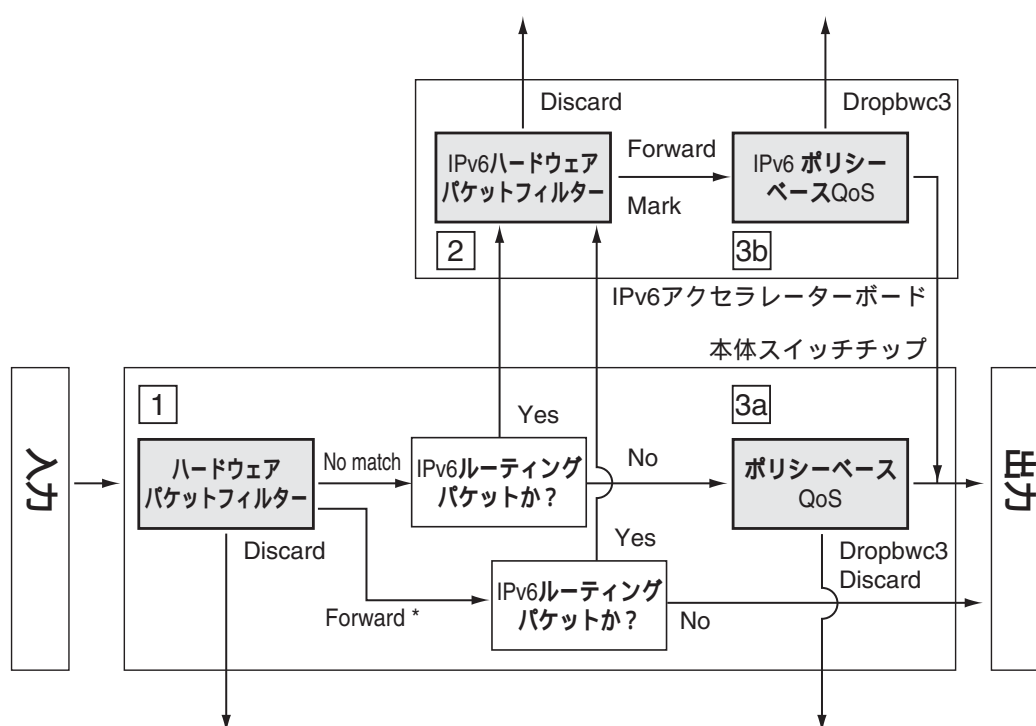
### 概要

クラシファイアは、パケットの分類条件を定義するためのメカニズムです。パケットのヘッダー情報（MAC アドレスや IP アドレス、プロトコルタイプなど）に基づき、パケットを「フロー」に分類する仕組みを提供します。

クラシファイアは分類条件を定義するだけなので、単体では意味をなしません。下記の機能と組み合わせて初めて効果を発揮します。

- 1. ハードウェアパケットフィルタ
- 2. IPv6 ハードウェアパケットフィルタ
- 3a. ポリシーベース QoS
- 3b. IPv6 ポリシーベース QoS

各機能の処理順序は次のようになります。



\* ハードウェアパケットフィルタにマッチしたパケットにはポリシーベースQoSが適用されない。  
パケットフィルタリングとポリシーベースQoSを併用する場合は、QoSポリシーのフィルタリング機能を使うほうがよい。

- ④ ハードウェアパケットフィルタにマッチしたパケットに対して、ポリシーベース QoS は適用されません（ここでの「マッチ」とは、破棄（Discard）だけでなく明示的な転送許可（Forward）も含まれます）。ポリシーベース QoS を利用しながらパケットフィルタリングを行いたい場合は、ハードウェアパケットフィルタを併用するのではなく、QoS ポリシーのフィルタリング機能（フローグループ、トラフィッククラスのアクション）を使ってください。

番号	機能	適用対象	備考
1	ハードウェアパケットフィルタ	すべてのパケット	-
2	IPv6 ハードウェアパケットフィルタ	IPv6 ルーティングパケット（1 で破棄されたパケットを除く）	IPv6 アクセラレーターボードが必要
3a	ポリシーベース QoS	IPv6 ルーティングパケット以外で、1 にマッチしなかったすべてのパケット	ここでの「マッチ」とは、破棄（Discard）、転送（Forward）の両方を指す
3b	IPv6 ポリシーベース QoS	IPv6 ルーティングパケット（2 で破棄されたパケットを除く）	IPv6 アクセラレーターボードが必要

表 18: クラシファイアを使用する機能

- ④ IPv6 アクセラレーターボードを装着していない場合、2、3b の処理は行われません。すべてのパケットが 1 3a の流れで処理されます。
- ④ トンネリング IPv6 パケット（IPv6 over IPv4 および 6to4）は処理 2（IPv6 ハードウェアパケットフィルタ）の対象になりません（フィルタリングできません）。

次に、使用できる条件パラメーターの一覧を示します。「機能別の使用可否」欄では、前述の機能（1、2、3a、3b）ごとに、どのパラメーターが使用可能であることを示しています（＝使用可能、＝必須、×＝使用不可）。

より詳しくは次節「基本設定」をご覧ください。また、各機能の詳細については、それぞれ該当するセクションをご覧ください。

項目名	説明	機能別の使用可否			
		1	2	3a	3b
レイヤー 2					
ETHFORMAT (Ethernet) フレームフォーマット (エンキャプセレーション)					
PROTOCOL (Ethernet) プロトコルタイプ					
MACTYPE	(Ethernet) レイヤー 2 アドレス種別。L2UCAST (ユニキャスト)、L2MCAST (マルチキャスト)、L2BCAST (ブロードキャスト)、ANY (すべて) のいずれか			×	

MACSADDR	( Ethernet ) 送信元 MAC アドレス			x	
MACDADDR	( Ethernet ) 宛先 MAC アドレス			x	
VLAN	入力 VLAN ( ただし、IPv6 ポリシーベース QoS(3b) では出力 VLAN )			x	
TPID	( 802.1Q ) TPID ( Tag Protocol Identifier )			x	x
VLANPRIORITY	( 802.1Q ) 802.1p ユーザープライオリティ			x	x
INNERTPID	( 2 つ目の 802.1Q ) TPID ( Tag Protocol Identifier )			x	x
INNERVLANPRIORITY	( 2 つ目の 802.1Q ) 802.1p ユーザープライオリティ			x	x
INNERVLANID	( 2 つ目の 802.1Q ) VLAN ID			x	x
レイヤー 3					
IPSADDR	( IPv4 ヘッダー ) 始点 IPv4 アドレス / マスク長			x	x
IPV6SADDR	( IPv6 ヘッダー ) 始点 IPv6 アドレス / プレフィックス長	x		x	x
IPDADDR	( IPv4 ヘッダー ) 終点 IPv4 アドレス / マスク長			x	x
IPV6DADDR	( IPv6 ヘッダー ) 始点 IPv6 アドレス / プレフィックス長	x		x	x
IPDSCP	( IPv4 / IPv6 ヘッダー ) DSCP ( DiffServ Code Point )				
IPTOS	( IPv4 ヘッダー ) TOS 優先度 ( precedence )			x	x
IPPROTOCOL	( IPv4 / IPv6 ヘッダー ) プロトコルタイプ ( レイヤー 4 プロトコルタイプ )				
レイヤー 4					
TCPSPORT	( TCP ヘッダー ) 始点ポート				x
TCPDPORT	( TCP ヘッダー ) 終点ポート				x
TCPFLAGS	( TCP ヘッダー ) 制御フラグ ( URG, ACK, RST, SYN, FIN )			x	x
UDPSOURCEPORT	( UDP ヘッダー ) 始点ポート				x
UDPDESTPORT	( UDP ヘッダー ) 終点ポート				x
L4SMASK	( TCP / UDP ヘッダー ) 始点ポートに対する AND マスク			x	x
L4DMASK	( TCP / UDP ヘッダー ) 終点ポートに対する AND マスク			x	x



レイヤー 5		
L5BYTE01	レイヤー 5 (セッション層) のデータパターン	x
~		x
L5BYTE16		

表 19: 条件パラメーター

## 基本設定

クラシファイアの基本的な設定方法について解説します。

### クラシファイアの作成

クラシファイアを作成するには、CREATE CLASSIFIER コマンド (198 ページ) を使います。CLASSIFIER パラメーターに指定するのは、各クラシファイアを識別するための番号です。この番号は単なる識別子であり、値の大小は意味を持ちません。

指定できる条件パラメーターは、クラシファイアをどの機能で使うかによって異なります。詳しくは以下の説明をお読みください。

```
CREATE CLASSIFIER=10 IPDADDR=192.168.10.0/24 ↵
```

#### ハードウェアパケットフィルター

ハードウェアパケットフィルターは、すべての入力パケットを対象とするパケットフィルターです。マッチしたパケットに対しては、転送、破棄のいずれかの処理を実行できます。処理は、本体スイッチチップで行われます。

ハードウェアパケットフィルター用のクラシファイアは、CREATE CLASSIFIER コマンド (198 ページ) の下記構文を使って作成してください。下記構文にないパラメーターを含んでいると、ADD SWITCH HWFILTER コマンド (188 ページ) 入力時にエラーが発生します。

```

CREATE CLASSIFIER=rule-id [ETHFORMAT={ETHII-TAGGED|ETHII-UNTAGGED|ANY}]
  [PROTOCOL={protocoltype|IP|ANY}] [MACTYPE={L2UCAST|L2MCAST|L2BCAST|ANY}]
  [MACSADDR={macadd|ANY}] [MACDADDR={macadd|ANY}]
  [VLAN={vlanname|1..4094|ANY}] [TPID={tpid|ANY}] [VLANPRIORITY={0..7|ANY}]
  [INNERTPID={tpid|ANY}] [INNERVLANPRIORITY={0..7|ANY}]
  [INNERVLANID={1..4094|ANY}] [IPSADDR={ipadd[/masklen]|ANY}]
  [IPDADDR={ipadd[/masklen]|ANY}] [IPDSCP={dscp-list|ANY}]
  [IPTOS={0..7|ANY}] [IPPROTOCOL={TCP|UDP|ICMP|IGMP|protocol|ANY}]
  [TCPSPORT={port|port-range|ANY}] [TCPDPORT={port|port-range|ANY}]
  [TCPFLAGS={{URG|ACK|RST|SYN|FIN}[,...]|ANY}]
  [UDPSPORT={port|port-range|ANY}] [UDPDPOR={port|port-range|ANY}]
  [L4SMASK={bitmask|ANY}] [L4DMASK={bitmask|ANY}]
  [L5BYTE01=byteoffset,bytevalue[,bytemask]]
  [L5BYTE02=byteoffset,bytevalue[,bytemask]]
  [L5BYTE03=byteoffset,bytevalue[,bytemask]]
  [L5BYTE04=byteoffset,bytevalue[,bytemask]]
  [L5BYTE05=byteoffset,bytevalue[,bytemask]]
  [L5BYTE06=byteoffset,bytevalue[,bytemask]]
  [L5BYTE07=byteoffset,bytevalue[,bytemask]]
  [L5BYTE08=byteoffset,bytevalue[,bytemask]]
  [L5BYTE09=byteoffset,bytevalue[,bytemask]]
  [L5BYTE010=byteoffset,bytevalue[,bytemask]]
  [L5BYTE011=byteoffset,bytevalue[,bytemask]]
  [L5BYTE012=byteoffset,bytevalue[,bytemask]]
  [L5BYTE013=byteoffset,bytevalue[,bytemask]]
  [L5BYTE014=byteoffset,bytevalue[,bytemask]]
  [L5BYTE015=byteoffset,bytevalue[,bytemask]]
  [L5BYTE016=byteoffset,bytevalue[,bytemask]]

```

#### IPv6 ハードウェアパケットフィルター

IPv6 ハードウェアパケットフィルターは、ルーティングされる IPv6 パケットだけを対象とするパケットフィルターです。マッチしたパケットに対しては、転送、破棄、DSCP/802.1p 書き換えのいずれかの処理を実行できます。処理は、IPv6 アクセラレーターボードで行われます。

IPv6 ハードウェアパケットフィルター用のクラシファイアは、CREATE CLASSIFIER コマンド (198 ページ) の下記構文を使って作成してください。下記構文にないパラメーターを含んでいると、ADD SWITCH ACCELERATOR HWFILTER コマンド (184 ページ) 入力時にエラーが発生します。

```
CREATE CLASSIFIER=rule-id ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6
  [IPSADDR={ip6add/plen|ANY}] [IPDADDR={ip6add/plen|ANY}]
  [IPDSCP={0..63|ANY}] [IPPROTOCOL={TCP|UDP|ICMP|IGMP|protocol|ANY}]
  [TCPSPORT={port|port-range|ANY}] [TCPDPORT={port|port-range|ANY}]
  [UDPSPORT={port|port-range|ANY}] [UDPDPOR= {port|port-range|ANY}]
```

- ④ IPv6 ハードウェアパケットフィルタ用のクラシファイアでは、ETHFORMAT=ETHII-TAGGED と PROTOCOL=IPV6 の指定が必須です (IPv6 ルーティングパケットは、VLAN タグが付加された状態で IPv6 アクセラレータボードに送られます)。

### ポリシーベース QoS

ポリシーベース QoS は、クラシファイアを用いてパケットを分類し、分類したそれぞれのトラフィックに異なるサービスレベル (帯域や優先度) を割り当てる機能です。

ポリシーベース QoS の処理は通常、本体スイッチチップで行われますが、ルーティングされる IPv6 パケットに対する QoS 処理は、IPv6 アクセラレータボードで行われます (IPv6 ポリシーベース QoS。次項を参照)。両者の設定はほぼ同じですが、クラシファイアで利用できる条件パラメーターに違いがあります。

ポリシーベース QoS 用のクラシファイアは、CREATE CLASSIFIER コマンド (198 ページ) の下記構文を使って作成してください (ハードウェアパケットフィルタと同じ構文です)。下記構文にないパラメーターを含んでいると、SET QOS PORT コマンド (365 ページ) でポートに QoS ポリシーを割り当てるときにエラーが発生します。

```

CREATE CLASSIFIER=rule-id [ETHFORMAT={ETHII-TAGGED|ETHII-UNTAGGED|ANY}]
  [PROTOCOL={protocoltype|IP|ANY}] [MACTYPE={L2UCAST|L2MCAST|L2BCAST|ANY}]
  [MACSADDR={macadd|DHCP Snooping|ANY}] [MACDADDR={macadd|ANY}]
  [VLAN={vlanname|1..4094|ANY}] [TPID={tpid|ANY}] [VLANPRIORITY={0..7|ANY}]
  [INNERTPID={tpid|ANY}] [INNERVLANPRIORITY={0..7|ANY}]
  [INNERVLANID={1..4094|ANY}] [IPSADDR={ipadd[/masklen]|DHCP Snooping|ANY}]
  [IPDADDR={ipadd[/masklen]|ANY}] [IPDSCP={dscp-list|ANY}]
  [IPTOS={0..7|ANY}] [IPPROTOCOL={TCP|UDP|ICMP|IGMP|protocol|ANY}]
  [TCPSPORT={port|port-range|ANY}] [TCPDPORT={port|port-range|ANY}]
  [TCPFLAGS={{URG|ACK|RST|SYN|FIN}[,...]|ANY}]
  [UDPSPORT={port|port-range|ANY}] [UDPDPOR={port|port-range|ANY}]
  [L4SMASK={bitmask|ANY}] [L4DMASK={bitmask|ANY}]
  [L5BYTE01=byteoffset,bytevalue[,bytemask]]
  [L5BYTE02=byteoffset,bytevalue[,bytemask]]
  [L5BYTE03=byteoffset,bytevalue[,bytemask]]
  [L5BYTE04=byteoffset,bytevalue[,bytemask]]
  [L5BYTE05=byteoffset,bytevalue[,bytemask]]
  [L5BYTE06=byteoffset,bytevalue[,bytemask]]
  [L5BYTE07=byteoffset,bytevalue[,bytemask]]
  [L5BYTE08=byteoffset,bytevalue[,bytemask]]
  [L5BYTE09=byteoffset,bytevalue[,bytemask]]
  [L5BYTE10=byteoffset,bytevalue[,bytemask]]
  [L5BYTE11=byteoffset,bytevalue[,bytemask]]
  [L5BYTE12=byteoffset,bytevalue[,bytemask]]
  [L5BYTE13=byteoffset,bytevalue[,bytemask]]
  [L5BYTE14=byteoffset,bytevalue[,bytemask]]
  [L5BYTE15=byteoffset,bytevalue[,bytemask]]
  [L5BYTE16=byteoffset,bytevalue[,bytemask]]

```

### IPv6 ポリシーベース QoS

IPv6 パケットに対するポリシーベース QoS の処理は、IPv6 アクセラレーターボードで行われます。通常のポリシーベース QoS と設定はほぼ同じですが、クラシファイアで利用できる条件パラメーターに違いがあります。

IPv6 ポリシーベース QoS 用のクラシファイアは、CREATE CLASSIFIER コマンド (198 ページ) の下記構文を使って作成してください。下記構文にないパラメーターを含んでいると、SET QOS ACCELERATOR POLICY コマンド (355 ページ) で QoS ポリシーを指定するときにエラーが発生します。

```
CREATE CLASSIFIER=rule-id ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6
[MACTYPE={L2UCAST|L2MCAST|L2BCAST|ANY}] [MACSADDR={macadd|ANY}]
[MACDADDR={macadd|ANY}] [VLAN={vlanname|1..4094|ANY}] [IPDSCP={0..63|ANY}]
[IPPROTOCOL={TCP|UDP|ICMP|IGMP|protocol|ANY}]
```

- IPv6 ポリシーベース QoS 用のクラシファイアでは、ETHFORMAT=ETHII-TAGGED と PROTOCOL=IPV6 の指定が必須です (IPv6 ルーティングパケットは、VLAN タグが付加された状態で IPv6 アクセラレーターボードに送られます)。
- IPv6 ポリシーベース QoS 用のクラシファイアでは、DSCP 値を除き L3 以上のパラメーターを指定できません。L3、L4 パラメーターによる分類をしたいときは、あらかじめ IPv6 ハードウェアパケットフィルターの MARK アクションを使って DSCP 値を書き換えておきます。

## クラシファイアの使用

前述のとおり、クラシファイアはパケットを分類するメカニズムを提供するだけです。実際になんらかの処理を行うには、ハードウェアパケットフィルター、QoS ポリシー、IPv6 ハードウェアパケットフィルターと関連付ける必要があります。

- ハードウェアパケットフィルターにマッチしたパケットに対して、ポリシーベース QoS は適用されません (ここでの「マッチ」とは、破棄 (Discard) だけでなく明示的な転送許可 (Forward) も含みます)。ポリシーベース QoS を利用しながらパケットフィルタリングを行いたい場合は、ハードウェアパケットフィルターを併用するのではなく、QoS ポリシーのフィルタリング機能 (フローグループ、トラフィッククラスのアクション) を使ってください。

ハードウェアパケットフィルターでは、クラシファイアとマッチ時のアクションの 2 つ 1 組でフィルターエントリーを構成します。ハードウェアパケットフィルターにエントリーを追加するには、ADD SWITCH HWFILTER コマンド (188 ページ) を使います。

次の例では、受信したパケットのうち、クラシファイア「12」にマッチするパケットを破棄します。

```
ADD SWITCH HWFILTER=1 CLASSIFIER=12 ACTION=DISCARD ↵
```

ポリシーベース QoS では、パケットをフローグループに分類するためにクラシファイアを使います。フローグループにクラシファイアを関連付けるには、ADD QOS FLOWGROUP コマンド (179 ページ) を使います。

```
ADD QOS FLOWGROUP=10 CLASSIFIER=1-5 ↵
```

- ポリシーベース QoS は、IPv6 ルーティングパケットは IPv6 アクセラレーターボードで、それ以外のパケットは本体スイッチチップで適用されますが、フローグループ、トラフィッククラス、QoS ポリシーの設定は同じです。異なるのは、クラシファイアで使用する条件パラメーターと、QoS ポリシーの適用先だけです。

実際にはさらに、トラフィッククラスにフローグループを関連付け、QoS ポリシーにトラフィッククラスを関連付け、QoS ポリシーをスイッチポートか IPv6 アクセラレーターボードに適用する必要があります。詳細は「スイッチング」の「QoS」をご覧ください。

IPv6 ハードウェアパケットフィルターでは、クラシファイアとマッチ時のアクションの 2 つ 1 組でフィルターエントリを構成します。IPv6 ハードウェアパケットフィルターにエントリを追加するには、ADD SWITCH ACCELERATOR HWFILTER コマンド (184 ページ) を使います。

次の例では、受信したパケットのうち、クラシファイア「120」にマッチするパケットを破棄します。

```
ADD SWITCH ACCELERATOR HWFILTER=1 CLASSIFIER=120 ACTION=DISCARD ↵
```

IPv6 ハードウェアパケットフィルターは、IPv6 ルーティングパケットに対するポリシーベース QoS でも使います。たとえば、次の例では、クラシファイア「220」にマッチするパケットの DSCP 値を 20 に書き換えています。QoS ポリシーでパケットを再分類するときには、この DSCP 値を用いることができます。詳しくは「スイッチング」の「QoS」をご覧ください。

```
ADD SWITCH ACCELERATOR HWFILTER=10 CLASSIFIER=220 ACTION=MARK
NEWIPDSCP=20 ↵
```

🔗 IPv6 ハードウェアパケットフィルターを使用するには、IPv6 アクセラレーターボードが必要です。

🔗 IPv6 ハードウェアパケットフィルターは、ルーティングされる IPv6 パケットにだけ適用されます。VLAN 内でスイッチングされる IPv6 パケットには適用されません。

ポリシーベース QoS、ハードウェアパケットフィルター、IPv6 ハードウェアパケットフィルターの詳細については、それぞれ「スイッチング」の「QoS」、「ハードウェアパケットフィルター」、「IPv6 ハードウェアパケットフィルター」をご覧ください。

## クラシファイアの変更・削除・確認

作成済みのクラシファイアを変更するには、SET CLASSIFIER コマンド (325 ページ) を使います。

```
SET CLASSIFIER=10 IPDADDR=192.168.10.0/16 ↵
```

クラシファイアを削除するには、DESTROY CLASSIFIER コマンド (243 ページ) を使います。ハードウェアパケットフィルターや QoS ポリシー (厳密にはフローグループ) に関連付けられているクラシファイアは削除できません。先に関連付けを削除してから DESTROY CLASSIFIER コマンド (243 ページ) を実行してください。

クラシファイア番号は、カンマ、ハイフンを使って複数指定が可能です。

```
DESTROY CLASSIFIER=1 ↓
DESTROY CLASSIFIER=10-15 ↓
DESTROY CLASSIFIER=23,25-27 ↓
DESTROY CLASSIFIER=ALL ↓
```

クラシファイアの一覧は SHOW CLASSIFIER コマンド (395 ページ) で確認できます。

```
SHOW CLASSIFIER ↓
```

クラシファイア番号を指定した場合は、該当クラシファイアのパラメーター一覧が表示されます。

```
SHOW CLASSIFIER=1 ↓
SHOW CLASSIFIER=ALL ↓
```

## クラシファイアとルール領域消費量

本製品では、ハードウェアによるフィルタリング機能を実現するために、システム内部の「ルールテーブル」を使用します。

クラシファイアは CREATE CLASSIFIER コマンド (198 ページ) で 9999 個まで作成できますが、実際に使用できる数 (フィルターやポリシーに関連付けられる数) はルールテーブル内にあるルール領域の空き容量に依存します。ルール領域の空きがなくなると、フィルター作成時やポリシーの適用時にエラーメッセージが表示され、それ以上フィルターやポリシーの追加ができなくなります。

ルールテーブルの使用状況は、SHOW SWITCH コマンド (490 ページ) で確認できます。「Traffic Control Unit, hardware resource usage」以下をご覧ください。

まずは、ルール領域に関する基本原則を列挙します。

- スイッチ本体には、いくつかのスイッチチップが搭載されている (通常 1~2 個)。以下の説明では、スイッチ本体に搭載されている個々のスイッチチップを「本体インスタンス」または単に「インスタンス」と呼ぶ。本製品のインスタンスは 2 個であり、それぞれにはポート 1~12 とポート 13~24 が所属している。
- 1 つのインスタンスには、1024 ルール分のルール領域がある。この領域は、ハードウェアパケットフィルター、ポリシーベース QoS、MLD Snooping が使用する。
- IPv6 アクセラレーターボードには、1024 ルール分のルール領域がある。この領域は、IPv6 ポリシーベース QoS が使用する。
- IPv6 ハードウェアパケットフィルターは、ルール領域を使用しない。
- ルール領域は、ルール 8 個単位で割り当てられる
- デフォルト有効の MLD Snooping が、スイッチ本体のルール領域を 1 個使用している

以下では、この原則をもとに、ハードウェアパケットフィルター、ポリシーベース QoS、MLD Snooping、IPv6 ポリシーベース QoS の各機能がルール領域をどのように消費するかを解説します。

☞ 以下の図は説明のためのイメージ図であり、内部実装を正確に表したものではありません。

### ハードウェアパケットフィルタのみ使用時

ここでは、ハードウェアパケットフィルタ（と MLD Snooping）だけを使用する場合の本体インスタンスのルール領域使用量について説明します。

☞ IPv6 ハードウェアパケットフィルタは、ルール領域を消費しません。ここで述べるのは、本体インスタンスのルール領域を使用する通常のハードウェアパケットフィルタです。

ハードウェアパケットフィルタは、1 つのフィルタ（1 クラシファイア）あたり、各インスタンスのルール領域を 1 つ使用します。

ここでは、8 個のクラシファイア（1～8）を作成し、8 個のハードウェアパケットフィルタを作成した場合のルール領域消費量について説明します。

MLD Snooping 有効時（デフォルト有効）

MLD Snooping が 1 個ルールを使用しているため、ハードウェアパケットフィルタ 8 個とあわせて、合計ルール数は 9 個となります。ただし、ルール領域は 8 個単位で割り当てられるため、この状態でのルール領域消費量は 16 となります。

本体インスタンスのルール領域

ルール番号	ポート番号	機能モジュール
1	すべて	MLD Snooping
2	すべて	HWFilter CLASSIFIER=1
3	すべて	HWFilter CLASSIFIER=2
4	すべて	HWFilter CLASSIFIER=3
5	すべて	HWFilter CLASSIFIER=4
6	すべて	HWFilter CLASSIFIER=5
7	すべて	HWFilter CLASSIFIER=6
8	すべて	HWFilter CLASSIFIER=7
9	すべて	HWFilter CLASSIFIER=8
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		

MLD Snooping 無効時

MLD Snooping が使用していた 1 個のルールがなくなるため、合計ルール数は 8 個となります。ルール領



域は 8 個単位で割り当てられるため、この例ではちょうど 1 単位におさまります。すなわち、ルール領域の消費量は 8 となります。

本体インスタンスのルール領域

ルール番号	ポート番号	機能モジュール
1	すべて	HWFilter CLASSIFIER=1
2	すべて	HWFilter CLASSIFIER=2
3	すべて	HWFilter CLASSIFIER=3
4	すべて	HWFilter CLASSIFIER=4
5	すべて	HWFilter CLASSIFIER=5
6	すべて	HWFilter CLASSIFIER=6
7	すべて	HWFilter CLASSIFIER=7
8	すべて	HWFilter CLASSIFIER=8
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		

### ポリシーベース QoS のみ使用時

次に、ポリシーベース QoS（と MLD Snooping）だけを使用する場合の本体インスタンスのルール領域使用量について説明します。

- ④ IPv6 ポリシーベース QoS は、本体インスタンスのルール領域ではなく IPv6 アクセラレーターボードのルール領域を消費します。ここで述べるのは、本体インスタンスのルール領域を使用する通常のポリシーベース QoS です。

ポリシーベース QoS では、QoS ポリシーを適用するスイッチポートごとに、ポートが所属するインスタンスのルール領域が 8 ルール単位で割り当てられ、ポートごとに 1 クラシファイアあたり 1 つのルールを使用します。また、デフォルトトラフィッククラスも 1 つのルールを使用します。

QoS ポリシーを全ポートに割り当てた場合、それだけで各インスタンスのルール領域を「インスタンスの所属ポート数 × 8」消費してしまいます。QoS ポリシーを適用するときは、なるべく必要なポートだけに限定するようにしてください。

ここでは、2 個のクラシファイア（9～10）を作成し、2 個の QoS フローグループ、1 個の QoS ポリシーを作成し、2 つのポート（1～2）に QoS ポリシーを適用した場合のルール領域消費量について説明します。

MLD Snooping 有効時（デフォルト有効）

スイッチポートに QoS ポリシーを適用すると、そのポート専用のルール領域が（ルール 8 個を 1 単位で）割り当てられます。

MLD Snooping が使用する 1 個のルールは、ポート専用のルール領域ごとに割り当てられます。さらに、QoS ポリシーを適用していないポート群のためのルール領域も割り当てられ、そこでも MLD Snooping 用のルール 1 個が使われます。

結果的に、この例では、MLD Snooping 用ルールが 3 個、QoS ポリシー用のルールが 6 個（ $= 3 \times 2$ ）で、合計ルール数は 9 個となります。ただし、ルール領域が、ポート 1 用、ポート 2 用、その他のポート用の 3 つに分けて割り当てられるため、ルール領域消費量は 24 となります。

本体インスタンスのルール領域

ルール番号	ポート番号	機能モジュール
1	1	MLD Snooping
2	1	QoS Flowgroup CLASSIFIER=9
3	1	QoS Flowgroup CLASSIFIER=10
4	1	QoS Policy Default Traffic Class
5		
6		
7		
8		
9	2	MLD Snooping
10	2	QoS Flowgroup CLASSIFIER=9
11	2	QoS Flowgroup CLASSIFIER=10
12	2	QoS Policy Default Traffic Class
13		
14		
15		
16		
17	その他	MLD Snooping
18		
19		
20		
21		
22		
23		
24		
25		
26		

#### MLD Snooping 無効時

MLD Snooping が使用していた 1 個のルールがなくなるため、QoS ポリシーを適用していないポート用の領域は解放されます。

結果的に、この例では、QoS ポリシー用のルールが 6 個（ $= 3 \times 2$ ）で、合計ルール数は 6 個となります。ただし、ルール領域が、ポート 1 用、ポート 2 用の 2 つに分けて割り当てられるため、ルール領域消費量は 16 となります。

本体インスタンスのルール領域

ルール番号	ポート番号	機能モジュール
1	1	QoS Flowgroup CLASSIFIER=9
2	1	QoS Flowgroup CLASSIFIER=10
3	1	QoS Policy Default Traffic Class
4		
5		
6		
7		
8		
9	2	QoS Flowgroup CLASSIFIER=9
10	2	QoS Flowgroup CLASSIFIER=10
11	2	QoS Policy Default Traffic Class
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		

### ハードウェアパケットフィルタとポリシーベース QoS 併用時

次に、ハードウェアパケットフィルタとポリシーベース QoS（と MLD Snooping）を併用する場合の本体ルール領域使用量について説明します。

- ハードウェアパケットフィルタにマッチしたパケットに対して、ポリシーベース QoS は適用されません（ここでの「マッチ」とは、破棄（Discard）だけでなく明示的な転送許可（Forward）も含みます）。ポリシーベース QoS を利用しながらパケットフィルタリングを行いたい場合は、ハードウェアパケットフィルタを併用するのではなく、QoS ポリシーのフィルタリング機能（フローグループ、トラフィッククラスのアクション）を使ってください。

この場合は、ポリシーベース QoS だけを使用するときと基本的に同じです。ハードウェアパケットフィルタを 1 つ追加するたびに、各ポート専用のルール領域に同じルールが 1 つずつ追加されます。

ここでは、4 個のクラシファイア（1～2、9～10）を作成し、そのうち 1～2 を 2 個のハードウェアパケットフィルタに割り当て、9～10 を 2 つの QoS フローグループに割り当てるものとします。さらに、2 つのフローグループを（トラフィッククラスを介して）1 個の QoS ポリシーに割り当て、これを 2 つのポート（1～2）に適用した場合のルール領域消費量について説明します。

MLD Snooping 有効時（デフォルト有効）

スイッチポートに QoS ポリシーを適用すると、そのポート専用のルール領域が（ルール 8 個を 1 単位で）割り当てられます。

MLD Snooping が使用する 1 個のルールと、ハードウェアパケットフィルタが使用する 2 個のルールは、

ポート専用のルール領域ごとに割り当てられます。さらに、QoS ポリシーを適用していないポート群のためのルール領域も割り当てられ、そこでも MLD Snooping 用のルール 1 個とハードウェアパケットフィルターのルール 2 個が使われます。

結果的に、この例では、MLD Snooping 用ルールが 3 個、QoS ポリシー用のルールが 6 個 ( $= 3 \times 2$ )、ハードウェアパケットフィルターのルールが 6 個 ( $= 2 \times 3$ )、合計ルール数は 15 個となります。ただし、ルール領域が、ポート 1 用、ポート 2 用、その他のポート用の 3 つに分けて割り当てられるため、ルール領域消費量は 24 となります。

本体インスタンスのルール領域

ルール番号	ポート番号	機能モジュール
1	1	MLD Snooping
2	1	HWFilter CLASSIFIER=1
3	1	HWFilter CLASSIFIER=2
4	1	QoS Flowgroup CLASSIFIER=9
5	1	QoS Flowgroup CLASSIFIER=10
6	1	QoS Policy Default Traffic Class
7		
8		
9	2	MLD Snooping
10	2	HWFilter CLASSIFIER=1
11	2	HWFilter CLASSIFIER=2
12	2	QoS Flowgroup CLASSIFIER=9
13	2	QoS Flowgroup CLASSIFIER=10
14	2	QoS Policy Default Traffic Class
15		
16		
17	その他	MLD Snooping
18	その他	HWFilter CLASSIFIER=1
19	その他	HWFilter CLASSIFIER=2
20		
21		
22		
23		
24		
25		
26		

#### MLD Snooping 無効時

各ポート専用のルール領域から、MLD Snooping が使用していた 1 個のルールがなくなるため、QoS ポリシー用のルールが 6 個 ( $= 3 \times 2$ )、ハードウェアパケットフィルターのルールが 6 個 ( $= 2 \times 3$ )、合計ルール数は 12 個となります。ただし、ルール領域が、ポート 1 用、ポート 2 用、その他のポート用の 3 つに分けて割り当てられるため、ルール領域消費量は 24 となります。

本体インスタンスのルール領域

ルール番号	ポート番号	機能モジュール
1	1	HWFilter CLASSIFIER=1
2	1	HWFilter CLASSIFIER=2
3	1	QoS Flowgroup CLASSIFIER=9
4	1	QoS Flowgroup CLASSIFIER=10
5	1	QoS Policy Default Traffic Class
6		
7		
8		
9	2	HWFilter CLASSIFIER=1
10	2	HWFilter CLASSIFIER=2
11	2	QoS Flowgroup CLASSIFIER=9
12	2	QoS Flowgroup CLASSIFIER=10
13	2	QoS Policy Default Traffic Class
14		
15		
16		
17	その他	HWFilter CLASSIFIER=1
18	その他	HWFilter CLASSIFIER=2
19		
20		
21		
22		
23		
24		
25		
26		

## IPv6 ポリシーベース QoS 使用時

次に、IPv6 ポリシーベース QoS を使用する場合はルール領域使用量について説明します。

IPv6 ポリシーベース QoS は、IPv6 アクセラレータボード用のルール領域 1024 個を単独で使用します。そのため、前節までに説明した他の機能、ハードウェアパケットフィルター、ポリシーベース QoS、MLD Snooping の設定には影響されません。

IPv6 ポリシーベース QoS では、1 クラシファイアあたり、IPv6 アクセラレータボード用のルール領域を 1 つ使用します。また、デフォルトトラフィッククラスも 1 つのルールを使用します。

ルール領域の割り当ては、本体インスタンスのルール領域と同様 8 個単位で行われます。

ここでは、2 個のクラシファイア (109 ~ 110) を作成し、2 個の QoS フローグループ、1 個の QoS ポリシーを作成し、IPv6 アクセラレータボードに QoS ポリシーを適用した場合のルール領域消費量について説明します。

この例では、デフォルトトラフィッククラス用のルール 1 個とクラシファイア用のルールが 2 個、合計 3 個が IPv6 アクセラレータボード用のルール領域から消費されます。ただし、ルール領域は 8 個単位で割り当てられるため、実際のルール領域消費量は 8 となります。

IPv6アクセラレーターボード ルール領域

ルール番号	機能モジュール
1	QoS Flowgroup CLASSIFIER=109
2	QoS Flowgroup CLASSIFIER=110
3	QoS Policy Default Traffic Class
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	

## IPv6 ハードウェアパケットフィルター使用時

IPv6 ハードウェアパケットフィルターは、ルール領域を使用しません。ルール領域の空き容量とは関係なく、最大 999 個のフィルターを作成することができます。

## QoS

QoS (Quality of Service) 関連機能について解説します。

本製品は、ユーザーが定義したポリシーに基づき、トラフィックに任意のサービスレベルを割り当てるポリシーベース QoS (Quality of Service) 機能を備えています。

ポリシーベース QoS では、クラシファイアと呼ばれる汎用のパケットフィルターを用いてパケットを分類し、それぞれに異なるサービスレベル (帯域や優先度) を割り当てます。クラシファイアを用いることにより、IP アドレスや TCP/UDP ポート、DSCP (DiffServ Code Point) などに基づいた QoS の制御が可能です。また本製品は、VLAN タグヘッダーの IEEE 802.1p ユーザープライオリティー値に基づいてパケットに送信キューを割り当てる 802.1p QoS もサポートしています。

- ☞ ハードウェアパケットフィルターにマッチしたパケットに対して、ポリシーベース QoS は適用されません (ここでの「マッチ」とは、破棄 (Discard) だけでなく明示的な転送許可 (Forward) も含みます)。ポリシーベース QoS を利用しながらパケットフィルタリングを行いたい場合は、ハードウェアパケットフィルターを併用するのではなく、QoS ポリシーのフィルタリング機能 (フローグループ、トラフィッククラスのアクション) を使ってください。

## 概要

本製品の QoS 機能では、次のことが可能です。

- 帯域保証：特定のトラフィッククラスに対し、一定の帯域を保証します。
- 帯域制限：特定のトラフィッククラスに与える帯域を、一定値までに制限します。
- 輻輳制御：RED (Random Early Detection/Discard) アルゴリズムを用いて、トラフィック量を段階的に制御します。
- 優先制御：8 レベルの送信キューを用いて、パケットの優先制御を行います。送信キューの割り当ては、802.1p または QoS ポリシーによって行います。送信時のスケジューリング方式は、絶対優先、重み付きラウンドロビン (WRR) の 2 種類から選択できます。絶対優先 + WRR など、同一ポート上で複数のスケジューリング方式を併用することも可能です。
- マーキング：VLAN タグヘッダーの 802.1p プライオリティー値、IP ヘッダーの DSCP (DiffServ Code Point) フィールド値の書き換えが可能です。

## 基本的な用語

ここでは、本章で使用する用語について簡単にまとめます。以後の説明でよくわからない言葉が出てきたときは、こちらをご参照ください。

- ☞ 以下に述べるのは本章の説明のための定義です。一般に使われている用語の意味とは必ずしも一致しない場合がありますのでご注意ください。

### 802.1p ユーザープライオリティー

802.1Q VLAN タグヘッダー内にある 3 ビットのフィールド。0~7 の値をとる。パケットを受信する機器に対して、パケット取り扱い時の優先度を示す目的で設けられている。802.1p 対応機器は、この値に基づいてパケットの優先制御ができる。また、送信時に値を書き換えることで、次の機器 (対向機器) に対して、新

たな優先度を指示できる。

#### DSCP ( DiffServ Code Point )

IPv4/IPv6 ヘッダーの DiffServ フィールド ( IPv4 では TOS フィールド、IPv6 では Traffic Class フィールドとも呼ばれる ) 内にある 6 ビットのフィールド。0 ~ 63 の値をとる。パケットを受信する機器に対して、該当パケットのトラフィッククラスを示すために使われる。DSCP 値の意味は各機器が独自に管理し、それに基づいてパケットを処理する。

パケットの DSCP 値にしたがって QoS を制御するネットワーク上の領域を DiffServ ドメインと呼ぶ。DiffServ ドメインの入り口にあたる機器では、IP アドレスやプロトコル、ポート番号など、DSCP 以外の条件をもとにパケットを分類し、DiffServ ドメイン内で規定された DSCP 値を付加する。これにより、DiffServ ドメイン内では DSCP 値による統一的な QoS の実施が可能になる。

#### 802.1p QoS

VLAN タグヘッダーの 802.1p ユーザープライオリティー値 ( 0 ~ 7 ) に基づいてパケットの優先制御を行うメカニズム。

802.1p QoS では、あらかじめ用意された 802.1p 値と送信キューの対応表を参照して、タグ付きパケット受信時に送信キューを割り当てる。また、パケット送信時には、各キュー間で送信順序を制御する。

本製品では、受信パケットを 8 レベルの送信キューに振り分けることができる。また、送信スケジューリング方式を、絶対優先と重み付きラウンドロビン ( WRR ) から選択できる。

#### ポリシーベースの QoS

受信パケットを L2 ~ L4 ヘッダーフィールドの内容に基づいて分類し、それぞれに任意のサービスレベル ( 帯域や優先度 ) を割り当てるメカニズム。

ポリシーベースの QoS では、受信ポートに設定された「QoS ポリシー」にしたがって処理が行われる。処理内容は、パケットの分類、帯域制限 ( 最大帯域 ) 帯域保証 ( 最小帯域 ) 802.1p や DSCP の書き換え、送信キューの割り当てなど多岐にわたる。

ポリシーベース QoS は、QoS ポリシー、トラフィッククラス、フローグループ、クラシファイアといった設定要素によって構成される。

#### QoS ポリシー

帯域・優先制御を行うために必要な情報をひとつにまとめる役割を持つ、ポリシーベース QoS の中心的な設定要素。

QoS ポリシーは、ユーザー定義のトラフィッククラス ( 複数 ) とデフォルトトラフィッククラス ( 1 つ ) から構成される。

QoS ポリシーをスイッチポート ( または IPv6 アクセラレーターボード ) に関連付けると、ポートで受信したトラフィックに対して ( または IPv6 アクセラレーターボードを経由するトラフィックに対して ) 該当するトラフィッククラスで定められた QoS 処理が行われる。

#### トラフィッククラス

同等のサービスレベルを与えるべきトラフィックを定義するポリシーベース QoS の設定要素。フローグループの集合体として定義する。

帯域制御や QoS パラメーターの割り当てなど、ポリシーベース QoS の処理の多くはトラフィッククラスで設定する。

トラフィッククラスは、QoS ポリシーに割り当てることによって使用する。なお、QoS ポリシーには、ユーザー定義のトラフィッククラスに加え、暗黙のデフォルトトラフィッククラスが存在する。ユーザー定義の



トラフィッククラスに分類されないトラフィックは、自動的にデフォルトトラフィッククラスの所属として処理される。

#### フローグループ

同等な性格を持つパケットのフローをグループ化したもの（アプリケーションの「行き」と「戻り」など）、クラシファイアの集合体として定義する。

ポリシーベース QoS の処理の多くはトラフィッククラスで設定するが、一部の項目については、フローグループのレベルでより細やかな設定が可能。

フローグループは、ポリシーベース QoS の最小設定単位。トラフィッククラスに割り当てて使う。

#### クラシファイア

IP アドレス、DSCP、ポート、プロトコルなど、さまざまな条件に基づいてパケットを「フロー」に分類する汎用のパケットフィルター。本製品では、ハードウェアパケットフィルターとポリシーベース QoS の両機能でクラシファイアを使用している。

ポリシーベース QoS では、クラシファイアを使ってパケットを「フロー」に分類する。ただし、ポリシーベース QoS の設定は、フローを束ねた「フローグループ」またはフローグループを束ねた「トラフィッククラス」を一単位として行う。

#### 4 つの QoS パラメーター

ポリシーベース QoS の処理過程でパケットに割り当てられる 4 つの属性値。DSCP 値、802.1p ユーザープライオリティー値、帯域クラス、送信キューのこと。プレマーキング、メータリング、リマーキングの各段階で参照・照合されたり、変更される可能性がある。

DSCP 値と 802.1p ユーザープライオリティー値は、実際にパケットのヘッダーに格納できる値。パケット受信時にすでに値がセットされている場合もあれば、されていない場合もある。いずれの場合も、QoS 処理の過程で変更が可能。

一方、帯域クラスと送信キューは、パケット受信後に割り当てられる内部的な属性値。帯域クラスと送信キューの値が意味を持つのは、パケットを送信キューに格納するところまで。後続の機器にこれらの情報を（間接的にながら）伝えるには、DSCP 値か 802.1p ユーザープライオリティー値を使う。

#### プレマーキング

ポリシーベース QoS において、クラシファイアによって分類されたパケットに対して最初に行われる処理。メータリングの前に行われる。プレマーキングでは、パケットの DSCP 値をもとに、新しい DSCP 値、802.1p ユーザープライオリティー値、帯域クラス、送信キューを割り当てることができる。

#### メータリング

ポリシーベース QoS における帯域制御の中心的メカニズム。各トラフィックが実際にどの程度の帯域を使用しているかを計測し、その結果に基づいてパケットを 3 つの「帯域クラス」に分類する処理を行う。

#### 帯域クラス

ポリシーベース QoS のメータリング段階において、帯域使用量に応じてパケットを 3 つのクラスに分類したもの。最大・最小帯域設定への適合性を示す。帯域クラス 1 は、あまり帯域を使っていないため、優先的に帯域を割り当てることができるクラス。帯域クラス 2 は、中程度の帯域使用量のクラス。帯域クラス 3 は、最大帯域の設定を超過しているクラスであり、キューイング前に無条件で破棄する設定、あるいは、送信キューの輻輳時に優先的に破棄する設定が可能。

#### リマーキング

ポリシーベース QoS において、メータリング後に行われる処理。メータリングの結果である帯域クラスの

値を考慮しつつ、プレマージング同様の書き換え処理が可能。また、送信キューをもとに 802.1p ユーザープライオリティ値を書き換えることもできる。

#### DSCPMAP テーブル

プレマージング、リマージング時に参照する QoS パラメーターの書き換えテーブル。プレマージング用とリマージング用の 2 種類がある。

プレマージング、リマージング時には、DSCP 値と帯域クラスをインデックスとして DSCPMAP テーブルを検索し、DSCP 値、帯域クラス、送信キュー、802.1p ユーザープライオリティ値を該当エントリーで指定された値に書き換える。

#### QUEUE2PRIOMAP テーブル

リマージング時に参照する 802.1p ユーザープライオリティ値の書き換えテーブル。リマージング直前の送信キューと帯域クラスの値をインデックスとして検索し、パケットの 802.1p ユーザープライオリティ値を該当エントリーで指定された値に書き換える。

#### PRIQ2QUEUEMAP テーブル

タグ付きパケット受信時に参照する送信キューの割り当てテーブル。パケットの 802.1p ユーザープライオリティ値と割り当てる送信キューの対応を管理している。

#### 送信キュー

本製品のスイッチポートは、それぞれ 8 レベルの送信キューを備えている。各キューに対しては、最大キュー長、最大帯域幅、送信スケジューリング方式（絶対優先、WRR）、WRR 時の重み値などを設定できる。

#### RED アルゴリズム

送信キューにおける輻輳制御アルゴリズムの 1 つ。キューがあふれる前にパケットの破棄を開始することで、TCP などトランスポート層の輻輳回避メカニズムを有効に機能させることができる。ただし、UDP のように輻輳回避を行わないトランスポート層に対しては逆効果となりうるので注意が必要。

#### RED カーブ

RED アルゴリズムの動作を規定するパラメーターセット（によって描かれる線）。START、STOP、DROP という 3 つのパラメーターからなる。START はパケットの破棄を開始するキュー長、STOP はパケットを完全に破棄し始めるキュー長、DROP はキュー長が STOP のときに破棄するパケットの割合を示す。なお、カーブとは言うものの曲線ではない。

#### RED カーブセット

RED カーブの集合体。本製品では、RED カーブセットをスイッチポートに割り当てることで、該当ポートで RED アルゴリズムを使用できるようにする。8 つの送信キューにはそれぞれ個別の RED カーブを設定できる。また、各キューでは、帯域クラスごとに個別の RED カーブを設定できる。すなわち、RED カーブセットは、 $8 \times 3 = 24$  個の RED カーブを組にしたものとなる。

#### Tail-drop アルゴリズム

送信キューにおける輻輳時のデフォルト動作。帯域クラスごとに設定された最大キュー長を超過したパケットを無条件に破棄する。最大キュー長は、デフォルト RED カーブセット「1」の STOP1、STOP2、STOP3 パラメーターで変更可能。

#### 送信スケジューリング方式

パケット処理の最終段階であるキューからの送信処理を、どのような順序で行うかを規定するもの。本製品では、絶対優先スケジューリングと重み付きラウンドロビンスケジューリング（WRR）の 2 種類から選択

できる。同一ポート内において、絶対優先で送信するキューと WRR で送信するキューのグループを分けたり、WRR を 2 段階で行うような設定も可能。

#### 絶対優先スケジューリング

デフォルトの送信スケジューリング方式。上位キューが空になるまで下位のキューからはパケットを送信しない。この方式はシンプルだが、上位キューに割り当てられるパケットが多いときに、下位キューのパケットが送信されなくなるという欠点がある。

#### 重み付きラウンドロビン (WRR) スケジューリング

送信スケジューリング方式の 1 つ。各キュー間の送信比率を設定し、その比率にしたがってパケットを送信する。たとえば、最上位キューから最下位キューまで、10:5:5:5:2:2:1:1 の比率でパケットを送信するような設定が可能。この方式だと、上位キューに割り当てられるパケットが多いときでも、一定比率下位キューからパケットを送信することが可能。

## 802.1p QoS の基本設定

802.1p QoS の設定は、受信時のキュー割り当て方式と、送信時のスケジューリング方式の 2 つの設定を組み合わせることによって行います。802.1p QoS を使用する場合、QoS ポリシーを作成する必要はありません。

### 設定手順例

次に基本的な設定手順例を示します。

1. タグ付きパケット受信時のキュー割り当てを設定します。これには、SET QOS PRIO2QUEUEMAP コマンド (369 ページ) を使います。たとえば、タグ付きパケットの 802.1p 値 0~7 に対して、送信キュー 0, 1, 2, 3, 4, 5, 6, 7 を割り当てるには、次のようにします。

```
SET QOS PRIO2QUEUEMAP=0,1,2,3,4,5,6,7 ↵
```

2. タグなしパケット受信時のキュー割り当てを設定します。これには、SET QOS PORT コマンド (365 ページ) の DEFAULTQUEUE パラメーターを使います。こちらは受信ポートごとに設定します。たとえば、すべてのポートにおいて、受信したタグなしパケットに送信キュー 1 を割り当てるには、次のようにします。

```
SET QOS PORT=ALL DEFAULTQUEUE=1 ↵
```

3. 受信時にタグなしだったパケットをタグ付きポートから送信するとき、802.1p ユーザープライオリティーの値としていくつをセットするかを指定するには、SET QOS DEFAULTPRIORITY コマンド (356 ページ) を使います。たとえば、送信キュー 0~7 に対して、802.1p 値 0, 1, 2, 3, 4, 5, 6, 7 を割り当てるには、次のようにします。

```
SET QOS DEFAULTPRIORITY=0,1,2,3,4,5,6,7 ↵
```

この場合、手順 2 で設定したデフォルト送信キューが 1 であれば、802.1p ユーザープライオリティー

値 1 が割り当てられます。

基本設定は以上です。

送信スケジューリング方式を変更するには、SET QOS PORT EGRESSQUEUE コマンド (367 ページ) を使います。たとえば、すべてのポートで重み付きラウンドロビン (WRR) を使用するには、次のようにします。WRRWEIGHT パラメーターで各キューの重み (各キュー間の送信比率をデータ量ベースで表す) を指定します。

ここでは、キュー 7、6、5、4、3、2、1、0 から、60:60:30:30:12:12:6:6、すなわち、10:10:5:5:2:2:1:1 の比率でパケットが順番に送信されるよう設定します。

```
SET QOS PORT=ALL EGRESSQUEUE=6-7 SCHEDULER=WRR1 WRRWEIGHT=60 ↓
SET QOS PORT=ALL EGRESSQUEUE=4-5 SCHEDULER=WRR1 WRRWEIGHT=30 ↓
SET QOS PORT=ALL EGRESSQUEUE=2-3 SCHEDULER=WRR1 WRRWEIGHT=12 ↓
SET QOS PORT=ALL EGRESSQUEUE=0-1 SCHEDULER=WRR1 WRRWEIGHT=6 ↓
```

タグ付きパケット受信時に割り当てる送信キューの設定は、SHOW QOS PRIO2QUEUEMAP コマンド (471 ページ) で確認できます。

```
SHOW QOS PRIO2QUEUEMAP ↓
```

タグなしパケット受信時に割り当てる送信キュー (デフォルト送信キュー) の設定は、SHOW QOS PORT コマンド (468 ページ) で確認できます。「Default Queue」をご覧ください。

```
SHOW QOS PORT ↓
SHOW QOS PORT=1 ↓
```

受信時にタグなしだったパケットをタグ付きポートから送信するときの 802.1p ユーザープライオリティ値の設定は、SHOW QOS DEFAULTPRIORITY コマンド (460 ページ) で確認できます。

```
SHOW QOS DEFAULTPRIORITY ↓
```

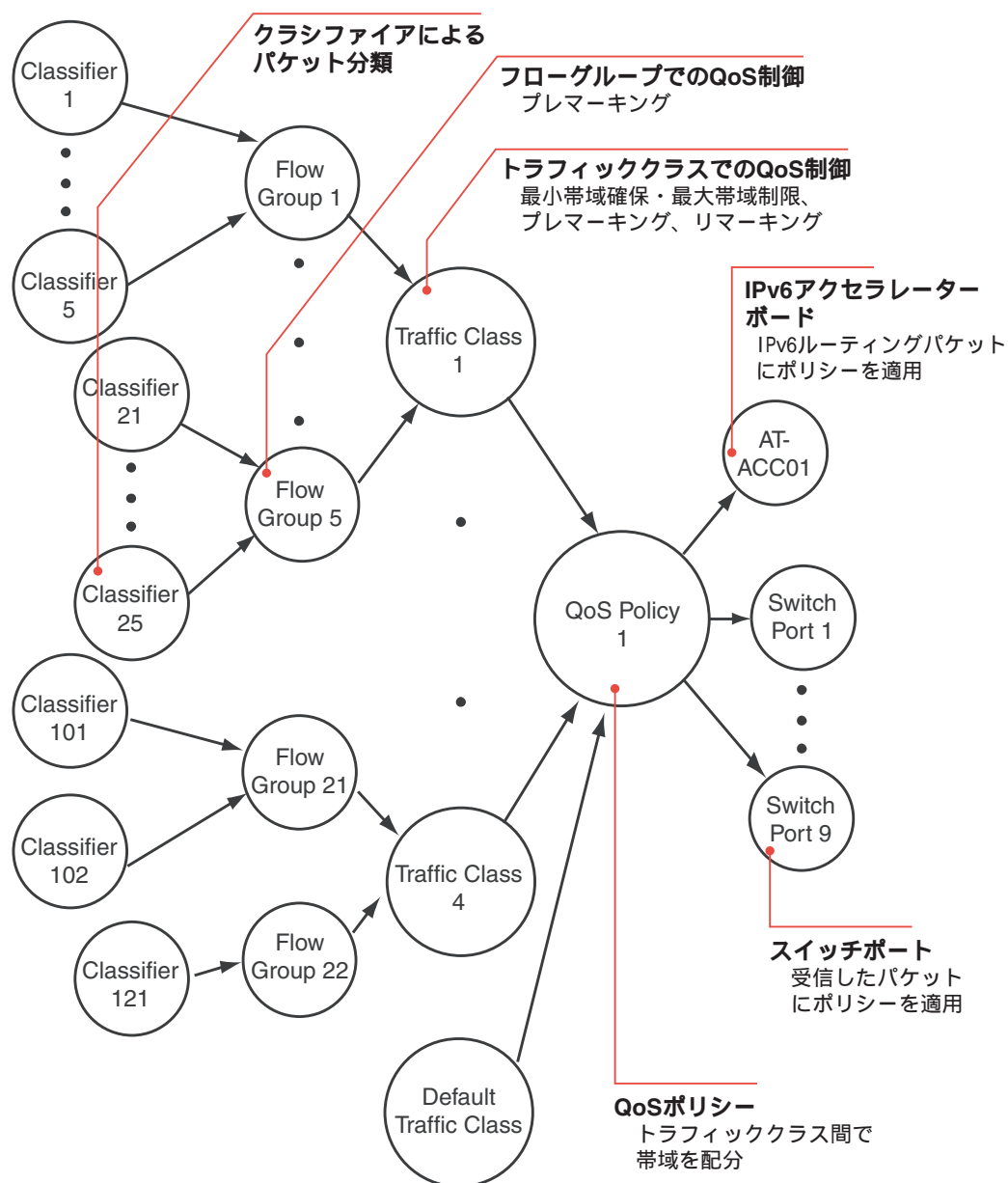
キューからパケットを送信するときのスケジューリング方式は、SHOW QOS PORT コマンド (468 ページ) で確認できます。各キューの「Scheduler」、「WRR Weight」をご覧ください。

```
SHOW QOS PORT=1 ↓
```

## ポリシーベース QoS の基本設定

ポリシーベース QoS の設定は、QoS ポリシーを作成し、スイッチポート (または IPv6 アクセラレーターボード) に関連付けることによって行います。QoS ポリシーは次図のような階層構造になっているため、ポ

リシーの作成はこの階層を形づくる作業と言えます。



QoS ポリシーの作成手順に明確な決まりはありません。最終的にすべての設定要素を1つにまとめられれば、どのような順番でもかまいません。ここでは、一例として次の手順を挙げておきます。

1. QoS ポリシーを作成する
2. QoS ポリシーをスイッチポート（またはIPv6 アクセラレーターボード）に関連付ける
3. トラフィッククラスを作成する
4. トラフィッククラスをQoS ポリシーに割り当てる
5. フローグループを作成する
6. フローグループをトラフィッククラスに割り当てる

7. クラシファイアを作成する
8. クラシファイアをフローグループに割り当てる

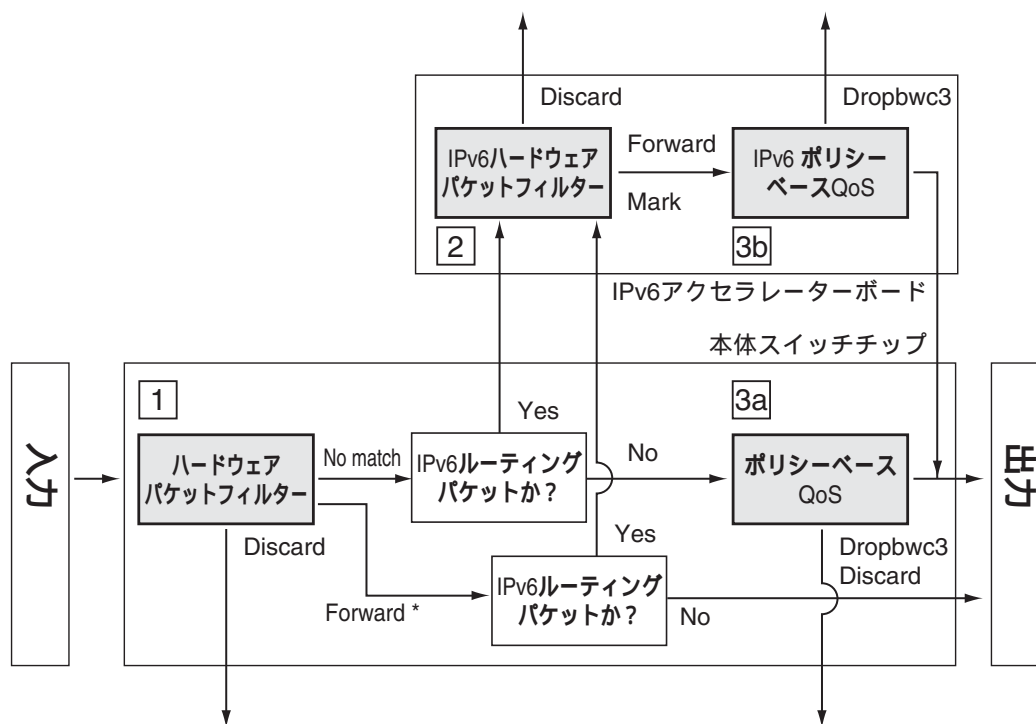
ここでは、ポリシーベース QoS の基本的な設定方法について解説します。

最初に、基本的な手順を示す設定例を紹介したのち、QoS ポリシーの基本設定要素である、スイッチポート、QoS ポリシー、トラフィッククラス、フローグループ、クラシファイアのそれぞれについて、設定の要点を説明します。

より詳細な設定方法については、「QoS 処理の流れ」をご覧ください。また、全体的な設定例については、「設定例」をご覧ください。

### 設定の前に

通常、ポリシーベース QoS の処理は本体スイッチチップで行われますが、IPv6 アクセラレーターボードを装着している場合、IPv6 ルーティングパケットに対する QoS 処理は、IPv6 アクセラレーターボードで行われます。次の図をご覧ください。



\* ハードウェアパケットフィルターにマッチしたパケットにはポリシーベースQoSが適用されない。  
パケットフィルタリングとポリシーベースQoSを併用する場合は、QoSポリシーのフィルタリング機能を使うほうがよい。

ポリシーベース QoS を使用するために必要な設定は次のとおりです。

- IPv6 アクセラレーターボードを装着していない場合、図中 3a の設定だけを行います。
- IPv6 アクセラレーターボードを装着しており、IPv4 と IPv6 を併用している場合、図中 3a (IPv4 用) と同 2、3b (IPv6 用) の設定を行います。



- IPv6 アクセラレーターボードを装着しており、IPv6 だけを使用している場合、図中 2、3b の設定を行います。

☞ IPv6 ルーティングパケットに対するポリシーベース QoS の設定では、IPv6 ハードウェアパケットフィルター（の MARK アクション）を併用します。

1 つ注意すべきなのは、ハードウェアパケットフィルターにマッチしたパケットに対して、ポリシーベース QoS が適用されないことです（ここでの「マッチ」とは、破棄（Discard）だけでなく明示的な転送許可（Forward）も含まれます）。

ポリシーベース QoS を利用しながらパケットフィルタリングを行いたい場合は、ハードウェアパケットフィルターを併用するのではなく、QoS ポリシーのフィルタリング機能（フローグループ、トラフィッククラスのアクション）を使ってください。フィルタリング機能については後述します。

### 設定手順例

次に基本的な設定手順例を示します。

#### 通常のパケット

通常のパケット（IPv6 ルーティングパケット以外のパケット）に対するポリシーベース QoS の基本設定を示します（上図の 3a の設定です）。

1. QoS ポリシー「1」を作成します。

```
CREATE QOS POLICY=1 ↵
```

2. QoS ポリシー「1」を受信スイッチポートである 1～3 に関連付けます。

```
SET QOS PORT=1-3 POLICY=1 ↵
```

3. 3 つのトラフィッククラスを作成し、それぞれに最大・最小帯域を割り当てます。この設定により、トラフィッククラス 1 には最低 50Mbps の帯域が保証されます。また、トラフィッククラス 1、2、3 は、それぞれ 80Mbps、30Mbps、20Mbps までに制限されます（帯域制限を機能させるため、DROPBWCLASS3=YES を指定し、最大帯域を上回るレートで受信したパケットをキューイング前に無条件で破棄するよう設定します）。

```
CREATE QOS TRAFFICCLASS=1 MAXBANDWIDTH=80M MINBANDWIDTH=50M
DROPBWCLASS3=YES ↵
```

```
CREATE QOS TRAFFICCLASS=2 MAXBANDWIDTH=30M DROPBWCLASS3=YES ↵
```

```
CREATE QOS TRAFFICCLASS=3 MAXBANDWIDTH=20M DROPBWCLASS3=YES ↵
```

4. QoS ポリシーにトラフィッククラスを割り当てます。

```
ADD QOS POLICY=1 TRAFFICCLASS=1-3 ↵
```

5. 各トラフィッククラスに対応する3つのフローグループを作成します。

```
CREATE QOS FLOWGROUP=1 ↓
```

```
CREATE QOS FLOWGROUP=2 ↓
```

```
CREATE QOS FLOWGROUP=3 ↓
```

6. トラフィッククラスにフローグループを割り当てます。

```
ADD QOS TRAFFICCLASS=1 FLOWGROUP=1 ↓
```

```
ADD QOS TRAFFICCLASS=2 FLOWGROUP=2 ↓
```

```
ADD QOS TRAFFICCLASS=3 FLOWGROUP=3 ↓
```

7. 各クライアントからのパケットに対応するクラシファイアを定義します。

```
CREATE CLASSIFIER=1 IPSADDR=192.168.1.1/32 ↓
```

```
CREATE CLASSIFIER=2 IPSADDR=192.168.1.2/32 ↓
```

```
CREATE CLASSIFIER=3 IPSADDR=192.168.1.3/32 ↓
```

8. フローグループにクラシファイアを割り当てます。

```
ADD QOS FLOWGROUP=1 CLASSIFIER=1 ↓
```

```
ADD QOS FLOWGROUP=2 CLASSIFIER=2 ↓
```

```
ADD QOS FLOWGROUP=3 CLASSIFIER=3 ↓
```

### IPv6 ルーティングパケット

IPv6 ルーティングパケットに対するポリシーベース QoS の設定（上図の 2、3b）は、基本的に通常のポリシーベース QoS と同じですが、以下の点が異なります。

- QoS ポリシーの関連付け先が、受信スイッチポートではなく、IPv6 アクセラレーターボードになります。関連付けに使用するコマンドも、SET QOS PORT コマンド（365 ページ）ではなく、SET QOS ACCELERATOR POLICY コマンド（355 ページ）になります。  
IPv6 アクセラレーターボードに関連付けられた QoS ポリシーは、IPv6 アクセラレーターボードを経由するすべてのパケット（すべての IPv6 ルーティングパケット）に適用されます。
- パケットの分類を IPv6 ハードウェアパケットフィルター（上図の 2）、QoS ポリシー（上図の 3b）の 2 段階で行います。
  1. IPv6 ハードウェアパケットフィルターの MARK アクションを使ってパケットを分類し、それぞれに異なる DSCP 値を割り当てます。分類には、L3、L4 の各パラメーターを使用できます。
  2. QoS ポリシーのクラシファイアでは、おもに 1 でセットされた DSCP 値に基づいてパケットをフローグループに分類します。QoS ポリシーのクラシファイアでは、DSCP 値を除き L3 以上のパラメーターを使用できないためです。



- クラシファイアの VLAN パラメーターが「出力 VLAN」の意味になります (通常は「入力 VLAN」)。
- プレマーキング、リマーキング時にパケットの DSCP 値を参照することができません。したがって、PREMARKING=USEDSCP (DTCPREMARKING も同様) REMARKING=USEDSCPMAP (DTCREMARKING も同様) の指定はできません。

以下、IPv6 ルーティングパケットに対するポリシーベース QoS の基本的な設定手順例を示します。

- ④ IPv6 ルーティングパケットに対してポリシーベース QoS を適用するには、IPv6 アクセラレーターボードが必要です。また、IPv6 ルーティングの設定も必要です。以下の例では、IPv6 の設定は完了しているものとします。

1. 最初に、IPv6 パケットを分類するためのクラシファイアを作成します。CREATE CLASSIFIER コマンド (198 ページ) の「IPv6 ハードウェアパケットフィルター用の構文」にしたがって作成してください。

```
CREATE CLASSIFIER=101 ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6
    IPSADDR=3ffe:b80:3c:1::1/128 ↵
CREATE CLASSIFIER=102 ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6
    IPSADDR=3ffe:b80:3c:1::2/128 ↵
CREATE CLASSIFIER=103 ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6
    IPSADDR=3ffe:b80:3c:1::3/128 ↵
```

2. 手順 1 のクラシファイアを用いて、DSCP フィールドを書き換える IPv6 ハードウェアパケットフィルターを設定します。QoS ポリシーでは、この DSCP 値に基づいてパケットをフローグループに分類します。

```
ADD SWITCH ACCELERATOR HWFILTER=101 CLASSIFIER=101 ACTION=MARK
    NEWIPDSCP=1 ↵
ADD SWITCH ACCELERATOR HWFILTER=102 CLASSIFIER=102 ACTION=MARK
    NEWIPDSCP=2 ↵
ADD SWITCH ACCELERATOR HWFILTER=103 CLASSIFIER=103 ACTION=MARK
    NEWIPDSCP=3 ↵
```

3. QoS ポリシー「10」を作成します。

```
CREATE QOS POLICY=10 ↵
```

4. QoS ポリシー「10」を IPv6 アクセラレーターボードに適用します。これには、SET QOS ACCELERATOR POLICY コマンド (355 ページ) を使います。

IPv6 ルーティングパケットに対する QoS 設定は、ルーティングされるすべての IPv6 パケットに適用されます。通常のポリシーベース QoS のように、受信スイッチポートを指定することはできません。

```
SET QOS ACCELERATOR POLICY=10 ↵
```

5. 3 つのトラフィッククラスを作成し、それぞれに最大・最小帯域を割り当てます。この設定により、トラフィッククラス 1 には最低 50Mbps の帯域が保証されます。また、トラフィッククラス 1、

2、3 は、それぞれ 80Mbps、30Mbps、20Mbps までに制限されます（帯域制限を機能させるため、DROPBWCLASS3=YES を指定し、最大帯域を上回るレートで受信したパケットをキューイング前に無条件で破棄するよう設定します）。

```
CREATE QOS TRAFFICCLASS=1 MAXBANDWIDTH=80M MINBANDWIDTH=50M
    DROPBWCLASS3=YES ↓
CREATE QOS TRAFFICCLASS=2 MAXBANDWIDTH=30M DROPBWCLASS3=YES ↓
CREATE QOS TRAFFICCLASS=3 MAXBANDWIDTH=20M DROPBWCLASS3=YES ↓
```

6. QoS ポリシーにトラフィッククラスを割り当てます。

```
ADD QOS POLICY=10 TRAFFICCLASS=1-3 ↓
```

7. 各トラフィッククラスに対応する 3 つのフローグループを作成します。

```
CREATE QOS FLOWGROUP=1 ↓
CREATE QOS FLOWGROUP=2 ↓
CREATE QOS FLOWGROUP=3 ↓
```

8. トラフィッククラスにフローグループを割り当てます。

```
ADD QOS TRAFFICCLASS=1 FLOWGROUP=1 ↓
ADD QOS TRAFFICCLASS=2 FLOWGROUP=2 ↓
ADD QOS TRAFFICCLASS=3 FLOWGROUP=3 ↓
```

9. 各クライアントからのパケットに対応するクラシファイアを定義します。ここでは、IPv6 ハードウェアパケットフィルタで書き換えた（マーキングした）DSCP 値に基づいてパケットを分類します。CREATE CLASSIFIER コマンド（198 ページ）の「IPv6 QoS ポリシー用の構文」にしたがって作成してください。

```
CREATE CLASSIFIER=1 ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6 IPDSCP=1 ↓
CREATE CLASSIFIER=2 ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6 IPDSCP=2 ↓
CREATE CLASSIFIER=3 ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6 IPDSCP=3 ↓
```

10. フローグループにクラシファイアを割り当てます。

```
ADD QOS FLOWGROUP=1 CLASSIFIER=1 ↓
ADD QOS FLOWGROUP=2 CLASSIFIER=2 ↓
ADD QOS FLOWGROUP=3 CLASSIFIER=3 ↓
```

## QoS ポリシー

ポリシーベース QoS の基本要素は QoS ポリシーです。本製品では、スイッチポート（または IPv6 アクセラレーターボード）に QoS ポリシーを関連付けることで、該当ポートで受信したパケット（またはルーティングされる IPv6 パケット）に対する動作を制御します。

QoS ポリシーを作成するには、CREATE QOS POLICY コマンド（212 ページ）を使います。同コマンドでは、DTCxxxx という名のパラメーターを用いて、デフォルトトラフィッククラスの各種属性を設定することもできます。

次の例では、QoS ポリシー「1」を作成すると同時に、同ポリシーのデフォルトトラフィッククラスに割り当てる最大帯域を 1Mbps に制限しています。

```
CREATE QOS POLICY=1 DTCMAXBANDWIDTH=1M ↵
```

QoS ポリシーをスイッチポートに割り当てるには、SET QOS PORT コマンド（365 ページ）を使います。これにより、該当ポートで受信したパケットに対して QoS ポリシーが適用されます。

```
SET QOS PORT=1-4 POLICY=1 ↵
```

- ✎ トランクグループに QoS ポリシーを割り当てるときは、グループ内のいずれかのポートにポリシーを適用してください。ただし、所属ポートがポートグループ「1～12」と「13～24」をまたいでいるトランクグループには QoS ポリシーを適用できません。

また、QoS ポリシーを IPv6 アクセラレーターボードに割り当てるには、SET QOS ACCELERATOR POLICY コマンド（355 ページ）を使います。これにより、IPv6 アクセラレーターボードを経由するすべてのパケット（IPv6 ルーティングパケット）に対して QoS ポリシーが適用されます。

```
SET QOS ACCELERATOR POLICY=10 ↵
```

- ✎ スwitchポート、IPv6 アクセラレーターボードには、QoS ポリシーを 1 つだけ割り当てることができます。
- ✎ QoS ポリシーは、複数のスイッチポートに割り当てることができます。また、QoS ポリシーには、複数のトラフィッククラスを割り当てることができます。
- ✎ ポリシーベース QoS の設定では、最初に QoS ポリシーを作成しスイッチポートや IPv6 アクセラレーターボードに割り当てたあとで、トラフィッククラスやフローグループの設定をすることをおすすめします。これは、QoS 設定パラメーター（帯域設定など）のエラーチェックが、「トラフィッククラス割り当て済みのポリシーをスイッチポートや IPv6 アクセラレーターボードに関連付けるとき」、または、「スイッチポートや IPv6 アクセラレーターボードに関連付けられた QoS ポリシーにトラフィッククラスやフローグループを追加したとき」に行われるためです。最初に QoS ポリシーを割り当てておくことで、設定の早い段階でエラーを検出できるようになります。
- ✎ QoS ポリシーを適用するポートの数が多いと、システムルール領域の消費量が多くなります。ポリシーベース

QoSを利用する場合は、ポリシーを割り当てるスイッチポートを選ぶようにしてください。詳しくは「スイッチング」の「クラシファイア」をご覧ください（「クラシファイアとルール領域消費量」を参照）。

ポートから QoS ポリシーを削除（関連付けを削除）するには、SET QOS PORT コマンド（365 ページ）の POLICY パラメーターに NONE を指定します。これにより、該当ポートで受信したパケットにはポリシーベース QoS が適用されなくなります。

```
SET QOS PORT=1-4 POLICY=NONE ↓
```

IPv6 アクセラレーターボードから QoS ポリシーを削除（関連付けを削除）するには、SET QOS ACCELERATOR POLICY コマンド（355 ページ）の POLICY パラメーターに NONE を指定します。これにより、IPv6 ルーティングパケットにはポリシーベース QoS が適用されなくなります。

```
SET QOS ACCELERATOR POLICY=NONE ↓
```

## トラフィッククラス

トラフィッククラスは、同等の QoS を与えるべきトラフィック（たとえば、「TCP トラフィック」）をひとまとめにしたものです。ポリシーベース QoS の設定項目の大部分は、トラフィッククラスごとに設定します。QoS ポリシーは、複数のトラフィッククラスで構成されます。QoS ポリシー内の各トラフィッククラスは、各クラスの設定に基づきポート帯域を分け合うことになります。

トラフィッククラスを作成するには、CREATE QOS TRAFFICCLASS コマンド（218 ページ）を使います。

```
CREATE QOS TRAFFICCLASS=1 ↓
```

トラフィッククラスに割り当てる最小帯域（保証帯域）、最大帯域（上限値）は、それぞれ MINBANDWIDTH、MAXBANDWIDTH パラメーターで指定します。

```
CREATE QOS TRAFFICCLASS=1 MINBANDWIDTH=1.5M MAXBANDWIDTH=3M ↓
```

プレマーキング、リマーキングの動作は、CREATE QOS TRAFFICCLASS コマンド（218 ページ）、SET QOS TRAFFICCLASS コマンド（373 ページ）の PREMARKING、MARKVALUE、REMARKING パラメーターで指定します。

```
SET QOS TRAFFICCLASS=1 PREMARKING=USEDSCP ↓
```

フローグループとトラフィッククラスの両方でプレマーキングの設定がされている場合は、フローグループの設定が使用されます。フローグループで設定されていない場合は、トラフィッククラスの設定が使用されます。どちらも設定されていない場合は、プレマーキングを行わずにメータリングに進みます。

作成したトラフィッククラスの設定を変更するには、SET QOS TRAFFICCLASS コマンド (373 ページ) を使います。

```
SET QOS TRAFFICCLASS=1 MINBANDWIDTH=2.0M ↓
```

トラフィッククラスを QoS ポリシーに割り当てるには、ADD QOS POLICY コマンド (180 ページ) を使います。パケットのチェック (クラシファイアとの照合) は、ポリシー内のトラフィッククラス番号順に行われます。

```
ADD QOS POLICY=1 TRAFFICCLASS=1-3 ↓
```

- ✎ QoS ポリシーには複数のトラフィッククラスを割り当てることができます。
- ✎ トラフィッククラスは、1 つの QoS ポリシーにしか割り当てることができません。あるポリシーに割り当てたトラフィッククラスは、別のポリシーでは使用できません。
- ✎ トラフィッククラスには、複数のフローグループを割り当てることができます。

## フローグループ

フローグループは、トラフィッククラスをさらに細分化したものです。QoS ポリシーの設定の大半はトラフィッククラスのレベルで行いますが、同一トラフィッククラス内でより細かな設定をしたい場合は、トラフィッククラスを構成するフローグループごとに微調整が可能です。

フローグループは、クラシファイアによって分類された「フロー」をグループ化したものです。同じ性格を持つフロー (特定アプリケーションの「行き」と「戻り」など) を束ねたものと言えます。フローグループは、複数のクラシファイアで構成されます。

フローグループを作成するには、CREATE QOS FLOWGROUP コマンド (209 ページ) を使います。

```
CREATE QOS FLOWGROUP=1 ↓
```

パケットがどのフローグループに所属するかを決定するのは、汎用のパケットフィルターであるクラシファイアです。クラシファイアは CREATE CLASSIFIER コマンド (198 ページ) で作成します。たとえば、Web トラフィック (HTTP と HTTPS) に対応するクラシファイアは次のようになります。

```
CREATE CLASSIFIER=1 TCPDPORT=80 ↓
CREATE CLASSIFIER=2 TCPSPORT=80 ↓
CREATE CLASSIFIER=3 TCPDPORT=443 ↓
CREATE CLASSIFIER=4 TCPSPORT=443 ↓
```

フローグループにクラシファイアを関連付けるには、ADD QOS FLOWGROUP コマンド (179 ページ)

を使います。

```
ADD QOS FLOWGROUP=1 CLASSIFIER=1-4 ↓
```

ポリシーベース QoS の設定項目の大部分はトラフィッククラスで指定しますが、プレマーキングの動作については、フローグループ単位でも設定可能です。これらは、CREATE QOS FLOWGROUP コマンド (209 ページ)、SET QOS FLOWGROUP コマンド (359 ページ) のPREMARKING、MARKVALUE パラメーターで指定します。

```
SET QOS FLOWGROUP=1 PREMARKING=USEMARKVALUE MARKVALUE=1 ↓
```

フローグループとトラフィッククラスの両方でプレマーキングの設定がされている場合は、フローグループの設定が使用されます。フローグループで設定されていない場合は、トラフィッククラスの設定が使用されます。

フローグループは、トラフィッククラスに割り当てて使います。フローグループをトラフィッククラスに割り当てするには、ADD QOS TRAFFICCLASS コマンド (181 ページ) を使います。パケットのチェック (クラシファイアとの照合) は、トラフィッククラス内のフローグループ番号順に行われます。

```
ADD QOS TRAFFICCLASS=1 FLOWGROUP=2,4 ↓
```

- ☞ フローグループは、1 つのトラフィッククラスにしか割り当てることができません。一方、トラフィッククラスには、複数のフローグループを割り当てることができます。

## クラシファイア

ポリシーベース QoS 機能の中心要素が QoS ポリシーだとすると、末端の要素はクラシファイアです。クラシファイアは、ハードウェアパケットフィルターでも用いられる汎用のパケットフィルターで、アドレス、プロトコルなどをもとにパケットを「フロー」に分類する働きを持ちます。

ポリシーベース QoS では、パケットをフローグループやトラフィッククラスに分類して、グループやクラスごとに処理を行いますが、これらの分類の第一歩はクラシファイアによって行われます。

クラシファイアは CREATE CLASSIFIER コマンド (198 ページ) で作成します。通常のポリシーベース QoS と IPv6 ポリシーベース QoS では、使用できる条件パラメーターが異なるので注意してください。

- 通常のポリシーベース QoS で使用するクラシファイアは、「ハードウェアパケットフィルター・QoS ポリシー用の構文」にしたがって作成してください。

```
CREATE CLASSIFIER=101 IPDADDR=192.168.10.5/32 ↓
```

- IPv6 ポリシーベース QoS で使用するクラシファイアは、「IPv6 QoS ポリシー用の構文」にしたがって作成してください。

```
CREATE CLASSIFIER=1001 ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6
      IPDSCP=23 ↓
```

📎 クラシファイアの詳細については、「スイッチング」の「クラシファイア」をご覧ください。

フローグループはクラシファイアの集合として定義します。フローグループにクラシファイアを割り当てるには、ADD QOS FLOWGROUP コマンド (179 ページ) を使います。

```
ADD QOS FLOWGROUP=1 CLASSIFIER=101 ↓
```

📎 クラシファイアは、複数のフローグループに割り当てることができます。ただし、同一ポリシー内で同じクラシファイアを複数回使うことは、動作が予測できないため避けてください。

## QoS 処理フロー詳細

ここでは、個々の QoS 機能について、全体的な QoS 処理の流れにしたがって解説します。

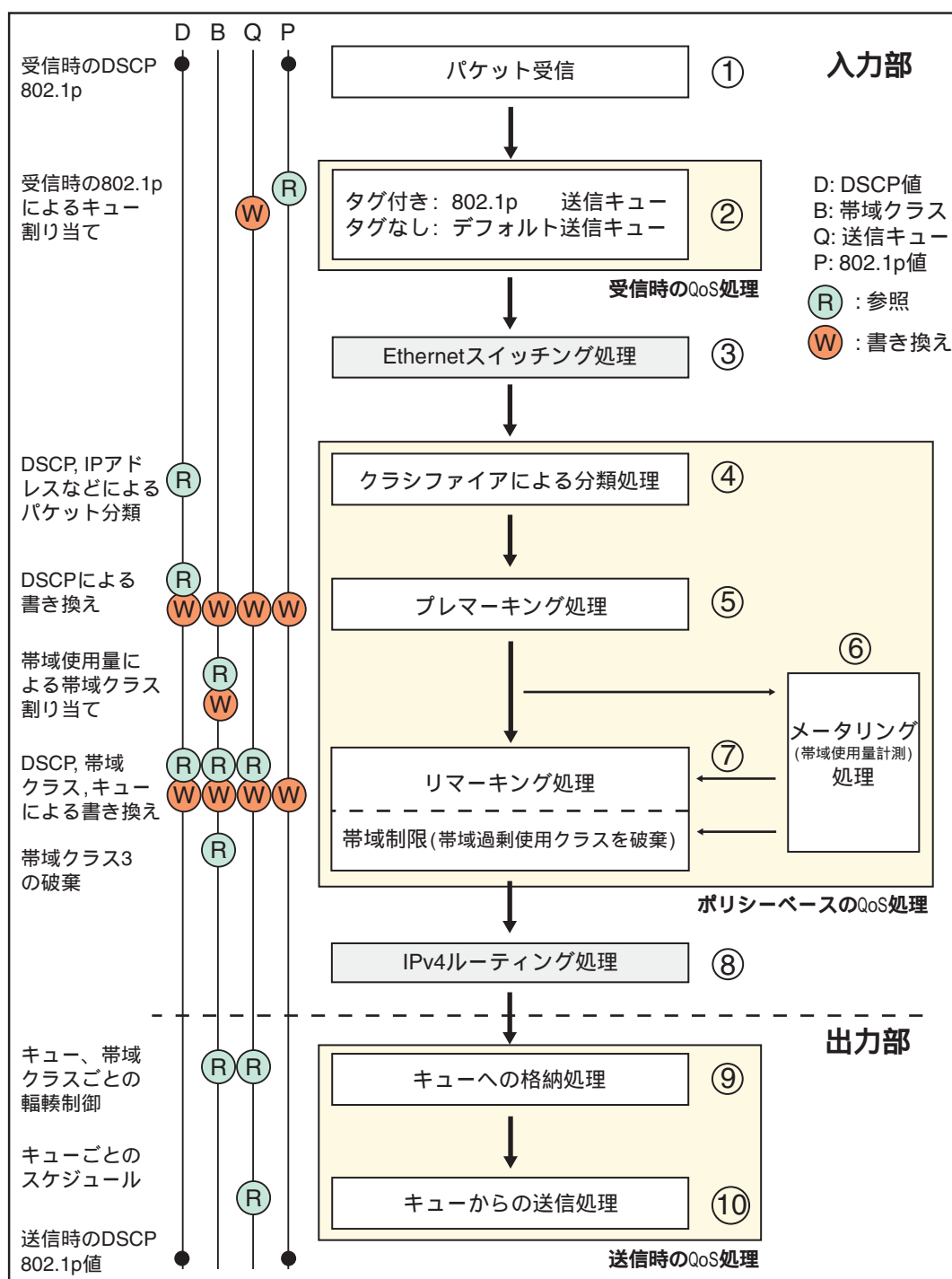
次に、パケットを受信してから送信するまでの、QoS 処理の大まかな流れを示します。一見すると非常に複雑ですが、通常はすべての段階を設定する必要はありません。

なお、図の左側では、QoS 処理過程で使用される「4 つの QoS パラメーター」がどこで参照 (使用) され、どこで書き換え (割り当て) されるのかを示しています。

また、IPv6 アクセラレーターボード装着時は、「ルーティングされる IPv6 パケット」と「それ以外のパケット」で処理の流れが若干異なります。

### 通常のパケット

通常のパケット (IPv6 ルーティングパケット以外) は次の流れで処理されます。IPv6 アクセラレーターボードを装着していないときは、すべてのパケットがこの流れで処理されます。



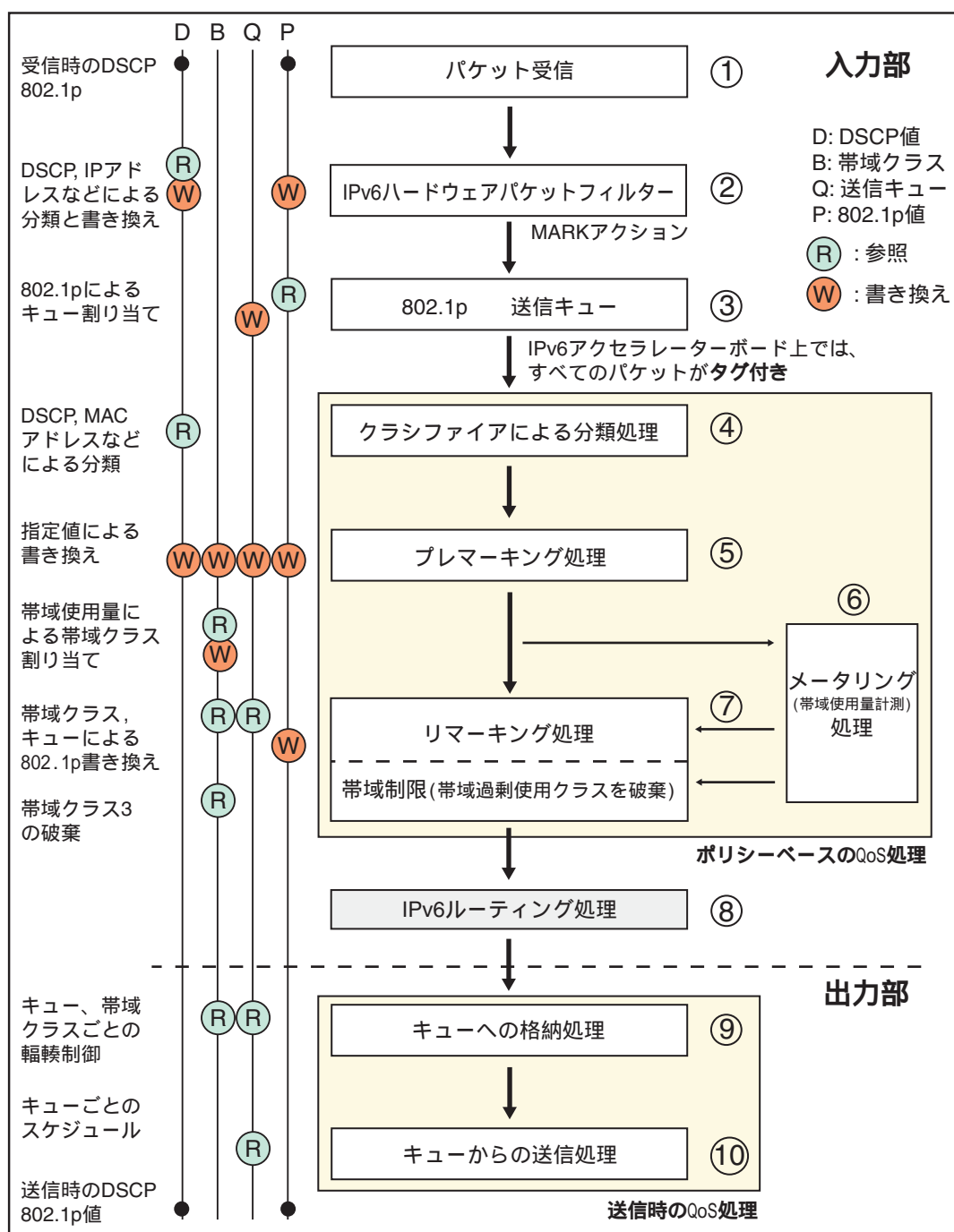


-	処理内容	備考
1	スイッチポートでパケットを受信します	-
2	受信パケットがタグ付きなら、SET QOS PRIO2QUEUEMAP コマンドの設定に基づき、802.1p ユーザープライオリティー値から初期の送信キュー（0～7）を決定します。また、タグなしパケットには、SET QOS PORT コマンドの DEFAULTQUEUE パラメーターで指定された送信キューを割り当てます	802.1p
3	受信パケットがレイヤー 2 スイッチングの対象なら、フォワーディングデータベースを参照して出力ポートを決定します	-
4	クラシファイアにより、パケットをフローグループ、トラフィッククラスに分類します。どのクラシファイアにもマッチしなかったパケットは、デフォルトトラフィッククラスに分類します	ポリシーベース
5	フローグループかトラフィッククラスでプレマージングの設定がなされている場合、受信パケットの DSCP 値、802.1p 値を書き換えます。また、帯域クラスと送信キューを割り当てます	ポリシーベース
6	トラフィッククラスで最大・最小帯域の設定がなされている場合、受信パケットの属するフローがどの程度帯域を使用しているかを計測します。計測結果に基づき、受信パケットを 3 つの「帯域クラス」に分類します	ポリシーベース
7	トラフィッククラスでリマージングの設定がなされている場合、受信パケットの DSCP 値、802.1p 値を書き換えます。また、帯域クラスと送信キューを割り当てます。CREATE QOS TRAFFICCLASS コマンドの DROPBWCLASS3 パラメーターが YES に設定されている場合は、「帯域クラス 3（帯域を使いすぎ）」に該当するパケットを破棄します	ポリシーベース
8	受信パケットが IPv4 ルーティングの対象なら、L3 テーブルを参照して出力ポートを決定します	-
9	ここまでの処理で決定した送信キューにパケットを格納します。デフォルトでは、キューがいっぱいならパケットを破棄します（Tail-drop）。SET QOS PORT コマンドの RED パラメーターの設定により、キュー長が限界に達する前にランダムにパケットを破棄して輻輳を回避することもできます（RED アルゴリズム）	802.1p/ポリシーベース
10	SET QOS PORT EGRESSQUEUE コマンドで指定されたスケジューリング方式にしたがい、送信キューからパケットを出力します。デフォルトの動作は絶対優先スケジューリング（STRICT）ですが、重み付きラウンドロビン（WRR）や絶対優先 + WRR の組み合わせ設定も可能です	802.1p/ポリシーベース

表 20: QoS 処理の流れ

### IPv6 ルーティングパケット

IPv6 アクセラレーターボード装着時、IPv6 ルーティングパケットに対する QoS 処理の流れは次のようになります。ほとんどの処理はその他のパケットと同じですが、分類処理が IPv6 ハードウェアパケットフィルター（手順 2）と QoS ポリシー（手順 4）の 2 段階にわかれている点が異なります。



処理内容	備考
1 スイッチポートでパケットを受信します。IPv6 ルーティングパケットは、本体スイッチチップから IPv6 アクセラレーターボードに送られて処理されます	-

2	IPv6 ハードウェアパケットフィルターの MARK アクションにより、IP アドレス、DSCP 値、ポート番号など L3、L4 フィールド値に基づいて IPv6 パケットを分類し、後の処理のため DSCP 値、802.1p ユーザープライオリティー値を書き換えます	-
3	SET QOS PRIO2QUEUEMAP コマンドの設定に基づき、802.1p ユーザープライオリティー値から初期の送信キュー（0～7）を決定します（IPv6 アクセラレーターボード内ではすべてのパケットにタグが付いています）	802.1p
4	クラシファイアにより、パケットをフローグループ、トラフィッククラスに分類します。ここで使える分類条件は L2（MAC アドレス、出力 VLAN）と DSCP 値だけなので、L3、L4 フィールド値に基づく分類が必要なときは、手順 2 でマーキングしておきます（DSCP 値を書き換えておく）。どのクラシファイアにもマッチしなかったパケットは、デフォルトトラフィッククラスに分類します	ポリシーベース
5	フローグループかトラフィッククラスでプレマーキングの設定がなされている場合、MARKVALUE パラメーターの値に基づき、受信パケットの DSCP 値、802.1p 値を書き換えます。また、帯域クラスと送信キューを割り当てます	ポリシーベース
6	トラフィッククラスで最大・最小帯域の設定がなされている場合、受信パケットの属するフローがどの程度帯域を使用しているかを計測します。計測結果に基づき、受信パケットを 3 つの「帯域クラス」に分類します	ポリシーベース
7	トラフィッククラスでリマーキングの設定がなされている場合、受信パケットの 802.1p 値を書き換えます。CREATE QOS TRAFFICCLASS コマンドの DROPBWCLASS3 パラメーターが YES に設定されている場合は、「帯域クラス 3（帯域を使いすぎ）」に該当するパケットを破棄します	ポリシーベース
8	IPv6 ルーティング処理を行います	-
9	ここまでの処理で決定した送信キューにパケットを格納します。デフォルトでは、キューがいっぱいならパケットを破棄します（Tail-drop）。SET QOS PORT コマンドの RED パラメーターの設定により、キュー長が限界に達する前にランダムにパケットを破棄して輻輳を回避することもできます（RED アルゴリズム）	802.1p/ポリシーベース
10	SET QOS PORT EGRESSQUEUE コマンドで指定されたスケジューリング方式にしたがい、送信キューからパケットを出力します。デフォルトの動作は絶対優先スケジューリング（STRICT）ですが、重み付きラウンドロビン（WRR）や絶対優先 + WRR の組み合わせ設定も可能です	802.1p/ポリシーベース

表 21: QoS 処理の流れ (IPv6 ルーティングパケット)

上記の各ステップは、さらに大きく 3 つのグループに分類できます。

1. パケット受信時の QoS 処理 (802.1p 値による送信キュー割り当て)
2. ポリシーベースの QoS 処理 (クラシファイアによる分類と各種サービスレベルの割り当て)
3. パケット送信時の QoS 処理 (キューへの格納、輻輳制御とキューからの送信)

通常、ポリシーベース QoS ではグループ 2 と 3 の設定を、802.1p QoS ではグループ 1 と 3 の設定を行うこととなります。

以下では、各グループでの処理について詳しく解説します。

### パケット受信時の QoS 処理

スイッチポートでパケットを受信した後、最初に行われる QoS 処理は、パケットに送信キューの初期値を割り当てることです。これは次のようにして行われます。

- タグ付きパケットの場合は、受信時に VLAN タグの 802.1p ユーザープライオリティー値をもとに送信キューを決定します。
- タグなしパケットの場合は、受信時に (受信ポートごとに設定された) デフォルトキューを割り当てます。
- IPv6 ルーティングパケットは、内部的にタグ付きパケットとして扱われます (受信時にタグなしだったパケットはプライオリティー「0」)。したがって、802.1p ユーザープライオリティー値をもとに送信キューが決定されます。

☞ パケット受信時の QoS 処理は、QoS ポリシーの有無にかかわらず実行されます。

☞ 受信時に決定された送信キューは、ポリシーベース QoS のプレマーキング、リマーキング段階において変更可能です。

### タグ付きパケット

タグ付きパケットの VLAN タグヘッダーには、3 ビットのユーザープライオリティーフィールド (802.1p) が設けられています。本製品は、このフィールドの値にしたがって、受信パケットの送信に優先度をつけることができます。

本製品の各ポートは、それぞれ 8 レベル (0~7) の送信キューを備えています (キュー 7 が優先度最高)。デフォルトの送信スケジューリング方式 (絶対優先スケジューリング) では、パケットは相対的にもっとも優先度の高いキューからのみ送信されます。たとえば、キュー 7 とキュー 6 にパケットが格納されている場合、キュー 7 が空になるまでキュー 6 内のパケットは送信されません。

受信パケットがどのキューに入れられるかは、802.1p ユーザープライオリティー値と送信キューのマッピング設定によって決まります。

タグ付きパケットの 802.1p ユーザープライオリティー値と送信キューのマッピングを変更するには、SET QOS PRIO2QUEUEMAP コマンド (369 ページ) を使います。

```
SET QOS PRIO2QUEUEMAP=0,0,3,3,4,5,6,7 ↵
```

ユーザープライオリティと送信キューのマッピングを確認するには SHOW QOS PRIO2QUEUEMAP コマンド (471 ページ) を使います。

```
SHOW QOS PRIO2QUEUEMAP ↵
```

IPv6 ルーティングパケットの場合は、IPv6 ハードウェアパケットフィルターの MARK アクションで 802.1p ユーザープライオリティ値を書き換えることができます。書き換え処理は送信キューの割り当て前に行われるため、この機能を利用すればパケットを任意のキューに入れることができます。

```
CREATE CLASSIFIER=201 ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6
  IPSADDR=3ffe:b80:3c:10::1/128 ↵
CREATE CLASSIFIER=202 ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6
  IPSADDR=3ffe:b80:3c:10::2/128 ↵
CREATE CLASSIFIER=203 ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6
  IPSADDR=3ffe:b80:3c:10::3/128 ↵
ADD SWITCH ACCELERATOR HWFILTER=1 CLASSIFIER=201 ACTION=MARK
  NEWPRIORITY=7 ↵
ADD SWITCH ACCELERATOR HWFILTER=2 CLASSIFIER=202 ACTION=MARK
  NEWPRIORITY=4 ↵
ADD SWITCH ACCELERATOR HWFILTER=3 CLASSIFIER=203 ACTION=MARK
  NEWPRIORITY=1 ↵
```

### タグなしパケット

受信したタグなしパケットには、SET QOS PORT コマンド (365 ページ) の DEFAULTQUEUE パラメーターで指定されたキュー (デフォルト送信キュー) に割り当てられます。

タグなしパケットに割り当てるデフォルトの送信キューは、SET QOS PORT コマンド (365 ページ) の DEFAULTQUEUE パラメーターで設定します。これは受信ポートごとに設定します。たとえば、すべてのポートにおいて、受信したタグなしパケットに送信キュー 1 を割り当てるには、次のようにします。

```
SET QOS PORT=ALL DEFAULTQUEUE=1 ↵
```

タグなしパケットに割り当てるデフォルトの送信キューは、SHOW QOS PORT コマンド (468 ページ) で確認できます。デフォルト送信キューは、SET QOS PORT コマンド (365 ページ) でスイッチポートごとに設定します。

SHOW QOS PORT=1 ↵

## ポリシーベースの QoS 処理

本製品の QoS 機能のうち、ポリシーベース QoS 独自の処理は、次の 4 ステップで構成されています。

1. クラシファイアによるパケット分類（フローグループ、トラフィッククラスへの分類）
2. プレマーキング（QoS パラメーターの初期値割り当て）
3. メータリング（帯域使用量の計測と帯域クラスの割り当て）
4. リマーキング（QoS パラメーターの再割り当て）

以下では、各ステップについて解説します。

### パケット分類

ポリシーベースの QoS 処理で最初に行われるのは、クラシファイアによってパケットをフローグループ、トラフィッククラスに分類することです。

パケットとクラシファイアの照合は、QoS ポリシー内のトラフィッククラス番号順で行われます。また、トラフィッククラス内では、フローグループの番号順に行われます。

クラシファイアの詳細については、「スイッチング」の「クラシファイア」をご覧ください。

### プレマーキング

プレマーキング（premarking）は、クラシファイアによってフローグループ、トラフィッククラスに分類されたパケットに対して行われる最初の QoS 処理です。

プレマーキングでは、フローグループ、トラフィッククラスごとに、受信パケットの DSCP 値、802.1p ユーザープライオリティ値を書き換えられます。また、帯域クラス（後述）と送信キューを割り当てることができます。

ポリシーベース QoS では、各パケットは QoS パラメーターとして次の 4 つの属性を持ちます。

- DSCP 値（0～63）
- 帯域クラス（1～3）
- 送信キュー（0～7）
- 802.1p ユーザープライオリティ値（0～7）

これらは、プレマーキング、メータリング、リマーキングの各段階において、変更されていきます。

プレマーキング段階では、プレマーキング用 DSCP MAP テーブルを参照して、パケットにパラメーターを割り当てます。DSCP MAP テーブルは、DSCP 値を主インデックス、帯域クラスを副インデックスとするテーブルで、各エントリーには前述の QoS パラメーター 4 種類の書き換え後の値が格納されています。

- ☞ DSCP MAP テーブルには DSCP 値と帯域クラスの 2 つのインデックスがありますが、プレマーキング用 DSCP MAP テーブルの場合は、副インデックスの帯域クラスは 1 しか存在しません。実質的には DSCP 値だけがインデックスとなります。



プレマーキングの設定は、トラフィッククラス単位、または、フローグループ単位で行うことができます。トラフィッククラスとフローグループの両方でプレマーキングを設定した場合は、フローグループでの設定が使用されます。トラフィッククラス全体に適用したい設定はトラフィッククラスで行い、これを上書きしたい場合はフローグループで設定を行います。

トラフィッククラスでプレマーキングの設定をするには、CREATE QOS TRAFFICCLASS コマンド (218 ページ) \ SET QOS TRAFFICCLASS コマンド (373 ページ) の PREMARKING パラメーターを使います。PREMARKING=USEMARKVALUE を指定した場合は、MARKVALUE パラメーターで指定した DSCP 値をインデックスとしてプレマーキング用 DSCPMAP テーブルを検索し、該当エントリーの内容にしたがってパケットに QoS パラメーターを割り当てます。PREMARKING=USEDSCP を指定した場合は、受信パケットの DSCP 値をインデックスとして使います。PREMARKING=NONE (デフォルト) の場合は、プレマーキングを行いません。

- ④ デフォルトトラフィッククラスに対しても、CREATE QOS POLICY コマンド (212 ページ) \ SET QOS POLICY コマンド (361 ページ) で同様の設定ができます。そのとき、各パラメーター名の前に DTC (デフォルトトラフィッククラスの略) を付けてください (以下同じ)。
- ④ IPv6 ルーティングパケットに対する QoS ポリシーでは、PREMARKING=USEDSCP を使用できません (パケットの DSCP 値に基づくプレマーキングができません)。USEDSCP を指定してもエラーにはなりませんが、プレマーキングが行われませんのでご注意ください。

フローグループでプレマーキングの設定をするには、CREATE QOS FLOWGROUP コマンド (209 ページ) \ SET QOS FLOWGROUP コマンド (359 ページ) の PREMARKING パラメーターを使います。設定方法は前述のトラフィッククラスと同じです。

プレマーキング用 DSCPMAP テーブルの設定は、SET QOS DSCPMAP コマンド (357 ページ) で行います。たとえば、DSCP 値 (MARKVALUE 値) が 1 のパケットに対して、DSCP 値 1、帯域クラス 1、送信キュー 7、802.1p ユーザープライオリティー 7 を割り当てるには、つぎのようにします。

```
SET QOS DSCPMAP=PREMARKING DSCP=1 NEWDSCP=1 NEWBWCLASS=1 NEWQUEUE=7
NEWPRIORITY=7 ↵
```

プレマーキング用 DSCPMAP テーブルの設定内容は、SHOW QOS DSCPMAP コマンド (461 ページ) で確認できます。

```
SHOW QOS DSCPMAP=PREMARKING ↵
SHOW QOS DSCPMAP=PREMARKING DSCP=1 ↵
```

## メータリング

本製品の帯域制御は、ユーザーの設定した最大・最小帯域と許容バーストサイズの値をもとに、各トラフィッククラスが実際にどの程度の帯域を使用しているかを計測することによって実現されます。

帯域使用量の計測 (metering) は、プレマーキングの後、リマーキングの前に行われます。本マニュアルでは、これをメータリングと呼びます。

計測の結果、各トラフィッククラスは次に示す3つの「帯域クラス」に分類されます。リマーケティング時やキューイング時には、帯域クラスごとに異なるレベルのサービスを提供することが可能です。

- ☞ ポリシーベース QoS の処理過程で帯域クラスが割り当てられなかった場合、パケットはデフォルトの帯域クラス1として扱われます。

帯域クラス	帯域使用量	取り扱い方法（一例）
1	少ない	帯域割り当ての優先度は最高
2	中程度	帯域割り当ての優先度は中
3	使いすぎ	帯域割り当ての優先度は最低。輻輳時は優先的に破棄

表 22: 3 つの帯域クラス

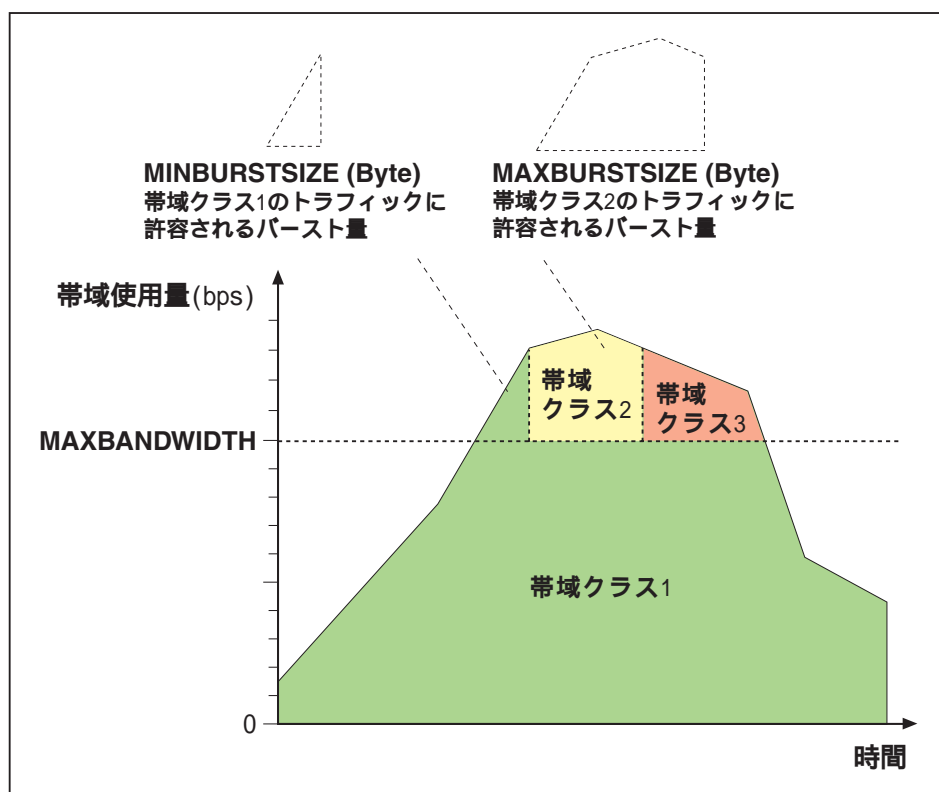
帯域クラスの分類基準は、シングルレート、ツインレートの2つから選択できます。

**シングルレート・メータリング** シングルレートのメータリングでは、1つの帯域しきい値 (MAXBANDWIDTH) と2つのバーストサイズしきい値 (MAXBURSTSIZE、MINBURSTSIZE) あわせて3つの設定値に基づいて、各トラフィッククラスを帯域クラスに分類します。

帯域クラス	帯域使用量	判定基準
1	少ない	バーストサイズ ≤ MINBURSTSIZE
2	中程度	MINBURSTSIZE < バーストサイズ ≤ MAXBURSTSIZE
3	使いすぎ	バーストサイズ > MAXBURSTSIZE

表 23: シングルレート・メータリングの判定基準





ここでのバーストサイズとは、トラフィックの流入量が MAXBANDWIDTH を超えた場合に、MAXBANDWIDTH 超過分としてバッファリングされたデータ量を示しています。トラフィック量が MAXBANDWIDTH 以下であれば、バーストサイズは 0 です。

トラフィックが瞬間的に MAXBANDWIDTH をオーバーしても、超過している時間が短ければ、バーストサイズは MINBURSTSIZE 以内にとどまり、すべてのパケットが帯域クラス 1 として扱われることになります。

これに対し、MAXBANDWIDTH をオーバーしている時間が長くなると、バーストサイズが MINBURSTSIZE を超えることがあります。この場合、MINBURSTSIZE を超えてバッファリングされたパケットには、帯域クラス 2 が割り当てられます。さらに時間が経過すると、バーストサイズが MAXBURSTSIZE を超えますが、この超過分は帯域クラス 3 となります。

シングルレートのメータリングを行うには、CREATE QOS TRAFFICCLASS コマンド (218 ページ) \ SET QOS TRAFFICCLASS コマンド (373 ページ) によるトラフィッククラスの設定で、MAXBANDWIDTH、MAXBURSTSIZE、MINBURSTSIZE の 3 つのパラメーターを指定します。このとき、MINBURSTSIZE < MAXBURSTSIZE となるように注意してください。

- ☞ デフォルトトラフィッククラスに対しても、CREATE QOS POLICY コマンド (212 ページ) \ SET QOS POLICY コマンド (361 ページ) で同様の設定ができます。そのとき、各パラメーター名の前に DTC (デフォルトトラフィッククラスの略) を付けてください (以下同じ)。

トラフィッククラスの設定で IGNOREBWCLASS=YES を指定すると、すでにプレマーキングで帯域クラスが割り当てられていた場合に、これを無視させることができます。この場合、純粋に帯域使用量の計測結果に基づいて新たな帯域クラスを割り当てます。一方、IGNOREBWCLASS=NO (デフォルト) を指定

したときは、プレマーキング時に割り当てられた帯域クラスを、そのままメータリングの結果とします。

トラフィッククラスの設定で DROPBWCLASS3=YES を指定すると、帯域クラス 3 (使いすぎ) に分類されたパケットをキューイング前に破棄することができます。

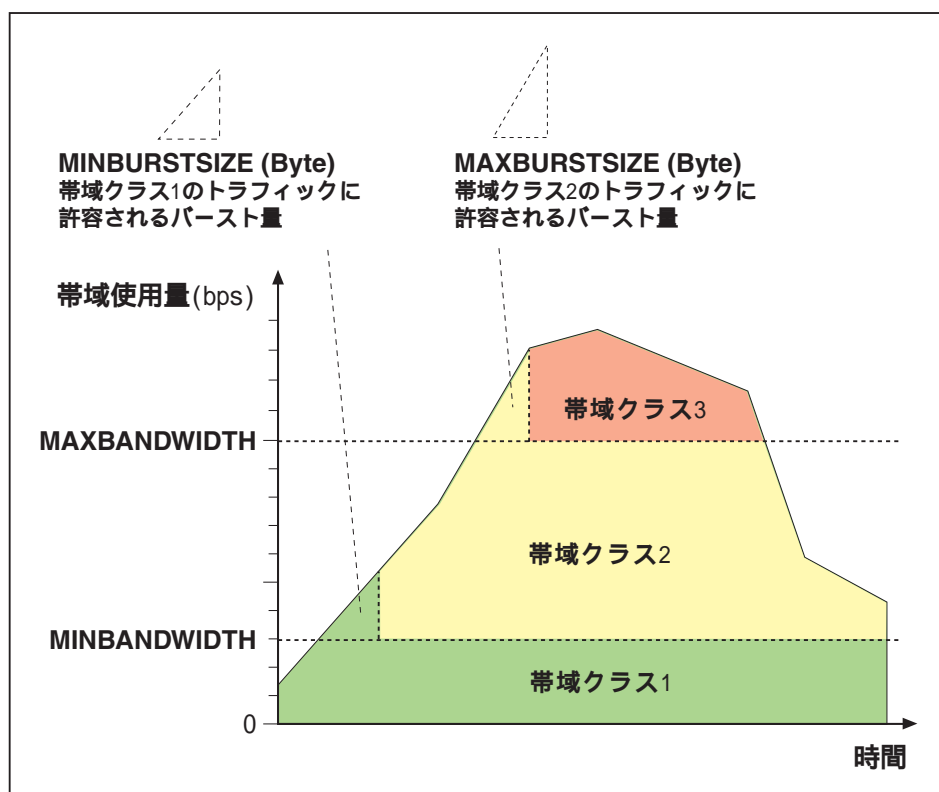
一方、DROPBWCLASS3=NO (デフォルト) の場合は、パケットはただちには破棄されませんが、リマーキングで低い優先度の送信キューを割り当てたり、輻輳発生時に優先的に破棄するような設定が可能です。前者は、トラフィッククラスの設定で REMARKING=USEDSCPMAP を指定し、リマーキング用 DSCPMAP テーブルを適切に設定しておくことで実現できます。

後者は、出力ポートの設定で、帯域クラス 3 を優先的に破棄するような RED カーブセットを適用するか、Tail-drop を使用するよう設定した上で、帯域クラス 3 を優先的に破棄するようデフォルト RED カーブセット 1 を設定することによって実現できます。

ツインレート・メータリング ツインレートのメータリングでは、2 つの帯域しきい値 (MAXBANDWIDTH、MINBANDWIDTH) と 2 つのバーストサイズしきい値 (MAXBURSTSIZE、MINBURSTSIZE) をあわせて 4 つの設定値に基づいて、各トラフィッククラスを帯域クラスに分類します。

帯域クラス	帯域使用量	判定基準
1	少ない	バーストサイズ (MIN) $\leq$ MINBURSTSIZE
2	中程度	バーストサイズ (MIN) $>$ MINBURSTSIZE かつ バーストサイズ (MAX) $\leq$ MAXBURSTSIZE
3	使いすぎ	バーストサイズ (MAX) $>$ MAXBURSTSIZE

表 24: ツインレート・メータリングの判定基準



ここでのバーストサイズ (MIN) とは、トラフィックの流入量が MINBANDWIDTH を超えた場合に、MINBANDWIDTH 超過分としてバッファリングされたデータ量を示しています。トラフィック量が MINBANDWIDTH 以下であれば、バーストサイズ (MIN) は 0 です。

同様に、バーストサイズ (MAX) とは、トラフィックの流入量が MAXBANDWIDTH を超えた場合に、MAXBANDWIDTH 超過分としてバッファリングされたデータ量を示しています。トラフィック量が MAXBANDWIDTH 以下であれば、バーストサイズ (MAX) は 0 です。

トラフィックが瞬間的に MINBANDWIDTH をオーバーしても、超過している時間が短ければ、バーストサイズ (MIN) は MINBURSTSIZE 以内にとどまり、すべてのパケットが帯域クラス 1 として扱われることになります。

これに対し、MINBANDWIDTH をオーバーしている時間が長くなると、バーストサイズ (MIN) が MINBURSTSIZE を超えることがあります。この場合、MINBURSTSIZE を超えてバッファリングされたパケットには、帯域クラス 2 が割り当てられます。

さらにトラフィックが増えると、今度は帯域使用量が MAXBANDWIDTH を超過することがありますが、その時間が長引きバーストサイズ (MAX) が MAXBURSTSIZE を超えると、超過分のパケットには帯域クラス 3 が割り当てられます。

ツインレートのメータリングを行うには、CREATE QOS TRAFFICCLASS コマンド (218 ページ)、SET QOS TRAFFICCLASS コマンド (373 ページ) によるトラフィッククラスの設定で、MAXBANDWIDTH、MAXBURSTSIZE、MINBANDWIDTH、MINBURSTSIZE の 4 つのパラメーターを指定します。

- ☞ デフォルトトラフィッククラスに対しても、CREATE QOS POLICY コマンド (212 ページ)、SET QOS POLICY コマンド (361 ページ) で同様の設定ができます。そのとき、各パラメーター名の前に DTC (デフォルトトラフィッククラスの略) を付けてください (以下同じ)。

トラフィッククラスの設定で IGNOREBWCLASS=YES を指定すると、すでにプレマーキングで帯域クラスが割り当てられていた場合に、これを無視させることができます。この場合、純粋に帯域使用量の計測結果に基づいて新たな帯域クラスを割り当てます。一方、IGNOREBWCLASS=NO（デフォルト）を指定したときは、プレマーキング時に割り当てられた帯域クラスを、そのままメータリングの結果とします。

トラフィッククラスの設定で DROPBWCLASS3=YES を指定することにより、帯域クラス 3（使いすぎ）に分類されたパケットをキューイング前に破棄することができます。

DROPBWCLASS3=NO（デフォルト）の場合は、パケットはただちには破棄されませんが、リマーキングで低い優先度の送信キューを割り当てたり、輻輳発生時に優先的に破棄するような設定が可能です。前者は、トラフィッククラスの設定で REMARKING=USEDSCPMAP を指定し、リマーキング用 DSCPMAP テーブルを適切に設定しておくことで実現できます。

後者は、出力ポートの設定で、帯域クラス 3 を優先的に破棄するような RED カーブセットを適用するか、Tail-drop を使用するよう設定した上で、帯域クラス 3 を優先的に破棄するようデフォルト RED カーブセット 1 を設定することによって実現できます。

### リマーキング

リマーキング（remarking）は、メータリング後にパケットに対して行われる QoS 処理です。

リマーキングでは、メータリングの結果として割り当てられた帯域クラスの値を使用して、最終的な QoS パラメーター（DSCP 値、802.1p ユーザープライオリティー値、帯域クラス、送信キュー）を割り当てることができます。

📎 ここまでの処理過程で帯域クラスが割り当てられなかった場合、パケットはデフォルトの帯域クラス 1 として扱われます。

また、CREATE QOS TRAFFICCLASS コマンド（218 ページ）の DROPBWCLASS3 パラメーターが YES に設定されている場合は、「帯域クラス 3（帯域を使いすぎ）」に該当するパケットを破棄します。

リマーキングを行うには、CREATE QOS TRAFFICCLASS コマンド（218 ページ）、SET QOS TRAFFICCLASS コマンド（373 ページ）の REMARKING パラメーターにリマーキングの方法を指定します。リマーキングの方法には次のものがあります。指定可能なオプション値は 5 つありますが、PRIORITY と PRIO+BWCLASS、BWCLASS と NONE がそれぞれ同じ意味なので、実質的には 3 つになります。

オプション名	参照するテーブル	参照する属性	変更する属性
USEDSCPMAP	DSCPMAP	DSCP, BWCLASS	DSCP, BWCLASS, QUEUE, PRIORITY
PRIORITY	QUEUE2PRIOMAP	BWCLASS, QUEUE	PRIORITY
PRIO+BWCLASS	QUEUE2PRIOMAP	BWCLASS, QUEUE	PRIORITY
BWCLASS	なし	なし	なし
NONE	なし	なし	なし

表 25: REMARKING のオプション

- USEDSCPMAP を指定した場合は、パケットの DSCP 値と帯域クラスの値をインデックスとしてリマーキング用 DSCPMAP テーブルを検索し、DSCP 値、帯域クラス、送信キュー、802.1p ユーザー

プライオリティー値を書き換えます。

- PRIORITY、PRIO+BWCLASS を指定した場合は、帯域クラスの値と送信キューをインデックスとして QUEUE2PRIOMAP テーブルを検索し、802.1p プライオリティー値を書き換えます。
- BWCLASS、NONE（デフォルト）を指定した場合は、書き換えを行いません。

☞ デフォルトトラフィッククラスに対しても、CREATE QOS POLICY コマンド（212 ページ）SET QOS POLICY コマンド（361 ページ）で同様の設定ができます。そのとき、各パラメーター名の前に DTC（デフォルトトラフィッククラスの略）を付けてください（以下同じ）。

☞ IPv6 ルーティングパケットに対する QoS ポリシーでは、REMARKING=USEDSCPMAP を使用できません（パケットの DSCP 値に基づくリマーキングができません）。USEDSCPMAP を指定してもエラーにはなりませんが、リマーキングが行われませんのでご注意ください。

リマーキング用 DSCPMAP テーブルの設定は、SET QOS DSCPMAP コマンド（357 ページ）で行います。たとえば、DSCP 値（MARKVALUE 値）が 10、帯域クラスが 2 のパケットに対して、DSCP 値 10、帯域クラス 2、送信キュー 3、802.1p ユーザープライオリティー 3 を割り当てるには、つぎのようにします。

```
SET QOS DSCPMAP=REMARKING BWCLASS=2 DSCP=10 NEWDSCP=10 NEWBWCLASS=2
NEWQUEUE=3 NEWPRIORITY=3 ↵
```

リマーキング用 DSCPMAP テーブルの設定内容は、SHOW QOS DSCPMAP コマンド（461 ページ）で確認できます。

```
SHOW QOS DSCPMAP=REMARKING ↵
SHOW QOS DSCPMAP=REMARKING DSCP=10 ↵
```

QUEUE2PRIOMAP テーブルの設定は、SET QOS QUEUE2PRIOMAP コマンド（370 ページ）で行います。たとえば、送信キューが 7 で帯域クラスが 2 のパケットに対し、802.1p ユーザープライオリティー 1 を割り当てるには、次のようにします。

```
SET QOS QUEUE2PRIOMAP QUEUE=7 BWCLASS=2 NEWPRIORITY=1 ↵
```

QUEUE2PRIOMAP テーブルの設定内容は、SHOW QOS QUEUE2PRIOMAP コマンド（472 ページ）で確認できます。

```
SHOW QOS QUEUE2PRIOMAP ↵
```

## パケット送信時の QoS 処理

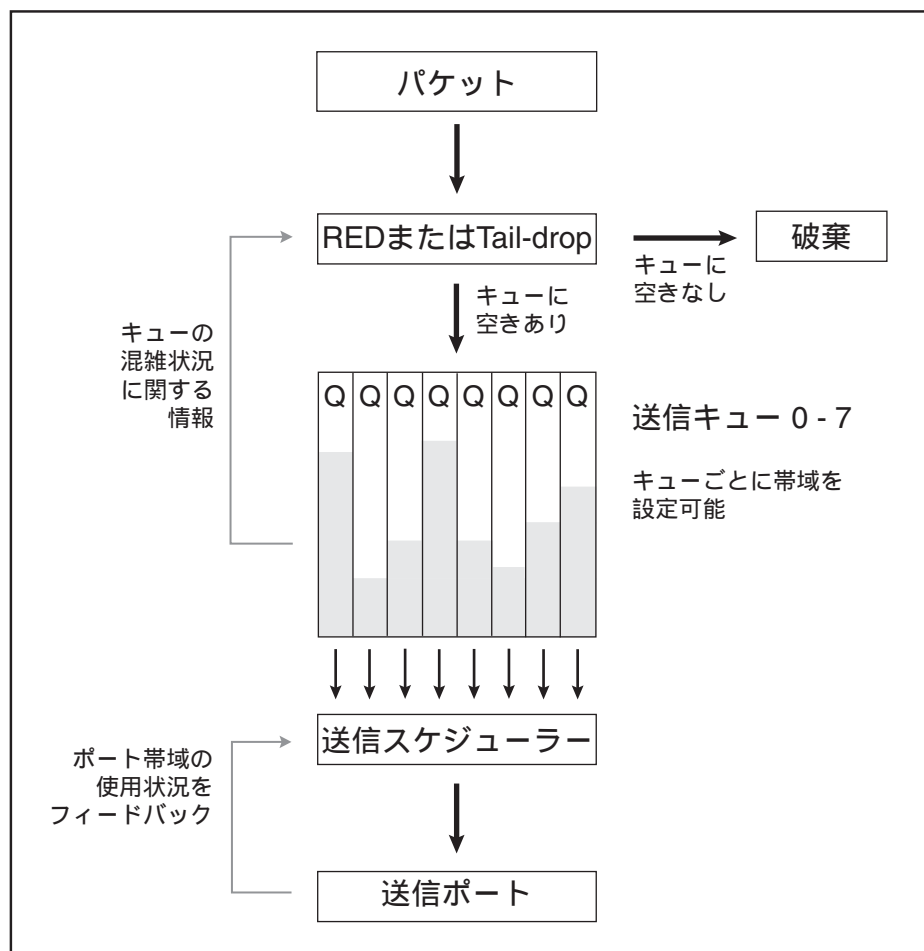
パケット出力時の QoS 処理には、次のものがあります。

- キューへの格納処理（パケットをキューに格納する。輻輳時は RED または Tail-drop アルゴリズム

にしたがってパケットを破棄する)

- キューからの送信処理 (指定されたスケジューリング方式にしたがってパケットをキューから送信する)

次に、キューへの格納処理と送信処理の流れを図示します。



### キューへの格納処理

本製品のスイッチポートはそれぞれ8個の送信キューを持っています。パケットをどのレベルのキューに格納するかは、次のいずれかによって決定されます。

- タグ付きパケットの場合、受信時の 802.1p プライオリティー値に基づきキューが決定されます (SET QOS PRIO2QUEUEMAP コマンド (369 ページ))
- タグなしパケットの場合、受信時にデフォルトキューが割り当てられます (SET QOS PORT コマンド (365 ページ) の DEFAULTQUEUE パラメーター)
- QoS ポリシーを使用している場合、ブリーマーキング時またはリマーキング時にキューを変更できます

送信キューが混雑している場合の動作には次の2つがあります。デフォルトは Tail-drop です。

- キュー長が限界に達した場合、超過分のパケットを破棄する (Tail-drop アルゴリズム)

- キュー長が限界に達する前に、パケットを徐々に破棄してゆく（RED アルゴリズム）

RED アルゴリズム 本製品のスイッチポートはそれぞれ 8 個の送信キューを持っています。通常は、キューがあふれると超過分のパケットを破棄します（Tail-drop アルゴリズム）。

これに対し、RED（Random Early Detection/Discard）は、キュー長が上限に達する前にパケットを徐々に破棄していくことで、キューの枯渇を予防したり、トランスポート層の輻輳回避メカニズムを有効に機能させたりするためのアルゴリズムです。RED を使用すれば、より細やかな帯域制御を実現できます。

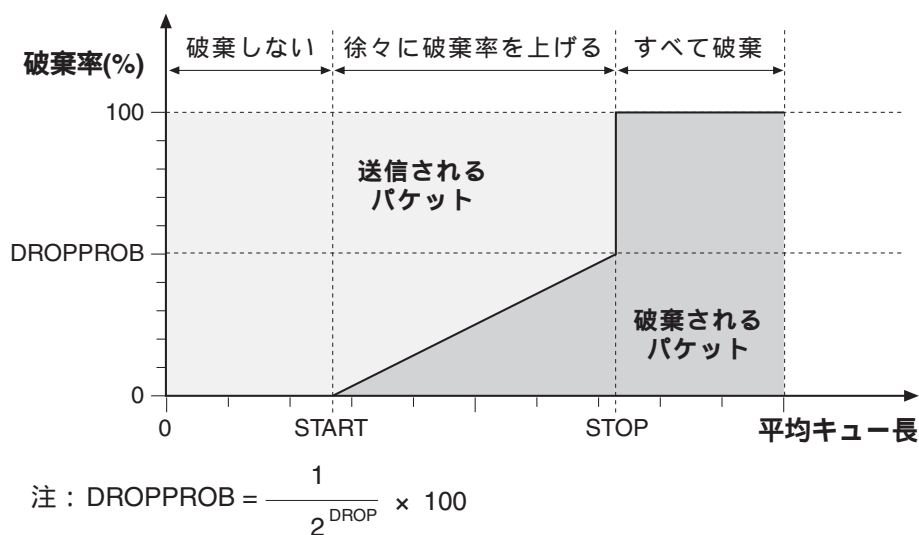
- ☞ RED アルゴリズムは流量制御や輻輳回避の機能を持つ TCP トラフィックに対してもっとも効果を発揮します。UDP のように輻輳制御機能を持たないプロトコルに対しては効果がありませんのでご注意ください。

RED アルゴリズムの設定は、平均キュー長とパケット破棄率の関係を示す「RED カーブ」を定義し、これをスイッチポートに割り当てることによって行います。

RED カーブは以下のパラメーターによって定義します。

- START：パケットを破棄し始めるポイント
- STOP：パケットを完全に破棄するポイント
- DROP：平均キュー長が STOP のときに破棄するパケットの割合（を示す係数）

各パラメーターを図示すると次のようになります。平均キュー長が START から STOP の間にある場合、パケットは 0 から DROPPROB（＝「2 の DROP 乗」分の 1）の間の確率でランダムに破棄されます。パケットの破棄率は平均キュー長が STOP に近づくにつれ高くなっていき、STOP のとき DROPPROB となります。平均キュー長が STOP を超えると、すべてのパケットが破棄されます。平均キュー長が START 以下のときはパケットは破棄されません。



本製品では、8 つの送信キュー × 3 つの帯域クラスのそれぞれに対して RED カーブを個別に設定できます。これら 24 個の RED カーブを束ねたものを「RED カーブセット」と呼びます。実際のところ、スイッチポートに割り当てるのは「RED カーブセット」です。

- ☞ ポリシーベース QoS の処理過程で帯域クラスが割り当てられなかった場合、パケットはデフォルトの帯域クラス 1 として扱われます。



デフォルトでは、1つのREDカーブセット「1」が定義されています。REDカーブセット「1」は変更できますが、削除することはできません。これに加え、3個のREDカーブセット（「2」～「4」）を定義することができます。

REDカーブセットは、CREATE QOS RED コマンド（216 ページ）で作成します。

```
CREATE QOS RED=2 ↓
```

REDカーブセットのパラメーター設定は、SET QOS RED コマンド（371 ページ）で行います。QUEUE パラメーターを省略した場合は、すべての送信キューレベルに同じREDカーブが適用されます。

```
SET QOS RED=2 START1=25 STOP1=35 DROP1=1 START2=15 STOP2=25 DROP2=1
START3=5 STOP3=15 DROP3=1 ↓
```

スイッチポートにREDカーブセットを適用するには、SET QOS PORT コマンド（365 ページ）のREDパラメーターを使います。これにより、該当ポートでパケットをキューイングするとき、REDカーブセット「2」の設定に基づいてREDアルゴリズムが適用されます。

```
SET QOS PORT=1 RED=2 ↓
```

REDアルゴリズムは、輻輳制御機能を持たないUDPのようなプロトコルに対しては効果がありません。こうしたトラフィックに対しては、AVERAGING=0 かつ STARTx、STOPx をほぼ同じ値にしたREDカーブを適用することで、Tail-drop 同様の動作が可能です。

**Tail-drop アルゴリズム** Tail-drop アルゴリズムは、超過分のパケットを廃棄する単純なアルゴリズムです。デフォルトの設定では、すべてのポートでTail-drop が使用されます。

Tail-drop を使用するには、SET QOS PORT コマンド（365 ページ）のREDパラメーターにNONEを指定します。これにより、該当ポートでパケットをキューイングするとき、Tail-drop アルゴリズムが適用されます。

```
SET QOS PORT=1 RED=NONE ↓
```

Tail-drop の動作は、デフォルトREDカーブセット「1」のSTOP1、STOP2、STOP3パラメーターで調整できます。これらはそれぞれ、帯域クラス1、2、3に適用する最大キュー長となります。

```
SET QOS RED=1 STOP1=50 STOP2=30 STOP3=10 ↓
```

- ☞ ポリシーベース QoS の処理過程で帯域クラスが割り当てられなかった場合、パケットはデフォルトの帯域クラス1として扱われます。

## キューからの送信処理



送信キューに格納されたパケットをどのような順序で出力するかは、キューごとに設定されるスケジューリング方式によって決まります。

特に設定を行わないと、送信キューのレベル（優先度）の高いパケットが優先的に送信され、レベルの高いキューのパケット送信が終了するまで次のレベルのキューのパケットは送信されません（STRICT：絶対優先スケジューリング）。

本製品では、高いレベルの送信キューのパケット送信が終了するまで待つことなく、低いレベルのキューのパケット送信を行うように設定することが可能です。

これは、送信キューに重み付けを行い、ラウンドロビンで送信していく方式（WRR：重み付きラウンドロビンスケジューリング）によって実現されます。

- ✎ スイッチポートの帯域制限機能（SET SWITCH PORT コマンド（387 ページ）の EGRESSLIMIT パラメーター）と WRR は併用できません。

設定は、SET QOS PORT EGRESSQUEUE コマンド（367 ページ）で行います。送信方式は SCHEDULER パラメーターで指定します。デフォルトは STRICT（絶対優先）ですので、ここでは WRR1（重み付きラウンドロビン 1）を指定しています。各キューの重み付け値（送信比率）は WRRWEIGHT パラメーターで指定します。

```
SET QOS PORT=ALL EGRESSQUEUE=6-7 SCHEDULER=WRR1 WRRWEIGHT=60 ↓
SET QOS PORT=ALL EGRESSQUEUE=4-5 SCHEDULER=WRR1 WRRWEIGHT=30 ↓
SET QOS PORT=ALL EGRESSQUEUE=2-3 SCHEDULER=WRR1 WRRWEIGHT=12 ↓
SET QOS PORT=ALL EGRESSQUEUE=0-1 SCHEDULER=WRR1 WRRWEIGHT=6 ↓
```

この例では、キュー 7、6、5、4、3、2、1、0 から、60:60:30:30:12:12:6:6、すなわち、10:10:5:5:2:2:1:1 の比率でパケットが順番に送信されます。

本製品では、2 段階のラウンドロビンスケジューリングを行うこともできます。まずは設定例を示します。

```
SET QOS PORT=ALL EGRESSQUEUE=7 SCHEDULER=WRR1 WRRWEIGHT=60 ↓
SET QOS PORT=ALL EGRESSQUEUE=6 SCHEDULER=WRR1 WRRWEIGHT=30 ↓
SET QOS PORT=ALL EGRESSQUEUE=5 SCHEDULER=WRR1 WRRWEIGHT=12 ↓
SET QOS PORT=ALL EGRESSQUEUE=4 SCHEDULER=WRR1 WRRWEIGHT=6 ↓
SET QOS PORT=ALL EGRESSQUEUE=3 SCHEDULER=WRR2 WRRWEIGHT=60 ↓
SET QOS PORT=ALL EGRESSQUEUE=2 SCHEDULER=WRR2 WRRWEIGHT=30 ↓
SET QOS PORT=ALL EGRESSQUEUE=1 SCHEDULER=WRR2 WRRWEIGHT=12 ↓
SET QOS PORT=ALL EGRESSQUEUE=0 SCHEDULER=WRR2 WRRWEIGHT=6 ↓
```

この例では、キュー 4、5、6、7 を WRR1 グループ、キュー 0、1、2、3 を WRR2 グループに所属させています。WRR1 と WRR2 はどちらも重み付きラウンドロビンを実行するスケジューリンググループですが、WRR1 のほうが優先度が高くなっています。

キュー 4、5、6、7 からは、60:30:12:6、つまり、10:5:2:1 の比率でパケットが順番に送信されます。キュー 0、1、2、3 からは、WRR1 グループのキューが空のとき、すなわち、キュー 4、5、6、7 が空のときだけ、

10:5:2:1 の比率でパケットが順番に送信されます。

送信キューのスケジューリング方式、ラウンドロビンの重み付け設定は、SHOW QOS PORT コマンド (468 ページ) で確認できます。各送信キューの「Scheduler」、「WRR Weight」をご覧ください。

```
SHOW QOS PORT=1 ↓
```

```
SHOW QOS PORT=1 EGRESSQUEUE=0-3 ↓
```

## QoS ポリシーのフィルタリング機能

ポリシーベース QoS では、フローグループ、トラフィッククラスの各レベルにおいて、パケットのフィルタリング (破棄、許可など) を行うこともできます。

パケットフィルタリングは、ハードウェアパケットフィルターでもできますが、QoS ポリシーのフィルタリング機能には、ポート単位のフィルタリングが可能という特長があります。

また、本製品には、ハードウェアパケットフィルターにマッチしたパケットに対して、ポリシーベース QoS が適用されないという仕様があるため、ポリシーベース QoS を利用しながらパケットフィルタリングを行いたい場合は、ハードウェアパケットフィルターを併用するのではなく、以下に述べる QoS ポリシーのフィルタリング機能を使ってください。

### 設定方法

QoS ポリシーにおけるフィルタリングの設定は、フローグループ、トラフィッククラスの「アクション」を指定することによって行います。

フローグループのレベルでフィルタリングを行う場合は、CREATE QOS FLOWGROUP コマンド (209 ページ) の ACTION パラメーターを使います。たとえば、フローグループ「2」に分類されたパケットを破棄したい場合は、次のようにします。

```
CREATE QOS FLOWGROUP=2 ACTION=DISCARD ↓
```

トラフィッククラスのレベルでフィルタリングを行う場合は、CREATE QOS TRAFFICCLASS コマンド (218 ページ) の ACTION パラメーターを使います。たとえば、トラフィッククラス「3」に分類されたパケットを破棄したい場合は、次のようにします。

```
CREATE QOS TRAFFICCLASS=3 ACTION=DISCARD ↓
```

- ☞ フローグループとトラフィッククラスの両方にアクション (NONE 以外) が設定されている場合、フローグループのアクションが実行されます。

デフォルトトラフィッククラス (ユーザー定義のトラフィッククラスに分類されないトラフィック) に対するフィルタリングの設定は、CREATE QOS POLICY コマンド (212 ページ) の DTCACTION パラメーターで行います。たとえば、QoS ポリシー「1」のデフォルトトラフィッククラスを破棄するには、次のよ

うにします。

```
CREATE QOS POLICY=1 DTCACTION=DISCARD ↓
```

### 具体例

フィルタリング機能の使用例をいくつか示します。

ポート 1 において、すべての IP マルチキャストパケットを破棄します。

```
CREATE CLASSIFIER=1 IPDADDR=224.0.0.0/3 ↓
CREATE QOS FLOWGROUP=1 ACTION=DISCARD ↓
ADD QOS FLOWGROUP=1 CLASSIFIER=1 ↓
CREATE QOS TRAFFICCLASS=1 ↓
ADD QOS TRAFFICCLASS=1 FLOWGROUP=1 ↓
CREATE QOS POLICY=1 ↓
ADD QOS POLICY=1 TRAFFICCLASS=1 ↓
SET QOS PORT=1 POLICY=1 ↓
```

ポート 1 において、マルチキャストグループ「236.5.8.213」以外のすべての IP マルチキャストパケットを破棄します。

```
CREATE CLASSIFIER=1 IPDADDR=236.5.8.213/32 ↓
CREATE CLASSIFIER=2 IPDADDR=224.0.0.0/3 ↓
CREATE QOS FLOWGROUP=1 ACTION=FORWARD ↓
ADD QOS FLOWGROUP=1 CLASSIFIER=1 ↓
CREATE QOS FLOWGROUP=2 ACTION=DISCARD ↓
ADD QOS FLOWGROUP=2 CLASSIFIER=2 ↓
CREATE QOS TRAFFICCLASS=1 ↓
ADD QOS TRAFFICCLASS=1 FLOWGROUP=1-2 ↓
CREATE QOS POLICY=1 ↓
ADD QOS POLICY=1 TRAFFICCLASS=1 ↓
SET QOS PORT=1 POLICY=1 ↓
```

### 設定例

ここでは、ポリシーベース QoS の設定例を 2 つ紹介します。

ポリシーベース QoS を使用すると、IP アドレスや DSCP、TOS 優先度などの IP ヘッダー情報、TCP や UDP のポート番号などに基づき、パケットに与えるサービスレベルを制御することができます。

最初に必要なのは「ポリシー」を設計することです。どのトラフィックにどの程度の QoS を提供するのかをよく考えてください。

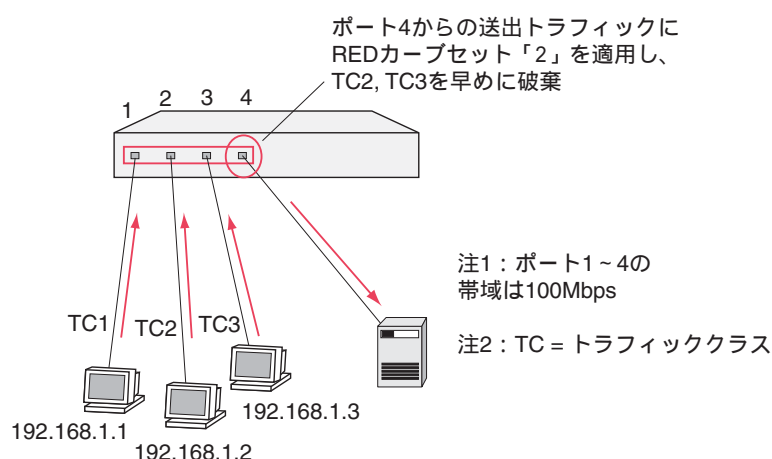
📎 以下の設定例はあくまでも説明のためのサンプルです。

### 最小帯域保証

入力ポートから出力ポートに向けて、出力ポートの帯域以上にパケットが流入すると、出力キューにパケットがたまりはじめます。このとき、出力キューがあふれると、QoS ポリシーで最小帯域を保証するよう設定していても、パケットが破棄されてしまいます。

ここでは、RED アルゴリズムの設定によって、出力キューでのパケット破棄を制御し、特定のトラフィックに対して最小帯域を保証する設定例を示します。

最初に、前提条件として次のような構成を考えます。



ポート1～3にはそれぞれ1台ずつクライアントが接続されており、ポート4のサーバーに向けて大量のトラフィックを送信しているものとします。ポート1～4の帯域はいずれも100Mbpsであると仮定します。この構成では、サーバーへのトラフィックが集中するスイッチポート4で輻輳が発生しがちです。

ここでは、クライアントが接続されているスイッチポート1～3にQoSポリシーを適用し、ポート1のクライアントに80Mbpsの最小帯域を保証するよう設定します。また、プレマーキングを利用して、クライアントごとに異なる送信キューを割り当てます。

さらに、ポート4でREDアルゴリズムを使用するよう設定し、輻輳発生時にポート2、3のクライアントからのトラフィックが優先的に破棄されるようにします。

ここでは、3つのトラフィッククラスを持つQoSポリシーを作成します。

	条件	最小帯域	最大帯域	プレマーキング
1	SrcIP = 192.168.1.1	80Mbps	設定なし	送信キュー 7 を割り当て
2	SrcIP = 192.168.1.2	設定なし	設定なし	送信キュー 4 を割り当て
3	SrcIP = 192.168.1.3	設定なし	設定なし	送信キュー 1 を割り当て

表 26: トラフィッククラスの設定

送信ポートにおける RED カーブセットの設定ポリシーは次のとおりです。この例では、帯域クラスの値を使用しないため、各キューにおいては、すべての帯域クラスに同じ RED カーブを適用します。

キュー番号	START	STOP	DROP ( % )
7	128Kbyte	256Kbyte	15 ( 0.003% )
4	0Kbyte	0.5Kbyte	0 ( 100% )
1	0Kbyte	0.5Kbyte	0 ( 100% )

表 27: RED カーブセットの設定

以下、設定内容を示します。

1. まず、ポリシーベース QoS の設定を行います。最初に QoS ポリシー「1」を作成します。ここでは、デフォルトトラフィッククラスに割り当てる最大帯域を 1Mbps に制限しています。

```
CREATE QOS POLICY=1 DTCMAXBANDWIDTH=1M ↵
```

2. QoS ポリシー「1」を受信スイッチポートである 1～3 に関連付けます。

```
SET QOS PORT=1-3 POLICY=1 ↵
```

3. プレマーキング用の DSCP MAP テーブルを編集し、インデックス (DSCP または MARKVALUE) が 7、4、1 のパケットに対して、送信キュー 7、4、1 を割り当てるような設定を行います。

```
SET QOS DSCP MAP=PREMARKING DSCP=7 NEWQUEUE=7 ↵
```

```
SET QOS DSCP MAP=PREMARKING DSCP=4 NEWQUEUE=4 ↵
```

```
SET QOS DSCP MAP=PREMARKING DSCP=1 NEWQUEUE=1 ↵
```

4. 各クライアントに対応する 3 つのトラフィッククラスを作成します。トラフィッククラス「1」には、80Mbps の帯域を保証します。また、各トラフィッククラスに対して、MARKVALUE パラメーターの値をインデックスとしたプレマーキングを行います。

```
CREATE QOS TRAFFICCLASS=1 MINBANDWIDTH=80M PREMARKING=USEMARKVALUE  
MARKVALUE=7 ↵
```

```
CREATE QOS TRAFFICCLASS=2 PREMARKING=USEMARKVALUE MARKVALUE=4 ↵
```

```
CREATE QOS TRAFFICCLASS=3 PREMARKING=USEMARKVALUE MARKVALUE=1 ↵
```

5. QoS ポリシーにトラフィッククラスを割り当てます。

```
ADD QOS POLICY=1 TRAFFICCLASS=1-3 ↵
```

6. 各トラフィッククラスに対応する3つのフローグループを作成します。

```
CREATE QOS FLOWGROUP=1-3 ↓
```

7. トラフィッククラスにフローグループを割り当てます。

```
ADD QOS TRAFFICCLASS=1 FLOWGROUP=1 ↓
```

```
ADD QOS TRAFFICCLASS=2 FLOWGROUP=2 ↓
```

```
ADD QOS TRAFFICCLASS=3 FLOWGROUP=3 ↓
```

8. 各クライアントからのパケットに対応するクラシファイアを定義します。

```
CREATE CLASSIFIER=1 IPSADDR=192.168.1.1/32 ↓
```

```
CREATE CLASSIFIER=2 IPSADDR=192.168.1.2/32 ↓
```

```
CREATE CLASSIFIER=3 IPSADDR=192.168.1.3/32 ↓
```

9. フローグループにクラシファイアを割り当てます。

```
ADD QOS FLOWGROUP=1 CLASSIFIER=1 ↓
```

```
ADD QOS FLOWGROUP=2 CLASSIFIER=2 ↓
```

```
ADD QOS FLOWGROUP=3 CLASSIFIER=3 ↓
```

10. 次に、パケット送信時のQoS処理について設定を行います。ここでは、QoSポリシーによって送信キュー「7」が割り当てられたトラフィッククラス「1」に優先的に帯域を与えるため、送信キュー「4」「1」では早めにパケットを破棄するようなREDカーブセットを作成します。

```
CREATE QOS RED=2 ↓
```

```
SET QOS RED=2 QUEUE=7 START1=128K STOP1=256K DROP1=15 START2=128K
```

```
STOP2=256K DROP2=15 START3=128K STOP3=256K DROP3=15 ↓
```

```
SET QOS RED=2 QUEUE=4 START1=0K STOP1=0.5K DROP1=0 START2=0K
```

```
STOP2=0.5K DROP2=0 START3=0K STOP3=0.5K DROP3=0 ↓
```

```
SET QOS RED=2 QUEUE=1 START1=0K STOP1=0.5K DROP1=0 START2=0K
```

```
STOP2=0.5K DROP2=0 START3=0K STOP3=0.5K DROP3=0 ↓
```

11. 送信ポートであるスイッチポート4にREDカーブセット「2」を適用します。

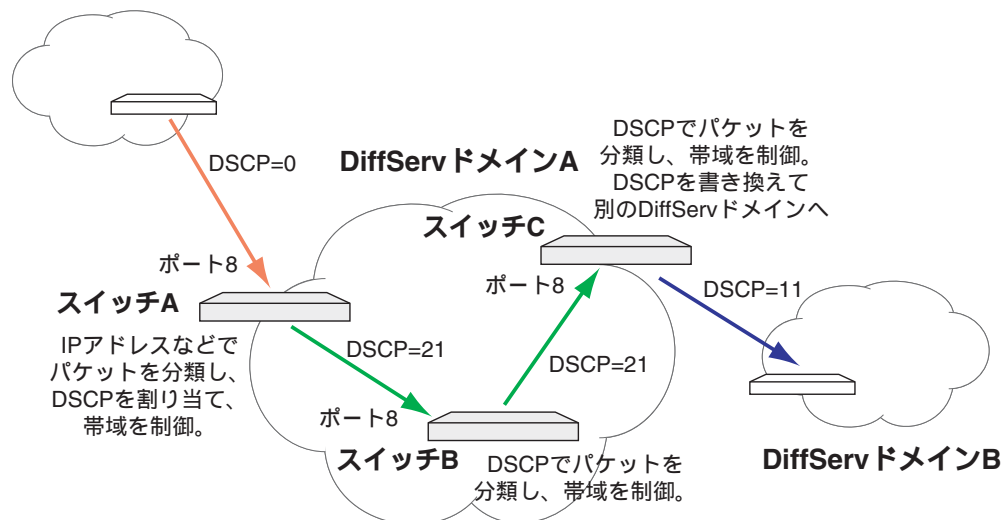
```
SET QOS PORT=4 RED=2 ↓
```

## DiffServ

DiffServ ( Differentiated Service ) は、ネットワーク境界 ( エッジ ) で流入トラフィックをクラス分け・マーキングし、ネットワーク内部ではマーカーだけを見て QoS を適用できるようにする技術です。

DiffServ では、マーキング用に IP ヘッダーの TOS オクテットを再定義しています。従来、TOS オクテットは 3 ビットの優先度フィールドと、3 または 4 ビットの TOS フラグフィールド、および予約済みフィールドで構成されていましたが、DiffServ では先頭 6 ビットを DSCP ( DiffServ Code Point ) として定義しなおしています。DSCP フィールドは 0 ~ 63 の値をとるマーカーフィールドであり、各値の意味は個々のネットワーク主体 ( DiffServ ドメイン ) が独自に定義します。たとえば、DSCP=20 は低遅延・狭帯域、DSCP=21 は中遅延・広帯域などといった定義が可能です。

### 非DiffServドメイン



ここでは、スイッチ A、B、C の DiffServ 設定を示します。

#### スイッチ A の設定

1. QoS ポリシー「1」を作成します。

```
CREATE QOS POLICY=1 ↵
```

2. QoS ポリシー「1」を受信スイッチポートに関連付けます。

```
SET QOS PORT=8 POLICY=1 ↵
```

3. プレマーキング用の DSCPMAP テーブルを編集し、パケットの DSCP フィールドを、インデックス ( DSCP または MARKVALUE ) と同じ値に書き換えるような設定を行います。

```
SET QOS DSCPMAP=PREMARKING DSCP=21 NEWDSCP=21 ↵
SET QOS DSCPMAP=PREMARKING DSCP=22 NEWDSCP=22 ↵
SET QOS DSCPMAP=PREMARKING DSCP=23 NEWDSCP=23 ↵
SET QOS DSCPMAP=PREMARKING DSCP=24 NEWDSCP=24 ↵
SET QOS DSCPMAP=PREMARKING DSCP=25 NEWDSCP=25 ↵
SET QOS DSCPMAP=PREMARKING DSCP=26 NEWDSCP=26 ↵
SET QOS DSCPMAP=PREMARKING DSCP=27 NEWDSCP=27 ↵
SET QOS DSCPMAP=PREMARKING DSCP=28 NEWDSCP=28 ↵
```

☞ プレマーキング用 DSCP テーブルは、デフォルトで上記の設定になっているため、以前に DSCPMAP テーブルの設定を変更していない場合、本手順は不要です。

4. 8 つのトラフィッククラス「1」～「8」を定義し、それぞれに最小帯域を割り当てます。また、各クラスに対し、プレマーキングで DSCP 値「21」～「28」を付加するよう設定します。

```
CREATE QOS TRAFFICCLASS=1 MINBANDWIDTH=20M PREMARKING=USEMARKVALUE
MARKVALUE=21 ↵
CREATE QOS TRAFFICCLASS=2 MINBANDWIDTH=10M PREMARKING=USEMARKVALUE
MARKVALUE=22 ↵
CREATE QOS TRAFFICCLASS=3 MINBANDWIDTH=5M PREMARKING=USEMARKVALUE
MARKVALUE=23 ↵
CREATE QOS TRAFFICCLASS=4 MINBANDWIDTH=3M PREMARKING=USEMARKVALUE
MARKVALUE=24 ↵
CREATE QOS TRAFFICCLASS=5 MINBANDWIDTH=1M PREMARKING=USEMARKVALUE
MARKVALUE=25 ↵
CREATE QOS TRAFFICCLASS=6 MINBANDWIDTH=1M PREMARKING=USEMARKVALUE
MARKVALUE=26 ↵
CREATE QOS TRAFFICCLASS=7 MINBANDWIDTH=1M PREMARKING=USEMARKVALUE
MARKVALUE=27 ↵
CREATE QOS TRAFFICCLASS=8 MINBANDWIDTH=1M PREMARKING=USEMARKVALUE
MARKVALUE=28 ↵
```

5. トラフィッククラス「1」～「8」を QoS ポリシー「1」に割り当てます。

```
ADD QOS POLICY=1 TRAFFICCLASS=1-8 ↵
```

6. トラフィックグループ「1」～「8」と 1 対 1 で対応するフローグループ「1」～「8」を作成します。

```
CREATE QOS FLOWGROUP=1-8 ↵
```

7. トラフィッククラス「1」～「8」にフローグループ「1」～「8」を割り当てます。



```

ADD QOS TRAFFICCLASS=1 FLOWGROUP=1 ↵
ADD QOS TRAFFICCLASS=2 FLOWGROUP=2 ↵
ADD QOS TRAFFICCLASS=3 FLOWGROUP=3 ↵
ADD QOS TRAFFICCLASS=4 FLOWGROUP=4 ↵
ADD QOS TRAFFICCLASS=5 FLOWGROUP=5 ↵
ADD QOS TRAFFICCLASS=6 FLOWGROUP=6 ↵
ADD QOS TRAFFICCLASS=7 FLOWGROUP=7 ↵
ADD QOS TRAFFICCLASS=8 FLOWGROUP=8 ↵

```

#### 8. ヘッダー情報に基づいてパケットを分類するクラシファイアを作成します。

```

CREATE CLASSIFIER=1 TCPSPORT=80 ↵
CREATE CLASSIFIER=2 TCPSPORT=20 ↵
CREATE CLASSIFIER=3 TCPSPORT=25 ↵
CREATE CLASSIFIER=4 IPPROTO=TCP ↵
CREATE CLASSIFIER=5 UDPSPORT=53 ↵
CREATE CLASSIFIER=6 UDPDPORT=53 ↵
CREATE CLASSIFIER=7 IPPROTO=UDP ↵
CREATE CLASSIFIER=8 IPPROTO=ICMP ↵

```

📌 本例はあくまでも説明のためのサンプルです。トラフィッククラスは綿密な計画とテストに基づいて作成してください。

#### 9. フローグループにクラシファイアを割り当てます。

```

ADD QOS FLOWGROUP=1 CLASSIFIER=1 ↵
ADD QOS FLOWGROUP=2 CLASSIFIER=2 ↵
ADD QOS FLOWGROUP=3 CLASSIFIER=3 ↵
ADD QOS FLOWGROUP=4 CLASSIFIER=4 ↵
ADD QOS FLOWGROUP=5 CLASSIFIER=5 ↵
ADD QOS FLOWGROUP=6 CLASSIFIER=6 ↵
ADD QOS FLOWGROUP=7 CLASSIFIER=7 ↵
ADD QOS FLOWGROUP=8 CLASSIFIER=8 ↵

```

### スイッチ B の設定

#### 1. QoS ポリシー「1」を作成します。

```
CREATE QOS POLICY=1 ↵
```

#### 2. QoS ポリシー「1」を受信スイッチポートに関連付けます。

```
SET QOS PORT=8 POLICY=1 ↵
```

3. DSCP 値「21」～「28」に対応する 8 つのトラフィッククラスを定義し、それぞれに最小帯域を割り当てます。

```
CREATE QOS TRAFFICCLASS=1 MINBANDWIDTH=20M ↵
CREATE QOS TRAFFICCLASS=2 MINBANDWIDTH=10M ↵
CREATE QOS TRAFFICCLASS=3 MINBANDWIDTH=5M ↵
CREATE QOS TRAFFICCLASS=4 MINBANDWIDTH=3M ↵
CREATE QOS TRAFFICCLASS=5 MINBANDWIDTH=1M ↵
CREATE QOS TRAFFICCLASS=6 MINBANDWIDTH=1M ↵
CREATE QOS TRAFFICCLASS=7 MINBANDWIDTH=1M ↵
CREATE QOS TRAFFICCLASS=8 MINBANDWIDTH=1M ↵
```

4. トラフィッククラス「1」～「8」を QoS ポリシー「1」に割り当てます。

```
ADD QOS POLICY=1 TRAFFICCLASS=1-8 ↵
```

5. トラフィックグループ「1」～「8」と 1 対 1 で対応するフローグループ「1」～「8」を作成します。

```
CREATE QOS FLOWGROUP=1-8 ↵
```

6. トラフィッククラス「1」～「8」にフローグループ「1」～「8」を割り当てます。

```
ADD QOS TRAFFICCLASS=1 FLOWGROUP=1 ↵
ADD QOS TRAFFICCLASS=2 FLOWGROUP=2 ↵
ADD QOS TRAFFICCLASS=3 FLOWGROUP=3 ↵
ADD QOS TRAFFICCLASS=4 FLOWGROUP=4 ↵
ADD QOS TRAFFICCLASS=5 FLOWGROUP=5 ↵
ADD QOS TRAFFICCLASS=6 FLOWGROUP=6 ↵
ADD QOS TRAFFICCLASS=7 FLOWGROUP=7 ↵
ADD QOS TRAFFICCLASS=8 FLOWGROUP=8 ↵
```

7. IP ヘッダーの DSCP 値によってパケットを分類するクラシファイアを作成します。

```

CREATE CLASSIFIER=1 IPDSCP=21 ↵
CREATE CLASSIFIER=2 IPDSCP=22 ↵
CREATE CLASSIFIER=3 IPDSCP=23 ↵
CREATE CLASSIFIER=4 IPDSCP=24 ↵
CREATE CLASSIFIER=5 IPDSCP=25 ↵
CREATE CLASSIFIER=6 IPDSCP=26 ↵
CREATE CLASSIFIER=7 IPDSCP=27 ↵
CREATE CLASSIFIER=8 IPDSCP=28 ↵

```

#### 8. フローグループにクラシファイアを割り当てます。

```

ADD QOS FLOWGROUP=1 CLASSIFIER=1 ↵
ADD QOS FLOWGROUP=2 CLASSIFIER=2 ↵
ADD QOS FLOWGROUP=3 CLASSIFIER=3 ↵
ADD QOS FLOWGROUP=4 CLASSIFIER=4 ↵
ADD QOS FLOWGROUP=5 CLASSIFIER=5 ↵
ADD QOS FLOWGROUP=6 CLASSIFIER=6 ↵
ADD QOS FLOWGROUP=7 CLASSIFIER=7 ↵
ADD QOS FLOWGROUP=8 CLASSIFIER=8 ↵

```

### スイッチ C の設定

#### 1. QoS ポリシー「1」を作成します。

```
CREATE QOS POLICY=1 ↵
```

#### 2. QoS ポリシー「1」を受信スイッチポートに関連付けます。

```
SET QOS PORT=8 POLICY=1 ↵
```

#### 3. プレマーキング用の DSCPMAP テーブルを編集し、パケットの DSCP フィールドを、インデックス (DSCP または MARKVALUE) と同じ値に書き換えるような設定を行います。

```
SET QOS DSCPMAP=PREMARKING DSCP=11 NEWDSCP=11 ↵
SET QOS DSCPMAP=PREMARKING DSCP=12 NEWDSCP=12 ↵
SET QOS DSCPMAP=PREMARKING DSCP=13 NEWDSCP=13 ↵
SET QOS DSCPMAP=PREMARKING DSCP=14 NEWDSCP=14 ↵
SET QOS DSCPMAP=PREMARKING DSCP=15 NEWDSCP=15 ↵
SET QOS DSCPMAP=PREMARKING DSCP=16 NEWDSCP=16 ↵
SET QOS DSCPMAP=PREMARKING DSCP=17 NEWDSCP=17 ↵
SET QOS DSCPMAP=PREMARKING DSCP=18 NEWDSCP=18 ↵
```

☞ プレマーキング用 DSCP テーブルは、デフォルトで上記の設定になっているため、以前に DSCPMAP テーブルの設定を変更していない場合、本手順は不要です。

4. DSCP 値「21」～「28」に対応する 8 つのトラフィッククラスを定義し、それぞれに最小帯域を割り当てます。また、各クラスに対し、DSCP 値を「11」～「18」に書き換えるよう設定します。

```
CREATE QOS TRAFFICCLASS=1 MINBANDWIDTH=20M PREMARKING=USEMARKVALUE
MARKVALUE=11 ↵
CREATE QOS TRAFFICCLASS=2 MINBANDWIDTH=10M PREMARKING=USEMARKVALUE
MARKVALUE=12 ↵
CREATE QOS TRAFFICCLASS=3 MINBANDWIDTH=5M PREMARKING=USEMARKVALUE
MARKVALUE=13 ↵
CREATE QOS TRAFFICCLASS=4 MINBANDWIDTH=3M PREMARKING=USEMARKVALUE
MARKVALUE=14 ↵
CREATE QOS TRAFFICCLASS=5 MINBANDWIDTH=1M PREMARKING=USEMARKVALUE
MARKVALUE=15 ↵
CREATE QOS TRAFFICCLASS=6 MINBANDWIDTH=1M PREMARKING=USEMARKVALUE
MARKVALUE=16 ↵
CREATE QOS TRAFFICCLASS=7 MINBANDWIDTH=1M PREMARKING=USEMARKVALUE
MARKVALUE=17 ↵
CREATE QOS TRAFFICCLASS=8 MINBANDWIDTH=1M PREMARKING=USEMARKVALUE
MARKVALUE=18 ↵
```

5. トラフィッククラス「1」～「8」を QoS ポリシー「1」に割り当てます。

```
ADD QOS POLICY=1 TRAFFICCLASS=1-8 ↵
```

6. トラフィックグループ「1」～「8」と 1 対 1 で対応するフローグループ「1」～「8」を作成します。

```
CREATE QOS FLOWGROUP=1-8 ↵
```

7. トラフィッククラス「1」～「8」にフローグループ「1」～「8」を割り当てます。

```

ADD QOS TRAFFICCLASS=1 FLOWGROUP=1 ↵
ADD QOS TRAFFICCLASS=2 FLOWGROUP=2 ↵
ADD QOS TRAFFICCLASS=3 FLOWGROUP=3 ↵
ADD QOS TRAFFICCLASS=4 FLOWGROUP=4 ↵
ADD QOS TRAFFICCLASS=5 FLOWGROUP=5 ↵
ADD QOS TRAFFICCLASS=6 FLOWGROUP=6 ↵
ADD QOS TRAFFICCLASS=7 FLOWGROUP=7 ↵
ADD QOS TRAFFICCLASS=8 FLOWGROUP=8 ↵

```

#### 8. IP ヘッダーの DSCP 値によってパケットを分類するクラシファイアを作成します。

```

CREATE CLASSIFIER=1 IPDSCP=21 ↵
CREATE CLASSIFIER=2 IPDSCP=22 ↵
CREATE CLASSIFIER=3 IPDSCP=23 ↵
CREATE CLASSIFIER=4 IPDSCP=24 ↵
CREATE CLASSIFIER=5 IPDSCP=25 ↵
CREATE CLASSIFIER=6 IPDSCP=26 ↵
CREATE CLASSIFIER=7 IPDSCP=27 ↵
CREATE CLASSIFIER=8 IPDSCP=28 ↵

```

#### 9. フローグループにクラシファイアを割り当てます。

```

ADD QOS FLOWGROUP=1 CLASSIFIER=1 ↵
ADD QOS FLOWGROUP=2 CLASSIFIER=2 ↵
ADD QOS FLOWGROUP=3 CLASSIFIER=3 ↵
ADD QOS FLOWGROUP=4 CLASSIFIER=4 ↵
ADD QOS FLOWGROUP=5 CLASSIFIER=5 ↵
ADD QOS FLOWGROUP=6 CLASSIFIER=6 ↵
ADD QOS FLOWGROUP=7 CLASSIFIER=7 ↵
ADD QOS FLOWGROUP=8 CLASSIFIER=8 ↵

```

## QoS ポリシーのルール領域消費量

SET QOS PORT コマンド (365 ページ)、または、SET QOS ACCELERATOR POLICY コマンド (355 ページ) で QoS ポリシーをスイッチポートや IPv6 アクセラレーターボードに割り当てると、システム内部の「ルールテーブル」内にあるルール領域が消費されます (ルールテーブルの使用状況は、SHOW SWITCH コマンド (490 ページ) で確認できます)。

詳しくは「スイッチング」の「クラシファイア」をご覧ください (「クラシファイアとルール領域消費量」を参照)。

## ハードウェアパケットフィルター

ハードウェアパケットフィルターは、ハードウェア（ASIC）レベルでパケットをフィルタリング（許可・拒否）する機能です。

- ④ ハードウェアパケットフィルターにマッチしたパケットに対して、ポリシーベース QoS は適用されません（ここでの「マッチ」とは、破棄（Discard）だけでなく明示的な転送許可（Forward）も含まれます）。ポリシーベース QoS を利用しながらパケットフィルタリングを行いたい場合は、ハードウェアパケットフィルターを併用するのではなく、QoS ポリシーのフィルタリング機能（フローグループ、トラフィッククラスのアクション）を使ってください。
- ④ IPv6 アクセラレーターボードを装着している場合、IPv6 ルーティングパケットのフィルタリングには、IPv6 ハードウェアパケットフィルターを使用します。ハードウェアパケットフィルターと IPv6 ハードウェアパケットフィルターは併用可能です。詳しくは「スイッチング」の「IPv6 ハードウェアパケットフィルター」をご覧ください。

ハードウェアパケットフィルターの処理は、スイッチチップの L2 入力部で行われます。そのため、ルーティングされないトラフィック（同一 VLAN 内のトラフィック）に対してもフィルタリングが可能です。たとえば、IP モジュールを有効にしていない状態、すなわち本製品をレイヤー 2 スwitchとして使用している場合でも IP のフィルタリングができます。

パケットのフィルタリング条件には、以下の各項目を使用できます。フィルタリング条件は、汎用のパケットフィルターであるクラシファイアによって定義します。クラシファイアの詳細については「スイッチング」の「クラシファイア」をご覧ください。

- 入力 VLAN
- Ethernet のフレームフォーマット、プロトコルタイプ、送信元・宛先 MAC アドレス
- レイヤー 2 アドレス種別（ユニキャストとそれ以外）
- IP ヘッダーの TOS 優先度（precedence）、DSCP（DiffServ Code Point）、プロトコル、始点・終点 IP アドレス
- TCP ヘッダーの始点・終点ポート
- UDP ヘッダーの始点・終点ポート

条件に一致したパケットに対しては、以下の処理（アクション）が可能です。アクションは最初に一致したフィルターで適用されます。どのフィルターにも一致しなかったパケットは通常通り処理（転送）されます。

- 転送（Forward）
  - 破棄（Discard）
- ④ ハードウェアパケットフィルターの L3 以上の条件パラメーター（L2 は使用可）とダブルタグ VLAN（Nested VLAN）は併用できません。

## 基本動作

ハードウェアパケットフィルターの基本動作について説明します。

## フィルターの構成

ハードウェアパケットフィルターは、複数のフィルターで構成される 1 つのリストです。個々のフィルターは、クラシファイア（汎用パケットフィルター）とアクションから構成されます。

## フィルター処理の流れ

ハードウェアパケットフィルターの処理は、おおむね次の手順にしたがって行われます。

- ✎ 以下の説明は、設定上の便宜を最優先して書いたものであり、実際の内部動作を正確に記述したものではありません。あらかじめご了承ください。
- 1. フィルターが 1 つでも定義されている場合、受信パケットとフィルターに関連付けられているクラシファイアの条件を、フィルター番号の小さい順に照合します。
- 2. 一致するフィルターが見つかった場合は、その場でアクション（破棄か転送）を実行し、ハードウェアパケットフィルターの処理を完了します。
- 3. 一致するフィルターがなかった場合はハードウェアパケットフィルターの処理を完了し、通常どおりパケットを出力します。
- ✎ ハードウェアパケットフィルターは、スイッチ本体から送信されるパケットには適用されません。

## 設定手順

ハードウェアパケットフィルターの設定は、次の流れで行います。

1. クラシファイアの作成（CREATE CLASSIFIER コマンド（198 ページ））
2. フィルターの追加（ADD SWITCH HWFILTER コマンド（188 ページ））

以下、各手順について詳しく解説します。

ここでは例として、ホスト 192.168.100.38 からサーバー 192.168.10.5 宛てのパケットを遮断するよう設定します。

1. クラシファイアを作成します（CREATE CLASSIFIER コマンド（198 ページ））

```
CREATE CLASSIFIER=1 IPSADDR=192.168.100.38/32
IPDADDR=192.168.10.5/32 ↵
```

- ✎ ハードウェアパケットフィルターで使用するクラシファイアは、CREATE CLASSIFIER コマンド（198 ページ）のページに掲載されている「ハードウェアパケットフィルター・QoS ポリシー用の構文」にしたがっている必要があります。同構文にないパラメーターを含むクラシファイアを使おうとすると、ADD SWITCH HWFILTER コマンド（188 ページ）実行時にエラーとなります。
- 2. フィルターを作成（リストに追加）します（ADD SWITCH HWFILTER コマンド（188 ページ））。フィルターを作成するには、フィルター番号に加え、クラシファイア番号とマッチ時のアクション（転送か破棄）を指定する必要があります。

```
ADD SWITCH HWFILTER=1 CLASSIFIER=1 ACTION=DISCARD ↵
```

- 📎 フィルター番号は省略することもできます。その場合、新規フィルターはリストの最後尾に追加されます。既存フィルターと同じ番号を指定した場合は、既存フィルターの位置に新規フィルターが挿入され、既存フィルター以降は番号が1つずつ後ろにずれます。

- 📎 ハードウェアパケットフィルターは、すべてのポートで受信したパケットに適用されます。

- 📎 ハードウェアパケットフィルターは、スイッチ本体から送信されるパケットには適用されません。

基本設定は以上です。

## コマンド例

次に具体的なコマンド例を示します。

192.168.10.100 から 192.168.20.0/24 への IP パケットを破棄。

```
CREATE CLASSIFIER=1 IPSADDR=192.168.10.100/32 IPDADDR=192.168.20.0/24 ↵
ADD SWITCH HWFILTER=1 CLASSIFIER=1 ACTION=DISCARD ↵
```

10.0.0.0/8 からの ICMP パケットを破棄。

```
CREATE CLASSIFIER=1 IPSADDR=10.0.0.0/8 IPPROTOCOL=ICMP ↵
ADD SWITCH HWFILTER=1 CLASSIFIER=1 ACTION=DISCARD ↵
```

192.168.30.100 への telnet パケットを破棄。

```
CREATE CLASSIFIER=1 IPDADDR=192.168.30.100/32 TCPDPORT=23 ↵
ADD SWITCH HWFILTER=1 CLASSIFIER=1 ACTION=DISCARD ↵
```

192.168.10.0/24 から 192.168.20.0/24 への TCP 接続（セッション開始）を禁止する。この例では、192.168.20.0/24 から 192.168.10.0/24 への Syn + Ack パケットを破棄することでこれを実現しています。

```
CREATE CLASSIFIER=1 IPSADDR=192.168.20.0/24 IPDADDR=192.168.10.0/24
TCPFLAGS=SYN,ACK ↵
ADD SWITCH HWFILTER=1 CLASSIFIER=1 ACTION=DISCARD ↵
```

- 📎 TCPFLAGS パラメーターでは、指定したフラグだけがチェック対象となります（指定しなかったフラグの状態には関知しません）。指定したフラグがすべてが立っていればマッチ、それ以外の場合は非マッチと判定されます。



ハードウェアパケットフィルターは、ルーティングされない同一サブネット内のトラフィックに対しても有効です。そのため、「192.168.10.0/24 から他のサブネットへの IP 通信を拒否」するつもりで次のような設定を行うと、192.168.10.0/24 内でも IP 通信ができなくなってしまいます。

```
CREATE CLASSIFIER=1 IPSADDR=192.168.10.0/24 ↵
ADD SWITCH HWFILTER=1 CLASSIFIER=1 ACTION=DISCARD ↵
```

このような場合は、次の例のように「始点 IP アドレスと終点 IP アドレスが同一サブネットなら許可」というルールを追加してください。

```
CREATE CLASSIFIER=1 IPSADDR=192.168.10.0/24 IPDADDR=192.168.10.0/24 ↵
CREATE CLASSIFIER=2 IPSADDR=192.168.10.0/24 IPDADDR=ANY ↵
ADD SWITCH HWFILTER=1 CLASSIFIER=1 ACTION=FORWARD ↵
ADD SWITCH HWFILTER=2 CLASSIFIER=2 ACTION=DISCARD ↵
```

- 🔗 ハードウェアパケットフィルターでは、最初にマッチしたフィルターのアクションが実行されます。デフォルト拒否の設定を行うには、最初に許可するフィルターを並べた上で、最後にすべてを破棄するフィルターを設定します。また、デフォルト許可に設定する場合は、拒否するフィルターだけを並べていきます。ハードウェアパケットフィルター自体は、デフォルト許可です。

ハードウェアパケットフィルターを使用するために、必ずしも IP モジュールを有効にする必要はありません。純粋なレイヤー 2 スイッチとして本製品を使用する場合であっても、ハードウェアパケットフィルターを使えば、IP アドレスやプロトコルに応じたフィルタリングが可能です。

ハードウェアパケットフィルターの一覧を表示するには、SHOW SWITCH HWFILTER コマンド (507 ページ) を使います。

```
SHOW SWITCH HWFILTER ↵
SHOW SWITCH HWFILTER=1 ↵
```

クラシファイアの一覧を表示するには、SHOW CLASSIFIER コマンド (395 ページ) を実行します。CLASSIFIER パラメーターに番号を指定すれば、該当するクラシファイアの詳細なパラメーターが表示されます。

```
SHOW CLASSIFIER ↵
SHOW CLASSIFIER=1-3 ↵
SHOW CLASSIFIER=ALL ↵
```

ハードウェアパケットフィルターのフィルター番号は可変です。ADD SWITCH HWFILTER コマンド (188 ページ) でフィルターを追加するとき、既存のフィルターと同じ番号を指定した場合は、既存フィルターの位置に新規フィルターが挿入され、既存フィルター以降は番号が 1 つずつ後ろにずれます。

ハードウェアパケットフィルターを削除するには、DELETE SWITCH HWFILTER コマンド (237 ページ) にフィルター番号を指定します。フィルター番号は可変なので、必ず SHOW SWITCH HWFILTER コマンド (507 ページ) で確認してから指定してください。フィルターを削除すると、削除によって空いた番号を埋める形で後続のフィルター番号が自動的に変更されるので注意してください。

```
DELETE SWITCH HWFILTER=1 ↵
```

```
DELETE SWITCH HWFILTER=1-3 ↵
```

- ☞ ハードウェアパケットフィルターを削除しても、クラシファイアは削除されません。ハードウェアパケットフィルターとクラシファイアの関連付けが削除されるだけです。クラシファイアを削除するには、DESTROY CLASSIFIER コマンド (243 ページ) を使います。

## ハードウェアパケットフィルターのルール領域消費量

ADD SWITCH HWFILTER コマンド (188 ページ) でハードウェアパケットフィルターを作成すると、システム内部の「ルールテーブル」内にあるルール領域が消費されます (ルールテーブルの使用状況は、SHOW SWITCH コマンド (490 ページ) で確認できます)。

ルール領域の消費量は、基本的にフィルターの数 (クラシファイアの数) に応じて増加します。ただし、ハードウェアパケットフィルターとポリシーベース QoS を併用する場合は、QoS ポリシーを割り当てているポートの数に応じて、ルール領域の使用量が急増しますので、ご注意ください。

詳しくは「スイッチング」の「クラシファイア」をご覧ください (「クラシファイアとルール領域消費量」を参照)。

## IPv6 ハードウェアパケットフィルター

IPv6 ハードウェアパケットフィルターは、IPv6 アクセラレーターボードの L3 処理部において、IPv6 パケットをフィルタリング（許可・拒否・DSCP/802.1p 書き換え）する機能です。

✎ トンネリング IPv6 パケット（IPv6 over IPv4 および 6to4）をフィルタリングすることはできません。

IPv6 ハードウェアパケットフィルターは、本体スイッチチップの L2 入力処理部で適用されるハードウェアパケットフィルターとは独立した機能であり、併用が可能です。

IPv6 ハードウェアパケットフィルターには以下の特長があります。

- ルーティングされる IPv6 パケットにだけ適用される（スイッチングされる IPv6 パケットをフィルタリングするには、通常のハードウェアパケットフィルターを使う）
- L3、L4 ヘッダーに基づくフィルタリング（L2 ヘッダーは見ない）
- パケットの許可・拒否に加え、DSCP、802.1p の書き換えも可能（ポリシーベース QoS の分類基準として利用できる）

IPv6 パケットのフィルタリング条件には、以下の各項目を使用できます。フィルタリング条件は、汎用のパケットフィルターであるクラシファイアによって定義します。クラシファイアの詳細については「スイッチング」の「クラシファイア」をご覧ください。

- IPv6 ヘッダーの DSCP（DiffServ Code Point）、プロトコル、始点・終点 IP アドレス
- TCP ヘッダーの始点・終点ポート
- UDP ヘッダーの始点・終点ポート

条件に一致したパケットに対しては、以下の処理（アクション）が可能です。アクションは最初に一致したエントリーで適用されます。どのエントリーにも一致しなかったパケットは通常通り処理（転送）されます。

- 転送（Forward）
- 破棄（Discard）
- DSCP/802.1p 書き換え（Mark）

## 基本動作

IPv6 ハードウェアパケットフィルターの基本動作について説明します。

### フィルターの構成

IPv6 ハードウェアパケットフィルターは、複数のフィルターで構成される 1 つのリストです。個々のフィルターは、クラシファイア（汎用パケットフィルター）とアクションから構成されます。

### フィルター処理の流れ

IPv6 ハードウェアパケットフィルターの処理は、おおむね次の手順にしたがって行われます。

- ✎ 以下の説明は、設定上の便宜を最優先して書いたものであり、実際の内部動作を正確に記述したものではありません。あらかじめご了承ください。
  - 1. IPv6 ハードウェアパケットフィルターが1つでも定義されている場合、ルーティング対象のIPv6 パケットとフィルターエントリーを、フィルター番号の小さい順に照合します。
  - 2. 一致するエントリーが見つかった場合は、その場でアクション（破棄、転送、DSCP/802.1p 書き換え）を実行し、フィルターの処理を完了します。
  - 3. 一致するエントリーがなかった場合はフィルター処理を完了し、通常どおりパケットを出力します。
- ✎ IPv6 ハードウェアパケットフィルターは、スイッチ本体から送信されるパケットには適用されません。

## 設定手順

IPv6 ハードウェアパケットフィルターの設定は、次の流れで行います。

1. クラシファイアの作成（CREATE CLASSIFIER コマンド（198 ページ））
2. フィルターエントリーの追加（ADD SWITCH ACCELERATOR HWFILTER コマンド（184 ページ））

以下、各手順について詳しく解説します。

ここでは例として、ホスト 3ffe:b80:3c:10::1a からサーバー 3ffe:b80:3c:20::2 宛てのパケットを遮断するように設定します。

1. クラシファイアを作成します（CREATE CLASSIFIER コマンド（198 ページ））

```
CREATE CLASSIFIER=1 ETHFORMAT=ETHII-TAGGED PROTOCOL=IPv6
IPSADDR=3ffe:b80:3c:10::1a/128 IPDADDR=3ffe:b80:3c:20::2/128 ↵
```

- ✎ IPv6 ハードウェアパケットフィルターで使用するクラシファイアは、CREATE CLASSIFIER コマンド（198 ページ）のページに掲載されている「IPv6 ハードウェアパケットフィルター用の構文」にしたがっている必要があります。同構文にないパラメーターを含むクラシファイアを使おうとすると、ADD SWITCH ACCELERATOR HWFILTER コマンド（184 ページ）実行時にエラーとなります。

2. フィルターを作成（リストに追加）します（ADD SWITCH ACCELERATOR HWFILTER コマンド（184 ページ））。フィルターを作成するには、フィルター番号に加え、クラシファイア番号とマッチ時のアクション（転送、破棄、DSCP/802.1p 書き換え）を指定する必要があります。

```
ADD SWITCH ACCELERATOR HWFILTER=1 CLASSIFIER=1 ACTION=DISCARD ↵
```

- ✎ 既存フィルターと同じ番号を指定した場合は、既存フィルターの位置に新規フィルターが挿入され、既存フィルター以降は番号が1つずつ後ろにずれます。
- ✎ IPv6 ハードウェアパケットフィルターは、ルーティングされるすべてのIPv6 パケットに適用されます。ただし、トンネリングIPv6 パケット（IPv6 over IPv4 および 6to4）は対象外です。

✎ IPv6 ハードウェアパケットフィルターは、スイッチ本体から送信されるパケットには適用されません。

基本設定は以上です。

## コマンド例

次に具体的なコマンド例を示します。

3ffe:b80:3c:10::100 から 3ffe:b80:3c:20::/64 への IPv6 ルーティングパケットを破棄。

```
CREATE CLASSIFIER=1 ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6
  IPSADDR=3ffe:b80:3c:10::100/128 IPDADDR=3ffe:b80:3c:20::/64 ↵
ADD SWITCH ACCELERATOR HWFILTER=1 CLASSIFIER=1 ACTION=DISCARD ↵
```

3ffe:b80:3c:10::/64 からの ICMP パケットを破棄。

```
CREATE CLASSIFIER=1 ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6
  IPSADDR=3ffe:b80:3c:10::/64 IPPROTOCOL=ICMP ↵
ADD SWITCH ACCELERATOR HWFILTER=1 CLASSIFIER=1 ACTION=DISCARD ↵
```

3ffe:b80:3c:30::100 への telnet パケットを破棄。

```
CREATE CLASSIFIER=1 ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6
  IPDADDR=3ffe:b80:3c:30::100/128 TCPDPORT=23 ↵
ADD SWITCH ACCELERATOR HWFILTER=1 CLASSIFIER=1 ACTION=DISCARD ↵
```

ポリシーベース QoS でパケットを分類するため、3ffe:b80:3c:1ff::/64 からの UDP パケットの DSCP 値を 10 に書き換える。

```
CREATE CLASSIFIER=1 ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6
  IPDADDR=3ffe:b80:3c:1ff::/64 IPPROTOCOL=UDP ↵
ADD SWITCH ACCELERATOR HWFILTER=1 CLASSIFIER=1 ACTION=MARK NEWIPDSCP=10 ↵
```

IPv6 ハードウェアパケットフィルターを使用するためには、必ず IPv6 モジュールを有効にする必要があります。IPv6 ハードウェアパケットフィルターは、ルーティングされる IPv6 パケットだけが対象だからです。レイヤー 2 スイッチングされる IPv6 パケット（同一 VLAN 内の IPv6 通信など）をフィルタリングするには、通常のハードウェアパケットフィルターを使ってください。ただしこの場合は、IPv6 アドレスなどの L3 パラメーターを条件に使うことはできません。

IPv6 ハードウェアパケットフィルターの一覧を表示するには、SHOW SWITCH ACCELERATOR HWFILTER コマンド（499 ページ）を使います。

```
SHOW SWITCH ACCELERATOR HWFILTER ↓
SHOW SWITCH ACCELERATOR HWFILTER=1 ↓
```

クラシファイアの一覧を表示するには、SHOW CLASSIFIER コマンド (395 ページ) を実行します。CLASSIFIER パラメーターに番号を指定すれば、該当するクラシファイアの詳細なパラメーターが表示されます。

```
SHOW CLASSIFIER ↓
SHOW CLASSIFIER=1-3 ↓
SHOW CLASSIFIER=ALL ↓
```

IPv6 ハードウェアパケットフィルターのフィルター番号は可変です。ADD SWITCH ACCELERATOR HWFILTER コマンド (184 ページ) でフィルターを追加するとき、既存のフィルターと同じ番号を指定した場合は、既存フィルターの位置に新規フィルターが挿入され、既存フィルター以降は番号が1つずつ後ろにずれます。

IPv6 ハードウェアパケットフィルターを削除するには、DELETE SWITCH ACCELERATOR HWFILTER コマンド (235 ページ) にフィルター番号を指定します。フィルター番号は可変なので、必ず SHOW SWITCH ACCELERATOR HWFILTER コマンド (499 ページ) で確認してから指定してください。フィルターを削除すると、削除によって空いた番号を埋める形で後続のフィルター番号が自動的に変更されるので注意してください。

```
DELETE SWITCH ACCELERATOR HWFILTER=1 ↓
DELETE SWITCH ACCELERATOR HWFILTER=ALL ↓
```

- 🔗 IPv6 ハードウェアパケットフィルターを削除しても、クラシファイアは削除されません。IPv6 ハードウェアパケットフィルターとクラシファイアの関連付けが削除されるだけです。クラシファイアを削除するには、DESTROY CLASSIFIER コマンド (243 ページ) を使います。

## IPv6 ハードウェアパケットフィルターのルール領域消費量

IPv6 ハードウェアパケットフィルターは、通常のハードウェアパケットフィルターなどと異なり、システム内部のルール領域を使用しません。ルール領域の空き容量とは関係なく、最大 999 個のフィルターを作成することができます。

なお、ルール領域については、「スイッチング」の「クラシファイア」をご覧ください（「クラシファイアとルール領域消費量」を参照）。

## ポート認証

本製品は、スイッチポート単位で LAN 上のユーザーや機器を認証するポート認証機能を実装しています。ポートに接続された機器（および機器を使用するユーザー。以下同様）の認証方法としては、大きく分けて次の 2 種類をサポートしています。

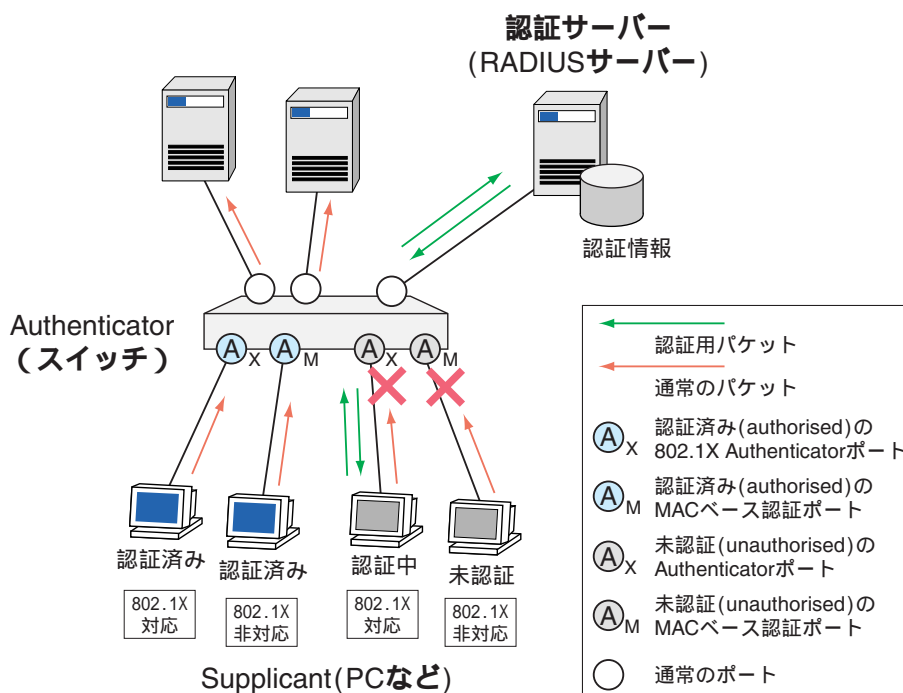
- IEEE 802.1X 認証（以下、802.1X 認証）
- MAC アドレスベース認証（以下、MAC ベース認証）

802.1X 認証は、EAP ( Extensible Authentication Protocol ) というプロトコルを使って、ユーザー単位で認証を行うしくみです。802.1X 認証を利用するには、認証する側と認証される側の両方が 802.1X に対応している必要があります。

一方、MAC ベース認証は、機器の MAC アドレスに基づいて機器単位で認証を行うしくみです。認証される側に特殊な機能を必要としないため、802.1X 認証の環境に 802.1X 非対応の機器（例：ネットワークプリンター）を接続したい場合などに利用できます。おもに、802.1X 認証を補完するものとして利用されます。802.1X および MAC ベースのポート認証機能を使用すれば、スイッチポートに接続された機器を認証し、認証に成功したときだけ同機器からの通信、および、同機器への通信を許可するよう設定できます。また、認証に成功した機器を特定の VLAN にアサインすることも可能です（ダイナミック VLAN）。さらに、本製品は Supplicant 機能にも対応しているため、他の機器から認証を受けるよう設定することもできます。

## 概要

ポート認証のシステムは、通常下記の3要素から成り立っています。





- Authenticator ( 認証者 ): ポートに接続してきた Supplicant ( クライアント ) を認証する機器またはソフトウェア。802.1X 認証では EAP メッセージの交換によって Supplicant を認証する ( ユーザー認証 )。また、MAC ベース認証では Supplicant の MAC アドレスによって認証を行う ( 機器認証 )。認証に成功した場合はポート経由の通信を許可、失敗した場合はポート経由の通信を拒否する。認証処理そのものは、認証サーバー ( RADIUS サーバー ) に依頼する ( Supplicant の情報を認証サーバーに中継して、認証結果 ( 成功・失敗 ) を受け取る )。
- 認証サーバー ( RADIUS サーバー ): Authenticator の要求に応じて、Supplicant を認証する機器またはソフトウェア。ユーザー名、パスワード、MAC アドレス、所属 VLAN などの認証情報を一元管理している。Authenticator との間の認証情報の受け渡しには RADIUS プロトコルを用いる。
- Supplicant ( クライアント ): ポートへの接続時に Authenticator から認証を受ける機器またはソフトウェア。802.1X の認証を受けるためには、802.1X Supplicant の機能を備えている必要がある。802.1X Supplicant 機能は、一部の OS に標準装備されているほか、単体のクライアントソフトウェアとして用意されていることもある。一方、MAC ベースの認証を受けるために特殊な機能は必要ない。

本製品の各スイッチポートは、上記のうち、Authenticator と Supplicant になることができます ( Authenticator であると同時に Supplicant でもあるような設定も可能 )。認証サーバー ( RADIUS サーバー ) は別途用意する必要があります。

## 802.1X 認証方式

802.1X 認証では、EAP-MD5、EAP-TLS、EAP-TTLS、EAP-PEAP など様々な認証方式が使用されています。このうち、本製品の 802.1X 認証モジュールが現在サポートしている EAP 認証方式は以下のとおりです。

- Authenticator 時 : EAP-MD5、EAP-TLS、EAP-TTLS、EAP-PEAP、EAP-OTP(MD4/MD5)
- Supplicant 時 : EAP-MD5、EAP-OTP(MD4/MD5)

## 基本設定

本製品を使ってポート認証のシステムを運用するための基本的な設定例を示します。以下の例では、メインの認証方式として 802.1X 認証を使用し、これを補うために MAC ベース認証を併用します。

### Authenticator

本製品を Authenticator として使用する場合の基本設定を示します。Authenticator としての動作には、IP の設定と RADIUS サーバーの指定が必須です。

ここでは、すべてのポートが VLAN default に所属していることを前提に、ポート 1 ~ 16 で 802.1X 認証を、ポート 17 ~ 23 で MAC ベース認証を行うものとします。また、RADIUS サーバーはポート 24 ( 通常のポート ) に接続されているものとします。

1. 802.1X では RADIUS サーバーを使って認証を行うため、最初に RADIUS サーバーと通信するための設定をします。IP モジュールを有効にし、VLAN default に IP アドレスを設定します。



```
ENABLE IP ↵
```

```
ADD IP INT=vlan-default IP=192.168.10.5 MASK=255.255.255.0 ↵
```

☞ ここでは RADIUS サーバーが VLAN default 上にあるものと仮定しています。他の VLAN 上にあるときは、RADIUS サーバーまでの経路を適切に設定してください。

2. RADIUS サーバーの IP アドレスと UDP ポート、共有パスワードを指定します。

```
ADD RADIUS SERVER=192.168.10.130 PORT=1812 ACCPORT=1813
SECRET=himitsu ↵
```

3. 802.1X 認証機能を有効にします。

```
ENABLE PORTAUTH=8021X ↵
```

4. ポート 1～16 で 802.1X 認証を行うよう設定します。「TYPE=AUTHENTICATOR」の指定により、ポート 1～16 は Authenticator ポートとなります。

```
ENABLE PORTAUTH=8021X PORT=1-16 TYPE=AUTHENTICATOR ↵
```

5. MAC ベース認証機能を有効にします。

```
ENABLE PORTAUTH=MACBASED ↵
```

6. ポート 17～23 で MAC ベース認証を行うよう設定します。

```
ENABLE PORTAUTH=MACBASED PORT=17-23 ↵
```

☞ 802.1X 認証の Authenticator ポートと MAC ベース認証ポートでは、ポートランキング、スパニングツリープロトコル、ポートセキュリティ、VRRP を使用できません。また、802.1X 認証の Authenticator ポートと MAC ベース認証ポートをタグ付きに設定することはできません。

☞ RADIUS サーバーを接続するポートは、Authenticator ポートにしないでください。Authenticator ポートにする場合は、ENABLE PORTAUTH PORT コマンド (291 ページ) / SET PORTAUTH PORT コマンド (346 ページ) の CONTROL パラメーターを AUTHORISED に設定してください。

## Authenticator (ダイナミック VLAN)

ダイナミック VLAN (Dynamic VLAN Assignemnt) は、RADIUS サーバーから受け取った認証情報に基づいてポートの所属 VLAN を動的に変更する機能です。802.1X 認証、MAC ベース認証のどちらでも利

用可能です。

以下、本製品を Authenticator として使用し、さらにダイナミック VLAN 機能を利用する場合の基本設定を示します。Authenticator としての動作には、IP の設定と RADIUS サーバーの指定が必須です。

ここでは、利用者機器のために 3 つの VLAN 「A」、「B」、「C」を用意します。また、RADIUS サーバーを接続するための VLAN 「R」も作成します。各ポートに接続された機器は、認証成功後、RADIUS サーバー側から返された VLAN (「A」、「B」、「C」のどれか) に自動的にアサインされます。

ここでは、ポート 1～16 で 802.1X 認証を、ポート 17～23 で MAC ベース認証を行うものとします。また、RADIUS サーバーは、VLAN 「R」所属のポート 24 (通常のポート) に接続されているものとします。

#### 1. VLAN を作成します。


```
CREATE VLAN=A VID=10 ↵
CREATE VLAN=B VID=20 ↵
CREATE VLAN=C VID=30 ↵
CREATE VLAN=R VID=1000 ↵
```

#### 2. RADIUS サーバーを接続するポート 24 を VLAN 「R」に割り当てます。

```
ADD VLAN=R PORT=24 ↵
```

#### 3. 802.1X では RADIUS サーバーを使って認証を行うため、最初に RADIUS サーバーと通信するための設定をします。IP モジュールを有効にし、VLAN 「R」に IP アドレスを設定します。

```
ENABLE IP ↵
ADD IP INT=vlan-R IP=192.168.10.5 MASK=255.255.255.0 ↵
```

 ここでは RADIUS サーバーが VLAN 「R」上にあるものと仮定しています。他の VLAN 上にあるときは、RADIUS サーバーまでの経路を適切に設定してください。

#### 4. RADIUS サーバーの IP アドレスと UDP ポート、共有パスワードを指定します。

```
ADD RADIUS SERVER=192.168.10.130 PORT=1812 ACCPORT=1813
SECRET=himitsu ↵
```

#### 5. 802.1X 認証機能を有効にします。

```
ENABLE PORTAUTH=8021X ↵
```

#### 6. ポート 1～16 で 802.1X 認証を行うよう設定します。「TYPE=AUTHENTICATOR」の指定により、ポート 1～16 は Authenticator ポートとなります。また、「VLANASSIGNMENT=ENABLED」の指定により、ダイナミック VLAN を有効にします。

```
ENABLE PORTAUTH=8021X PORT=1-16 TYPE=AUTHENTICATOR
VLANASSIGNMENT=ENABLED ↵
```

7. MAC ベース認証機能を有効にします。

```
ENABLE PORTAUTH=MACBASED ↵
```

8. ポート 17～23 で MAC ベース認証を行うよう設定します。また、「VLANASSIGNMENT=ENABLED」の指定により、ダイナミック VLAN を有効にします。

```
ENABLE PORTAUTH=MACBASED PORT=17-23 VLANASSIGNMENT=ENABLED ↵
```

✎ 802.1X 認証の Authenticator ポートと MAC ベース認証ポートでは、ポートランキング、スパンニングツリープロトコル、ポートセキュリティを使用できません。また、802.1X 認証の Authenticator ポートと MAC ベース認証ポートをタグ付きに設定することはできません。

✎ RADIUS サーバーを接続するポートは、Authenticator ポートにしないでください。Authenticator ポートにする場合は、ENABLE PORTAUTH PORT コマンド (291 ページ) / SET PORTAUTH PORT コマンド (346 ページ) の CONTROL パラメーターを AUTHORISED に設定してください。

ダイナミック VLAN の動作仕様は次のとおりです。

- Supplicant の認証に失敗した場合、ポートは本来の VLAN ( ADD VLAN PORT コマンド (191 ページ) で指定した VLAN ) の所属となります。ポート越えの通信は不可能です。
- RADIUS サーバーから有効な VLAN の情報が返ってきた場合、ポートはその VLAN の所属となります。認証に成功すれば、ポート越えの通信も可能です。
- RADIUS サーバーから無効な VLAN の情報が返ってきた場合、ポートは本来の VLAN 所属となります。また、認証も失敗となるため、ポート越えの通信は不可能です。
- RADIUS サーバーから VLAN の情報が返ってこなかった場合、ポートは本来の VLAN 所属となります。認証に成功すれば、ポート越えの通信も可能です。
- 該当ポートまたはシステム全体でポート認証が無効に設定された場合、ポートは本来の VLAN 所属となります。ポート認証が無効なので、ポート越えの通信に関する制限はありません。
- 未認証のポート、および、CONTROL=UNAUTHORISED (未認証固定) または CONTROL=AUTHORISED (認証済み固定) に設定されたポートは、本来の VLAN 所属となります。

ポートがダイナミック VLAN にアサインされているときは、ADD VLAN PORT コマンド (191 ページ) で該当ポートの所属 VLAN を変更しても、設定変更は直ちには反映されません。ポートがダイナミック VLAN から本来の VLAN に戻るのは、次のときです。

- 認証済みの Supplicant がなくなったとき。
- リンクがダウンしたとき。
- ポート上でポート認証が無効にされたとき ( DISABLE PORTAUTH PORT コマンド (264 ページ) )。

- システム上でポート認証が無効にされたとき (DISABLE PORTAUTH コマンド (262 ページ))。

## Supplicant

本製品を 802.1X Supplicant として使用する場合の基本設定を示します。ここでは、ポート 1 が認証を受けるものとします。Supplicant としての動作においては、IP の設定は必須ではありません。

1. 802.1X 認証モジュールを有効にします。

```
ENABLE PORTAUTH=8021X ↵
```

2. ポート 1 で認証を受けるよう設定します。認証を受けるためのユーザー名とパスワードを指定してください。「TYPE=SUPPLICANT」の指定により、ポート 1 は Supplicant ポートとなります。

```
ENABLE PORTAUTH=8021X PORT=1 TYPE=SUPPLICANT USERNAME=atswitch
PASSWORD=atpasswd ↵
```

- ✎ 802.1X 認証の Supplicant ポートでは、ポートランキング、スパニングツリープロトコル、ポートセキュリティを使用できません。

## 認証サーバー

ポート認証機能を利用するために必要な認証サーバー (RADIUS サーバー) の設定項目について簡単に説明します。

- ✎ 認証サーバーの詳細な設定方法については、ご使用のサーバー製品のマニュアルをご参照ください。
- 802.1X 認証において、ダイナミック VLAN を使用しないときは、ユーザーごとに下記の属性を定義してください。

属性名	属性値	備考
User-Name	ユーザー名	認証対象のユーザー名 (例: "user1", "userB")
User-Password	パスワード	(EAP-MD5、EAP-PEAP、EAP-TTLS 使用時) ユーザー名に対応するパスワード (例: "dbf8a9hve", "h1mi2uDa4o") EAP-TLS 使用時は不要 (別途、ユーザー電子証明書の用意が必要)

表 28: 802.1X 認証 (ダイナミック VLAN なし)

- ✎ 認証方式として EAP-TLS を使う場合は、RADIUS サーバーの電子証明書と各ユーザーの電子証明書を用意し、各コンピューター上に適切にインストールしておく必要があります。また、認証方式として EAP-PEAP、EAP-TTLS を使う場合は、RADIUS サーバーの電子証明書を用意し、各コンピューター上に適切にインストールしておく必要があります。詳細は RADIUS サーバーおよび Supplicant (OS や専用ソフトウェアなど) のマニュアルをご参照ください。

- MAC ベース認証において、ダイナミック VLAN を使用しないときは、機器ごとに下記の属性を定義してください。

属性名	属性値	備考
User-Name	MAC アドレス	認証対象機器の MAC アドレス（例：“00-00-f4-11-22-33”）、 a～f は小文字で指定
User-Password	MAC アドレス	認証対象機器の MAC アドレス。User-Name と同じ値を指定すること

表 29: MAC ベース認証（ダイナミック VLAN なし）

- また、802.1X 認証、MAC ベース認証でダイナミック VLAN を使用するときは、前述の諸属性に加え、下記の 3 属性を追加設定してください。

属性名	属性値	備考
Tunnel-Type	VLAN (13)	固定値。指定方法はサーバーに依存
Tunnel-Medium-Type	IEEE-802 (6)	固定値。指定方法はサーバーに依存
Tunnel-Private-Group-ID	VLAN 名 か VLAN ID	認証対象のユーザーや機器が認証をパスした後に所属させる VLAN の名前か VLAN ID（例：“sales”, 10）

表 30: ダイナミック VLAN 用の属性

## DHCP Snooping

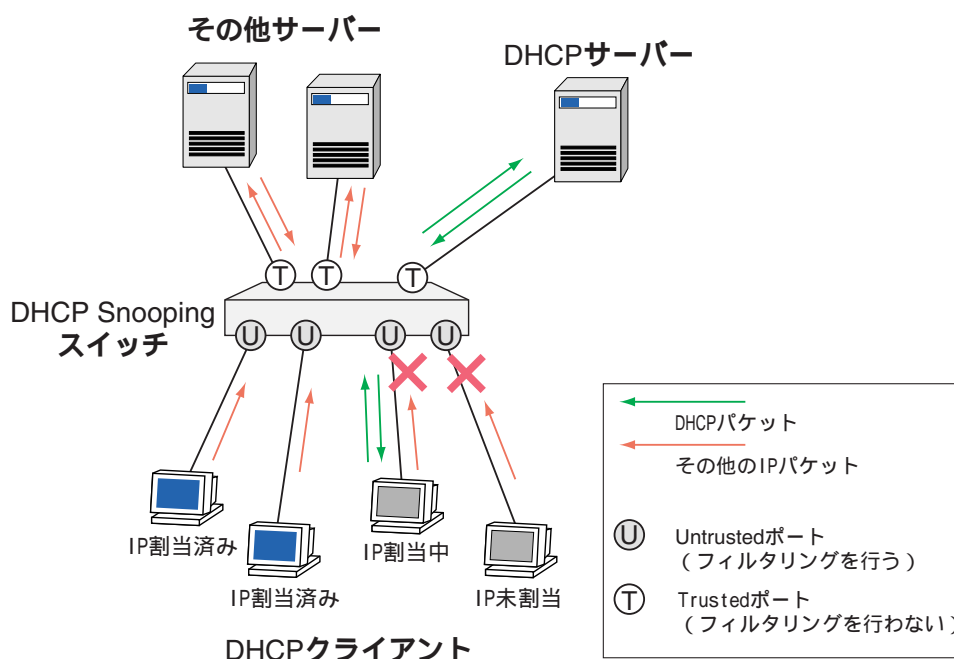
DHCP Snooping は、DHCP サーバー・クライアント間でやりとりされる DHCP メッセージを監視して動的な IP ソースフィルタリングを行う機能です。本機能を利用すれば、DHCP サーバーを用いたネットワーク環境において、正当な DHCP クライアントにだけ IP 通信を許可することができます。

- ✎ 本機能はレイヤー 2 の機能であるため、IP の設定などをしていなくても使用できます。
- ✎ DHCP クライアント機能と DHCP Snooping は併用できません。
- ✎ DHCP サーバー機能と DHCP Snooping は併用できません。

### 概要

DHCP Snooping では、DHCP メッセージのやりとりを監視して DHCP クライアントがどのポート配下に存在するかを追跡し、その情報に基づいて IP パケットのフィルタリングを行います。

DHCP Snooping を利用する場合は、次の図のように本製品を DHCP サーバーと DHCP クライアントの間に配置します。このとき、本製品が DHCP/BOOTP リレーエージェントとして動作していてもかまいません。



DHCP Snooping では、スイッチポートを次の 2 つに分類・設定します。デフォルトではすべてのポートが Untrusted ポートとして設定されています。

- Trusted ポート：DHCP Snooping によるフィルタリングが無効なポート。Trusted ポートでは、パケットに対して特別な処理を行わず、すべてのパケットを通過させます。ネットワーク機器やサーバーのように常時接続で信頼のおける装置を接続するポートは通常 Trusted ポートに設定します。DHCP サーバーを接続するポートも Trusted ポートに設定してください。
- Untrusted ポート：DHCP Snooping によるフィルタリングが有効なポート。Untrusted ポートでは、DHCP サーバーから IP アドレスの割り当てを受けたクライアントからの IP パケットだけを通過させ、その他の IP パケットは破棄します（DHCP のクライアントパケットを除く）。クライアント PC のように不特定多数の必ずしも信頼のおけない装置を接続するポートは Untrusted ポートに設定します（デフォルトではすべてのポートが Untrusted になります）。

DHCP Snooping を有効にすると、本製品は DHCP サーバー・クライアント間で交換される DHCP メッセージを監視するようになります。

Untrusted ポートに接続されているクライアントが DHCP サーバーから IP アドレスの割り当てを受けると、本製品はクライアントの IP アドレスや MAC アドレス、ポート番号などを DHCP Snooping テーブル（バインディングデータベース）に登録します。

Untrusted ポートでは、バインディングデータベースに登録されているクライアントからの IP パケットだけを許可し、その他の IP パケットは破棄します。これにより、不正に接続されたクライアントがポートを越えてネットワークにアクセスすることを防ぐことができます。

- ☞ デフォルト設定では、Untrusted ポートには DHCP クライアントを 1 台しか接続できません。クライアントを複数接続した場合、最初に IP アドレスを割り当てられたクライアントだけが通信できます。

一方、Trusted ポートでは特別な処理を行いません。Trusted ポートで受信したパケットは（他のフィルタリング機能によって破棄されないかぎり）通常どおり転送されます。

### 登録できるクライアントの数

DHCP Snooping 機能で登録できるクライアントの数は次のとおりです。

本製品では、1 ポートあたり最大 100 クライアント、システム全体では最大 520 クライアントまで登録できます。

なお、本機能はハードウェアパケットフィルタと記憶領域を共有しているため、本機能の使用によってハードウェアパケットフィルタの設定可能数が増減します。設定可能なフィルタの数は、システムテーブルの空き容量に依存します。システムテーブルの空き容量は SHOW SWITCH コマンド（490 ページ）で確認できます。

### 基本設定

DHCP Snooping を使用するための基本的な設定手順は次のとおりです。

ここでは、ポート 1 に DHCP サーバーが接続されており、ポート 2～24 には不特定多数の DHCP クライアントが接続されるものと仮定します。

1. DHCP Snooping を有効にします。



```
ENABLE DHCP Snooping ↓
```

2. DHCP サーバーが接続されているポートを Trusted ポートに設定します。

```
SET DHCP Snooping PORT=1 TRUSTED=YES ↓
```

3. 正当なクライアントにだけ IP 通信を許可するため、次のクラシファイアを作成します。

```
CREATE CLASSIFIER=1 MACSADDR=DHCP Snooping PROTOCOL=IP
  IPSADDR=DHCP Snooping ↓
CREATE CLASSIFIER=9999 PROTOCOL=IP ↓
```

- クラシファイア「1」は、送信元 MAC アドレスと始点 IP アドレスの両方がバインディングデータベースに登録されている IP パケットにマッチします。
  - クラシファイア「9999」はすべての IP パケットにマッチします。
4. DHCP クライアントが接続されているポート 2～24 にパケットフィルタリングのための QoS ポリシー「1」を割り当て、前項で作成したクラシファイアを関連付けます。

```
CREATE QoS POLICY=1 ↓
SET QoS PORT=2-24 POLICY=1 ↓
CREATE QoS TRAFFICCLASS=1 ↓
CREATE QoS TRAFFICCLASS=2 ↓
CREATE QoS FLOWGROUP=1 ACTION=FORWARD ↓
CREATE QoS FLOWGROUP=2 ACTION=DISCARD ↓
ADD QoS POLICY=1 TRAFFICCLASS=1,2 ↓
ADD QoS FLOWGROUP=1 CLASSIFIER=1 ↓
ADD QoS FLOWGROUP=2 CLASSIFIER=9999 ↓
ADD QoS TRAFFICCLASS=1 FLOWGROUP=1 ↓
ADD QoS TRAFFICCLASS=2 FLOWGROUP=2 ↓
```

基本設定は以上です。

デフォルトではすべてのポートが Untrusted ポートに設定されているため、手順 2 で Trusted ポートに設定した DHCP サーバーの接続ポートを除き、他のすべてのポートで IP パケット（DHCP のクライアントパケットを除く）が破棄されます。

Untrusted ポートにおいて、DHCP クライアントが DHCP サーバーから IP アドレスを割り当てられたことを検知すると（DHCPACK をクライアントに転送すると）、手順 3～4 で設定した QoS ポリシー/クラシファイアの働きにより、そのポートでは該当クライアントからの IP パケットを通過させるようになります。

ネットワーク機器やサーバーなど、DHCP Snooping の対象外にしたい装置を接続しているポートは、Trusted ポートに設定します。Trusted ポートでは DHCP Snooping によるフィルタリングが行われず、原則的にすべての受信パケットが転送されます。



- ④ DHCP サーバーを接続するポートは Trusted ポートに設定してください。

ポート種別の設定は、SET DHCP Snooping PORT コマンド (330 ページ) の TRUSTED パラメーターで行います。たとえば、DHCP サーバーがポート 1 に接続されている場合は、次のようにして該当ポートを Trusted ポートに設定します。

```
SET DHCP Snooping PORT=1 TRUSTED=YES ↓
```

デフォルト設定では、Untrusted ポートには DHCP クライアントを 1 台しか接続できません。クライアントを複数接続した場合、最初に IP アドレスを割り当てられたクライアントだけが通信できます。複数のクライアントを接続したい場合は、SET DHCP Snooping PORT コマンド (330 ページ) の MAXLEASES パラメーターで接続台数を 1~100 の範囲で指定します。

```
SET DHCP Snooping PORT=1 MAXLEASES=5 ↓
```

IP アドレスを固定設定している装置 (DHCP クライアント機能を無効化している装置や DHCP クライアント機能を持たない装置など) を Untrusted ポートで利用したい場合は、バインディングデータベースにクライアント情報をスタティック登録します。

クライアントの登録は ADD DHCP Snooping BINDING コマンド (173 ページ) で行います。登録には、IP アドレス、MAC アドレス (省略可)、所属 VLAN、接続ポートの情報がが必要です。

```
ADD DHCP Snooping BINDING=00-00-00-00-00-01 INTERFACE=vlan-default
IP=192.168.10.5 PORT=5 ↓
```

- ④ MAC アドレスは省略できますが、MAC アドレス無指定のスタティックエントリーを追加する場合は、DHCP Snooping のオプション機能である ARP セキュリティーを有効化しないでください (デフォルトは無効。有効時は DISABLE DHCP Snooping ARPSECURITY コマンド (254 ページ) で無効化できます)。また、クラシファイアの設定も変更が必要です (次項をご覧ください)。
- ④ デフォルト設定では、ポートあたり 1 つしかスタティックエントリーを登録できません。1 つのポートに複数のスタティックエントリーを登録したいときは、SET DHCP Snooping PORT コマンド (330 ページ) の MAXLEASES パラメーターの値を増やす必要があります。

MAC アドレス無指定のスタティックエントリーを使用する場合は、「基本設定」のクラシファイア「1」を次のように変更してください。

変更前

```
CREATE CLASSIFIER=1 MACSADDR=DHCP Snooping PROTOCOL=IP
IPSADDR=DHCP Snooping ↓
```

変更後

```
CREATE CLASSIFIER=1 PROTOCOL=IP IPSADDR=DHCP Snooping ↓
```

DHCP Snooping では、IP パケットだけでなく、ARP パケットに対してもフィルタリングを行うことができます。

ENABLE DHCP Snooping ARPSECURITY コマンド (281 ページ) で ARP セキュリティを有効にすると、Untrusted ポートにおいて、登録済み DHCP クライアントからの ARP パケットだけを他ポートに転送し、その他の ARP パケットは転送せずに破棄するようになります。

```
ENABLE DHCP Snooping ARPSECURITY ↓
```

```
CREATE CLASSIFIER=2 PROTOCOL=ARP ETHFORMAT=ETHII-UNTAGGED ↓
```

```
ADD SWITCH HWFILTER CLASSIFIER=2 ACTION=COPY,DISCARD ↓
```

- ✎ 本機能は、DHCP Snooping が有効になっていないと動作しません。
- ✎ バインディングデータベースに MAC アドレス無指定のスタティックエントリを追加している場合は、ARP セキュリティを有効化しないでください。
- ✎ ENABLE DHCP Snooping ARPSECURITY コマンド (281 ページ) はブロードキャストの ARP パケットだけをフィルタリングします。マルチキャストやユニキャストの ARP パケットをフィルタリングするには、すべての ARP パケットを通常の転送動作から除外して CPU にだけ転送するハードウェアパケットフィルタを設定します。このように設定すると、Trusted ポートとバインディングデータベースに登録されている送信元からの ARP パケットだけが CPU 経由で転送され、その他の ARP パケットは破棄されます。なお、ハードウェアパケットフィルタのアクション「COPY,DISCARD」は ARP セキュリティと組み合わせて使うときだけサポートの対象となります。それ以外の用途ではサポート対象外となりますのでご注意ください。

DHCP Snooping では、監視している DHCP メッセージに対して、リレーエージェント情報オプション (オプションコード 82) の付加と削除を行うことも可能です。

ENABLE DHCP Snooping OPTION82 コマンド (283 ページ) でリレーエージェント情報オプションの付加・検査・削除を有効にすると、Untrusted ポートに接続されたクライアントからの DHCP/BOOTP パケットを転送するときに、リレーエージェント情報オプションを挿入するようになります。また、サーバーからの戻りパケットを Untrusted ポートに直接接続されたクライアントに転送するときは同オプションを削除するようになります。

```
ENABLE DHCP Snooping OPTION82 ↓
```

SET DHCP Snooping PORT コマンド (330 ページ) の SUBSCRIBERID パラメーターを利用すれば、リレーエージェント情報オプションに Subscriber-ID サブオプションを含めるかどうか (含めるならばその内容も) をスイッチポートごとに設定することができます。

```
SET DHCP Snooping PORT=5 SUBSCRIBERID="ud-mahahiha" ↓
```

- ✎ 本機能は、DHCP Snooping が有効になっていないと動作しません。
- ✎ 本機能は、DHCP/BOOTP リレーの同種機能 (ENABLE BOOTP RELAY OPTION82 コマンド (「IP」の 255 ページ)) とは併用できません。

DHCP Snooping 有効時は、バインディングデータベースの内容を定期的にチェックして、IP アドレスの使用期限が切れたクライアントの情報をデータベースから削除します。デフォルトのチェック間隔は 60 秒です。

- ✎ スタティック登録したクライアントの情報は削除されません。

チェック間隔は、SET DHCP Snooping CHECKINTERVAL コマンド (329 ページ) で変更できます。有効範囲は 1 ~ 3600 秒です。

```
SET DHCP Snooping CHECKINTERVAL=120 ↵
```

本製品は、バインディングデータベースをチェックするたびに、その時点で有効な (ダイナミック登録された) クライアントの情報を bindXXXX.dsn ファイル (「XXXX」の部分にはファームウェアのバージョンを表す 4 桁の数値が入ります) に書き込みます。DHCP Snooping を無効から有効に変更したときは、最初にこのファイルを読み込み、その時点でまだ有効なクライアントがあれば、それをバインディングデータベースに登録します。

DHCP Snooping の全般的な情報を確認するには、SHOW DHCP Snooping コマンド (401 ページ) を使います。

```
SHOW DHCP Snooping ↵
```

ポートごとの DHCP Snooping 設定を確認するには、SHOW DHCP Snooping PORT コマンド (409 ページ) を使います。

```
SHOW DHCP Snooping PORT ↵
SHOW DHCP Snooping PORT=1 ↵
```

バインディングデータベースの内容を確認するには、SHOW DHCP Snooping DATABASE コマンド (405 ページ) を使います。

```
SHOW DHCP Snooping DATABASE ↵
```

## コマンドリファレンス編

### 機能別コマンド索引

#### 一般コマンド

DISABLE SWITCH STPFORWARD . . . . .	279
ENABLE SWITCH STPFORWARD . . . . .	309
RESET SWITCH . . . . .	322
RESET SWITCH ACCELERATOR COUNTER . . . . .	323
SET SWITCH CPUTXPRIORITY . . . . .	382
SET SWITCH CPUTXQUEUE . . . . .	383
SET SWITCH DLFLIMIT . . . . .	384
SET SWITCH THRASHLIMIT . . . . .	391
SHOW SWITCH . . . . .	490
SHOW SWITCH ACCELERATOR . . . . .	494
SHOW SWITCH ACCELERATOR COUNTER . . . . .	496
SHOW SWITCH COUNTER . . . . .	501

#### ポート

ACTIVATE SWITCH PORT AUTONEGOTIATE . . . . .	171
ACTIVATE SWITCH PORT LOCK . . . . .	172
ADD SWITCH TRUNK . . . . .	190
CREATE SWITCH TRUNK . . . . .	223
DELETE SWITCH TRUNK . . . . .	238
DESTROY SWITCH TRUNK . . . . .	251
DISABLE SWITCH HASH . . . . .	270
DISABLE SWITCH MCLIMITING . . . . .	272
DISABLE SWITCH MIRROR . . . . .	273
DISABLE SWITCH PORT . . . . .	274
DISABLE SWITCH PORT AUTOMDI . . . . .	275
DISABLE SWITCH PORT EGRESSQUEUE . . . . .	276
DISABLE SWITCH PORT FLOW . . . . .	277
DISABLE SWITCH PORT VLAN . . . . .	278
ENABLE SWITCH HASH . . . . .	300
ENABLE SWITCH MCLIMITING . . . . .	302
ENABLE SWITCH MIRROR . . . . .	303
ENABLE SWITCH PORT . . . . .	304
ENABLE SWITCH PORT AUTOMDI . . . . .	305
ENABLE SWITCH PORT EGRESSQUEUE . . . . .	306
ENABLE SWITCH PORT FLOW . . . . .	307
ENABLE SWITCH PORT VLAN . . . . .	308

RESET SWITCH PORT . . . . .	324
SET SWITCH MIRROR . . . . .	385
SET SWITCH PORT . . . . .	387
SET SWITCH TRUNK . . . . .	392
SHOW SWITCH PORT . . . . .	509
SHOW SWITCH PORT COUNTER . . . . .	513
SHOW SWITCH PORT INTRUSION . . . . .	516
SHOW SWITCH TRUNK . . . . .	517
<b>LACP ( IEEE 802.3ad )</b>	
ADD LACP PORT . . . . .	176
DELETE LACP PORT . . . . .	229
DISABLE LACP . . . . .	259
DISABLE LACP DEBUG . . . . .	260
ENABLE LACP . . . . .	286
ENABLE LACP DEBUG . . . . .	287
PURGE LACP . . . . .	311
RESET LACP PORT COUNTER . . . . .	317
SET LACP PORT . . . . .	335
SET LACP . . . . .	336
SHOW LACP . . . . .	417
SHOW LACP PORT . . . . .	419
SHOW LACP TRUNK . . . . .	423
<b>バーチャル LAN</b>	
ADD VLAN PORT . . . . .	191
ADD VLAN PROTOCOL . . . . .	194
ADD VLAN SUBNET . . . . .	197
CREATE VLAN . . . . .	225
DELETE VLAN PORT . . . . .	239
DELETE VLAN PROTOCOL . . . . .	241
DELETE VLAN SUBNET . . . . .	242
DESTROY VLAN . . . . .	252
SET SWITCH NESTEDTPID . . . . .	386
SET VLAN PORT . . . . .	394
SHOW VLAN . . . . .	519
SHOW VLAN PORT . . . . .	526
<b>スパニングツリープロトコル ( STP/RSTP )</b>	
ADD STP VLAN . . . . .	182
CREATE STP . . . . .	222
DELETE STP VLAN . . . . .	234
DESTROY STP . . . . .	250
DISABLE STP . . . . .	265

DISABLE STP DEBUG . . . . .	266
DISABLE STP PORT . . . . .	267
DISABLE STP PORT DEBUG . . . . .	268
ENABLE STP . . . . .	295
ENABLE STP DEBUG . . . . .	296
ENABLE STP PORT . . . . .	297
ENABLE STP PORT DEBUG . . . . .	298
PURGE STP . . . . .	315
RESET STP . . . . .	321
SET STP . . . . .	377
SET STP PORT . . . . .	379
SHOW STP . . . . .	480
SHOW STP COUNTER . . . . .	484
SHOW STP DEBUG . . . . .	486
SHOW STP PORT . . . . .	487

#### マルチブルスパニングツリープロトコル (MSTP)

ADD MSTP MSTI VLAN . . . . .	178
CREATE MSTP MSTI . . . . .	208
DELETE MSTP MSTI VLAN . . . . .	230
DESTROY MSTP MSTI . . . . .	245
DISABLE MSTP . . . . .	261
ENABLE MSTP . . . . .	288
PURGE MSTP . . . . .	312
RESET MSTP COUNTER PORT . . . . .	318
SET MSTP . . . . .	338
SET MSTP CIST . . . . .	340
SET MSTP CIST PORT . . . . .	341
SET MSTP MSTI . . . . .	343
SET MSTP MSTI PORT . . . . .	344
SHOW MSTP . . . . .	425
SHOW MSTP CIST . . . . .	428
SHOW MSTP CIST PORT . . . . .	431
SHOW MSTP COUNTER PORT . . . . .	434
SHOW MSTP MSTI . . . . .	436
SHOW MSTP MSTI PORT . . . . .	439

#### イーサネットリングプロテクション (EPSR)

ADD EPSR DATAVLAN . . . . .	175
CREATE EPSR . . . . .	205
DELETE EPSR DATAVLAN . . . . .	228
DESTROY EPSR . . . . .	244
DISABLE EPSR . . . . .	257

DISABLE EPSR DEBUG . . . . .	258
ENABLE EPSR . . . . .	284
ENABLE EPSR DEBUG . . . . .	285
PURGE EPSR . . . . .	310
SET EPSR . . . . .	332
SET EPSR PORT . . . . .	334
SHOW EPSR . . . . .	411
SHOW EPSR COUNTER . . . . .	414
SHOW EPSR DEBUG . . . . .	416
<b>フォワーディングデータベース</b>	
ADD SWITCH FILTER . . . . .	186
DELETE SWITCH FILTER . . . . .	236
DISABLE SWITCH AGEINGTIMER . . . . .	269
DISABLE SWITCH LEARNING . . . . .	271
ENABLE SWITCH AGEINGTIMER . . . . .	299
ENABLE SWITCH LEARNING . . . . .	301
SET SWITCH AGEINGTIMER . . . . .	381
SHOW SWITCH FDB . . . . .	503
SHOW SWITCH FILTER . . . . .	505
<b>クラシファイア</b>	
CREATE CLASSIFIER . . . . .	198
DESTROY CLASSIFIER . . . . .	243
SET CLASSIFIER . . . . .	325
SHOW CLASSIFIER . . . . .	395
<b>QoS</b>	
ADD QOS FLOWGROUP . . . . .	179
ADD QOS POLICY . . . . .	180
ADD QOS TRAFFICCLASS . . . . .	181
CREATE QOS FLOWGROUP . . . . .	209
CREATE QOS POLICY . . . . .	212
CREATE QOS RED . . . . .	216
CREATE QOS TRAFFICCLASS . . . . .	218
DELETE QOS FLOWGROUP . . . . .	231
DELETE QOS POLICY . . . . .	232
DELETE QOS TRAFFICCLASS . . . . .	233
DESTROY QOS FLOWGROUP . . . . .	246
DESTROY QOS POLICY . . . . .	247
DESTROY QOS RED . . . . .	248
DESTROY QOS TRAFFICCLASS . . . . .	249
PURGE QOS . . . . .	314
SET QOS ACCELERATOR POLICY . . . . .	355

SET QOS DEFAULTPRIORITY . . . . .	356
SET QOS DSCPMAP . . . . .	357
SET QOS FLOWGROUP . . . . .	359
SET QOS POLICY . . . . .	361
SET QOS PORT . . . . .	365
SET QOS PORT EGRESSQUEUE . . . . .	367
SET QOS PRIO2QUEUEMAP . . . . .	369
SET QOS QUEUE2PRIOMAP . . . . .	370
SET QOS RED . . . . .	371
SET QOS TRAFFICCLASS . . . . .	373
SHOW QOS DEFAULTPRIORITY . . . . .	460
SHOW QOS DSCPMAP . . . . .	461
SHOW QOS FLOWGROUP . . . . .	463
SHOW QOS POLICY . . . . .	465
SHOW QOS PORT . . . . .	468
SHOW QOS PRIO2QUEUEMAP . . . . .	471
SHOW QOS QUEUE2PRIOMAP . . . . .	472
SHOW QOS RED . . . . .	474
SHOW QOS TRAFFICCLASS . . . . .	477
 ハードウェアパケットフィルター	
ADD SWITCH HWFILTER . . . . .	188
DELETE SWITCH HWFILTER . . . . .	237
SHOW SWITCH HWFILTER . . . . .	507
 IPv6 ハードウェアパケットフィルター	
ADD SWITCH ACCELERATOR HWFILTER . . . . .	184
DELETE SWITCH ACCELERATOR HWFILTER . . . . .	235
SHOW SWITCH ACCELERATOR HWFILTER . . . . .	499
 ポート認証	
ACTIVATE PORTAUTH PORT REAUTHENTICATE . . . . .	170
DISABLE PORTAUTH . . . . .	262
DISABLE PORTAUTH DEBUG . . . . .	263
DISABLE PORTAUTH PORT . . . . .	264
ENABLE PORTAUTH . . . . .	289
ENABLE PORTAUTH DEBUG . . . . .	290
ENABLE PORTAUTH PORT . . . . .	291
PURGE PORTAUTH PORT . . . . .	313
RESET PORTAUTH PORT . . . . .	319
RESET PORTAUTH PORT MULTIMIB . . . . .	320
SET PORTAUTH IDTOGGLE . . . . .	345
SET PORTAUTH PORT . . . . .	346
SET PORTAUTH PORT SUPPLICANTMAC . . . . .	350



SET PORTAUTH USERNAME . . . . .	353
SHOW PORTAUTH . . . . .	441
SHOW PORTAUTH COUNTER . . . . .	444
SHOW PORTAUTH MULTISUPPLICANT PORT . . . . .	447
SHOW PORTAUTH PORT . . . . .	451
SHOW PORTAUTH TIMER . . . . .	456

## **DHCP Snooping**

ADD DHCP Snooping BINDING . . . . .	173
DELETE DHCP Snooping BINDING . . . . .	227
DISABLE DHCP Snooping . . . . .	253
DISABLE DHCP Snooping ARPSECURITY . . . . .	254
DISABLE DHCP Snooping LOG . . . . .	255
DISABLE DHCP Snooping OPTION82 . . . . .	256
ENABLE DHCP Snooping . . . . .	280
ENABLE DHCP Snooping ARPSECURITY . . . . .	281
ENABLE DHCP Snooping LOG . . . . .	282
ENABLE DHCP Snooping OPTION82 . . . . .	283
RESET DHCP Snooping COUNTER . . . . .	316
SET DHCP Snooping CHECKINTERVAL . . . . .	329
SET DHCP Snooping PORT . . . . .	330
SHOW DHCP Snooping . . . . .	401
SHOW DHCP Snooping COUNTER . . . . .	403
SHOW DHCP Snooping DATABASE . . . . .	405
SHOW DHCP Snooping FILTER . . . . .	408
SHOW DHCP Snooping PORT . . . . .	409

## ACTIVATE PORTAUTH PORT REAUTHENTICATE

カテゴリー：スイッチング / ポート認証

**ACTIVATE PORTAUTH** [= {8021X|MACBASED}] **PORT**={*port-list*|ALL} **REAUTHENTICATE**  
[SUPPLICANTMAC=*macadd*]

*port-list*: スイッチポート番号 (1~。ハイフン、カンマを使った複数指定も可能)

*macadd*: MAC アドレス (xx-xx-xx-xx-xx-xx の形式)

### 解説

指定ポートに接続されている Supplicant を再認証する。

### パラメーター

**PORTAUTH** 認証メカニズム。8021X (802.1X 認証)、MACBASED (MAC ベース認証) から選択する。  
省略時は 8021X と見なされる。

**PORT** スイッチポート。複数指定が可能。実際には、指定したポートのうち、PORTAUTH で指定した認証方式を使用しているポートだけが対象となる。また、PORTAUTH に 8021X を指定した場合は、Authenticator として設定されているポート (TYPE=AUTHENTICATOR または TYPE=BOTH) のみ、認証プロセスが再実行される。

**SUPPLICANTMAC** Supplicant の MAC アドレス。本パラメーターは、Multi-Supplicant モード (MODE=MULTI) のポートか、MAC ベース認証のポートでのみ使用可能。

### 例

ポート 5 に接続されている 802.1X Supplicant を再認証する。

```
ACTIVATE PORTAUTH PORT=5 REAUTHENTICATE
```

ポート 2 に接続されている MAC ベース Supplicant を再認証する。

```
ACTIVATE PORTAUTH=MACBASED PORT=2 REAUTHENTICATE
```

### 関連コマンド

ENABLE PORTAUTH (289 ページ)

ENABLE PORTAUTH PORT (291 ページ)

SHOW PORTAUTH MULTISUPPLICANT PORT (447 ページ)

SHOW PORTAUTH PORT (451 ページ)

## ACTIVATE SWITCH PORT AUTONEGOTIATE

カテゴリー：スイッチング / ポート

**ACTIVATE SWITCH PORT={*port-list*|ALL} AUTONEGOTIATE**

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

指定ポートでオートネゴシエーションプロセスを強制起動し、接続先ポートと通信モード (速度/デュプレックス) のネゴシエーションを行わせる。

### パラメーター

**PORT** スイッチポート。複数指定が可能。通信モード (SET SWITCH PORT コマンドの SPEED パラメーター) が AUTONEGOTIATE に設定されているポートでのみ有効。

### 例

ポート 6 にオートネゴシエーションを行わせる。

```
ACTIVATE SWITCH PORT=6 AUTONEGOTIATE
```

### 備考・注意事項

本コマンドは、通信モードがオートネゴシエーション (AUTONEGOTIATE) に設定されているポートでのみ有効。

### 関連コマンド

SET SWITCH PORT ( 387 ページ )

SHOW SWITCH PORT ( 509 ページ )

## ACTIVATE SWITCH PORT LOCK

カテゴリー：スイッチング / ポート

**ACTIVATE SWITCH PORT={*port-list*|ALL} LOCK**

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

ポートをただちにロックし、これ以上 MAC アドレスの学習を行えないようにする (ポートセキュリティ機能)。

本コマンド実行後に未学習の送信元 MAC アドレスを持つパケットを受信した場合は、SET SWITCH PORT コマンドの INTRUSIONACTION パラメーターで指定されたアクションが実行される。SET SWITCH PORT コマンドの LEARN パラメーターは、本コマンド実行時に登録されていたダイナミックエントリー数になるよう自動的に調整される。

### パラメーター

**PORT** スイッチポート。複数指定が可能。

### 例

ポート 1 を手動でロックする。

```
SET SWITCH PORT=1 LEARN=10 INTRUSIONACTION=DISCARD
ACTIVATE SWITCH PORT=1 LOCK
```

### 備考・注意事項

本コマンドは、あらかじめ SET SWITCH PORT コマンドの LEARN パラメーターに 0 以外の値を設定しておいたポート (ポートセキュリティ機能がオンのポート) に対してのみ有効。

### 関連コマンド

SET SWITCH PORT ( 387 ページ )

SHOW SWITCH PORT ( 509 ページ )

## ADD DHCP Snooping BINDING

カテゴリー：スイッチング / DHCP Snooping

**ADD DHCP Snooping BINDING** [=macadd] **INTERFACE=vlan-if** **IP=ipadd**  
**PORT=port-number**

*macadd*: MAC アドレス (xx-xx-xx-xx-xx-xx の形式)

*vlan-if*: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)

*ipadd*: IP アドレス

*port-number*: スイッチポート番号 (1 ~ )

### 解説

DHCP Snooping テーブル (バインディングデータベース) にスタティックエントリ (IP アドレスを固定的に設定しているクライアントの情報) を追加する。

### パラメーター

**BINDING** クライアントの MAC アドレス

**INTERFACE** クライアントの所属 VLAN

**IP** クライアントの IP アドレス

**PORT** クライアントが接続されているスイッチポート

### 例

IP アドレス 192.168.10.5、MAC アドレス 00-00-00-00-00-01 のクライアントをバインディングデータベースにスタティック登録する。所属 VLAN は「default」、接続するスイッチポートは 5 とする。

```
ADD DHCP Snooping BINDING=00-00-00-00-00-01 INTERFACE=vlan-default
    IP=192.168.10.5 PORT=5
```

### 備考・注意事項

デフォルト設定では、ポートあたり 1 つしかスタティックエントリを登録できない。1 つのポートに複数のスタティックエントリを登録したいときは、SET DHCP Snooping PORT コマンドの MAXLEASES パラメーターの値を増やす必要がある。

MAC アドレス無指定のスタティックエントリを追加する場合は、DHCP Snooping のオプション機能である ARP セキュリティを有効化してはならない (デフォルトは無効。有効時は DISABLE DHCP Snooping ARPSECURITY コマンドで無効化できる)。

### 関連コマンド

DELETE DHCP Snooping Binding ( 227 ページ )

DISABLE DHCP Snooping ARP Security ( 254 ページ )

SET DHCP Snooping Port ( 330 ページ )

SHOW DHCP Snooping Database ( 405 ページ )

## ADD EPSR DATAVLAN

カテゴリー：スイッチング / イーサネットリングプロテクション (EPSR)

**ADD EPSR=***epsrname* **DATAVLAN=**{*vlanname*|1..4094}

*epsrname*: EPSR ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ ) ハイフンを使用可能。大文字小文字を区別しない)

*vlanname*: VLAN 名 (1~32 文字。英数字とアンダースコア ( \_ ) ハイフンを使用可能。大文字小文字は区別しない)

### 解説

EPSR ドメインにデータ VLAN (保護対象の VLAN) を追加する。

本コマンド実行時は、次のルールが適用される。

- ・1 つの EPSR ドメインに追加できるデータ VLAN の数は 512 個まで
- ・データ VLAN、コントロール VLAN を問わず、追加対象の EPSR ドメインにすでに追加されている VLAN は指定できない
- ・他の EPSR ドメインにコントロール VLAN として追加されている VLAN は指定できない
- ・他の EPSR ドメインにデータ VLAN として追加されている VLAN を指定するときは、リング接続用のポートが EPSR ドメイン間で重複しないようにする必要がある
- ・EPSR ドメインに VLAN を追加するとき、あらかじめ VLAN にメンバーポートを割り当てておく必要はない (ループを避ける意味ではそのほうが望ましい場合もある)

### パラメーター

**EPSR** EPSR ドメイン名

**DATAVLAN** データ VLAN。VLAN 名または VLAN ID (VID) で指定する。

### 例

EPSR ドメイン「blues」に VLAN skyblue をデータ VLAN として追加する。

```
ADD EPSR=blues DATAVLAN=skyblue
```

### 関連コマンド

CREATE EPSR (205 ページ)

CREATE VLAN (225 ページ)

DELETE EPSR DATAVLAN (228 ページ)

SHOW EPSR (411 ページ)

## ADD LACP PORT

カテゴリー：スイッチング / LACP (IEEE 802.3ad)

```
ADD LACP PORT={port-list|ALL} [ADMINKEY=0..65535] [PRIORITY=0..65535]
[MODE={ACTIVE|PASSIVE}] [PERIODIC={FAST|SLOW}]
```

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

指定したスイッチポートを LACP の管理下に置く (該当ポートで LACP を有効にする)。

ただし、手動設定したトランクポート (CREATE SWITCH TRUNK コマンド、ADD SWITCH TRUNK コマンド) と Half Duplex で動作しているポートでは LACP を使用できないため、これらのポートは (本コマンドで指定したとしても) 自動的に LACP の管理下から外される。

なお、デフォルトでは、すべてのスイッチポートが LACP の管理下に置かれている。

### パラメーター

**PORT** ポート番号。

**ADMINKEY** LACP ポート鍵の元となる値を指定する (ポート鍵の値そのものではない)。LACP では、対向機器、所属 VLAN、通信速度、ポート鍵のすべてが等しいポート群で 1 つのトランクグループを構成する。したがって、本来なら 1 つのトランクグループを構成するポート群を複数のグループに分けたい場合は、グループごとに異なる ADMINKEY を設定すればよい。なお、ADMINKEY は自機内でのみ意味を持つ (対向機器と同じに設定する必要はない)。デフォルトは 1。

**PRIORITY** LACP ポートプライオリティー。小さいほど優先度が高い。使用可能な LACP ポート数がトランクグループの最大ポート数 (4 ポート) よりも多い場合、本パラメーターの小さいポートほどメンバーに選ばれる可能性が高くなる。なお、ポートプライオリティーが等しい場合は、ポート番号の小さいほうが優先的に使用される。また、メンバーに選ばれなかったポートはスタンバイ状態となり、現行のメンバーポートがリンクダウンするときに備えて待機する。デフォルトは 32768。

**MODE** LACP ポートの動作モード。ACTIVE (PERIODIC パラメーターで設定した間隔で LACP パケットを自発的に送信する)、PASSIVE (対向ポートから LACP パケットを受信したときだけ LACP パケットを送信する) から選択する。デフォルトは ACTIVE。

**PERIODIC** ACTIVE モード時の LACP パケットの送信間隔。FAST (1 秒)、SLOW (30 秒) から選択する。デフォルトは FAST。

### 例

ポート 1～4 を LACP の管理下に置く。

```
ADD LACP PORT=1-4
```



関連コマンド

DELETE LACP PORT ( 229 ページ )

SET LACP PORT ( 335 ページ )

SHOW LACP PORT ( 419 ページ )

## ADD MSTP MSTI VLAN

カテゴリー：スイッチング / マルチプルスパニングツリープロトコル (MSTP)

**ADD MSTP MSTI=instance VLAN={1..4094|ALL}**

*instance*: MST インスタンス ID (1 ~ 4094)

### 解説

MST インスタンスに VLAN を関連付ける。

デフォルトでは、すべての VLAN が CIST (Common and Internal Spanning Tree) に関連付けられている。本コマンドを実行すると、VLAN は CIST との関連付けを解除され、指定した MST インスタンスに関連付けられる。

各 VLAN は、1 つの MST インスタンスまたは CIST とのみ関連付けることができる。ある MST インスタンスから別の MST インスタンスに関連付けを変更するときは、あらかじめ DELETE MSTP MSTI VLAN コマンドを実行して、該当 VLAN を CIST 所属に戻した上で本コマンドを実行しなくてはならない。

### パラメーター

**MSTI** MST インスタンス ID

**VLAN** VLAN ID (VID)。ALL を指定した場合はすべての VLAN が指定した MST インスタンスに関連付けられる。

### 例

MST インスタンス「1」に VLAN「10」を関連付ける。

```
ADD MSTP MSTI=1 VLAN=10
```

### 関連コマンド

CREATE MSTP MSTI (208 ページ)

DELETE MSTP MSTI VLAN (230 ページ)

SHOW MSTP (425 ページ)

SHOW MSTP MSTI (436 ページ)

## ADD QOS FLOWGROUP

カテゴリー：スイッチング / QoS

**ADD QOS FLOWGROUP=***flow-id* **CLASSIFIER=***rule-list*

*flow-id*: フローグループ番号 (0~1023)

*rule-list*: クラシファイア番号 (1~9999)。ハイフン、カンマを使った複数指定も可能)

### 解説

フローグループにクラシファイア (汎用パケットフィルター) を割り当てる。

### パラメーター

**FLOWGROUP** フローグループ番号

**CLASSIFIER** クラシファイア番号。複数指定も可能。

### 例

フローグループ「100」にクラシファイア「1」「5」「6」を追加する。

```
ADD QOS FLOWGROUP=100 CLASSIFIER=1,5-6
```

### 関連コマンド

CREATE QOS FLOWGROUP ( 209 ページ )

DELETE QOS FLOWGROUP ( 231 ページ )

DESTROY QOS FLOWGROUP ( 246 ページ )

SET QOS FLOWGROUP ( 359 ページ )

SHOW QOS FLOWGROUP ( 463 ページ )

## ADD QOS POLICY

カテゴリー：スイッチング / QoS

**ADD QOS POLICY=*qos-id* TRAFFICCLASS=*tc-list***

*qos-id*: QoS ポリシー番号 (0~255)

*tc-list*: トラフィッククラス番号 (0~1023。ハイフン、カンマを使った複数指定も可能)

### 解説

QoS ポリシーにトラフィッククラスを割り当てる。

### パラメーター

**POLICY** QoS ポリシー番号

**TRAFFICCLASS** トラフィッククラス番号。複数指定が可能。パケットの照合は、ポリシー内のトラフィッククラス番号順に行われる。

### 例

QoS ポリシー「10」にトラフィッククラス「1」「2」「3」を追加する。

ADD QOS POLICY=10 TRAFFICCLASS=1-3

### 関連コマンド

CREATE QOS POLICY ( 212 ページ )

DELETE QOS POLICY ( 232 ページ )

DESTROY QOS POLICY ( 247 ページ )

SET QOS POLICY ( 361 ページ )

SET QOS PORT ( 365 ページ )

SHOW QOS POLICY ( 465 ページ )

## ADD QOS TRAFFICCLASS

カテゴリー：スイッチング / QoS

**ADD QOS TRAFFICCLASS=tc-id FLOWGROUP=flow-list**

*tc-id*: トラフィッククラス番号 (0~1023)

*flow-list*: フローグループ番号 (0~1023)。ハイフン、カンマを使った複数指定も可能)

### 解説

トラフィッククラスにフローグループを割り当てる。

### パラメーター

**TRAFFICCLASS** トラフィッククラス番号

**FLOWGROUP** フローグループ番号。複数指定が可能。パケットの照合は、トラフィッククラス内のフローグループ番号順に行われる。

### 例

トラフィッククラス「20」にフローグループ「1」「3」を割り当てる。

ADD QOS TRAFFICCLASS=20 FLOWGROUP=1,3

### 関連コマンド

CREATE QOS TRAFFICCLASS ( 218 ページ )

DELETE QOS TRAFFICCLASS ( 233 ページ )

DESTROY QOS TRAFFICCLASS ( 249 ページ )

SET QOS TRAFFICCLASS ( 373 ページ )

SHOW QOS TRAFFICCLASS ( 477 ページ )

## ADD STP VLAN

カテゴリー：スイッチング / スパニングツリープロトコル (STP/RSTP)

**ADD STP=stpname VLAN={vlanname|2..4094}**

*stpname*: STP ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

*vlanname*: VLAN 名 (1~32 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字は区別しない)

### 解説

ユーザー定義の STP ドメインに VLAN を所属させる。

STP ドメインには、デフォルトで存在する「default STP」(削除不可)と、CREATE STP コマンドで作成したユーザー定義の STP ドメインがある。

- ・VLAN default はつねに default STP の所属となり、他の STP に所属させることはできない。
- ・CREATE VLAN コマンドで作成したユーザー定義の VLAN も、本コマンドで所属を変えない限り default STP の所属となる。
- ・ユーザー定義 STP ドメインから削除された VLAN は default STP の所属に戻る。
- ・他のユーザー定義 STP に所属している VLAN の所属を本コマンドで変えることはできない。その場合、いったん STP から VLAN を削除し ( default STP 所属に戻し )、その後本コマンドを実行する。
- ・スイッチポートが複数の VLAN に所属している場合、該当ポートは複数の STP ドメインに所属できる (オーバーラップ STP)。ただし、オーバーラップ STP は標準規格でないため、他製品との相互接続性は保証されない。

### パラメーター

**STP** STP ドメイン名。default は指定できない。ユーザー定義の STP ドメインから default STP に戻したときは、DELETE STP VLAN コマンドを使って、該当 VLAN をユーザー定義 STP の所属からはずせばよい。

**VLAN** VLAN 名または VLAN ID (VID)

### 例

STP ドメイン「mystp」に VLAN white を追加する。

```
ADD STP=mystp VLAN=white
```

### 備考・注意事項

本コマンドを実行すると、該当 VLAN 所属ポートのスパニングツリーパラメーターはすべてデフォルト値に戻る。

### 関連コマンド

DELETE STP VLAN ( 234 ページ )

SHOW STP ( 480 ページ )

## ADD SWITCH ACCELERATOR HWFILTER

カテゴリー：スイッチング / IPv6 ハードウェアパケットフィルター

備考：IPv6 アクセラレーターボード AT-ACC01 と拡張メモリー AT-SD512A-001 が必要（本機能は 9924SP では使用できません）

```
ADD SWITCH ACCELERATOR HWFILTER [=filter-id] CLASSIFIER=rule-id
ACTION={FORWARD|DISCARD|MARK} [NEWIPDSCP=0..63] [NEWPRIORITY=0..7]
```

*filter-id*: フィルター番号（1～999）

*rule-id*: クラシファイア番号（1～9999）

### 解説

IPv6 ハードウェアパケットフィルターを追加する。

IPv6 ハードウェアパケットフィルターは、IPv6 のルーティングパケットだけを対象としたフィルタリング機能。IPv6 アクセラレーターボードの L3 処理部で処理が行われる（IPv6 アクセラレーターボードが必要）。IPv6 ハードウェアパケットフィルターでは、始点・終点 IPv6 アドレス、DSCP 値、L4 プロトコル、L4 ポート番号に基づいて、IPv6 パケットのフィルタリング（転送・破棄・マーク）が可能。これらの条件は、クラシファイア（CREATE CLASSIFIER コマンドで作成）で定義する。本コマンドでは、クラシファイア番号とマッチ時のアクションを組として、フィルターリストに追加する。

IPv6 ハードウェアパケットフィルターで使用するクラシファイアは、CREATE CLASSIFIER コマンドのページに掲載されている「IPv6 ハードウェアパケットフィルター用の構文」にしたがっていないとエラーになる。同構文にないパラメーターを含むクラシファイアを使おうとすると、エラーになる。

IPv6 ハードウェアパケットフィルターは番号の小さい順に検索され、最初にマッチしたフィルターのアクションが実行される。

設定可能なフィルター数は 999 個。システムテーブルの空き容量には依存しない。

なお、その他のパケット（ただし IPv6 ルーティングパケットも含む。詳細は後述）のフィルタリングには、通常のハードウェアパケットフィルターを用いる（ADD SWITCH HWFILTER コマンド）。通常のハードウェアパケットフィルターは、本体スイッチチップの L2 処理部で適用される。

2 つのハードウェアパケットフィルターは独立しており、次の順序で処理が行われる。

- (1) ハードウェアパケットフィルター（すべてのパケット）
  - (2) IPv6 ハードウェアパケットフィルター（IPv6 ルーティングパケットのみ）
- (1) のハードウェアパケットフィルターでは、IPv6 ルーティングパケットも対象になることに注意。(1) で IPv6 パケットをすべて破棄するような設定をすると、ルーティングパケットであっても (2) の処理は行われない（(1) でパケットが破棄されるため）。

### パラメーター

**HWFILTER** フィルター番号。省略時は現在最後尾のフィルターの後に追加される（最後尾のフィルター番号を「n」とすると、新規フィルターは「n+1」になる）。「n+1」より大きなフィルター番号を指定するとエラーになる。既存フィルターと同じ番号を指定した場合は、既存フィルターの位置に新規



フィルターが挿入され、既存フィルター以降は番号が1つずつ後ろにずれる。

**CLASSIFIER** クラシファイア番号。本パラメーターに指定するクラシファイアは、CREATE CLASSIFIER コマンドのページに掲載されている「IPv6 ハードウェアパケットフィルター用の構文 (IPv6 ルーティングパケット)」に準拠していること。

**ACTION** パケットがクラシファイアに一致したときのアクション。FORWARD (転送)、DISCARD (破棄)、MARK (DSCP/802.1p を書き換え) から選択する。MARK を指定したときは、NEWIPDSCP パラメーターか NEWPRIORITY パラメーターで書き換え後のフィールド値を指定すること (両方を指定することも可)。

**NEWIPDSCP** ACTION=MARK のとき、書き換え後の IPv6 DSCP (DiffServ Code Point) フィールド値を指定する。

**NEWPRIORITY** ACTION=MARK のとき、書き換え後の 802.1p ユーザープライオリティーフィールド値を指定する。

## 例

ホスト 3ffe:b80:3c:20::200 からネットワーク 3ffe:b80:3c:10::/64 宛ての IPv6 パケットを破棄。

```
CREATE CLASSIFIER=10 ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6
  IPSADDR=3ffe:b80:3c:20::200/128 IPDADDR=3ffe:b80:3c:10::/64
ADD SWITCH ACCELERATOR HWFILTER=1 CLASSIFIER=10 ACTION=DISCARD
```

IPv6 上の UDP パケットの DSCP 値を 17 に書き換える。

```
CREATE CLASSIFIER=11 ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6 IPPROTO=UDP
ADD SWITCH ACCELERATOR HWFILTER=2 CLASSIFIER=11 ACTION=MARK NEWIPDSCP=17
```

## 備考・注意事項

本コマンドで指定するクラシファイアは、CREATE CLASSIFIER コマンドのページに掲載されている「IPv6 ハードウェアパケットフィルター用の構文」に準拠している必要がある。

トンネリング IPv6 パケット (IPv6 over IPv4 および 6to4) はフィルタリングの対象にならないので注意。

## 関連コマンド

CREATE CLASSIFIER (198 ページ)

DELETE SWITCH ACCELERATOR HWFILTER (235 ページ)

SHOW SWITCH ACCELERATOR HWFILTER (499 ページ)

## ADD SWITCH FILTER

カテゴリー：スイッチング / フォワーディングデータベース

**ADD SWITCH FILTER DESTADDRESS=macadd PORT=port-number ACTION={FORWARD|DISCARD} [ENTRY=entry-id] [LEARN] [VLAN={vlanname|1..4094}]**

*macadd*: MAC アドレス (xx-xx-xx-xx-xx-xx の形式)

*port-number*: スイッチポート番号 (1 ~ )

*entry-id*: エントリー番号 (0 ~ 319)

*vlanname*: VLAN 名 (1 ~ 32 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字は区別しない)

### 解説

フォワーディングデータベース (FDB) にスタティックエントリー (スイッチフィルター) を登録する。スタティックエントリーは 1 ポートあたり 320 件まで登録可能。

### パラメーター

**DESTADDRESS** 登録する MAC アドレス。ユニキャスト (個体) アドレスでなくてはならない。ユニキャストアドレスは先頭オクテットが偶数。

**PORT** 出力ポート番号。ACTION に FORWARD を指定した場合、DESTADDRESS 宛てのフレームは、ここで指定したポートから出力される。

**ACTION** 該当フレームの処理方法。FORWARD (転送) と DISCARD (破棄) から選択。

**ENTRY** 該当ポートの FDB エントリー番号。省略時はエントリーリストの末尾に追加される。すでに n 個のエントリーが存在している場合 (0 ~ n-1 が存在) 本パラメーターを省略すると「n」を指定したのと同じ動作になる。「n」より大きなエントリー番号を指定することはできない。既存エントリーと同じ番号を指定した場合は、既存エントリーの前に新規エントリーが追加され、既存エントリー以降は番号が 1 つずつ後ろにずれる。

**LEARN** 登録するエントリーを、ポートセキュリティの学習済み MAC アドレス (Learn エントリー) の 1 つとして数えるようにする。ポートセキュリティ機能は、SET SWITCH PORT コマンドの LEARN パラメーターで設定する。

**VLAN** VLAN 名か VLAN ID (VID)。出力ポートに VLAN タグが設定されている場合に指定する。省略時は該当ポートのタグなし VLAN を指定したものと見なされる。そのため、ポートがタグ付き VLAN にしか所属していないとき (タグなし VLAN に所属していないとき) は省略できない。出力ポートがタグなしの場合は不要。

### 例

ポート 10 (タグなし) 配下のステーションを FDB に登録する。

```
ADD SWITCH FILTER DEST=00-00-f4-12-34-56 PORT=10 ACTION=FORWARD
```

ポート 6 (タグなし) 配下のステーション 00-00-f4-ab-cd-ef 宛てのフレームを破棄する。

```
ADD SWITCH FILTER DEST=00-00-f4-ab-cd-ef PORT=6 ACTION=DISCARD
```

ポート 2 (タグなし) 配下のステーション 00-00-f4-c9-73-ff をポートセキュリティの学習済みアドレスとして追加する。

```
ADD SWITCH FILTER DEST=00-00-f4-c9-73-ff PORT=2 ACTION=FORWARD LEARN
```

ポート 5 (タグ付き) 配下のステーションを FDB に登録する。所属 VLAN は orange。

```
ADD SWITCH FILTER DEST=00-00-f4-11-11-11 PORT=5 VLAN=orange  
ACTION=FORWARD
```

### 備考・注意事項

スタティックエントリーの出力ポートが指定 VLAN から削除された場合、同エントリーも自動的に削除される。

### 関連コマンド

DELETE SWITCH FILTER (236 ページ)

SET SWITCH PORT (387 ページ)

SHOW SWITCH FILTER (505 ページ)

## ADD SWITCH HWFILTER

カテゴリー：スイッチング / ハードウェアパケットフィルター

```
ADD SWITCH HWFILTER [=filter-id] CLASSIFIER=rule-id ACTION={FORWARD|
DISCARD|SETL2QOS} [L2QOSQUEUE=0..7] [PRIORITY=0..7]
```

*filter-id*: フィルター番号 (1~1024)

*rule-id*: クラシファイア番号 (1~9999)

### 解説

ハードウェアパケットフィルターを追加する。

ハードウェアパケットフィルターは、すべてのパケットを対象としたフィルタリング機能。本体スイッチチップの L2 処理部で処理が行われる。

ハードウェアパケットフィルターでは、L2 から L4 までの各種条件 (MAC アドレス、L3 プロトコル、IPv4 アドレス、L4 プロトコル、L4 ポートなど) に基づいて、パケットのフィルタリング (転送・破棄) が可能。これらの条件は、クラシファイア (CREATE CLASSIFIER コマンドで作成) で定義する。本コマンドでは、クラシファイア番号とマッチ時のアクションを組として、フィルターリストに追加する。

ハードウェアパケットフィルターで使用するクラシファイアは、CREATE CLASSIFIER コマンドのページに掲載されている「ハードウェアパケットフィルター・QoS ポリシー用の構文」にしたがっていないとしない。同構文にないパラメーターを含むクラシファイアを使おうとすると、エラーになる。

ハードウェアパケットフィルターは番号の小さい順に検索され、最初にマッチしたフィルターのアクションが実行される。どのフィルターにもマッチしなかったパケットは通常通り処理 (転送) される。

ハードウェアパケットフィルターは、すべてのポートで受信したパケットに対して適用される。ただし、クラシファイアの VLAN パラメーターを使えば、特定の VLAN で受信したパケットだけを識別することが可能。

設定可能なフィルター数は、システムテーブルの空き容量に依存する。システムテーブルの空き容量は、SHOW SWITCH コマンドで確認できる。

なお、IPv6 アクセラレーターボード装着時は、IPv6 のルーティングパケットに対して、IPv6 ハードウェアパケットフィルターを適用することも可能 (ADD SWITCH ACCELERATOR HWFILTER コマンド)。IPv6 ハードウェアパケットフィルターでは、始点・終点 IPv6 アドレス、DSCP 値、L4 プロトコル、L4 ポート番号に基づいて、IPv6 パケットのフィルタリング (転送・破棄・マーク) が可能。IPv6 ハードウェアパケットフィルターは、IPv6 アクセラレーターボードの L3 処理部で適用される。

2 つのハードウェアパケットフィルターは独立しており、次の順序で処理が行われる。

(1) ハードウェアパケットフィルター (すべてのパケット)

(2) IPv6 ハードウェアパケットフィルター (IPv6 ルーティングパケットのみ)

(1) のハードウェアパケットフィルターでは、IPv6 ルーティングパケットも対象になることに注意。(1) で IPv6 パケットをすべて破棄するような設定をすると、ルーティングパケットであっても (2) の処理は行われない ( (1) でパケットが破棄されるため )。

### パラメーター

**HWFILTER** フィルター番号。省略時は現在最後尾のフィルターの後に追加される（最後尾のフィルター番号を「n」とすると、新規フィルターは「n+1」になる）。「n+1」より大きなフィルター番号を指定するとエラーになる。既存フィルターと同じ番号を指定した場合は、既存フィルターの位置に新規フィルターが挿入され、既存フィルター以降は番号が1つずつ後ろにずれる。

**CLASSIFIER** クラシファイア番号。本パラメーターに指定するクラシファイアは、CREATE CLASSIFIER コマンドのページに掲載されている「ハードウェアパケットフィルター・QoS ポリシー用の構文」に準拠していること。

**ACTION** マッチしたパケットに対するアクション。FORWARD（転送）、DISCARD（破棄）、SETL2QOS（L2 QoS を適用）から選択する。

**L2QOSQUEUE** マッチしたパケットを格納するキュー。ACTION=SETL2QOS のときだけ有効。CPU 宛てのパケットの場合は CPU の受信キュー、その他のパケット（CPU 宛てでないパケット）の場合は出力ポートの送信キューを指定する。CPU 宛てのパケットに対して本パラメーターを指定した場合は、該当パケットを CPU に渡すときの優先順位を制御できる。また、その他のパケットに対して本パラメーターを指定した場合は、パケットをポートから出力するときの優先順位を制御できる。デフォルトは 0。

**PRIORITY** マッチしたパケットにセットする 802.1p ユーザープライオリティー値。ACTION=SETL2QOS のときだけ有効。なお、CPU 宛てのパケットに対して本パラメーターを指定することは意味を持たない。デフォルトは 0。

## 例

ホスト 192.168.20.200 からネットワーク 192.168.10.0/24 宛ての IP パケットを破棄。

```
CREATE CLASSIFIER=11 IPSADDR=192.168.20.200 IPDADDR=192.168.10.0/24
ADD SWITCH HWFILTER=1 CLASSIFIER=11 ACTION=DISCARD
```

## 備考・注意事項

本コマンドで指定するクラシファイアは、CREATE CLASSIFIER コマンドのページに掲載されている「ハードウェアパケットフィルター・QoS ポリシー用の構文」に準拠している必要がある。

ACTION=SETL2QOS を指定すると IP TOS の値が 0 に書き換えられる。

## 関連コマンド

CREATE CLASSIFIER ( 198 ページ )

DELETE SWITCH HWFILTER ( 237 ページ )

SHOW SWITCH HWFILTER ( 507 ページ )

## ADD SWITCH TRUNK

カテゴリー：スイッチング / ポート

**ADD SWITCH TRUNK=*trunk* PORT=*port-list***

*trunk*: トランクグループ名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

*port-list*: スイッチポート番号 (1~)。ハイフン、カンマを使った複数指定も可能)

### 解説

既存のトランクグループにポートを追加する。

### パラメーター

**TRUNK** トランクグループ名

**PORT** ポート番号。複数指定が可能。トランクグループには、最大 4 ポートまで所属可能。ミラーポートをトランクグループに参加させることはできない。また、他のトランクグループに所属しているポートは指定できない。トランクポートは同一 VLAN に所属している必要がある。

### 例

トランクグループ「aggr1」にポート 1~4 を追加する。

```
ADD SWITCH TRUNK=aggr1 PORT=1-4
```

### 関連コマンド

CREATE SWITCH TRUNK ( 223 ページ )

DELETE SWITCH TRUNK ( 238 ページ )

DESTROY SWITCH TRUNK ( 251 ページ )

ENABLE SWITCH HASH ( 300 ページ )

SET SWITCH TRUNK ( 392 ページ )

SHOW SWITCH TRUNK ( 517 ページ )

## ADD VLAN PORT

カテゴリー：スイッチング / バーチャル LAN

```
ADD VLAN={vlanname|1..4094} PORT={port-list|ALL} [FRAME={TAGGED|
    UNTAGGED}] [UPLINK]
```

```
ADD VLAN={vlanname|1..4094} PORT={port-list|ALL} SUBNET={ipadd|ALL}
    [UPLINK]
```

```
ADD VLAN={vlanname|1..4094} PORT={port-list|ALL} PROTOCOL={protocoltype|
    index-list|ALL} [UPLINK]
```

```
ADD VLAN={vlanname|1..4094} PORT=port-list NESTEDTYPE={CORE|CUSTOMER}
```

```
ADD VLAN={vlanname|1..4094} PORT={port-list|ALL} SUBNET={ipadd|ALL}
    NESTEDTYPE={CUSTOMER}
```

```
ADD VLAN={vlanname|1..4094} PORT={port-list|ALL} PROTOCOL={protocoltype|
    index-list|ALL} NESTEDTYPE={CUSTOMER}
```

*vlanname*: VLAN 名 (1～32 文字。英数字とアンダースコア ( \_ ) ハイフンを使用可能。大文字小文字は区別しない)

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

*ipadd*: IP アドレス

*protocoltype*: L3 プロトコル番号 (16 進数。「0x」を前置すること)

*index-list*: インデックス番号 (0～。ハイフン、カンマを使った複数指定も可能)

### 解説

VLAN にポートを追加する。

VLAN と PORT 以外のパラメーターを指定しなかった場合は、該当 VLAN のタグなし (Untagged) ポート VLAN メンバーに追加される。VLAN、PORT と FRAME=TAGGED を指定した場合は、該当 VLAN のタグ付き (Tagged) ポート VLAN メンバーに追加される。

VLAN、PORT に加え、SUBNET、PROTOCOL のいずれかを指定した場合は、それぞれ該当 VLAN のサブネット VLAN メンバー、プロトコル VLAN メンバーに追加される。

ポートをサブネット VLAN、プロトコル VLAN のいずれかに追加する場合、該当ポートをあらかじめ任意のポート VLAN にタグなしポートとして参加させておく必要がある。

### パラメーター

**VLAN** VLAN 名または VLAN ID (VID)

**PORT** ポート番号。複数指定が可能。ALL を指定した場合はすべてのスイッチポートが対象となる。各ポートは、ポート VLAN のタグなしポートとしては 1 つの VLAN だけに、タグ付きポートとしては



複数の VLAN に所属できる。ミラーポートを VLAN に追加することはできない。

**FRAME** 該当 VLAN のタグ設定。TAGGED (タグ付き)、UNTAGGED (タグなし) から選択する。UNTAGGED を指定する場合、該当ポートがすでに default 以外の VLAN にタグなしポートとして所属しているときは、同 VLAN から削除した上で本コマンドを実行する必要がある。ポートが VLAN default に所属している状態で UNTAGGED を指定して別の VLAN に追加すると、自動的に VLAN default から削除される。デフォルトは UNTAGGED。

**SUBNET** サブネットアドレス。ポートをサブネット VLAN に追加するときに指定する。ただし、ダブルタグ VLAN (Nested VLAN) のコアポートの場合は、本パラメーターを指定する必要はない (指定するとエラーになる)。PROTOCOL パラメーター、および、FRAME=TAGGED とは同時に指定できない。

**PROTOCOL** プロトコル。ポートをプロトコル VLAN に追加するときに指定する。ただし、ダブルタグ VLAN (Nested VLAN) のコアポートの場合は、本パラメーターを指定する必要はない (指定するとエラーになる)。プロトコルは、定義済みのプロトコル名 (ADD VLAN PROTOCOL コマンドの表を参照) か、16 進表記 (「0x」を前置すること) のプロトコル番号で指定する。あるいは、SHOW VLAN コマンドで表示されるインデックス番号 (複数指定可) で指定することもできる。SUBNET パラメーター、および、FRAME=TAGGED とは同時に指定できない。

**UPLINK** VLAN パラメーターでマルチプル VLAN (Private VLAN) を指定した場合、本オプション付きで追加したポートはアップリンクポートになる。また、本オプションなしで追加したポートはプライベートポートになる。本オプションを指定する場合、PORT パラメーターで指定するポートは、VLAN default 以外の非 Private VLAN に所属してはならない。また、いずれかの Private VLAN において、プライベートポートになってはならない。

**NESTEDTYPE** VLAN パラメーターでダブルタグ VLAN (Nested VLAN) を指定した場合、追加するポートの種類を CORE (コアポート)、CUSTOMER (カスタマーポート) から選択する。なお、コアポートをサブネット VLAN、プロトコル VLAN に追加するときは、SUBNET、PROTOCOL パラメーターの指定は不要 (指定するとエラーになる)。コアポートの場合は NESTEDTYPE=CORE だけを指定すればよい。

## 例

ポート 1~4 を VLAN orange のポート VLAN メンバー (タグなしポート) に追加する。

```
ADD VLAN=orange PORT=1-4
```

ポート 12 を VLAN white と orange のタグ付きポートに設定する。

```
ADD VLAN=white PORT=12 FRAME=TAGGED
ADD VLAN=orange PORT=12 FRAME=TAGGED
```

ポート 1~2 を VLAN orange のサブネット VLAN メンバー (サブネット 192.168.10.0) に追加する。



```
ADD VLAN=orange PORT=1-2 SUBNET=192.168.10.0
```

ポート 4～8 を VLAN beige のプロトコル VLAN メンバー（プロトコル NetBEUI）に追加する。

```
ADD VLAN=beige PORT=4-8 PROTOCOL=NetBEUI
```

ポート 5～8 をダブルタグ VLAN（Nested VLAN）AAAinc, BBBinc, CCCinc のコアポートとして追加する。また、ポート 1、2、3 をそれぞれ Nested VLAN AAAinc、BBBinc、CCCinc のカスタマーポートとして追加する。

```
ADD VLAN=AAAinc PORT=5-8 NESTEDTYPE=CORE
ADD VLAN=BBBinc PORT=5-8 NESTEDTYPE=CORE
ADD VLAN=CCCinc PORT=5-8 NESTEDTYPE=CORE
ADD VLAN=AAAinc PORT=1 NESTEDTYPE=CUSTOMER
ADD VLAN=BBBinc PORT=2 NESTEDTYPE=CUSTOMER
ADD VLAN=CCCinc PORT=3 NESTEDTYPE=CUSTOMER
```

### 備考・注意事項

ダブルタグ VLAN（Nested VLAN）は別売のフィーチャーライセンス AT-FL-09 が必要。

### 関連コマンド

```
ADD VLAN PROTOCOL ( 194 ページ )
ADD VLAN SUBNET ( 197 ページ )
DELETE VLAN PORT ( 239 ページ )
SET VLAN PORT ( 394 ページ )
SHOW VLAN ( 519 ページ )
SHOW VLAN PORT ( 526 ページ )
```

## ADD VLAN PROTOCOL

カテゴリー：スイッチング / バーチャル LAN

**ADD VLAN={vlanname|1..4094} PROTOCOL=protocoltype**

*vlanname*: VLAN 名 (1~32 文字。英数字とアンダースコア ( \_ ) ハイフンを使用可能。大文字小文字は区別しない)

*protocoltype*: L3 プロトコル番号 (16 進数。「0x」を前置すること)

### 解説

VLAN にパケット分類基準となるプロトコルを追加する (関連付ける)。

追加したプロトコルは、ADD VLAN PORT コマンドでタグなしポートと関連付ける必要がある。

### パラメーター

**VLAN** VLAN 名または VLAN ID (VID)

**PROTOCOL** プロトコル。定義済みのプロトコル名 (別表を参照) か、16 進表記 (「0x」を前置すること) のプロトコル番号で指定する。プロトコル番号で指定する場合、802.2 なら 1 バイト (DSAP のみ) で、Ethernet Version 2 なら 2 バイトで、SNAP なら 5 バイトの 16 進数で指定する

SAP (Service Access Point)	
IPX 802.2	E0 (SAP)
NetBEUI	F0 (SAP)
SNA Path Control	04 (SAP)
PROWAY-LAN	0E (SAP)
EIA-RS	4E (SAP)
PROWAY	8E (SAP)
ISO CLNS IS	FE (SAP)
Ethernet Version 2	
IP ETHII	0800 (Ethernet Version 2)
X.75 Internet	0801 (Ethernet Version 2)
NBS Internet	0802 (Ethernet Version 2)
ECMA Internet	0803 (Ethernet Version 2)
Chaosnet	0804 (Ethernet Version 2)
X.25 Level 3	0805 (Ethernet Version 2)
ARP	0806 (Ethernet Version 2)
XNS Compat	0807 (Ethernet Version 2)
Banyan Systems	0BAD (Ethernet Version 2)
BBN Simnet	5208 (Ethernet Version 2)

DEC MOP Dump/Ld	6001 ( Ethernet Version 2 )
DEC MOP Rem Cons	6002 ( Ethernet Version 2 )
DEC DECNET	6003 ( Ethernet Version 2 )
DEC LAT	6004 ( Ethernet Version 2 )
DEC Diagnostic	6005 ( Ethernet Version 2 )
DEC Customer	6006 ( Ethernet Version 2 )
DEC LAVC	6007 ( Ethernet Version 2 )
RARP	8035 ( Ethernet Version 2 )
DEC LANBridge	8038 ( Ethernet Version 2 )
DEC Encryption	803D ( Ethernet Version 2 )
Appletalk	809B ( Ethernet Version 2 )
IBM SNA	80D5 ( Ethernet Version 2 )
AppleTalk AARP	80F3 ( Ethernet Version 2 )
IPX EthII	8137 ( Ethernet Version 2 )
SNMP	814C ( Ethernet Version 2 )
IPv6	86DD ( Ethernet Version 2 )
IPX 802.3	FFFF ( NetWare 802.3 raw )
SNAP ( Sub-Network Access Protocol )	
ETHERTALK 2	080007809B ( SNAP )
ETHERTALK 2 AARP	00000080F3 ( SNAP )
IPX SNAP	0000008137 ( SNAP )

表 31: 定義済みのプロトコル名一覧

## 例

VLAN sales にプロトコル IPX 802.2 ( 802.2 の IPX ) を追加する。

```
ADD VLAN=sales PROTOCOL="IPX 802.2"
```

VLAN mktg にプロトコル NetBEUI を追加する。

```
ADD VLAN=mktg PROTOCOL="NetBEUI"
```

## 備考・注意事項

本コマンドで追加したプロトコルは、これ以降インデックス番号で指定することができる。インデックス番号を確認するには SHOW VLAN コマンドを使う。なお、インデックス番号は可変（追加、削除により番号がずれる）なので、インデックス番号を指定するときは、必ず SHOW VLAN コマンドで確認すること。

## 関連コマンド

ADD VLAN PORT ( 191 ページ )

DELETE VLAN PORT ( 239 ページ )

DELETE VLAN PROTOCOL ( 241 ページ )

SHOW VLAN ( 519 ページ )

## ADD VLAN SUBNET

カテゴリー：スイッチング / バーチャル LAN

**ADD VLAN**={*vlanname*|1..4094} **SUBNET**=*ipadd* [MASK=*ipadd*]

*vlanname*: VLAN 名 (1~32 文字。英数字とアンダースコア ( \_ ) ハイフンを使用可能。大文字小文字は区別しない)

*ipadd*: IP アドレスまたはネットマスク

### 解説

VLAN にパケット分類基準となる IP サブネットを追加する (関連付ける)。

追加したサブネットは、ADD VLAN PORT コマンドでタグなしポートと関連付ける必要がある。

### パラメーター

**VLAN** VLAN 名または VLAN ID (VID)

**SUBNET** サブネットアドレス。アドレス範囲が他のサブネット VLAN と重なるような設定はできない

**MASK** SUBNET に対するネットマスク。省略時はサブネットアドレスのクラス標準マスクが適用される

### 例

VLAN yomo にサブネット 172.16.56.0/24 を追加する。

```
ADD VLAN=yomo SUBNET=172.16.56.0 MASK=255.255.255.0
```

### 関連コマンド

ADD VLAN PORT (191 ページ)

DELETE VLAN PORT (239 ページ)

DELETE VLAN SUBNET (242 ページ)

SHOW VLAN (519 ページ)

## CREATE CLASSIFIER

カテゴリー：スイッチング / クラシファイア

ハードウェアパケットフィルター・QoS ポリシー用の構文

```
CREATE CLASSIFIER=rule-id [ETHFORMAT={ETHII-TAGGED|ETHII-UNTAGGED|ANY}]
  [PROTOCOL={protocoltype|IP|ANY}] [MACTYPE={L2UCAST|L2MCAST|L2BCAST|ANY}]
  [MACSADDR={macadd|DHCP Snooping|ANY}] [MACDADDR={macadd|ANY}]
  [VLAN={vlanname|1..4094|ANY}] [TPID={tpid|ANY}] [VLANPRIORITY={0..7|
  ANY}] [INNERTPID={tpid|ANY}] [INNERVLANPRIORITY={0..7|ANY}]
  [INNERVLANID={1..4094|ANY}] [IPSADDR={ipadd[/masklen]|DHCP Snooping|ANY}]
  [IPDADDR={ipadd[/masklen]|ANY}] [IPDSCP={dscp-list|ANY}] [IPTOS={0..7|
  ANY}] [IPPROTOCOL={TCP|UDP|ICMP|IGMP|protocol|ANY}] [TCPSPORT={port|
  port-range|ANY}] [TCPDPORT={port|port-range|ANY}] [TCPFLAGS={ {URG|ACK|
  RST|SYN|FIN}[, ...]|ANY}] [UDPSPORT={port|port-range|ANY}]
  [UDPSPORT={port|port-range|ANY}] [L4SMASK={bitmask|ANY}]
  [L4DMASK={bitmask|ANY}] [L5BYTE01=byteoffset,bytevalue[,bytemask]]
  [L5BYTE02=byteoffset,bytevalue[,bytemask]]
  [L5BYTE03=byteoffset,bytevalue[,bytemask]]
  [L5BYTE04=byteoffset,bytevalue[,bytemask]]
  [L5BYTE05=byteoffset,bytevalue[,bytemask]]
  [L5BYTE06=byteoffset,bytevalue[,bytemask]]
  [L5BYTE07=byteoffset,bytevalue[,bytemask]]
  [L5BYTE08=byteoffset,bytevalue[,bytemask]]
  [L5BYTE09=byteoffset,bytevalue[,bytemask]]
  [L5BYTE10=byteoffset,bytevalue[,bytemask]]
  [L5BYTE11=byteoffset,bytevalue[,bytemask]]
  [L5BYTE12=byteoffset,bytevalue[,bytemask]]
  [L5BYTE13=byteoffset,bytevalue[,bytemask]]
  [L5BYTE14=byteoffset,bytevalue[,bytemask]]
  [L5BYTE15=byteoffset,bytevalue[,bytemask]]
  [L5BYTE16=byteoffset,bytevalue[,bytemask]]
```

IPv6 ハードウェアパケットフィルター用の構文 (IPv6 ルーティングパケット)

```
CREATE CLASSIFIER=rule-id ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6
  [IPSADDR={ip6add/plen|ANY}] [IPDADDR={ip6add/plen|ANY}] [IPDSCP={0..63|
  ANY}] [IPPROTOCOL={TCP|UDP|ICMP|IGMP|protocol|ANY}] [TCPSPORT={port|
  port-range|ANY}] [TCPDPORT={port|port-range|ANY}] [UDPSPORT={port|
  port-range|ANY}] [UDPSPORT={port|port-range|ANY}]
```

IPv6 QoS ポリシー用の構文 (IPv6 ルーティングパケット)

```
CREATE CLASSIFIER=rule-id ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6
```

```
[MACTYPE={L2UCAST|L2MCAST|L2BCAST|ANY}] [MACSADDR={macadd|ANY}]
[MACDADDR={macadd|ANY}] [VLAN={vlanname|1..4094|ANY}] [IPDSCP={0..63|
ANY}] [IPPROTOCOL={TCP|UDP|ICMP|IGMP|protocol|ANY}]
```

**rule-id:** クラシファイア番号 (1～9999)

**macadd:** MAC アドレス (xx-xx-xx-xx-xx-xx の形式)

**protocoltype:** L3 プロトコル (Ethernet) 番号 (16 進数)

**vlanname:** VLAN 名 (1～32 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字は区別しない)

**tpid:** TPID (16 ビット長。16 進数最大 4 文字)

**ipadd:** IP アドレス

**masklen:** マスク長 (0～32)

**dscp-list:** DSCP 値 (0～63。ハイフン、カンマを使った複数指定も可能)

**protocol:** IP プロトコル番号 (1～255)

**port:** TCP/UDP ポート番号 (0～65535)

**port-range:** TCP/UDP ポート番号範囲 (「1-99」のように 2 つの番号をハイフンで区切って指定する。有効範囲は 0～65535)

**bitmask:** マスク値 (16 ビット長。16 進数最大 4 文字)

**ip6add:** IPv6 アドレス

**plen:** プレフィックス長 (0～128 ビット)

**byteoffset:** データ部の先頭バイト (TCP・UDP ヘッダーの直後のバイト) を 0 として数えたオフセット (10 進数。0～37)

**bytevalue:** byteoffset で指定したバイトの内容 (16 進数。00～ff)

**bytemask:** bytevalue に対する AND マスク (16 進数。省略時は ff)

## 解説

クラシファイア (汎用パケットフィルター) を作成する。

クラシファイアはパケットを分類 (Classify = クラス分け) するための条件を定義するもの。ハードウェアパケットフィルター、IPv6 ハードウェアパケットフィルター、ポリシーベース QoS で共通に用いられる (ただし、使用できるパラメーターや構文に違いがあるので注意)。

クラシファイアを作成しただけでは何も行われないことに注意。クラシファイアは、ハードウェアパケットフィルター、IPv6 ハードウェアパケットフィルター、または、QoS ポリシーのフローグループに割り当てて初めて効果を発揮する。

## パラメーター

**CLASSIFIER** クラシファイア番号。この番号は単なる識別子であり、番号の大小は意味を持たない。番号は固定なので、他のクラシファイアを削除しても変更されることはない。また、番号に空きがあってもよい

**ETHFORMAT** Ethernet のフレームフォーマット (エンキャプセレーション)。ETHII-UNTAGGED (Ethernet Version 2。タグなし)、ETHII-TAGGED (Ethernet Version 2。タグ付き)、ANY (すべて) から選択する。ETHII-UNTAGGED、ETHII-TAGGED を指定した場合は、必ず PROTOCOL パラメーターもあわせて指定すること。また、PROTOCOL に IPV6 を指定するときは、本パラメーターに ETHII-TAGGED か ETHII-UNTAGGED を指定する必要がある。省略時は ANY。

**PROTOCOL** レイヤー 3 プロトコルタイプ (Ethertype) フィールド値。特殊なプロトコル名 (IP、ANY) か、定義済みのプロトコル名 (別表を参照) または、16 進表記の Ethertype プロトコル番号で指定する。ETHFORMAT に ETHII-UNTAGGED か ETHII-TAGGED を指定した場合は、必ず本パラメーターもあわせて指定すること (ANY は不可)。省略時は ANY。

**MACTYPE** レイヤー 2 アドレス種別。L2UCAST (ユニキャスト)、L2MCAST (マルチキャスト)、L2BCAST (ブロードキャスト)、ANY (すべて) から選択する。省略時は ANY。

**MACSADDR** 送信元 MAC アドレス。「DHCP Snooping」は、DHCP Snooping の設定時に QoS ポリシーとクラシファイアを組み合わせて使用するための特殊なキーワードで、「送信元 MAC アドレスが DHCP Snooping テーブル (バインディングデータベース) に登録されている」という条件を示す。省略時は ANY。

**MACDADDR** 宛先 MAC アドレス。省略時は ANY。

**VLAN** 入力 VLAN。パケットの入力元が指定した VLAN のときだけマッチする。ただし、IPv6 QoS ポリシー用のクラシファイアでは出力 VLAN の意味になる。省略時は ANY。

**TPID** 802.1Q VLAN タグヘッダーの TPID (Tag Protocol Identifier) 値。2 バイトの 16 進数で指定する。省略時は ANY。

**VLANPRIORITY** 802.1p ユーザープライオリティー (0~7) 値。省略時は ANY。

**INNERTPID** ダブルタグパケットにおける内側 802.1Q VLAN タグヘッダーの TPID (Tag Protocol Identifier) 値。2 バイトの 16 進数で指定する。省略時は ANY。

**INNERVLANPRIORITY** ダブルタグパケットにおける内側 802.1Q VLAN タグヘッダーの 802.1p ユーザープライオリティー (0~7) 値。省略時は ANY。

**INNERVLANID** ダブルタグパケットにおける内側 802.1Q VLAN タグヘッダーの VLAN ID。省略時は ANY。

**IPSADDR** 始点 IPv4/IPv6 アドレス。IP アドレス/マスク長 (IPv4) または IP アドレス/プレフィックス長 (IPv6) の形式で指定する。マスク長、プレフィックス長を省略した場合は、それぞれ 32 ビットマスク/128 ビットプレフィックス (ホストアドレス) と見なされる。「DHCP Snooping」は、DHCP Snooping の設定時に QoS ポリシーとクラシファイアを組み合わせて使用するための特殊なキーワードで、「始点 IP アドレスが DHCP Snooping テーブル (バインディングデータベース) に登録されている」という条件を示す。省略時は ANY

**IPDADDR** 終点 IPv4/IPv6 アドレス。IP アドレス/マスク長 (IPv4) または IP アドレス/プレフィックス長 (IPv6) の形式で指定する。マスク長、プレフィックス長を省略した場合は、それぞれ 32 ビットマスク/128 ビットプレフィックス (ホストアドレス) と見なされる。省略時は ANY

**IPDSCP** IPv4/IPv6 ヘッダーの DSCP (DiffServ Code Point) フィールド値。有効範囲は 0~63。IPv4 の場合は、ハイフン、カンマを使った複数指定も可能。IPTOS とは同時に指定できない。省略時は ANY

**IPTOS** IPv4 ヘッダーの TOS 優先度 (precedence) フィールド値。有効範囲は 0~7。IPDSCP とは同時に指定できない。省略時は ANY。

**IPPROTOCOL** IPv4/IPv6 ヘッダーのプロトコルタイプ (IPv4) / 次ヘッダー (IPv6) フィールド値。定義済みのプロトコル名 (TCP、UDP、ICMP、IGMP) か 10 進表記のプロトコル番号 (1~255。0 も指定できるが、ハードウェアパケットフィルターや QoS ポリシーに割り当てた時点でエラーになるため使用不可) で指定する。なお、TCPSPORT、TCPDPORT パラメーターを使っている場合は、本パラメーターに TCP を指定したものと見なされる (他の値は指定できない)。また、UDPSPORT、UDPDPDPORT パラメーターを使っている場合は、本パラメーターに UDP を指定したものと見なされ



る（他の値は指定できない）。省略時は ANY

**TCPSPORT** TCP 始点ポート。単一のポート番号かポート番号の範囲を指定する。範囲を指定した場合、L4SMASK パラメーターは無効。省略時は ANY

**TCPDPORT** TCP 終点ポート。単一のポート番号かポート番号の範囲を指定する。範囲を指定した場合、L4DMASK パラメーターは無効。省略時は ANY

**TCPFLAGS** TCP 制御フラグ。カンマ区切りで複数指定が可能。本パラメーターでは、指定したフラグだけがチェック対象となる（指定しなかったフラグの状態には関知しない）。指定したフラグがすべてが立っていればマッチ、それ以外の場合は非マッチと判定される。省略時は ANY

**UDPSPORT** UDP 始点ポート。単一のポート番号かポート番号の範囲を指定する。範囲を指定した場合、L4SMASK パラメーターは無効。省略時は ANY

**UDPDPOR** UDP 終点ポート。単一のポート番号かポート番号の範囲を指定する。範囲を指定した場合、L4DMASK パラメーターは無効。省略時は ANY

**L4SMASK** TCP/UDP 始点ポートに対する AND マスク。「f800」のような 16 ビットの 16 進数で指定する。本パラメーターは、必ず TCPSPORT、UDPSPORT のどちらかと組で指定すること。またこのとき、TCPSPORT、UDPSPORT には単一のポート番号を指定すること。

**L4DMASK** TCP/UDP 終点ポートに対する AND マスク。「f800」のような 16 ビットの 16 進数で指定する。本パラメーターは、必ず TCPDPORT、UDPDPOR のどちらかと組で指定すること。またこのとき、TCPDPORT、UDPDPOR には単一のポート番号を指定すること。

**L5BYTE01 ~ L5BYTE16** TCP/UDP パケットのデータ部の値。1 バイトごとに、byteoffset（位置）、bytevalue（値）、bytemask（マスク）を指定する（bytemask は省略可）。本パラメーターは、必ず L5BYTE01、L5BYTE02..の順に使用しなければならない。またこのとき、byteoffset の値がしだいに大きくなるように設定しなくてはならない。本パラメーターは、IPv4 上の有効な TCP・UDP パケットに対してのみ機能するが、これは自動的に行われるので、L5BYTExx パラメーターを指定するときに、PROTOCOL、IPPROTOCOL パラメーターを指定する必要はない。

IP ETHII	0800 (Ethernet Version 2)
X.75 Internet	0801 (Ethernet Version 2)
NBS Internet	0802 (Ethernet Version 2)
ECMA Internet	0803 (Ethernet Version 2)
Chaosnet	0804 (Ethernet Version 2)
X.25 Level 3	0805 (Ethernet Version 2)
ARP	0806 (Ethernet Version 2)
XNS Compat	0807 (Ethernet Version 2)
Banyan Systems	0BAD (Ethernet Version 2)
BBN Simnet	5208 (Ethernet Version 2)
DEC MOP Dump/Ld	6001 (Ethernet Version 2)
DEC MOP Rem Cons	6002 (Ethernet Version 2)
DEC DECNET	6003 (Ethernet Version 2)
DEC LAT	6004 (Ethernet Version 2)
DEC Diagnostic	6005 (Ethernet Version 2)

DEC Customer	6006 ( Ethernet Version 2 )
DEC LAVC	6007 ( Ethernet Version 2 )
RARP	8035 ( Ethernet Version 2 )
DEC LANBridge	8038 ( Ethernet Version 2 )
DEC Encryption	803D ( Ethernet Version 2 )
Appletalk	809B ( Ethernet Version 2 )
IBM SNA	80D5 ( Ethernet Version 2 )
AppleTalk AARP	80F3 ( Ethernet Version 2 )
IPX EthII	8137 ( Ethernet Version 2 )
SNMP	814C ( Ethernet Version 2 )
IPv6	86DD ( Ethernet Version 2 )

表 32: 定義済みのプロトコル名一覧

マスク	対象ポート数	対象ポート範囲	ポート範囲の具体例
FFFF	1	指定したポートだけが対象	0、1、2 ... 65535
FFFE	2	$2n \sim 2(n+1) - 1$	0 ~ 1、2 ~ 3 ... 65534 ~ 65535
FFFC	4	$4n \sim 4(n+1) - 1$	0 ~ 3、4 ~ 7 ... 65532 ~ 65535
FFF8	8	$8n \sim 8(n+1) - 1$	0 ~ 7、8 ~ 15 ... 65528 ~ 65535
FFF0	16	$16n \sim 16(n+1) - 1$	0 ~ 15、16 ~ 31 ... 65520 ~ 65535
FFE0	32	$32n \sim 32(n+1) - 1$	0 ~ 31、32 ~ 63 ... 65504 ~ 65535
FFC0	64	$64n \sim 64(n+1) - 1$	0 ~ 63、64 ~ 127 ... 65472 ~ 65535
FF80	128	$128n \sim 128(n+1) - 1$	0 ~ 127、128 ~ 255 ... 65408 ~ 65535
FF00	256	$256n \sim 256(n+1) - 1$	0 ~ 255、256 ~ 511 ... 65280 ~ 65535
FE00	512	$512n \sim 512(n+1) - 1$	0 ~ 511、512 ~ 1023 ... 65024 ~ 65535
FC00	1024	$1024n \sim 1024(n+1) - 1$	0 ~ 1023、1024 ~ 2047 ... 64512 ~ 65535
F800	2048	$2048n \sim 2048(n+1) - 1$	0 ~ 2047、2048 ~ 4095 ... 63488 ~ 65535
F000	4096	$4096n \sim 4096(n+1) - 1$	0 ~ 4095、4096 ~ 8191 ... 61440 ~ 65535
E000	8192	$8192n \sim 8192(n+1) - 1$	0 ~ 8191、8192 ~ 16383 ... 57344 ~ 65535
C000	16384	$16384n \sim 16384(n+1) - 1$	0 ~ 16383、16384 ~ 32767、32768 ~ 49151、49152 ~ 65535
8000	32768	$32768n \sim 32768(n+1) - 1$	0 ~ 32767、32768 ~ 65535
0000	65536	すべてのポートが対象	0 ~ 65535

表 33: L4SMASK/L4DMASK 設定早見表

## 例

SSH サーバー宛てのパケットにマッチするクラシファイア「100」を作成する。

```
CREATE CLASSIFIER=100 TCPDPORT=22
```

IPv6 パケットにマッチするクラシファイア「201」を作成する。

```
CREATE CLASSIFIER=201 ETHFORMAT=ETHII-UNTAGGED PROTOCOL=IPV6
```

サブネット 172.16.10.128/28 からの UDP パケットにマッチするクラシファイア「10」を作成する。

```
CREATE CLASSIFIER=10 IPSADDR=172.16.10.128/28 IPPROTOCOL=UDP
```

サブネット 3ffe:b80:3c:10::/64 の Web クライアントが送信する IPv6 ルーティングパケットにマッチするクラシファイア「110」を作成する。

```
CREATE CLASSIFIER=110 ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6
IPSADDR=3ffe:b80:3c:10::/64 IPPROTOCOL=TCP TCPDPORT=80
```

すべてのパケットにマッチするクラシファイア「9999」を作成する。

```
CREATE CLASSIFIER=9999
```

## 備考・注意事項

IGMP を有効にしている場合は、IGMP モジュールの処理が優先されるため、IPPROTOCOL=IGMP を指定しても IGMP パケットをフィルタリングできない。

L5BYTEXX パラメーターは、必ず L5BYTE01、L5BYTE02..の順に使用しなければならない。たとえば、L5BYTE02 だけを指定したり、L5BYTE01 と L5BYTE03 だけを設定したりすることはできない。またこのとき、byteoffset の値がしだいに大きくなるように設定しなくてはならない。すなわち、L5BYTE01 の byteoffset が 2 なら、L5BYTE02 の byteoffset は 3 以上でなくてはならない。

L5BYTExx パラメーターでマッチングできるのは、IP パケットの先頭から 80Byte 以内だけであることに注意。IP パケットや TCP パケットにオプションがついている場合など、L5BYTExx パラメーターで指定したバイトが IP パケットの先頭から 80Byte より後ろに来た場合は、該当パケットの値が bytevalue、bytemask の指定と一致していても、クラシファイアはマッチしない。

L5BYTExx パラメーターは、IPv4 上の有効な TCP・UDP パケットに対してのみ機能する。これは自動的に行われるので、L5BYTExx パラメーターを指定するときに、PROTOCOL、IPPROTOCOL パラメーターを指定する必要はない。

## 関連コマンド

ADD QOS FLOWGROUP ( 179 ページ )

ADD SWITCH ACCELERATOR HWFILTER ( 184 ページ )

ADD SWITCH HWFILTER ( 188 ページ )

DELETE QOS FLOWGROUP ( 231 ページ )

DELETE SWITCH ACCELERATOR HWFILTER ( 235 ページ )

[DELETE SWITCH HWFILTER \( 237 ページ \)](#)

[DESTROY CLASSIFIER \( 243 ページ \)](#)

[SET CLASSIFIER \( 325 ページ \)](#)

[SHOW CLASSIFIER \( 395 ページ \)](#)

## CREATE EPSR

カテゴリー：スイッチング / イーサネットリングプロテクション (EPSR)

```
CREATE EPSR=epsrname MODE=MASTER CONTROLVLAN={vlanname|1..4094}
    PRIMARYPORT=port-number [HELLOTIME=timer1] [FAILOVERTIME=timer2]
    [RINGFLAPTIME=0..65535] [TRAP={ENABLED|DISABLED}]
```

```
CREATE EPSR=epsrname MODE=TRANSIT CONTROLVLAN={vlanname|1..4094}
    [TRAP={ENABLED|DISABLED}]
```

*epsrname*: EPSR ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。ただし、「ALL」は指定できない。大文字小文字を区別しない)

*vlanname*: VLAN 名 (1~32 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字は区別しない)

*port-number*: スイッチポート番号 (1~)

*timer1*: 時間 (100ms ~ 32767s)

*timer2*: 時間 (200ms ~ 65535s)

### 解説

EPSR ドメインを作成する。

本コマンド実行時は、次のルールが適用される。

- ・1 台のスイッチ上に作成できる EPSR ドメインは最大 16 個
- ・コントロール VLAN の所属ポートはちょうど 2 ポートでなくてはならない (ただし、トランクグループは全体で 1 ポートと見なす)。また、これらのポートはタグ付き設定でなくてはならない。
- ・データ VLAN、コントロール VLAN を問わず、他の EPSR ドメインに追加されている VLAN はコントロール VLAN として指定できない
- ・トランクポートは、グループ内のポートが 1 つでもリンクアップしていれば全体としてリンクアップのステータスとなる。また、SNMP トラップでトランクポートのポート番号を通知するときは、トランクグループ内でポート番号のもっとも小さいポートの番号が使われる。
- ・LACP、スパニングツリープロトコル (STP/RSTP)、ダイナミック VLAN (ポート認証) が有効なポートは EPSR ドメインに追加できない。
- ・マルチプルスパニングツリープロトコル (MSTP) が有効なときは、EPSR を使用できない。

### パラメーター

**EPSR** EPSR ドメイン名

**MODE** EPSR ドメインにおける役割。MASTER (マスターノード)、TRANSIT (トランジットノード) から選択する。

**CONTROLVLAN** コントロール VLAN。VLAN 名または VLAN ID (VID) で指定する。

**PRIMARYPORT** (マスターノードのみ) プライマリーポート。

**HELLOTIME** (マスターノードのみ) Healthcheck メッセージの送信間隔。数値だけで指定する場合の単位は s (秒)。ただし、数値のあとに「s」、「ms」をつけると、それぞれ「秒」、「ミリ秒」の意味に

なる。「ms」を指定する場合は、100ms の倍数で指定すること。デフォルトは 1s (1 秒)。

**FAILOVERTIME** (マスターノードのみ) Healthcheck メッセージのタイムアウト時間。HELLOTIME の 2 倍の値に設定すること。マスターノードは、プライマリーポートから送信した Healthcheck メッセージが、ここで指定した時間内にセカンダリーポートに到達しないとリングに障害が発生したと判断する。数値だけで指定する場合の単位は s (秒)。ただし、数値のあとに「s」、「ms」をつけると、それぞれ「秒」、「ミリ秒」の意味になる。「ms」を指定する場合は、100ms の倍数で指定すること。デフォルトは 2s (2 秒)。

**RINGFLAPTIME** (マスターノードのみ) リング障害の回復後、Failed 状態から Complete 状態に移る前に待機する最小時間 (秒)。この時間内にリング障害が回復しても、Failed 状態を維持する。リングの状態が頻繁に切り替わるような場合、この値を調整することで不必要な状態遷移を防ぐことができる。デフォルトは 0。

**TRAP** EPSR ドメインの状態が変化したときに SNMP トラップ (SNMPv2c、SNMPv3 形式のみ) を送信するかどうか。デフォルトは ENABLED (送信する)。

## 例

EPSR ドメイン「blues」を作成し、マスターノードとして動作するよう設定する。コントロール VLAN には VLAN「blues\_control」を、プライマリーポートにはポート 1 を指定する。

```
CREATE EPSR=blues MODE=MASTER CONTROLVLAN=blues_control PRIMARYPORT=1
```

EPSR ドメイン「blues」を作成し、トランジットノードとして動作するよう設定する。コントロール VLAN には VLAN「blues\_control」を指定する。

```
CREATE EPSR=blues MODE=TRANSIT CONTROLVLAN=blues_control
```

## 備考・注意事項

EPSR が使用するスイッチポートでは、自動的にインGRESSフィルタリング (SET SWITCH PORT コマンドの INFILTERING パラメーター) が有効になる。同パラメーターは、EPSR ドメインを削除して該当ポートを EPSR で使用されないようにするまで変更できない。

コントロール VLAN にはレイヤー 3 以上の設定 (IP アドレスの設定など) を行わないこと (コントロール VLAN はリングを構成・制御するためだけに存在する)。

EPSR ドメインの状態変化を知らせる SNMP トラップを利用するためには、SNMPv2c のトラップホストまたは SNMPv3 のターゲットを設定する必要がある。SNMPv1 トラップホストの設定だけでは、EPSR の SNMP トラップは利用できないので注意。

## 関連コマンド

ADD EPSR DATAVLAN (175 ページ)

CREATE VLAN (225 ページ)

DESTROY EPSR ( 244 ページ )

ENABLE EPSR ( 284 ページ )

SET EPSR ( 332 ページ )

SET EPSR PORT ( 334 ページ )

SHOW EPSR ( 411 ページ )

## CREATE MSTP MSTI

カテゴリー：スイッチング / マルチプルスパニングツリープロトコル (MSTP)

**CREATE MSTP MSTI=instance** [PRIORITY=0..65535]

*instance*: MST インスタンス ID (1 ~ 4094)

### 解説

MST インスタンスを作成する。

1 つのリージョン内、もしくは、1 台のスイッチ上に作成できる MST インスタンスの数は最大 64 個。  
作成した MST インスタンスに VLAN を追加するには、ADD MSTP MSTI VLAN コマンドを使う。

### パラメーター

**MSTI** MST インスタンス ID。0 は CIST (Common and Internal Spanning Tree) 用に予約されているため指定できない。

**PRIORITY** 該当 MST インスタンスにおけるブリッジプライオリティ。小さいほど優先度が高く、MST インスタンス内のルートブリッジ (リージョナルルート) になる可能性が高くなる。設定できる値の範囲は 0 ~ 65535 だが、実際に使用される値は 4096 の倍数に丸められる (指定値が 4096 の倍数でない場合、指定値よりも小さい直近の倍数が使われる)。デフォルトは 32768。

### 例

MST インスタンス「1」を作成する。

```
CREATE MSTP MSTI=1
```

### 関連コマンド

ADD MSTP MSTI VLAN (178 ページ)

DESTROY MSTP MSTI (245 ページ)

SHOW MSTP (425 ページ)

SHOW MSTP MSTI (436 ページ)



## CREATE QOS FLOWGROUP

カテゴリー：スイッチング / QoS

```
CREATE QOS FLOWGROUP=flow-list [PREMARKING={USEMARKVALUE|USEDSCP|NONE}]
    [MARKVALUE={0..63|NONE}] [DESCRIPTION=string] [ACTION={FORWARD|DISCARD|
    SENDMIRROR|SENDVLANPORT|FORWARD, SENDMIRROR|SENDMIRROR, SENDVLANPORT|
    NONE}] [VLAN=1..4094 PORT=port-number]
```

*flow-list*: フローグループ番号 (0~1023。ハイフン、カンマを使った複数指定も可能)

*string*: 文字列 (1~15 文字。空白を含む場合はダブルクォートで囲む)

*port-number*: スイッチポート番号 (1~)

### 解説

フローグループを作成する。

フローグループは、クラシファイア (汎用パケットフィルタ) を用いて、パケットを一連の「フロー」として定義するもの。トラフィッククラスよりも細かい QoS 制御を行いたい場合は、フローグループごとにプレマーキング (QoS パラメーターの初期値割り当て) の設定をすることができる。

### パラメーター

**FLOWGROUP** フローグループ番号

**PREMARKING** プレマーキングの動作を指定する。具体的には、フローグループに割り当てる QoS パラメーター (DSCP 値、帯域クラス、送信キュー、802.1p プライオリティー値) をプレマーキング用 DSCP MAP テーブルから検索するときに、どの値をインデックスとして使うかを指定する。USEMARKVALUE を指定した場合は、MARKVALUE パラメーターの値をインデックスとして使う。USEDSCP を指定した場合は、パケットの DSCP フィールド値をインデックスとして使う。いずれの場合も、DSCP MAP テーブルのもう 1 つのインデックスである帯域クラスは 1 を使う。NONE を指定した場合は、フローグループではプレマーキングを行わず、トラフィックグループの処理に移る。省略時は NONE。なお、トラフィッククラスとフローグループの両方で本パラメーターが指定されている場合は、フローグループの設定が使われる。なお、IPv6 ルーティングパケットに対する QoS ポリシーでは、USEDSCP を使用できないので注意すること (指定しても効果がない)。

**MARKVALUE** PREMARKING パラメーターに USEMARKVALUE を指定した場合、プレマーキング用 DSCP MAP テーブルの検索インデックスとして使う DSCP 値を指定する。省略時は NONE

**DESCRIPTION** フローグループの説明 (メモとして使う)

**ACTION** 本フローグループに対するアクション。アクションの詳細は別表を参照のこと。アクションはフローグループとトラフィッククラスの両方に設定できるが、フローグループのアクションのほうが優先される (ただし、フローグループのアクションが NONE のときは、トラフィッククラスのアクションが実行される)。省略時は NONE

**VLAN** 本フローグループに属するパケットの出力先 VLAN。ACTION パラメーターに SENDVLANPORT を指定したときのみ有効かつ必須。本パラメーターは、必ず PORT パラメーターと組で指定

すること。

**PORT** 本フローグループに属するパケットの出力先ポート。ACTION パラメーターに SENDVLANPORT を指定したときのみ有効かつ必須。本パラメーターは、必ず VLAN パラメーターと組で指定すること。

FORWARD	パケットを通常どおり出力する
DISCARD	パケットを破棄する
SENDVLANPORT	パケットの出力先を VLAN パラメーターと PORT パラメーターで指定されたポートに変更する。このとき、出力ポート (PORT) は出力 VLAN (VLAN) に所属していなくてはならないので、設定には注意すること
SENDMIRROR	パケットのコピーをミラーポートから出力する。あらかじめ、SET SWITCH MIRROR コマンドでミラーポートを指定し、ENABLE SWITCH MIRROR コマンドでポートミラーリング機能を有効にしておく必要がある
FORWARD,SENDMIRROR	FORWARD と SENDMIRROR の両方の処理を行う。SENDMIRROR だけ指定した場合と同じ動作
SENDMIRROR,SENDVLANPORT	SENDMIRROR と SENDVLANPORT の両方の処理を行う
NONE	本フローグループが所属しているトラフィッククラスのアクションにしたがってパケットを処理する

表 34: ACTION パラメーターに指定できるオプション

## 例

フローグループ「50」を作成する。このグループに属するパケットには、プレマーキング用 DSCPMAP テーブルのインデックス 50 番、帯域クラス 1 のエントリで指定された DSCP 値、帯域クラス、送信キュー、802.1p プライオリティー値を割り当てる。

```
CREATE QOS FLOWGROUP=50 PREMARKING=USEMARKVALUE MARKVALUE=50
```

## 備考・注意事項

ACTION、VLAN、PORT パラメーターは、IPv6 アクセラレーター用の QoS ポリシーでは未サポート。

## 関連コマンド

ADD QOS FLOWGROUP ( 179 ページ )

DELETE QOS FLOWGROUP ( 231 ページ )

DESTROY QOS FLOWGROUP ( 246 ページ )

SET QOS DSCPMAP ( 357 ページ )

SET QOS FLOWGROUP ( 359 ページ )

SHOW QOS DSCPMAP ( 461 ページ )

SHOW QOS FLOWGROUP ( 463 ページ )

## CREATE QOS POLICY

カテゴリー：スイッチング / QoS

```
CREATE QOS POLICY=qos-list [DTCDROPBWCLASS3={YES|NO}]
[DTCIGNOREBWCLASS={YES|NO}] [DTCMAXBANDWIDTH={bandwidth|NONE}]
[DTCMAXBURSTSIZE=burstsize] [DTCMINBANDWIDTH={bandwidth|NONE}]
[DTCMINBURSTSIZE=burstsize] [DTCPREMARKING={USEMARKVALUE|USEDSCP|NONE}]
[DTCREMARKING={USEDSCPMAP|PRIORITY|PRIO+BWCLASS|BWCLASS|NONE}]
[MARKVALUE={0..63|NONE}] [DESCRIPTION=string] [DTCACTION={FORWARD|
DISCARD|SENDMIRROR|SENDVLANPORT|FORWARD,SENDMIRROR|
SENDMIRROR,SENDVLANPORT}] [VLAN=1..4094 PORT=port-number]
```

*qos-list*: QoS ポリシー番号 (0~255。ハイフン、カンマを使った複数指定も可能)

*bandwidth*: 帯域幅 (1~16998400Kbps)

*burstsize*: バーストサイズ (0~268435455Byte)

*string*: 文字列 (1~15 文字。空白を含む場合はダブルクォートで囲む)

*port-number*: スイッチポート番号 (1~)

### 解説

QoS ポリシーを作成する。

QoS ポリシーは受信パケットに対して様々な QoS を適用するためのメカニズムで、ユーザー定義のトラフィッククラス (複数) とデフォルトトラフィッククラス (1 つ) から構成される。

QoS ポリシーをスイッチポートに関連付けると、同ポートで受信したトラフィックに対して、該当するトラフィッククラスで定められた QoS 処理が行われる。

本コマンドでは、QoS ポリシーの作成と同時に、デフォルトトラフィッククラスの各種パラメーターを設定できる。

### パラメーター

**POLICY** QoS ポリシー番号

**DTCDROPBWCLASS3** 本ポリシーのデフォルトトラフィッククラスにおいて、最大帯域設定 (DTCMAXBANDWIDTH と DTCMAXBURSTSIZE) を上回るレートで受信したパケットをキューイング前に無条件で破棄するかどうか。YES を指定した場合、超過分のパケットは送信キューに格納される前に破棄される。NO を指定した場合、超過分のパケットは「帯域クラス 3 (使いすぎクラス)」に分類されるだけでただちには破棄されない。ただし、RED アルゴリズムの設定により、送信キューにおいて「帯域クラス 3」を優先的に破棄するような設定が可能。省略時は NO。

**DTCIGNOREBWCLASS** 本ポリシーのデフォルトトラフィッククラスに対して最大・最小帯域の設定 (DTCMAXBANDWIDTH、DTCMINBANDWIDTH) がなされている場合、メータリング時にプレマーキングで割り当てられた「帯域クラス」を考慮するか無視するかを指定する。YES を指定した場合、プレマーキングで割り当てられた帯域クラスは無視され、実際の帯域使用量にのみ基づいて帯域クラスが決定される。NO を指定した場合は、プレマーキングで割り当てられた帯域クラスが、そ

のままメータリング結果として採用される。省略時は NO。

**DTCMAXBANDWIDTH** 本ポリシーのデフォルトトラフィッククラスに割り当てる最大帯域幅 (Kbps)。デフォルトトラフィッククラスに割り当てる帯域は、原則としてここで指定した値までに制限される。数値だけで指定する場合の単位は Kbps。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「Kbps」、「Mbps」、「Gbps」の意味になる。「M」、「G」を指定する場合は、「2.256G」や「128.4M」のように小数を指定することもできる。QoS ポリシーを適用するスイッチポートの帯域と矛盾しないように設定すること。省略時は NONE。

**DTCMAXBURSTSIZE** デフォルトトラフィッククラスの最大帯域幅設定 (DTCMAXBANDWIDTH) に対する、最大許容バーストサイズ (Byte)。トラフィックの流入量が DTCMAXBANDWIDTH を超えた場合に、DTCMAXBANDWIDTH 超過分としてバッファリング可能な最大データ量を指定する。数値だけで指定する場合の単位は Byte。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「Kbyte」、「Mbyte」、「Gbyte」の意味になる。「K」、「M」、「G」を指定する場合は、「2.256G」や「128.4M」のように小数を指定することもできる。バーストサイズが DTCMAXBURSTSIZE を上回った場合、超過分のパケットはキューイング前に破棄されるか (DTCDROPBWCLASS3=YES のとき)、帯域クラス 3 に分類される (DTCDROPBWCLASS3=NO のとき)。省略時は 0。

**DTCMINBANDWIDTH** 本ポリシーのデフォルトトラフィックに割り当てる最小帯域幅 (Kbps)。デフォルトトラフィッククラスには、原則としてここで指定した帯域が確保される。数値だけで指定する場合の単位は Kbps。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「Kbps」、「Mbps」、「Gbps」の意味になる。「M」、「G」を指定する場合は、「2.256G」や「128.4M」のように小数を指定することもできる。QoS ポリシーを適用するスイッチポートの帯域と矛盾しないように設定すること。省略時は NONE。

**DTCMINBURSTSIZE** デフォルトトラフィッククラスの最小帯域幅設定 (DTCMINBANDWIDTH) に対する、「帯域クラス 1」の最大許容バーストサイズ (Byte)。DTCMINBANDWIDTH が NONE のときは、最大帯域幅設定 (DTCMAXBANDWIDTH) に対する、「帯域クラス 2」の最大許容バーストサイズ (Byte)。数値だけで指定する場合の単位は Byte。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「Kbyte」、「Mbyte」、「Gbyte」の意味になる。「K」、「M」、「G」を指定する場合は、「2.256G」や「128.4M」のように小数を指定することもできる。DTCMINBANDWIDTH が NONE のときは、DTCMAXBURSTSIZE よりも小さい値でなくてはならない。詳細は解説編を参照。省略時は 0。

**DTCPREMARKING** 本ポリシーのデフォルトトラフィッククラスに対するプレマーキングの動作を指定する。具体的には、デフォルトトラフィッククラスに割り当てる QoS パラメータをプレマーキング用 DSCPMAP テーブルから検索するときに、どの値をインデックスとして使うかを指定する。USEMARKVALUE を指定した場合は、MARKVALUE パラメータの値をインデックスとして使う。USEDSCP を指定した場合は、パケットの DSCP フィールド値をインデックスとして使う。いずれの場合も、DSCPMAP テーブルのもう 1 つのインデックスである帯域クラスは 1 を使う。NONE を指定した場合は、プレマーキングを行わずに、メータリングの処理に移る。省略時は NONE。なお、IPv6 ルーティングパケットに対する QoS ポリシーでは、USEDSCP を使用できないので注意すること (指定しても効果がない)。

**DTCREMARKING** 本ポリシーのデフォルトトラフィッククラスに対するリマーキングの動作を指定する。具体的には、メータリング後の QoS パラメータ書き換え動作を何に基づいて実施するか、および、どのパラメータを書き換えるかを指定する。USEDSCPMAP を指定した場合は、リマーキング直前の帯域クラスとパケットの DSCP 値をインデックスとしてリマーキング用 DSCPMAP

テーブルを検索し、DSCP 値、帯域クラス、送信キュー、802.1p プライオリティー値を書き換える。PRIORITY、PRIO+BWCLASS を指定した場合は、リマーケティング直前の送信キューと帯域クラスをインデックスとして QUEUE2PRIOMAP テーブルを検索し、802.1p プライオリティー値を書き換える。BWCLASS、NONE を指定した場合は書き換えを行わない。省略時は NONE。なお、PRIORITY と PRIO+BWCLASS、BWCLASS と NONE はそれぞれ同じ意味になる。また、IPv6 ルーティングパケットに対する QoS ポリシーでは、USEDSCPMAP を使用できないので注意すること（指定しても効果がない）。

**MARKVALUE** PREMARKING パラメーターに USEMARKVALUE を指定した場合、プレマーケティング用 DSCPMAP テーブルの検索インデックスとして使う DSCP 値を指定する。省略時は NONE

**DESCRIPTION** ポリシーの説明（メモとして使う）。POLICY パラメーターに複数の番号を指定した場合は、すべてのポリシーに同じメモ文字列が設定される

**DTCACTION** 本ポリシーのデフォルトトラフィッククラスに対するアクション。アクションの詳細は別表を参照のこと。アクションはフローグループとトラフィッククラスの両方に設定できるが、フローグループのアクションのほうが優先される（ただし、フローグループのアクションが NONE のときは、トラフィッククラスのアクションが実行される）。省略時は FORWARD

**VLAN** 本ポリシーのデフォルトトラフィッククラスに属するパケットの出力先 VLAN。DTCACTION パラメーターに SENDVLANPORT を指定したときのみ有効かつ必須。本パラメーターは、必ず PORT パラメーターと組で指定すること。

**PORT** 本ポリシーのデフォルトトラフィッククラスに属するパケットの出力先ポート。DTCACTION パラメーターに SENDVLANPORT を指定したときのみ有効かつ必須。本パラメーターは、必ず VLAN パラメーターと組で指定すること。

FORWARD	パケットを通常どおり出力する
DISCARD	パケットを破棄する
SENDVLANPORT	パケットの出力先を VLAN パラメーターと PORT パラメーターで指定されたポートに変更する。このとき、出力ポート（PORT）は出力 VLAN（VLAN）に所属していなくてはならないので、設定には注意すること
SENDMIRROR	パケットのコピーをミラーポートから出力する。あらかじめ、SET SWITCH MIRROR コマンドでミラーポートを指定し、ENABLE SWITCH MIRROR コマンドでポートミラーリング機能を有効にしておく必要がある
FORWARD,SENDMIRROR	FORWARD と SENDMIRROR の両方の処理を行う。SEND-MIRROR だけ指定した場合と同じ動作
SENDMIRROR,SENDVLANPORT	SENDMIRROR と SENDVLANPORT の両方の処理を行う

表 35: DTCACTION パラメーターに指定できるオプション

## 例

QoS ポリシー「10」を作成する。

CREATE QOS POLICY=10

### 備考・注意事項

DTC ACTION、VLAN、PORT パラメーターは、IPv6 アクセラレーター用の QoS ポリシーでは未サポート。

### 関連コマンド

ADD QOS POLICY ( 180 ページ )  
DELETE QOS POLICY ( 232 ページ )  
DESTROY QOS POLICY ( 247 ページ )  
SET QOS DSCPMAP ( 357 ページ )  
SET QOS POLICY ( 361 ページ )  
SET QOS PORT ( 365 ページ )  
SET QOS QUEUE2PRIOMAP ( 370 ページ )  
SHOW QOS DSCPMAP ( 461 ページ )  
SHOW QOS POLICY ( 465 ページ )  
SHOW QOS QUEUE2PRIOMAP ( 472 ページ )



## CREATE QOS RED

カテゴリー：スイッチング / QoS

**CREATE QOS RED=red-id** [DESCRIPTION=string]

*red-id*: RED カーブセット番号 (2~4)

*string*: 文字列 (1~15 文字。空白を含む場合はダブルクォートで囲む)

### 解説

RED (Random Early Detection/Discard) アルゴリズムの動作を規定する RED カーブセットを作成する。本製品のスイッチポートは各々 8 個の送信キューを持っている。通常は、キューがあふれると超過分のパケットを破棄する (Tail-drop アルゴリズム)。

これに対し、RED (Random Early Detection/Discard) は、キュー長が制限に達しないうちに、徐々にパケット破棄率を高くしていくことで、輻輳回避やより細やかな帯域制御を実現するアルゴリズム。

RED の設定は、キュー長とパケット破棄率の関係を示す「RED カーブ」を定義することによって行う。本コマンドでは、RED カーブの集合である「RED カーブセット」を作成する。作成直後の RED カーブセットに含まれる RED カーブはデフォルト値を持つので、これを変更するには SET QOS RED コマンドを使う。詳細は解説編を参照のこと。

実際に RED を使用するには、SET QOS PORT コマンドの RED パラメーターでスイッチポートに RED カーブセットを割り当てる必要がある。RED パラメーターに NONE (デフォルト値) を指定した場合は、Tail-drop 動作となる。

なお、デフォルトの RED カーブセット「1」の設定の一部は、Tail-drop にも使用される (STOP1、STOP2、STOP3 パラメーターが、それぞれ帯域クラス 1、2、3 の最大キュー長を示す)。

### パラメーター

**RED** RED カーブセット番号。1 はデフォルトの RED カーブセットが使っているため指定できない

**DESCRIPTION** RED カーブセットの説明 (メモとして使う)

### 例

RED カーブセット「2」を作成する。

```
CREATE QOS RED=2 DESCRIPTION="Sample RED curve set"
```

### 関連コマンド

DESTROY QOS RED (248 ページ)

SET QOS PORT (365 ページ)



SET QOS RED ( 371 ページ )

SHOW QOS RED ( 474 ページ )

## CREATE QOS TRAFFICCLASS

カテゴリー：スイッチング / QoS

```
CREATE QOS TRAFFICCLASS=tc-list [DROPBWCLASS3={YES|NO}]
    [IGNOREBWCLASS={YES|NO}] [MAXBANDWIDTH={bandwidth|NONE}]
    [MAXBURSTSIZE=burstsize] [MINBANDWIDTH={bandwidth|NONE}]
    [MINBURSTSIZE=burstsize] [PREMARKING={USEMARKVALUE|USEDSCP|NONE}]
    [REMARKING={USEDSCPMAP|PRIORITY|PRIO+BWCLASS|BWCLASS|NONE}]
    [MARKVALUE={0..63|NONE}] [DESCRIPTION=string] [ACTION={FORWARD|DISCARD|
    SENDMIRROR|SENDVLANPORT|FORWARD, SENDMIRROR|SENDMIRROR, SENDVLANPORT}]
    [VLAN=1..4094 PORT=port-number]
```

*tc-list*: トラフィッククラス番号 (0~1023。ハイフン、カンマを使った複数指定も可能)

*bandwidth*: 帯域幅 (1~16998400Kbps)

*burstsize*: バーストサイズ (0~268435455Byte)

*string*: 文字列 (1~15 文字。空白を含む場合はダブルクォートで囲む)

*port-number*: スイッチポート番号 (1~)

### 解説

トラフィッククラスを作成する。

トラフィッククラスは、同等の QoS (帯域) を与えるべきフローグループをひとまとめにしたもの。トラフィッククラスは、複数のフローグループで構成される。

ポリシーベース QoS では、トラフィッククラスごとに最大・最小帯域幅、プレマーキング、リマーキングの設定が可能。トラフィッククラスは、QoS ポリシーに割り当てることによって効果を発揮する。QoS ポリシーには、ユーザー定義のトラフィッククラスに加え、暗黙のデフォルトトラフィッククラスが存在する。

### パラメーター

**TRAFFICCLASS** トラフィッククラス番号

**DROPBWCLASS3** 本トラフィッククラスにおいて、最大帯域設定 (MAXBANDWIDTH と MAXBURSTSIZE) を上回るレートで受信したパケットをキューイング前に無条件で破棄するかどうか。YES を指定した場合、超過分のパケットは送信キューに格納される前に破棄される。NO を指定した場合、超過分のパケットは「帯域クラス 3 (使いすぎクラス)」に分類されるだけでただちに破棄されない。ただし、RED アルゴリズムの設定により、送信キューにおいて「帯域クラス 3」を優先的に破棄するような設定が可能。省略時は NO。

**IGNOREBWCLASS** 本トラフィッククラスに対して最大・最小帯域の設定 (MAXBANDWIDTH、MINBANDWIDTH) がなされている場合、メータリング時にプレマーキングで割り当てられた「帯域クラス」を考慮するか無視するかを指定する。YES を指定した場合、プレマーキング時に割り当てられた帯域クラスは無視され、実際の帯域使用量にのみ基づいて帯域クラスが決定される。NO を指定した場合は、プレマーキングで割り当てられた帯域クラスが、そのままメータリング結果として採用される。省略時は NO。

**MAXBANDWIDTH** トラフィッククラスに割り当てる最大帯域幅 (Kbps)。トラフィッククラスに割り当てる帯域は、原則としてここで指定した値までに制限される。数値だけで指定する場合の単位は Kbps。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「Kbps」、「Mbps」、「Gbps」の意味になる。「M」、「G」を指定する場合は、「2.256G」や「128.4M」のように小数を指定することもできる。QoS ポリシーを適用するスイッチポートの帯域と矛盾しないように設定すること。省略時は NONE。

**MAXBURSTSIZE** トラフィッククラスの最大帯域幅設定 (MAXBANDWIDTH) に対する、最大許容バーストサイズ (Byte)。トラフィックの流入量が MAXBANDWIDTH を超えた場合に、MAXBANDWIDTH 超過分としてバッファリング可能な最大データ量を指定する。数値だけで指定する場合の単位は Byte。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「Kbyte」、「Mbyte」、「Gbyte」の意味になる。「K」、「M」、「G」を指定する場合は、「2.256G」や「128.4M」のように小数を指定することもできる。バーストサイズが MAXBURSTSIZE を上回った場合、超過分のパケットはキューイング前に破棄されるか (DROPBWCLASS3=YES のとき) 帯域クラス 3 に分類される (DROPBWCLASS3=NO のとき)。省略時は 0。

**MINBANDWIDTH** トラフィックに割り当てる最小帯域幅 (Kbps)。トラフィッククラスには、原則としてここで指定した帯域が確保される。数値だけで指定する場合の単位は Kbps。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「Kbps」、「Mbps」、「Gbps」の意味になる。「M」、「G」を指定する場合は、「2.256G」や「128.4M」のように小数を指定することもできる。QoS ポリシーを適用するスイッチポートの帯域と矛盾しないように設定すること。省略時は NONE。

**MINBURSTSIZE** トラフィッククラスの最小帯域幅設定 (MINBANDWIDTH) に対する、「帯域クラス 1」の最大許容バーストサイズ (Byte)。MINBANDWIDTH が NONE のときは、最大帯域幅設定 (MAXBANDWIDTH) に対する、「帯域クラス 2」の最大許容バーストサイズ (Byte)。数値だけで指定する場合の単位は Byte。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「Kbyte」、「Mbyte」、「Gbyte」の意味になる。「K」、「M」、「G」を指定する場合は、「2.256G」や「128.4M」のように小数を指定することもできる。MINBANDWIDTH が NONE のときは、MAXBURSTSIZE よりも小さい値でなくてはならない。詳細は解説編を参照。省略時は 0。

**PREMARKING** 本トラフィッククラスに対するプレマーキングの動作を指定する。具体的には、トラフィッククラスに割り当てる QoS パラメータをプレマーキング用 DSCP MAP テーブルから検索するときに、どの値をインデックスとして使うかを指定する。USEMARKVALUE を指定した場合は、MARKVALUE パラメータの値をインデックスとして使う。USEDSCP を指定した場合は、パケットの DSCP フィールド値をインデックスとして使う。いずれの場合も、DSCP MAP テーブルのもう 1 つのインデックスである帯域クラスは 1 を使う。NONE を指定した場合は、プレマーキングを行わずに、メータリングの処理に移る。省略時は NONE。なお、トラフィッククラスとフローグループの両方で本パラメータが指定されている場合は、フローグループの設定が使われる。なお、IPv6 ルーティングパケットに対する QoS ポリシーでは、USEDSCP を使用できないので注意すること (指定しても効果がない)。

**REMARKING** 本トラフィッククラスに対するリマーキングの動作を指定する。具体的には、メータリング後の QoS パラメータ書き換え動作を何に基づいて実施するか、および、どのパラメータを書き換えるかを指定する。USEDSCP MAP を指定した場合は、リマーキング直前の帯域クラスとパケットの DSCP 値をインデックスとしてリマーキング用 DSCP MAP テーブルを検索し、DSCP 値、帯域クラス、送信キュー、802.1p プライオリティー値を書き換える。PRIORITY、PRIO+BWCLASS を指定した場合は、リマーキング直前の送信キューと帯域クラスをインデックスとして QUEUE2PRIOMAP

テーブルを検索し、802.1p プライオリティー値を書き換える。BWCLASS、NONE を指定した場合は書き換えを行わない。省略時は NONE。なお、PRIORITY と PRIO+BWCLASS、BWCLASS と NONE はそれぞれ同じ意味になる。また、IPv6 ルーティングパケットに対する QoS ポリシーでは、USEDSCPMAP を使用できないので注意すること（指定しても効果がない）。

**MARKVALUE** PREMARKING パラメーターに USEMARKVALUE を指定した場合、プレマーキング用 DSCPMAP テーブルの検索インデックスとして使う DSCP 値を指定する。省略時は NONE

**DESCRIPTION** トラフィッククラスの説明（メモとして使う）。TRAFFICCLASS パラメーターに複数の番号を指定した場合は、すべてのトラフィッククラスに同じメモ文字列が設定される

**ACTION** 本トラフィッククラスに対するアクション。アクションの詳細は別表を参照のこと。アクションはフローグループとトラフィッククラスの両方に設定できるが、フローグループのアクションのほうが優先される（ただし、フローグループのアクションが NONE のときは、トラフィッククラスのアクションが実行される）。省略時は FORWARD

**VLAN** 本トラフィッククラスに属するパケットの出力先 VLAN。ACTION パラメーターに SENDVLANPORT を指定したときのみ有効かつ必須。本パラメーターは、必ず PORT パラメーターと組で指定すること。

**PORT** 本トラフィッククラスに属するパケットの出力先ポート。ACTION パラメーターに SENDVLANPORT を指定したときのみ有効かつ必須。本パラメーターは、必ず VLAN パラメーターと組で指定すること。

FORWARD	パケットを通常どおり出力する
DISCARD	パケットを破棄する
SENDVLANPORT	パケットの出力先を VLAN パラメーターと PORT パラメーターで指定されたポートに変更する。このとき、出力ポート（PORT）は出力 VLAN（VLAN）に所属していなくてはならないので、設定には注意すること
SENDMIRROR	パケットのコピーをミラーポートから出力する。あらかじめ、SET SWITCH MIRROR コマンドでミラーポートを指定し、ENABLE SWITCH MIRROR コマンドでポートミラーリング機能を有効にしておく必要がある
FORWARD,SENDMIRROR	FORWARD と SENDMIRROR の両方の処理を行う。SENDMIRROR だけ指定した場合と同じ動作
SENDMIRROR,SENDVLANPORT	SENDMIRROR と SENDVLANPORT の両方の処理を行う

表 36: ACTION パラメーターに指定できるオプション

## 備考・注意事項

ACTION、VLAN、PORT パラメーターは、IPv6 アクセラレーター用の QoS ポリシーでは未サポート。

## 関連コマンド

ADD QOS TRAFFICCLASS ( 181 ページ )

DELETE QOS TRAFFICCLASS ( 233 ページ )  
DESTROY QOS TRAFFICCLASS ( 249 ページ )  
SET QOS DSCPMAP ( 357 ページ )  
SET QOS QUEUE2PRIOMAP ( 370 ページ )  
SET QOS TRAFFICCLASS ( 373 ページ )  
SHOW QOS DSCPMAP ( 461 ページ )  
SHOW QOS QUEUE2PRIOMAP ( 472 ページ )  
SHOW QOS TRAFFICCLASS ( 477 ページ )

## CREATE STP

カテゴリー：スイッチング / スパニングツリープロトコル (STP/RSTP)

**CREATE STP=*stpname***

*stpname*: STP ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

### 解説

STP ドメインを作成する。STP ドメインは「default」を含め 32 個まで作成できる。  
作成直後の STP ドメインはディセーブル状態になっている。

### パラメーター

**STP** STP ドメイン名

### 例

STP ドメイン「mystp」を作成する。

```
CREATE STP=mystp
```

### 関連コマンド

DESTROY STP ( 250 ページ )

ENABLE STP ( 295 ページ )

SET STP ( 377 ページ )

SHOW STP ( 480 ページ )

## CREATE SWITCH TRUNK

カテゴリー：スイッチング / ポート

```
CREATE SWITCH TRUNK=trunk [PORT=port-list] [SPEED={10M|100M|1000M}]
[THRASHACTION={NONE|LEARNDISABLE|PORTDISABLE|VLANDISABLE|LINKDOWN}]
[THRASHTIMEOUT={NONE|1..86400}]
```

*trunk*: トランクグループ名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

*port-list*: スイッチポート番号 (1~)。ハイフン、カンマを使った複数指定も可能)

### 解説

トランクグループを作成する。

トランクグループは 12 個まで作成可能 (LACP により自動設定されたトランクグループを含む)。また、トランクグループの所属ポート数は最大 4 ポート。

### パラメーター

**TRUNK** トランクグループ名。「LACP」で始まる名前は、LACP (Link Aggregation Control Protocol) によって自動生成されたトランクグループ用に予約されているため使用できない。

**PORT** トランクに所属するポートの一覧。グループあたりの最大ポート数は 4。他のトランクグループに所属するポートやミラーポートは追加できない。また、トランクポートは同じ VLAN に所属していなくてはならない。

**SPEED** トランクポートの通信速度。トランクグループに参加したポートは、ここで指定した速度のオートネゴシエーション (AUTONEGOTIATE) となる

**THRASHACTION** 該当トランクグループで MAC アドレススラッシング (同一 MAC アドレスの登録ポートが頻繁に変更されること) を検出した場合の動作。NONE (なにもしない)、LEARNDISABLE (トランクグループ内の全ポートで MAC アドレスの学習を停止する)、PORTDISABLE (トランクグループ内の全ポートをディセーブルにする)、VLANDISABLE (スラッシングが発生した VLAN に対してのみトランクグループ内の全ポートをディセーブルにする)、LINKDOWN (トランクグループ内の全ポートを物理的にリンクダウンさせる) から選択する。これらの動作は、THRASHTIMEOUT パラメーターで指定した時間が経過すると終了する (通常のポート動作に戻る)。ただし、PORTDISABLE、LINKDOWN の場合は、ENABLE SWITCH PORT コマンドにより手動で動作を終了させられる。また、VLANDISABLE の場合は、ENABLE SWITCH PORT VLAN コマンドにより手動で動作を終了させられる。デフォルトは LEARNDISABLE。

**THRASHTIMEOUT** MAC アドレススラッシング検出時の動作の持続時間 (秒)。NONE は無期限を示す。THRASHACTION パラメーターに LEARNDISABLE を指定している場合、本パラメーターを NONE に変更することはできない。また、本パラメーターを NONE に設定している状態で、THRASHACTION パラメーターの値を LEARNDISABLE に変更した場合、本パラメーターの値は自動的に 1 に変更される。デフォルトは 1 秒。

## 例

トランクグループ「aggr1」を作成する。

```
CREATE SWITCH TRUNK=aggr1
```

## 備考・注意事項

THRASHACTION パラメーターの値を VLANDISABLE に変更すると、トランクグループ内の全ポートで自動的にイングレスフィルタリング (SET SWITCH PORT コマンドの INFILTERING パラメーター) が有効になる。また、VLANDISABLE からそれ以外に変更すると、イングレスフィルタリングが無効になる。

## 関連コマンド

ADD SWITCH TRUNK ( 190 ページ )  
DELETE SWITCH TRUNK ( 238 ページ )  
DESTROY SWITCH TRUNK ( 251 ページ )  
ENABLE SWITCH HASH ( 300 ページ )  
SET SWITCH THRASHLIMIT ( 391 ページ )  
SET SWITCH TRUNK ( 392 ページ )  
SHOW SWITCH TRUNK ( 517 ページ )



## CREATE VLAN

カテゴリー：スイッチング / バーチャル LAN

**CREATE VLAN=*vlanname* VID=2..4094** [PRIVATE]

**CREATE VLAN=*vlanname* VID=2..4094 SUBNET=*ipadd*** [MASK=*ipadd*] [PRIVATE]

**CREATE VLAN=*vlanname* VID=2..4094 PROTOCOL=*protocoltype*** [PRIVATE]

**CREATE VLAN=*vlanname* VID=2..4094** [NESTED]

**CREATE VLAN=*vlanname* VID=2..4094 SUBNET=*ipadd*** [MASK=*ipadd*] [NESTED]

**CREATE VLAN=*vlanname* VID=2..4094 PROTOCOL=*protocoltype*** [NESTED]

*vlanname*: VLAN 名 (1～32 文字。英数字とアンダースコア ( \_ ) ハイフンを使用可能。ただし、数字だけの文字列と「default」、**「ALL」**は指定できない。大文字小文字は区別しない)

*ipadd*: IP アドレスまたはネットマスク

*protocoltype*: L3 プロトコル番号 (16 進数。「0x」を前置すること)

### 解説

VLAN を作成する。

本製品がサポートする基本的な VLAN は次の 3 種類。

- ・ポート VLAN (タグ VLAN を含む)
- ・IP サブネット VLAN
- ・プロトコル VLAN

さらに、特殊な VLAN として次の 2 種類がある (ダブルタグ VLAN (Nested VLAN) は別売のフィーチャーライセンス AT-FL-09 が必要)。

- ・マルチプル VLAN (Private VLAN)
- ・ダブルタグ VLAN (Nested VLAN)

### パラメーター

**VLAN** VLAN 名。半角英数字とアンダースコア、ハイフンからなる 1～32 文字の文字列で指定する。ただし、数字だけの文字列と、予約済みの文字列「default」、「ALL」は指定できない。また、「vlanXXXX」(XXXX は数字) 形式の名前を指定する場合は、XXXX の部分が VID (VLAN ID) と一致していなくてはならない。VLAN 名の大文字小文字は区別されないが、SHOW VLAN コマンドなどの表示では、VLAN 作成時に指定した大文字小文字の違いが反映される。VLAN 名は製品内部における管理用の識別子であり、外部に送信されることはない。

**VID** VLAN ID。タグ付きポートでは、送信フレームにこの値を含んだタグが付加される。1 は VLAN

default に割り当て済みなので指定できない。なお、NESTED オプションを指定した場合（ダブルタグ VLAN（Nested VLAN）を作成する場合）、VID パラメーターにはカスタマー ID（CID）、すなわち、外側タグに含める ID を指定する。

**SUBNET** サブネット VLAN のサブネットアドレス。MASK と組み合わせて指定する。サブネットは、ADD VLAN SUBNET コマンドを使って後から追加することも可能

**MASK** サブネット VLAN の所属サブネットアドレスに対するマスク。省略時は SUBNET で指定したアドレスのクラス標準マスクが使われる

**PROTOCOL** プロトコル VLAN の対象プロトコル。定義済みのプロトコル名（ADD VLAN PROTOCOL コマンドの表を参照）か、16 進表記（「0x」を前置すること）のプロトコル番号で指定する。プロトコル番号で指定する場合、802.2 なら 1 バイト（DSAP のみ）で、Ethernet Version 2 なら 2 バイトで、SNAP なら 5 バイトの 16 進数で指定する。プロトコルは、ADD VLAN PROTOCOL コマンドを使って後から追加することも可能

**PRIVATE** マルチプル VLAN（Private VLAN）を作成するときに指定する。

**NESTED** ダブルタグ VLAN（Nested VLAN）を作成するときに指定する。

## 例

ポート VLAN「orange」（VLAN ID=20）を作成する。

```
CREATE VLAN=orange VID=20
```

プロトコル VLAN「NetWare」（VLAN ID=100）を作成する。

```
CREATE VLAN=NetWare VID=100 PROTOCOL="IPX 802.2"
```

## 備考・注意事項

VLAN は 4094 個（VLAN default を含む）まで作成できる。IP アドレスを設定可能な VLAN の数に制限はない。

作成した直後の VLAN はデフォルトの STP ドメイン「default」に所属している。

ダブルタグ VLAN（Nested VLAN）は別売のフィーチャーライセンス AT-FL-09 が必要。

ダブルタグ VLAN（Nested VLAN）はレイヤー 2 を前提とした機能なので、ルーティングとの併用はサポート対象外。

## 関連コマンド

ADD VLAN PROTOCOL（194 ページ）

ADD VLAN SUBNET（197 ページ）

DESTROY VLAN（252 ページ）

SHOW SWITCH（490 ページ）

SHOW VLAN（519 ページ）

## DELETE DHCP Snooping BINDING

カテゴリー：スイッチング / DHCP Snooping

**DELETE DHCP Snooping BINDING IP=*ipadd***

*ipadd*: IP アドレス

### 解説

DHCP Snooping テーブル（バインディングデータベース）からエントリを削除する。

### パラメーター

**IP** クライアントの IP アドレス

### 関連コマンド

ADD DHCP Snooping BINDING ( 173 ページ )

SHOW DHCP Snooping DATABASE ( 405 ページ )

## DELETE EPSR DATAVLAN

カテゴリー：スイッチング / イーサネットリングプロテクション (EPSR)

**DELETE EPSR=***epsrname* **DATAVLAN=**{*vlannname*|1..4094|ALL}

*epsrname*: EPSR ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ ) ハイフンを使用可能。大文字小文字を区別しない)

*vlannname*: VLAN 名 (1~32 文字。英数字とアンダースコア ( \_ ) ハイフンを使用可能。大文字小文字は区別しない)

### 解説

EPSR ドメインからデータ VLAN を削除する。

なお、本コマンドを実行すると該当 VLAN でループが発生する可能性があるため、本コマンドを実行する前には、次のいずれかの手順をとることが望ましい。

- ・ DISABLE SWITCH PORT コマンドで該当 VLAN のリング接続用ポートをディセーブルにする
- ・ 該当 VLAN のリング接続用ポートからケーブルを抜く
- ・ DELETE VLAN PORT コマンドで該当 VLAN からリング接続用ポートを削除する

### パラメーター

**EPSR** EPSR ドメイン名

**DATAVLAN** データ VLAN。VLAN 名または VLAN ID (VID) で指定する。ALL を指定した場合は該当 EPSR ドメインに所属しているすべてのデータ VLAN が対象となる。

### 関連コマンド

ADD EPSR DATAVLAN (175 ページ)

CREATE EPSR (205 ページ)

DELETE VLAN PORT (239 ページ)

DISABLE SWITCH PORT (274 ページ)

SHOW EPSR (411 ページ)

## DELETE LACP PORT

カテゴリー：スイッチング / LACP (IEEE 802.3ad)

**DELETE LACP PORT=*port-list***

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

指定したスイッチポートを LACP の管理下から除外する (該当ポートで LACP を無効にする)。  
なお、デフォルトでは、すべてのスイッチポートが LACP の管理下に置かれている。

### パラメーター

**PORT** ポート番号。

### 例

ポート 4 を LACP の管理下から外す。

```
DELETE LACP PORT=4
```

### 関連コマンド

ADD LACP PORT ( 176 ページ )

SET LACP PORT ( 335 ページ )

SHOW LACP PORT ( 419 ページ )

## DELETE MSTP MSTI VLAN

カテゴリー：スイッチング / マルチプルスパニングツリープロトコル (MSTP)

**DELETE MSTP MSTI=*instance* VLAN={1..4094|ALL}**

*instance*: MST インスタンス ID (1 ~ 4094)

### 解説

MST インスタンスと VLAN の関連付けを解除する。

MST インスタンスとの関連付けを解除された VLAN は、自動的に CIST (Common and Internal Spanning Tree) の所属に戻る。

### パラメーター

**MSTI** MST インスタンス ID

**VLAN** VLAN ID (VID)。ALL を指定した場合は、MSTI パラメーターで指定した MST インスタンスに関連付けられているすべての VLAN が対象となる。

### 例

MST インスタンス「1」と VLAN「20」の関連付けを解除する。

DELETE MSTP MSTI=1 VLAN=20

### 関連コマンド

ADD MSTP MSTI VLAN (178 ページ)

SHOW MSTP (425 ページ)

SHOW MSTP MSTI (436 ページ)

## DELETE QOS FLOWGROUP

カテゴリー：スイッチング / QoS

**DELETE QOS FLOWGROUP**=*flow-id* **CLASSIFIER**=*{rule-list|ALL}*

*flow-id*: フローグループ番号 (0~1023)

*rule-list*: クラシファイア番号 (1~9999)。ハイフン、カンマを使った複数指定も可能)

### 解説

フローグループからクラシファイア (汎用パケットフィルター) を削除する。

### パラメーター

**FLOWGROUP** フローグループ番号

**CLASSIFIER** クラシファイア番号

### 関連コマンド

ADD QOS FLOWGROUP ( 179 ページ )

CREATE QOS FLOWGROUP ( 209 ページ )

DESTROY QOS FLOWGROUP ( 246 ページ )

SET QOS FLOWGROUP ( 359 ページ )

SHOW QOS FLOWGROUP ( 463 ページ )

## DELETE QOS POLICY

カテゴリー：スイッチング / QoS

**DELETE QOS POLICY**=*qos-id* **TRAFFICCLASS**=*{tc-list|ALL}*

*qos-id*: QoS ポリシー番号 (0~255)

*tc-list*: トラフィッククラス番号 (0~1023)。ハイフン、カンマを使った複数指定も可能)

### 解説

QoS ポリシーからトラフィッククラスを削除する。

### パラメーター

**POLICY** QoS ポリシー番号

**TRAFFICCLASS** トラフィッククラス番号

### 関連コマンド

ADD QOS POLICY ( 180 ページ )

CREATE QOS POLICY ( 212 ページ )

DESTROY QOS POLICY ( 247 ページ )

SET QOS POLICY ( 361 ページ )

SET QOS PORT ( 365 ページ )

SHOW QOS POLICY ( 465 ページ )



## DELETE QOS TRAFFICCLASS

カテゴリー：スイッチング / QoS

**DELETE QOS TRAFFICCLASS=***tc-id* **FLOWGROUP=**{*flow-list*|**ALL**}

*tc-id*: トラフィッククラス番号 (0~1023)

*flow-list*: フローグループ番号 (0~1023)。ハイフン、カンマを使った複数指定も可能)

### 解説

トラフィッククラスからフローグループを削除する。

### パラメーター

**TRAFFICCLASS**    トラフィッククラス番号

**FLOWGROUP**    フローグループ番号

### 関連コマンド

ADD QOS TRAFFICCLASS ( 181 ページ )

CREATE QOS TRAFFICCLASS ( 218 ページ )

DESTROY QOS TRAFFICCLASS ( 249 ページ )

SET QOS TRAFFICCLASS ( 373 ページ )

SHOW QOS TRAFFICCLASS ( 477 ページ )

## DELETE STP VLAN

カテゴリー：スイッチング / スパニングツリープロトコル (STP/RSTP)

**DELETE STP=stpname VLAN={vlanname|2..4094|ALL}**

*stpname*: STP ドメイン名 (1～15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

*vlanname*: VLAN 名 (1～32 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字は区別しない)

### 解説

ユーザー定義の STP ドメインに所属している VLAN を削除する。

### パラメーター

**STP** STP ドメイン名。本コマンドを使って、VLAN を default STP から削除することはできない。

**VLAN** STP ドメインから削除する VLAN 名または VLAN ID を指定する。削除された VLAN は default STP の所属に戻る。

### 関連コマンド

ADD STP VLAN ( 182 ページ )

SHOW STP ( 480 ページ )

## DELETE SWITCH ACCELERATOR HWFILTER

カテゴリー：スイッチング / IPv6 ハードウェアパケットフィルター

備考：IPv6 アクセラレータボード AT-ACC01 と拡張メモリー AT-SD512A-001 が必要（本機能は 9924SP では使用できません）

**DELETE SWITCH ACCELERATOR HWFILTER={*filter-id*|ALL}**

*filter-id*: フィルター番号（1～999）

### 解説

IPv6 ハードウェアパケットフィルター（クラシファイアとアクションのペア）を削除する。

フィルター番号は可変なので、必ず SHOW SWITCH ACCELERATOR HWFILTER コマンドで確認してから指定すること。

本コマンドは、IPv6 ハードウェアパケットフィルターとクラシファイアの関連付けを削除するだけで、クラシファイアそのものを削除するわけではない。クラシファイアの削除は DESTROY CLASSIFIER コマンドで行う。

### パラメーター

**HWFILTER** フィルター番号。ALL を指定した場合は、すべてのフィルターが削除される。フィルター番号は可変なので、必ず SHOW SWITCH ACCELERATOR HWFILTER コマンドで確認してから指定すること。フィルターを削除すると、削除によって空いた番号を埋める形で後続のフィルター番号が自動的に変更されるので注意。

### 例

IPv6 ハードウェアパケットフィルター「16」を削除する。

```
DELETE SWITCH ACCELERATOR HWFILTER=16
```

### 関連コマンド

ADD SWITCH ACCELERATOR HWFILTER（184 ページ）

CREATE CLASSIFIER（198 ページ）

SHOW SWITCH ACCELERATOR HWFILTER（499 ページ）

## DELETE SWITCH FILTER

カテゴリー：スイッチング / フォワーディングデータベース

**DELETE SWITCH FILTER** **PORT=***port-number* **ENTRY=***entry-list*

*port-number*: スイッチポート番号 (1 ~ )

*entry-list*: エントリー番号 (0 ~ 319)。ハイフン、カンマを使った複数指定も可能)

### 解説

フォワーディングデータベース (FDB) からスタティックエントリー (スイッチフィルター) を削除する。エントリーを削除すると、後続のエントリー番号が 1 つずつ前にずれるので注意。

### パラメーター

**PORT** 該当エントリーの出力ポート

**ENTRY** エントリー番号。ハイフン、カンマを使った複数指定も可能。エントリー番号は可変なので、必ず SHOW SWITCH FILTER コマンドで確認してから指定すること。

### 例

ポート 2 のスタティックエントリー 2、4、5、6、7 番を削除する。

```
DELETE SWITCH FILTER PORT=2 ENTRY=2,4-7
```

### 関連コマンド

ADD SWITCH FILTER ( 186 ページ )

SHOW SWITCH FILTER ( 505 ページ )

## DELETE SWITCH HWFILTER

カテゴリー：スイッチング / ハードウェアパケットフィルター

**DELETE SWITCH HWFILTER=***filter-list*

*filter-list*: フィルター番号（1～1024。ハイフン、カンマを使った複数指定も可能）

### 解説

ハードウェアパケットフィルター（クラシファイアとアクションのペア）を削除する。  
フィルター番号は可変なので、必ず SHOW SWITCH HWFILTER コマンドで確認してから指定すること。  
本コマンドは、ハードウェアパケットフィルターとクラシファイアの関連付けを削除するだけで、クラシファイアそのものを削除するわけではない。クラシファイアの削除は DESTROY CLASSIFIER コマンドで行う。

### パラメーター

**HWFILTER** フィルター番号。ハイフン、カンマ区切りで複数のフィルター番号を指定可能。フィルター番号は可変なので、必ず SHOW SWITCH HWFILTER コマンドで確認してから指定すること。フィルターを削除すると、削除によって空いた番号を埋める形で後続のフィルター番号が自動的に変更されるので注意。

### 例

ハードウェアパケットフィルター「39」と「96」を削除する。

```
DELETE SWITCH HWFILTER=39,96
```

### 関連コマンド

ADD SWITCH HWFILTER（188 ページ）

CREATE CLASSIFIER（198 ページ）

SHOW SWITCH HWFILTER（507 ページ）

## DELETE SWITCH TRUNK

カテゴリー：スイッチング / ポート

**DELETE SWITCH TRUNK=***trunk* **PORT=**{*port-list*|**ALL**}

*trunk*: トランクグループ名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

*port-list*: スイッチポート番号 (1~。ハイフン、カンマを使った複数指定も可能)

### 解説

トランクグループからポートを削除する。

### パラメーター

**TRUNK** トランクグループ名

**PORT** 削除するポートの一覧。ALL を指定した場合は所属するすべてのポートが削除される。

### 関連コマンド

ADD SWITCH TRUNK ( 190 ページ )

CREATE SWITCH TRUNK ( 223 ページ )

DESTROY SWITCH TRUNK ( 251 ページ )

SET SWITCH TRUNK ( 392 ページ )

SHOW SWITCH TRUNK ( 517 ページ )

## DELETE VLAN PORT

カテゴリー：スイッチング / バーチャル LAN

**DELETE VLAN**={*vlannname*|1..4094} **PORT**={*port-list*|ALL}

**DELETE VLAN**={*vlannname*|1..4094} **PORT**={*port-list*|ALL} **SUBNET**={*ipadd*|ALL}

**DELETE VLAN**={*vlannname*|1..4094} **PORT**={*port-list*|ALL}  
**PROTOCOL**={*protocoltype*|*index-list*|ALL}

*vlannname*: VLAN 名 (1~32 文字。英数字とアンダースコア ( \_ ) ハイフンを使用可能。大文字小文字は区別しない)

*port-list*: スイッチポート番号 (1~。ハイフン、カンマを使った複数指定も可能)

*ipadd*: IP アドレス

*protocoltype*: L3 プロトコル番号 (16 進数。「0x」を前置すること)

*index-list*: インデックス番号 (0~。ハイフン、カンマを使った複数指定も可能)

### 解説

VLAN からポートを削除する。または、ポートとプロトコル、ポートと IP サブネットの関連付けを削除する。

VLAN と PORT パラメーターだけを指定した場合は、指定した VLAN のポート VLAN メンバーから指定ポートを削除する。

VLAN、PORT パラメーターに加え、SUBNET、PROTOCOL のいずれかを指定した場合は、それぞれ指定 VLAN のサブネット VLAN メンバー、プロトコル VLAN メンバーから指定ポートを削除する。

VLAN default 以外の VLAN からタグなし設定のみのポートを削除すると、そのポートは VLAN default のタグなしポートに戻る。

### パラメーター

**VLAN** VLAN 名または VLAN ID。VLAN default にのみ所属しているポートを VLAN default から削除することはできない。

**PORT** 削除するポートの一覧。ALL を指定した場合は、該当 VLAN の所属ポートがすべて削除される。

**SUBNET** サブネットアドレス。サブネット VLAN からポートを削除するときに指定する。PROTOCOL パラメーターとは同時に指定できない。

**PROTOCOL** プロトコル。プロトコル VLAN からポートを削除するときに指定する。プロトコルは、定義済みのプロトコル名 (ADD VLAN PROTOCOL コマンドの表を参照) か、16 進表記 (「0x」を前置すること) のプロトコル番号で指定する。あるいは、SHOW VLAN コマンドで表示されるインデックス番号 (複数指定可) で指定することもできる。SUBNET パラメーターとは同時に指定できない。

### 例

VLAN orange からポート 2 を削除する。

```
DELETE VLAN=orange PORT=2
```

VLAN net10 のサブネット VLAN メンバー（所属サブネット 192.168.10.0/24）からポート 1～4 を削除する。

```
DELETE VLAN=net10 PORT=1-4 SUBNET=192.168.10.0
```

VLAN nw のプロトコル VLAN メンバー（所属プロトコル IPX 802.2）からポート 3 と 5 を削除する。

```
DELETE VLAN=nw PORT=3,5 PROTOCOL="IPX 802.2"
```

### 備考・注意事項

PORT パラメーターにトランクグループを指定する場合は、該当グループに所属するすべてのポートを同時に指定すること。

マルチプル VLAN（Private VLAN）のアップリンクポートは、プライベートポートを削除してからでないと削除できない。

### 関連コマンド

ADD VLAN PORT（191 ページ）

ADD VLAN SUBNET（197 ページ）

DELETE VLAN PROTOCOL（241 ページ）

DELETE VLAN SUBNET（242 ページ）

SHOW VLAN（519 ページ）



## DELETE VLAN PROTOCOL

カテゴリー：スイッチング / バーチャル LAN

**DELETE VLAN**={*vlanname*|1..4094} **PROTOCOL**={*protocoltype*|*index-list*|ALL}

*vlanname*: VLAN 名 (1~32 文字。英数字とアンダースコア ( \_ ) ハイフンを使用可能。大文字小文字は区別しない)

*protocoltype*: L3 プロトコル番号 (16 進数。「0x」を前置すること)

*index-list*: インデックス番号 (0~。ハイフン、カンマを使った複数指定も可能)

### 解説

VLAN に関連付けられているプロトコルを削除する。

### パラメーター

**VLAN** VLAN 名または VLAN ID

**PROTOCOL** プロトコルまたはインデックス番号 (SHOW VLAN コマンドで確認可能)

### 関連コマンド

ADD VLAN PORT (191 ページ)

ADD VLAN PROTOCOL (194 ページ)

DELETE VLAN PORT (239 ページ)

SHOW VLAN (519 ページ)

## DELETE VLAN SUBNET

カテゴリー：スイッチング / バーチャル LAN

**DELETE VLAN**={*vlanname*|1..4094} **SUBNET**={*ipadd*|ALL}

*vlanname*: VLAN 名 (1~32 文字。英数字とアンダースコア ( \_ ) ハイフンを使用可能。大文字小文字は区別しない)

*ipadd*: IP アドレス

### 解説

VLAN に関連付けられている IP サブネットを削除する。

### パラメーター

**VLAN** VLAN 名または VLAN ID

**SUBNET** サブネットアドレス

### 関連コマンド

ADD VLAN PORT ( 191 ページ )

ADD VLAN PROTOCOL ( 194 ページ )

DELETE VLAN PORT ( 239 ページ )

SHOW VLAN ( 519 ページ )

## DESTROY CLASSIFIER

カテゴリー：スイッチング / クラシファイア

**DESTROY CLASSIFIER**={*rule-list*|ALL}

*rule-list*: クラシファイア番号 (1～9999)。ハイフン、カンマを使った複数指定も可能)

### 解説

クラシファイア (汎用パケットフィルター) を削除する。

ハードウェアパケットフィルターや QoS フローグループに関連付けられているクラシファイアは削除できない。

### パラメーター

**CLASSIFIER** クラシファイア番号。ALL を指定した場合は、すべてのクラシファイアが削除される

### 例

クラシファイア「10」「12」「13」を削除する。

DESTROY CLASSIFIER=10,12-13

すべてのクラシファイアを削除する。

DESTROY CLASSIFIER=ALL

### 関連コマンド

CREATE CLASSIFIER (198 ページ)

SET CLASSIFIER (325 ページ)

SHOW CLASSIFIER (395 ページ)

## DESTROY EPSR

カテゴリー：スイッチング / イーサネットリングプロテクション (EPSR)

**DESTROY EPSR**={*epsrname*|ALL}

*epsrname*: EPSR ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

### 解説

EPSR ドメインを削除する。

本コマンドを実行する前には、DISABLE EPSR コマンドで対象となる EPSR ドメインを無効化し、DELETE EPSR DATAVLAN コマンドでデータ VLAN を削除しておく必要がある。

また、本コマンドを実行するとループが発生する可能性があるので、本コマンドを実行する前には、次のいずれかの手順をとることが望ましい。

- ・ DISABLE SWITCH PORT コマンドで該当 VLAN のリング接続用ポートをディセーブルにする
- ・ 該当 VLAN のリング接続用ポートからケーブルを抜く
- ・ DELETE VLAN PORT コマンドで該当 VLAN からリング接続用ポートを削除する

### パラメーター

**EPSR** EPSR ドメイン名。ALL を指定した場合は、すべての EPSR ドメインが対象となる。

### 備考・注意事項

EPSR が使用するスイッチポートでは、自動的にイングレスフィルタリング (SET SWITCH PORT コマンドの INFILTERING パラメーター) が有効になる。その反対に、EPSR ドメインを削除すると、EPSR で使用されなくなったスイッチポートでは、自動的にイングレスフィルタリングが無効になる。

### 関連コマンド

CREATE EPSR ( 205 ページ )

DELETE EPSR DATAVLAN ( 228 ページ )

DELETE VLAN PORT ( 239 ページ )

DISABLE EPSR ( 257 ページ )

DISABLE SWITCH PORT ( 274 ページ )

SHOW EPSR ( 411 ページ )

## DESTROY MSTP MSTI

カテゴリー：スイッチング / マルチプルスパニングツリープロトコル (MSTP)

**DESTROY MSTP MSTI=*instance***

*instance*: MST インスタンス ID (1 ~ 4094)

### 解説

MST インスタンスを削除する。

VLAN が関連付けられている MST インスタンスは削除できないので、あらかじめ DELETE MSTP MSTI VLAN コマンドを実行して、所属 VLAN をすべて削除してから本コマンドを実行すること。

### パラメーター

**MSTI** MST インスタンス ID

### 例

MST インスタンス「1」を削除する。

```
DESTROY MSTP MSTI=1
```

### 関連コマンド

CREATE MSTP MSTI ( 208 ページ )

DELETE MSTP MSTI VLAN ( 230 ページ )

SHOW MSTP ( 425 ページ )

## DESTROY QOS FLOWGROUP

カテゴリー：スイッチング / QoS

**DESTROY QOS FLOWGROUP**=**{*flow-list*|ALL}**

*flow-list*: フローグループ番号 (0~1023)。ハイフン、カンマを使った複数指定も可能)

### 解説

フローグループを削除する。

### パラメーター

**FLOWGROUP** フローグループ番号

### 関連コマンド

ADD QOS POLICY ( 180 ページ )

CREATE QOS FLOWGROUP ( 209 ページ )

DELETE QOS POLICY ( 232 ページ )

SET QOS POLICY ( 361 ページ )

SET QOS PORT ( 365 ページ )

SHOW QOS POLICY ( 465 ページ )

## DESTROY QOS POLICY

カテゴリー：スイッチング / QoS

**DESTROY QOS POLICY**={*qos-list*|**ALL**}

*qos-list*: QoS ポリシー番号 (0~255。ハイフン、カンマを使った複数指定も可能)

### 解説

QoS ポリシーを削除する。

### パラメーター

**POLICY** QoS ポリシー番号

### 関連コマンド

ADD QOS POLICY ( 180 ページ )

CREATE QOS FLOWGROUP ( 209 ページ )

DELETE QOS POLICY ( 232 ページ )

SET QOS POLICY ( 361 ページ )

SET QOS PORT ( 365 ページ )

SHOW QOS POLICY ( 465 ページ )

## DESTROY QOS RED

カテゴリー：スイッチング / QoS

**DESTROY QOS RED**={*red-list*|ALL}

*red-list*: RED カーブセット番号（2～4。ハイフン、カンマを使った複数指定も可能）

### 解説

RED（Random Early Detection/Discard）カーブセットを削除する。

### パラメーター

**RED** RED カーブセット番号。1 はデフォルトの RED カーブセットが使っているため指定できない。また、スイッチポートに割り当てられている RED カーブセットは削除できない。

### 関連コマンド

CREATE QOS RED（216 ページ）

SET QOS PORT（365 ページ）

SET QOS RED（371 ページ）

SHOW QOS RED（474 ページ）



## DESTROY QOS TRAFFICCLASS

カテゴリー：スイッチング / QoS

**DESTROY QOS TRAFFICCLASS**={*tc-list*|ALL}

*tc-list*: トラフィッククラス番号 (0~1023。ハイフン、カンマを使った複数指定も可能)

### 解説

トラフィッククラスを削除する。

### パラメーター

**TRAFFICCLASS**    トラフィッククラス番号

### 関連コマンド

ADD QOS TRAFFICCLASS ( 181 ページ )

CREATE QOS TRAFFICCLASS ( 218 ページ )

DELETE QOS TRAFFICCLASS ( 233 ページ )

SET QOS TRAFFICCLASS ( 373 ページ )

SHOW QOS TRAFFICCLASS ( 477 ページ )

## DESTROY STP

カテゴリー：スイッチング / スパニングツリープロトコル (STP/RSTP)

**DESTROY STP**={*stpname*|**ALL**}

*stpname*: STP ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

### 解説

ユーザー定義の STP ドメインを削除する。

所蔵 VLAN が存在する STP ドメインは削除できない。あらかじめ DELETE STP VLAN コマンドで VLAN を削除してから本コマンドを実行すること。

### パラメーター

**STP** STP ドメイン名。default STP は削除できない。ALL を指定した場合は、default STP を除くすべての STP ドメインを削除する。ただし、ひとつでも削除できない STP がある場合 (所属 VLAN が残っていた場合など) 本コマンドは失敗する (何も変化しない)。

### 関連コマンド

CREATE STP ( 222 ページ )

DISABLE STP ( 265 ページ )

ENABLE STP ( 295 ページ )

SET STP ( 377 ページ )

SHOW STP ( 480 ページ )

## DESTROY SWITCH TRUNK

カテゴリー：スイッチング / ポート

**DESTROY SWITCH TRUNK=*trunk***

*trunk*: トランクグループ名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

### 解説

トランクグループを削除する。

所属ポートがある場合は削除できない。その場合は、DELETE SWITCH TRUNK コマンドでポートをすべて削除してから、本コマンドを実行すること。

### パラメーター

**TRUNK** トランクグループ名

### 関連コマンド

ADD SWITCH TRUNK ( 190 ページ )

CREATE SWITCH TRUNK ( 223 ページ )

DELETE SWITCH TRUNK ( 238 ページ )

SET SWITCH TRUNK ( 392 ページ )

SHOW SWITCH TRUNK ( 517 ページ )

## DESTROY VLAN

カテゴリー：スイッチング / バーチャル LAN

**DESTROY VLAN**={*vlanname*|2..4094|ALL}

*vlanname*: VLAN 名 (1~32 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字は区別しない)

### 解説

VLAN を削除する。

VLAN default は削除できない。また、所属ポートがある場合や、IP サブネットやプロトコルと関連付けられている場合、他のソフトウェアモジュールとバインドされている場合 (VLAN に IP アドレスが設定されている場合など) も削除できない。あらかじめポートを削除したり、IP アドレスを削除したりしてから本コマンドを実行すること。

### パラメーター

**VLAN** VLAN 名または VLAN ID。VLAN default は削除できない。

### 関連コマンド

CREATE VLAN ( 225 ページ )

SHOW VLAN ( 519 ページ )

## DISABLE DHCP Snooping

カテゴリー：スイッチング / DHCP Snooping

### **DISABLE DHCP Snooping**

#### 解説

DHCP Snooping を無効にする。デフォルトは無効。

#### 関連コマンド

ENABLE DHCP Snooping ( 280 ページ )

SHOW DHCP Snooping ( 401 ページ )

## DISABLE DHCP Snooping ARPSECURITY

カテゴリー：スイッチング / DHCP Snooping

### DISABLE DHCP Snooping ARPSECURITY

#### 解説

DHCP Snooping のオプション機能である ARP セキュリティーを無効にする。デフォルトは無効。

#### 関連コマンド

ENABLE DHCP Snooping ( 280 ページ )

ENABLE DHCP Snooping ARPSECURITY ( 281 ページ )

SHOW DHCP Snooping ( 401 ページ )

## DISABLE DHCP Snooping LOG

カテゴリー：スイッチング / DHCP Snooping

**DISABLE DHCP Snooping LOG=ARPSECURITY**

### 解説

DHCP Snooping のログ機能を無効にする。デフォルトは無効。

### パラメーター

**LOG** ログに記録するイベントの種類。現時点では ARPSECURITY のみサポート。ARPSECURITY イベントは、ARP セキュリティー機能によってバインディングデータベース未登録の送信元からの ARP パケットを破棄したときに発生する。

### 関連コマンド

ENABLE DHCP Snooping ( 280 ページ )

ENABLE DHCP Snooping ARPSECURITY ( 281 ページ )

ENABLE DHCP Snooping LOG ( 282 ページ )

SHOW DHCP Snooping ( 401 ページ )

SHOW LOG (「運用・管理」の 393 ページ)

## DISABLE DHCP Snooping OPTION82

カテゴリー：スイッチング / DHCP Snooping

### **DISABLE DHCP Snooping OPTION82**

#### 解説

DHCP Snooping のオプション機能であるリレーエージェント情報オプション（オプションコード 82）の処理機能を無効にする。デフォルトは無効。

#### 関連コマンド

ENABLE DHCP Snooping（280 ページ）

ENABLE DHCP Snooping OPTION82（283 ページ）

SHOW DHCP Snooping（401 ページ）



## DISABLE EPSR

カテゴリー：スイッチング / イーサネットリングプロテクション (EPSR)

**DISABLE EPSR**={*epsrname*|ALL}

*epsrname*: EPSR ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ ) ハイフンを使用可能。大文字小文字を区別しない)

### 解説

EPSR ドメインを無効化する。

本コマンドを実行するとループが発生する可能性があるので、本コマンドを実行する前には、次のいずれかの手順をとることが望ましい。

- ・ DISABLE SWITCH PORT コマンドで該当 VLAN のリング接続用ポートをディセーブルにする
- ・ 該当 VLAN のリング接続用ポートからケーブルを抜く
- ・ DELETE VLAN PORT コマンドで該当 VLAN からリング接続用ポートを削除する

### パラメーター

**EPSR** EPSR ドメイン名。ALL を指定した場合は、すべての EPSR ドメインが対象となる。

### 関連コマンド

CREATE EPSR ( 205 ページ )

DELETE VLAN PORT ( 239 ページ )

DISABLE SWITCH PORT ( 274 ページ )

ENABLE EPSR ( 284 ページ )

SHOW EPSR ( 411 ページ )

## DISABLE EPSR DEBUG

カテゴリー：スイッチング / イーサネットリングプロテクション (EPSR)

**DISABLE EPSR**=**{*epsrname*|ALL}** **DEBUG**=**{INFO|MSG|PKT|STATE|ALL}**

*epsrname*: EPSR ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

### 解説

EPSR ドメインのデバッグオプションを無効化する。デフォルトはすべて無効。

### パラメーター

**EPSR** EPSR ドメイン名。ALL を指定した場合は、すべての EPSR ドメインが対象となる。

**DEBUG** 無効にするデバッグオプション。INFO (EPSR に関する全般的情報を表示)、MSG (EPSR パケットをデコードして表示)、PKT (EPSR パケットを ASCII 表示)、STATE (EPSR の状態遷移を表示)、ALL (すべてのオプション) から選択する。

### 関連コマンド

CREATE EPSR (205 ページ)

ENABLE EPSR DEBUG (285 ページ)

SHOW EPSR DEBUG (416 ページ)

## DISABLE LACP

カテゴリー：スイッチング / LACP (IEEE 802.3ad)

### **DISABLE LACP**

#### 解説

LACP モジュールを無効にする。デフォルトは無効。

LACP を無効にしても、各ポートの LACP 関連設定は保持される。

#### 関連コマンド

ENABLE LACP (286 ページ)

SHOW LACP (417 ページ)

## DISABLE LACP DEBUG

カテゴリー：スイッチング / LACP (IEEE 802.3ad)

**DISABLE LACP DEBUG**=**{MSG|PACKET|STATE|TRACE|ALL}**

### 解説

LACP モジュールのデバッグを無効にする。デフォルトはすべて無効。

### パラメーター

**DEBUG** デバッグオプション。MSG (LACP パケットをデコードして表示)、PKT (LACP パケットを 16 進表示)、STATE (状態遷移を表示)、TRACE (関数呼び出しをトレース表示)、ALL (すべてのオプション) から選択する。

### 関連コマンド

ENABLE LACP DEBUG (287 ページ)

SHOW LACP (417 ページ)

## DISABLE MSTP

カテゴリー：スイッチング / マルチプルスパニングツリープロトコル (MSTP)

### **DISABLE MSTP**

#### 解説

マルチプルスパニングツリープロトコル (MSTP) を無効にする。デフォルトは無効。  
MSTP が有効のときは、スパニングツリープロトコル (STP/RSTP) を有効化することができない。その場合は、本コマンドで MSTP を無効化してから、ENABLE STP コマンドを実行すればよい。

#### 関連コマンド

ENABLE MSTP (288 ページ)

ENABLE STP (295 ページ)

SHOW MSTP (425 ページ)

## DISABLE PORTAUTH

カテゴリー：スイッチング / ポート認証

**DISABLE PORTAUTH** [= {8021X|MACBASED}]

### 解説

ポート認証機能（802.1X 認証または MAC ベース認証）を無効にする。デフォルトはどちらとも無効。

### パラメーター

**PORTAUTH** 認証メカニズム。8021X（802.1X 認証）、MACBASED（MAC ベース認証）から選択する。  
省略時は 8021X と見なされる。

### 関連コマンド

DISABLE PORTAUTH PORT（264 ページ）

ENABLE PORTAUTH（289 ページ）

ENABLE PORTAUTH PORT（291 ページ）

SHOW PORTAUTH MULTISUPPLICANT PORT（447 ページ）

SHOW PORTAUTH PORT（451 ページ）

## DISABLE PORTAUTH DEBUG

カテゴリー：スイッチング / ポート認証

**DISABLE PORTAUTH** [= {8021X|MACBASED}] **DEBUG**={ALL|PACKET|STATE}  
**PORT**={*port-list*|ALL}

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

指定ポートで、ポート認証機能 (802.1X 認証または MAC ベース認証) のデバッグを無効にする。デフォルトは全ポート無効。

### パラメーター

**PORTAUTH** 認証メカニズム。8021X (802.1X 認証) 又は MACBASED (MAC ベース認証) から選択する。省略時は 8021X と見なされる。

**DEBUG** デバッグオプション。ALL (すべて) 又は PACKET (パケット送受信) 又は STATE (状態遷移) から選択する。PACKET は、PORTAUTH に 8021X を指定したときだけ有効。

**PORT** スイッチポート。複数指定が可能。

### 関連コマンド

ENABLE PORTAUTH (289 ページ)

ENABLE PORTAUTH DEBUG (290 ページ)

ENABLE PORTAUTH PORT (291 ページ)

SHOW PORTAUTH PORT (451 ページ)

## DISABLE PORTAUTH PORT

カテゴリー：スイッチング / ポート認証

**DISABLE PORTAUTH** [= {8021X|MACBASED}] **PORT**={*port-list*|ALL}

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

指定ポートで、ポート認証機能 (802.1X 認証または MAC ベース認証) を無効にする。デフォルトは全ポート無効。

### パラメーター

**PORTAUTH** 認証メカニズム。8021X (802.1X 認証)、MACBASED (MAC ベース認証) から選択する。

省略時は 8021X と見なされる。

**PORT** スイッチポート。複数指定が可能。

### 関連コマンド

DISABLE PORTAUTH (262 ページ)

ENABLE PORTAUTH (289 ページ)

ENABLE PORTAUTH PORT (291 ページ)

SHOW PORTAUTH PORT (451 ページ)



## DISABLE STP

カテゴリー：スイッチング / スパニングツリープロトコル (STP/RSTP)

**DISABLE STP**={*stpname*|ALL}

*stpname*: STP ドメイン名 (1～15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

### 解説

指定した STP ドメイン、あるいは、スイッチ全体でスパニングツリープロトコルを無効にする。

default STP、ユーザー定義の STP とともに、デフォルトは無効。

### パラメーター

**STP** STP ドメイン名。ALL を指定したときはスイッチ全体でスパニングツリープロトコルの動作が停止する。

### 関連コマンド

CREATE STP ( 222 ページ )

DESTROY STP ( 250 ページ )

ENABLE STP ( 295 ページ )

SET STP ( 377 ページ )

SHOW STP ( 480 ページ )

## DISABLE STP DEBUG

カテゴリー：スイッチング / スパニングツリープロトコル (STP/RSTP)

**DISABLE STP**={*stpname*|ALL} **DEBUG**={MSG|PKT|STATE|ALL}

*stpname*: STP ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

### 解説

STP ドメインのデバッグオプションを無効にする。

### パラメーター

**STP** STP ドメイン名。

**DEBUG** 無効にするデバッグオプション。MSG (STP パケットをデコードして表示)、PKT (STP パケットを ASCII 表示)、STATE (ポートの状態遷移を表示)、ALL (すべてのオプション) から選択する。

### 関連コマンド

DISABLE STP PORT DEBUG (268 ページ)

ENABLE STP DEBUG (296 ページ)

SHOW STP DEBUG (486 ページ)

## DISABLE STP PORT

カテゴリー：スイッチング / スパニングツリープロトコル (STP/RSTP)

**DISABLE STP PORT**={*port-list*|ALL}

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

指定ポートでスパニングツリープロトコルを無効にする。

無効にしたポートはスパニングツリーというディセーブル状態となり、同ポートではSTP パケットの送受信が行われなくなる。

### パラメーター

**PORT** ポート番号。複数指定が可能。ALL を指定した場合はすべてのスイッチポートでスパニングツリープロトコルを無効にする。

### 関連コマンド

ENABLE STP PORT (297 ページ)

SET STP PORT (379 ページ)

SHOW STP PORT (487 ページ)

## DISABLE STP PORT DEBUG

カテゴリー：スイッチング / スパニングツリープロトコル (STP/RSTP)

**DISABLE STP PORT**={*port-list*|**ALL**} **DEBUG**={**MSG**|**PKT**|**STATE**|**ALL**}

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

STP ポートのデバッグオプションを無効にする。

### パラメーター

**PORT** ポート番号。複数指定が可能。

**DEBUG** 無効にするデバッグオプション。MSG (STP パケットをデコードして表示)、PKT (STP パケットを ASCII 表示)、STATE (ポートの状態遷移を表示)、ALL (すべてのオプション) から選択する。

### 関連コマンド

DISABLE STP DEBUG (266 ページ)

ENABLE STP DEBUG (296 ページ)

ENABLE STP PORT DEBUG (298 ページ)

SHOW STP DEBUG (486 ページ)

## DISABLE SWITCH AGEINGTIMER

カテゴリー：スイッチング / フォワーディングデータベース

### DISABLE SWITCH AGEINGTIMER

#### 解説

FDB のエージングタイマーを無効にし、ダイナミックエントリーがエージアウトされないようにする。デフォルトは有効。

#### 関連コマンド

ENABLE SWITCH AGEINGTIMER ( 299 ページ )

SET SWITCH AGEINGTIMER ( 381 ページ )

SHOW SWITCH ( 490 ページ )

## DISABLE SWITCH HASH

カテゴリー：スイッチング / ポート

**DISABLE SWITCH HASH**={L2|L3|L4}[,...]

### 解説

ポートランキングの送出ポート決定アルゴリズムにおいて、指定した種類のヘッダー情報を使わないよう設定する。

デフォルトでは、L2 と L3 のヘッダー情報を使用して送出ポートを決定する。

### パラメーター

**HASH** 送出ポート決定アルゴリズムで使用しないヘッダー情報の種別。L2（送信元・宛先 MAC アドレス） L3（始点・終点 IP アドレス） L4（始点・終点ポート）から選択する。カンマ区切りで複数指定が可能。

### 備考・注意事項

ルーティング後トランクグループから送信される IP パケットの送出ポートは、本コマンドの設定とは関係なく、L3 ヘッダー情報にのみ基づいて決定される。

### 関連コマンド

ADD SWITCH TRUNK（190 ページ）

CREATE SWITCH TRUNK（223 ページ）

ENABLE SWITCH HASH（300 ページ）

SHOW SWITCH（490 ページ）

## DISABLE SWITCH LEARNING

カテゴリー：スイッチング / フォワーディングデータベース

### DISABLE SWITCH LEARNING

#### 解説

フォワーディングデータベース（FDB）の学習機能を無効にする。デフォルトは有効。

#### 備考・注意事項

学習機能を無効にし、ダイナミックエントリーがすべてエージアウトされた場合、スタティックエントリーにマッチしなかったフレームは、入力ポートを除くすべてのポート（ただし、同一 VLAN 所属）から出力されるようになる。

#### 関連コマンド

ENABLE SWITCH LEARNING（301 ページ）

SHOW SWITCH（490 ページ）

## DISABLE SWITCH MCLIMITING

カテゴリー：スイッチング / ポート

### **DISABLE SWITCH MCLIMITING**

#### 解説

マルチキャストパケットの受信レート制限機能を無効にする。デフォルトは無効。

#### 関連コマンド

ENABLE SWITCH MCLIMITING ( 302 ページ )

SET SWITCH PORT ( 387 ページ )

SHOW SWITCH PORT ( 509 ページ )



## DISABLE SWITCH MIRROR

カテゴリー：スイッチング / ポート

### DISABLE SWITCH MIRROR

#### 解説

ポートミラーリング機能を無効にする。ミラーポートの設定は変化しない。デフォルトは無効。

#### 関連コマンド

ENABLE SWITCH MIRROR ( 303 ページ )

SET SWITCH MIRROR ( 385 ページ )

SET SWITCH PORT ( 387 ページ )

SHOW SWITCH ( 490 ページ )

SHOW SWITCH PORT ( 509 ページ )

## DISABLE SWITCH PORT

カテゴリー：スイッチング / ポート

**DISABLE SWITCH PORT**={*port-list*|**ALL**} [LINK={DISABLE|ENABLE}]

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

スイッチポートをディセーブルにする。

### パラメーター

**PORT** ポート番号

**LINK** ( 本体内蔵 10/100/1000Mbps ポートのみ ) ポートを物理的にリンクダウンさせるかどうか。  
DISABLE ( 物理的にリンクダウンさせる )、ENABLE ( 物理的にはリンクアップのまま ) から選択する。  
省略時は ENABLE。

### 備考・注意事項

本コマンド実行後に LINK パラメーターの設定を変更することはできない。いったん ENABLE SWITCH PORT コマンドを実行してポートをイネーブルにしたのち、本コマンドを再実行すること。

### 関連コマンド

ENABLE SWITCH PORT ( 304 ページ )

SHOW SWITCH PORT ( 509 ページ )

## DISABLE SWITCH PORT AUTOMDI

カテゴリー：スイッチング / ポート

**DISABLE SWITCH PORT={*port-list*|ALL} AUTOMDI**

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

指定したスイッチポートで MDI/MDI-X 自動切替を無効にする。デフォルトは有効。

本コマンドで MDI/MDI-X 自動切替を無効にした直後、スイッチポートは MDI-X になる (SET SWITCH PORT コマンドの POLARITY パラメーターで変更可能)。

### パラメーター

**PORT** ポート番号

### 関連コマンド

ENABLE SWITCH PORT AUTOMDI (305 ページ)

SET SWITCH PORT (387 ページ)

SHOW SWITCH PORT (509 ページ)

## DISABLE SWITCH PORT EGRESSQUEUE

カテゴリー：スイッチング / ポート

**DISABLE SWITCH PORT**={*port-list*|**ALL**} **EGRESSQUEUE**[=*queue-list*]

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

*queue-list*: 送信キュー (0～7。ハイフン、カンマを使った複数指定も可能)

### 解説

指定ポートの送信キューを無効にする。デフォルトではすべての送信キューが有効。  
無効状態のキューに割り当てられたパケットは破棄される。

### パラメーター

**PORT** スイッチポート番号

**EGRESSQUEUE** 送信キュー番号

### 関連コマンド

ENABLE SWITCH PORT EGRESSQUEUE ( 306 ページ )

SET QOS PORT EGRESSQUEUE ( 367 ページ )

SHOW QOS PORT ( 468 ページ )

SHOW SWITCH PORT ( 509 ページ )

## DISABLE SWITCH PORT FLOW

カテゴリー：スイッチング / ポート

**DISABLE SWITCH PORT**={*port-list*|ALL} **FLOW**={PAUSE}

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

指定したスイッチポートでフローコントロール (802.3x PAUSE) を無効にする。デフォルトは無効。

### パラメーター

**PORT** ポート番号

**FLOW** フロー制御方式。PAUSE (802.3x PAUSE。オートネゴシエーションによる Full Duplex 接続時) のみサポート。

### 備考・注意事項

本製品の実装では PAUSE フレームの受信 (受信により送信を一時停止) のみをサポート。PAUSE フレームの送信についてはサポート対象外。

### 関連コマンド

ENABLE SWITCH PORT FLOW (307 ページ)

SHOW SWITCH PORT (509 ページ)

## DISABLE SWITCH PORT VLAN

カテゴリー：スイッチング / ポート

**DISABLE SWITCH PORT**={*port-list*|ALL} **VLAN**[={*vlanname*|1..4094|ALL}]

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

*vlanname*: VLAN 名 (1~32 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字は区別しない)

### 解説

指定した VLAN においてのみ、スイッチポートをディセーブルにする。

### パラメーター

**PORT** ポート番号

**VLAN** VLAN 名または VLAN ID (VID)。省略時および ALL 指定時は、該当ポートが所属しているすべての VLAN が対象になる。

### 備考・注意事項

本コマンドを実行すると、該当ポートでは自動的にインGRESフィルタリング (SET SWITCH PORT コマンドの INFILTERING パラメーター) が有効になる。

### 関連コマンド

ENABLE SWITCH PORT VLAN (308 ページ)

SET SWITCH PORT (387 ページ)

SHOW SWITCH PORT (509 ページ)

## DISABLE SWITCH STPFORWARD

カテゴリー：スイッチング / 一般コマンド

**DISABLE SWITCH STPFORWARD**

### 解説

BPDU フォワーディングを無効にする。デフォルトは無効。

### 関連コマンド

ENABLE SWITCH STPFORWARD ( 309 ページ )

SHOW SWITCH ( 490 ページ )

## ENABLE DHCP Snooping

カテゴリー：スイッチング / DHCP Snooping

### **ENABLE DHCP Snooping**

#### 解説

DHCP Snooping を有効にする。デフォルトは無効。

#### 関連コマンド

DISABLE DHCP Snooping ( 253 ページ )

SHOW DHCP Snooping ( 401 ページ )



## ENABLE DHCP Snooping ARPSECURITY

カテゴリー：スイッチング / DHCP Snooping

### ENABLE DHCP Snooping ARPSECURITY

#### 解説

DHCP Snooping のオプション機能である ARP セキュリティーを有効にする。デフォルトは無効。

#### 備考・注意事項

本機能は、DHCP Snooping が有効になっていないと動作しない。

バインディングデータベースに MAC アドレス無指定のスタティックエントリーを追加している場合は、ARP セキュリティーを有効化してはならない。

#### 関連コマンド

ADD DHCP Snooping BINDING ( 173 ページ )

DISABLE DHCP Snooping ( 253 ページ )

DISABLE DHCP Snooping ARPSECURITY ( 254 ページ )

ENABLE DHCP Snooping LOG ( 282 ページ )

SHOW DHCP Snooping ( 401 ページ )

## ENABLE DHCP Snooping LOG

カテゴリー：スイッチング / DHCP Snooping

**ENABLE DHCP Snooping LOG=ARPSECURITY**

### 解説

DHCP Snooping のログ機能を有効にする。デフォルトは無効。

### パラメーター

**LOG** ログに記録するイベントの種類。現時点では ARPSECURITY のみサポート。ARPSECURITY イベントは、ARP セキュリティ機能によってバインディングデータベース未登録の送信元からの ARP パケットを破棄したときに発生する。

### 関連コマンド

DISABLE DHCP Snooping LOG ( 255 ページ )

ENABLE DHCP Snooping ( 280 ページ )

ENABLE DHCP Snooping ARPSECURITY ( 281 ページ )

SHOW DHCP Snooping ( 401 ページ )

SHOW LOG ( 「運用・管理」の 393 ページ )

## ENABLE DHCP Snooping OPTION82

カテゴリー：スイッチング / DHCP Snooping

### ENABLE DHCP Snooping OPTION82

#### 解説

DHCP Snooping のオプション機能であるリレーエージェント情報オプション（オプションコード 82）の付加・検査・削除を有効にする。デフォルトは無効。

本機能を有効にした場合、Untrusted ポートで受信したクライアントからの DHCP/BOOTP パケットを転送するときに、リレーエージェント情報オプションを挿入する。同オプションには次の情報が含まれる。

- ・ Remote-ID: 本製品の MAC アドレス
- ・ Circuit-ID: クライアントパケットを受信したスイッチポートと VLAN ID
- ・ Subscriber-ID: (オプション) 任意の文字列 (SET DHCP Snooping PORT コマンドの SUBSCRIBERID パラメーターで設定した場合のみ含める)

受信した DHCP/BOOTP パケットにリレーエージェント情報オプションがすでに付加されていた場合の動作は、受信ポートの DHCP Snooping ポート種別によって異なる。なお、このときの動作は、本機能の有効・無効とは関係なくつねに同じとなる。

- ・ Untrusted ポートでは破棄
- ・ Trusted ポートでは変更せずにそのまま転送

本機能が有効のとき、サーバーからの戻りパケットを Untrusted ポート配下のクライアントに転送するときは、クライアントが Untrusted ポートに直接接続されている場合にかぎって同オプションを削除する。

#### 備考・注意事項

本機能は、DHCP Snooping が有効になっていないと動作しない。

本機能は、DHCP/BOOTP リレーの同種機能（ENABLE BOOTP RELAY OPTION82 コマンド）とは併用できない。

#### 関連コマンド

DISABLE DHCP Snooping (253 ページ)

DISABLE DHCP Snooping OPTION82 (256 ページ)

SHOW DHCP Snooping (401 ページ)

## ENABLE EPSR

カテゴリー：スイッチング / イーサネットリングプロテクション (EPSR)

**ENABLE EPSR**={*epsrname*|ALL}

*epsrname*: EPSR ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ ) ハイフンを使用可能。大文字小文字を区別しない)

### 解説

EPSR ドメインを有効化する。

### パラメーター

**EPSR** EPSR ドメイン名。ALL を指定した場合は、すべての EPSR ドメインが対象となる。

### 関連コマンド

CREATE EPSR ( 205 ページ )

DISABLE EPSR ( 257 ページ )

SHOW EPSR ( 411 ページ )

## ENABLE EPSR DEBUG

カテゴリー：スイッチング / イーサネットリングプロテクション (EPSR)

**ENABLE EPSR**={*epsrname*|ALL} **DEBUG**={INFO|MSG|PKT|STATE|ALL}  
 [OUTPUT=CONSOLE] [TIMEOUT={1..4000000000|NONE}]

*epsrname*: EPSR ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

### 解説

EPSR ドメインのデバッグオプションを有効化する。デフォルトはすべて無効。

### パラメーター

**EPSR** EPSR ドメイン名。ALL を指定した場合は、すべての EPSR ドメインが対象となる。

**DEBUG** 有効にするデバッグオプション。INFO (EPSR に関する全般的情報を表示)、MSG (EPSR パケットをデコードして表示)、PKT (EPSR パケットを ASCII 表示)、STATE (EPSR の状態遷移を表示)、ALL (すべてのオプション) から選択する。

**OUTPUT** デバッグ情報の出力先を指定する。CONSOLE (コンソール) のみ指定可能。省略時はコマンドを入力した端末画面に出力される。本オプションは、スクリプト中での使用を想定したもの。

**TIMEOUT** デバッグオプションの有効期限 (秒)。省略時は以前に設定した値、あるいは、無期限。

### 関連コマンド

CREATE EPSR (205 ページ)

DISABLE EPSR DEBUG (258 ページ)

SHOW EPSR DEBUG (416 ページ)

## ENABLE LACP

カテゴリー：スイッチング / LACP (IEEE 802.3ad)

### **ENABLE LACP**

#### 解説

LACP モジュールを有効にする。デフォルトは無効。

#### 関連コマンド

ADD LACP PORT ( 176 ページ )

DELETE LACP PORT ( 229 ページ )

DISABLE LACP ( 259 ページ )

SHOW LACP ( 417 ページ )

## ENABLE LACP DEBUG

カテゴリー：スイッチング / LACP (IEEE 802.3ad)

**ENABLE LACP DEBUG={MSG|PACKET|STATE|TRACE|ALL}**

### 解説

LACP モジュールのデバッグを有効にする。デフォルトはすべて無効。

### パラメーター

**DEBUG** デバッグオプション。MSG (LACP パケットをデコードして表示)、PKT (LACP パケットを 16 進表示)、STATE (状態遷移を表示)、TRACE (関数呼び出しをトレース表示)、ALL (すべてのオプション) から選択する。

### 備考・注意事項

本コマンドは、トラブルシューティング時など、内部情報の確認が必要な場合を想定したものですので、ご使用に際しては弊社技術担当にご相談ください。

### 関連コマンド

DISABLE LACP DEBUG (260 ページ)

SHOW LACP (417 ページ)

## ENABLE MSTP

カテゴリー：スイッチング / マルチプルスパニングツリープロトコル (MSTP)

### ENABLE MSTP

#### 解説

マルチプルスパニングツリープロトコルを有効にする。デフォルトは無効。

スパニングツリープロトコル (STP/RSTP) が有効のときは、マルチプルスパニングツリープロトコル (MSTP) を有効化できないので、あらかじめ DISABLE STP コマンドを実行してスパニングツリープロトコル (STP/RSTP) あるいは、STP ドメインを無効化しておくこと。

また、イーサネットリングプロテクション (EPSR) を使用しているときも、マルチプルスパニングツリープロトコル (MSTP) を有効化できない。

#### 関連コマンド

DISABLE MSTP (261 ページ)

DISABLE STP (265 ページ)

SHOW MSTP (425 ページ)



## ENABLE PORTAUTH

カテゴリー：スイッチング / ポート認証

**ENABLE PORTAUTH** [= {8021X|MACBASED}]

### 解説

ポート認証機能（802.1X 認証または MAC ベース認証）を有効にする。デフォルトはどちらも無効。  
ポート認証を使用するためには、個々のスイッチポートでもポート認証機能を有効にする必要がある  
（ENABLE PORTAUTH PORT コマンド）。

### パラメーター

**PORTAUTH** 認証メカニズム。8021X（802.1X 認証）、MACBASED（MAC ベース認証）から選択する。  
省略時は 8021X と見なされる。

### 関連コマンド

DISABLE PORTAUTH（262 ページ）  
DISABLE PORTAUTH PORT（264 ページ）  
ENABLE PORTAUTH PORT（291 ページ）  
SHOW PORTAUTH MULTISUPPLICANT PORT（447 ページ）  
SHOW PORTAUTH PORT（451 ページ）

## ENABLE PORTAUTH DEBUG

カテゴリー：スイッチング / ポート認証

**ENABLE PORTAUTH** [= {8021X|MACBASED}] **DEBUG** = {ALL|PACKET|STATE}  
**PORT** = {*port-list*|ALL}

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

指定ポートで、ポート認証機能 (802.1X 認証または MAC ベース認証) のデバッグを有効にする。デフォルトは全ポート無効。

### パラメーター

**PORTAUTH** 認証メカニズム。8021X (802.1X 認証) \ MACBASED (MAC ベース認証) から選択する。省略時は 8021X と見なされる。

**DEBUG** デバッグオプション。ALL (すべて) \ PACKET (パケット送受信) \ STATE (状態遷移) から選択する。PACKET は、PORTAUTH に 8021X を指定したときだけ有効。

**PORT** スイッチポート。複数指定が可能。

### 備考・注意事項

本コマンドは、トラブルシューティング時など、内部情報の確認が必要な場合を想定したものですので、ご使用に際しては弊社技術担当にご相談ください。

### 関連コマンド

DISABLE PORTAUTH DEBUG (263 ページ)

ENABLE PORTAUTH (289 ページ)

ENABLE PORTAUTH PORT (291 ページ)

SHOW PORTAUTH PORT (451 ページ)

## ENABLE PORTAUTH PORT

カテゴリー：スイッチング / ポート認証

```
ENABLE PORTAUTH[=8021X] PORT={port-list|ALL} TYPE=AUTHENTICATOR
[CONTROL={AUTHORISED|AUTO|UNAUTHORISED}] [MAXREQ=1..10] [MODE={MULTI|
SINGLE}] [PIGGYBACK={TRUE|FALSE}] [QUIETPERIOD=0..65535]
[REAUTHENABLED={TRUE|FALSE}] [REAUTHMAX=1..10] [REAUTHPERIOD=1..86400]
[SERVERTIMEOUT=1..60] [SUPPTIMEOUT=1..60] [TXPERIOD=1..65535]
[GUESTVLAN={vlanname|1..4094|NONE}] [SECUREVLAN={ON|OFF}]
[VLANASSIGNMENT={ENABLED|DISABLED}] [MIBRESET={ENABLED|DISABLED}]
[TRAP={SUCCESS|FAILURE|BOTH|NONE}]
```

```
ENABLE PORTAUTH[=8021X] PORT={port-list|ALL} TYPE=BOTH
[CONTROL={AUTHORISED|UNAUTHORISED|AUTO}] [MAXREQ=1..10] [MODE=SINGLE]
[PIGGYBACK={TRUE|FALSE}] [QUIETPERIOD=0..65535] [REAUTHENABLED={TRUE|
FALSE}] [REAUTHMAX=1..10] [REAUTHPERIOD=1..86400] [SERVERTIMEOUT=1..60]
[SUPPTIMEOUT=1..60] [TXPERIOD=1..65535] [GUESTVLAN={vlanname|1..4094|
NONE}] [VLANASSIGNMENT={ENABLED|DISABLED}] [MIBRESET={ENABLED|DISABLED}]
[TRAP={SUCCESS|FAILURE|BOTH|NONE}] [AUTHPERIOD=1..60]
[HELDPERIOD=0..65535] [MAXSTART=1..10] [STARTPERIOD=1..60]
[USERNAME=login-name PASSWORD=password [METHOD={OTP [ENCRYPTION={MD4|
MD5}}]|STANDARD}]]
```

```
ENABLE PORTAUTH[=8021X] PORT={port-list|ALL} TYPE=SUPPLICANT
[AUTHPERIOD=1..60] [HELDPERIOD=0..65535] [MAXSTART=1..10]
[STARTPERIOD=1..60] [USERNAME=login-name PASSWORD=password [METHOD={OTP
[ENCRYPTION={MD4|MD5}}]|STANDARD}]]
```

```
ENABLE PORTAUTH=MACBASED PORT={port-list|ALL} [CONTROL={AUTHORISED|AUTO|
UNAUTHORISED}] [QUIETPERIOD=0..65535] [REAUTHENABLED={TRUE|FALSE}]
[REAUTHPERIOD=1..86400] [SECUREVLAN={ON|OFF}] [VLANASSIGNMENT={ENABLED|
DISABLED}] [MIBRESET={ENABLED|DISABLED}] [TRAP={SUCCESS|FAILURE|BOTH|
NONE}]
```

*port-list*: スイッチポート番号 (1~。ハイフン、カンマを使った複数指定も可能)

*vlanname*: VLAN 名 (1~32 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

*login-name*: ログイン名 (1~64 文字。英数字のみ使用可能)

*password*: パスワード (1~64 文字。英数字のみ使用可能)

### 解説

指定ポートで、ポート認証機能(802.1X 認証または MAC ベース認証)を有効にする。各ポートでは、802.1X 認証か MAC ベース認証のどちらか一方だけを使用できる。また、802.1X 認証を使用する場合は、各ポートを Authenticator、Supplicant、Authenticator かつ Supplicant (Both) のいずれかに設定できる。デフォルトは全ポート無効。

## パラメーター

**PORTAUTH** 認証メカニズム。8021X (802.1X 認証) MACBASED (MAC ベース認証) から選択する。省略時は 8021X と見なされる。

**PORT** スイッチポート。複数指定が可能。

**TYPE** (802.1X ポート)802.1X 認証におけるスイッチポートの役割。AUTHENTICATOR( Authenticator ポート) SUPPLICANT( Supplicant ポート) BOTH( Authenticator ポートかつ Supplicant ポート) のいずれかを指定する。なお、Multi-Supplicant モード (MODE=MULTI) を使用する場合、TYPE=BOTH は指定できない。TYPE=AUTHENTICATOR を指定すること。

**CONTROL** (802.1X Authenticator ポート、MAC ベース認証ポート) 手動設定による Authenticator ポートの状態。AUTO( 認証結果に応じて変動) UNAUTHORISED( 未認証固定) AUTHORISED ( 認証済み固定) から選択する。デフォルトは AUTO。通常は AUTO のままでよい。ただし、RADIUS サーバーの接続先ポートを Authenticator に設定している場合は、本パラメーターを AUTHORISED に設定する必要がある。

**MAXREQ** (802.1X Authenticator ポート) Supplicant に対する EAPOL-Request パケットの最大再送回数。デフォルトは 2 回。

**MODE** (802.1X Authenticator ポート) Authenticator ポートのモード。Supplicant が 1 台だけ接続されていることを想定した Single-Supplicant モード (MODE=SINGLE) と、Supplicant が複数台接続されていることを想定した Multi-Supplicant モード (MODE=MULTI) がある。Single-Supplicant モードでは、該当ポート配下に最初に接続された Supplicant だけが認証対象となる (その他の Supplicant からの通信を許可するかどうかは、PIGGYBACK パラメーターで制御可能)。Multi-Supplicant モードでは、該当ポート配下に接続された個々の Supplicant を識別し、個別に認証を行う。なお、Multi-Supplicant モードを使用する場合、TYPE パラメーターには BOTH を指定できない。AUTHENTICATOR を指定すること。デフォルトは SINGLE。

**PIGGYBACK** (802.1X Single-Supplicant Authenticator ポート) Single-Supplicant モード (MODE=SINGLE) において、最初に接続された Supplicant の認証に成功した後、他のデバイスからのパケットも許可するかどうかを指定する。TRUE なら許可、FALSE なら拒否。デフォルトは TRUE。

**QUIETPERIOD** (802.1X Authenticator ポート、MAC ベース認証ポート) Supplicant の認証に失敗した後、Supplicant との通信を拒否する期間 (秒)。この期間中は受信したパケットをすべて破棄する。デフォルトは 60 秒。

**REAUTHENABLED** (802.1X Authenticator ポート、MAC ベース認証ポート) 認証に成功した Supplicant を定期的に再認証するかどうか。TRUE なら再認証する、FALSE なら再認証しない。デフォルトは FALSE。

**REAUTHMAX** (802.1X Authenticator ポート) 再認証時における EAPOL-Request パケットの最大再送回数。デフォルトは 2 回。

**REAUTHPERIOD** (802.1X Authenticator ポート、MAC ベース認証ポート) Supplicant の再認証間隔 (秒)。デフォルトは 3600 秒。

**SERVERTIMEOUT** (802.1X Authenticator ポート) RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間 (秒)。デフォルトは 30 秒。

**SUPPTIMEOUT** (802.1X Authenticator ポート) Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間 (秒)。デフォルトは 30 秒。

**TXPERIOD** (802.1X Authenticator ポート) Supplicant に EAPOL パケットを再送信する間隔 (秒)。デフォルトは 30 秒。

**GUESTVLAN** (802.1X Single-Supplicant Authenticator ポート) ゲスト VLAN を指定する。装置上に設定されている VLAN の名前か VLAN ID を指定すること。NONE はゲスト VLAN を使用しないことを意味する。EAPOL パケットをまだ受信していないとき、該当ポートはゲスト VLAN の所属となる。最初の EAPOL パケットを受信すると、該当ポートはゲスト VLAN から削除され、本来の所属 VLAN に復帰する。本パラメーターは、Single-Supplicant モード (MODE=SINGLE) でのみ有効。デフォルトは NONE。

**SECUREVLAN** (802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート) 802.1X 認証の Multi-Supplicant モード (MODE=MULTI) か MAC ベース認証でダイナミック VLAN を使用しているとき、2 番目以降の Supplicant の認証方法を指定する。本パラメーターに ON を指定した場合は、2 番目以降の Supplicant は、最初に認証を通った Supplicant と同じ VLAN でないと認証されない。一方、OFF を指定した場合は、有効な VLAN でありさえすれば認証をパスする。ただし、2 番目以降の Supplicant は、実際には最初に認証をパスした Supplicant と同じ VLAN の所属となる。本パラメーターは、Multi-Supplicant モード (MODE=MULTI) のポートか、MAC ベース認証のポートでのみ使用可能。デフォルトは ON。

**VLANASSIGNMENT** (802.1X Authenticator ポート、MAC ベース認証ポート) ダイナミック VLAN の有効・無効。有効時は、RADIUS サーバーが返してきた Tunnel-Private-Group-ID の値をもとに、指定ポートの所属 VLAN を動的に変更する。デフォルトは ENABLED。

**MIBRESET** (802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート) 802.1X 認証の Multi-Supplicant モード (MODE=MULTI) か MAC ベース認証を使用しているポートにおいて、古い Supplicant 情報をエージアウトするかどうか。デフォルトは ENABLED。

**TRAP** (802.1X Authenticator ポート、MAC ベース認証ポート) ポート認証機能に関する SNMP トラップを送信するかどうか。SUCCESS を指定した場合は、Supplicant の認証に成功したときと、認証情報が時間切れになったときに SNMP トラップを送信する。FAILURE を指定した場合は、Supplicant の認証に失敗したときに SNMP トラップを送信する。BOTH を指定したときは、SUCCESS と FAILURE の両方の場合に SNMP トラップを送信する。NONE はトラップを送信しない。デフォルトは NONE。

**AUTHPERIOD** (802.1X Supplicant ポート) Authenticator に EAP-Response パケットを送信した後、Authenticator からの応答を待つ時間 (秒)。デフォルトは 30 秒。

**HELDPERIOD** (802.1X Supplicant ポート) 認証失敗後、Authenticator との通信を試みない期間 (秒)。デフォルトは 60 秒。

**MAXSTART** (802.1X Supplicant ポート) EAPOL-Start パケットの最大送信回数。Supplicant ポートは、EAPOL-Start パケットを MAXSTART 回送信しても応答がない場合、Authenticator が存在しておらずポート認証の必要はないと判断する。デフォルトは 3 回。

**STARTPERIOD** (802.1X Supplicant ポート) Authenticator に EAPOL-Start パケットを再送信する間隔 (秒)。デフォルトは 30 秒。

**USERNAME** (802.1X Supplicant ポート) 指定スイッチポートが Supplicant として動作する場合に使

ユーザー名。必ず PASSWORD パラメーターと組で指定すること。本パラメーターを設定した場合、該当ポートでは、SET PORTAUTH USERNAME コマンドで設定するグローバルなユーザー名・パスワード・暗号化方式ではなく、本コマンドで設定した値が使用される。

**PASSWORD** (802.1X Supplicant ポート) 指定スイッチポートが Supplicant として動作する場合に使うパスワード。必ず USERNAME パラメーターと組で指定すること。METHOD パラメーターに STANDARD を指定した場合、または、METHOD パラメーターを省略した場合は、6～63 文字の文字列を指定する。METHOD パラメーターに OTP を指定した場合は、10～63 文字の文字列（認証サーバー上で設定した OTP Initialisation Password と同じ値）を指定する。本パラメーターを設定した場合、該当ポートでは、SET PORTAUTH USERNAME コマンドで設定するグローバルなユーザー名・パスワード・暗号化方式ではなく、本コマンドで設定した値が使用される。

**METHOD** (802.1X Supplicant ポート) パスワード送信時の暗号化方式。STANDARD (EAP-MD5) または OTP (One-Time Password) から選択する。OTP を指定した場合は、ENCRYPTION パラメーターでワンタイムパスワードの生成アルゴリズムも指定する必要がある。デフォルトは STANDARD。

**ENCRYPTION** (802.1X Supplicant ポート) ワンタイムパスワードの生成アルゴリズム。MD4、MD5 から選択する。デフォルトは MD5。METHOD パラメーターに OTP を指定した場合の必須パラメーター。

### 備考・注意事項

802.1X 認証を有効にしたポート (Authenticator、Supplicant とともに) では、ポートトラッキング、スパニングツリープロトコル、ポートセキュリティを使用できない。また、Authenticator ポートをタグ付きに設定することはできない。

Multi-Supplicant モード (MODE=MULTI) は 802.1X 規格に準拠しておらず、セキュリティ上のリスクがあるため、通常は Single-Supplicant モード (MODE=SINGLE) のまま使用すること。

### 関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (170 ページ)

ENABLE PORTAUTH (289 ページ)

ENABLE PORTAUTH PORT (291 ページ)

SET PORTAUTH PORT (346 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (350 ページ)

SHOW PORTAUTH (441 ページ)

SHOW PORTAUTH COUNTER (444 ページ)

SHOW PORTAUTH MULTISUPPLICANT PORT (447 ページ)

SHOW PORTAUTH PORT (451 ページ)

SHOW PORTAUTH TIMER (456 ページ)

## ENABLE STP

カテゴリー：スイッチング / スパニングツリープロトコル (STP/RSTP)

**ENABLE STP**{=*stpname*|**ALL**}

*stpname*: STP ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

### 解説

STP ドメイン、あるいは、スイッチ全体でスパニングツリープロトコルを有効にする。デフォルトはどちらも無効。

### パラメーター

**STP** STP ドメイン名。

### 関連コマンド

CREATE STP ( 222 ページ )

DESTROY STP ( 250 ページ )

DISABLE STP ( 265 ページ )

SET STP ( 377 ページ )

SHOW STP ( 480 ページ )



## ENABLE STP DEBUG

カテゴリー：スイッチング / スパニングツリープロトコル (STP/RSTP)

```
ENABLE STP={stpname|ALL} DEBUG={MSG|PKT|STATE|ALL} [OUTPUT=CONSOLE]
[TIMEOUT={1..4000000000|NONE}]
```

*stpname*: STP ドメイン名 (1~15 文字。英数字とアンダースコア (-)、ハイフンを使用可能。大文字小文字を区別しない)

### 解説

指定した STP ドメインのデバッグオプションを有効にする。

デバッグをオンにすると、端末 (コンソールや Telnet クライアント) 画面に大量のデバッグ情報が出力されるため注意が必要。

### パラメーター

**STP** STP ドメイン名。

**DEBUG** デバッグオプション。MSG (STP パケットをデコードして表示)、PKT (STP パケットを ASCII 表示)、STATE (ポートの状態遷移を表示)、ALL (すべてのオプション) から選択する。

**OUTPUT** デバッグ情報の出力先を指定する。CONSOLE (コンソール) のみ指定可能。省略時はコマンドを入力した端末画面に出力される。本オプションは、スクリプト中での使用を想定したもの。

**TIMEOUT** デバッグオプションの有効期限 (秒)。省略時は以前に設定した値、あるいは、無期限。

### 備考・注意事項

本コマンドは、トラブルシューティング時など、内部情報の確認が必要な場合を想定したものですので、ご使用に際しては弊社技術担当にご相談ください。

### 関連コマンド

DISABLE STP DEBUG (266 ページ)

SHOW STP DEBUG (486 ページ)



## ENABLE STP PORT

カテゴリー：スイッチング / スパニングツリープロトコル (STP/RSTP)

**ENABLE STP PORT**={*port-list*|**ALL**}

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

指定ポートでスパニングツリープロトコルを有効にする。

有効にすると、該当ポートで BPDU が生成されるようになり、所属ドメインのスパニングツリーが再構成される。

### パラメーター

**PORT** ポート番号。複数指定が可能。ALL を指定した場合はすべてのスイッチポートでスパニングツリープロトコルを有効にする。

### 関連コマンド

DISABLE STP PORT (267 ページ)

SET STP PORT (379 ページ)

SHOW STP PORT (487 ページ)

## ENABLE STP PORT DEBUG

カテゴリー：スイッチング / スパニングツリープロトコル (STP/RSTP)

**ENABLE STP PORT**={*port-list*|ALL} **DEBUG**={MSG|PKT|STATE|ALL}  
 [OUTPUT=CONSOLE] [TIMEOUT={1..4000000000|NONE}]

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

STP ポートのデバッグオプションを有効にする。

### パラメーター

**PORT** ポート番号。複数指定が可能。

**DEBUG** デバッグオプション。MSG (STP パケットをデコードして表示)、PKT (STP パケットを ASCII 表示)、STATE (ポートの状態遷移を表示)、ALL (すべてのオプション) から選択する。

**OUTPUT** デバッグ情報の出力先を指定する。CONSOLE (コンソール) のみ指定可能。省略時はコマンドを入力した端末画面に出力される。本オプションは、スクリプト中での使用を想定したもの。

**TIMEOUT** デバッグオプションの有効期限 (秒)。省略時は以前に設定した値、あるいは、無期限。

### 備考・注意事項

本コマンドは、トラブルシューティング時など、内部情報の確認が必要な場合を想定したものですので、ご使用に際しては弊社技術担当にご相談ください。

### 関連コマンド

DISABLE STP DEBUG (266 ページ)

DISABLE STP PORT DEBUG (268 ページ)

ENABLE STP (295 ページ)

SHOW STP DEBUG (486 ページ)

## ENABLE SWITCH AGEINGTIMER

カテゴリー：スイッチング / フォワーディングデータベース

### **ENABLE SWITCH AGEINGTIMER**

#### 解説

FDB のエージングタイマーを有効にし、ダイナミックエントリーがエージアウトされるようにする。デフォルトは有効。

#### 関連コマンド

DISABLE SWITCH AGEINGTIMER ( 269 ページ )

SET SWITCH AGEINGTIMER ( 381 ページ )

SHOW SWITCH ( 490 ページ )

## ENABLE SWITCH HASH

カテゴリー：スイッチング / ポート

**ENABLE SWITCH HASH**={L2|L3|L4}[,...]

### 解説

ポートランキングの送出ポート決定アルゴリズムにおいて、指定した種類のヘッダー情報を使うよう設定する。

デフォルトでは、L2 と L3 のヘッダー情報を使用して送出ポートを決定する。

### パラメーター

**HASH** 送出ポート決定アルゴリズムで使用するヘッダー情報の種別。L2 (送信元・宛先 MAC アドレス)、L3 (始点・終点 IP アドレス)、L4 (始点・終点ポート) から選択する。カンマ区切りで複数指定が可能。

### 備考・注意事項

ルーティング後トランクグループから送信される IP パケットの送出ポートは、本コマンドの設定とは関係なく、L3 ヘッダー情報にのみ基づいて決定される。

### 関連コマンド

ADD SWITCH TRUNK (190 ページ)

CREATE SWITCH TRUNK (223 ページ)

DISABLE SWITCH HASH (270 ページ)

SHOW SWITCH (490 ページ)

## ENABLE SWITCH LEARNING

カテゴリー：スイッチング / フォワーディングデータベース

### **ENABLE SWITCH LEARNING**

#### 解説

フォワーディングデータベース（FDB）の学習機能を有効にする。デフォルトは有効。

#### 関連コマンド

DISABLE SWITCH LEARNING (271 ページ)

SHOW SWITCH (490 ページ)

## ENABLE SWITCH MCLIMITING

カテゴリー：スイッチング / ポート

### ENABLE SWITCH MCLIMITING

#### 解説

マルチキャストパケットの受信レート制限機能を有効にする。デフォルトは無効。

本機能の有効時は、各スイッチポートにおいて、マルチキャストパケットおよびブロードキャストパケットの受信レートが、SET SWITCH PORT コマンドの BCLIMIT パラメーターで指定された値までに制限される。本機能の無効時は、マルチキャストパケットの受信レートは制限されないが、BCLIMIT パラメーターが NONE 以外に設定されていれば、ブロードキャストパケットの受信レートは制限される。

なお、マルチキャストパケットは制限するが、ブロードキャストパケットは制限しないという設定はできない。

#### 関連コマンド

DISABLE SWITCH MCLIMITING ( 272 ページ )

SET SWITCH PORT ( 387 ページ )

SHOW SWITCH PORT ( 509 ページ )

## ENABLE SWITCH MIRROR

カテゴリー：スイッチング / ポート

### **ENABLE SWITCH MIRROR**

#### 解説

ポートミラーリング機能を有効にする。ミラーポートの設定は変化しない。デフォルトは無効。

#### 関連コマンド

DISABLE SWITCH MIRROR ( 273 ページ )

SET SWITCH MIRROR ( 385 ページ )

SET SWITCH PORT ( 387 ページ )

SHOW SWITCH ( 490 ページ )

SHOW SWITCH PORT ( 509 ページ )

## ENABLE SWITCH PORT

カテゴリー：スイッチング / ポート

**ENABLE SWITCH PORT**={*port-list*|ALL}

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

スイッチポートをイネーブルにする。

### パラメーター

PORT ポート番号

### 備考・注意事項

ポートセキュリティ機能によってロック後ディセーブルにされたポートは、本コマンドでイネーブルにできない。その場合は、SET SWITCH PORT コマンドで LEARN パラメーターに 0 を指定し、ポートセキュリティをオフにする必要がある。

### 関連コマンド

DISABLE SWITCH PORT ( 274 ページ )

SHOW SWITCH PORT ( 509 ページ )



## ENABLE SWITCH PORT AUTOMDI

カテゴリー：スイッチング / ポート

**ENABLE SWITCH PORT={*port-list*|ALL} AUTOMDI**

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

指定したスイッチポートで MDI/MDI-X 自動切替を有効にする。オートネゴシエーションがオンのポートではデフォルト有効。

オートネゴシエーションがオフのポートでは、MDI/MDI-X 自動切替を有効化できない。

### パラメーター

**PORT** ポート番号

### 関連コマンド

DISABLE SWITCH PORT AUTOMDI (275 ページ)

SET SWITCH PORT (387 ページ)

SHOW SWITCH PORT (509 ページ)

## ENABLE SWITCH PORT EGRESSQUEUE

カテゴリー：スイッチング / ポート

**ENABLE SWITCH PORT**={*port-list*|ALL} **EGRESSQUEUE**[=*queue-list*]

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

*queue-list*: 送信キュー (0～7。ハイフン、カンマを使った複数指定も可能)

### 解説

指定ポートの送信キューを有効にする。デフォルトではすべての送信キューが有効。

### パラメーター

**PORT** スイッチポート番号

**EGRESSQUEUE** 送信キュー番号

### 関連コマンド

DISABLE SWITCH PORT EGRESSQUEUE (276 ページ)

SET QOS PORT EGRESSQUEUE (367 ページ)

SHOW QOS PORT (468 ページ)

SHOW SWITCH PORT (509 ページ)

## ENABLE SWITCH PORT FLOW

カテゴリー：スイッチング / ポート

**ENABLE SWITCH PORT={*port-list*|ALL} FLOW={PAUSE}**

*port-list*: スイッチポート番号 (1~。ハイフン、カンマを使った複数指定も可能)

### 解説

指定したスイッチポートでフローコントロール (802.3x PAUSE) を有効にする。デフォルトは無効。  
有効に設定している場合は、オートネゴシエーション時に AS/SY ビットをオンにして、フローコントロール動作可であることを対向機器に通知する (無効のときは AS/SY ビットオフ)。

### パラメーター

**PORT** ポート番号

**FLOW** フロー制御方式。PAUSE (802.3x PAUSE。オートネゴシエーションによる Full Duplex 接続時) のみサポート。

### 備考・注意事項

本製品の実装では PAUSE フレームの受信 (受信により送信を一時停止) のみをサポート。PAUSE フレームの送信についてはサポート対象外。

### 関連コマンド

DISABLE SWITCH PORT FLOW (277 ページ)

SHOW SWITCH PORT (509 ページ)

## ENABLE SWITCH PORT VLAN

カテゴリー：スイッチング / ポート

**ENABLE SWITCH PORT**={*port-list*|ALL} **VLAN**[={*vlanname*|1..4094|ALL}]

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

*vlanname*: VLAN 名 (1～32 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字は区別しない)

### 解説

指定した VLAN においてのみ、スイッチポートをイネーブルにする。

### パラメーター

**PORT** ポート番号

**VLAN** VLAN 名または VLAN ID (VID)。省略時および ALL 指定時は、該当ポートが所属しているすべての VLAN が対象になる。

### 備考・注意事項

本コマンドを実行すると、該当ポートでは自動的にインGRESフィルタリング (SET SWITCH PORT コマンドの INFILTERING パラメーター) が無効になる (ただし、該当ポートがまだ特定の VLAN に対してディセーブル状態にある場合、および、手動で該当ポートのインGRESフィルタリングを有効化していた場合は除く)。

### 関連コマンド

DISABLE SWITCH PORT VLAN (278 ページ)

SET SWITCH PORT (387 ページ)

SHOW SWITCH PORT (509 ページ)

## ENABLE SWITCH STPFORWARD

カテゴリー：スイッチング / 一般コマンド

### ENABLE SWITCH STPFORWARD

#### 解説

BPDU フォワーディングを有効にする。デフォルトは無効。

いずれかの STP ドメインでスパニングツリープロトコルが有効になっているときは、エラーメッセージが表示され、BPDU フォワーディングを有効化できない。

また、BPDU フォワーディング有効時に、いずれかの STP ドメインでスパニングツリープロトコルを有効化すると、メッセージが表示され、BPDU フォワーディングは無効化される。

BPDU フォワーディング無効時は、受信した BPDU ( Bridge Procotol Data Unit ) を転送 ( スイッチング ) しないが、有効時は転送する。

#### 関連コマンド

DISABLE SWITCH STPFORWARD ( 279 ページ )

SHOW SWITCH ( 490 ページ )

## PURGE EPSR

カテゴリー：スイッチング / イーサネットリングプロテクション (EPSR)

### PURGE EPSR

#### 解説

EPSR (Ethernet Protected Switching Ring) の設定をデフォルト状態に戻す。

EPSR ドメインはすべて削除され、各種タイマーはデフォルト値に戻る。

本コマンドを実行するとループが発生する可能性があるので、本コマンドを実行する前には、次のいずれかの手順をとることが望ましい。

- ・ DISABLE SWITCH PORT コマンドで該当 VLAN のリング接続用ポートをディセーブルにする
- ・ 該当 VLAN のリング接続用ポートからケーブルを抜く
- ・ DELETE VLAN PORT コマンドで該当 VLAN からリング接続用ポートを削除する

#### 備考・注意事項

ランタイムメモリー上にある EPSR 関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意すること。

#### 関連コマンド

CREATE EPSR ( 205 ページ )

SHOW EPSR ( 411 ページ )

## PURGE LACP

カテゴリー：スイッチング / LACP (IEEE 802.3ad)

### **PURGE LACP**

#### 解説

LACP の設定情報をすべて削除する。

#### 備考・注意事項

ランタイムメモリー上にある LACP 関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意すること。

#### 関連コマンド

DISABLE LACP (259 ページ)

SHOW LACP (417 ページ)

## PURGE MSTP

カテゴリー：スイッチング / マルチプルスパニングツリープロトコル (MSTP)

### **PURGE MSTP**

#### 解説

マルチプルスパニングツリープロトコルの設定をデフォルト状態に戻す。

ユーザーが作成した MST インスタンスはすべて削除され、すべての VLAN は CIST (Common and Internal Spanning Tree) の所属に戻る。各種設定パラメーターもすべてデフォルト値に戻り、MSTP モジュールも無効化される。

#### 備考・注意事項

ランタイムメモリー上にあるマルチプルスパニングツリープロトコル関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意すること。

#### 関連コマンド

SHOW MSTP ( 425 ページ )

SHOW MSTP MSTI ( 436 ページ )



## PURGE PORTAUTH PORT

カテゴリー：スイッチング / ポート認証

**PURGE PORTAUTH** [= {8021X|MACBASED}] **PORT**={*port-list*|ALL}

*port-list*: スイッチポート番号 (1~。ハイフン、カンマを使った複数指定も可能)

### 解説

指定ポートにおけるポート認証機能 (802.1X 認証、MAC ベース認証) の設定をすべて削除する。

### パラメーター

**PORTAUTH** 認証メカニズム。8021X (802.1X 認証)、MACBASED (MAC ベース認証) から選択する。

省略時は 8021X と見なされる。

**PORT** スイッチポート。複数指定が可能。

### 備考・注意事項

ランタイムメモリー上にある、指定ポートの 802.1X 関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意すること。

### 関連コマンド

DISABLE PORTAUTH (262 ページ)

DISABLE PORTAUTH PORT (264 ページ)

SHOW PORTAUTH PORT (451 ページ)

## PURGE QOS

カテゴリー：スイッチング / QoS

### **PURGE QOS**

#### 解説

QoS の設定をすべて削除する。

#### 備考・注意事項

ランタイムメモリー上にある QoS 関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意すること。

#### 関連コマンド

SHOW QOS POLICY ( 465 ページ )

## PURGE STP

カテゴリー：スイッチング / スパニングツリープロトコル (STP/RSTP)

### **PURGE STP**

#### 解説

スパニングツリープロトコルの設定をデフォルト状態に戻す。

default STP 以外の STP ドメインはすべて削除され、各種タイマー（Hello Time など）はデフォルト値に戻る。

#### 備考・注意事項

ランタイムメモリー上にあるスパニングツリープロトコル関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意すること。

#### 関連コマンド

RESET STP ( 321 ページ )

SET STP ( 377 ページ )

SET STP PORT ( 379 ページ )

SHOW STP ( 480 ページ )

SHOW STP COUNTER ( 484 ページ )

## RESET DHCP Snooping COUNTER

カテゴリー：スイッチング / DHCP Snooping

### RESET DHCP Snooping COUNTER

#### 解説

DHCP Snooping の統計情報をクリアする。

#### 関連コマンド

SHOW DHCP Snooping COUNTER ( 403 ページ )

## RESET LACP PORT COUNTER

カテゴリー：スイッチング / LACP (IEEE 802.3ad)

**RESET LACP PORT** [= {*port-list* | ALL}] **COUNTER**

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

スイッチポートの LACP 関連統計カウンターをクリアする。

### パラメーター

**PORT** ポート番号。

### 関連コマンド

PURGE LACP (311 ページ)

SHOW LACP (417 ページ)

SHOW LACP PORT (419 ページ)

## RESET MSTP COUNTER PORT

カテゴリー：スイッチング / マルチプルスパニングツリープロトコル (MSTP)

**RESET MSTP COUNTER PORT**=**{*port-list*|ALL}**

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

指定ポートの MSTP 統計カウンターをリセットする。

### パラメーター

**PORT** ポート番号。ALL を指定した場合はすべてのポートが対象となる。

### 関連コマンド

SHOW MSTP COUNTER PORT (434 ページ)

## RESET PORTAUTH PORT

カテゴリー：スイッチング / ポート認証

**RESET PORTAUTH** [= {8021X|MACBASED}] **PORT**={*port-list*|**ALL**}  
 [SUPPLICANTMAC=*macadd*]

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

*macadd*: MAC アドレス (xx-xx-xx-xx-xx-xx の形式)

### 解説

指定ポートにおけるポート認証機能 (802.1X 認証、MAC ベース認証) の状態をリセットする。

### パラメーター

**PORTAUTH** 認証メカニズム。8021X (802.1X 認証)、MACBASED (MAC ベース認証) から選択する。  
 省略時は 8021X と見なされる。

**PORT** スイッチポート。複数指定が可能。

**SUPPLICANTMAC** Supplicant の MAC アドレス。本パラメーターは、Multi-Supplicant モード (MODE=MULTI) のポートか、MAC ベース認証のポートでのみ使用可能。

### 関連コマンド

DISABLE PORTAUTH (262 ページ)

DISABLE PORTAUTH PORT (264 ページ)

ENABLE PORTAUTH (289 ページ)

ENABLE PORTAUTH PORT (291 ページ)

SHOW PORTAUTH MULTISUPPLICANT PORT (447 ページ)

SHOW PORTAUTH PORT (451 ページ)

## RESET PORTAUTH PORT MULTIMIB

カテゴリー：スイッチング / ポート認証

**RESET PORTAUTH** [= {8021X|MACBASED}] **PORT**={*port-list*|ALL} **MULTIMIB**

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

802.1X Multi-SupPLICANT モードの Authenticator ポート、または、MAC ベース認証ポートにおいて、未認証かつ SET PORTAUTH PORT SUPPLICANTMAC コマンドで設定していない SupPLICANT の情報をクリアする。

### パラメーター

**PORTAUTH** 認証メカニズム。8021X (802.1X 認証)、MACBASED (MAC ベース認証) から選択する。省略時は 8021X と見なされる。

**PORT** スイッチポート。複数指定が可能。本コマンドは、Multi-SupPLICANT モード (MODE=MULTI) のポートか、MAC ベース認証のポートでのみ使用可能。

### 関連コマンド

DISABLE PORTAUTH (262 ページ)

DISABLE PORTAUTH PORT (264 ページ)

ENABLE PORTAUTH (289 ページ)

ENABLE PORTAUTH PORT (291 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (350 ページ)

SHOW PORTAUTH MULTISUPPLICANT PORT (447 ページ)

SHOW PORTAUTH PORT (451 ページ)



## RESET STP

カテゴリー：スイッチング / スパニングツリープロトコル (STP/RSTP)

**RESET STP**={*stpname*|**ALL**}

*stpname*: STP ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

### 解説

指定した STP ドメインにおけるスパニングツリープロトコルの状態をリセットする。  
該当 STP ドメインのカウンター、STP 所属ポートのカウンターはすべてリセットされる。

### パラメーター

**STP** STP ドメイン名。ALL を指定した場合はすべての STP ドメインが対象となる。

### 関連コマンド

PURGE STP ( 315 ページ )

SET STP ( 377 ページ )

SHOW STP ( 480 ページ )

SHOW STP COUNTER ( 484 ページ )

## RESET SWITCH

カテゴリー：スイッチング / 一般コマンド

### RESET SWITCH

#### 解説

スイッチングモジュールをリセットする。

すべてのスイッチポートがリセットされ、FDB のダイナミックエントリーなど、動的に取得した情報はすべてクリアされる。また、スイッチングに関するタイマーと統計カウンターもクリアされる。

#### 関連コマンド

SHOW SWITCH ( 490 ページ )

SHOW SWITCH FDB ( 503 ページ )

## RESET SWITCH ACCELERATOR COUNTER

カテゴリー：スイッチング / 一般コマンド

備考：IPv6 アクセラレーターボード AT-ACC01 と拡張メモリー AT-SD512A-001 が必要（本機能は 9924SP では使用できません）

**RESET SWITCH ACCELERATOR COUNTER** [= {ALL|DEFAULT|FAB|MAC|MIB}]

### 解説

IPv6 アクセラレーターボードの統計カウンターをクリアする。

### パラメーター

**COUNTER** クリアするカウンターの種類を指定する。FAB（ファブリックインターフェースカウンター）、MAC（MAC カウンター）、MIB（SNMP カウンター）、DEFAULT（MAC、MIB カウンター）、ALL（すべてのカウンター）から選択する。カウンターの種類を指定しなかった場合は、DEFAULT を指定したのと同じ意味になる。

## RESET SWITCH PORT

カテゴリー：スイッチング / ポート

**RESET SWITCH PORT**=**{*port-list*|ALL}** [COUNTER]

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

スイッチポートをハードウェア的にリセットする。

リセットを実行すると、(1) 送受信キュー内のパケットを破棄し、(2) オートネゴシエーションプロセスを開始し、(3) ポートの統計カウンターをクリアする。

### パラメーター

**PORT** ポート番号

**COUNTER** 統計カウンターだけをリセットしたいときに指定する。

### 備考・注意事項

本コマンドは、SFP ポートに対しては機能しない。

### 関連コマンド

DISABLE SWITCH PORT ( 274 ページ )

ENABLE SWITCH PORT ( 304 ページ )

SHOW SWITCH PORT ( 509 ページ )

## SET CLASSIFIER

カテゴリー：スイッチング / クラシファイア

ハードウェアパケットフィルター・QoS ポリシー用の構文

```
SET CLASSIFIER=rule-id [ETHFORMAT={ETHII-TAGGED|ETHII-UNTAGGED|ANY}]
[PROTOCOL={protocoltype|IP|ANY}] [MACTYPE={L2UCAST|L2MCAST|L2BCAST|ANY}]
[MACSADDR={macadd|DHCP Snooping|ANY}] [MACDADDR={macadd|ANY}]
[VLAN={vlanname|1..4094|ANY}] [TPID={tpid|ANY}] [VLANPRIORITY={0..7|
ANY}] [INNERTPID={tpid|ANY}] [INNERVLANPRIORITY={0..7|ANY}]
[INNERVLANID={1..4094|ANY}] [IPSADDR={ipadd[/masklen]|DHCP Snooping|ANY}]
[IPDADDR={ipadd[/masklen]|ANY}] [IPDSCP={dscp-list|ANY}] [IPTOS={0..7|
ANY}] [IPPROTOCOL={TCP|UDP|ICMP|IGMP|protocol|ANY}] [TCPSPORT={port|
port-range|ANY}] [TCPDPORT={port|port-range|ANY}] [TCPFLAGS={ {URG|ACK|
RST|SYN|FIN}[, ...]|ANY}] [UDPSPORT={port|port-range|ANY}]
[UDPSPORT={port|port-range|ANY}] [L4SMASK={bitmask|ANY}]
[L4DMASK={bitmask|ANY}] [L5BYTE01=byteoffset,bytevalue[,bytemask]]
[L5BYTE02=byteoffset,bytevalue[,bytemask]]
[L5BYTE03=byteoffset,bytevalue[,bytemask]]
[L5BYTE04=byteoffset,bytevalue[,bytemask]]
[L5BYTE05=byteoffset,bytevalue[,bytemask]]
[L5BYTE06=byteoffset,bytevalue[,bytemask]]
[L5BYTE07=byteoffset,bytevalue[,bytemask]]
[L5BYTE08=byteoffset,bytevalue[,bytemask]]
[L5BYTE09=byteoffset,bytevalue[,bytemask]]
[L5BYTE10=byteoffset,bytevalue[,bytemask]]
[L5BYTE11=byteoffset,bytevalue[,bytemask]]
[L5BYTE12=byteoffset,bytevalue[,bytemask]]
[L5BYTE13=byteoffset,bytevalue[,bytemask]]
[L5BYTE14=byteoffset,bytevalue[,bytemask]]
[L5BYTE15=byteoffset,bytevalue[,bytemask]]
[L5BYTE16=byteoffset,bytevalue[,bytemask]]
```

IPv6 ハードウェアパケットフィルター用の構文 (IPv6 ルーティングパケット)

```
SET CLASSIFIER=rule-id ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6
[IPSADDR={ip6add/plen|ANY}] [IPDADDR={ip6add/plen|ANY}] [IPDSCP={0..63|
ANY}] [IPPROTOCOL={TCP|UDP|ICMP|IGMP|protocol|ANY}] [TCPSPORT={port|
port-range|ANY}] [TCPDPORT={port|port-range|ANY}] [UDPSPORT={port|
port-range|ANY}] [UDPSPORT={port|port-range|ANY}]
```

IPv6 QoS ポリシー用の構文 (IPv6 ルーティングパケット)

```
SET CLASSIFIER=rule-id ETHFORMAT=ETHII-TAGGED PROTOCOL=IPV6
```

```
[MACTYPE={L2UCAST|L2MCAST|L2BCAST|ANY}] [MACSADDR={macadd|ANY}]
[MACDADDR={macadd|ANY}] [VLAN={vlanname|1..4094|ANY}] [IPDSCP={0..63|
ANY}] [IPPROTOCOL={TCP|UDP|ICMP|IGMP|protocol|ANY}]
```

**rule-id:** クラシファイア番号 (1～9999)

**macadd:** MAC アドレス (xx-xx-xx-xx-xx-xx の形式)

**protocoltype:** L3 プロトコル (Ethertype) 番号 (16 進数)

**vlanname:** VLAN 名 (1～32 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字は区別しない)

**tpid:** TPID (16 ビット長。16 進数最大 4 文字)

**ipadd:** IP アドレス

**masklen:** マスク長 (0～32)

**dscp-list:** DSCP 値 (0～63。ハイフン、カンマを使った複数指定も可能)

**protocol:** IP プロトコル番号 (1～255)

**port:** TCP/UDP ポート番号 (0～65535)

**port-range:** TCP/UDP ポート番号範囲 (「1-99」のように 2 つの番号をハイフンで区切って指定する。有効範囲は 0～65535)

**bitmask:** マスク値 (16 ビット長。16 進数最大 4 文字)

**ip6add:** IPv6 アドレス

**plen:** プレフィックス長 (1～128 ビット)

**byteoffset:** データ部の先頭バイト (TCP・UDP ヘッダーの直後のバイト) を 0 として数えたオフセット (10 進数。0～37)

**bytevalue:** byteoffset で指定したバイトの内容 (16 進数。00～ff)

**bytemask:** bytevalue に対する AND マスク (16 進数。省略時は ff)

## 解説

クラシファイア (汎用パケットフィルター) の設定を変更する。

## パラメーター

**CLASSIFIER** クラシファイア番号。この番号は単なる識別子であり、番号の大小は意味を持たない。番号は固定なので、他のクラシファイアを削除しても変更されることはない。また、番号に空きがあってもよい

**ETHFORMAT** Ethernet のフレームフォーマット (エンキャプセレーション)。ETHII-UNTAGGED (Ethernet Version 2。タグなし)、ETHII-TAGGED (Ethernet Version 2。タグ付き)、ANY (すべて) から選択する。ETHII-UNTAGGED、ETHII-TAGGED を指定した場合は、必ず PROTOCOL パラメーターもあわせて指定すること。また、PROTOCOL に IPV6 を指定するときは、本パラメーターに ETHII-TAGGED か ETHII-UNTAGGED を指定する必要がある。省略時は ANY。

**PROTOCOL** レイヤー 3 プロトコルタイプ (Ethertype) フィールド値。特殊なプロトコル名 (IP、ANY) か、定義済みのプロトコル名 (別表を参照) または、16 進表記の Ethertype プロトコル番号で指定する。ETHFORMAT に ETHII-UNTAGGED か ETHII-TAGGED を指定した場合は、必ず本パラメーターもあわせて指定すること (ANY は不可)。省略時は ANY。

**MACTYPE** レイヤー 2 アドレス種別。L2UCAST (ユニキャスト)、L2MCAST (マルチキャスト)、L2BCAST (ブロードキャスト)、ANY (すべて) から選択する。省略時は ANY。

**MACSADDR** 送信元 MAC アドレス。「DHCP Snooping」は、DHCP Snooping の設定時に QoS ポリシーとクラシファイアを組み合わせるための特殊なキーワードで、「送信元 MAC アドレスが DHCP Snooping テーブル ( バインディングデータベース ) に登録されている」という条件を示す。省略時は ANY。

**MACDADDR** 宛先 MAC アドレス。省略時は ANY。

**VLAN** 入力 VLAN。パケットの入力元が指定した VLAN のときだけマッチする。ただし、IPv6 QoS ポリシー用のクラシファイアでは出力 VLAN の意味になる。省略時は ANY。

**TPID** 802.1Q VLAN タグヘッダーの TPID ( Tag Protocol Identifier ) 値。2 バイトの 16 進数で指定する。省略時は ANY。

**VLANPRIORITY** 802.1p ユーザープライオリティー ( 0 ~ 7 ) 値。省略時は ANY。

**INNERTPID** ダブルタグパケットにおける内側 802.1Q VLAN タグヘッダーの TPID ( Tag Protocol Identifier ) 値。2 バイトの 16 進数で指定する。省略時は ANY。

**INNERVLANPRIORITY** ダブルタグパケットにおける内側 802.1Q VLAN タグヘッダーの 802.1p ユーザープライオリティー ( 0 ~ 7 ) 値。省略時は ANY。

**INNERVLANID** ダブルタグパケットにおける内側 802.1Q VLAN タグヘッダーの VLAN ID。省略時は ANY。

**IPSADDR** 始点 IPv4/IPv6 アドレス。IP アドレス/マスク長 ( IPv4 ) または IP アドレス/プレフィックス長 ( IPv6 ) の形式で指定する。マスク長、プレフィックス長を省略した場合は、それぞれ 32 ビットマスク/128 ビットプレフィックス ( ホストアドレス ) と見なされる。「DHCP Snooping」は、DHCP Snooping の設定時に QoS ポリシーとクラシファイアを組み合わせるための特殊なキーワードで、「始点 IP アドレスが DHCP Snooping テーブル ( バインディングデータベース ) に登録されている」という条件を示す。省略時は ANY

**IPDADDR** 終点 IPv4/IPv6 アドレス。IP アドレス/マスク長 ( IPv4 ) または IP アドレス/プレフィックス長 ( IPv6 ) の形式で指定する。マスク長、プレフィックス長を省略した場合は、それぞれ 32 ビットマスク/128 ビットプレフィックス ( ホストアドレス ) と見なされる。省略時は ANY

**IPDSCP** IPv4/IPv6 ヘッダーの DSCP ( DiffServ Code Point ) フィールド値。有効範囲は 0 ~ 63。IPv4 の場合は、ハイフン、カンマを使った複数指定も可能。IPTOS とは同時に指定できない。省略時は ANY

**IPTOS** IPv4 ヘッダーの TOS 優先度 ( precedence ) フィールド値。有効範囲は 0 ~ 7。IPDSCP とは同時に指定できない。省略時は ANY。

**IPPROTOCOL** IPv4/IPv6 ヘッダーのプロトコルタイプ ( IPv4 ) / 次ヘッダー ( IPv6 ) フィールド値。定義済みのプロトコル名 ( TCP、UDP、ICMP、IGMP ) か 10 進表記のプロトコル番号 ( 1 ~ 255。0 も指定できるが、ハードウェアパケットフィルタや QoS ポリシーに割り当てた時点でエラーになるため使用不可 ) で指定する。なお、TCPSPORT、TCPDPORT パラメーターを使っている場合は、本パラメーターに TCP を指定したものと見なされる ( 他の値は指定できない )。また、UDPSPORT、UDPDPDPORT パラメーターを使っている場合は、本パラメーターに UDP を指定したものと見なされる ( 他の値は指定できない )。省略時は ANY

**TCPSPORT** TCP 始点ポート。単一のポート番号かポート番号の範囲を指定する。範囲を指定した場合、L4SMASK パラメーターは無効。省略時は ANY

**TCPDPORT** TCP 終点ポート。単一のポート番号かポート番号の範囲を指定する。範囲を指定した場合、L4DMASK パラメーターは無効。省略時は ANY

**TCPFLAGS** TCP 制御フラグ。カンマ区切りで複数指定が可能。本パラメーターでは、指定したフラグだ

けがチェック対象となる（指定しなかったフラグの状態には関知しない）。指定したフラグがすべてが立っていればマッチ、それ以外の場合は非マッチと判定される。省略時は ANY

**UDPSPORT** UDP 始点ポート。単一のポート番号かポート番号の範囲を指定する。範囲を指定した場合、L4SMASK パラメーターは無効。省略時は ANY

**UDPDPOR** UDP 終点ポート。単一のポート番号かポート番号の範囲を指定する。範囲を指定した場合、L4DMASK パラメーターは無効。省略時は ANY

**L4SMASK** TCP/UDP 始点ポートに対する AND マスク。「f800」のような 16 ビットの 16 進数で指定する。本パラメーターは、必ず TCPSPORT、UDPSPORT のどちらかと組で指定すること。またこのとき、TCPSPORT、UDPSPORT には単一のポート番号を指定すること。

**L4DMASK** TCP/UDP 終点ポートに対する AND マスク。「f800」のような 16 ビットの 16 進数で指定する。本パラメーターは、必ず TCPDPOR、UDPDPOR のどちらかと組で指定すること。またこのとき、TCPDPOR、UDPDPOR には単一のポート番号を指定すること。

**L5BYTE01 ~ L5BYTE16** TCP/UDP パケットのデータ部の値。1 バイトごとに、byteoffset（位置）、bytevalue（値）、bytemask（マスク）を指定する（bytemask は省略可）。本パラメーターは、必ず L5BYTE01、L5BYTE02..の順に使用しなければならない。またこのとき、byteoffset の値がしだいに大きくなるように設定しなくてはならない。本パラメーターは、IPv4 上の有効な TCP・UDP パケットに対してのみ機能するが、これは自動的に行われるので、L5BYTExx パラメーターを指定するときに、PROTOCOL、IPPROTOCOL パラメーターを指定する必要はない。

## 備考・注意事項

IGMP を有効にしている場合は、IGMP モジュールの処理が優先されるため、IPPROTOCOL=IGMP を指定しても IGMP パケットをフィルタリングできない。

L5BYTExx パラメーターは、必ず L5BYTE01、L5BYTE02..の順に使用しなければならない。たとえば、L5BYTE02 だけを指定したり、L5BYTE01 と L5BYTE03 だけを指定したりすることはできない。またこのとき、byteoffset の値がしだいに大きくなるように設定しなくてはならない。すなわち、L5BYTE01 の byteoffset が 2 なら、L5BYTE02 の byteoffset は 3 以上でなくてはならない。

L5BYTExx パラメーターでマッチングできるのは、IP パケットの先頭から 80Byte 以内だけであることに注意。IP パケットや TCP パケットにオプションがついている場合など、L5BYTExx パラメーターで指定したバイトが IP パケットの先頭から 80Byte より後ろに来た場合は、該当パケットの値が bytevalue、bytemask の指定と一致していても、クラシファイアはマッチしない。

L5BYTExx パラメーターは、IPv4 上の有効な TCP・UDP パケットに対してのみ機能する。これは自動的に行われるので、L5BYTExx パラメーターを指定するときに、PROTOCOL、IPPROTOCOL パラメーターを指定する必要はない。

## 関連コマンド

CREATE CLASSIFIER ( 198 ページ )

DESTROY CLASSIFIER ( 243 ページ )

SHOW CLASSIFIER ( 395 ページ )



## SET DHCP Snooping CHECKINTERVAL

カテゴリー：スイッチング / DHCP Snooping

**SET DHCP Snooping CHECKINTERVAL=1..3600**

### 解説

DHCP Snooping テーブル（バインディングデータベース）のチェック間隔を変更する。

デフォルトでは、60 秒間隔でテーブル内のダイナミックエントリーをチェックし、IP アドレスの使用期限が切れたクライアントの情報をデータベースから削除する。スタティックエントリーはチェックされない（削除されない）。

### パラメーター

**CHECKINTERVAL** チェック間隔（秒）。デフォルトは 60 秒。

### 備考・注意事項

本製品は、バインディングデータベースをチェックするたびに、その時点で有効な（ダイナミック登録された）クライアントの情報を bindXXXX.dsn ファイル（「XXXX」の部分にはファームウェアのバージョンを表す 4 桁の数値が入る）に書き込む。DHCP Snooping を無効から有効に変更したときは、最初にこのファイルを読み込み、その時点でまだ有効なクライアントがあれば、それをバインディングデータベースに登録する。

### 関連コマンド

ENABLE DHCP Snooping（280 ページ）

SHOW DHCP Snooping（401 ページ）

## SET DHCP Snooping PORT

カテゴリー：スイッチング / DHCP Snooping

**SET DHCP Snooping PORT**={*port-list*|**ALL**} [**MAXLEASES**=0..100]  
 [SUBSCRIBERID=*string*] [TRUSTED={YES|NO|ON|OFF|TRUE|FALSE}]

*port-list*: スイッチポート番号 (1~。ハイフン、カンマを使った複数指定も可能)

*string*: 文字列 (0~50 文字。英数字と空白のみ使用可能。空白を含む場合はダブルクォートで囲む)

### 解説

指定したスイッチポートにおける DHCP Snooping の動作を変更する。

### パラメーター

**PORT** スイッチポート。複数指定が可能。

**MAXLEASES** 指定ポート経由の IP 通信を許可するクライアントの数 (ダイナミック (DHCP クライアント)、スタティック (IP 固定設定クライアント) の合計)。デフォルトは 1。

**SUBSCRIBERID** 指定ポートの Subscriber-ID を指定する。DHCP Snooping のオプション機能である リレーエージェント情報オプション (オプションコード 82) の付加・検査・削除機能が有効化されている場合、本パラメーターに 1 文字以上の文字列が指定されているときは、リレーエージェント情報オプションに Subscriber-ID サブオプションを含める。本パラメーターが指定されていない、あるいは、空文字列 (長さが 0 の文字列) が指定されている場合は、Subscriber-ID サブオプションを含めない。デフォルトは指定なし (Subscriber-ID サブオプションを含めない)。

**TRUSTED** DHCP Snooping におけるポート種別。YES、ON、TRUE を指定した場合、DHCP Snooping によるフィルタリングが行われない Trusted ポートとなる (サーバーなどの接続用)。NO、OFF、FALSE を指定した場合は、DHCP Snooping によるフィルタリングが行われる Untrusted ポートとなる (不特定多数のクライアント接続用)。デフォルトは NO (Untrusted ポート)。

### 備考・注意事項

MAXLEASES パラメーターは、ダイナミックエントリー (DHCP クライアント) だけでなく、ADD DHCP Snooping BINDING コマンドで登録するスタティックエントリー (IP 固定設定のクライアント) の数にも影響する (デフォルトでは、ポートあたり 1 つしかスタティックエントリーを登録できない)。

### 関連コマンド

ADD DHCP Snooping BINDING (173 ページ)

ENABLE DHCP Snooping (280 ページ)

ENABLE DHCP Snooping OPTION82 (283 ページ)

SHOW DHCP Snooping (401 ページ)

SHOW DHCP Snooping Port ( 409 ページ )

## SET EPSR

カテゴリー：スイッチング / イーサネットリングプロテクション (EPSR)

```
SET EPSR={epsrname|ALL} [HELLOTIME=timer1] [FAILOVERTIME=timer2]
[RINGFLAPTIME=0..65535] [TRAP={ENABLED|DISABLED}]
```

*epsrname*: EPSR ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

*timer1*: 時間 (100ms ~ 32767s)

*timer2*: 時間 (200ms ~ 65535s)

### 解説

EPSR ドメインのパラメーターを変更する。

### パラメーター

**EPSR** EPSR ドメイン名

**HELLOTIME** (マスターノードのみ) Healthcheck メッセージの送信間隔。数値だけで指定する場合の単位は s (秒)。ただし、数値のあとに「s」、「ms」をつけると、それぞれ「秒」、「ミリ秒」の意味になる。「ms」を指定する場合は、100ms の倍数で指定すること。デフォルトは 1s (1 秒)。

**FAILOVERTIME** (マスターノードのみ) Healthcheck メッセージのタイムアウト時間。HELLOTIME の 2 倍の値に設定すること。マスターノードは、プライマリーポートから送信した Healthcheck メッセージが、ここで指定した時間内にセカンダリーポートに到達しないとリングに障害が発生したと判断する。数値だけで指定する場合の単位は s (秒)。ただし、数値のあとに「s」、「ms」をつけると、それぞれ「秒」、「ミリ秒」の意味になる。「ms」を指定する場合は、100ms の倍数で指定すること。デフォルトは 2s (2 秒)。

**RINGFLAPTIME** (マスターノードのみ) リング障害の回復後、Failed 状態から Complete 状態に移る前に待機する最小時間 (秒)。この時間内にリング障害が回復しても、Failed 状態を維持する。リングの状態が頻繁に切り替わるような場合、この値を調整することで不必要な状態遷移を防ぐことができる。デフォルトは 0。

**TRAP** EPSR ドメインの状態が変化したときに SNMP トラップ (SNMPv2c、SNMPv3 形式のみ) を送信するかどうか。デフォルトは ENABLED (送信する)。

### 備考・注意事項

EPSR ドメインの状態変化を知らせる SNMP トラップを利用するためには、SNMPv2c のトラップホストまたは SNMPv3 のターゲットを設定する必要がある。SNMPv1 トラップホストの設定だけでは、EPSR の SNMP トラップは利用できないので注意。

### 関連コマンド

ADD EPSR DATAVLAN ( 175 ページ )

CREATE EPSR ( 205 ページ )

CREATE VLAN ( 225 ページ )

DESTROY EPSR ( 244 ページ )

ENABLE EPSR ( 284 ページ )

SET EPSR PORT ( 334 ページ )

SHOW EPSR ( 411 ページ )

## SET EPSR PORT

カテゴリー：スイッチング / イーサネットリングプロテクション (EPSR)

**SET EPSR=***epsrname* **PORT=***port-number* **TYPE={PRIMARY|SECONDARY}**

*epsrname*: EPSR ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

*port-number*: スイッチポート番号 (1~)

### 解説

EPSR ドメインの所属ポートの種別 (プライマリー、セカンダリー) を変更する。

本コマンドは該当 EPSR ドメインのマスターノードでのみ有効。また、本コマンドを実行するときは、該当 EPSR ドメインが無効化されていない (DISABLE EPSR コマンド)。

### パラメーター

**EPSR** EPSR ドメイン名

**PORT** スイッチポート番号

**TYPE** ポートの種別。PRIMARY (プライマリー)、SECONDARY (セカンダリー) から選択する。あるポートを PRIMARY に設定すると、もう一方のポートは自動的に SECONDARY となる。逆も同じ。

### 関連コマンド

CREATE EPSR (205 ページ)

CREATE VLAN (225 ページ)

DISABLE EPSR (257 ページ)

SET EPSR (332 ページ)

SHOW EPSR (411 ページ)

## SET LACP PORT

カテゴリー：スイッチング / LACP (IEEE 802.3ad)

```
SET LACP PORT={port-list|ALL} [ADMINKEY=0..65535] [PRIORITY=0..65535]
[MODE={ACTIVE|PASSIVE}] [PERIODIC={FAST|SLOW}]
```

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

指定したスイッチポートの LACP 関連パラメーターを変更する。

### パラメーター

**PORT** ポート番号。

**ADMINKEY** LACP ポート鍵の元となる値を指定する (ポート鍵の値そのものではない)。LACP では、対向機器、所属 VLAN、通信速度、ポート鍵のすべてが等しいポート群で 1 つのトランクグループを構成する。したがって、本来なら 1 つのトランクグループを構成するポート群を複数のグループに分けたい場合は、グループごとに異なる ADMINKEY を設定すればよい。なお、ADMINKEY は自機内でのみ意味を持つ (対向機器と同じに設定する必要はない)。デフォルトは 1。

**PRIORITY** LACP ポートプライオリティ。小さいほど優先度が高い。使用可能な LACP ポートの数がトランクグループの最大ポート数 (4 ポート) よりも多い場合、本パラメーターの小さいポートほどメンバーに選ばれる可能性が高くなる。なお、ポートプライオリティが等しい場合は、ポート番号の小さいほうが優先的に使用される。また、メンバーに選ばれなかったポートはスタンバイ状態となり、現行のメンバーポートがリンクダウンするときに備えて待機する。デフォルトは 32768。

**MODE** LACP ポートの動作モード。ACTIVE (PERIODIC パラメーターで設定した間隔で LACP パケットを自発的に送信する) PASSIVE (対向ポートから LACP パケットを受信したときだけ LACP パケットを送信する) から選択する。デフォルトは ACTIVE。

**PERIODIC** ACTIVE モード時の LACP パケットの送信間隔。FAST (1 秒) SLOW (30 秒) から選択する。デフォルトは FAST。

### 関連コマンド

ADD LACP PORT (176 ページ)

DELETE LACP PORT (229 ページ)

SHOW LACP PORT (419 ページ)

## SET LACP

カテゴリー：スイッチング / LACP (IEEE 802.3ad)

**SET LACP** [PRIORITY=0..65535] [THRASHACTION={NONE|LEARNDISABLE|PORTDISABLE|VLANDISABLE|LINKDOWN}] [THRASHTIMEOUT={NONE|1..86400}]

### 解説

LACP のグローバル設定パラメーターを変更する。

### パラメーター

**PRIORITY** LACP システムプライオリティ。小さいほど優先度が高い。相互接続された LACP システムは、システムプライオリティとシステム ID (MAC アドレス) を組み合わせた値 (System priority data identifier) を互いに比較し、値の小さいほうにリンクの制御権を付与する。デフォルトは 32768。

**THRASHACTION** LACP によって自動生成されたトランクグループで MAC アドレススラッシング (同一 MAC アドレスの登録ポートが頻繁に変更されること) を検出した場合の動作。NONE (なにもしない)、LEARNDISABLE (トランクグループ内の全ポートで MAC アドレスの学習を停止する)、PORTDISABLE (トランクグループ内の全ポートをディセーブルにする)、VLANDISABLE (スラッシングが発生した VLAN に対してのみトランクグループ内の全ポートをディセーブルにする)、LINKDOWN (トランクグループ内の全ポートを物理的にリンクダウンさせる) から選択する。これらの動作は、THRASHTIMEOUT パラメーターで指定した時間が経過すると終了する (通常のポート動作に戻る)。ただし、PORTDISABLE、LINKDOWN の場合は、ENABLE SWITCH PORT コマンドにより手動で動作を終了させられる。また、VLANDISABLE の場合は、ENABLE SWITCH PORT VLAN コマンドにより手動で動作を終了させられる。デフォルトは LEARNDISABLE。

**THRASHTIMEOUT** MAC アドレススラッシング検出時の動作の持続時間 (秒)。NONE は無期限を示す。THRASHACTION パラメーターに LEARNDISABLE を指定している場合、本パラメーターを NONE に変更することはできない。また、本パラメーターを NONE に設定している状態で、THRASHACTION パラメーターの値を LEARNDISABLE に変更した場合、本パラメーターの値は自動的に 1 に変更される。デフォルトは 1 秒。

### 備考・注意事項

THRASHACTION パラメーターの値を VLANDISABLE に変更すると、トランクグループ内の全ポートで自動的にイングレスフィルタリング (SET SWITCH PORT コマンドの INFILTERING パラメーター) が有効になる。また、VLANDISABLE からそれ以外に変更すると、イングレスフィルタリングが無効になる。

### 関連コマンド

SET SWITCH THRASHLIMIT (391 ページ)



SHOW LACP ( 417 ページ )

## SET MSTP

カテゴリー：スイッチング / マルチプルスパニングツリープロトコル (MSTP)

```
SET MSTP [CONFIGNAME=string] [REVISIONLEVEL=0..65535] [MAXHOPS=1..40]
[MAXAGE=6..40] [HELLOTIME=1..10] [FORWARDDELAY=4..30]
[PROTOCOLVERSION={STP|RSTP|MSTP}] [STATICVLAN={YES|NO|ON|OFF|TRUE|
FALSE}]
```

*string*: 文字列 (1~32 文字。英数字とアンダースコアが使用可能)

### 解説

マルチプルスパニングツリープロトコル (MSTP) のパラメーターを変更する。

### パラメーター

**CONFIGNAME** MST リージョン名。同一リージョンに所属させたい装置には、同じ名前を指定する。デフォルトは製品の MAC アドレス (xx-xx-xx-xx-xx-xx の型式)。

**REVISIONLEVEL** MST リージョン設定のレビジョン。同一リージョンに所属させたい装置には、同じ数値を指定する。デフォルトは 0。

**MAXHOPS** 最大ホップ数。BPDU が MSTP ブリッジを抜けるごとにカウントダウンされる。BPDU の寿命カウンタ。デフォルトは 20。

**MAXAGE** 最大エージタイム。ルートブリッジから BPDU が届かなくなったことを認識するまでの時間 (秒)。この時間内に BPDU を受信できなかった場合、各ブリッジはスパニングツリーの再構成を開始する。2 × (HELLOTIME + 1) 以上、かつ、2 × (FORWARDDELAY - 1) 以下でなくてはならない。デフォルトは 20 秒。

**HELLOTIME** ハロータイム。ルートブリッジが BPDU (Bridge Protocol Data Unit) を送信する間隔 (秒)。デフォルトは 2 秒。

**FORWARDDELAY** フォワードディレイタイム。ネットワーク構成の変更後に、ルートブリッジ内のポートがディスカードイングからラーニング、ラーニングからフォワーディング状態に遷移するまでの最大時間 (秒) を示す。デフォルトは 15 秒。

**PROTOCOLVERSION** MSTP の動作モード。MSTP (MSTP BPDU を使う)、RSP (RSTP BPDU を使う)、STP (STP BPDU を使う) から選択する。デフォルトは MSTP。

**STATICVLAN** スパニングツリーのトポロジ計算時、MST インスタンスに所属している VLAN のポート構成を考慮するかどうか。YES を指定した場合は、VLAN のポート構成を考慮して計算を行う (MST インスタンスに所属している VLAN のメンバーポートだけを利用してトポロジを計算する)。NO を指定した場合は、VLAN のポート構成を考慮せずに通常の MSTP の方法で計算を行う (MST インスタンスに所属している VLAN のメンバーポートだけでなく、すべての物理ポートを使用して計算を行う)。ブリッジ (スイッチ) 間を接続しているすべてのポートが同じ VLAN 設定であるなら OFF でよいが、そうでない場合は、特定の MST インスタンスにおいて、所属 VLAN のメンバーでないポートがルートポートになる可能性がある。このようなときは ON を指定するとよい。

( OFF のままでも、メンバーポートのポートプライオリティーやポートパスコストを調整すれば同じ効果を得られる )。デフォルトは OFF。

### 関連コマンド

SHOW MSTP ( 425 ページ )

## SET MSTP CIST

カテゴリー：スイッチング / マルチプルスパニングツリープロトコル (MSTP)

**SET MSTP CIST PRIORITY=0..65535**

### 解説

CIST (Common and Internal Spanning Tree) におけるブリッジプライオリティを設定する。

### パラメーター

**PRIORITY** CIST におけるブリッジプライオリティ。小さいほど優先度が高く、ネットワーク全体のルートブリッジ (CIST ルート) になる可能性が高くなる。設定できる値の範囲は 0 ~ 65535 だが、実際に使用される値は 4096 の倍数に丸められる (指定値が 4096 の倍数でない場合、指定値よりも小さい直近の倍数が使われる)。デフォルトは 32768。

### 例

CIST におけるブリッジプライオリティを 4096 に設定する。

SET MSTP CIST PRIORITY=4096

### 関連コマンド

SHOW MSTP (425 ページ)

SHOW MSTP CIST (428 ページ)

## SET MSTP CIST PORT

カテゴリー：スイッチング / マルチプルスパニングツリープロトコル (MSTP)

```
SET MSTP CIST PORT={port-list|ALL} [PRIORITY=0..255]
[INTPATHCOST={1..200000000|DEFAULT}] [EXTPATHCOST={1..200000000|
DEFAULT}] [EDGEPORT={YES|NO|ON|OFF|TRUE|FALSE}] [POINTTOPOINT={YES|NO|ON|
OFF|TRUE|FALSE|AUTO}]
```

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

CIST (Common and Internal Spanning Tree) における指定ポートのマルチプルスパニングツリー関連パラメーターを変更する。

### パラメーター

**PORT** ポート番号。複数指定が可能。ALL を指定した場合はすべてのポートが対象となる。

**PRIORITY** CIST 内のトポロジー形成で使用するポートプライオリティ。小さいほど優先度が高く、ルートポートになる可能性が高くなる。設定できる値の範囲は 0～255 だが、実際に使用される値は 16 の倍数に丸められる (指定値が 16 の倍数でない場合、指定値よりも小さい直近の倍数が使われる)。デフォルトは 128。

**INTPATHCOST** CIST リージョナルルート (MST リージョン内における CIST ツリーのルートブリッジ) までのパスに対するポート通過コスト。有効範囲は 1～200000000。デフォルトでは、ポートの通信速度に応じた既定値が使われる (別表を参照)。なお、一度値を設定したあとでデフォルト状態に戻すときはキーワード DEFAULT を指定する

**EXTPATHCOST** CIST ルートブリッジが所属するリージョンまでのパスに対するポート通過コスト。有効範囲は 1～200000000。デフォルトでは、ポートの通信速度に応じた既定値が使われる (別表を参照)。なお、一度値を設定したあとでデフォルト状態に戻すときはキーワード DEFAULT を指定する

**EDGEPORT** 該当ポートがエッジポートかどうかを指定する。エッジポートとは、他のブリッジが存在しない末端 (エッジ) の LAN に接続されているポートのこと。ただし、EDGEPORT=YES を指定した場合でも、同ポートで MSTP BPDU を受信した場合はエッジポートとしては扱われなくなる。デフォルトは NO。

**POINTTOPOINT** 該当ポートが他のブリッジとポイントツーポイントで接続されているかどうかを指定する。AUTO を指定した場合は、本製品が自動判別する。デフォルトは AUTO。

通信速度	推奨範囲	デフォルト値
10Mbps	200000 ~ 2000000	2000000
100Mbps	20000 ~ 200000	200000

1000Mbps	2000 ~ 20000	20000
----------	--------------	-------

表 37: パスコストの推奨範囲とデフォルト値

### 関連コマンド

SHOW MSTP CIST ( 428 ページ )

SHOW MSTP CIST PORT ( 431 ページ )

## SET MSTP MSTI

カテゴリー：スイッチング / マルチプルスパニングツリープロトコル (MSTP)

**SET MSTP MSTI=*instance* PRIORITY=0..65535**

*instance*: MST インスタンス ID (1 ~ 4094)

### 解説

MST インスタンスにおけるブリッジプライオリティを設定する。

### パラメーター

**MSTI** MST インスタンス ID

**PRIORITY** 該当 MST インスタンスにおけるブリッジプライオリティ。小さいほど優先度が高く、MST インスタンス内のルートブリッジ (リージョナルルート) になる可能性が高くなる。設定できる値の範囲は 0 ~ 65535 だが、実際に使用される値は 4096 の倍数に丸められる (指定値が 4096 の倍数でない場合、指定値よりも小さい直近の倍数が使われる)。デフォルトは 32768。

### 例

MST インスタンス「1」におけるブリッジプライオリティを 8192 に設定する。

```
SET MSTP MSTI MSTIID=1 PRIORITY=8192
```

### 関連コマンド

SHOW MSTP (425 ページ)

SHOW MSTP MSTI (436 ページ)

## SET MSTP MSTI PORT

カテゴリー：スイッチング / マルチプルスパニングツリープロトコル (MSTP)

**SET MSTP MSTI=instance PORT={port-list|ALL}** [PRIORITY=0..255]  
[PATHCOST={1..200000000|DEFAULT}]

*instance*: MST インスタンス ID (1~4094)

*port-list*: スイッチポート番号 (1~。ハイフン、カンマを使った複数指定も可能)

### 解説

指定した MST インスタンスにおける指定ポートのマルチプルスパニングツリー関連パラメーターを変更する。

### パラメーター

**MSTI** MST インスタンス ID

**PORT** ポート番号。複数指定が可能。ALL を指定した場合はすべてのポートが対象となる。

**PRIORITY** MST インスタンス内でのトポロジ形成で使用するポートプライオリティ。小さいほど優先度が高く、ルートポートになる可能性が高くなる。設定できる値の範囲は 0~255 だが、実際に使用される値は 16 の倍数に丸められる (指定値が 16 の倍数でない場合、指定値よりも小さい直近の倍数が使われる)。デフォルトは 128。

**PATHCOST** リージョナルルート (MST インスタンスのルートブリッジ) までのパスに対するポート通過コスト。通信速度ごとのデフォルト値と推奨範囲は別表を参照のこと。なお、一度値を設定したあとでデフォルト状態に戻すときはキーワード DEFAULT を指定する。

通信速度	推奨範囲	デフォルト値
10Mbps	200000 ~ 2000000	2000000
100Mbps	20000 ~ 200000	200000
1000Mbps	2000 ~ 20000	20000

表 38: パスコストの推奨範囲とデフォルト値

### 備考・注意事項

MIGRATIONCHECK の設定は、設定ファイルに保存されない。

### 関連コマンド

ENABLE MSTP MSTI PORT

SHOW MSTP MSTI ( 436 ページ )



## SET PORTAUTH IDTOGGLE

カテゴリー：スイッチング / ポート認証

**SET PORTAUTH**[=8021X] **IDTOGGLE**=**{ON|OFF}**

### 解説

802.1X Multi-Suppliant モードで動作している Authenticator ポートにおいて、EAP パケットの Identifier フィールドに値をどのようにセットするかを指定する。

Suppliant として Windows XP SP2 ホストを使用している場合は、IDTOGGLE=ON に設定することで、ログインプロンプトが正しく表示されるようになる。

### パラメーター

**PORTAUTH** 認証メカニズム。本コマンドでは 8021X ( 802.1X 認証 ) のみ有効。省略時は 8021X と見なされるため、特に指定する必要はない。

**IDTOGGLE** EAP パケットの Identifier フィールドに値をどのようにセットするか。ON を指定した場合は 0 と 1 を交互にセットする。OFF を指定した場合は常に 0 をセットする。デフォルトは OFF。

### 備考・注意事項

IDTOGGLE=ON に設定すると、ポート認証を必要としない Windows XP ホストが同一ポートに接続されている場合、同ホスト上でログインプロンプトが常に表示されてしまうという弊害がある。

## SET PORTAUTH PORT

カテゴリー：スイッチング / ポート認証

```
SET PORTAUTH[=8021X] PORT={port-list|ALL} TYPE=AUTHENTICATOR
[CONTROL={AUTHORISED|AUTO|UNAUTHORISED}] [MAXREQ=1..10] [MODE={MULTI|
SINGLE}] [PIGGYBACK={TRUE|FALSE}] [QUIETPERIOD=0..65535]
[REAUTHENABLED={TRUE|FALSE}] [REAUTHMAX=1..10] [REAUTHPERIOD=1..86400]
[SERVERTIMEOUT=1..60] [SUPPTIMEOUT=1..60] [TXPERIOD=1..65535]
[GUESTVLAN={vlanname|1..4094|NONE}] [SECUREVLAN={ON|OFF}]
[VLANASSIGNMENT={ENABLED|DISABLED}] [MIBRESET={ENABLED|DISABLED}]
[TRAP={SUCCESS|FAILURE|BOTH|NONE}]
```

```
SET PORTAUTH[=8021X] PORT={port-list|ALL} TYPE=BOTH [CONTROL={AUTHORISED|
UNAUTHORISED|AUTO}] [MAXREQ=1..10] [MODE=SINGLE] [PIGGYBACK={TRUE|
FALSE}] [QUIETPERIOD=0..65535] [REAUTHENABLED={TRUE|FALSE}]
[REAUTHMAX=1..10] [REAUTHPERIOD=1..86400] [SERVERTIMEOUT=1..60]
[SUPPTIMEOUT=1..60] [TXPERIOD=1..65535] [GUESTVLAN={vlanname|1..4094|
NONE}] [VLANASSIGNMENT={ENABLED|DISABLED}] [MIBRESET={ENABLED|DISABLED}]
[TRAP={SUCCESS|FAILURE|BOTH|NONE}] [AUTHPERIOD=1..60]
[HELDPERIOD=0..65535] [MAXSTART=1..10] [STARTPERIOD=1..60]
[USERNAME=login-name PASSWORD=password [METHOD={OTP [ENCRYPTION={MD4|
MD5}}]|STANDARD}]]
```

```
SET PORTAUTH[=8021X] PORT={port-list|ALL} TYPE=SUPPLICANT
[AUTHPERIOD=1..60] [HELDPERIOD=0..65535] [MAXSTART=1..10]
[STARTPERIOD=1..60] [USERNAME=login-name PASSWORD=password [METHOD={OTP
[ENCRYPTION={MD4|MD5}}]|STANDARD}]]
```

```
SET PORTAUTH=MACBASED PORT={port-list|ALL} [CONTROL={AUTHORISED|AUTO|
UNAUTHORISED}] [QUIETPERIOD=0..65535] [REAUTHENABLED={TRUE|FALSE}]
[REAUTHPERIOD=1..86400] [SECUREVLAN={ON|OFF}] [VLANASSIGNMENT={ENABLED|
DISABLED}] [MIBRESET={ENABLED|DISABLED}] [TRAP={SUCCESS|FAILURE|BOTH|
NONE}]
```

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

*login-name*: ログイン名 (1～64 文字。英数字のみ使用可能)

*password*: パスワード (1～64 文字。英数字のみ使用可能)

*vlanname*: VLAN 名 (1～32 文字。英数字とアンダースコア ( \_ ) ハイフンを使用可能。大文字小文字は区別しない)

### 解説

指定ポートにおけるポート認証機能（802.1X 認証または MAC ベース認証）の設定を変更する。

## パラメーター

**PORTAUTH** 認証メカニズム。8021X（802.1X 認証）MACBASED（MAC ベース認証）から選択する。省略時は 8021X と見なされる。

**PORT** スイッチポート。複数指定が可能。

**TYPE**（802.1X ポート）802.1X 認証におけるスイッチポートの役割。AUTHENTICATOR（Authenticator ポート）SUPPLICANT（Supplicant ポート）BOTH（Authenticator ポートかつ Supplicant ポート）のいずれかを指定する。なお、Multi-Supplicant モード（MODE=MULTI）を使用する場合、TYPE=BOTH は指定できない。TYPE=AUTHENTICATOR を指定すること。

**CONTROL**（802.1X Authenticator ポート、MAC ベース認証ポート）手動設定による Authenticator ポートの状態。AUTO（認証結果に応じて変動）UNAUTHORISED（未認証固定）AUTHORISED（認証済み固定）から選択する。デフォルトは AUTO。通常は AUTO のままでよい。ただし、RADIUS サーバーの接続先ポートを Authenticator に設定している場合は、本パラメーターを AUTHORISED に設定する必要がある。

**MAXREQ**（802.1X Authenticator ポート）Supplicant に対する EAPOL-Request パケットの最大再送回数。デフォルトは 2 回。

**MODE**（802.1X Authenticator ポート）Authenticator ポートのモード。Supplicant が 1 台だけ接続されていることを想定した Single-Supplicant モード（MODE=SINGLE）と、Supplicant が複数台接続されていることを想定した Multi-Supplicant モード（MODE=MULTI）がある。Single-Supplicant モードでは、該当ポート配下に最初に接続された Supplicant だけが認証対象となる（その他の Supplicant からの通信を許可するかどうかは、PIGGYBACK パラメーターで制御可能）。Multi-Supplicant モードでは、該当ポート配下に接続された個々の Supplicant を識別し、個別に認証を行う。なお、Multi-Supplicant モードを使用する場合、TYPE パラメーターには BOTH を指定できない。AUTHENTICATOR を指定すること。デフォルトは SINGLE。

**PIGGYBACK**（802.1X Single-Supplicant Authenticator ポート）Single-Supplicant モード（MODE=SINGLE）において、最初に接続された Supplicant の認証に成功した後、他のデバイスからのパケットも許可するかどうかを指定する。TRUE なら許可、FALSE なら拒否。デフォルトは TRUE。

**QUIETPERIOD**（802.1X Authenticator ポート、MAC ベース認証ポート）Supplicant の認証に失敗した後、Supplicant との通信を拒否する期間（秒）。この期間中は受信したパケットをすべて破棄する。デフォルトは 60 秒。

**REAUTHENABLED**（802.1X Authenticator ポート、MAC ベース認証ポート）認証に成功した Supplicant を定期的に再認証するかどうか。TRUE なら再認証する、FALSE なら再認証しない。デフォルトは FALSE。

**REAUTHMAX**（802.1X Authenticator ポート）再認証時における EAPOL-Request パケットの最大再送回数。デフォルトは 2 回。

**REAUTHPERIOD**（802.1X Authenticator ポート、MAC ベース認証ポート）Supplicant の再認証間隔（秒）。デフォルトは 3600 秒。

**SERVERTIMEOUT**（802.1X Authenticator ポート）RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間（秒）。デフォルトは 30 秒。

**SUPPTIMEOUT**（802.1X Authenticator ポート）Supplicant に EAP-Request を送信した後、Supplicant

からの応答を待つ時間（秒）。デフォルトは 30 秒。

**TXPERIOD** （802.1X Authenticator ポート）Supplicant に EAPOL パケットを再送信する間隔（秒）。デフォルトは 30 秒。

**GUESTVLAN** （802.1X Single-Supplicant Authenticator ポート）ゲスト VLAN を指定する。装置上に設定されている VLAN の名前か VLAN ID を指定すること。NONE はゲスト VLAN を使用しないことを意味する。EAPOL パケットをまだ受信していないとき、該当ポートはゲスト VLAN の所属となる。最初の EAPOL パケットを受信すると、該当ポートはゲスト VLAN から削除され、本来の所属 VLAN に復帰する。本パラメーターは、Single-Supplicant モード（MODE=SINGLE）でのみ有効。デフォルトは NONE。

**SECUREVLAN** （802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート）802.1X 認証の Multi-Supplicant モード（MODE=MULTI）か MAC ベース認証でダイナミック VLAN を使用しているとき、2 番目以降の Supplicant の認証方法を指定する。本パラメーターに ON を指定した場合は、2 番目以降の Supplicant は、最初に認証を通った Supplicant と同じ VLAN でないと認証されない。一方、OFF を指定した場合は、有効な VLAN でありさえすれば認証をパスする。ただし、2 番目以降の Supplicant は、実際には最初に認証をパスした Supplicant と同じ VLAN の所属となる。本パラメーターは、Multi-Supplicant モード（MODE=MULTI）のポートか、MAC ベース認証のポートでのみ使用可能。デフォルトは ON。

**VLANASSIGNMENT** （802.1X Authenticator ポート、MAC ベース認証ポート）ダイナミック VLAN の有効・無効。有効時は、RADIUS サーバーが返してきた Tunnel-Private-Group-ID の値をもとに、指定ポートの所属 VLAN を動的に変更する。デフォルトは ENABLED。

**MIBRESET** （802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート）802.1X 認証の Multi-Supplicant モード（MODE=MULTI）か MAC ベース認証を使用しているポートにおいて、古い Supplicant 情報をエージアウトするかどうか。デフォルトは ENABLED。

**TRAP** （802.1X Authenticator ポート、MAC ベース認証ポート）ポート認証機能に関する SNMP トラップを送信するかどうか。SUCCESS を指定した場合は、Supplicant の認証に成功したときと、認証情報が時間切れになったときに SNMP トラップを送信する。FAILURE を指定した場合は、Supplicant の認証に失敗したときに SNMP トラップを送信する。BOTH を指定したときは、SUCCESS と FAILURE の両方の場合に SNMP トラップを送信する。NONE はトラップを送信しない。デフォルトは NONE。

**AUTHPERIOD** （802.1X Supplicant ポート）Authenticator に EAP-Response パケットを送信した後、Authenticator からの応答を待つ時間（秒）。デフォルトは 30 秒。

**HELDPERIOD** （802.1X Supplicant ポート）認証失敗後、Authenticator との通信を試みない期間（秒）。デフォルトは 60 秒。

**MAXSTART** （802.1X Supplicant ポート）EAPOL-Start パケットの最大送信回数。Supplicant ポートは、EAPOL-Start パケットを MAXSTART 回送信しても応答がない場合、Authenticator が存在しておらずポート認証の必要はないと判断する。デフォルトは 3 回。

**STARTPERIOD** （802.1X Supplicant ポート）Authenticator に EAPOL-Start パケットを再送信する間隔（秒）。デフォルトは 30 秒。

**USERNAME** （802.1X Supplicant ポート）指定スイッチポートが Supplicant として動作する場合に使うユーザー名。必ず PASSWORD パラメーターと組で指定すること。本パラメーターを設定した場合、該当ポートでは、SET PORTAUTH USERNAME コマンドで設定するグローバルなユーザー名・パスワード・暗号化方式ではなく、本コマンドで設定した値が使用される。

**PASSWORD** (802.1X Supplicant ポート) 指定スイッチポートが Supplicant として動作する場合に使うパスワード。必ず USERNAME パラメーターと組で指定すること。METHOD パラメーターに STANDARD を指定した場合、または、METHOD パラメーターを省略した場合は、6～63 文字の文字列を指定する。METHOD パラメーターに OTP を指定した場合は、10～63 文字の文字列（認証サーバー上で設定した OTP Initialisation Password と同じ値）を指定する。本パラメーターを設定した場合、該当ポートでは、SET PORTAUTH USERNAME コマンドで設定するグローバルなユーザー名・パスワード・暗号化方式ではなく、本コマンドで設定した値が使用される。

**METHOD** (802.1X Supplicant ポート) パスワード送信時の暗号化方式。STANDARD (EAP-MD5) または OTP (One-Time Password) から選択する。OTP を指定した場合は、ENCRYPTION パラメーターでワンタイムパスワードの生成アルゴリズムも指定する必要がある。デフォルトは STANDARD。

**ENCRYPTION** (802.1X Supplicant ポート) ワンタイムパスワードの生成アルゴリズム。MD4、MD5 から選択する。デフォルトは MD5。METHOD パラメーターに OTP を指定した場合の必須パラメーター。

## 関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (170 ページ)

ENABLE PORTAUTH (289 ページ)

ENABLE PORTAUTH PORT (291 ページ)

SET PORTAUTH PORT (346 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (350 ページ)

SHOW PORTAUTH (441 ページ)

SHOW PORTAUTH COUNTER (444 ページ)

SHOW PORTAUTH MULTISUPPLICANT PORT (447 ページ)

SHOW PORTAUTH PORT (451 ページ)

SHOW PORTAUTH TIMER (456 ページ)

## SET PORTAUTH PORT SUPPLICANTMAC

カテゴリー：スイッチング / ポート認証

```
SET PORTAUTH[=8021X] PORT={port-list|ALL} SUPPLICANTMAC=macadd
[CONTROL={AUTHORISED|AUTO|UNAUTHORISED}] [MAXREQ=1..10]
[QUIETPERIOD=0..65535] [REAUTHENABLED={TRUE|FALSE}] [REAUTHMAX=1..10]
[REAUTHPERIOD=1..86400] [SERVERTIMEOUT=1..60] [SUPPTIMEOUT=1..60]
[TXPERIOD=1..65535] [SECUREVLAN={ON|OFF}] [VLANASSIGNMENT={ENABLED|
DISABLED}] [MIBRESET={ENABLED|DISABLED}] [TRAP={SUCCESS|FAILURE|BOTH|
NONE}] [DEFAULT]

SET PORTAUTH=MACBASED PORT={port-list|ALL} SUPPLICANTMAC=macadd
[CONTROL={AUTHORISED|AUTO|UNAUTHORISED}] [QUIETPERIOD=0..65535]
[REAUTHENABLED={TRUE|FALSE}] [REAUTHPERIOD=1..86400] [SECUREVLAN={ON|
OFF}] [VLANASSIGNMENT={ENABLED|DISABLED}] [MIBRESET={ENABLED|DISABLED}]
[TRAP={SUCCESS|FAILURE|BOTH|NONE}] [DEFAULT]
```

*port-list*: スイッチポート番号 (1 ~)。ハイフン、カンマを使った複数指定も可能)

*macadd*: MAC アドレス (xx-xx-xx-xx-xx-xx の形式)

### 解説

802.1X Multi-SupPLICANT モードで動作している Authenticator ポート、または、MAC ベース認証ポートに対し、特定の MAC アドレスを持つ SupPLICANT 固有のパラメーターを設定する。

### パラメーター

**PORTAUTH** 認証メカニズム。8021X (802.1X 認証)、MACBASED (MAC ベース認証) から選択する。省略時は 8021X と見なされる。

**PORT** スイッチポート。複数指定が可能。本コマンドは、Multi-SupPLICANT モード (MODE=MULTI) のポートか、MAC ベース認証のポートでのみ使用可能。

**SUPPLICANTMAC** SupPLICANT の MAC アドレス。

**CONTROL** (802.1X Authenticator ポート、MAC ベース認証ポート) 手動設定による Authenticator ポートの状態。AUTO (認証結果に応じて変動)、UNAUTHORISED (未認証固定)、AUTHORISED (認証済み固定) から選択する。デフォルトは AUTO。通常は AUTO のままでよい。ただし、RADIUS サーバーの接続先ポートを Authenticator に設定している場合は、本パラメーターを AUTHORISED に設定する必要がある。

**MAXREQ** (802.1X Authenticator ポート) SupPLICANT に対する EAPOL-Request パケットの最大再送回数。デフォルトは 2 回。

**QUIETPERIOD** (802.1X Authenticator ポート、MAC ベース認証ポート) SupPLICANT の認証に失敗した後、SupPLICANT との通信を拒否する期間 (秒)。この期間中は受信したパケットをすべて破棄する。



デフォルトは 60 秒。

**REAUTHENABLED** (802.1X Authenticator ポート、MAC ベース認証ポート) 認証に成功した Supplicant を定期的に再認証するかどうか。TRUE なら再認証する、FALSE なら再認証しない。デフォルトは FALSE。

**REAUTHMAX** (802.1X Authenticator ポート) 再認証時における EAPOL-Request パケットの最大再送回数。デフォルトは 2 回。

**REAUTHPERIOD** (802.1X Authenticator ポート、MAC ベース認証ポート) Supplicant の再認証間隔 (秒)。デフォルトは 3600 秒。

**SERVERTIMEOUT** (802.1X Authenticator ポート) RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間 (秒)。デフォルトは 30 秒。

**SUPPTIMEOUT** (802.1X Authenticator ポート) Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間 (秒)。デフォルトは 30 秒。

**TXPERIOD** (802.1X Authenticator ポート) Supplicant に EAPOL パケットを再送信する間隔 (秒)。デフォルトは 30 秒。

**SECUREVLAN** (802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート) 802.1X 認証の Multi-Supplicant モード (MODE=MULTI) か MAC ベース認証でダイナミック VLAN を使用しているとき、2 番目以降の Supplicant の認証方法を指定する。本パラメーターに ON を指定した場合は、2 番目以降の Supplicant は、最初に認証を通った Supplicant と同じ VLAN でないと認証されない。一方、OFF を指定した場合は、有効な VLAN でありさえすれば認証をパスする。ただし、2 番目以降の Supplicant は、実際には最初に認証をパスした Supplicant と同じ VLAN の所属となる。本パラメーターは、Multi-Supplicant モード (MODE=MULTI) のポートか、MAC ベース認証のポートでのみ使用可能。デフォルトは ON。

**VLANASSIGNMENT** (802.1X Authenticator ポート、MAC ベース認証ポート) ダイナミック VLAN の有効・無効。有効時は、RADIUS サーバーが返してきた Tunnel-Private-Group-ID の値をもとに、指定ポートの所属 VLAN を動的に変更する。デフォルトは ENABLED。

**MIBRESET** (802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート) 802.1X 認証の Multi-Supplicant モード (MODE=MULTI) か MAC ベース認証を使用しているポートにおいて、古い Supplicant 情報をエージアウトするかどうか。デフォルトは ENABLED。

**TRAP** (802.1X Authenticator ポート、MAC ベース認証ポート) ポート認証機能に関する SNMP トラップを送信するかどうか。SUCCESS を指定した場合は、Supplicant の認証に成功したときと、認証情報が時間切れになったときに SNMP トラップを送信する。FAILURE を指定した場合は、Supplicant の認証に失敗したときに SNMP トラップを送信する。BOTH を指定したときは、SUCCESS と FAILURE の両方の場合に SNMP トラップを送信する。NONE はトラップを送信しない。デフォルトは NONE。

**DEFAULT** 指定した Supplicant 固有のポート認証設定を破棄するときに指定する。

## 関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (170 ページ)

ENABLE PORTAUTH (289 ページ)

ENABLE PORTAUTH PORT (291 ページ)

SET PORTAUTH PORT (346 ページ)

SET PORTAUTH PORT SUPPLICANTMAC ( 350 ページ )

SHOW PORTAUTH ( 441 ページ )

SHOW PORTAUTH COUNTER ( 444 ページ )

SHOW PORTAUTH MULTISUPPLICANT PORT ( 447 ページ )

SHOW PORTAUTH PORT ( 451 ページ )

SHOW PORTAUTH TIMER ( 456 ページ )



## SET PORTAUTH USERNAME

カテゴリー：スイッチング / ポート認証

**SET PORTAUTH** [=8021X] **USERNAME**=*login-name* **PASSWORD**=*password* [METHOD={OTP  
[ENCRYPTION={MD4|MD5}]]|STANDARD}]

*login-name*: ログイン名 (1~64 文字。英数字のみ使用可能。大文字小文字を区別しない)

*password*: パスワード (文字数は認証方式によって異なる。英数字のみ使用可能。大文字小文字を区別する)

### 解説

Supplicant 時に使用するグローバルなユーザー名、パスワード、パスワード暗号化方式およびアルゴリズムを設定する。

本コマンドで設定するのは、Supplicant ポート固有のユーザー名、パスワードが設定されていないときに使用するグローバル値。ENABLE PORTAUTH PORT コマンド、SET PORTAUTH PORT コマンドで Supplicant ポート固有のユーザー名が設定されているときは、本コマンドで設定した値ではなく、Supplicant ポート固有の設定値が使用される。

### パラメーター

**PORTAUTH** 認証メカニズム。本コマンドでは 8021X (802.1X 認証) のみ有効。省略時は 8021X と見なされるため、特に指定する必要はない。

**USERNAME** 認証を受けるためのユーザー名。デフォルトは portAuthportAuth

**PASSWORD** 認証を受けるためのパスワード。METHOD パラメーターに STANDARD を指定した場合は、6~63 文字の文字列を指定する。METHOD パラメーターに OTP を指定した場合は、10~63 文字の文字列 (認証サーバー上で設定した OTP Initialisation Password と同じ値) を指定する。デフォルトは portAuthportAuth

**METHOD** パスワード送信時の暗号化方式。STANDARD (EAP-MD5) または OTP (One-Time Password) から選択する。OTP を指定した場合は、ENCRYPTION パラメーターでワンタイムパスワードの生成アルゴリズムも指定する必要がある。デフォルトは STANDARD。

**ENCRYPTION** ワンタイムパスワードの生成アルゴリズム。MD4、MD5 から選択する。デフォルトは MD5。METHOD パラメーターに OTP を指定した場合の必須パラメーター。

### 備考・注意事項

パスワードは設定ファイルに平文のまま保存されるため、管理には注意すること。

### 関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (170 ページ)

ENABLE PORTAUTH (289 ページ)

ENABLE PORTAUTH PORT ( 291 ページ )

SET PORTAUTH PORT ( 346 ページ )

SET PORTAUTH PORT SUPPLICANTMAC ( 350 ページ )

SHOW PORTAUTH ( 441 ページ )

SHOW PORTAUTH COUNTER ( 444 ページ )

SHOW PORTAUTH MULTISUPPLICANT PORT ( 447 ページ )

SHOW PORTAUTH PORT ( 451 ページ )

SHOW PORTAUTH TIMER ( 456 ページ )

## SET QOS ACCELERATOR POLICY

カテゴリー：スイッチング / QoS

備考：IPv6 アクセラレーターボード AT-ACC01 と拡張メモリー AT-SD512A-001 が必要（本機能は 9924SP では使用できません）

**SET QOS ACCELERATOR POLICY={*qos-id*|NONE}**

*qos-id*: QoS ポリシー番号（0～255）

### 解説

IPv6 ルーティングパケット（IPv6 アクセラレーターボードを経由したパケット）に適用する QoS ポリシーを指定する。

本 QoS ポリシーで使用するクラシファイアは、CREATE CLASSIFIER コマンドのページに掲載されている「IPv6 QoS ポリシー用の構文」にしたがっていないとエラーになる。同構文にないパラメーターを含むクラシファイアを使おうとすると、エラーになる。

### パラメーター

**POLICY** QoS ポリシー番号。該当ポートで受信したパケットに対しては、本パラメーターで指定した QoS ポリシーが適用される。すでに別のポリシーが割り当てられていた場合は、本パラメーターで指定したポリシーに変更される。NONE を指定した場合、該当ポートには QoS ポリシーを割り当てない（割り当てを解除する）。

### 例

IPv6 ルーティングパケットに対して、QoS ポリシー 10 を割り当てる。

```
SET QOS ACCELERATOR POLICY=10
```

### 備考・注意事項

IPv6 ルーティングパケットに適用できる QoS ポリシーは 1 つだけ。

### 関連コマンド

CREATE QOS POLICY（212 ページ）

SHOW QOS POLICY（465 ページ）

## SET QOS DEFAULTPRIORITY

カテゴリー：スイッチング / QoS

**SET QOS DEFAULTPRIORITY=*p0,p1,p2,p3,p4,p5,p6,p7***

*p0*~7: 送信キュー 0~7 に対応する送信時のユーザープライオリティー (0~7)

### 解説

受信時にタグなしだったパケットをタグ付きポートから送信するときの 802.1p ユーザープライオリティー値を指定する。

具体的には、パケットが格納されている送信キュー（デフォルト送信キュー）と送信時のユーザープライオリティーのマッピングを行う。

なお、本コマンドの設定が適用されるのは、受信時にタグなしで、なおかつ、他の QoS 機能（DSCP MAP や QUEUE2PRIOMAP）によってユーザープライオリティーが明示的に割り当てられなかったパケットだけ。

### パラメーター

**DEFAULTPRIORITY** 送信キュー 0~7 に対応する送信時のユーザープライオリティー値をカンマ区切りで指定する。本パラメーターには、*p0* から *p7* まですべての値を指定すること。デフォルトは 1,2,0,3,4,5,6,7。

### 関連コマンド

SET QOS PORT ( 365 ページ )

SHOW QOS DEFAULTPRIORITY ( 460 ページ )

SHOW QOS PORT ( 468 ページ )

## SET QOS DSCPMAP

カテゴリー：スイッチング / QoS

**SET QOS DSCPMAP** [= {PREMARKING|REMARKING}] **DSCP=dscp-list**

[BWCLASS=bwclass-list] [NEWDSCP=0..63] [NEWBWCLASS=1..3] [NEWQUEUE=0..7]  
[NEWPRIORITY=0..7]

*dscp-list*: DSCP 値 (0~63。ハイフン、カンマを使った複数指定も可能)

*bwclass-list*: 帯域クラス (1~3。ハイフン、カンマを使った複数指定も可能)

### 解説

DSCPMAP テーブルの設定を変更する。

DSCPMAP テーブルは、受信パケットに 4 つの QoS パラメーター (DSCP 値、帯域クラス、送信キュー、802.1p プライオリティー値) を割り当てるためのテーブル。プレマールキング用とリマールキング用の 2 つがあり、それぞれポリシーベース QoS のプレマールキングステージとリマールキングステージで使用される。

DSCPMAP テーブルは、DSCP 値 (0~63) と帯域クラス (1~3) をインデックスとし、各エントリーには書き換え後の QoS パラメーター値が格納されている (プレマールキング用 DSCPMAP テーブルの帯域クラスインデックス値は 1 のみ)。

なお、明示的に帯域クラスが割り当てられていないパケットは、デフォルトの帯域クラス 1 として扱われる。

### パラメーター

**DSCPMAP** DSCPMAP テーブルの種類。PREMARKING (プレマールキング用)、REMARKING (リマールキング用) から選択する。省略時は両方が対象。

**DSCP** テーブルのインデックスとしての DSCP 値。ハイフン、カンマを使った複数指定も可能。

**BWCLASS** テーブルのインデックスとしての帯域クラス。DSCPMAP=PREMARKING のときは 1 のみ、DSCPMAP=REMARKING のときは 1~3 から選択する。省略時はすべての帯域クラスが対象。

**NEWDSCP** 対象パケットに割り当てる新しい DSCP 値。DSCPMAP テーブルのデフォルト設定では、インデックスの DSCP 値と同じ値

**NEWBWCLASS** 対象パケットに割り当てる新しい帯域クラス。DSCPMAP テーブルのデフォルト設定では、インデックスの帯域クラスと同じ値

**NEWQUEUE** 対象パケットに割り当てる新しい送信キュー。DSCPMAP テーブルのデフォルト設定では、すべて 0

**NEWPRIORITY** 対象パケットに割り当てる新しい 802.1p ユーザープライオリティー値。DSCPMAP テーブルのデフォルト設定では、すべて 0

### 例

DSCP 値が 32~63 で帯域クラスが 2 のパケットに対し、DSCP 値を 2 に、帯域クラスを 3 に、送信キューを 0 に、802.1p プライオリティー値を 1 に書き換えるよう、リマールキング用 DSCPMAP テーブルの設定を

変更する。

```
SET QOS DSCPMAP=REMARKING DSCP=32-63 BWCLASS=2 NEWDSCP=2 NEWBWCLASS=3  
NEWQUEUE=0 NEWPRIORITY=1
```

### 関連コマンド

CREATE QOS FLOWGROUP ( 209 ページ )  
CREATE QOS POLICY ( 212 ページ )  
CREATE QOS TRAFFICCLASS ( 218 ページ )  
SET QOS FLOWGROUP ( 359 ページ )  
SET QOS POLICY ( 361 ページ )  
SET QOS TRAFFICCLASS ( 373 ページ )  
SHOW QOS DSCPMAP ( 461 ページ )

## SET QOS FLOWGROUP

カテゴリー：スイッチング / QoS

```
SET QOS FLOWGROUP=flow-list [PREMARKING={USEMARKVALUE|USEDSCP|NONE}]
[MARKVALUE={0..63|NONE}] [DESCRIPTION=string] [ACTION={FORWARD|DISCARD|
SENDMIRROR|SENDVLANPORT|FORWARD, SENDMIRROR|SENDMIRROR, SENDVLANPORT|
NONE}] [VLAN=1..4094 PORT=port-number]
```

*flow-list*: フローグループ番号 (0~1023)。ハイフン、カンマを使った複数指定も可能)

*string*: 文字列 (1~15 文字。空白を含む場合はダブルクォートで囲む)

*port-number*: スイッチポート番号 (1~)

### 解説

フローグループの設定を変更する。

### パラメーター

**FLOWGROUP** フローグループ番号

**PREMARKING** プレマーキングの動作を指定する。具体的には、フローグループに割り当てる QoS パラメーターをプレマーキング用 DSCP MAP テーブルから検索するときに、どの値をインデックスとして使うかを指定する。USEMARKVALUE を指定した場合は、MARKVALUE パラメーターの値をインデックスとして使う。USEDSCP を指定した場合は、パケットの DSCP フィールド値をインデックスとして使う。いずれの場合も、DSCP MAP テーブルのもう 1 つのインデックスである帯域クラスは 1 を使う。NONE を指定した場合は、フローグループではプレマーキングを行わず、トラフィックグループの処理に移る。省略時は NONE。なお、トラフィッククラスとフローグループの両方で本パラメーターが指定されている場合は、フローグループの設定が使われる。なお、IPv6 ルーティングパケットに対する QoS ポリシーでは、USEDSCP を使用できないので注意すること (指定しても効果がない)。

**MARKVALUE** PREMARKING パラメーターに USEMARKVALUE を指定した場合、プレマーキング用 DSCP MAP テーブルの検索インデックスとして使う DSCP 値を指定する。省略時は NONE

**DESCRIPTION** フローグループの説明 (メモとして使う)

**ACTION** 本フローグループのパケットに対するアクション。アクションの詳細は別表を参照のこと。アクションはフローグループとトラフィッククラスの両方に設定できるが、フローグループのアクションのほうが優先される (ただし、フローグループのアクションが NONE のときは、トラフィッククラスのアクションが実行される)。省略時は NONE

**VLAN** 本フローグループに属するパケットの出力先 VLAN。ACTION パラメーターに SENDVLANPORT を指定したときのみ有効かつ必須。本パラメーターは、必ず PORT パラメーターと組で指定すること。

**PORT** 本フローグループに属するパケットの出力先ポート。ACTION パラメーターに SENDVLANPORT を指定したときのみ有効かつ必須。本パラメーターは、必ず VLAN パラメーターと組で指定する

こと。

FORWARD	パケットを通常どおり出力する
DISCARD	パケットを破棄する
SENDVLANPORT	パケットの出力先を VLAN パラメーターと PORT パラメーターで指定されたポートに変更する。このとき、出力ポート (PORT) は出力 VLAN (VLAN) に所属していなくてはならないので、設定には注意すること
SENDMIRROR	パケットのコピーをミラーポートから出力する。あらかじめ、SET SWITCH MIRROR コマンドでミラーポートを指定し、ENABLE SWITCH MIRROR コマンドでポートミラーリング機能を有効にしておく必要がある
FORWARD,SENDMIRROR	FORWARD と SENDMIRROR の両方の処理を行う。SENDMIRROR だけ指定した場合と同じ動作
SENDMIRROR,SENDVLANPORT	SENDMIRROR と SENDVLANPORT の両方の処理を行う
NONE	本フローグループが所属しているトラフィッククラスのアクションにしたがってパケットを処理する

表 39: ACTION パラメーターに指定できるオプション

### 備考・注意事項

ACTION、VLAN、PORT パラメーターは、IPv6 アクセラレーター用の QoS ポリシーでは未サポート。

### 関連コマンド

ADD QOS FLOWGROUP ( 179 ページ )  
 CREATE QOS FLOWGROUP ( 209 ページ )  
 DELETE QOS FLOWGROUP ( 231 ページ )  
 DESTROY QOS FLOWGROUP ( 246 ページ )  
 SET QOS DSCP MAP ( 357 ページ )  
 SHOW QOS DSCP MAP ( 461 ページ )  
 SHOW QOS FLOWGROUP ( 463 ページ )



## SET QOS POLICY

カテゴリー：スイッチング / QoS

```
SET QOS POLICY=qos-list [DTCDROPBWCLASS3={YES|NO}]
[DTCIGNOREBWCLASS={YES|NO}] [DTCMAXBANDWIDTH={bandwidth|NONE}]
[DTCMAXBURSTSIZE=burstsize] [DTCMINBANDWIDTH={bandwidth|NONE}]
[DTCMINBURSTSIZE=burstsize] [DTCPREMARKING={USEMARKVALUE|USEDSCP|NONE}]
[DTCREMARKING={USEDSCPMAP|PRIORITY|PRIO+BWCLASS|BWCLASS|NONE}]
[MARKVALUE={0..63|NONE}] [DESCRIPTION=string] [DTCACTION={FORWARD|
DISCARD|SENDMIRROR|SENDVLANPORT|FORWARD,SENDMIRROR|
SENDMIRROR,SENDVLANPORT}] [VLAN=1..4094 PORT=port-number]
```

*qos-list*: QoS ポリシー番号 (0~255。ハイフン、カンマを使った複数指定も可能)

*bandwidth*: 帯域幅 (1~16998400Kbps)

*burstsize*: バーストサイズ (0~268435455Byte)

*string*: 文字列 (1~15 文字。空白を含む場合はダブルクォートで囲む)

*port-number*: スイッチポート番号 (1~)

### 解説

QoS ポリシーの設定を変更する。

### パラメーター

**POLICY** QoS ポリシー番号

**DTCDROPBWCLASS3** 本ポリシーのデフォルトトラフィッククラスにおいて、最大帯域設定 (DTCMAXBANDWIDTH と DTCMAXBURSTSIZE) を上回るレートで受信したパケットをキューイング前に無条件で破棄するかどうか。YES を指定した場合、超過分のパケットは送信キューに格納される前に破棄される。NO を指定した場合、超過分のパケットは「帯域クラス 3 (使いすぎクラス)」に分類されるだけでただしには破棄されない。ただし、RED アルゴリズムの設定により、送信キューにおいて「帯域クラス 3」を優先的に破棄するような設定が可能。省略時は NO。

**DTCIGNOREBWCLASS** 本ポリシーのデフォルトトラフィッククラスに対して最大・最小帯域の設定 (DTCMAXBANDWIDTH、DTCMINBANDWIDTH) がなされている場合、メータリング時にプレマーキングで割り当てられた「帯域クラス」を考慮するか無視するかを指定する。YES を指定した場合、プレマーキング時に割り当てられた帯域クラスは無視され、実際の帯域使用量にのみ基づいて帯域クラスが決定される。NO を指定した場合は、プレマーキングで割り当てられた帯域クラスが、そのままメータリング結果として採用される。省略時は NO。

**DTCMAXBANDWIDTH** 本ポリシーのデフォルトトラフィッククラスに割り当てる最大帯域幅 (Kbps)。デフォルトトラフィッククラスに割り当てる帯域は、原則としてここで指定した値までに制限される。数値だけで指定する場合の単位は Kbps。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「Kbps」、「Mbps」、「Gbps」の意味になる。「M」、「G」を指定する場合は、「2.256G」や「128.4M」のように小数を指定することもできる。QoS ポリシーを適用するスイッチポートの帯域と

矛盾しないように設定すること。省略時は NONE。

**DTCMAXBURSTSIZE** デフォルトトラフィッククラスの最大帯域幅設定 (DTCMAXBANDWIDTH) に対する、最大許容バーストサイズ (Byte)。トラフィックの流入量が DTCMAXBANDWIDTH を超えた場合に、DTCMAXBANDWIDTH 超過分としてバッファリング可能な最大データ量を指定する。数値だけで指定する場合の単位は Byte。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「Kbyte」、「Mbyte」、「Gbyte」の意味になる。「K」、「M」、「G」を指定する場合は、「2.256G」や「128.4M」のように小数を指定することもできる。バーストサイズが DTCMAXBURSTSIZE を上回った場合、超過分のパケットはキューイング前に破棄されるか (DTCDROPBWCLASS3=YES のとき)、帯域クラス 3 に分類される (DTCDROPBWCLASS3=NO のとき)。省略時は 0。

**DTCMINBANDWIDTH** 本ポリシーのデフォルトトラフィックに割り当てる最小帯域幅 (Kbps)。デフォルトトラフィッククラスには、原則としてここで指定した帯域が確保される。数値だけで指定する場合の単位は Kbps。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「Kbps」、「Mbps」、「Gbps」の意味になる。「M」、「G」を指定する場合は、「2.256G」や「128.4M」のように小数を指定することもできる。QoS ポリシーを適用するスイッチポートの帯域と矛盾しないように設定すること。省略時は NONE。

**DTCMINBURSTSIZE** デフォルトトラフィッククラスの最小帯域幅設定 (DTCMINBANDWIDTH) に対する、「帯域クラス 1」の最大許容バーストサイズ (Byte)。DTCMINBANDWIDTH が NONE のときは、最大帯域幅設定 (DTCMAXBANDWIDTH) に対する、「帯域クラス 2」の最大許容バーストサイズ (Byte)。数値だけで指定する場合の単位は Byte。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「Kbyte」、「Mbyte」、「Gbyte」の意味になる。「K」、「M」、「G」を指定する場合は、「2.256G」や「128.4M」のように小数を指定することもできる。DTCMINBANDWIDTH が NONE のときは、DTCMAXBURSTSIZE よりも小さい値でなくてはならない。詳細は解説編を参照。省略時は 0。

**DTCPREMARKING** 本ポリシーのデフォルトトラフィッククラスに対するプレマーキングの動作を指定する。具体的には、デフォルトトラフィッククラスに割り当てる QoS パラメーターをプレマーキング用 DSCPMAP テーブルから検索するときに、どの値をインデックスとして使うかを指定する。USEMARKVALUE を指定した場合は、MARKVALUE パラメーターの値をインデックスとして使う。USEDSCP を指定した場合は、パケットの DSCP フィールド値をインデックスとして使う。いずれの場合も、DSCPMAP テーブルのもう 1 つのインデックスである帯域クラスは 1 を使う。NONE を指定した場合は、プレマーキングを行わずに、メータリングの処理に移る。省略時は NONE。なお、IPv6 ルーティングパケットに対する QoS ポリシーでは、USEDSCP を使用できないので注意すること (指定しても効果がない)。

**DTCREMARKING** 本ポリシーのデフォルトトラフィッククラスに対するリマーキングの動作を指定する。具体的には、メータリング後の QoS パラメーター書き換え動作を何に基づいて実施するか、および、どのパラメーターを書き換えるかを指定する。USEDSCPMAP を指定した場合は、リマーキング直前の帯域クラスとパケットの DSCP 値をインデックスとしてリマーキング用 DSCPMAP テーブルを検索し、DSCP 値、帯域クラス、送信キュー、802.1p プライオリティー値を書き換える。PRIORITY、PRIO+BWCLASS を指定した場合は、リマーキング直前の送信キューと帯域クラスをインデックスとして QUEUE2PRIOMAP テーブルを検索し、802.1p プライオリティー値を書き換える。BWCLASS、NONE を指定した場合は書き換えを行わない。省略時は NONE。なお、PRIORITY と PRIO+BWCLASS、BWCLASS と NONE はそれぞれ同じ意味になる。また、IPv6 ルーティングパケットに対する QoS ポリシーでは、USEDSCPMAP を使用できないので注意すること (指定しても

効果がない)。

**MARKVALUE** PREMARKING パラメーターに USEMARKVALUE を指定した場合、プレマーキング用 DSCPMAP テーブルの検索インデックスとして使う DSCP 値を指定する。省略時は NONE

**DESCRIPTION** ポリシーの説明 (メモとして使う)。POLICY パラメーターに複数の番号を指定した場合は、すべてのポリシーに同じメモ文字列が設定される

**DTCACTION** 本ポリシーのデフォルトトラフィッククラスに対するアクション。アクションの詳細は別表を参照のこと。アクションはフローグループとトラフィッククラスの両方に設定できるが、フローグループのアクションのほうが優先される (ただし、フローグループのアクションが NONE のときは、トラフィッククラスのアクションが実行される)。省略時は FORWARD

**VLAN** 本ポリシーのデフォルトトラフィッククラスに属するパケットの出力先 VLAN。DTCACTION パラメーターに SENDVLANPORT を指定したときのみ有効かつ必須。本パラメーターは、必ず PORT パラメーターと組で指定すること。

**PORT** 本ポリシーのデフォルトトラフィッククラスに属するパケットの出力先ポート。DTCACTION パラメーターに SENDVLANPORT を指定したときのみ有効かつ必須。本パラメーターは、必ず VLAN パラメーターと組で指定すること。

FORWARD	パケットを通常どおり出力する
DISCARD	パケットを破棄する
SENDVLANPORT	パケットの出力先を VLAN パラメーターと PORT パラメーターで指定されたポートに変更する。このとき、出力ポート (PORT) は出力 VLAN (VLAN) に所属していなくてはならないので、設定には注意すること
SENDMIRROR	パケットのコピーをミラーポートから出力する。あらかじめ、SET SWITCH MIRROR コマンドでミラーポートを指定し、ENABLE SWITCH MIRROR コマンドでポートミラーリング機能を有効にしておく必要がある
FORWARD,SENDMIRROR	FORWARD と SENDMIRROR の両方の処理を行う。SENDMIRROR だけ指定した場合と同じ動作
SENDMIRROR,SENDVLANPORT	SENDMIRROR と SENDVLANPORT の両方の処理を行う

表 40: DTCACTION パラメーターに指定できるオプション

## 備考・注意事項

DTCACTION、VLAN、PORT パラメーターは、IPv6 アクセラレーター用の QoS ポリシーでは未サポート。

## 関連コマンド

ADD QOS POLICY ( 180 ページ )

CREATE QOS POLICY ( 212 ページ )

DELETE QOS POLICY ( 232 ページ )

DESTROY QOS POLICY ( 247 ページ )

SET QOS DSCPMAP ( 357 ページ )

SET QOS PORT ( 365 ページ )

SET QOS QUEUE2PRIOMAP ( 370 ページ )

SHOW QOS DSCPMAP ( 461 ページ )

SHOW QOS POLICY ( 465 ページ )

SHOW QOS QUEUE2PRIOMAP ( 472 ページ )

## SET QOS PORT

カテゴリー：スイッチング / QoS

```
SET QOS PORT={port-list|ALL} [POLICY={qos-id|NONE}] [DEFAULTQUEUE=0..7]
[FORCEDEFQUEUE={YES|NO}] [RED={red-id|NONE}]
```

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

*qos-id*: QoS ポリシー番号 (0～255)

*red-id*: RED カーブセット番号 (1～4)

### 解説

指定ポートで受信したパケットに対する QoS の適用方法を指定する。また、指定ポートの送信キューで使用する輻輳回避アルゴリズムを指定する。

本コマンドでは、受信パケットに適用する QoS ポリシーの指定をはじめ、タグなしパケットに割り当てるデフォルトの送信キューや、キューイング時に適用する輻輳回避アルゴリズムの指定などができる。

### パラメーター

**PORT** スイッチポート番号

**POLICY** QoS ポリシー番号。該当ポートで受信したパケットに対しては、本パラメーターで指定した QoS ポリシーが適用される。NONE を指定した場合、該当ポートには QoS ポリシーを割り当てない (割り当てを解除する)。

**DEFAULTQUEUE** 該当ポートで受信したタグなしパケットに割り当てるデフォルトの送信キュー。プレマッキング、リマッキングステージで送信キューが変更されなかった場合、該当パケットはここで指定されたキューから送信される。デフォルトは 2。

**FORCEDEFQUEUE** DEFAULTQUEUE パラメーターの設定をすべての受信パケットに適用するかどうか。YES を指定した場合、タグの有無に関わらず、すべての受信パケットに DEFAULTQUEUE パラメーターで指定した送信キューを割り当てる。NO を指定した場合は、タグなしパケットにだけ DEFAULTQUEUE を割り当て、タグ付きパケットの送信キューは SET QOS PRIO2QUEUEMAP コマンドの設定内容に基づいて決定する。デフォルトは NO。

**RED** RED カーブセット番号。パケットを該当ポートの送信キューに格納する際に、どのような輻輳回避アルゴリズムを適用するかを指定する。NONE を指定した場合は、最大キュー長を超えたパケットを単純に破棄する Tail-drop アルゴリズムを使用する (最大キュー長はデフォルトの RED カーブセット「1」の STOP1、STOP2、STOP3 パラメーターによって指定する)。RED カーブセット番号を指定した場合は、指定したセットの設定に基づいて RED アルゴリズムを適用する。パケット受信時の動作を規定する他のパラメーターとは異なり、本パラメーターは PORT で指定したポートからパケットを送信するときの動作を指定するものなので注意。

### 例

スイッチポート 1 に QoS ポリシー 1 を割り当てる。

```
SET QOS PORT=1 POLICY=1
```

すべてのスイッチポートに対し、受信したタグなしパケットのデフォルト送信キューを 0 番に設定する。

```
SET QOS PORT=ALL DEFAULTQUEUE=0
```

スイッチポート 1-8 から送信するパケットに対し、RED カーブセット「3」に基づく RED アルゴリズムを適用する。

```
SET QOS PORT=1-8 RED=3
```

### 備考・注意事項

トランクグループに QoS ポリシーを割り当てるときは、いずれかの所属ポートにポリシーを適用すればよい。ただし、所属ポートがポートグループ「1～12」と「13～24」をまたいでいるトランクグループには QoS ポリシーを適用できないので注意。

### 関連コマンド

SHOW QOS POLICY ( 465 ページ )

SHOW QOS PORT ( 468 ページ )

## SET QOS PORT EGRESSQUEUE

カテゴリー：スイッチング / QoS

```
SET QOS PORT={port-list|ALL} EGRESSQUEUE [= queue-list] [LENGTH=1..65520]
[MAXBANDWIDTH={bandwidth|NONE}] [SCHEDULER={STRICT|WRR1|WRR2}]
[WRRWEIGHT=6..255]
```

*port-list*: スイッチポート番号 (1~。ハイフン、カンマを使った複数指定も可能)

*queue-list*: 送信キュー (0~7。ハイフン、カンマを使った複数指定も可能)

*bandwidth*: 帯域幅 (1~2665845Kbps)

### 解説

指定ポートの送信キューに関する設定を変更する。

### パラメーター

**PORT** スイッチポート番号

**EGRESSQUEUE** 送信キュー。値を指定しなかった場合は、該当ポートのすべての送信キューが対象となる。

**LENGTH** 最大キュー長。単位はパケット数。指定値が16の倍数でない場合は、もっとも近い16の倍数に丸められる。デフォルトは128。

**MAXBANDWIDTH** 送信キューの最大帯域幅 (Kbps)。設定値の刻み幅はおよそ651Kbpsであり、指定値はもっとも近い刻み値に丸められる。NONEは制限なし。NONE以外の値を指定した場合は、該当ポートのすべての送信キューのLENGTHパラメーターに最小値の16を指定する必要がある。数値だけで指定する場合の単位はKbps。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「Kbps」、「Mbps」、「Gbps」の意味になる。「M」、「G」を指定する場合は、「0.256G」や「128.4M」のように小数を指定することもできる。スイッチポートの帯域 (SET SWITCH PORT コマンドのEGRESSLIMITパラメーター) と矛盾しないように設定すること。デフォルトはNONE。

**SCHEDULER** 該当キューで使用する送信スケジューリング方式。STRICT (絶対優先)、WRR1 (重み付きラウンドロビン1)、WRR2 (重み付きラウンドロビン2) の3つから選択する。同一ポート上の送信キューは、前記3つのスケジューリンググループのどれかに所属し、グループごとに送信動作が実行される。STRICTグループでは、上位キュー (番号の大きなキュー) の送信が完了するまで下位キューからはパケットが送信されない。WRR1グループでは、各キューの重み付け (WRRWEIGHT) に基づきラウンドロビンでパケットが送信される。ただし、WRR1グループ内のキューからの送信は、STRICTグループのキューがすべて空になっているときだけ行われる。WRR2グループでは、WRR1と同じく各キューの重み付け (WRRWEIGHT) に基づきラウンドロビンでパケットが送信されるが、WRR2グループ内のキューからの送信は、STRICTグループ、WRR1グループのキューがすべて空になっているときだけ行われる。デフォルトはSTRICT。

**WRRWEIGHT** 送信キューの重み付け値。スケジューリング方式としてWRR1、WRR2を指定している場合、同一グループ内での送信比率 (パケット数ではなくデータ量) を指定する。たとえば、WRR1



グループに所属する2つのキューがそれぞれ WRRWEIGHT=6、WRRWEIGHT=24 の重み付け値を持つ場合、前者から1単位のデータを送信する間に後者からは4単位のデータが送信される。デフォルトは6。

### 例

すべてのスイッチポートに対し、送信スケジューリング方式として重み付きラウンドロビンを使うよう設定する。各キューからの送信比率は、上位キューから 10:10:5:5:2:2:1:1 とする。

```
SET QOS PORT=ALL EGRESSQUEUE=6-7 SCHEDULER=WRR1 WRRWEIGHT=60
SET QOS PORT=ALL EGRESSQUEUE=4-5 SCHEDULER=WRR1 WRRWEIGHT=30
SET QOS PORT=ALL EGRESSQUEUE=2-3 SCHEDULER=WRR1 WRRWEIGHT=12
SET QOS PORT=ALL EGRESSQUEUE=0-1 SCHEDULER=WRR1 WRRWEIGHT=6
```

### 備考・注意事項

スイッチポートの帯域制限機能 (SET SWITCH PORT コマンドの EGRESSLIMIT パラメーター) と重み付きラウンドロビン (WRR) スケジューリングは併用できない。

### 関連コマンド

DISABLE SWITCH PORT EGRESSQUEUE (276 ページ)  
 ENABLE SWITCH PORT EGRESSQUEUE (306 ページ)  
 SHOW QOS PORT (468 ページ)  
 SHOW SWITCH PORT (509 ページ)



## SET QOS PRIO2QUEUEMAP

カテゴリー：スイッチング / QoS

**SET QOS PRIO2QUEUEMAP=p0,p1,p2,p3,p4,p5,p6,p7**

p0~7: ユーザープライオリティー 0~7 のフレームに対応する送信キュー (0~7。大きいほど優先度が高い)

### 解説

IEEE 802.1p QoS (Quality of Service) の基本設定を変更する。

具体的には、受信したタグ付きパケットの 802.1p ユーザープライオリティー値と、本製品の送信キューのマッピングを変更する。

タグなしパケットに割り当てるデフォルトの送信キューは、スイッチポートごとに SET QOS PORT コマンドの DEFAULTQUEUE パラメーターで設定する。

### パラメーター

**PRIO2QUEUEMAP** ユーザープライオリティー 0~7 に対応する送信キューの番号をカンマで区切って指定する。送信キューはポートごとに 0~7 の 8 つがあり、7 がもっとも優先度が高い。8 つのキューからパケットがどのような順序で送信されるかは、SET QOS PORT EGRESSQUEUE コマンドの SCHEDULER パラメーターの設定による。また、タグなしパケットに割り当てるデフォルトの送信キューは、スイッチポートごとに SET QOS PORT コマンドの DEFAULTQUEUE パラメーターで設定する。本パラメーターには、p0 から p7 まですべての値を指定すること。デフォルトは 2,0,1,3,4,5,6,7。

### 例

タグ付きパケットの 802.1p ユーザープライオリティー値 0~7 に対し、送信キュー 0, 0, 3, 3, 4, 5, 6, 7 を割り当てる。

```
SET QOS PRIO2QUEUEMAP=0,0,3,3,4,5,6,7
```

### 関連コマンド

SHOW QOS PRIO2QUEUEMAP (471 ページ)

## SET QOS QUEUE2PRIOMAP

カテゴリー：スイッチング / QoS

**SET QOS QUEUE2PRIOMAP QUEUE=queue-list** [BWCLASS=bwclass-list]  
[NEWPRIORITY=0..7]

*queue-list*: 送信キュー（0～7。ハイフン、カンマを使った複数指定も可能）

*bwclass-list*: 帯域クラス（1～3。ハイフン、カンマを使った複数指定も可能）

### 解説

リマーケティング時に使用される 802.1p ユーザープライオリティー値の書き換えテーブル（QUEUE2PRIOMAP テーブル）を編集する。

具体的には、パケットが格納されている送信キューとパケットに割り当てられている帯域クラスの組み合わせに対して、書き換え後のユーザープライオリティー値を指定する（明示的に帯域クラスが割り当てられていないパケットは、デフォルトの帯域クラス 1 として扱われる）。

QUEUE2PRIOMAP テーブルは、トラフィッククラスの REMARKING パラメーターに PRIORITY か PRIO+BWCLASS を指定した場合に使用される。

### パラメーター

**QUEUE** テーブルのインデックスとしての送信キュー番号。

**BWCLASS** テーブルのインデックスとしての帯域クラス。省略時はすべての帯域クラスが対象になる。

**NEWPRIORITY** 対象パケットに割り当て新しい 802.1p ユーザープライオリティー値。

### 例

送信キューが 7 で帯域クラスが 2 のパケットに対し、送信時の 802.1p ユーザープライオリティー値として 1 を割り当てよう QUEUE2PRIOMAP テーブルを編集する。

```
SET QOS QUEUE2PRIOMAP QUEUE=7 BWCLASS=2 NEWPRIORITY=1
```

### 関連コマンド

SHOW QOS QUEUE2PRIOMAP (472 ページ)

## SET QOS RED

カテゴリー：スイッチング / QoS

```
SET QOS RED=red-id [AVERAGING=0..15] [QUEUE=queue-list] [START1=length]
[STOP1=length] [DROP1=0..15] [START2=length] [STOP2=length]
[DROP2=0..15] [START3=length] [STOP3=length] [DROP3=0..15]
[DESCRIPTION=string]
```

*red-id*: RED カーブセット番号 (1~4)

*queue-list*: 送信キュー (0~7。ハイフン、カンマを使った複数指定も可能)

*length*: キュー長 (0~16000000Kbyte)

*string*: 文字列 (1~15 文字。空白を含む場合はダブルクォートで囲む)

### 解説

RED (Random Early Detection/Discard) カーブセットの設定を変更する。

RED カーブセットは、8 つの送信キュー × 3 つの帯域クラスのそれぞれに対する RED カーブ (24 個) を束ねたもの。RED カーブは、それぞれ START<sub>x</sub>、STOP<sub>x</sub>、DROP<sub>x</sub> (x は帯域クラス) という 3 つのパラメータを持つ。詳細は解説編を参照のこと。

実際に RED を使用するには、SET QOS PORT コマンドの RED パラメータでスイッチポートに RED カーブセットを割り当てる必要がある。RED パラメータに NONE (デフォルト値) を指定した場合は、Tail-drop 動作となる。

なお、デフォルトの RED カーブセット「1」の設定の一部は、Tail-drop にも使用される (STOP1、STOP2、STOP3 パラメータが、それぞれ帯域クラス 1、2、3 の最大キュー長を示す)。

また、RED、Tail-drop のどちらの場合も、明示的に帯域クラスが割り当てられていないパケットは、デフォルトの帯域クラス 1 として扱われる。

### パラメーター

**RED** RED カーブセット番号

**AVERAGING** 平均キュー長の算出に使う期間を示す係数。0 を指定した場合、算出された平均キュー長はその時点でのキュー長に等しくなる。また、本パラメータの値が大きいくほど、時間的に広い範囲のデータを使用して平均キュー長を算出するようになる。これにより、キュー長が STOP<sub>x</sub> (x は 1~3) に近い状況における TCP のパフォーマンスが向上する。デフォルトは 9。

**QUEUE** 送信キュー。値を指定しなかった場合は、すべての送信キューが対象となる。

**START1** 帯域クラス 1 のパケットを破棄し始めるポイント。キュー長 (Kbyte) で指定する。キュー長がこのポイントを超えると、帯域クラス 1 のパケット破棄率が徐々に高くなり、STOP1 に達したときに破棄率が DROP1 で指定された値となる。デフォルトは 25Kbyte。

**STOP1** 帯域クラス 1 のパケットを完全に破棄し始めるポイント。キュー長 (Kbyte) で指定する。キュー長がこのポイントを超えると、帯域クラス 1 のすべてのパケットが破棄されるようになる。デフォルトは 30Kbyte。なお、デフォルトの RED カーブセット「1」では、本パラメータの値が、Tail-drop

における帯域クラス 1 の最大キュー長としても使われる。

**DROP1** キュー長が STOP1 に達したときの帯域クラス 1 のパケット破棄率を示す係数。実際の破棄率は、「2 の DROP1 乗」の逆数として求められる。たとえば、DROP1=0 なら破棄率は 100%、DROP1=1 なら 50%、DROP1=2 なら 25%、DROP1=3 なら 12.5%、DROP1=4 なら 6.25%となる。言い換えると、DROP1 が 0 のときは破棄率が 100%で、以後 DROP1 が 1 増えるたびに破棄率が半分になっていく。デフォルトは 1 ( 50% )。

**START2** 帯域クラス 2 のパケットを破棄し始めるポイント。キュー長 ( Kbyte ) で指定する。キュー長がこのポイントを超えると、帯域クラス 2 のパケット破棄率が徐々に高くなり、STOP2 に達したときに破棄率が DROP2 で指定された値となる。デフォルトは 15Kbyte。

**STOP2** 帯域クラス 2 のパケットを完全に破棄し始めるポイント。キュー長 ( Kbyte ) で指定する。キュー長がこのポイントを超えると、帯域クラス 2 のすべてのパケットが破棄されるようになる。デフォルトは 25Kbyte。なお、デフォルトの RED カーブセット「1」では、本パラメーターの値が、Tail-drop における帯域クラス 2 の最大キュー長としても使われる。

**DROP2** キュー長が STOP2 に達したときの帯域クラス 2 のパケット破棄率を示す係数。実際の破棄率は、「2 の DROP2 乗」の逆数として求められる。たとえば、DROP2=0 なら破棄率は 100%、DROP2=1 なら 50%、DROP2=2 なら 25%、DROP2=3 なら 12.5%、DROP2=4 なら 6.25%となる。言い換えると、DROP2 が 0 のときは破棄率が 100%で、以後 DROP2 が 1 増えるたびに破棄率が半分になっていく。デフォルトは 1 ( 50% )。

**START3** 帯域クラス 3 のパケットを破棄し始めるポイント。キュー長 ( Kbyte ) で指定する。キュー長がこのポイントを超えると、帯域クラス 3 のパケット破棄率が徐々に高くなり、STOP3 に達したときに破棄率が DROP3 で指定された値となる。デフォルトは 5Kbyte。

**STOP3** 帯域クラス 3 のパケットを完全に破棄し始めるポイント。キュー長 ( Kbyte ) で指定する。キュー長がこのポイントを超えると、帯域クラス 3 のすべてのパケットが破棄されるようになる。デフォルトは 15Kbyte。なお、デフォルトの RED カーブセット「1」では、本パラメーターの値が、Tail-drop における帯域クラス 3 の最大キュー長としても使われる。

**DROP3** キュー長が STOP3 に達したときの帯域クラス 3 のパケット破棄率を示す係数。実際の破棄率は、「2 の DROP3 乗」の逆数として求められる。たとえば、DROP3=0 なら破棄率は 100%、DROP3=1 なら 50%、DROP3=2 なら 25%、DROP3=3 なら 12.5%、DROP3=4 なら 6.25%となる。言い換えると、DROP3 が 0 のときは破棄率が 100%で、以後 DROP3 が 1 増えるたびに破棄率が半分になっていく。デフォルトは 1 ( 50% )。

**DESCRIPTION** RED カーブセットの説明 ( メモとして使う )

## 関連コマンド

CREATE QOS RED ( 216 ページ )

DESTROY QOS RED ( 248 ページ )

SHOW QOS RED ( 474 ページ )

## SET QOS TRAFFICCLASS

カテゴリー：スイッチング / QoS

```
SET QOS TRAFFICCLASS=tc-list [DROPBWCLASS3={YES|NO}] [IGNOREBWCLASS={YES|NO}] [MAXBANDWIDTH={bandwidth|NONE}] [MAXBURSTSIZE=burstsize] [MINBANDWIDTH={bandwidth|NONE}] [MINBURSTSIZE=burstsize] [PREMARKING={USEMARKVALUE|USEDSCP|NONE}] [REMARKING={USEDSCPMAP|PRIORITY|PRIO+BWCLASS|BWCLASS|NONE}] [MARKVALUE={0..63|NONE}] [DESCRIPTION=string] [ACTION={FORWARD|DISCARD|SENDMIRROR|SENDVLANPORT|FORWARD,SENDMIRROR|SENDMIRROR,SENDVLANPORT}] [VLAN=1..4094] [PORT=port-number]
```

*tc-list*: トラフィッククラス番号 (0~1023。ハイフン、カンマを使った複数指定も可能)

*bandwidth*: 帯域幅 (1~16998400Kbps)

*burstsize*: バーストサイズ (0~268435455Byte)

*string*: 文字列 (1~15 文字。空白を含む場合はダブルクォートで囲む)

*port-number*: スイッチポート番号 (1~)

### 解説

トラフィッククラスの設定を変更する。

### パラメーター

**TRAFFICCLASS** トラフィッククラス番号

**DROPBWCLASS3** 本トラフィッククラスにおいて、最大帯域設定 (MAXBANDWIDTH と MAXBURSTSIZE) を上回るレートで受信したパケットをキューイング前に無条件で破棄するかどうか。YES を指定した場合、超過分のパケットは送信キューに格納される前に破棄される。NO を指定した場合、超過分のパケットは「帯域クラス 3 (使いすぎクラス)」に分類されるだけでただちには破棄されない。ただし、RED アルゴリズムの設定により、送信キューにおいて「帯域クラス 3」を優先的に破棄するような設定が可能。省略時は NO。

**IGNOREBWCLASS** 本トラフィッククラスに対して最大・最小帯域の設定 (MAXBANDWIDTH、MINBANDWIDTH) がなされている場合、メータリング時にプレマーキングで割り当てられた「帯域クラス」を考慮するか無視するかを指定する。YES を指定した場合、プレマーキング時に割り当てられた帯域クラスは無視され、実際の帯域使用量にのみ基づいて帯域クラスが決定される。NO を指定した場合は、プレマーキングで割り当てられた帯域クラスが、そのままメータリング結果として採用される。省略時は NO。

**MAXBANDWIDTH** トラフィッククラスに割り当てる最大帯域幅 (Kbps)。トラフィッククラスに割り当てる帯域は、原則としてここで指定した値までに制限される。数値だけで指定する場合の単位は Kbps。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「Kbps」、「Mbps」、「Gbps」の意味になる。「M」、「G」を指定する場合は、「2.256G」や「128.4M」のように小数を指定することもできる。QoS ポリシーを適用するスイッチポートの帯域と矛盾しないように設定すること。省略時

は NONE。

**MAXBURSTSIZE** トラフィッククラスの最大帯域幅設定 (MAXBANDWIDTH) に対する、最大許容バーストサイズ (Byte)。トラフィックの流入量が MAXBANDWIDTH を超えた場合に、MAXBANDWIDTH 超過分としてバッファリング可能な最大データ量を指定する。数値だけで指定する場合の単位は Byte。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「Kbyte」、「Mbyte」、「Gbyte」の意味になる。「K」、「M」、「G」を指定する場合は、「2.256G」や「128.4M」のように小数を指定することもできる。バーストサイズが MAXBURSTSIZE を上回った場合、超過分のパケットはキューイング前に破棄されるか (DROPBWCLASS3=YES のとき) 帯域クラス 3 に分類される (DROPBWCLASS3=NO のとき) 省略時は 0。

**MINBANDWIDTH** トラフィックに割り当てる最小帯域幅 (Kbps)。トラフィッククラスには、原則としてここで指定した帯域が確保される。数値だけで指定する場合の単位は Kbps。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「Kbps」、「Mbps」、「Gbps」の意味になる。「M」、「G」を指定する場合は、「2.256G」や「128.4M」のように小数を指定することもできる。QoS ポリシーを適用するスイッチポートの帯域と矛盾しないように設定すること。省略時は NONE。

**MINBURSTSIZE** トラフィッククラスの最小帯域幅設定 (MINBANDWIDTH) に対する、「帯域クラス 1」の最大許容バーストサイズ (Byte)。MINBANDWIDTH が NONE のときは、最大帯域幅設定 (MAXBANDWIDTH) に対する、「帯域クラス 2」の最大許容バーストサイズ (Byte)。数値だけで指定する場合の単位は Byte。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「Kbyte」、「Mbyte」、「Gbyte」の意味になる。「K」、「M」、「G」を指定する場合は、「2.256G」や「128.4M」のように小数を指定することもできる。MINBANDWIDTH が NONE のときは、MAXBURSTSIZE よりも小さい値でなくてはならない。詳細は解説編を参照。省略時は 0。

**PREMARKING** 本トラフィッククラスに対するプレマーキングの動作を指定する。具体的には、トラフィッククラスに割り当てる QoS パラメーターをプレマーキング用 DSCP MAP テーブルから検索するときに、どの値をインデックスとして使うかを指定する。USEMARKVALUE を指定した場合は、MARKVALUE パラメーターの値をインデックスとして使う。USEDSCP を指定した場合は、パケットの DSCP フィールド値をインデックスとして使う。いずれの場合も、DSCP MAP テーブルのもう 1 つのインデックスである帯域クラスは 1 を使う。NONE を指定した場合は、プレマーキングを行わずに、メータリングの処理に移る。省略時は NONE。なお、トラフィッククラスとフローグループの両方で本パラメーターが指定されている場合は、フローグループの設定が使われる。なお、IPv6 ルーティングパケットに対する QoS ポリシーでは、USEDSCP を使用できないので注意すること (指定しても効果がない)。

**REMARKING** 本トラフィッククラスに対するリマーキングの動作を指定する。具体的には、メータリング後の QoS パラメーター書き換え動作を何に基づいて実施するか、および、どのパラメーターを書き換えるかを指定する。USEDSCPMAP を指定した場合は、リマーキング直前の帯域クラスとパケットの DSCP 値をインデックスとしてリマーキング用 DSCP MAP テーブルを検索し、DSCP 値、帯域クラス、送信キュー、802.1p プライオリティー値を書き換える。PRIORITY、PRIO+BWCLASS を指定した場合は、リマーキング直前の送信キューと帯域クラスをインデックスとして QUEUE2PRIOMAP テーブルを検索し、802.1p プライオリティー値を書き換える。BWCLASS、NONE を指定した場合は書き換えを行わない。省略時は NONE。なお、PRIORITY と PRIO+BWCLASS、BWCLASS と NONE はそれぞれ同じ意味になる。また、IPv6 ルーティングパケットに対する QoS ポリシーでは、USEDSCPMAP を使用できないので注意すること (指定しても効果がない)。

**MARKVALUE** PREMARKING パラメーターに USEMARKVALUE を指定した場合、プレマーキング



用 DSCPMAP テーブルの検索インデックスとして使う DSCP 値を指定する。省略時は NONE

**DESCRIPTION** トラフィッククラスの説明（メモとして使う）。TRAFFICCLASS パラメーターに複数の番号を指定した場合は、すべてのトラフィッククラスに同じメモ文字列が設定される

**ACTION** 本トラフィッククラスに対するアクション。アクションの詳細は別表を参照のこと。アクションはフローグループとトラフィッククラスの両方に設定できるが、フローグループのアクションのほうが優先される（ただし、フローグループのアクションが NONE のときは、トラフィッククラスのアクションが実行される）。省略時は FORWARD

**VLAN** 本トラフィッククラスに属するパケットの出力先 VLAN。ACTION パラメーターに SENDVLAN-PORT を指定したときのみ有効かつ必須。本パラメーターは、必ず PORT パラメーターと組で指定すること。

**PORT** 本トラフィッククラスに属するパケットの出力先ポート。ACTION パラメーターに SENDVLAN-PORT を指定したときのみ有効かつ必須。本パラメーターは、必ず VLAN パラメーターと組で指定すること。

FORWARD	パケットを通常どおり出力する
DISCARD	パケットを破棄する
SENDVLANPORT	パケットの出力先を VLAN パラメーターと PORT パラメーターで指定されたポートに変更する。このとき、出力ポート（PORT）は出力 VLAN（VLAN）に所属していなくてはならないので、設定には注意すること
SENDMIRROR	パケットのコピーをミラーポートから出力する。あらかじめ、SET SWITCH MIRROR コマンドでミラーポートを指定し、ENABLE SWITCH MIRROR コマンドでポートミラーリング機能を有効にしておく必要がある
FORWARD,SENDMIRROR	FORWARD と SENDMIRROR の両方の処理を行う。SEND-MIRROR だけ指定した場合と同じ動作
SENDMIRROR,SENDVLANPORT	SENDMIRROR と SENDVLANPORT の両方の処理を行う

表 41: ACTION パラメーターに指定できるオプション

## 備考・注意事項

ACTION、VLAN、PORT パラメーターは、IPv6 アクセラレーター用の QoS ポリシーでは未サポート。

## 関連コマンド

ADD QOS TRAFFICCLASS ( 181 ページ )

CREATE QOS TRAFFICCLASS ( 218 ページ )

DELETE QOS TRAFFICCLASS ( 233 ページ )

DESTROY QOS TRAFFICCLASS ( 249 ページ )

SET QOS DSCPMAP ( 357 ページ )

SET QOS QUEUE2PRIOMAP ( 370 ページ )

SHOW QOS DSCPMAP ( 461 ページ )

SHOW QOS QUEUE2PRIOMAP ( 472 ページ )

SHOW QOS TRAFFICCLASS ( 477 ページ )



## SET STP

カテゴリー：スイッチング / スパニングツリープロトコル (STP/RSTP)

```
SET STP={stpname|ALL} [FORWARDDELAY=4..30] [HELLOTIME=1..10]
      [MAXAGE=6..40] [PRIORITY=0..65535] [MODE={STANDARD|RAPID}]
      [RSTPTYPE={NORMAL|STPCOMPATIBLE}] [DEFAULT]
```

*stpname*: STP ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

### 解説

STP ドメインのスパニングツリーパラメーターを変更する。

### パラメーター

**STP** STP ドメイン名。ALL を指定した場合はすべての STP ドメインが対象となる。

**FORWARDDELAY** フォワードディレイタイム。ルートブリッジのポートがフォワーディング状態に移するまでの時間を調整するためのパラメーター。MODE が STANDARD のときは、ルートブリッジ内のポートがリスニングからラーニング、ラーニングからフォワーディング状態に移するまでの時間 (秒) を示す。MODE が RAPID のときは、ディスカードイングからラーニング、ラーニングからフォワーディング状態に移するまでの最大時間 (秒) を示す。デフォルトは 15 秒。

**HELLOTIME** ハロータイム。ルートブリッジが BPDU (Bridge Protocol Data Unit) を送信する間隔 (秒)。デフォルトは 2 秒。

**MAXAGE** 最大エーゲタイム。ルートブリッジから BPDU が届かなくなったことを認識するまでの時間 (秒)。この時間内に BPDU を受信できなかった場合、STPD 内の各ブリッジはスパニングツリーの再構成を開始する。2 × (HELLOTIME + 1) 以上、かつ、2 × (FORWARDDELAY - 1) 以下でなくてはならない。デフォルトは 20 秒。

**PRIORITY** ブリッジプライオリティ。小さいほど優先度が高く、ルートブリッジになる可能性が高くなる。MODE が RAPID のときは 4096 の倍数で指定する (4096 の倍数でない値を指定したときは、指定値より小さい直近の倍数に変換される)。デフォルトは 32768。

**MODE** STP の動作モード。STANDARD (802.1d)、RAPID (802.1w) から選択する。動作モードを変更すると、STP のプロセスが初期化される。デフォルトは STANDARD。

**RSTPTYPE** Rapid STP (MODE=RAPID) の動作モード。NORMAL (RSTP BPDU を使う)、STPCOMPATIBLE (標準の BPDU を使う) から選択する。デフォルトは NORMAL。

**DEFAULT** FORWARDDELAY、HELLOTIME、MAXAGE、PRIORITY パラメーターをデフォルト値に戻したいときに指定する。STP 以外のパラメーターと同時に指定することはできない。

### 例

STP ドメイン「foobar」のパラメーターをデフォルト値に戻す。

SET STP=foobar DEFAULT

### 関連コマンド

PURGE STP ( 315 ページ )

RESET STP ( 321 ページ )

SET STP PORT ( 379 ページ )

SHOW STP ( 480 ページ )

## SET STP PORT

カテゴリー：スイッチング / スパニングツリープロトコル (STP/RSTP)

**SET STP** [= {*stpname*|ALL}] **PORT**={*port-list*|ALL} [PATHCOST={1..1000000|1..200000000}] [PORTPRIORITY=0..255] [EDGEPORT={YES|NO}] [PTP={AUTO|YES|NO}] [DEFAULT]

*stpname*: STP ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

*port-list*: スイッチポート番号 (1~)。ハイフン、カンマを使った複数指定も可能)

### 解説

指定ポートのスパニングツリーパラメーターを変更する。

### パラメーター

**STP** STP ドメイン名。ドメインを指定しなかった場合、および、ALL を指定した場合はすべての STP ドメインが対象となる。

**PORT** ポート番号。複数指定が可能。ALL を指定した場合はすべてのポートが対象となる。

**PATHCOST** パスコスト。該当ポートを通過する際のコストを示すもので、一般的にはポートの通信速度に応じて設定する。通信速度ごとのデフォルト値と推奨値範囲は別表を参照。なお、SET STP コマンドの MODE パラメーターで STP の動作モードを変更すると、PATHCOST も自動的に変更される。

**PORTPRIORITY** ポートプライオリティー。小さいほど優先度が高く、ルートポートになる可能性が高くなる。MODE が RAPID のときは 16 の倍数で指定する (16 の倍数でない値を指定したときは、指定値より小さい直近の倍数に変換される)。デフォルトは 128。

**EDGEPORT** MODE が RAPID のとき、該当ポートがエッジポートかどうかを指定する。エッジポートとは、他のブリッジが存在しない末端 (エッジ) の LAN に接続されているポートのこと。ただし、EDGEPORT=YES を指定した場合でも、同ポートで RSTP BPDU を受信した場合はエッジポートとしては扱われなくなる。デフォルトは NO。

**PTP** MODE が RAPID のとき、該当ポートが他のブリッジとポイントツーポイントで接続されているかどうかを指定する。AUTO を指定した場合は、本製品が自動判別する。デフォルトは AUTO。

**DEFAULT** PATHCOST、PORTPRIORITY パラメーターをデフォルト値に戻したいときに指定する。PORT 以外のパラメーターと同時に指定することはできない。

通信速度	推奨範囲	デフォルト値
10Mbps	50 ~ 600	100
100Mbps	10 ~ 60	19
1000Mbps	3 ~ 10	4

表 42: STANDARD モードにおけるパスコストの推奨範囲とデフォルト値

通信速度	推奨範囲	デフォルト値
10Mbps	200000 ~ 2000000	2000000
100Mbps	20000 ~ 200000	200000
1000Mbps	2000 ~ 20000	20000

表 43: RAPID モードにおけるバスコストの推奨範囲とデフォルト値

### 関連コマンド

PURGE STP ( 315 ページ )

RESET STP ( 321 ページ )

SET STP ( 377 ページ )

SHOW STP ( 480 ページ )

## SET SWITCH AGEINGTIMER

カテゴリー：スイッチング / フォワーディングデータベース

**SET SWITCH AGEINGTIMER=10..630**

### 解説

フォワーディングデータベース（FDB）のエージングタイム（MAC アドレス保持時間）を変更する。

### パラメーター

**AGEINGTIMER** エージングタイム。この時間内に受信されなかったダイナミックエントリは削除される。指定値が 10 の倍数でない場合は切り捨てが行われる（101 を指定した場合は 100 となる）。デフォルトは 300 秒。

### 関連コマンド

DISABLE SWITCH AGEINGTIMER (269 ページ)

ENABLE SWITCH AGEINGTIMER (299 ページ)

SHOW SWITCH (490 ページ)

## SET SWITCH CPUTXPRIORITY

カテゴリー：スイッチング / 一般コマンド

**SET SWITCH CPUTXPRIORITY={NONE|0..7}**

### 解説

スイッチ本体（CPU）発の packets にセットする 802.1p ユーザープライオリティ値を指定する。

### パラメーター

**CPUTXPRIORITY** CPU 発の packets にセットする 802.1p ユーザープライオリティ値。NONE は ユーザープライオリティ値をセットしないことを意味する。デフォルトは NONE。

### 関連コマンド

SET IP DSCPOVERRIDE（「IP」の 320 ページ）

SET SWITCH CPUTXQUEUE（383 ページ）

SHOW SWITCH（490 ページ）

## SET SWITCH CPUTXQUEUE

カテゴリー：スイッチング / 一般コマンド

**SET SWITCH CPUTXQUEUE={NONE|0..7}**

### 解説

スイッチ本体（CPU）発のパケットを格納する出力キューを指定する。

### パラメーター

**CPUTXQUEUE** CPU 発のパケットを格納する出力キュー番号。NONE はキュー 0 を意味する。デフォルトは NONE。

### 関連コマンド

SET IP DSCPOVERRIDE（「IP」の 320 ページ）

SET SWITCH CPUTXPRIORITY（382 ページ）

SHOW SWITCH（490 ページ）

## SET SWITCH DLFLIMIT

カテゴリー：スイッチング / 一般コマンド

**SET SWITCH DLFLIMIT={NONE|100..95300}**

### 解説

未学習ユニキャストパケットの受信レート制限値を設定する。

### パラメーター

**DLFLIMIT** 未学習ユニキャストパケットの受信上限値。1 秒間の最大受信レート（Kbyte/秒）を指定する。ただし、指定値が 100 の倍数でない場合は切り上げが行われる（101 を指定した場合は 200 となる）。上限を超えて受信したパケットは破棄される。NONE を指定した場合は、制限なしとなる。デフォルトは NONE。本パラメーターはシステム全体に適用される。

### 関連コマンド

SHOW SWITCH (490 ページ)



## SET SWITCH MIRROR

カテゴリー：スイッチング / ポート

**SET SWITCH MIRROR**={**NONE**|*port-number*}

*port-number*: スイッチポート番号 (1～)

### 解説

ミラーポートの設定および解除を行う。

ソースポートと対象トラフィックは、SET SWITCH PORT コマンドの MIRROR パラメーターで指定する。

### パラメーター

**MIRROR** ミラーポートとして使用するポートを指定する。VLAN default 以外に所属しているポートはミラーポートに設定できない。また、トランクポートも不可。本コマンド実行時に別のポートがミラーポートとして設定されていた場合、先に設定されていたポートはミラーポートでなくなり、VLAN default 所属のタグなしポートとなる。ミラーポートになったポートは、どの VLAN にも所属しない。ミラーポートを削除するには NONE を指定する。

### 備考・注意事項

ミラーポートとして設定されたポートは通常のスイッチポートとしては機能しない。また、ポートトランキングの所属ポートをミラーポートに設定することはできない。

### 関連コマンド

DISABLE SWITCH MIRROR (273 ページ)

ENABLE SWITCH MIRROR (303 ページ)

SET SWITCH PORT (387 ページ)

SHOW SWITCH (490 ページ)

SHOW SWITCH PORT (509 ページ)

## SET SWITCH NESTEDTPID

カテゴリー：スイッチング / バーチャル LAN

**SET SWITCH NESTEDTPID=*protocoltype***

*protocoltype*: プロトコル番号 (16 進数 4 桁)

### 解説

ダブルタグ VLAN (Nested VLAN) のコアポートで使用する外側タグの TPID (Tag Protocol Identifier = プロトコルタイプ値) を指定する。

本コマンドで設定した値は、すべてのダブルタグ VLAN (Nested VLAN) で使用される。

### パラメーター

**NESTEDTPID** 外側タグの TPID (プロトコルタイプ値)。 「88ff」のように 16 進数 4 桁で指定する。デフォルトは 8100 (16 進)。

### 関連コマンド

ADD VLAN PORT (191 ページ)

CREATE VLAN (225 ページ)

SHOW SWITCH (490 ページ)

## SET SWITCH PORT

カテゴリー：スイッチング / ポート

```
SET SWITCH PORT={port-list|ALL} [ACCEPTABLE={ALL|VLAN}] [BCLIMIT={NONE|
100..95300}] [DESCRIPTION=string] [EGRESSLIMIT={NONE|bandwidth}]
[INFILTERING={OFF|ON}] [INTRUSIONACTION={DISABLE|DISCARD|TRAP}]
[LEARN={0|1..256}] [RELEARN={ON|OFF}] [MIRROR={BOTH|NONE|RX|TX}]
[MODE={AUTONEGOTIATE|MASTER|SLAVE}] [POLARITY={MDI|MDIX}]
[SPEED={AUTONEGOTIATE|10MHALF|10MFULL|100MHALF|100MFULL|1000MFULL}]
[IGMPACTION={DENY|REPLACE}] [IGMPFILTER={NONE|filter-id}]
[IGMPMAXGROUP={NONE|1..65535}] [THRASHACTION={NONE|LEARNDISABLE|
PORTDISABLE|VLANDISABLE|LINKDOWN}] [THRASHTIMEOUT={NONE|1..86400}]
[VLANSTATUSTRAP={ON|OFF}]
```

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

*string*: 文字列 (1～47文字)

*bandwidth*: 帯域幅 (0～2641248Kbps)

*filter-id*: フィルター番号 (1～99)

### 解説

スイッチポートの各種設定を行う。

### パラメーター

**PORT** ポート番号。複数指定が可能。ALL を指定した場合はすべてのポートが対象となる。

**ACCEPTABLE** 受信可能なフレームタイプ。VLAN (VLAN タグ付きフレームのみ。VID=0 のプライオリティータグフレームは破棄) か ALL (すべて) から選択する。タグなし VLAN 所属ポートのデフォルトは ALL。タグ VLAN にしか所属していないポートでは、自動的に本パラメーターが VLAN に設定され変更できない。

**BCLIMIT** ブロードキャストおよびマルチキャストパケットの受信上限値。1 秒間の最大受信レート (Kbyte/秒) を指定する。ただし、指定値が 100 の倍数でない場合は切り上げが行われる (101 を指定した場合は 200 となる)。上限を超えて受信したパケットは破棄される。NONE を指定した場合は、制限なしとなる。デフォルトは NONE。なお、マルチキャストパケットの受信レートを制限するには、本パラメーターで上限値を指定するだけでなく、ENABLE SWITCH MCLIMITING コマンドを実行する必要もある。

**DESCRIPTION** ポート名称。SHOW SWITCH PORT コマンドなどで表示されるもので、メモ的に使用する。

**EGRESSLIMIT** 該当ポートの送信レート上限値 (帯域制限機能)。指定可能な値の範囲は 0～2641248Kbps。ただし、指定値が 648 の倍数でない場合は倍数になるよう丸められる。NONE および 0 は帯域を制限しないの意味になる。EGRESSLIMIT の値は、パケットをスイッチ内部のキューから送り出すとき

のデータレートであり、フレームヘッダーやトレーラーは含まない。デフォルトは NONE。

**INFILTERING** イングレスフィルタリングを行うかどうか。ON ( 行う ) が OFF ( 行わない ) を指定する。

ON のときは、受信フレームの VLAN ID が受信ポートの所属 VLAN と一致した場合のみフレームを受け入れ、それ以外は破棄する。OFF の場合はすべてのフレームを受け入れる。デフォルトは OFF。

**INTRUSIONACTION** 未学習の送信元 MAC アドレスを持つパケットを、LEARN パラメーターで指定した制限値を超えて受信した場合のアクション。DISCARD ( 受信パケットを破棄する ) TRAP ( 受信パケットを破棄した後、SNMP トラップを送信する。トラップは各 MAC アドレスに対して最初の一回だけ送信 ) DISABLE ( 受信パケットを破棄し、SNMP トラップを送信した後、ポートをディセーブルにする ) から選択する。デフォルトは DISCARD。

**LEARN** 該当ポートで学習可能な送信元 MAC アドレス ( ダイナミックエントリー ) の最大数。0 を指定した場合は無制限となる ( ポートセキュリティをオフにする )。すでに学習済み MAC アドレスが制限値に達している状態で未知の送信元 MAC アドレスを持つパケットを受信した場合、INTRUSIONACTION パラメーターの設定に基づいた処理が行われる。デフォルトは 0 ( ポートセキュリティオフ )

**RELEARN** ポートセキュリティの動作モード。OFF を指定した場合、ポートセキュリティエントリー ( Learn エントリー ) はエージアウトされない。ON を指定した場合は、Learn エントリーもエージアウトされる ( ダイナミックポートセキュリティ )。本パラメーターは、ポートセキュリティが有効でないとき ( LEARN=0 のとき ) は意味を持たない。デフォルトは OFF。

**MIRROR** ミラーリングするトラフィックの向き。該当ポートをポートミラーリングのソースポートにしたいときに指定する。BOTH ( 送受信パケット ) RX ( 受信パケット ) TX ( 送信パケット ) NONE ( ミラーリングしない ) から選択する。デフォルトは NONE。

**MODE** 1000BASE-T ポートのマスター/スレーブ。デフォルトは AUTONEGOTIATE。

**POLARITY** MDI/MDI-X 自動切替オフ時の MDI/MDI-X を指定する。デフォルトは MDI-X。本パラメーターは、MDI/MDI-X 自動切替がオン ( デフォルト ) のときには変更できない。

**SPEED** ポートの通信速度とデュプレックスモードを設定する ( 別表を参照 )。トランクグループ所属ポートに対して本コマンドで SPEED オプションを変更した場合、ポートレベルの設定値は変更されるが、実際の値はトランクグループ全体の設定値のまま変化しない。同ポートをトランクグループから除外した時点で設定値が有効になる。また、1000BASE-T 以外の SFP ポートは AUTONEGOTIATE による 1000M 通信のみサポート。1000BASE-T の SFP ポートは 1000MFULL 設定もサポートするが、通信速度は他の SFP と同じく 1000M のみサポートとなる ( 9924T/4SP は 1000BASE-T の SFP をサポートしていないので注意 )。デフォルトは AUTONEGOTIATE ( オートネゴシエーション )。なお、AUTONEGOTIATE から AUTONEGOTIATE 以外に設定を変更すると、該当ポートでは MDI/MDI-X 自動切替が無効になる。また、AUTONEGOTIATE 以外から AUTONEGOTIATE に設定を変更すると、MDI/MDI-X 自動切替が有効になる。

**IGMPACTION** 該当ポート配下から Join されたマルチキャストグループの数が IGMPMAXGROUP パラメーターで設定した最大数に達した場合の動作。DENY ( それ以降の Join を拒否 ) と REPLACE ( タイマーの残り時間がもっとも少ないエントリーを削除して新しいエントリーを登録 ) から選択する。デフォルトは DENY。

**IGMPFILTER** 該当スイッチポートに適用する IGMP フィルターの番号 ( 1 ~ 99 )。適用を解除するときは NONE を指定する。デフォルトは NONE。

**IGMPMAXGROUP** 該当ポート配下から Join できるマルチキャストグループの最大数。制限を解除するときは NONE を指定する。デフォルトは NONE ( 制限なし )。

**THRASHACTION** 該当スイッチポートでMACアドレススラッシング(同一MACアドレスの登録ポートが頻繁に変更されること)を検出した場合の動作。NONE(なにもしない)、LEARNDISABLE(MACアドレスの学習を停止する)、PORTDISABLE(ポートをディセーブルにする)、VLANDISABLE(スラッシングが発生したVLANに対してのみポートをディセーブルにする)、LINKDOWN(ポートを物理的にリンクダウンさせる)から選択する。これらの動作は、THRASHTIMEOUTパラメーターで指定した時間が経過すると終了する(通常のポート動作に戻る)。ただし、PORTDISABLE、LINKDOWNの場合は、ENABLE SWITCH PORT コマンドにより手動で動作を終了させられる。また、VLANDISABLEの場合は、ENABLE SWITCH PORT VLAN コマンドにより手動で動作を終了させられる。デフォルトはLEARNDISABLE。

**THRASHTIMEOUT** MACアドレススラッシング検出時の動作の持続時間(秒)。NONEは無期限を示す。THRASHACTIONパラメーターにLEARNDISABLEを指定している場合、本パラメーターをNONEに変更することはできない。また、本パラメーターをNONEに設定している状態で、THRASHACTIONパラメーターの値をLEARNDISABLEに変更した場合、本パラメーターの値は自動的に1に変更される。デフォルトは1秒。

**VLANSTATUSTRAP** 特定VLANにおけるポートステータス(イネーブル、ディセーブル)が変化した場合に、SNMPトラップを送信するかどうか。デフォルトはOFF。

AUTONEGOTIATE	オートネゴシエーション
10MHALF	10M Half Duplex 固定(本体の1000BASE-Tポートのみ)
10MFULL	10M Full Duplex 固定(本体の1000BASE-Tポートのみ)
100MHALF	100M Half Duplex 固定(本体の1000BASE-Tポートのみ)
100MFULL	100M Full Duplex 固定(本体の1000BASE-Tポートのみ)
1000MFULL	1000M Full Duplex 固定(本体と1000BASE-T SFP上の1000BASE-Tポートのみ。なお、9924T/4SPは1000BASE-T SFPをサポートしていないので注意)

表 44: SPEEDパラメーターの設定

## 備考・注意事項

帯域制限機能(EGRESSLIMIT)とQoSの重み付きラウンドロビン(WRR)スケジューリング(SET QOS PORT EGRESSQUEUE コマンドのSCHEDULERパラメーターで設定)は併用できない。

THRASHACTIONパラメーターの値をVLANDISABLEに変更すると、該当ポートで自動的にイングレスフィルタリング(SET SWITCH PORT コマンドのINFILTERINGパラメーター)が有効になる。また、VLANDISABLEからそれ以外に変更すると、イングレスフィルタリングが無効になる。

## 関連コマンド

ADD IGMP FILTER (「IP マルチキャスト」の27ページ)

CREATE IGMP FILTER (「IP マルチキャスト」の35ページ)

DISABLE SWITCH PORT (274ページ)

DISABLE SWITCH PORT VLAN (278ページ)

ENABLE SWITCH PORT ( 304 ページ )

ENABLE SWITCH PORT VLAN ( 308 ページ )

SET SWITCH THRASHLIMIT ( 391 ページ )

SHOW IGMP FILTER (「IP マルチキャスト」の 86 ページ)

SHOW SWITCH PORT ( 509 ページ )

## SET SWITCH THRASHLIMIT

カテゴリー：スイッチング / 一般コマンド

**SET SWITCH THRASHLIMIT=5..255**

### 解説

MAC アドレススラッシング（同一 MAC アドレスの登録ポートが頻繁に変更されること）の検出しきい値を設定する。

### パラメーター

**THRASHLIMIT** MAC アドレススラッシングの検出しきい値。同一の MAC アドレスが 1 秒間に本パラメーターで指定した回数ポート間を移動すると、本製品は MAC アドレススラッシングが発生したと見なし、関連するポートにおいて、SET SWITCH PORT コマンド、CREATE SWITCH TRUNK コマンド、SET SWITCH TRUNK コマンド、SET LACP コマンドの THRASHACTION パラメーターで指定された動作を実行する。デフォルトは 10。

### 関連コマンド

CREATE SWITCH TRUNK ( 223 ページ )

DISABLE SWITCH PORT VLAN ( 278 ページ )

ENABLE SWITCH PORT VLAN ( 308 ページ )

SET LACP ( 336 ページ )

SET SWITCH PORT ( 387 ページ )

SET SWITCH TRUNK ( 392 ページ )

SHOW LACP ( 417 ページ )

SHOW SWITCH ( 490 ページ )

SHOW SWITCH PORT ( 509 ページ )

SHOW SWITCH TRUNK ( 517 ページ )

## SET SWITCH TRUNK

カテゴリー：スイッチング / ポート

```
SET SWITCH TRUNK=trunk [SPEED={10M|100M|1000M}] [THRASHACTION={NONE|
LEARNDISABLE|PORTDISABLE|VLANDISABLE|LINKDOWN}] [THRASHTIMEOUT={NONE|
1..86400}]
```

**trunk**: トランクグループ名 (1~15 文字。英数字とアンダースコア ( - )、ハイフンを使用可能。大文字小文字を区別しない)

### 解説

トランクグループの設定を変更する。

### パラメーター

**TRUNK** トランクグループ名

**SPEED** トランクポートの通信速度。トランクグループに参加したポートは、ここで指定した速度のオートネゴシエーション (AUTONEGOTIATE) となる

**THRASHACTION** 該当トランクグループで MAC アドレススラッシング (同一 MAC アドレスの登録ポートが頻繁に変更されること) を検出した場合の動作。NONE (なにもしない)、LEARNDISABLE (トランクグループ内の全ポートで MAC アドレスの学習を停止する)、PORTDISABLE (トランクグループ内の全ポートをディセーブルにする)、VLANDISABLE (スラッシングが発生した VLAN に対してのみトランクグループ内の全ポートをディセーブルにする)、LINKDOWN (トランクグループ内の全ポートを物理的にリンクダウンさせる) から選択する。これらの動作は、THRASHTIMEOUT パラメーターで指定した時間が経過すると終了する (通常のポート動作に戻る)。ただし、PORTDISABLE、LINKDOWN の場合は、ENABLE SWITCH PORT コマンドにより手動で動作を終了させられる。また、VLANDISABLE の場合は、ENABLE SWITCH PORT VLAN コマンドにより手動で動作を終了させられる。デフォルトは LEARNDISABLE。

**THRASHTIMEOUT** MAC アドレススラッシング検出時の動作の持続時間 (秒)。NONE は無期限を示す。THRASHACTION パラメーターに LEARNDISABLE を指定している場合、本パラメーターを NONE に変更することはできない。また、本パラメーターを NONE に設定している状態で、THRASHACTION パラメーターの値を LEARNDISABLE に変更した場合、本パラメーターの値は自動的に 1 に変更される。デフォルトは 1 秒。

### 備考・注意事項

THRASHACTION パラメーターの値を VLANDISABLE に変更すると、トランクグループ内の全ポートで自動的にイングレスフィルタリング (SET SWITCH PORT コマンドの INFILTERING パラメーター) が有効になる。また、VLANDISABLE からそれ以外に変更すると、イングレスフィルタリングが無効になる。



関連コマンド

ADD SWITCH TRUNK ( 190 ページ )  
CREATE SWITCH TRUNK ( 223 ページ )  
DELETE SWITCH TRUNK ( 238 ページ )  
DESTROY SWITCH TRUNK ( 251 ページ )  
SET SWITCH THRASHLIMIT ( 391 ページ )  
SHOW SWITCH TRUNK ( 517 ページ )

## SET VLAN PORT

カテゴリー：スイッチング / バーチャル LAN

**SET VLAN**={*vlannname*|1..4094} **PORT**={*port-list*|ALL} **FRAME**={UNTAGGED|TAGGED}

*vlannname*: VLAN 名 (1~32 文字。英数字とアンダースコア ( \_ ) ハイフンを使用可能。大文字小文字は区別しない)

*port-list*: スイッチポート番号 (1~。ハイフン、カンマを使った複数指定も可能)

### 解説

VLAN 所属ポートのタグ付き・タグなし設定を変更する。

### パラメーター

**VLAN** VLAN 名または VLAN ID

**PORT** ポート番号

**FRAME** 該当 VLAN のタグ設定。TAGGED (タグ付き) 、 UNTAGGED (タグなし) から選択する。

### 関連コマンド

ADD VLAN PORT ( 191 ページ )

DELETE VLAN PORT ( 239 ページ )

SHOW VLAN ( 519 ページ )

## SHOW CLASSIFIER

カテゴリー：スイッチング / クラシファイア

```
SHOW CLASSIFIER [= {rule-list | ALL}] [ETHFORMAT={ETHII-TAGGED|
ETHII-UNTAGGED|ANY}] [PROTOCOL={protocoltype | IP | IPV6 | ANY}]
[MACTYPE={L2UCAST|L2MCAST|L2BCAST|ANY}] [MACSADDR={macadd | DHCP Snooping |
ANY}] [MACDADDR={macadd | ANY}] [VLAN={vlanname | 1..4094 | ANY}]
[IPSADDR={ipadd [/masklen] | ip6add /plen | DHCP Snooping | ANY}]
[IPDADDR={ipadd [/masklen] | ip6add /plen | ANY}] [IPDSCP={dscp-list | ANY}]
[IPTOS={0..7 | ANY}] [IPPROTOCOL={TCP|UDP|ICMP|IGMP|protocol | ANY}]
[TCPSPORT={port | port-range | ANY}] [TCPDPORT={port | port-range | ANY}]
[TCPFLAGS={ {URG|ACK|RST|SYN|FIN} [, ...] | ANY}] [UDPSPORT={port | port-range |
ANY}] [UDPDPOR={port | port-range | ANY}]
[L5BYTE01=byteoffset, bytevalue [, bytemask]]
[L5BYTE02=byteoffset, bytevalue [, bytemask]]
[L5BYTE03=byteoffset, bytevalue [, bytemask]]
[L5BYTE04=byteoffset, bytevalue [, bytemask]]
[L5BYTE05=byteoffset, bytevalue [, bytemask]]
[L5BYTE06=byteoffset, bytevalue [, bytemask]]
[L5BYTE07=byteoffset, bytevalue [, bytemask]]
[L5BYTE08=byteoffset, bytevalue [, bytemask]]
[L5BYTE09=byteoffset, bytevalue [, bytemask]]
[L5BYTE10=byteoffset, bytevalue [, bytemask]]
[L5BYTE11=byteoffset, bytevalue [, bytemask]]
[L5BYTE12=byteoffset, bytevalue [, bytemask]]
[L5BYTE13=byteoffset, bytevalue [, bytemask]]
[L5BYTE14=byteoffset, bytevalue [, bytemask]]
[L5BYTE15=byteoffset, bytevalue [, bytemask]]
[L5BYTE16=byteoffset, bytevalue [, bytemask]]
```

*rule-list*: クラシファイア番号 (1~9999)。ハイフン、カンマを使った複数指定も可能)

*macadd*: MAC アドレス (xx-xx-xx-xx-xx-xx の形式)

*protocoltype*: L3 プロトコル (Ethernet) 番号 (16 進数)

*vlanname*: VLAN 名 (1~32 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字は区別しない)

*ipadd*: IP アドレス

*masklen*: マスク長 (0~32)

*dscp-list*: DSCP 値 (0~63)。ハイフン、カンマを使った複数指定も可能)

*protocol*: IP プロトコル番号 (1~255)

*port*: TCP/UDP ポート番号 (0~65535)

*port-range*: TCP/UDP ポート番号範囲 (「1-99」のように 2 つの番号をハイフンで区切って指定する。有効範囲は 0~65535)

*ip6add*: IPv6 アドレス

*plen*: プレフィックス長 (0~128 ビット)

**byteoffset:** データ部の先頭バイト (TCP・UDP ヘッダーの直後のバイト) を 0 として数えたオフセット (10 進数。0 ~ 37)

**bytevalue:** byteoffset で指定したバイトの内容 (16 進数。00 ~ ff)

**bytemask:** bytevalue に対する AND マスク (16 進数。省略時は ff)

## 解説

クラシファイア (汎用パケットフィルター) の設定内容を表示する。

## パラメーター

**CLASSIFIER** クラシファイア番号。番号を指定した場合は該当するクラシファイアのパラメーターがすべて表示される。ALL を指定した場合はすべてのクラシファイアのパラメーターが表示される。値を指定しなかった場合は、クラシファイアの一覧が簡潔に表示される。本パラメーターになんらかの値を指定した場合は、以下の各パラメーターを使って表示するクラシファイアの絞り込みが可能。本パラメーターに値を指定しなかった場合は、以下の各パラメーターは無効

**ETHFORMAT** Ethernet のフレームフォーマット (エンキャプセレーション)

**PROTOCOL** レイヤー 3 プロトコルタイプフィールド値

**MACTYPE** レイヤー 2 アドレス種別

**MACSADDR** 送信元 MAC アドレス

**MACDADDR** 宛先 MAC アドレス

**VLAN** 入力 VLAN (ただし、IPv6 ポリシーベース QoS では出力 VLAN)

**IPSADDR** 始点 IPv4/IPv6 アドレス

**IPDADDR** 終点 IPv4/IPv6 アドレス

**IPDSCP** IPv4/IPv6 ヘッダーの DSCP (DiffServ Code Point) フィールド値

**IPTOS** IPv4 ヘッダーの TOS 優先度 (precedence) フィールド値

**IPPROTOCOL** IPv4/IPv6 ヘッダーのプロトコルタイプ (IPv4) / 次ヘッダー (IPv6) フィールド値

**TCPSPORT** TCP 始点ポート

**TCPDPORT** TCP 終点ポート

**TCPFLAGS** TCP 制御フラグ

**UDPSPORT** UDP 始点ポート

**UDPDPORT** UDP 終点ポート

**L5BYTE01 ~ L5BYTE16** TCP/UDP パケットのデータ部の値

## 入力・出力・画面例

```
Manager > show classifier

Classifier General Info
-----
Total number of rules .... 7

Rule ..... 1000
```

```

    Related module(s) ..... L3 switch

Rule ..... 1010
    Related module(s) ..... L3 switch

Rule ..... 1020
    Related module(s) ..... None

Rule ..... 2000
    Related module(s) ..... SWNP

Rule ..... 2010
    Related module(s) ..... SWNP

Rule ..... 3000
    Related module(s) ..... QOS

Rule ..... 3010
    Related module(s) ..... QOS

```

-----

Manager > show classifier=1000

#### Classifier Rules

-----

```

Rule ..... 1000
D-MAC Address ..... ANY
S-MAC Address ..... ANY
M-Type ..... ANY
VLAN ..... ANY
E-Format ..... ANY
Protocol ..... IP
S-IP Address ..... 172.17.28.0/24
D-IP Address ..... 172.17.28.0/24
IP Protocol ..... ANY
TOS/DSCP ..... ANY
Layer 5 Byte 01:
    Offset ..... 8
    Value ..... 16
    Mask ..... 24

```

-----

Manager > show classifier=1010

#### Classifier Rules

-----

```

Rule ..... 1010
D-MAC Address ..... ANY
S-MAC Address ..... ANY

```

```

M-Type ..... ANY
VLAN ..... ANY
E-Format ..... ANY
Protocol ..... IP
S-IP Address ..... 172.17.28.0/24
D-IP Address ..... ANY
IP Protocol ..... ANY
TOS/DSCP ..... ANY

```

```

Manager > show classifier=2000

```

#### Classifier Rules

```

Rule ..... 2003
D-MAC Address ..... ANY
S-MAC Address ..... ANY
M-Type ..... ANY
VLAN ..... ANY
E-Format ..... ETHII-TAGGED
Protocol ..... 86DD (IPV6 ETHII)
S-IP Address ..... 3ffe:0b80::0001/128
D-IP Address ..... ANY
IP Protocol ..... ANY

```

Total number of rules	クラシファイアの総数
Rule	クラシファイア番号
Related module(s)	クラシファイアを使用している上位モジュール。L3 switch (ハードウェアパケットフィルタ)、QOS (ポリシーベース QoS)、SWNP (IPv6 ハードウェアパケットフィルタ)、None (モジュールに関連付けられていない)

表 45: パラメーター無指定時

Rule	クラシファイア番号
D-MAC Address	宛先 MAC アドレス
S-MAC Address	送信元 MAC アドレス
M-Type	レイヤー 2 アドレス種別
VLAN	入力 VLAN (ただし、IPv6 ポリシーベース QoS では出力 VLAN)。カッコ内は VLAN ID
E-Format	レイヤー 2 フレームタイプ (エンキャプセレーション)
Protocol	プロトコルタイプ。カッコ内は定義済みのプロトコル名
TPID	TPID (Tag Protocol Identifier)

VLAN Priority	802.1p ユーザープライオリティ
Inner TPID	ダブルタグパケットにおける内側 802.1Q VLAN タグヘッダーの TPID ( Tag Protocol Identifier )
Inner VLAN Priority	ダブルタグパケットにおける内側 802.1Q VLAN タグヘッダーの 802.1p ユーザープライオリティ
Inner VLAN ID	ダブルタグパケットにおける内側 802.1Q VLAN タグヘッダーの VLAN ID
S-IP Address	始点 IP アドレス/マスクまたは始点 IPv6 アドレス/プレフィックス長
D-IP Address	終点 IP アドレス/マスクまたは終点 IPv6 アドレス/プレフィックス長
IP Protocol	IP プロトコルタイプ
TOS/DSCP	TOS または DSCP 値
S-TCP Port	TCP 始点ポート
D-TCP Port	TCP 終点ポート
S-TCP Mask	TCP 始点ポートに対する AND マスク
D-TCP Mask	TCP 終点ポートに対する AND マスク
TCP Flags	TCP 制御フラグ
S-UDP Port	UDP 始点ポート
D-UDP Port	UDP 終点ポート
S-UDP Mask	UDP 始点ポートに対する AND マスク
D-UDP Mask	UDP 終点ポートに対する AND マスク
Layer 5 Byte 01 ~ Layer 5 Byte 16	L5BYTE01 ~ L5BYTE16 パラメーターの設定内容
Offset	データ部の先頭バイト ( TCP・UDP ヘッダーの直後のバイト ) を 0 として数えたオフセット ( 10 進数 )
Value	Offset で指定されたバイトの内容 ( 16 進数 )
Mask	Value に対する AND マスク ( 16 進数 )

表 46: CLASSIFIER パラメーター指定時 ( 表示項目はクラシファイアの設定により異なる )

## 例

クラシファイアの一覧を表示する。

```
SHOW CLASSIFIER
```

IP プロトコルとして UDP を含むクラシファイアの詳細を表示する。

```
SHOW CLASSIFIER=ALL IPPROTOCOL=UDP
```

関連コマンド

CREATE CLASSIFIER ( 198 ページ )

DESTROY CLASSIFIER ( 243 ページ )

SET CLASSIFIER ( 325 ページ )



SHOW DHCP Snooping

カテゴリー：スイッチング / DHCP Snooping

SHOW DHCP Snooping

解説

DHCP Snooping の全般的な設定情報を表示する。

入力・出力・画面例

```
Manager > show dhcp Snooping

DHCP Snooping Information
-----
DHCP Snooping ..... Enabled
Option 82 status ..... Enabled
Ip Filtering ..... Enabled
ARP security ..... Enabled
Strict Unicast ..... Disabled
Logging enabled ..... None
XLA ..... Disabled
Debug enabled ..... None

DHCP Snooping Database:
Full Leases/Max Leases ... 2/26
Check Interval ..... 60 seconds
-----
```

DHCP Snooping	DHCP Snooping の有効・無効
Option 82 status	リレーエージェント情報オプション（オプションコード 82）の付加・検査・削除機能の有効・無効
Ip Filtering	未サポート
ARP security	ARP セキュリティー機能の有効・無効
Strict Unicast	未サポート
Logging enabled	ログ機能の有効・無効。無効時は None、有効時はログへの記録対象イベント（現時点では ArpSecurity のみ）が表示される
XLA	未サポート
Debug enabled	未サポート
Full Leases/Max Leases	DHCP Snooping テーブル（バインディングデータベース）に現在登録されているクライアントの数 / 登録可能なクライアントの総数

Check Interval	バインディングデータベースのチェック間隔
----------------	----------------------

表 47:

関連コマンド

- ENABLE DHCP Snooping ( 280 ページ )
- ENABLE DHCP Snooping ARPSECURITY ( 281 ページ )
- ENABLE DHCP Snooping LOG ( 282 ページ )
- ENABLE DHCP Snooping OPTION82 ( 283 ページ )
- SET DHCP Snooping CHECKINTERVAL ( 329 ページ )
- SET DHCP Snooping PORT ( 330 ページ )

## SHOW DHCP Snooping COUNTER

カテゴリー：スイッチング / DHCP Snooping

### SHOW DHCP Snooping COUNTER

#### 解説

DHCP Snooping の統計情報を表示する。

#### 入力・出力・画面例

```
Manager > show dhcp Snooping counter
```

```
DHCP Snooping Counters
```

```
DHCP Snooping
```

```
InPackets ..... 16
InBootpRequests ..... 14
InBootpReplies ..... 2
InDiscards ..... 0
```

```
ARP Security
```

```
InPackets ..... 6
InDiscards ..... 3
NoLease ..... 3
Invalid ..... 0
```

DHCP Snooping セクション	
InPackets	受信した DHCP/BOOTP パケットの総数
InBootpRequests	受信した DHCP/BOOTP 要求パケットの数
InBootpReplies	受信した DHCP/BOOTP 応答パケットの数
InDiscards	受信後破棄した DHCP/BOOTP パケットの数
ARP Security セクション	
InPackets	受信した ARP パケットの総数
InDiscards	受信後破棄した ARP パケットの総数
NoLease	上記「受信後破棄した ARP パケットの総数」のうち、DHCP Snooping テーブル（バインディングデータベース）未登録のため破棄したものの数

Invalid	上記「受信後破棄した ARP パケットの総数」のうち、パケットフォーマット不正のため破棄したもの数
---------	---

表 48:

関連コマンド

- ENABLE DHCP Snooping ( 280 ページ )
- ENABLE DHCP Snooping ARP Security ( 281 ページ )
- RESET DHCP Snooping Counter ( 316 ページ )

## SHOW DHCP SNOOPING DATABASE

カテゴリー：スイッチング / DHCP Snooping

### SHOW DHCP SNOOPING DATABASE

#### 解説

DHCP Snooping テーブル ( バインディングデータベース ) の内容を表示する。

#### 入力・出力・画面例

```

Manager > show dhcp snooping database

DHCP Snooping Binding Database
-----
Full Leases/Max Leases ... 2/26
Check Interval ..... 60 seconds
Database Listeners ..... CLASSIFIER

Current valid entries
MAC Address          IP Address          Expires(s)  VLAN  Port        ID        Source
Router list
-----
00-00-00-00-00-01   192.168.10.5        Static      1      5           4         User
-
00-0a-79-34-06-12   192.168.10.200      2231        1     11           1        Dynamic
192.168.10.254
-----

Entries with client lease but no listeners
MAC Address          IP Address          Expires(s)  VLAN  Port        ID        Source
-----
None...
-----

Entries with no client lease and no listeners
MAC Address          IP Address          Expires(s)  VLAN  Port        ID        Source
-----
None...
-----

```

Full Leases/Max Leases

バインディングデータベースに現在登録されているクライアントの数 / 登録可能なクライアントの総数

Check Interval	バインディングデータベースのチェック間隔
Database Listeners	バインディングデータベースを利用しているソフトウェアモジュール名
Current valid entries セクション	現在有効なクライアントの登録情報が MAC アドレスの昇順で表示される
Entries with client lease but no listeners セクション	DHCP サーバーからの DHCP ACK パケットが DHCP クライアントに転送されたが、該当する Listener (CLASSIFIER) が存在しない、もしくは CLASSIFIER モジュールに何らかの問題が発生したためそれが利用できない場合に、クライアントの登録情報が表示される
Entries with no client lease and no listeners セクション	DHCP メッセージに問題があったなどの理由で、DHCP サーバーからの DHCP ACK パケットが DHCP クライアントに転送されなかった場合に、クライアントの登録情報が表示される
MAC Address	クライアントの MAC アドレス
IP Address	クライアントの IP アドレス
Expires(s)	該当エントリーの残り有効時間 (秒) (IP アドレス使用期限までの残り時間)
VLAN	クライアントが所属している VLAN
Port	クライアントが接続されているスイッチポート
ID	バインディングデータベースにおけるエントリー ID
Source	エントリー (クライアント) の種類。Dynamic (ダイナミックエントリー。DHCP クライアント) User (スタティックエントリー。IP 固定設定クライアント) File (DHCP Snooping が有効化されたときに bindXXXX.dsn ファイル (「XXXX」の部分にはファームウェアのバージョンを表す 4 桁の数値が入る) からロードしたエントリー)

Router list	クライアントに通知されたデフォルトゲートウェイの一覧( DHCP の router オプションの内容 )
-------------	--

表 49:

関連コマンド

ENABLE DHCP Snooping ( 280 ページ )

## SHOW DHCP Snooping FILTER

カテゴリー：スイッチング / DHCP Snooping

### SHOW DHCP Snooping FILTER

#### 解説

DHCP Snooping によって自動生成されたフィルターエントリーの内容を表示する。

#### 入力・出力・画面例

Manager > show dhcp snooping filter				
DHCP Snooping ACL ( 2 entries )				
ClassID	FlowID	Port	EntryID	IP Address/Port/Mac
-----				
20001	0	11	1	192.168.10.200/11/00-0a-79-34-06-12
20004	0	5	4	192.168.10.5/5/00-00-00-00-00-01

DHCP Snooping ACL	エントリー数
ClassID	内部的なクラシファイア ID
FlowID	つねに 0
Port	スイッチポート番号
EntryID	DHCP Snooping テーブル ( バインディングデータベース ) のエントリー ID
IP Address	クライアントの IP アドレス
Port	クライアントが接続されているスイッチポート
Mac	クライアントの MAC アドレス

表 50:

#### 関連コマンド

ADD DHCP Snooping BINDING ( 173 ページ )

ENABLE DHCP Snooping ( 280 ページ )



# SHOW DHCP Snooping PORT

カテゴリー：スイッチング / DHCP Snooping

**SHOW DHCP Snooping PORT** [= {port-list|ALL}]

port-list: スイッチポート番号（1～。ハイフン、カンマを使った複数指定も可能）

## 解説

指定したスイッチポートにおける DHCP Snooping の設定情報を表示する。

## パラメーター

**PORT** スイッチポート。複数指定が可能。

## 入力・出力・画面例

```

Manager > show dhcp snooping port=11

DHCP Snooping Port Information:
-----

Port ..... 11
Trusted ..... No
Full Leases/Max Leases ... 1/1
Subscriber-ID .....
-----

```

Port	スイッチポート番号
Trusted	DHCP Snooping における ポート 種 別。Yes ( Trusted ポ ー ト )、No ( Untrusted ポ ー ト ) のいずれか
Full Leases/Max Leases	DHCP Snooping テーブル ( バインディングデータベース ) に現在登録されている該当ポート上のクライアントの数 / 該当ポート上で登録可能なクライアントの総数
Subscriber-ID	該当ポートの Subscriber-ID

表 51:

## 関連コマンド

ENABLE DHCP Snooping ( 280 ページ )



## SHOW EPSR

カテゴリー：スイッチング / イーサネットリングプロテクション (EPSR)

**SHOW EPSR** [= {*epsrname* | ALL}]

*epsrname*: EPSR ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

### 解説

EPSR ドメインの情報を表示する。

### パラメーター

**EPSR** EPSR ドメイン名。省略時および ALL 指定時はすべての EPSR ドメインの情報が表示される。

### 入力・出力・画面例

```
Manager > show epsr
```

```
EPSR Information
```

```
-----
Name ..... domain_two
Mode ..... Master
Status ..... Enabled
State ..... Complete
Control Vlan ..... controlB (3)
Data VLAN(s) ..... dataB (300)
Primary Port ..... 3
Primary Port Status ..... Forwarding
Secondary Port ..... 4
Secondary Port Status ..... Blocked
Hello Time ..... 1 s
Failover Time ..... 2 s
Ring Flap Time ..... 0 s
Trap ..... Enabled
```

```
Name ..... domain_one
Mode ..... Transit
Status ..... Enabled
State ..... Links-Up
Control Vlan ..... control (2)
Data VLAN(s) ..... data (100)
First Port ..... 1
First Port Status ..... Forwarding
First Port Direction ..... Downstream
```

```

Second Port ..... 2
Second Port Status ..... Forwarding
Second Port Direction ..... Upstream
Trap ..... Enabled
Master Node ..... 00-00-cd-24-03-4e
-----

```

Name	EPSR ドメイン名
Mode	EPSR ドメインにおける役割。Master ( マスターノード )、Transit ( トランジットノード ) のいずれか
Status	EPSR ドメインの有効・無効
State	EPSR ドメインの状態。マスターノードでは、Idle、Complete、Failed のいずれか。トランジットノードでは、Idle、Links-Up、Links-Down、Pre-Forwarding のいずれか
Control Vlan	コントロール VLAN。カッコ内は VLAN ID ( VID )
Data VLAN(s)	データ VLAN の一覧。カッコ内は VLAN ID ( VID )
Primary Port	( マスターノードのみ ) プライマリーポートの番号
Primary Port Status	( マスターノードのみ ) プライマリーポートの状態。Unknown、Forwarding、Down、Blocking のいずれか。Unknown は EPSR ドメインが無効に設定されていることを示す
Secondary Port	( マスターノードのみ ) セカンダリーポートの番号
Secondary Port Status	( マスターノードのみ ) セカンダリーポートの状態。Unknown、Forwarding、Down、Blocking のいずれか。Unknown は EPSR ドメインが無効に設定されていることを示す
Hello Time	( マスターノードのみ ) Healthcheck メッセージの送信間隔。数値の後の「s」は時間の単位でそれぞれ「秒」、「ミリ秒」を示す
Failover Time	( マスターノードのみ ) Healthcheck メッセージのタイムアウト時間。数値の後の「s」、「ms」は時間の単位でそれぞれ「秒」、「ミリ秒」を示す
Ring Flap Time	( マスターノードのみ ) リング障害の回復後、Failed 状態から Complete 状態に遷移する前に待機する最少時間 ( 秒 )
First Port	( トランジットノードのみ ) リングを構成する第 1 ポートの番号
First Port Status	( トランジットノードのみ ) リングを構成する第 1 ポートの状態。Unknown、Forwarding、Down、Blocking のいずれか。Unknown は EPSR ドメインが無効に設定されていることを示す
First Port Direction	( トランジットノードのみ ) リングを構成する第 1 ポートの向き。Upstream ( マスターノードのプライマリーポート方向 )、Downstream ( マスターノードのセカンダリーポート方向 )、Unknown ( EPSR ドメインが無効に設定されている ) のいずれか

Second Port	(トランジットノードのみ) リングを構成する第 2 ポートの番号
Second Port Status	(トランジットノードのみ) リングを構成する第 2 ポートの状態。Unknown、Forwarding、Down、Blocking のいずれか。Unknown は EPSR ドメインが無効に設定されていることを示す
Second Port Direction	(トランジットノードのみ) リングを構成する第 2 ポートの向き。Upstream (マスターノードのプライマリーポート方向)、Downstream (マスターノードのセカンダリーポート方向)、Unknown (EPSR ドメインが無効に設定されている) のいずれか
Master Node	(トランジットノードのみ) マスターノードの MAC アドレス。マスターノードからのメッセージをまだ受信していない場合は Unknown と表示される
Trap	EPSR ドメインの状態が変化したときに SNMP トラップを送信するかどうか。Enabled (送信する)、Disabled (送信しない) のいずれか

表 52:

### 関連コマンド

ADD EPSR DATAVLAN (175 ページ)

CREATE EPSR (205 ページ)

CREATE VLAN (225 ページ)

ENABLE EPSR (284 ページ)

SET EPSR (332 ページ)

SET EPSR PORT (334 ページ)

SHOW EPSR COUNTER (414 ページ)

SHOW EPSR COUNTER

カテゴリー：スイッチング / イーサネットリングプロテクション (EPSR)

**SHOW EPSR** [= {*epsrname* | ALL}] **COUNTER**

*epsrname*: EPSR ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ ) ハイフンを使用可能。大文字小文字を区別しない)

解説

EPSR ドメインの統計カウンターを表示する。

パラメーター

**EPSR** EPSR ドメイン名。省略時および ALL 指定時はすべての EPSR ドメインの情報が表示される。

入力・出力・画面例

```
Manager > show epsr counter

EPSR Counters
-----
Name: domain_two
Receive:
Total EPSR Packets      4674
Health                  4671
Ring Up                  2
Ring Down                0
Link Down                1
Invalid EPSR Packets    0
Transmit:
Total EPSR Packets      4697
Health                  4693
Ring Up                  2
Ring Down                2
Link Down                0

Name: domain_one
Receive:
Total EPSR Packets      1609
Health                  1603
Ring Up                  3
Ring Down                3
Link Down                0
Invalid EPSR Packets    0
Transmit:
Total EPSR Packets      3
Health                  0
Ring Up                  0
Ring Down                0
Link Down                3
```

Name	EPSR ドメイン名
Receive セクション	受信パケット数が表示される

Total EPSR Packets	受信した EPSR 制御パケットの総数
Health	受信した Healthcheck メッセージの数
Ring Up	受信した Ring Up メッセージの数
Ring Down	受信した Ring Down メッセージの数
Link Down	受信した Link Down メッセージの数
Invalid EPSR Packets	無効な EPSR 制御パケットの数
Transmit セクション	送信パケット数が表示される
Total EPSR Packets	送信した EPSR 制御パケットの総数
Health	送信した Healthcheck メッセージの数
Ring Up	送信した Ring Up メッセージの数
Ring Down	送信した Ring Down メッセージの数
Link Down	送信した Link Down メッセージの数

表 53:

関連コマンド

SHOW EPSR ( 411 ページ )

SHOW EPSR DEBUG

カテゴリー：スイッチング / イーサネットリングプロテクション (EPSR)

**SHOW EPSR** [= {*epsrname* | ALL}] **DEBUG**

*epsrname*: EPSR ドメイン名 (1 ~ 15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

解説

EPSR ドメインで有効になっているデバッグオプションを表示する。

パラメーター

**EPSR** EPSR ドメイン名。省略時および ALL 指定時はすべての EPSR ドメインの情報が表示される。

入力・出力・画面例

Manager > show epsr debug

EPSR Name	Enabled Debug Modes	Output	Timeout
domain_two	None		
domain_one	None		

EPSR Name	EPSR ドメイン名
Enabled Debug Modes	現在有効になっている EPSR デバッグオプション。INFO ( EPSR に関する全般的情報を表示 )、MSG ( EPSR パケットをデコードして表示 )、PKT ( EPSR パケットを ASCII 表示 )、STATE ( EPSR の状態遷移を表示 )、ALL ( すべてのオプション )、None ( なし ) がある
Output	デバッグ情報の出力先 ( 仮想端末 ( TTY ) 番号 )
Timeout	デバッグオプションの残り有効期間 ( 秒 )

表 54:

関連コマンド

SHOW EPSR ( 411 ページ )



## SHOW LACP

カテゴリー：スイッチング / LACP (IEEE 802.3ad)

### SHOW LACP

#### 解説

LACP の一般情報を表示する。

#### 入力・出力・画面例

```
Manager > show lacp
```

```
LACP Information
```

```
-----
Status ..... Enabled
Actor System Priority ..... 32768
Actor System ..... 00-00-cd-24-02-0e
Address learn thrash action ..... Learn Disable
Address learn thrash timeout ..... 1 second
LACP Ports ..... 1-24
  Active ..... 1-24
  Passive ..... None
```

Status	LACP モジュールの状態。Enabled か Disabled
Actor System Priority	システムプライオリティー
Actor System	システム ID (MAC アドレス)
Address learn thrash action	MAC アドレススラッシング検出時の動作。None (何もしない)、Learn Disable (トランクグループ内の全ポートで MAC アドレスの学習を停止する)、Port Disable (トランクグループ内の全ポートをディセーブルにする)、VLAN Disable (スラッシングが発生した VLAN に対してのみトランクグループ内の全ポートをディセーブルにする)、Link Down (トランクグループ内の全ポートを物理的にリンクダウンさせる) のいずれか
Address learn thrash timeout	MAC アドレススラッシング検出時の動作の持続時間 (秒)。動作の実行中は、カッコ内に残り秒数が表示される。None は無期限であることを示す
LACP Ports	LACP の管理下にあるポートの一覧
Active	LACP の管理下にあるポートのうち、Active モードで動作しているものの一覧

Passive	LACP の管理下にあるポートのうち、Passive モードで動作している ものの一覧
---------	--

表 55:

関連コマンド

- DISABLE LACP ( 259 ページ )
- ENABLE LACP ( 286 ページ )
- SET LACP ( 336 ページ )
- SHOW LACP PORT ( 419 ページ )

# SHOW LACP PORT

カテゴリー：スイッチング / LACP (IEEE 802.3ad)

**SHOW LACP PORT** [= {*port-list* | ALL}]

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

## 解説

スイッチポートの LACP 関連情報を表示する。

## パラメーター

**PORT** ポート番号。

## 入力・出力・画面例

```

Manager > show lacp port=1,5
LACP Port Information
-----

Actor Port ..... 1
  Trunk Group ..... lacp26
  Selected ..... Selected
  Port Priority ..... 32768
  LACP Port Number ..... 1
  Port Key ..... 2
    Admin Key ..... 1
  Mode ..... Active
  Periodic ..... Fast
  Individual ..... No
  Synchronised ..... Yes
  Collecting ..... Yes
  Distributing ..... Yes
  Defaulted ..... No
  Expired ..... No
  Actor Churn ..... No
  Partner Churn ..... No

Partner Information:
  Partner Sys Priority ..... 32768
  Partner System .. 00-00-f4-27-2c-74
  Port Key ..... 3
  Port Priority ..... 32768
  Port Number ..... 1
  Mode ..... Active
  Periodic ..... Fast
  Individual ..... No
  Synchronised ..... Yes
  Collecting ..... Yes
  Distributing ..... Yes
  Defaulted ..... No
  Expired ..... No

Actor Port ..... 5
  Trunk Group ..... -
  Selected ..... Selected
  Port Priority ..... 32768
  LACP Port Number ..... 5
  Port Key ..... 1
    Admin Key ..... 1

Partner Information:
  Partner Sys Priority ..... 0
  Partner System .. 00-00-00-00-00-00
  Port Key ..... 0
  Port Priority ..... 0
  Port Number ..... 0
  
```

```

Mode ..... Active
Periodic ..... Fast
Individual ..... No
Synchronised ..... Yes
Collecting ..... No
Distributing ..... No
Defaulted ..... Yes
Expired ..... No
Actor Churn ..... No
Partner Churn ..... No

```

```

Mode ..... Passive
Periodic ..... Fast
Individual ..... Yes
Synchronised ..... No
Collecting ..... Yes
Distributing ..... Yes
Defaulted ..... Yes
Expired ..... No

```

Actor Port	ポート番号
Port is LACP Disabled - Port in a Manual Trunk	該当ポートが手動設定されたトランクポートであるため、LACP が自動的に無効化されたことを示す
Port is LACP Disabled - Half Duplex Link	該当ポートが Half Duplex で動作しているため、LACP が自動的に無効化されたことを示す
Trunk Group	所属先のトランクグループ名。LACP によって自動設定されたトランクグループには「lacpXXXX」形式の名前が自動的に割り当てられる (XXXX は SHOW INTERFACE コマンドで表示されるインターフェースインデックス)。トランクグループに所属していない場合は「-」と表示される
Selected	LACP の状態。Selected (LACP の管理下にある)、Standby (LACP の管理下にあり、現在スタンバイ状態である)、Unselected (LACP の管理下でない) がある
Priority	LACP ポートプライオリティー
LACP Port Number	エンコードされたポート番号
Port Key	LACP ポート鍵
Admin Key	LACP ポート鍵のもととなる設定可能値 (ADMINKEY)
Mode	LACP 動作モード。Active、Passive のどちらか
Periodic	Active モード時の LACP パケットの送信間隔。Fast (1 秒)、Slow (30 秒) のどちらか
Individual	Aggregation フラグの状態。Yes (Individual = 同一トランクグループを構成可能な他のポートがない)、No (Aggregatable = 同一トランクグループを構成可能な他のポートがある) のどちらか

Synchronised	Synchronization フラグの状態。Yes (IN_SYNC) \ No (OUT_OF_SYNC) のどちらか
Collecting	Collecting フラグの状態。Yes (パケットを受信できる) \ No (パケットを受信できない) のどちらか
Distributing	Distributing フラグの状態。Yes (パケットを送信できる) \ No (パケットを送信できない) のどちらか
Defaulted	Defaulted フラグの状態。Yes (対向機器から LACP パケットを受け取っていないため、対向機器の情報としてデフォルトの値を仮定している) \ No (対向機器から受信した LACP パケットの情報を使っている)
Expired	Expired フラグの状態。Yes (Receive Machine が EXPIRED 状態にある) \ No (Receive Machine が EXPIRED 状態にない)
Actor Churn	自ポート側で Churn (Synchronized フラグが安定せず、一定時間内に LACP グループに所属できなかった状態) を検出したかどうか。Yes (Churn を検出した) \ No (Churn を検出していない)
Partner Churn	対向ポート側で Churn (Synchronized フラグが安定せず、一定時間内に LACP グループに所属できなかった状態) を検出したかどうか。Yes (Churn を検出した) \ No (Churn を検出していない)
Partner Information セクション	対向する機器・ポートの情報が表示される。
Partner Sys Priority	対向機器の LACP システムプライオリティ
Partner System	対向機器の LACP システム ID (MAC アドレス)
Port Key	対向機器の LACP ポート鍵
Port Priority	対向機器の LACP ポートプライオリティ
Port Number	対向機器のポート番号
Mode	対向機器の LACP 動作モード。Active、Passive のどちらか
Periodic	対向機器の LACP パケットの送信間隔。Fast (1 秒) \ Slow (30 秒) のどちらか
Individual	対向機器の Aggregation フラグの状態

Synchronised	対向機器の Synchronization フラグの状態
Collecting	対向機器の Collecting フラグの状態
Distributing	対向機器の Distributing フラグの状態
Defaulted	対向機器の Defaulted フラグの状態
Expired	対向機器の Expired フラグの状態

表 56:

### 関連コマンド

ADD LACP PORT ( 176 ページ )

SET LACP PORT ( 335 ページ )

SHOW LACP ( 417 ページ )

SHOW LACP TRUNK

カテゴリー：スイッチング / LACP (IEEE 802.3ad)

SHOW LACP TRUNK

解説

LACPによって自動生成されたトランクグループの情報を表示する。

入力・出力・画面例

```
Manager > show lacp trunk

LACP Dynamic Trunk Group Information
-----

Trunk group name ..... lacp26:
Speed ..... 100 Mbps
Ports in Trunk ..... 1-4
LAG ID:
[(8000,00-00-cd-24-02-0e,0002,00,0000),(8000,00-00-f4-27-2c-74,0003,00,0000)]
-----
```

Trunk group name	トランクグループ名。LACPによって自動設定されたトランクグループには「lacp-XXXX」形式の名前が自動的に割り当てられる（XXXXはSHOW INTERFACEコマンドで表示されるインターフェースインデックス）
Speed	トランクポートの通信速度。10Mbps、100Mbps、1000Mbps、-（未設定）のいずれか
Ports in Trunk	所属ポート
LAG ID	LAG ID（Link Aggregation Identifier）。自システム（Actor）と対向システム（Partner）それぞれのシステムプライオリティー、システムID（MACアドレス）、ポート鍵、ポートプライオリティー、ポート番号を組み合わせたもの

表 57:

関連コマンド

- ADD LACP PORT (176 ページ)
- SET LACP (336 ページ)
- SET LACP PORT (335 ページ)
- SHOW LACP (417 ページ)

SHOW LACP TRUNK

SHOW LACP PORT ( 419 ページ )



## SHOW MSTP

カテゴリー：スイッチング / マルチプルスパニングツリープロトコル (MSTP)

**SHOW MSTP** [CONFIGID] [TABLE]

### 解説

マルチプルスパニングツリープロトコルの設定情報を表示する。

### パラメーター

**CONFIGID** 所属先 MST リージョンの識別情報を表示する。このオプションで表示される情報が等しい装置は、同一の MST リージョンに所属していると見なされる。

**TABLE** MST 設定テーブル (MST インスタンスと VLAN の対応付け一覧表) を表示する。

### 入力・出力・画面例

```
Manager > show mstp
```

```
MSTP Information
```

```
-----
MSTP status ..... Enabled
MST Configuration Name ..... Test
Revision Level ..... 0
Number of MSTIs ..... 2
Hello Time ..... 2
Forward Delay ..... 15
Message Max Age ..... 20
Max Hops ..... 20
Protocol Version ..... MSTP
Support Static VLANs ..... Disabled
Transmission Limit ..... 3
Migrate Time ..... 3
-----
```

```
Manager > show mstp configid
```

```
MST Configuration Identification
```

```
-----
Configuration Name ..... Test
Format Selector ..... 0
Revision Level ..... 0
Configuration Digest ..... 0x87957342F6B0029D887BAAEC6212B0BF
-----
```

```
Manager > show mstp table
```

```
MST Configuration Table
```

```
-----
Multiple Spanning Tree Instance    VLAN Members
-----
CIST                               1-9,11-19,21-4094
MSTI 10                            10
MSTI 20                            20
-----
```

MSTP Status	MSTP の有効・無効
MST Configuration Name	MST リージョン名
MST Revision Level	MST リージョン設定のリビジョン
Number of MSTIs	MST インスタンス数
Hello Time	本機のハロータイム設定値 (SET MSTP コマンドの HELLOTIME パラメーター)。ルートブリッジになったときにこの値が使用される
Forward Delay	本機のフォワードディレイタイム設定値 (SET MSTP コマンドの FORWARDDELAY パラメーター)。ルートブリッジになったときにこの値が使用される
Max Message Age	本機の最大エージタイム設定値 (SET MSTP コマンドの MAXAGE パラメーター)。ルートブリッジになったときにこの値が使用される
Max Hops	本機の最大ホップ数設定値 (SET MSTP コマンドの MAXHOPS パラメーター)。ルートブリッジになったときにこの値が使用される
Protocol Version	MSTP の動作モード (使用しているプロトコルバージョン)。STP、RSTP、MSTP のいずれか
Support Static VLAN	スパンニングツリーのトポロジ計算時、MST インスタンスに所属している VLAN のポート構成を考慮するかどうか。Enabled (考慮する)、Disabled (考慮せず通常の MSTP の方法を用いる) のいずれか
Transmission Limit	ハロータイムの間に送信可能な BPDU の数。この値は標準規格で規定されており、3 で固定に設定されている

表 58: 無指定時

Configuration Name	MST リージョン名
Format Selector	フォーマットセレクター。MSTP を示す 0 で固定
Revision Level	MST リージョン設定のリビジョン
Configuration digest	MST 設定テーブル (MST インスタンスと VLAN の対応付け一覧表) のメッセージダイジェスト (HMAC-MD5)

表 59: CONFIGID 指定時

Multiple Spanning Tree Instance	MST インスタンス ID または CIST (Common and Internal Spanning Tree)
VLAN Members	MST インスタンスまたは CIST に関連付けられている VLAN の一覧

表 60: TABLE 指定時

### 関連コマンド

ADD MSTP MSTI VLAN ( 178 ページ )  
 DELETE MSTP MSTI VLAN ( 230 ページ )  
 DISABLE MSTP ( 261 ページ )  
 ENABLE MSTP ( 288 ページ )  
 SET MSTP ( 338 ページ )  
 SET MSTP CIST ( 340 ページ )  
 SET MSTP MSTI ( 343 ページ )  
 SHOW MSTP CIST ( 428 ページ )

SHOW MSTP CIST

カテゴリー：スイッチング / マルチプルスパニングツリープロトコル (MSTP)

SHOW MSTP CIST

解説

CIST (Common and Internal Spanning Tree) の情報を表示する。

入力・出力・画面例

```
Manager > show mstp cist

Common Internal Spanning Tree
-----
Bridge Identifier ..... 4096 : 00-00-f4-27-2c-74
Bridge Role ..... Regional Root Bridge
VLAN Members ..... 1-9,11-19,21-4094
CIST Root Bridge ..... 0 : 00-00-cd-24-03-4e
CIST Regional Root Bridge ..... 4096 : 00-00-f4-27-2c-74
Designated Bridge ..... 0 : 00-00-cd-24-03-4e
Root Port ..... 2
Designated Port ..... 128:1
External Root Path Cost ..... 200000
Internal Root Path Cost ..... 0

Performance:
Max Age ..... 20
Hello Time ..... 2
Forward Delay ..... 15
Max Hops ..... 20
Bridge Max Age ..... 20
Bridge Hello Time ..... 2
Bridge Forward Delay ..... 15
Bridge Max Hops ..... 20
Transmission Limit ..... 3

Topology Changes:
Time Since Topology Change ..... 5
Topology Change Count ..... 12
Topology Change ..... FALSE
-----
```

Bridge Identifier	ブリッジ識別子。CIST プライオリティと MAC アドレスで構成される
-------------------	--------------------------------------

Bridge Role	CIST におけるブリッジの役割。Root Bridge、Regional Root Bridge、Designated Bridge のいずれか
VLAN Members	所属 VLAN の VLAN ID
CIST Root Bridge	CIST ルートブリッジ (CIST 全体のルート) のブリッジ識別子
CIST Regional Root Bridge	CIST リージョナルルート (MST リージョン内における CIST ツリーのルートブリッジ) のブリッジ識別子
Designated Bridge	代表ブリッジのブリッジ識別子
Root Port	ルートポートの番号。ルートブリッジのときは N/A と表示される
Designated Port	代表ポートのポート識別子
External Root Path Cost	CIST ルートブリッジが所属するリージョンまでのパスコスト
Internal Root Path Cost	CIST リージョナルルート (MST リージョン内における CIST ツリーのルートブリッジ) までのパスコスト
Max Age	最大エージタイム (秒)。ルートブリッジによって決定された値
Hello Time	ハロータイム (秒)。ルートブリッジによって決定された値
Forward Delay	フォワードディレイタイム (秒)。ルートブリッジによって決定された値
Max Hops	最大ホップ数。ルートブリッジによって決定された値
Bridge Max Age	本機の最大エージタイム設定値 (SET MSTP コマンドの MAXAGE パラメーター)。ルートブリッジになったときにこの値が使用される
Bridge Hello Time	本機のハロータイム設定値 (SET MSTP コマンドの HELLOTIME パラメーター)。ルートブリッジになったときにこの値が使用される
Bridge Forward Delay	本機のフォワードディレイタイム設定値 (SET MSTP コマンドの FORWARDDELAY パラメーター)。ルートブリッジになったときにこの値が使用される
Bridge Max Hops	本機の最大ホップ数設定値 (SET MSTP コマンドの MAXHOPS パラメーター)。ルートブリッジになったときにこの値が使用される
Transmission Limit	ハロータイムの間に送信可能な BPDU の数。この値は標準規格で規定されており、3 で固定に設定されている
Time Since Topology Change	最後に Topology Change が発生してから経過した時間 (秒)
Topology Change Count	Topology Change が発生した回数
Topology Change	Topology Change の最中かどうか

表 61:

## 関連コマンド

DISABLE MSTP (261 ページ)

DISABLE MSTP CIST PORT

ENABLE MSTP (288 ページ)

ENABLE MSTP CIST PORT

SET MSTP CIST (340 ページ)

SET MSTP CIST PORT (341 ページ)

SHOW MSTP ( 425 ページ )

## SHOW MSTP CIST PORT

カテゴリー：スイッチング / マルチプルスパニングツリープロトコル (MSTP)

**SHOW MSTP CIST PORT** [= {*port-list* | ALL}]

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

CIST (Common and Internal Spanning Tree) におけるスイッチポートの MSTP 情報を表示する。

### パラメーター

**PORT** ポート番号

### 入力・出力・画面例

```
Manager > show mstp cist port

CIST Port Information
-----
Port Number ..... 1
  Port Identifier ..... 128:1
  Port Role ..... Alternate Port
  Port State ..... Discarding
  Switch Port State ..... Enabled
  Link Status ..... Up

Port Number ..... 2
  Port Identifier ..... 128:2
  Port Role ..... Root Port
  Port State ..... Forwarding
  Switch Port State ..... Enabled
  Link Status ..... Up

Port Number ..... 3
  Port Identifier ..... 128:3
  Port Role ..... Alternate Port
  Port State ..... Discarding
  Switch Port State ..... Enabled
  Link Status ..... Up

Port Number ..... 4
  Port Identifier ..... 128:4
  Port Role ..... Disabled Port
  Port State ..... Discarding
```

```
Switch Port State ..... Enabled
Link Status ..... Down
...
```

```
Manager > show mstp cist port=2
```

#### CIST Port Information

```
-----
Port Number ..... 2
Port Identifier ..... 128:2
Port Role ..... Root Port
Port State ..... Forwarding
Switch Port State ..... Enabled
Link Status ..... Up
Port Path Cost ..... 200000
External Port Path Cost ..... 200000
Designated Bridge ..... 32768 : 00-00-cd-24-03-4e
Designated Port ..... 128:1
Regional Root Path Cost ..... 0
External Root Path Cost ..... 0
Edge Port ..... No
Point to Point Link ..... Yes (Auto)
Boundary Port ..... No
-----
```

Port Number	ポート番号
Port Identifier	ポート識別子。ポートプライオリティとポート番号で構成される
Port Role	ポートの役割。Alternate Port、Backup Port、Designated Port、Disabled Port、Root Port のいずれか
Port State	ポートの状態。Disabled、Discarding、Learning、Forwarding のいずれか
Switch Port State	スイッチポートのステータス。Enabled か Disabled
Link Status	スイッチポートのリンクステータス。Up か Down

表 62: ポート番号省略時

Port Number	ポート番号
Port Identifier	ポート識別子。ポートプライオリティとポート番号で構成される
Port Role	ポートの役割。Alternate Port、Backup Port、Designated Port、Disabled Port、Root Port のいずれか
Port State	ポートの状態。Disabled、Discarding、Learning、Forwarding のいずれか
Switch Port State	スイッチポートのステータス。Enabled か Disabled
Link Status	スイッチポートのリンクステータス。Up か Down
Port Path Cost	CIST リージョナルルート (MST リージョン内における CIST ツリーのルートブリッジ) までのパスに対するポート通過コスト



External Port Path Cost	CIST ルートブリッジが所属するリージョンまでのパスに対するポート通過コスト
Designated Bridge	代表ブリッジのブリッジ識別子
Designated Port	代表ポート。代表ブリッジが BPDU を送出するポートのポート識別子
Regional Root Path Cost	CIST リージョナルルート (MST リージョン内における CIST ツリーのルートブリッジ) までのパスコスト
External Root Path Cost	CIST ルートブリッジが所属するリージョンまでのパスコスト
Edge Port	ポートがエッジポートかどうか。Yes、No のいずれか
Point to Point Link	ポートが他のブリッジとポイントツーポイントで接続されているかどうか。No、Yes で表示される。(Auto) は自動判別の結果であることを示す
Boundary Port	ポートがリージョン外との接続点になっているかどうか。Yes、No のいずれか

表 63: ポート番号指定時

関連コマンド

DISABLE MSTP ( 261 ページ )

DISABLE MSTP CIST PORT

ENABLE MSTP ( 288 ページ )

ENABLE MSTP CIST PORT

SET MSTP CIST ( 340 ページ )

SET MSTP CIST PORT ( 341 ページ )

SHOW MSTP ( 425 ページ )

SHOW MSTP MSTI PORT ( 439 ページ )

## SHOW MSTP COUNTER PORT

カテゴリー：スイッチング / マルチプルスパニングツリープロトコル (MSTP)

**SHOW MSTP COUNTER PORT** [= {*port-list* | ALL}]

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

指定ポートの MSTP 統計カウンターを表示する。

### パラメーター

**PORT** ポート番号

### 入力・出力・画面例

```
Manager > show mstp counter port=5

MSTP Port Counters
-----
Port Number      5
Receive:
  Total BPDUs          581
  MSTP BPDUs           581
  RSTP BPDUs           0
  STP BPDUs            0
  Invalid BPDUs        0
Transmit:
  Total BPDUs          579
  MSTP BPDUs           579
  RSTP BPDUs           0
  STP BPDUs            0
Discarded:
  Port Disabled        0
  Invalid Protocol     0
  Invalid Type         0
  Invalid BPDU length  0
-----
```

Port Number	ポート番号
Receive セクション	受信パケット数が表示される
Total BPDUs	受信した各種 BPDU (STP/RSTP/MSTP BPDU) の総数
MSTP BPDUs	MSTP BPDU 受信数
RSTP BPDUs	RSTP BPDU 受信数
STP BPDUs	STP BPDU 受信数

Invalid BPDUs	無効な BPDU 受信数
Transmit セクション	送信パケット数が表示される
Total BPDUs	送信した各種 BPDU ( STP/RSTP/MSTP BPDU ) の総数
MSTP BPDUs	MSTP BPDU 送信数
RSTP BPDUs	RSTP BPDU 送信数
STP BPDUs	STP BPDU 送信数
Discarded セクション	破棄されたパケット数が表示される
Port Disabled	受信ポートがディセーブル状態だったために破棄された BPDU の数
Invalid Protocol	プロトコル ID フィールドかプロトコルバージョン ID フィールドの値が無効であったため破棄された BPDU 数
Invalid Type	Type フィールドの値が無効であったため破棄された BPDU 数
Invalid Message Age	メッセージエージが無効であったため破棄された BPDU 数
Invalid BPDU Length	長さが無効であったため破棄された BPDU 数

表 64:

関連コマンド

- DISABLE MSTP ( 261 ページ )
- ENABLE MSTP ( 288 ページ )
- RESET MSTP COUNTER PORT ( 318 ページ )
- SET MSTP CIST ( 340 ページ )

## SHOW MSTP MSTI

カテゴリー：スイッチング / マルチプルスパニングツリープロトコル (MSTP)

**SHOW MSTP MSTI** [= {*instance* | ALL}]

*instance*: MST インスタンス ID (1 ~ 4094)

### 解説

MST インスタンスの情報を表示する。

### パラメーター

**MSTI** MST インスタンス ID。省略時はすべての MST インスタンスの情報が簡潔に一覧表示される。ALL 指定時はすべての MST インスタンスの詳細情報が一覧表示される。

### 入力・出力・画面例

```
Manager > show mstp msti
```

```
Multiple Spanning Tree Instances
```

```
-----
MSTI ..... 10
  Bridge Identifier ..... 4096 : 00-00-f4-27-2c-74
  Bridge Role ..... Regional Root Bridge
  VLAN members ..... 10
```

```
MSTI ..... 20
  Bridge Identifier ..... 8192 : 00-00-f4-27-2c-74
  Bridge Role ..... Designated Bridge
  VLAN members ..... 20
-----
```

```
Manager > show mstp msti=all
```

```
Multiple Spanning Tree Instances
```

```
-----
MSTI ..... 10
  Bridge Identifier ..... 4096 : 00-00-f4-27-2c-74
  Bridge Role ..... Regional Root Bridge
  VLAN members ..... 10
  Regional Root Identifier ..... 4096 : 00-00-f4-27-2c-74
  Designated Bridge ..... 4096 : 00-00-f4-27-2c-74
  Root Path Cost ..... 0
  Root Port ..... N/A
```

```

Designated Port ..... N/A
Topology Changes:
  Time Since Topology Change .... 94
  Topology Change Count ..... 5
  Topology Change ..... FALSE

MSTI ..... 20
  Bridge Identifier ..... 8192 : 00-00-f4-27-2c-74
  Bridge Role ..... Designated Bridge
  VLAN members ..... 20
  Regional Root Identifier ..... 4096 : 00-00-cd-24-03-4e
  Designated Bridge ..... 4096 : 00-00-cd-24-03-4e
  Root Path Cost ..... 200000
  Root Port ..... 2
  Designated Port ..... 128:1
  Topology Changes:
    Time Since Topology Change .... 95
    Topology Change Count ..... 3
    Topology Change ..... FALSE
-----

```

MSTI	MST インスタンス ID
Bridge Identifier	ブリッジ識別子。ブリッジプライオリティーと MAC アドレスで構成される
Bridge Role	ブリッジの役割。Regional Root Bridge、Designated Bridge のいずれか
VLAN Members	所属 VLAN の VLAN ID

表 65: MST インスタンス ID 省略時

MSTI	MST インスタンス ID
Bridge Identifier	ブリッジ識別子。ブリッジプライオリティーと MAC アドレスで構成される
Bridge Role	ブリッジの役割。Regional Root Bridge、Designated Bridge のいずれか
VLAN Members	所属 VLAN の VLAN ID
Regional Root Identifier	リージョナルルート (MST インスタンスのルートブリッジ) のブリッジ識別子
Designated Bridge	代表ブリッジのブリッジ識別子
Root Path Cost	リージョナルルート (MST インスタンスのルートブリッジ) までのパスコスト
Root Port	ルートポートの番号。ルートブリッジのときは N/A と表示される
Designated Port	代表ポートのポート識別子。ルートブリッジのときは N/A と表示される
Time Since Topology Change	最後に Topology Change が発生してから経過した時間 (秒)
Topology Change Count	Topology Change が発生した回数

Topology Change	Topology Change の最中かどうか
-----------------	-------------------------

表 66: MST インスタンス ID 指定時

関連コマンド

- DISABLE MSTP ( 261 ページ )
- ENABLE MSTP ( 288 ページ )
- SET MSTP ( 338 ページ )
- SET MSTP MSTI PORT ( 344 ページ )

## SHOW MSTP MSTI PORT

カテゴリー：スイッチング / マルチプルスパニングツリープロトコル (MSTP)

**SHOW MSTP MSTI=instance PORT** [= {port-list|ALL}]

*instance*: MST インスタンス ID (1~4094)

*port-list*: スイッチポート番号 (1~。ハイフン、カンマを使った複数指定も可能)

### 解説

指定した MST インスタンスにおけるスイッチポートの MSTP 情報を表示する。

### パラメーター

**MSTI** MST インスタンス ID

**PORT** ポート番号

### 入力・出力・画面例

```
Manager > show mstp msti=10 port=1
```

```
MSTI 10 Port Information
```

```
-----
Port Number ..... 1
Port Identifier ..... 128:1
Port Role ..... Designated Port
Port State ..... Forwarding
Switch Port State ..... Enabled
Link Status ..... Up
Port Path Cost ..... 200000
Designated Bridge ..... 4096 : 00-00-f4-27-2c-74
Designated Port ..... 128:1
Regional Root Path Cost ..... 0
-----
```

```
Manager > show mstp msti=20 port=1
```

```
MSTI 20 Port Information
```

```
-----
Port Number ..... 1
Port Identifier ..... 128:1
Port Role ..... Designated Port
Port State ..... Forwarding
Switch Port State ..... Enabled
Link Status ..... Up
-----
```

```

Port Path Cost ..... 200000
Designated Bridge ..... 8192 : 00-00-f4-27-2c-74
Designated Port ..... 128:1
Regional Root Path Cost ..... 200000
-----

```

Port Number	ポート番号
Port Identifier	ポート識別子。ポートプライオリティーとポート番号で構成される
Port Role	ポートの役割。Alternate Port、Backup Port、Designated Port、Disabled Port、Root Port のいずれか
Port State	ポートの状態。Disabled、Discarding、Learning、Forwarding のいずれか
Switch Port State	スイッチポートのステータス。Enabled か Disabled
Link Status	スイッチポートのリンクステータス。Up か Down
Port Path Cost	パスコスト
Designated Bridge	代表ブリッジのブリッジ識別子
Designated Port	代表ポート。代表ブリッジが BPDU を送出するポートのポート識別子
Regional Root Path Cost	リージョナルルート (MST インスタンスのルートブリッジ) までのパスコスト

表 67:

## 関連コマンド

DISABLE MSTP ( 261 ページ )

DISABLE MSTP MSTI PORT

ENABLE MSTP ( 288 ページ )

ENABLE MSTP MSTI PORT

SET MSTP MSTI ( 343 ページ )

SET MSTP MSTI PORT ( 344 ページ )

SHOW MSTP CIST PORT ( 431 ページ )

SHOW MSTP MSTI ( 436 ページ )



## SHOW PORTAUTH

カテゴリー：スイッチング / ポート認証

**SHOW PORTAUTH** [= {8021X|MACBASED}]

### 解説

ポート認証機能（802.1X 認証、MAC ベース認証）の全般的な設定と状態を表示する。

### パラメーター

**PORTAUTH** 認証メカニズム。8021X（802.1X 認証）、MACBASED（MAC ベース認証）から選択する。  
省略時は 8021X と見なされる。

### 入力・出力・画面例

```
Manager > show portauth=8021x
```

```
802.1X System
```

```
-----
SystemAuthControl..... ENABLED
Global Username..... portAuthPortAuth
Global Password..... portAuthPortAuth
Global Encryption Method..... Standard
Number of Multi Supplicants.. 0    (limit 480)
```

Port	PAE Capabilities	Protocol Version
port1	Authenticator (Single)	1
port2	Authenticator (Single)	1
port3	Authenticator (Single)	1
port4	Authenticator (Single)	1
port5	Authenticator (Single)	1
port6	Authenticator (Single)	1
port7	Authenticator (Single)	1
port8	Authenticator (Multi)	1
port9	None	1
port10	None	1
port11	None	1
port12	None	1
port13	None	1
port14	None	1
port15	None	1
port16	None	1

## SHOW PORTAUTH

port17	None	1
port18	None	1
port19	None	1
port20	None	1
port21	None	1
port22	None	1
port23	None	1
port24	None	1
port25	None	1
port26	None	1

Manager > show portauth=macbased

### MAC Based Authentication System

SystemAuthControl..... ENABLED  
 Number of Supplicants..... 0 (limit 480)

Port	PAE Status
port1	Disabled
port2	Disabled
port3	Disabled
port4	Disabled
port5	Disabled
port6	Disabled
port7	Disabled
port8	Disabled
port9	Enabled
port10	Enabled
port11	Enabled
port12	Enabled
port13	Enabled
port14	Enabled
port15	Enabled
port16	Enabled
port17	Disabled
port18	Disabled
port19	Disabled
port20	Disabled
port21	Disabled
port22	Disabled
port23	Disabled
port24	Disabled
port25	Disabled
port26	Disabled

SystemAuthControl

802.1X 認証機能の有効・無効

Global Username	Supplicant 時のユーザー名 ( Supplicant として動作しているポートが認証を受けるときに使用するユーザー名。該当ポート固有のユーザー名が設定されているときは、本ユーザー名ではなくポート固有のユーザー名を使用する )
Global Password	Supplicant 時のパスワード ( Supplicant として動作しているポートが認証を受けるときに使用するパスワード。該当ポート固有のパスワードが設定されているときは、本パスワードではなくポート固有のパスワードを使用する )
Global Encryption Method	Supplicant 時のパスワード暗号化方式。Standard、OTP のいずれか
Global Encryption Type	Supplicant 時のパスワード暗号化方式に OTP を使用している場合のワンタイムパスワード生成アルゴリズム。MD4、MD5 のいずれか
Number of Multi Supplicants	Supplicant の数 ( カッコ内はシステムがサポートしている Supplicant の最大数 )
Port	スイッチポートのインターフェース名
PAE Capabilities	802.1X 認証におけるスイッチポートの役割。Authenticator (Single)、Authenticator (Multi)、Supplicant、Both、None のいずれか
Protocol Version	EAPOL プロトコルバージョン

表 68: PORTAUTH=8021X のとき

SystemAuthControl	MAC ベース認証機能の有効・無効
Port	スイッチポートのインターフェース名
PAE Capabilities	該当スイッチポートにおける MAC ベース認証の有効・無効

表 69: PORTAUTH=MACBASED のとき

## 関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE ( 170 ページ )

ENABLE PORTAUTH ( 289 ページ )

ENABLE PORTAUTH PORT ( 291 ページ )

SET PORTAUTH PORT ( 346 ページ )

SET PORTAUTH PORT SUPPLICANTMAC ( 350 ページ )

SHOW PORTAUTH ( 441 ページ )

SHOW PORTAUTH COUNTER ( 444 ページ )

SHOW PORTAUTH MULTISUPPLICANT PORT ( 447 ページ )

SHOW PORTAUTH PORT ( 451 ページ )

SHOW PORTAUTH TIMER ( 456 ページ )

## SHOW PORTAUTH COUNTER

カテゴリー：スイッチング / ポート認証

**SHOW PORTAUTH** [=8021X] **COUNTER PORT**={*port-list*|ALL}

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

指定ポートの 802.1X 統計カウンターを表示する。

### パラメーター

**PORTAUTH** 認証メカニズム。本コマンドでは 8021X ( 802.1X 認証 ) のみ有効。省略時は 8021X と見なされるため、特に指定する必要はない。

**PORT** スイッチポート。複数指定が可能。

### 入力・出力・画面例

```
Manager > show portauth counter port=5
802.1X Counters
-----
port5
PAE Type..... Authenticator
  Last EAPOL Frame Version.... 1
  Last EAPOL Frame Source..... 00-00-e2-59-56-48

  Receive                                Transmit
    EAPOL Frames..... 32      EAPOL Frames..... 122
    EAPOL Start Frames..... 0    EAP Req/Id Frames..... 70
    EAPOL Logoff Frames..... 0    EAP Request Frames..... 3
    EAP Resp/Id Frames..... 29
    EAP Response Frames..... 3
    EAP Length Error Frames.... 0
    Invalid EAPOL Frames..... 0

Manager > show portauth counter port=7
802.1X Counters
-----
port7
PAE Type..... Both

Authenticator - Attached Supplicant(s)
  Last EAPOL Frame Source..... 00-00-f4-95-30-6a
```

MAC Address..... 00-00-e2-59-56-48			
Last EAPOL Frame Version..... 1			
Receive		Transmit	
EAPOL Frames.....	3	EAPOL Frames.....	3
EAPOL Start Frames.....	0	EAP Req/Id Frames.....	1
EAPOL Logoff Frames.....	0	EAP Request Frames.....	1
EAP Resp/Id Frames.....	2		
EAP Response Frames.....	1		
EAP Length Error Frames....	0		
Invalid EAPOL Frames.....	0		
MAC Address..... 00-00-f4-95-30-6a			
Last EAPOL Frame Version..... 1			
Receive		Transmit	
EAPOL Frames.....	3	EAPOL Frames.....	3
EAPOL Start Frames.....	0	EAP Req/Id Frames.....	1
EAPOL Logoff Frames.....	0	EAP Request Frames.....	1
EAP Resp/Id Frames.....	2		
EAP Response Frames.....	1		
EAP Length Error Frames....	0		
Invalid EAPOL Frames.....	0		
Supplicant			
Last EAPOL Frame Version.... 0			
Last EAPOL Frame Source..... ff-ff-ff-ff-ff-ff			
Receive		Transmit	
EAPOL Frames.....	0	EAPOL Frames.....	3
EAP Req/Id Frames.....	0	EAPOL Start Frames.....	3
EAP Request Frames.....	0	EAPOL Logoff Frames.....	0
Invalid EAPOL Frames.....	0	EAP Resp/Id Frames.....	0
EAP Length Error Frames....	0	EAP Response Frames.....	0

Interface	スイッチポートのインターフェース名
PAE Type	802.1X 認証におけるスイッチポートの役割。Authenticator、Supplicant、Both のいずれか
Authenticator としての設定	
Last EAPOL Frame Version	最後に受信した EAPOL パケットのバージョン
MAC Address	本ポートに接続されている Supplicant の MAC アドレス
Last EAPOL Frame Source	最後に受信した EAPOL パケットの送信元 MAC アドレス
EAPOL Frames(Receive)	EAPOL パケットの受信総数
EAPOL Start Frames(Receive)	EAPOL-Start パケットの受信数
EAPOL Logoff Frames(Receive)	EAPOL-Logoff パケットの受信数
EAP Resp/Id Frames(Receive)	EAP-Response/Identity パケットの受信数

EAP Response Frames(Receive)	EAP-Response パケットの受信数
EAP Length Error Frames(Receive)	受信した EAP パケットのうち、Length フィールドにエラーがあったものの数
Invalid EAPOL Frames(Receive)	受信した EAPOL パケットのうち、Type フィールドにエラーがあったものの数
EAPOL Frames(Transmit)	EAPOL パケットの送信総数
EAP Req/Id Frames(Transmit)	EAPOL-Request/Identity パケットの送信数
EAP Request Frames(Transmit)	EAP-Request パケットの送信数
Supplicant としての設定	
EAPOL Frames(Receive)	EAPOL パケットの受信数
EAP Req/Id Frames(Receive)	EAPOL-Request/Identity パケットの受信数
EAP Request Frames(Receive)	EAP-Request パケットの受信数
Invalid EAPOL Frames(Receive)	受信した EAPOL パケットのうち、Type フィールドにエラーがあったものの数
EAP Length Error Frames(Receive)	受信した EAP パケットのうち、Length フィールドにエラーがあったものの数
EAPOL Frames(Transmit)	EAPOL パケットの送信総数
EAPOL Start Frames(Transmit)	EAPOL-Start パケットの送信数
EAPOL Logoff Frames(Transmit)	EAPOL-Logoff パケット送信数
EAP Resp/Id Frames(Transmit)	EAP-Response/Identity パケットの送信数
EAP Response Frames(Transmit)	EAP-Response パケットの送信数

表 70:

## 関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE ( 170 ページ )

ENABLE PORTAUTH ( 289 ページ )

ENABLE PORTAUTH PORT ( 291 ページ )

SET PORTAUTH PORT ( 346 ページ )

SET PORTAUTH PORT SUPPLICANTMAC ( 350 ページ )

SHOW PORTAUTH ( 441 ページ )

SHOW PORTAUTH COUNTER ( 444 ページ )

SHOW PORTAUTH MULTISUPPLICANT PORT ( 447 ページ )

SHOW PORTAUTH PORT ( 451 ページ )

SHOW PORTAUTH TIMER ( 456 ページ )

## SHOW PORTAUTH MULTISUPPLICANT PORT

カテゴリー：スイッチング / ポート認証

**SHOW PORTAUTH** [= {8021X|MACBASED}] **MULTISUPPLICANT PORT** = {*port-list*|ALL}  
 [SUPPLICANTMAC=*macadd*]

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

*macadd*: MAC アドレス (xx-xx-xx-xx-xx-xx の形式)

### 解説

802.1X Multi-SupPLICant モードで動作している Authenticator ポート、または、MAC ベース認証ポートの基本設定、および、接続/設定されている SupPLICant の情報を表示する。

### パラメーター

**PORTAUTH** 認証メカニズム。8021X (802.1X 認証)、MACBASED (MAC ベース認証) から選択する。

省略時は 8021X と見なされる。

**PORT** スイッチポート。複数指定が可能。

**SUPPLICANTMAC** SupPLICant の MAC アドレス。

### 入力・出力・画面例

```
Manager > show portauth multisuppllicant port=8
802.1X Multi-SupPLICant Configuration
-----
Interface: port8
Multi-SupPLICant Authenticator
Number of Multi SupPLICants..... 1
  Default Settings
    AuthControlPortControl..... Auto
    quietPeriod..... 60
    txPeriod..... 30
    suppTimeout..... 30
    serverTimeout..... 30
    maxReq..... 2
    reAuthMax..... 2
    reAuthPeriod..... 3600
    reAuthEnabled..... False
    secureVlan..... On
    trap..... None
    mibReset..... Enabled
    vlanAssignment..... Enabled

Attached SupPLICant(s)
```

```

MAC Address..... 00-00-f4-95-30-6a
Authenticator PAE State..... AUTHENTICATED
Port Status..... authorised
Backend Authenticator State... IDLE
AuthControlPortControl..... Auto
quietPeriod..... 60
txPeriod..... 30
suppTimeout..... 30
serverTimeout..... 30
maxReq..... 2
reAuthMax..... 2
reAuthPeriod..... 1800
reAuthEnabled..... True
keyTransmissionEnabled..... False (not supported)
adminControlledDirections.... Both (not supported)
secureVlan..... On
trap..... None
mibReset..... Enabled
vlanAssignment..... Enabled

```

Manager > show portauth=macbased multisuppliant port=9

#### MAC Based Authentication Configuration

Interface: port9

```

PAE Status..... Enabled
Number of Supplicants.... 1
Default Settings
AuthControlPortControl..... Auto
quietPeriod..... 60
reAuthPeriod..... 3600
reAuthEnabled..... False
secureVlan..... On
trap..... None
mibReset..... Enabled
vlanAssignment..... Enabled

```

#### Attached Supplicant(s)

```

MAC Address..... 00-00-f4-22-33-44
Authenticator PAE State..... INITIALISE
Port Status..... unauthorised
Backend Authenticator State... IDLE
AuthControlPortControl..... Auto
quietPeriod..... 60
reAuthPeriod..... 3600
reAuthEnabled..... False
secureVlan..... On
trap..... Both
mibReset..... Enabled
vlanAssignment..... Enabled

```



Default Settings	明示的に設定していない Supplicant に適用される設定値の一覧
Attached Supplicant(s)	明示的に設定した Supplicant に適用される設定値の一覧、および、ポート配下に接続されている Supplicant の情報一覧
Authenticator PAE State	Authenticator としての状態。INITIALISE (初期化)、DISCONNECTED (未接続)、CONNECTING (接続中)、AUTHENTICATING (認証中)、AUTHENTICATED (認証済み)、ABORTING (認証断念中)、HELD (待機中)、FORCEAUTH (「認証済み」に固定設定)、FORCEUNAETH (「未認証」に固定設定) のいずれか
Port Status	ポートの状態。unauthorised (未認証) か authorised (認証済み)
Backend Authenticator State	認証機構の状態。IDLE (アイドル)、INITIALISE (初期化)、RESPONSE (Supplicant から応答受信)、REQUEST (認証サーバーに要求送信)、SUCCESS (認証成功)、FAIL (認証失敗)、TIMEOUT (タイムアウト) のいずれか
AuthControlPortControl	手動設定によるポート状態。Auto (認証結果に応じて変動。通常の設定)、forceUnauthorised (未認証に固定)、forceAuthorised (認証済みに固定) のいずれか
quietPeriod	認証失敗後、Supplicant との通信を拒否する期間 (秒)
txPeriod	Supplicant に EAPOL パケットを再送信する間隔 (秒)
suppTimeout	Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間 (秒)
serverTimeout	RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間 (秒)
maxReq	Supplicant に対する EAPOL-Request パケットの最大再送回数
reAuthMax	再認証時における EAPOL-Request パケットの最大再送回数
reAuthPeriod	Supplicant を再認証する間隔 (秒)
reAuthEnabled	再認証の有効・無効
keyTransmissionEnabled	未サポート
adminControlledDirections	未サポート
secureVlan	ダイナミック VLAN 有効時、2 番目以降に接続された Supplicant の所属 VLAN が、最初に認証を通った Supplicant と同じでないと認証を許可しない機能の有効・無効
trap	ポート認証機能に関する SNMP トラップを送信するかどうか。また、どのようなときに送信するか
mibReset	古い Supplicant 情報をエージアウトするかどうか
vlanAssignment	ダイナミック VLAN の有効・無効

表 71: PORTAUTH=8021X のとき

Default Settings	明示的に設定していない Supplicant に適用される設定値の一覧
Attached Supplicant(s)	明示的に設定した Supplicant に適用される設定値の一覧、および、ポート配下に接続されている Supplicant の情報一覧

Authenticator PAE State	Authenticator としての状態。INITIALISE ( 初期化 )、DISCONNECTED ( 未接続 )、CONNECTING ( 接続中 )、AUTHENTICATING ( 認証中 )、AUTHENTICATED ( 認証済み )、ABORTING ( 認証断念中 )、HELD ( 待機中 )、FORCEAUTH ( 「 認証済み 」 に固定設定 )、FORCEUNAUTH ( 「 未認証 」 に固定設定 ) のいずれか
Port Status	ポートの状態。unauthorised ( 未認証 ) か authorised ( 認証済み )
Backend Authenticator State	認証機構の状態。IDLE ( アイドル )、INITIALISE ( 初期化 )、RESPONSE ( Supplicant から応答受信 )、REQUEST ( 認証サーバーに要求送信 )、SUCCESS ( 認証成功 )、FAIL ( 認証失敗 )、TIMEOUT ( タイムアウト ) のいずれか
AuthControlPortControl	手動設定によるポート状態。Auto ( 認証結果に応じて変動。通常の設定 )、forceUnauthorised ( 未認証に固定 )、forceAuthorised ( 認証済みに固定 ) のいずれか
quietPeriod	認証失敗後、Supplicant との通信を拒否する期間 ( 秒 )
reAuthPeriod	Supplicant を再認証する間隔 ( 秒 )
reAuthEnabled	再認証の有効・無効
secureVlan	ダイナミック VLAN 有効時、2 番目以降に接続された Supplicant の所属 VLAN が、最初に認証を通った Supplicant と同じでないと認証を許可しない機能の有効・無効
trap	ポート認証機能に関する SNMP トラップを送信するかどうか。また、どのようなときに送信するか
mibReset	古い Supplicant 情報をエージアウトするかどうか
vlanAssignment	ダイナミック VLAN の有効・無効

表 72: PORTAUTH=MACBASED のとき

## 関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE ( 170 ページ )

ENABLE PORTAUTH ( 289 ページ )

ENABLE PORTAUTH PORT ( 291 ページ )

SET PORTAUTH PORT ( 346 ページ )

SET PORTAUTH PORT SUPPLICANTMAC ( 350 ページ )

SHOW PORTAUTH ( 441 ページ )

SHOW PORTAUTH COUNTER ( 444 ページ )

SHOW PORTAUTH MULTISUPPLICANT PORT ( 447 ページ )

SHOW PORTAUTH PORT ( 451 ページ )

SHOW PORTAUTH TIMER ( 456 ページ )

## SHOW PORTAUTH PORT

カテゴリー：スイッチング / ポート認証

**SHOW PORTAUTH** [= {8021X|MACBASED}] **PORT**={*port-list*|ALL}

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

指定ポートにおけるポート認証機能 (802.1X 認証、MAC ベース認証) の設定を表示する。

### パラメーター

**PORTAUTH** 認証メカニズム。8021X (802.1X 認証) MACBASED (MAC ベース認証) から選択する。

省略時は 8021X と見なされる。

**PORT** スイッチポート。複数指定が可能。

### 入力・出力・画面例

```
Manager > show portauth=8021x port=1

802.1X Configuration
-----
Interface: port1
  PAE Type..... Authenticator
    Authenticator PAE State..... AUTHENTICATED
    Port Status..... authorised
    Backend Authenticator State... IDLE
    AuthControlPortControl..... Auto
    quietPeriod..... 60
    txPeriod..... 30
    suppTimeout..... 30
    serverTimeout..... 30
    maxReq..... 2
    reAuthMax..... 2
    reAuthPeriod..... 3600
    reAuthEnabled..... False
    piggyBack..... True
    keyTransmissionEnabled..... False (not supported)
    adminControlledDirections..... Both (not supported)
    guestVlan..... None (VLAN ID=0)
    trap..... None
    vlanAssignment..... Enabled

Manager > show portauth=8021x port=7
```

## 802.1X Configuration

Interface: port7

PAE Type..... Both

## Multi-SupPLICant Authenticator

## Default Settings

AuthControlPortControl..... Auto  
 quietPeriod..... 60  
 txPeriod..... 30  
 suppTimeout..... 30  
 serverTimeout..... 30  
 maxReq..... 2  
 reAuthMax..... 2  
 reAuthPeriod..... 3600  
 reAuthEnabled..... False  
 secureVlan..... On  
 trap..... None  
 mibReset..... Enabled  
 vlanAssignment..... Enabled

## Attached SupPLICant(s)

MAC Address..... 00-00-e2-59-56-48  
 Authenticator PAE State..... AUTHENTICATED  
 Port Status..... authorised  
 Backend Authenticator State... IDLE  
 AuthControlPortControl..... Auto  
 quietPeriod..... 60  
 txPeriod..... 30  
 suppTimeout..... 30  
 serverTimeout..... 30  
 maxReq..... 2  
 reAuthMax..... 2  
 reAuthPeriod..... 3600  
 reAuthEnabled..... False  
 keyTransmissionEnabled..... False (not supported)  
 operControlledDirections..... False (not supported)  
 secureVlan..... On  
 trap..... None  
 mibReset..... Enabled  
 vlanAssignment..... Disabled

Manager &gt; show portauth=macbased port=10

## MAC Based Authentication Configuration

Interface: port10

PAE Status..... Enabled

Number of SupPLICants.... 1

## Default Settings

AuthControlPortControl.....	Auto
quietPeriod.....	60
reAuthPeriod.....	3600
reAuthEnabled.....	False
secureVlan.....	On
trap.....	None
mibReset.....	Enabled
vlanAssignment.....	Enabled
Attached Supplicant(s)	
MAC Address.....	00-00-f4-42-01-6b
Authenticator PAE State.....	AUTHENTICATED
Port Status.....	authorised
Backend Authenticator State...	IDLE
AuthControlPortControl.....	Auto
quietPeriod.....	60
reAuthPeriod.....	3600
reAuthEnabled.....	False
secureVlan.....	On
trap.....	None
mibReset.....	Enabled
vlanAssignment.....	Enabled

Interface	スイッチポートのインターフェース名
PAE Type	802.1X 認証におけるスイッチポートの役割。Authenticator、Supplicant、Both のいずれか
	Authenticator としての設定
MAC Address	Supplicant の MAC アドレス
Authenticator PAE State	Authenticator としての状態。INITIALISE (初期化)、DISCONNECTED (未接続)、CONNECTING (接続中)、AUTHENTICATING (認証中)、AUTHENTICATED (認証済み)、ABORTING (認証断念中)、HELD (待機中)、FORCEAUTH (「認証済み」に固定設定)、FORCEUNAUTH (「未認証」に固定設定) のいずれか
Port Status	ポートの状態。unauthorised (未認証) か authorised (認証済み)
Backend Authenticator State	認証機構の状態。IDLE (アイドル)、INITIALISE (初期化)、RESPONSE (Supplicant から応答受信)、REQUEST (認証サーバーに要求送信)、SUCCESS (認証成功)、FAIL (認証失敗)、TIMEOUT (タイムアウト) のいずれか
AuthControlPortControl	手動設定によるポート状態。Auto (認証結果に応じて変動。通常の設定)、forceUnauthorised (未認証に固定)、forceAuthorised (認証済みに固定) のいずれか
quietPeriod	認証失敗後、Supplicant との通信を拒否する期間 (秒)
txPeriod	Supplicant に EAPOL パケットを再送信する間隔 (秒)

suppTimeout	Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間（秒）
serverTimeout	RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間（秒）
maxReq	Supplicant に対する EAPOL-Request パケットの最大再送回数
reAuthMax	再認証時における EAPOL-Request パケットの最大再送回数
reAuthPeriod	Supplicant を再認証する間隔（秒）
reAuthEnabled	再認証の有効・無効
piggyBack	Single-Supplicant モードにおいて、最初に接続された Supplicant の認証に成功した後、他のデバイスからのパケットも許可するかどうか
keyTransmissionEnabled	未サポート
adminControlledDirections	未サポート
secureVlan	ダイナミック VLAN 有効時、2 番目以降に接続された Supplicant の所属 VLAN が、最初に認証を通った Supplicant と同じでないと認証を許可しない機能の有効・無効
trap	ポート認証機能に関する SNMP トラップを送信するかどうか。また、どのようなときに送信するか
mibReset	古い Supplicant 情報をエージアウトするかどうか
vlanAssignment	ダイナミック VLAN の有効・無効
Supplicant としての設定	
heldPeriod	認証失敗後、Authenticator との通信を試みない期間（秒）
authPeriod	Authenticator に EAP-Response パケットを送信した後、Authenticator からの応答を待つ時間（秒）
startPeriod	Authenticator に EAPOL-Start パケットを再送信する間隔（秒）
maxStart	EAPOL-Start パケットの最大送信回数。Supplicant ポートは、EAPOL-Start パケットを MAXSTART 回送信しても応答がない場合、Authenticator が存在しておらずポート認証の必要はないと判断する
Supplicant PAE State	Supplicant としての状態。Authorised と Unauthorised のいずれか

表 73: PORTAUTH=8021X のとき

Interface	スイッチポートのインターフェース名
PAE Status	該当スイッチポートにおける MAC ベース認証の有効・無効
Number of Supplicants	MAC ベース Supplicant の数
MAC Address	Supplicant の MAC アドレス
Authenticator PAE State	Authenticator としての状態。INITIALISE（初期化）、DISCONNECTED（未接続）、CONNECTING（接続中）、AUTHENTICATING（認証中）、AUTHENTICATED（認証済み）、ABORTING（認証断念中）、HELD（待機中）、FORCEAUTH（「認証済み」に固定設定）、FORCEUNAETH（「未認証」に固定設定）のいずれか

Port Status	ポートの状態。unauthorised (未認証) か authorised (認証済み)
Backend Authenticator State	認証機構の状態。IDLE(アイドル) INITIALISE(初期化) RESPONSE (Supplicant から応答受信) REQUEST (認証サーバーに要求送信) SUCCESS (認証成功) FAIL (認証失敗) TIMEOUT (タイムアウト) のいずれか
AuthControlPortControl	手動設定によるポート状態。Auto (認証結果に応じて変動。通常の設定) forceUnauthorised (未認証に固定) forceAuthorised (認証済みに固定) のいずれか
quietPeriod	認証失敗後、Supplicant との通信を拒否する期間 (秒)
reAuthPeriod	Supplicant を再認証する間隔 (秒)
reAuthEnabled	再認証の有効・無効
secureVlan	ダイナミック VLAN 有効時、2 番目以降に接続された Supplicant の所属 VLAN が、最初に認証を通った Supplicant と同じでないと認証を許可しない機能の有効・無効
trap	ポート認証機能に関する SNMP トラップを送信するかどうか。また、どのようなときに送信するか
mibReset	古い Supplicant 情報をエージアウトするかどうか
vlanAssignment	ダイナミック VLAN の有効・無効

表 74: PORTAUTH=MACBASED のとき

## 関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (170 ページ)

ENABLE PORTAUTH (289 ページ)

ENABLE PORTAUTH PORT (291 ページ)

SET PORTAUTH PORT (346 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (350 ページ)

SHOW PORTAUTH (441 ページ)

SHOW PORTAUTH COUNTER (444 ページ)

SHOW PORTAUTH MULTISUPPLICANT PORT (447 ページ)

SHOW PORTAUTH PORT (451 ページ)

SHOW PORTAUTH TIMER (456 ページ)

SHOW PORTAUTH TIMER

カテゴリー：スイッチング / ポート認証

**SHOW PORTAUTH** [= {8021X|MACBASED}] **TIMER PORT**={*port-list*|ALL}

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

解説

指定ポートにおけるポート認証機能 (802.1X 認証または MAC ベース認証) の各種タイマー (残り時間) を表示する。

パラメーター

**PORTAUTH** 認証メカニズム。8021X (802.1X 認証) MACBASED (MAC ベース認証) から選択する。  
省略時は 8021X と見なされる。  
**PORT** スイッチポート。複数指定が可能。

入力・出力・画面例

```

Manager > show portauth=8021x timer port=7
802.1X Timers
-----
Interface: port7                                PAE Type..... Both

Authenticator
  aWhile      quietWhile      reAuthWhen      txWhen
  00          00000          00048          00000

Supplicant
  authWhile    heldWhile      startWhen
  00           00000          20

Manager > show portauth=8021x timer port=8
802.1X Timers
-----
Interface: port7                                PAE Type..... Both

Attached Supplicant: 00-00-e2-59-56-48
  aWhile      quietWhile      reAuthWhen      txWhen
  00          00000          00000          00000

Attached Supplicant: 00-00-f4-95-30-6a
  aWhile      quietWhile      reAuthWhen      txWhen
  00          00000          00000          00000

```



Supplicant		
authWhile	heldWhile	startWhen
00	00000	26

Manager > show portauth=macbased timer port=2

MAC Based Authentication Timers

---

Interface: port2

Supplicant	quietWhile	reAuthWhen
-----	-----	-----
00-00-f4-42-01-6b	00000	00000

Interface	スイッチポートのインターフェース名
PAE Type	802.1X 認証におけるスイッチポートの役割。Authenticator、Supplicant、Both のいずれか
Authenticator 用タイマー	
aWhile	Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間（秒）。または、RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間（秒）。前者の初期値は SUPPTIMEOUT パラメーターの値、後者の初期値は SERVERTIMEOUT パラメーターの値となる
quietWhile	認証失敗後、Supplicant との通信を拒否する期間（秒）を示すタイマー。QUIETPERIOD パラメーターの値が初期値となる
reAuthWhen	Supplicant を再認証するまでの残り時間（秒）。REAUTHPERIOD パラメーターの値が初期値となる
txWhen	Supplicant に EAPOL パケットを再送信するまでの待ち時間（秒）。TXPERIOD パラメーターの値が初期値となる
Supplicant 用タイマー	
authWhile	Authenticator に EAP-Response パケットを送信した後、Authenticator からの応答を待つ時間（秒）。AUTHPERIOD パラメーターの値が初期値となる
heldWhile	認証失敗後、Authenticator との通信を試みない期間（秒）を示すタイマー。HELDPERIOD パラメーターの値が初期値となる
startWhen	Authenticator に EAPOL-Start パケットを送信するまでの待ち時間（秒）。STARTPERIOD パラメーターの値が初期値となる

表 75: PORTAUTH=8021X のとき

Interface	スイッチポートのインターフェース名
Supplicant	MAC ベース Supplicant の MAC アドレス
quietWhile	認証失敗後、Supplicant との通信を拒否する期間（秒）を示すタイマー。QUI-ETPERIOD パラメーターの値が初期値となる

reAuthWhen	Supplicant を再認証するまでの残り時間 ( 秒 )。 REAUTHPERIOD パラメーターの値が初期値となる
------------	--

表 76: PORTAUTH=MACBASE のとき

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE ( 170 ページ )

ENABLE PORTAUTH ( 289 ページ )

ENABLE PORTAUTH PORT ( 291 ページ )

SET PORTAUTH PORT ( 346 ページ )

SET PORTAUTH PORT SUPPLICANTMAC ( 350 ページ )

SHOW PORTAUTH ( 441 ページ )

SHOW PORTAUTH COUNTER ( 444 ページ )

SHOW PORTAUTH MULTISUPPLICANT PORT ( 447 ページ )

SHOW PORTAUTH PORT ( 451 ページ )

SHOW PORTAUTH TIMER ( 456 ページ )

SHOW QOS DEFAULTPRIORITY

カテゴリー：スイッチング / QoS

SHOW QOS DEFAULTPRIORITY

解説

受信時にタグなしだったパケットをタグ付きポートから送信するときの 802.1p ユーザープライオリティー値の設定を表示する。

入力・出力・画面例

```
Manager > show qos defaultpriority

QOS Queue to Vlan Tag User Priority Mapping
-----

Queue      user priority
-----
0           1
1           2
2           0
3           3
4           4
5           5
6           6
7           7
-----
```

Queue	パケットが格納されている送信キュー番号（デフォルト送信キュー）
UserPriority	送信パケットに割り当てる 802.1p ユーザープライオリティー値

表 77:

関連コマンド

SET QOS DEFAULTPRIORITY ( 356 ページ )

## SHOW QOS DSCPMAP

カテゴリー：スイッチング / QoS

**SHOW QOS DSCPMAP** [= {PREMARKING|REMARKING}] [DSCP=*dscp-list*]

*dscp-list*: DSCP 値 (0~63。ハイフン、カンマを使った複数指定も可能)

### 解説

DSCPMAP テーブルの内容を表示する。

### パラメーター

**DSCPMAP** DSCPMAP テーブルの種類。PREMARKING (プレマーキング用)、REMARKING (リマーキング用) から選択する。省略時は両方が表示される。

**DSCP** テーブルのインデックスとしての DSCP 値。本パラメーターを指定した場合は、該当するエントリだけが表示される。省略時はすべてのエントリが表示される。

### 入力・出力・画面例

```
Manager > show qos dscpmap dscp=63
```

DSCP-based QOS Marking Parameters

DSCP/Markvalue 63

BandwidthClass	1	2	3
-----			
NewDSCP	63	-	-
NewBandwidthClass	1	-	-
NewQueue	0	-	-
NewPriority	0	-	-
-----			

DSCP-based QOS Remarking Parameters

DSCP/Markvalue 63

BandwidthClass	1	2	3
-----			
NewDSCP	63	63	63
NewBandwidthClass	1	2	3
NewQueue	0	0	0
NewPriority	0	0	0
-----			

DSCP-based QOS Marking Parameters	プレマールキング用 DSCP テーブルのエントリーが表示される
DSCP-based QOS Remarking Parameters	リマールキング用 DSCP テーブルのエントリーが表示される
DSCP/Markvalue	テーブルインデックスとしての DSCP 値 (MARKVALUE パラメーター値)
BandwidthClass	テーブルインデックスとしての帯域クラス (プレマールキング用 DSCP テーブルには、帯域クラス 1 のエントリーしか存在しない)
NewDSCP	対象パケットに割り当てる新しい DSCP 値
NewBandwidthClass	対象パケットに割り当てる新しい帯域クラス
NewQueue	対象パケットに割り当てる新しい送信キュー
NewPriority	対象パケットに割り当てる新しい 802.1p ユーザープライオリティー値

表 78:

関連コマンド

SET QOS DSCPMAP ( 357 ページ )

SHOW QOS FLOWGROUP

カテゴリー：スイッチング / QoS

SHOW QOS FLOWGROUP [= { flow-id | ALL }]

flow-id: フローグループ番号 (0~1023)

解説

フローグループの設定内容を表示する。

パラメーター

FLOWGROUP    フローグループ番号

入力・出力・画面例

```
Manager > show qos flowgroup

Flow Group Information
  Id      Description      Assigned TC    Classifiers
-----
  1              1          1-4
  2              1          5-6

Manager > show qos flowgroup=1

Identifier ..... 1
Description .....
TC Assigned to ..... 1
Classifiers ..... 1-4
Premarking ..... USEMARKVALUE
Mark Value ..... 1
Action ..... None
```

Id	フローグループ番号
Description	説明 (メモ)
Assigned TC	割り当て先のトラフィッククラス
Classifiers	割り当てられているクラシファイア

表 79: 番号省略時

Identifier	フローグループ番号
Description	説明 (メモ)
TC Assigned to	割り当て先のトラフィッククラス
Classifiers	割り当てられているクラシファイア
Premarking	プレマーキング動作。USEMARKVALUE (Mark Value をインデックスとして DSCPMAP テーブルを検索)、USEDSCP (パケットの DSCP 値をインデックスとして DSCPMAP テーブルを検索)、NONE (プレマーキングを行わない) のいずれか
Mark Value	プレマーキング動作が USEMARKVALUE の場合に、DSCPMAP テーブルの検索インデックスとして使う DSCP 値
Action	本フローグループに対するアクション。None、FORWARD、DISCARD、SEND-VLANPORT、SENDMIRROR がある
VLAN	本フローグループに属するパケットの出力先 VLAN。Action が「SENDVLANPORT」のときだけ表示される
PORT	本フローグループに属するパケットの出力先ポート。Action が「SENDVLANPORT」のときだけ表示される

表 80: 番号指定時

### 関連コマンド

ADD QOS FLOWGROUP ( 179 ページ )  
 CREATE QOS FLOWGROUP ( 209 ページ )  
 DELETE QOS FLOWGROUP ( 231 ページ )  
 DESTROY QOS FLOWGROUP ( 246 ページ )  
 SET QOS FLOWGROUP ( 359 ページ )



## SHOW QOS POLICY

カテゴリー：スイッチング / QoS

**SHOW QOS POLICY** [= {*qos-id* | ALL}]

*qos-id*: QoS ポリシー番号 (0~255)

### 解説

QoS ポリシーの設定内容を表示する。

### パラメーター

**POLICY** QoS ポリシー番号

### 入力・出力・画面例

```
Manager > show qos policy
```

QOS Policy Information

Id	Description	Trafficclasses	Ports Assigned to
1		1-2	Port: 1-52

```
Manager > show qos policy=1
```

```
Identifier ..... 1
Description .....
TCs Assigned ..... 1-2
Port Assigned to ..... 1-52
```

Default Traffic Class:

```
Minimum Bandwidth ..... 1000 Kbps
Minimum Burst Size ..... 0 b
Maximum Bandwidth ..... 2000 Kbps
Maximum Burst Size ..... 0 b
Drop BandwidthClass3 ..... No
Ignore BandwidthClass ..... No
Premarking ..... None
Remarking ..... None
Mark value ..... None
Action ..... FORWARD
```

Id	QoS ポリシー番号
Description	説明 (メモ)
Trafficclasses	割り当てられているトラフィッククラス
Ports Assigned to	割り当て先のスイッチポート。IPv6 アクセラレーターボードに適用されているときは ACCELERATOR と表示される

表 81: 番号省略時

Identifier	QoS ポリシー番号
Description	説明 (メモ)
TCs Assigned	割り当てられているトラフィッククラス
Port Assigned to	割り当て先のスイッチポート。IPv6 アクセラレーターボードに適用されているときは ACCELERATOR と表示される
Default Traffic Class セクション	本ポリシーのデフォルトトラフィックに関する設定値が表示される
Minimum Bandwidth	最小帯域幅
Minimum Burst Size	最小帯域幅に対する「帯域クラス 1」の最大許容バーストサイズ、あるいは、最大帯域幅に対する「帯域クラス 2」の最大許容バーストサイズ
Maximum Bandwidth	最大帯域幅
Maximum Burst Size	最大帯域幅に対する最大許容バーストサイズ
Drop BandwidthClass3	最大帯域設定を上回るレートで受信したパケットをキューイング前に無条件で破棄するかどうか
Ignore BandwidthClass	最大・最小帯域の設定がなされているとき、メータリング時にプレマーキングで割り当てられた帯域クラスを無視するかどうか
Premarking	プレマーキング動作。USEMARKVALUE (Mark Value をインデックスとして DSCPMAP テーブルを検索)、USEDSCP (パケットの DSCP 値をインデックスとして DSCPMAP テーブルを検索)、NONE (プレマーキングを行わない) のいずれか
Remarking	リマーキング動作。BWCLASS (リマーキング直前の帯域クラスを最終的な帯域クラスとして採用)、PRIO+BWCLASS (リマーキング直前の帯域クラスを最終的な帯域クラスとして採用。また、リマーキング直前の送信キューと帯域クラスをインデックスとして QUEUE2PRIOMAP テーブルを検索し、802.1p プライオリティー値を決定)、PRIORITY (リマーキング直前の送信キューと帯域クラスをインデックスとして QUEUE2PRIOMAP テーブルを検索し、802.1p プライオリティー値を決定)、USEDSCPMAP (リマーキング直前の帯域クラスとパケットの DSCP 値をインデックスとして DSCPMAP テーブルを検索し、最終的な DSCP 値、帯域クラス、送信キュー、802.1p プライオリティー値を決定)、NONE (リマーキングを行わない) のいずれか

Mark Value	プレマーキング動作が USEMARKVALUE の場合、プレマーキング用 DSCP MAP テーブルの検索インデックスとして使う DSCP 値
Action	デフォルトトラフィッククラスに対するアクション。FORWARD、DISCARD、SENDVLANPORT、SENDMIRROR がある
VLAN	デフォルトトラフィッククラスに属するパケットの出力先 VLAN。Action が「SENDVLANPORT」のときだけ表示される
PORT	デフォルトトラフィッククラスに属するパケットの出力先ポート。Action が「SENDVLANPORT」のときだけ表示される

表 82: 番号指定時

関連コマンド

ADD QOS POLICY ( 180 ページ )

CREATE QOS POLICY ( 212 ページ )

DELETE QOS POLICY ( 232 ページ )

DESTROY QOS POLICY ( 247 ページ )

SET QOS POLICY ( 361 ページ )

SET QOS PORT ( 365 ページ )

## SHOW QOS PORT

カテゴリー：スイッチング / QoS

**SHOW QOS PORT** [= {*port-list* | ALL}] [EGRESSQUEUE=*queue-list*]

*port-list*: スイッチポート番号 (1~。ハイフン、カンマを使った複数指定も可能)

*queue-list*: 送信キュー (0~7。ハイフン、カンマを使った複数指定も可能)

### 解説

スイッチポートの QoS 設定を表示する。

### パラメーター

**PORT** スイッチポート番号。

**EGRESSQUEUE** 送信キュー。値を指定しなかった場合は、すべての送信キューが表示される。

### 入力・出力・画面例

```
Manager > show qos port=1

QOS Port Configuration

Port.....1
Policy Assigned.....1 ()
Default Queue.....2
Force Default Queue.....No
Red Curve.....1

Egress Queue Configuration:

Egress Queue 0
  Status ..... ENABLED
  Queue length ..... 128
  Maximum Bandwidth..... None
  Scheduler..... Strict
  WRR Weight..... 6

Egress Queue 1
  Status ..... ENABLED
  Queue length ..... 128
  Maximum Bandwidth..... None
  Scheduler..... Strict
  WRR Weight..... 6

Egress Queue 2
```

```

Status ..... ENABLED
Queue length ..... 128
Maximum Bandwidth..... None
Scheduler..... Strict
WRR Weight..... 6

Egress Queue 3
Status ..... ENABLED
Queue length ..... 128
Maximum Bandwidth..... None
Scheduler..... Strict
WRR Weight..... 6

Egress Queue 4
Status ..... ENABLED
Queue length ..... 128
Maximum Bandwidth..... None
Scheduler..... Strict
WRR Weight..... 6

Egress Queue 5
Status ..... ENABLED
Queue length ..... 128
Maximum Bandwidth..... None
Scheduler..... Strict
WRR Weight..... 6

Egress Queue 6
Status ..... ENABLED
Queue length ..... 128
Maximum Bandwidth..... None
Scheduler..... Strict
WRR Weight..... 6

Egress Queue 7
Status ..... ENABLED
Queue length ..... 128
Maximum Bandwidth..... None
Scheduler..... Strict
WRR Weight..... 6

```

Port	スイッチポート番号
Policy Assigned	割り当てられている QoS ポリシー
Default Queue	タグなしパケットに割り当てるデフォルトの送信キュー番号
Force Default Queue	すべてのパケットにデフォルトの送信キュー（Default Queue）を割り当てるかどうか
Red Curve	割り当てられている RED カーブセット

Egress Queue	送信キュー番号
Status	送信キューの有効・無効
Queue length	キュー長（パケット数）
Maximum Bandwidth	キューの最大帯域幅
Scheduler	キューのスケジューリング方式( 所属するスケジューリンググループ ), Strict、WRR1、WRR2 のいずれか
WRR Weight	WRR1、WRR2 スケジューリンググループにおける、キューの重み付け値（キュー間の送信比率）

表 83:

### 関連コマンド

DISABLE SWITCH PORT EGRESSQUEUE ( 276 ページ )

ENABLE SWITCH PORT EGRESSQUEUE ( 306 ページ )

SET QOS PORT ( 365 ページ )

SET QOS PORT EGRESSQUEUE ( 367 ページ )

SHOW QOS PRIO2QUEUEMAP

カテゴリー：スイッチング / QoS

SHOW QOS PRIO2QUEUEMAP

解説

タグ付きパケットの 802.1p ユーザープライオリティー値と、本製品の送信キューのマッピングを表示する。

入力・出力・画面例

```
Manager > show qos prio2queuemap

Vlan Tag user Priority to Queue Mapping
-----

User Priority      Queue
-----
0                  2
1                  0
2                  1
3                  3
4                  4
5                  5
6                  6
7                  7
-----
```

User Priority	タグ付きパケットの 802.1p ユーザープライオリティー値
Queue	タグ付きパケットに割り当てる送信キュー番号

表 84:

関連コマンド

SET QOS PRIO2QUEUEMAP ( 369 ページ )

## SHOW QOS QUEUE2PRIOMAP

カテゴリー：スイッチング / QoS

**SHOW QOS QUEUE2PRIOMAP** [QUEUE=queue-list]

*queue-list*: 送信キュー（0～7。ハイフン、カンマを使った複数指定も可能）

### 解説

リマーキング時に使用される 802.1p ユーザープライオリティー値の書き換えテーブル（QUEUE2PRIOMAP テーブル）の内容を表示する。

### パラメーター

**QUEUE** 送信キュー。値を指定しなかった場合は、すべての送信キューが表示される。

### 入力・出力・画面例

Manager > show qos queue2priomap			
DSCP-based QOS Remarking Parameters			
Queue 0			
BandwidthClass	1	2	3
-----			
NewPriority	0	0	0
-----			
Queue 1			
BandwidthClass	1	2	3
-----			
NewPriority	0	0	0
-----			
Queue 2			
BandwidthClass	1	2	3
-----			
NewPriority	0	0	0
-----			
Queue 3			
BandwidthClass	1	2	3
-----			
NewPriority	0	0	0
-----			



Queue 4			
BandwidthClass	1	2	3
-----			
NewPriority	0	0	0
-----			
Queue 5			
BandwidthClass	1	2	3
-----			
NewPriority	0	0	0
-----			
Queue 6			
BandwidthClass	1	2	3
-----			
NewPriority	0	0	0
-----			
Queue 7			
BandwidthClass	1	2	3
-----			
NewPriority	0	0	0
-----			

Queue	パケットが格納されている送信キュー番号
BandwidthClass	パケットに割り当てられている帯域クラス
NewPriority	パケットに割り当てる新しい802.1p ユーザープライオリティ値

表 85:

関連コマンド

SET QOS QUEUE2PRIOMAP ( 370 ページ )

## SHOW QOS RED

カテゴリー：スイッチング / QoS

**SHOW QOS RED** [= {*red-id* | ALL}] [QUEUE=*queue-list*]

*red-id*: RED カーブセット番号 (1~4)

*queue-list*: 送信キュー (0~7。ハイフン、カンマを使った複数指定も可能)

### 解説

RED (Random Early Detection/Discard) カーブセットの設定内容を表示する。

### パラメーター

**RED** RED カーブセット番号。指定した場合は該当 RED カーブセットの詳細設定を表示する。番号を指定しなかった場合は、RED カーブセットの一覧を表示する。

**QUEUE** 送信キュー。値を指定しなかった場合は、すべての送信キューが対象となる。

### 入力・出力・画面例

```
Manager > show qos red
```

```
Random Early Detection Information
```

Id	Description	Assigned Ports	Ports Using Tail Drop
1	Default	0-47	48-51
2	Test RED set	None	None

```
Manager > show qos red=1
```

```
Identifier ..... 1 (default)
```

```
Description ..... Default
```

```
Ports Assigned to ..... 0-47
```

```
Ports using Tail-Drop..... 48-51
```

```
Queue 0
```

```
Queue length averaging factor ... 9
```

BandwidthClass	Start	Stop	Drop Probability Factor
1	25 Kb	30 Kb	1 (50%)
2	15 Kb	25 Kb	1 (50%)
3	5 Kb	15 Kb	1 (50%)

```
Queue 1
```

Queue length averaging factor ... 9				
BandwidthClass	Start	Stop	Drop Probability Factor	
1	25 Kb	30 Kb	1	(50%)
2	15 Kb	25 Kb	1	(50%)
3	5 Kb	15 Kb	1	(50%)
-----				
Queue 2				
Queue length averaging factor ... 9				
BandwidthClass	Start	Stop	Drop Probability Factor	
1	25 Kb	30 Kb	1	(50%)
2	15 Kb	25 Kb	1	(50%)
3	5 Kb	15 Kb	1	(50%)
-----				
Queue 3				
Queue length averaging factor ... 9				
BandwidthClass	Start	Stop	Drop Probability Factor	
1	25 Kb	30 Kb	1	(50%)
2	15 Kb	25 Kb	1	(50%)
3	5 Kb	15 Kb	1	(50%)
-----				
Queue 4				
Queue length averaging factor ... 9				
BandwidthClass	Start	Stop	Drop Probability Factor	
1	25 Kb	30 Kb	1	(50%)
2	15 Kb	25 Kb	1	(50%)
3	5 Kb	15 Kb	1	(50%)
-----				
Queue 5				
Queue length averaging factor ... 9				
BandwidthClass	Start	Stop	Drop Probability Factor	
1	25 Kb	30 Kb	1	(50%)
2	15 Kb	25 Kb	1	(50%)
3	5 Kb	15 Kb	1	(50%)
-----				
Queue 6				
Queue length averaging factor ... 9				
BandwidthClass	Start	Stop	Drop Probability Factor	
1	25 Kb	30 Kb	1	(50%)
2	15 Kb	25 Kb	1	(50%)
3	5 Kb	15 Kb	1	(50%)

```
-----
Queue 7
```

```
Queue length averaging factor ... 9
```

```
BandwidthClass    Start          Stop          Drop Probability Factor
```

```
-----
1                25 Kb          30 Kb          1    (50%)
```

```
2                15 Kb          25 Kb          1    (50%)
```

```
3                5 Kb           15 Kb          1    (50%)
-----
```

Id	RED カーブセット番号
Description	説明 (メモ)
Assigned Ports	割り当て先のスイッチポート
Ports Using Tail Drop	Tail-drop アルゴリズムを使用しているスイッチポート

表 86: 番号省略時

Identifier	RED カーブセット番号
Description	説明 (メモ)
Ports Assigned to	割り当て先のスイッチポート
Ports using Tail-Drop	Tail-drop アルゴリズムを使用しているスイッチポート
Queue	送信キュー番号
Queue length averaging factor	平均キュー長の算出に使う期間を示す係数
BandwidthClass	帯域クラス
Start	該当帯域クラスの packets を破棄し始めるキュー長
Stop	該当帯域クラスの packets を完全に破棄するキュー長
Drop Probability Factor	キュー長が Stop のときの該当帯域クラスの packets 破棄率を決める係数 (カッコ内は係数から求めた実際の破棄率 (%))

表 87: 番号指定時

## 関連コマンド

CREATE QOS RED ( 216 ページ )

DESTROY QOS RED ( 248 ページ )

SET QOS RED ( 371 ページ )

## SHOW QOS TRAFFICCLASS

カテゴリー：スイッチング / QoS

**SHOW QOS TRAFFICCLASS** [= {*tc-id* | ALL}]

*tc-id*: トラフィッククラス番号 (0~1023)

### 解説

トラフィッククラスの設定内容を表示する。

### パラメーター

**TRAFFICCLASS**    トラフィッククラス番号

### 入力・出力・画面例

```
Manager > show qos trafficclass
```

QOS Traffic Class Information

Id	Description	Policy	FlowGroups
1		1	1-2
2		1	3

```
Manager > show qos trafficclass=1
```

```
Identifier ..... 1
Description .....
Policy Assigned to ..... 1
Flow Groups ..... 1-2
Drop BandwidthClass3 ..... No
Ignore BandwidthClass ..... No
Minimum Bandwidth ..... 1500 Kbps
Minimum Burst Size ..... 0 b
Maximum Bandwidth ..... 3000 Kbps
Maximum Burst Size ..... 0 b
Premarking ..... None
Remarking ..... None
Mark Value ..... None
Action ..... FORWARD
```

Id

トラフィッククラス番号

Description	説明（メモ）
Policy	割り当て先の QoS ポリシー
FlowGroups	割り当てられているフローグループ

表 88: 番号省略時

Identifier	トラフィッククラス番号
Description	説明（メモ）
Policy Assigned to	割り当て先の QoS ポリシー
Flow Groups	割り当てられているフローグループ
Drop BandwidthClass3	最大帯域設定を上回るレートで受信したパケットを無条件で破棄するかどうか
Ignore BandwidthClass	最大・最小帯域の設定がなされているとき、メータリング時にプレマーキングで割り当てられた帯域クラスを無視するかどうか
Minimum Bandwidth	最小帯域幅
Minimum Burst Size	最小帯域幅に対する「帯域クラス 1」の最大許容バーストサイズ、あるいは、最大帯域幅に対する「帯域クラス 2」の最大許容バーストサイズ
Maximum Bandwidth	最大帯域幅
Maximum Burst Size	最大帯域幅に対する最大許容バーストサイズ
Premarking	プレマーキング動作。USEMARKVALUE（Mark Value をインデックスとして DSCPMAP テーブルを検索）、USEDSCP（パケットの DSCP 値をインデックスとして DSCPMAP テーブルを検索）、NONE（プレマーキングを行わない）のいずれか
Remarking	リマーキング動作。BWCLASS（リマーキング直前の帯域クラスを最終的な帯域クラスとして採用）、PRIO+BWCLASS（リマーキング直前の帯域クラスを最終的な帯域クラスとして採用。また、リマーキング直前の送信キューと帯域クラスをインデックスとして QUEUE2PRIOMAP テーブルを検索し、802.1p プライオリティー値を決定）、PRIORITY（リマーキング直前の送信キューと帯域クラスをインデックスとして QUEUE2PRIOMAP テーブルを検索し、802.1p プライオリティー値を決定）、USEDSCPMAP（リマーキング直前の帯域クラスとパケットの DSCP 値をインデックスとして DSCPMAP テーブルを検索し、最終的な DSCP 値、帯域クラス、送信キュー、802.1p プライオリティー値を決定）、NONE（リマーキングを行わない）のいずれか

Mark Value	プレマーキング動作が USEMARKVALUE の場合、プレマーキング用 DSCPMAP テーブルの検索インデックスとして使う DSCP 値
Action	本トラフィッククラスに対するアクション。FORWARD、DISCARD、SENDVLANPORT、SENDMIRROR がある
VLAN	本トラフィッククラスに属するパケットの出力先 VLAN。Action が「SENDVLANPORT」のときだけ表示される
PORT	本トラフィッククラスに属するパケットの出力先ポート。Action が「SENDVLANPORT」のときだけ表示される

表 89: 番号指定時

### 関連コマンド

ADD QOS TRAFFICCLASS ( 181 ページ )

CREATE QOS TRAFFICCLASS ( 218 ページ )

DELETE QOS TRAFFICCLASS ( 233 ページ )

DESTROY QOS TRAFFICCLASS ( 249 ページ )

SET QOS TRAFFICCLASS ( 373 ページ )

## SHOW STP

カテゴリー：スイッチング / スパニングツリープロトコル (STP/RSTP)

**SHOW STP** [= {*stpname*|ALL}] [SUMMARY]

*stpname*: STP ドメイン名 (1~15 文字。英数字とアンダースコア (-)、ハイフンを使用可能。大文字小文字を区別しない)

### 解説

STP ドメインの設定情報を表示する。

### パラメーター

**STP** STP ドメイン名。省略時および ALL 指定時はすべての STP ドメインの情報が表示される。

**SUMMARY** STP ドメインの情報を簡潔に一覧表示する。

### 入力・出力・画面例

```
Manager > show stp

STP Information
-----
Name ..... default
Mode ..... Standard
RSTP Type ..... (n/a)
VLAN members ..... default (1)
                        white (10)
                        orange (20)
                        beige (30)
                        uplink (1000)
Status ..... ON
Number of Ports ..... 24
  Number Enabled ..... 24
  Number Disabled ..... 0
Bridge Identifier ..... 32768 : 00-90-99-40-4f-00
Bridge Priority ..... 32768
Designated Root ..... 32768 : 00-90-99-40-4f-00
Root Port ..... (n/a)
Root Path Cost ..... 0
Max Age ..... 20
Hello Time ..... 2
Forward Delay ..... 15
Switch Max Age ..... 20
Switch Hello Time ..... 2
Switch Forward Delay .. 15
```



```

Hold Time ..... 1
TC ..... False
TC Detected ..... False
Number of TC ..... 1
Time since last TC .... 126

```

```

Manager > show stp

```

#### STP Information

```

Name ..... default
Mode ..... Rapid
RSTP Type ..... Normal
VLAN members ..... default (1)
                  alpha (10)
                  beta (20)
Status ..... ON
Number of Ports ..... 16
  Number Enabled ..... 16
  Number Disabled ..... 0
Bridge Identifier ..... 32768 : 00-00-cd-08-17-0c
Bridge Priority ..... 32768
Root Bridge ..... 32768 : 00-00-cd-08-17-0c
Designated Bridge ..... 32768 : 00-00-cd-08-17-0c
Root Port ..... (n/a)
Root Path Cost ..... 0
Max Age ..... 20
Hello Time ..... 2
Forward Delay ..... 15
Switch Max Age ..... 20
Switch Hello Time ..... 2
Switch Forward Delay .. 15
Transmission Limit .... 3
Number of TC ..... 1
Time since last TC .... 112

```

```

Manager > show stp summary

```

STP Name	Mode	Ports Enabled	Ports Disabled	Bridge Role
default	Standard	24	0	Root Bridge

Name	STP ドメイン名
Mode	STP の動作モード。Standard ( 802.1d ) か Rapid ( 802.1w )

RSTP Type	Rapid STP の動作モード。Normal か STP Compatible
VLAN members	所属 VLAN。カッコ内は VLAN ID
Status	STP ドメインの状態。ON か OFF
Number of Ports	STP ドメインに所属しているポートの総数
Number Enabled	イネーブル状態のポート数
Number Disabled	ディセーブル状態のポート数
Bridge Identifier	ブリッジ識別子。ブリッジプライオリティと MAC アドレスで構成される
Bridge Priority	ブリッジプライオリティ
Designated Root	ルートブリッジのブリッジ識別子。Standard モードのときだけ表示される
Root Bridge	ルートブリッジのブリッジ識別子。Rapid モードのときだけ表示される
Designated Bridge	代表ブリッジのブリッジ識別子。Rapid モードのときだけ表示される
Root Port	ルートポートの番号。ルートブリッジのときは (n/a) と表示される
Root Path Cost	ルートパスコスト。ルートブリッジまでのパスコスト
Max Age	最大エージタイム (秒)。ルートブリッジによって決定された値
Hello Time	ハロータイム (秒)。ルートブリッジによって決定された値
Forward Delay	フォワードディレイタイム (秒)。ルートブリッジによって決定された値
Switch Max Age	本機の最大エージタイム設定値 (SET STP コマンドの MAXAGE パラメーター)。ルートブリッジになったときにこの値が使用される
Switch Hello Time	本機のハロータイム設定値 (SET STP コマンドの HELLOTIME パラメーター)。ルートブリッジになったときにこの値が使用される
Switch Forward Delay	本機のフォワードディレイタイム設定値 (SET STP コマンドの FORWARD-DELAY パラメーター)。ルートブリッジになったときにこの値が使用される
Hold Time	ルートブリッジが Configuration BPDU を送信するときの最小送信間隔 (秒)。この値は標準規格で規定されており、1 秒固定に設定されている。Standard モードのときだけ表示される。
Transmission Limit	ハロータイムの間に送信可能な BPDU の数。この値は標準規格で規定されており、3 で固定に設定されている。Rapid モードのときだけ表示される
TC	ルートブリッジのときは、TC ビットを付けた BPDU を送信している時に True、その他の場合は False。ルートブリッジでないときは、TC ビットを付けた BPDU を受信している時に True、その他の場合は False となる。Standard モードのときだけ表示される
TC Detected	ルートブリッジのときは、TCN を送信または受信して TC ビットを付けた BPDU を送信している時に True、その他の場合は False。ルートブリッジでないときは、TCN を送信した時に True、その他の場合は False となる。Standard モードのときだけ表示される

Number of TC	Topology Change が発生した回数
Time since last TC	最後に Topology Change が発生してから経過した時間

表 90:

STP Name	STP ドメイン名
Mode	STP の動作モード。Standard ( 802.1d ) か Rapid ( 802.1w )
Ports Enabled	イネーブル状態のポート数
Ports Disabled	ディセーブル状態のポート数
Bridge Role	STP ドメインにおける役割。None、Designated、Root のいずれか

表 91: SUMMARY オプション指定時

### 関連コマンド

CREATE STP ( 222 ページ )

DESTROY STP ( 250 ページ )

DISABLE STP ( 265 ページ )

ENABLE STP ( 295 ページ )

SET STP ( 377 ページ )

SHOW STP COUNTER ( 484 ページ )

SHOW STP PORT ( 487 ページ )

SHOW STP COUNTER

カテゴリー：スイッチング / スパニングツリープロトコル (STP/RSTP)

**SHOW STP** [= {stpname|ALL}] **COUNTER**

*stpname*: STP ドメイン名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

解説

STP ドメインの統計カウンターを表示する。

パラメーター

**STP** STP ドメイン名。省略時および ALL 指定時はすべての STP ドメインの統計カウンターが表示される。

入力・出力・画面例

```
Manager > show stp counter

STP Counters
-----
STP Name: default
Receive:
Total STP Packets          351
Configuration BPDU         351
TCN BPDU                   0
Invalid BPDU                0

Transmit:
Total STP Packets          544
Configuration BPDU         544
TCN BPDU                   0

Discarded:
Port Disabled              0
Invalid Protocol           0
Invalid Type               0
Invalid Message Age        0
Config BPDU length         0
TCN BPDU length            0
-----
```

STP Name	STP ドメイン名
Receive セクション	受信パケット数が表示される
Total STP Packets	受信した STP パケット ( Configuration BPDU と Topology Change Notification BPDU ) の総数

Configuration BPDU	Configuration BPDU 受信数
TCN BPDU	Topology Change Notification BPDU 受信数
Invalid BPDU	無効な STP パケット受信数
Transmit セクション	送信パケット数が表示される
Total STP Packets	送信した STP パケット ( Configuration BPDU と Topology Change Notification BPDU ) の総数
Configuration BPDU	Configuration BPDU 送信数
TCN BPDU	Topology Change Notification BPDU 送信数
Discarded セクション	破棄されたパケット数が表示される
Port Disabled	受信ポートがディセーブル状態だったために破棄された BPDU の数
Invalid Protocol	プロトコル ID フィールドかプロトコルバージョン ID フィールドの値が無効であったため破棄された STP パケット数
Invalid Type	Type フィールドの値が無効であったため破棄された STP パケット数
Invalid Message Age	メッセージエージが無効であったため破棄された STP パケット数
Config BPDU length	長さが無効だった Configuration BPDU の数
TCN BPDU length	長さが無効だった Topology Change Notification BPDU の数

表 92:

関連コマンド

RESET STP ( 321 ページ )

SHOW STP ( 480 ページ )

SHOW STP PORT ( 487 ページ )

## SHOW STP DEBUG

カテゴリー：スイッチング / スパニングツリープロトコル (STP/RSTP)

### SHOW STP DEBUG

#### 解説

各ポートで有効になっている STP デバッグオプションを表示する。

#### 入力・出力・画面例

Manager > show stp debug			
Port	Enabled Debug Modes	Output	Timeout
-----	-----	-----	-----
Port1	MSG, PKT, STATE	16	NONE
-----	-----	-----	-----
Port	Enabled Debug Modes	Output	Timeout
-----	-----	-----	-----
Port2	STATE	16	12345
-----	-----	-----	-----
Port	Enabled Debug Modes	Output	Timeout
-----	-----	-----	-----
Port3	None		
-----	-----	-----	-----

Port	ポート番号
Enabled Debug Modes	現在有効になっている STP デバッグオプション。MSG (STP パケットをデコードして表示)、PKT (STP パケットを ASCII 表示)、STATE (ポートの状態遷移を表示)、ALL (すべてのオプション) がある
Output	デバッグ情報の出力先 (仮想端末 (TTY) 番号)
Timeout	デバッグオプションの残り有効期間 (秒)

表 93:

#### 関連コマンド

- DISABLE STP DEBUG (266 ページ)
- ENABLE STP DEBUG (296 ページ)
- SHOW STP COUNTER (484 ページ)

## SHOW STP PORT

カテゴリー：スイッチング / スパニングツリープロトコル (STP/RSTP)

**SHOW STP PORT** [= {*port-list* | ALL}]

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

各ポートの STP 情報を表示する。

### パラメーター

**PORT** ポート番号

### 入力・出力・画面例

```
Manager > show stp port=1
```

```
STP Port Information
```

```
-----
STP ..... default
  STP Status ..... OFF
  Port ..... 1
    State ..... Disabled
    Port Priority ..... 128
    Port Identifier ..... 8001
    Pathcost ..... 4 (auto configured)
    Designated Root ..... 32768 : 00-00-cd-08-17-0c
    Designated Cost ..... 0
    Designated Bridge ... 32768 : 00-00-cd-08-17-0c
    Designated Port ..... 8001
-----
```

```
Manager > show stp port=5
```

```
STP Port Information
```

```
-----
STP ..... default
  STP Status ..... ON

  Port ..... 5
    RSTP Port Role ..... Designated
    State ..... Forwarding
    Point To Point ..... Yes (Auto)
```

```

Port Priority ..... 128
Port Identifier ..... 8005
Pathcost ..... 20000 (auto configured)
Designated Root ..... 32768 : 00-00-cd-08-17-0c
Designated Cost ..... 0
Designated Bridge ... 32768 : 00-00-cd-08-17-0c
Designated Port ..... 8005
EdgePort ..... No
Counters:
    Loopback Disabled          0

```

-----

STP	所属する STP ドメイン名
STP Status	所属 STP ドメインの状態。ON か OFF。
Port	ポート番号
RSTP Port Role	ポートの役割。Disabled、Alternate、Backup、Backup (Loopback Disabled)、Designated、Root のいずれか。Backup (Loopback Disabled) は、ループ検出機能によりポートがディセーブルにされたことを示す。Rapid モードのときだけ表示される
State	ポートの状態。Standard モード時は、Disabled、Blocking、Listening、Learning、Forwarding のいずれか。Rapid モード時は、Disabled、Discarding、Learning、Forwarding のいずれか
Point To Point	ポートが他のブリッジとポイントツーポイントで接続されているかどうか。No、Yes で表示される。(Auto) は自動判別の結果であることを示す。Rapid モードのときだけ表示される
Port Priority	ポートプライオリティ
Port Identifier	ポート識別子
Pathcost	パスコスト
Designated Root	ルートブリッジのブリッジ識別子
Designated Cost	ポートの代表コスト
Designated Bridge	代表ブリッジのブリッジ識別子
Designated Port	代表ポート。代表ブリッジが BPDU を送信するポートのポート識別子
EdgePort	ポートがエッジポートかどうか。Yes、No のいずれか。Rapid モードのときだけ表示される
Counters/Loopback Disabled	ループ検出によりポートをディセーブルにした回数。Rapid モードのときだけ表示される

表 94:

備考・注意事項



トランクポート上でスパニングツリープロトコル (STP) が動作しているとき、非マスターポートの State は「Disabled - Port in trunk group」となる。(ここで、「マスターポート」はトランクグループ内でもっとも番号の小さいポート、「非マスターポート」はそれ以外のポートを示す)

### 関連コマンド

SET STP ( 377 ページ )

SET STP PORT ( 379 ページ )

SHOW STP ( 480 ページ )

## SHOW SWITCH

カテゴリー：スイッチング / 一般コマンド

### SHOW SWITCH

#### 解説

スイッチ機能の全般的情報を表示する。

#### 入力・出力・画面例

```
Manager > show switch

Switch Configuration
-----
Switch Address ..... 00-00-cd-24-02-0e
Learning ..... ON
Ageing Timer ..... ON
Jumbo Frames ..... OFF
IP route learn delay ..... 4 ms
Number of Fixed Ports ..... 24
Number of Uplink Ports ..... 0
Mirroring ..... DISABLED
Mirror port ..... None
Ports mirroring on Rx ..... None
Ports mirroring on Tx ..... None
Ports mirroring on Both .... None
Nested TPID ..... 0x8100
Thrash limit ..... 10
Number of WAN Interfaces ... 0
Name of Interface(s) ..... -
Ageingtime ..... 300
DLF rate limit ..... -
STP Forwarding ..... Disabled
UpTime ..... 05:30:04
Hashingfield ..... L2 L3
-----

Traffic Control Unit, hardware resource usage:
Total system rule space ..... 2048
Total number of rules used .... 2
Total rule space usage ..... 16
Number of rules per application:
  MLD Snooping ..... 2
Total number of actions ..... 2048
Number of actions used ..... 4
Device Resource, device #0:
  Number of rules used ..... 1
```

```

Rule space usage ..... 8
Number of rules per application:
  MLD Snooping ..... 1
Device rule space limit ..... 1024
Profile Usage:
  Profile #1:
    IPv4 bytes used ..... 0 of 16
    IPv6 bytes used ..... 1 of 16
    Other-Eth bytes used .... 0 of 16
  Profile #2:
    IPv4 bytes used ..... 0 of 16
    IPv6 bytes used ..... 0 of 16
    Other-Eth bytes used .... 0 of 16
Device Resource, device #1:
  Number of rules used ..... 1
  Rule space usage ..... 8
  Number of rules per application:
    MLD Snooping ..... 1
  Device rule space limit ..... 1024
  Profile Usage:
    Profile #1:
      IPv4 bytes used ..... 0 of 16
      IPv6 bytes used ..... 1 of 16
      Other-Eth bytes used .... 0 of 16
    Profile #2:
      IPv4 bytes used ..... 0 of 16
      IPv6 bytes used ..... 0 of 16
      Other-Eth bytes used .... 0 of 16

```

-----

Switch Address	MAC アドレス
Learning	フォワーディングデータベースの自動学習機能。ON か OFF
Ageing Timer	フォワーディングデータベースのエージングタイマーが機能しているかどうか。ON か OFF
Jumbo Frames	未サポート
IP route learn delay	未サポート
Number of Fixed Ports	固定ポートの数
Number of Uplink Ports	拡張ポートの数
Mirroring	ポートミラーリング機能の状態。ENABLED か DISABLED
Mirror port	ミラーポート
Ports mirroring on Rx	受信トラフィックだけをミラーリングしているソースポート
Ports mirroring on Tx	送信トラフィックだけをミラーリングしているソースポート

Ports mirroring on Both	送受信両方のトラフィックをミラーリングしているソースポート
Nested TPID	ダブルタグ VLAN (Nested VLAN) で使用する外側タグのプロトコルタイプ (TPID)
Thrash limit	MAC アドレススラッシング (同一 MAC アドレスの登録ポートが頻繁に変更されること) の検出しきい値
Number of WAN Interfaces	未サポート
Name of Interface(s)	未サポート
Ageingtime	フォワーディングデータベースのエージングタイム (MAC アドレス保持時間)
DLF rate limit	未学習ユニキャストパケットの受信レート上限値
STP Forwarding	BPDU フォワーディングの有効・無効
Uptime	再起動後の経過時間 (時:分:秒の形式)。MIB-II オブジェクト sysUpTime と同じ
Hashingfield	ポートランキングの送出ポート決定アルゴリズムが使用するヘッダー情報の種類
Traffic Control Unit, hardware resource usage セクション	ハードウェアパケットフィルター、ポリシーベース QoS などが利用するルールテーブルの使用状況が表示される
Total system rule space	システム全体のルール領域総容量 (最大ルール数)
Total number of rules used	システム全体で現在使用しているルール数
Total rule space usage	システム全体のルール領域消費量 (ルール領域は、ルール 8 個単位で消費される。そのため使用しているルール数が 1~8 個のとき、ルール領域の使用量は 8 となる)
Number of rules per application セクション	各機能 (モジュール) が使用しているルール数 (システム全体)。ルールテーブルを使用する機能には、MLD Snooping、Switch HwFilter (ハードウェアパケットフィルター)、QoS (ポリシーベース QoS) などがある
Total number of actions	システム全体で使用可能なアクションの総数
Number of actions used	現在使用しているアクションの数
Device Resource セクション	デバイスごとのリソース使用状況が表示される
device #	デバイス番号。デバイスには、本体インスタンス (スイッチチップ) や IPv6 アクセラレーターボードがある。本製品ではデバイス #0 と #1 が本体インスタンス (それぞれ、ポート 1~12 と 13~24 が所属)、#2 が IPv6 アクセラレーターとなる

Number of rules used	該当デバイスで現在使用しているルール数
Rule space usage	該当デバイスのルール領域消費量（ルール領域は、ルール 8 個単位で消費される。そのため使用しているルール数が 1～8 個のとき、ルール領域の使用量は 8 となる）
Number of rules per application セクション	各機能（モジュール）が該当デバイス上で使用しているルール数
Device rule space limit	該当デバイスのルール領域総容量（最大ルール数）
Profile Usage セクション	プロファイルの使用量（プロファイルとは、クラシファイアで定義したパケットの特徴を記述したもの）
Profile #	プロファイル番号
IPv4 bytes used	IPv4 フィールドの消費量と総容量（Byte）、「m of n」の形式で表される。m は消費量、n は総容量
IPv6 bytes used	IPv6 フィールドの消費量と総容量（Byte）、「m of n」の形式で表される。m は消費量、n は総容量
Other-Eth bytes used	Ethernet フィールドの消費量と総容量（Byte）、「m of n」の形式で表される。m は消費量、n は総容量

表 95:

## 関連コマンド

RESET SWITCH ( 322 ページ )

SET SWITCH THRASHLIMIT ( 391 ページ )

## SHOW SWITCH ACCELERATOR

カテゴリー：スイッチング / 一般コマンド

備考：IPv6 アクセラレーターボード AT-ACC01 と拡張メモリー AT-SD512A-001 が必要（本機能は 9924SP では使用できません）

### SHOW SWITCH ACCELERATOR

#### 解説

IPv6 アクセラレーターボードの情報を表示する。

#### 入力・出力・画面例

```
Manager > show switch accelerator

Switch Accelerator Configuration
-----
Hardware Type ..... AT-ACC01
Mode ..... IPv6 Acceleration
Status ..... IPv6 active
Search memory size ..... 128 MBytes
Counter memory size ..... 36 Mbits
MAC address ..... 00-00-cd-10-00-74
-----
```

Hardware Type	IPv6 アクセラレーターボードの製品名称
Mode	IPv6 アクセラレーターボードの動作モード。IPv6 Acceleration（有効）、Disabled（無効）のいずれか
Status	IPv6 アクセラレーターボードの状態。IPv6 active（アクティブ）、Absent（カード未装着）、Disabled（無効）のいずれか
Search memory size	IPv6 アクセラレーターボードの検索メモリーサイズ。検索メモリーには、マルチキャストテーブルや経路ツリーが格納される
Counter memory size	IPv6 アクセラレーターボードのカウンターメモリーサイズ。カウンターメモリーには、統計カウンター情報が格納される
MAC address	IPv6 ルーティングに使用する MAC アドレス

表 96:

#### 関連コマンド

SHOW SWITCH（490 ページ）

SHOW SWITCH ACCELERATOR（494 ページ）

SHOW SWITCH ACCELERATOR COUNTER ( 496 ページ )

## SHOW SWITCH ACCELERATOR COUNTER

カテゴリー：スイッチング / 一般コマンド

備考：IPv6 アクセラレーターボード AT-ACC01 と拡張メモリー AT-SD512A-001 が必要（本機能は 9924SP では使用できません）

**SHOW SWITCH ACCELERATOR COUNTER** [= {ALL|DEFAULT|FAB|MAC|MIB|MISC}]

### 解説

IPv6 アクセラレーターボードの統計カウンターを表示する。

### パラメーター

**COUNTER** 表示するカウンターの種類を指定する。FAB（ファブリックインターフェースカウンター）、MAC（MAC カウンター）、MIB（SNMP カウンター）、MISC（各種ステータス）、DEFAULT（MAC、MIB カウンター）、ALL（すべてのカウンター）から選択する。カウンターの種類を指定しなかった場合は、DEFAULT を指定したのと同じ意味になる。

### 入力・出力・画面例

```
Manager > show switch accelerator counter

Switch Accelerator Counters
-----

Accelerator Ethernet MAC counters:
Combined receive/transmit packets by size (octets) counters:
 64                      0 512 - 1023                      2862
65 - 127                 21242 1024 - 1518                  78
128 - 255                584 1519 - 1522                   32004
256 - 511                40

General Counters:
Receive                      Transmit
Octets                      26554898 Octets                      26554554
Pkts                        28407 Pkts                        28403
FCSErrors                   0 FCSErrors                   0
MulticastPkts               4 MulticastPkts               0
BroadcastPkts               0 BroadcastPkts               0
PauseCtrlFrms               0 PauseCtrlFrms               0
OversizePkts                0 OversizePkts                0
Fragments                   0 Fragments                   0
Jabbers                     0 Jabbers                     0
UndersizePkts               0 UndersizePkts               0
```



Control	0	Control	0
LengthError	0	LengthError	0
CodeError	0		
UnknownOffset	0		
Accelerator IPv6 MIB counters:			
InReceives	28407	OutForwDatagrm	28353
InNoRoutes	0		
InDiscards	0	OutDiscards	0
InAddrErrors	0		
InTruncatedPkts	0		
InMcastPkts	4	OutMcastPkts	0
InDelivers	0		
InHdrErrors	0		
InTooBigErrors	0		
-----			

## Accelerator Ethernet MAC counters セクション

Combined receive/transmit packets by size (octets) counters セクション	フレームサイズ別送受信数分布
64	64 オクテット長のフレーム送受信数
65 - 127	65 ~ 127 オクテット長のフレーム送受信数
128 - 255	128 ~ 255 オクテット長のフレーム送受信数
256 - 511	256 ~ 511 オクテット長のフレーム送受信数
512 - 1023	512 ~ 1023 オクテット長のフレーム送受信数
1024 - 1518	1024 ~ 1518 オクテット長のフレーム送受信数
1519 - 1522	1519 ~ 1522 オクテット長のフレーム送受信数

## General Counters セクション

Receive サブセクション	受信トラフィックカウンターが表示される
Octets	受信オクテット数
Pkts	受信パケット数
FCSErrors	FCS エラーフレーム受信数
MulticastPkts	マルチキャストフレーム受信数
BroadcastPkts	ブロードキャストフレーム受信数
PauseCtrlFrms	有効な PAUSE フレーム受信数
OversizePkts	オーバーサイズフレーム受信数。正しい形式であるが、長さが 1518 オクテットより長いパケットの総数
Fragments	フラグメントフレーム受信数。不正な FCS を持ち、なおかつ、長さが 64 オクテットより短いフレームの総数。アライメントエラーを含む

Jabbers	ジャバーフレーム受信数。1518 オクテットより長いフレームのうち、不正な FCS を持つものの総数。アライメントエラーを含む
UndersizePkts	アンダーサイズフレーム受信数。正しい形式であるが、長さが 64 オクテットより短いフレームの総数
Control	コントロールフレーム受信数
LengthError	長さが不正なフレーム受信数
CodeError	構造が不正なフレーム受信数
UnknownOffset	未サポートのコントロールフレーム受信数
Transmit サブセクション	送信トラフィックカウンターが表示される
Octets	送信オクテット数
Pkts	送信パケット数
FCSErrors	FCS エラーフレーム送信数
MulticastPkts	マルチキャストフレーム送信数
BroadcastPkts	ブロードキャストフレーム送信数
PauseCtrlFrms	有効な PAUSE フレーム送信数
OversizePkts	オーバーサイズフレーム送信数
Fragments	フラグメントフレーム送信数
Jabbers	ジャバーフレーム送信数
UndersizePkts	アンダーサイズフレーム送信数
Control	コントロールフレーム送信数
LengthError	長さが不正なフレーム送信数
Accelerator IPv6 MIB counters セクション	
InReceives	受信パケット数
InNoRoutes	受信パケットのうち、宛先への経路がないため破棄されたものの数
InDiscards	受信パケットのうち、破棄されたものの数
InAddrErrors	受信パケットのうち、アドレスエラーがあったものの数
InTruncatedPkts	切り詰められたパケットの受信数
InMcastPkts	受信マルチキャストパケット数
InDelivers	受信パケットのうち、上位層への配送に成功したものの数
InHdrErrors	受信パケットのうち、ヘッダーエラーがあったものの数
InTooBigErrors	受信パケットのうち、サイズ過大で破棄されたものの数
OutForwDatagrm	転送のため送出されたパケットの数
OutDiscards	送信前破棄パケット数
OutMcastPkts	マルチキャストパケット送信数

表 97:

## 関連コマンド

RESET SWITCH ACCELERATOR COUNTER ( 323 ページ )

SHOW SWITCH ( 490 ページ )

SHOW SWITCH ACCELERATOR ( 494 ページ )

# SHOW SWITCH ACCELERATOR HWFILTER

カテゴリー：スイッチング / IPv6 ハードウェアパケットフィルター

備考：IPv6 アクセラレーターボード AT-ACC01 と拡張メモリー AT-SD512A-001 が必要（本機能は 9924SP では使用できません）

**SHOW SWITCH ACCELERATOR HWFILTER** [= {*filter-id* | ALL}]

*filter-id*: フィルター番号（1～999）

## 解説

IPv6 ハードウェアパケットフィルターの情報を表示する。  
クラシファイアの設定は SHOW CLASSIFIER コマンドで確認できる。

## パラメーター

**HWFILTER** フィルター番号。省略時および ALL を指定した場合は、すべてのフィルターの情報が表示される。

## 入力・出力・画面例

```

Manager > show switch accelerator hwfilter=all
Accelerator Hardware-based Packet Filters
-----
Rule position ..... 1
Rule Id ..... 5
Action ..... MARK
    New Priority ..... 7

Rule position ..... 2
Rule Id ..... 1
Action ..... MARK
    New DSCP ..... 1
-----

```

Rule position	フィルター番号
Rule Id	クラシファイア（汎用パケットフィルター）番号
Action	アクション
New DSCP	書き換え後の IPv6 DSCP 値
New Priority	書き換え後の 802.1p ユーザープライオリティー値

表 98:

### 関連コマンド

ADD SWITCH ACCELERATOR HWFILTER ( 184 ページ )

SHOW CLASSIFIER ( 395 ページ )

SHOW SWITCH COUNTER

カテゴリー：スイッチング / 一般コマンド

SHOW SWITCH COUNTER

解説

スイッチングモジュールの統計カウンターを表示する。

入力・出力・画面例

```
Manager > show switch counter

Switch Counters
-----
Switch instance:      0

Packet DMA counters:

  Receive:                Transmit:
Packets                71202    Packets                71196
Discards                0        Discards                2
TooFewBuffers           0        Aborts                  0
DescriptorsExhausteds   0        DescriptorAreaFilleds   0
QueueLength             0        QueueLength             12

  PCI bus counters:
ParityErrors            0        ErrorChannel            0
FatalErrors             0

  General counters:
Resets                  0
-----
```

Packet DMA counters セクション	DMA に関するカウンターが表示される
Receive サブセクション	受信パケットに関する統計が表示される
Packets	スイッチチップから CPU に渡されたパケットの数
Discards	スイッチチップから受け取ったパケットのうち、受信キューが 4096 を超えたか、空きバッファ容量が BufferLevel3 を下回った、あるいは、パケットにデータが含まれていなかったために破棄されたものの数

TooFewBuffers	スイッチチップから受け取ったパケットのうち、空きバッファ容量が BufferLevel3 を下回ったために破棄されたものの数
DescriptorsExhausteds	受信バッファディスクリプターの枯渇により、スイッチチップからバッファへの DMA 転送に失敗した回数
QueueLength	スイッチチップから受け取ったパケットのうち、CPU による処理を待っているものの数
Transmit サブセクション	送信パケットに関する統計が表示される
Packets	CPU からスイッチチップに渡されたパケットの数
Discards	エラーによる DMA プロセスのリセットが原因で、送信されずに破棄されたパケットの数
Aborts	時間がかかりすぎたために送信を中断されたパケットの数
DescriptorAreaFilledds	CPU からスイッチチップに大量のパケットが転送されたか、PCI バスの使用率が高くなり DMA 転送が遅くなったことが原因で、送信ディスクリプター領域がいっぱいになった回数
QueueLength	送信キューに格納されているパケットの数
PCI bus counters セクション	PCI バスに関するカウンタが表示される
ParityErrors	PCI バス上のデータ転送におけるパリティエラーの発生回数 (スイッチチップが報告したもの)
FatalErrors	PCI バス上のデータ転送における致命的エラーの発生回数 (スイッチチップが報告したもの)
ErrorChannel	データ転送中にエラーが発生した DMA チャンネル
General counters セクション	一般的なカウンタが表示される。
Resets	エラーによる DMA チャンネルのリセット回数

表 99:

## 関連コマンド

RESET SWITCH ( 322 ページ )

SHOW SWITCH ( 490 ページ )

# SHOW SWITCH FDB

カテゴリー：スイッチング / フォワーディングデータベース

```
SHOW SWITCH FDB [ADDRESS=macadd] [PORT={port-list|ALL}] [STATUS={STATIC|
DYNAMIC}] [VLAN={vlanname|1..4094}]
```

macadd: MAC アドレス (xx-xx-xx-xx-xx-xx の形式)  
port-list: スイッチポート番号 (1~。ハイフン、カンマを使った複数指定も可能)  
vlanname: VLAN 名 (1~32 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字は区別しない)

## 解説

フォワーディングデータベース (FDB) の内容を表示する。  
オプション指定により、表示するエントリーの絞り込みが可能。

## パラメーター

- ADDRESS 指定したアドレスと一致するエントリーだけを表示する
- PORT 指定したポートと一致するエントリーだけを表示する
- STATUS 表示するエントリー種別。STATIC (スタティックエントリー) か DYNAMIC (ダイナミックエントリー) を指定する。DYNAMIC にはポートセキュリティの学習済みエントリー (Learn エントリー) も含まれる
- VLAN VLAN 名または VLAN ID。指定した VLAN に所属するエントリーだけが表示される。

## 入力・出力・画面例

Manager > show switch fdb

Switch Forwarding Database (software)

Total number of entries = 8

VLAN	MAC Address	Port/Vidx	Status	daRoute
1	00-00-5e-00-01-06	1	dynamic	0
1	00-00-cd-12-ae-ac	CPU	static	0
1	00-06-5b-88-80-41	1	dynamic	0
1	00-80-92-0c-52-86	1	dynamic	0
1	00-90-99-1b-65-c7	1	dynamic	0
1	00-90-99-42-00-f2	47	dynamic	0
1	00-90-99-c2-2b-00	1	dynamic	0
1	00-a0-c9-5a-b3-33	1	dynamic	0

VLAN	VLAN ID
MAC Address	MAC アドレス
Port/Vidx	該当 MAC アドレスを持つ機器が接続されているポート
Status	エントリーの種類。dynamic (ダイナミックエントリー) か static (スタティックエントリー)

表 100:

例

FDB を表示する。

```
SHOW SWITCH FDB
```

ポート 2 の FDB エントリーだけを表示する。

```
SHOW SWITCH FDB PORT=2
```

ダイナミックエントリーだけを表示する。

```
SHOW SWITCH FDB STATUS=DYNAMIC
```

関連コマンド

ENABLE SWITCH LEARNING ( 301 ページ )

SHOW SWITCH ( 490 ページ )

SHOW SWITCH FILTER ( 505 ページ )



## SHOW SWITCH FILTER

カテゴリー：スイッチング / フォワーディングデータベース

**SHOW SWITCH FILTER** [PORT={*port-list*|ALL}] [ACTION={FORWARD|DISCARD}]  
[DESTADDRESS=*macadd*] [ENTRY=*entry-id*] [VLAN={*vlanname*|1..4094}]

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

*macadd*: MAC アドレス (xx-xx-xx-xx-xx-xx の形式)

*entry-id*: エントリー番号 (0～319)

*vlanname*: VLAN 名 (1～32 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字は区別しない)

### 解説

フォワーディングデータベース (FDB) のスタティックエントリー (スイッチフィルター) を表示する。  
オプション指定により、表示するエントリーの絞り込みが可能。

### パラメーター

**PORT** 出力ポート番号

**ACTION** スタティックエントリーのアクション。FORWARD (転送) か DISCARD (破棄)。

**DESTADDRESS** 宛先 MAC アドレス

**ENTRY** エントリー番号

**VLAN** VLAN 名または VLAN ID

### 入力・出力・画面例

```
Manager > show switch filter
```

Switch Filters					
Entry	VLAN	Destination Address	Port	Action	Source
0	white (10)	00-00-f4-12-12-12	8	Forward	Static
1	white (10)	00-00-f4-12-12-13	8	Forward	Learn
2	white (10)	00-00-f4-12-12-14	8	Forward	Learn
0	orange (20)	00-00-f4-01-01-01	11	Forward	Static

Entry	スタティックエントリーの番号
Destination Address	宛先 MAC アドレス
VLAN	VLAN 名と VLAN ID

Port	マッチしたパケットの出力先ポート
Action	マッチしたパケットに適用するアクション。Forward（転送）か Discard（破棄）
Source	エントリーのタイプ。Static は通常のスタティックエントリー。Learn はポートセキュリティ機能がオンのときに学習した特殊なスタティックエントリー（Learn エントリー）。ADD SWITCH FILTER コマンドで LEARN パラメータを指定した場合も Learn エントリーとして「学習済みアドレス」の 1 つに数えられる

表 101:

### 例

FDB のスタティックエントリーを表示する。

```
SHOW SWITCH FILTER
```

ポート 2 のスタティックエントリーだけを表示する。

```
SHOW SWITCH FILTER PORT=2
```

### 関連コマンド

ADD SWITCH FILTER ( 186 ページ )

DELETE SWITCH FILTER ( 236 ページ )

SET SWITCH MIRROR ( 385 ページ )

## SHOW SWITCH HWFILTER

カテゴリー：スイッチング / ハードウェアパケットフィルター

**SHOW SWITCH HWFILTER** [=*filter-list*]

*filter-list*: フィルター番号（1～1024。ハイフン、カンマを使った複数指定も可能）

### 解説

ハードウェアパケットフィルターの情報を表示する。  
クラシファイアの設定は SHOW CLASSIFIER コマンドで確認できる。

### パラメーター

**HWFILTER** フィルター番号。省略時はすべてのフィルターの情報が簡潔に表示される

### 入力・出力・画面例

```
Manager > show switch hwfilter
```

```
Switch Hardware Filter Summary Information
```

```
-----
Number of Filters ..... 2
Status ..... ENABLED
```

```
Filter ..... 1
  Classifier ..... 1
```

```
Filter ..... 2
  Classifier ..... 2
```

```
-----
Manager > show switch hwfilter=2
```

```
Switch Hardware Filter Information
```

```
-----
Filter ..... 2
  Classifier ..... 2
  Action ..... DISCARD
-----
```

Number of Filters	定義されているフィルターの数
Status	ハードウェアパケットフィルターの状態。常に ENABLED
Filter	フィルター番号
Classifier	クラシファイア（汎用パケットフィルター）番号

表 102: HWFILTER 無指定時

Filter	フィルター番号
Classifier	クラシファイア（汎用パケットフィルター）番号
Action	アクション。FORWARD、DISCARD、SETL2QOS のいずれか
Priority	マッチしたパケットにセットする 802.1p ユーザープライオリティ値。Action が「SETL2QOS」のときだけ表示される
TC(queue)	マッチしたパケットを格納するキュー。Action が「SETL2QOS」のときだけ表示される
BW class	未サポート

表 103: HWFILTER 指定時

## 関連コマンド

ADD SWITCH HWFILTER ( 188 ページ )

SHOW CLASSIFIER ( 395 ページ )

## SHOW SWITCH PORT

カテゴリー：スイッチング / ポート

**SHOW SWITCH PORT** [= {*port-list* | ALL}]

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

スイッチポートの情報を表示する。

### パラメーター

**PORT** ポート番号。省略時および ALL 指定時は、全ポートの情報が表示される。

### 入力・出力・画面例

```
Manager > show switch port=1
```

```
Switch Port Information
```

```
-----
Port ..... 1
  Description ..... -
  Status ..... ENABLED
  Link State ..... Down
  UpTime ..... -
  Port Media Type ..... ISO8802-3 CSMACD
  Configured speed/duplex ..... Autonegotiate
  Actual speed/duplex ..... -
  MDI Configuration (Polarity) .. Automatic ( - )
  Loopback ..... Off
  Configured master/slave mode .. Not applicable
  Actual master/slave mode ..... -
  Acceptable Frames Type ..... Admit All Frames
  Disabled Egress Queues ..... -
  BCast & MCast rate limit ..... -
  BCSC rate Limiting ..... disabled
  Egress rate limit ..... -
  Learn limit ..... -
  Intrusion action ..... Discard
  Current learned, lock state ... -, not locked
  Address learn thrash status ... Not Detected
  Address learn thrash action ... Learn Disable
  Address learn thrash timeout .. 1 second
  VLAN Status Trap ..... OFF
  Relearn ..... OFF
```

```

Mirroring ..... Disabled
Is this port mirror port ..... No
VLAN(s) ..... default (1)
Ingress Filtering ..... Off
Trunk Group ..... -
STP ..... default
IGMP Filter ..... None
Max-groups/Joined ..... Undefined/0
IGMP Max-groups Action ..... Deny

```

Port	ポート番号
Description	ポート名称 (メモ)
Status	ポートの管理ステータス。ENABLED か DISABLED
Link State	ポートのリンクステータス。Up か Down
UpTime	ポートがリセット(初期化)されてから現在までの経過時間( hh:mm:ss の形式 )
Port Media Type	MIB-II オブジェクト ifType で定義される物理層インターフェースタイプ
Configured speed/duplex	通信モードの設定値。Autonegotiate または速度 10Mbps、100Mbps とデュプレックスモード half duplex、full duplex の組み合わせで表示される。また、オートネゴシエーションで特定の通信モードを使うよう設定されているときは、「(by autonegotiation)」という文字列も表示される
Actual speed/duplex	実際の通信モード。速度 10 Mbps、100 Mbps、1000 Mbps とデュプレックスモード half duplex、full duplex の組み合わせで表示される。通信モードが固定に設定されている場合は、Configured speed/duplex と同じ。ポートがオートネゴシエーションに設定されている場合は、ネゴシエーションで決定された通信モードが表示される。ポートがリンクアップしていない場合は「-」(未決定)と表示される
MDI Configuration (Polarity)	MDI/MDI-X 自動切替機能の状態と、実際の MDI/MDI-X。自動切替の状態は、有効なら Automatic、無効なら Manual と表示される。また、実際の MDI/MDI-X は、カッコ内に MDI-X、MDI、- (未決定) のいずれかで表示される
Loopback	未サポート
Configured master/slave mode	1000BASE-T ポートのマスター/スレーブ設定値。Autonegotiate、Master、Slave のいずれか。1000BASE-T 以外のポートでは、Not applicable と表示される
Actual master/slave mode	1000BASE-T ポートの実際のマスター/スレーブ。その他のポートの場合は、Not applicable と表示される

Acceptable Frames Type	受信可能なフレームタイプ。Admit All Frames か Admit Only VLAN-tagged Frames
Disabled Egress Queue	未サポート
BCast & MCast rate limit	ブロードキャストおよびマルチキャストパケットの受信上限値（パケットストームプロテクション機能）
BCSC rate Limiting	パケットストームプロテクションで受信レートを制限するパケットの種類。Broadcast enabled(ブロードキャストのみ)、Broadcast and Multicast enabled(ブロードキャストとマルチキャスト)、disabled(制限なし)のいずれか
Egress rate limit	送信レート上限値（帯域制限機能）
Learn limit	MAC アドレス登録数の上限。設定した数まで MAC アドレスを学習すると、それ以上の MAC アドレスの登録を行わない
Intrusion action	Learn limit まで MAC アドレスを学習した後で未学習の MAC アドレスを受信した場合のアクション。Discard、Trap、Disable がある
Current learned, lock state	Learn limit を設定した場合の現在の MAC アドレス登録数。lock state はポートのロック状態を示すもので、not locked、locked by limit (Learn limit 到達によるロック)、locked by command (ACTIVATE SWITCH PORT LOCK コマンドによるロック)、locked by address thrashing(MAC アドレススラッシングプロテクションのしきい値 thrash limit 到達によるロック)で表示される
Address learn thrash status	MAC アドレススラッシング検出機能の状態。Not Detected (スラッシング未検出)、Thrashing (スラッシング検出中)、Disabled (検出機能が無効。THRASHACTION=NONE に設定されていることを示す)、Trunk (該当ポートがトランクグループに所属しているため、検出機能の状態がトランクグループ側で管理されていることを示す)のいずれか
Address learn thrash action	MAC アドレススラッシング検出時の動作。None (何もしない)、Learn Disable (MAC アドレスの学習を停止する)、Port Disable (ポートをディセーブルにする)、VLAN Disable (スラッシングが発生した VLAN に対してのみポートをディセーブルにする)、Link Down (ポートを物理的にリンクダウンさせる)のいずれか
Address learn thrash timeout	MAC アドレススラッシング検出時の動作の持続時間 (秒)。動作の実行中は、カッコ内に残り秒数が表示される。None は無期限であることを示す
VLAN Status Trap	特定 VLAN におけるポートステータス (イネーブル、ディセーブル) が変化した場合に、SNMP トラップを送信するかどうか。OFF (送信しない)、ON (送信する) のどちらか

Relearn	ポートセキュリティの動作モード。OFF (スタティック)、ON (ダイナミック) のどちらか
Mirroring	ミラーリング対象パケットの向きとミラーポート。「Disabled」、「Enabled, Rx, frames mirrored to Port X」、「Enabled, TX, frames mirrored to Port X」、「Enabled, Both, frames mirrored to Port X」のように表示される。ミラーポートが設定されていないときは「Enabled, ..., no mirror Port set」のように表示される
Is this port mirror port	ミラーポートに設定されているかどうか
VLAN(s)	所属 VLAN の名前と VLAN ID
Ingress Filtering	インGRESSフィルタリングのオン・オフ
Trunk Group	ポートが所属するトランクグループ名
STP	ポートが所属する STP ドメイン名
IGMP Filter	該当ポートに適用されている IGMP フィルターの番号。適用されていない場合は None と表示される
Max-groups/Joined	該当ポート配下から Join 可能なマルチキャストグループの最大数と実際に Join されているグループ数。最大数が設定されていないときは Undefined と表示される
IGMP Max-groups Action	該当ポート配下から Join されたマルチキャストグループの数が最大数に達した場合の動作
Cable Length	未サポート
SFP vendor name	SFP ベンダー名 (SFP ポートのみ)
SFP part number	SFP の製品名または型番 (SFP ポートのみ)
SFP vendor SN	SFP のベンダーシリアル番号 (SFP ポートのみ)
SFP date code	SFP の日付コード (SFP ポートのみ)

表 104:

## 関連コマンド

SET SWITCH PORT (387 ページ)



## SHOW SWITCH PORT COUNTER

カテゴリー：スイッチング / ポート

**SHOW SWITCH PORT**[={*port-list*|ALL}] **COUNTER**

*port-list*: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

### 解説

スイッチポートの統計カウンターを表示する。

### パラメーター

**PORT** ポート番号。省略時および ALL 指定時は、全ポートの情報が表示される。

### 入力・出力・画面例

```
Manager > show switch port=1 counter

Switch Port Counters
-----

Port 1. Ethernet MAC counters:
Combined receive/transmit packets by size (octets) counters:
 64                      2898 512 - 1023                      3
 65 - 127                 312 1024 - MaxPktSz                  0
 128 - 255                 157
 256 - 511                 20

General Counters:
Receive                      Transmit
Octets                      249838 Octets                      5533
Pkts                        3333 Pkts                        57
CRCErrors                    0
MulticastPkts                2770 MulticastPkts                0
BroadcastPkts                269 BroadcastPkts                2
FlowCtrlFrms                 0 FlowCtrlFrms                 0
OversizePkts                  0
Fragments                    0
Jabbers                       0
UpsupportOpcode               0
UndersizePkts                 0
                               Collisions                      0
                               LateCollisions                  0
                               ExcessivCollsns                 0
```

## Miscellaneous Counters:

MAC TxErr	0
MAC RxErr	0
Drop Events	0

Combined receive/transmit packets by size (octets) counters セクション

フレームサイズ別送受信数分布

64	64 オクテット長のフレーム送受信数
65 - 127	65 ~ 127 オクテット長のフレーム送受信数
128 - 255	128 ~ 255 オクテット長のフレーム送受信数
256 - 511	256 ~ 511 オクテット長のフレーム送受信数
512 - 1023	512 ~ 1023 オクテット長のフレーム送受信数
1024 - MaxPktSz	1024 ~ 最大サイズのフレーム送受信数

General Counters セクション

一般的な送受信カウンター

Receive Subsection	受信トラフィックカウンターが表示される
Octets	受信オクテット数
Pkts	受信パケット数
CRCErrors	CRC エラーフレーム受信数
MulticastPkts	マルチキャストフレーム受信数
BroadcastPkts	ブロードキャストフレーム受信数
FlowCtrlFrms	有効な PAUSE フレーム受信数
OversizePkts	オーバーサイズフレーム受信数。正しい形式であるが、長さが 1518 オクテットより長いパケットの総数
Fragments	フラグメントフレーム受信数。不正な FCS を持ち、なおかつ、長さが 64 オクテットより短いフレームの総数。アライメントエラーを含む
Jabbers	ジャバースフレーム受信数。1518 オクテットより長いフレームのうち、不正な FCS を持つものの総数。アライメントエラーを含む
UnsupportOpcode	未サポートのコントロールフレーム受信数
UndersizePkts	アンダーサイズフレーム受信数。正しい形式であるが、長さが 64 オクテットより短いフレームの総数
Transmit Subsection	送信トラフィックカウンターが表示される
Octets	送信オクテット数
Pkts	送信パケット数
MulticastPkts	マルチキャストフレーム送信数
BroadcastPkts	ブロードキャストフレーム送信数

FlowCtrlFrms	有効な PAUSE フレーム送信数
Collisions	コリジョン発生総数
LateCollisions	レートコリジョン発生数
ExcessivCollsns	コリジョン多発のため送信が中止されたフレームの数
Miscellaneous Counters	その他の統計カウンター
セクション	
MAC TxErr	MAC エラーにより送信に失敗したフレームの数
MAC RxErr	MAC エラーにより受信に失敗したフレームの数
Drop Events	資源不足により取りこぼしたフレームの数

表 105:

関連コマンド

SET SWITCH PORT ( 387 ページ )

SHOW SWITCH PORT ( 509 ページ )

## SHOW SWITCH PORT INTRUSION

カテゴリー：スイッチング / ポート

**SHOW SWITCH PORT=*port-number* INTRUSION**

*port-number*: スイッチポート番号 (1 ~ )

### 解説

ポートセキュリティ機能がオンのポート (LEARN パラメーターが 0 以外に設定されているポート) において、学習済み MAC アドレス数が上限に達した後で受信した未学習の MAC アドレス (INTRUSIONACTION の対象となったアドレス) の一覧を表示する。

### パラメーター

**PORT** ポート番号

### 入力・出力・画面例

```
Manager > show switch port=11 intrusion
```

```
Switch Port Information
```

```
-----  
Port 11 -      1 intrusion(s) detected  
          00-00-f4-1e-e0-0a  
-----
```

### 関連コマンド

SET SWITCH PORT ( 387 ページ )

SHOW SWITCH TRUNK

カテゴリー：スイッチング / ポート

SHOW SWITCH TRUNK [=trunk]

trunk: トランクグループ名 (1~15 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字を区別しない)

解説

トランクグループの情報を表示する。

パラメーター

TRUNK トランクグループ名。省略時はすべてのトランクグループの情報が表示される。

入力・出力・画面例

```
Manager > show switch trunk

Switch Trunk Groups
-----
Trunk group name ..... aggr1
Speed ..... 100 Mbps
Ports ..... 1-4
Address learn thrash status ..... Not Detected
Address learn thrash action ..... Learn Disable
Address learn thrash timeout ..... 1 second
Ports disabled by learn thrashing ... Not Applicable
-----
```

Trunk group name	トランクグループ名
Speed	トランクポートの通信速度。10Mbps、100Mbps、1000Mbps、 - (未設定) のいずれか
Ports	所属ポート
Address learn thrash status	MAC アドレススラッシング検出機能の状態。Not Detected (スラッシング未検出) Thrashing(スラッシング検出中) Disabled (検出機能が無効。THRASHACTION=NONE に設定されていることを示す) のいずれか

Address learn thrash action	MAC アドレススラッシング検出時の動作。None (何もしない)、Learn Disable (トランクグループ内の全ポートで MAC アドレスの学習を停止する)、Port Disable (トランクグループ内の全ポートをディセーブルにする)、VLAN Disable (スラッシングが発生した VLAN に対してのみトランクグループ内の全ポートをディセーブルにする)、Link Down (トランクグループ内の全ポートを物理的にリンクダウンさせる) のいずれか
Address learn thrash timeout	MAC アドレススラッシング検出時の動作の持続時間 (秒)。動作の実行中は、カッコ内に残り秒数が表示される。None は無期限であることを示す
Ports disabled by learn thrashing	MAC アドレススラッシング検出によりディセーブルにされたポート。Address learn thrash action が Port Disable か Link Down のときだけ有効。Address learn thrash action が前記以外に設定されている場合、および、検出機能が無効に設定されている場合は、Not Applicable と表示される

表 106:

## 関連コマンド

ADD SWITCH TRUNK ( 190 ページ )

CREATE SWITCH TRUNK ( 223 ページ )

DELETE SWITCH TRUNK ( 238 ページ )

DESTROY SWITCH TRUNK ( 251 ページ )

SET SWITCH TRUNK ( 392 ページ )

## SHOW VLAN

カテゴリー：スイッチング / バーチャル LAN

**SHOW VLAN** [= {*vlanname* | 1..4094 | ALL}]

*vlanname*: VLAN 名 (1~32 文字。英数字とアンダースコア ( \_ ) ハイフンを使用可能。大文字小文字は区別しない)

### 解説

VLAN 情報を表示する。

### パラメーター

**VLAN** VLAN 名または VLAN ID。省略時はすべての VLAN が表示される

### 入力・出力・画面例

```
Manager > show vlan
```

```
VLAN Information
```

```
-----
Name ..... default
Identifier ..... 1
Status ..... static
Type ..... Port-based
Private ..... No
Nested ..... No
Untagged ports ..... 49-52
Tagged ports ..... None
Port associations .. 49-52
Spanning Tree ..... default
Trunk ports ..... None
Mirror port ..... None
```

```
Attachments:
```

Module	Protocol	Format	Discrim	MAC address
-----				
GARP	Spanning tree	802.2	42	-
-----				

```
Name ..... A
Identifier ..... 10
Status ..... static
Type ..... Multiple Type
Private ..... No
Nested ..... No
Untagged ports ..... 1-24
```

## SHOW VLAN

```

Tagged ports ..... None
Associations ..... Port only
Port associations .. 1-24
Spanning Tree ..... default
Trunk ports ..... None
Mirror port ..... None
Attachments:
Module          Protocol          Format      Discrim      MAC address
-----
GARP            Spanning tree      802.2       42           -
-----

Name ..... net11
Identifier ..... 11
Status ..... static
Type ..... Multiple Type
Private ..... No
Nested ..... No
Untagged ports ..... 1-24
Tagged ports ..... None
Associations:
IP Address      NetWork Mask      Ports
-----
192.168.11.0    255.255.255.0     1-24

Index   Encap.      Protocol Name      Prot   Ports
-----
None

Port associations .. None
Spanning Tree ..... default
Trunk ports ..... None
Mirror port ..... None
Attachments:
Module          Protocol          Format      Discrim      MAC address
-----
GARP            Spanning tree      802.2       42           -
-----

Name ..... net12
Identifier ..... 12
Status ..... static
Type ..... Multiple Type
Private ..... No
Nested ..... No
Untagged ports ..... 1-24
Tagged ports ..... None
Associations:
IP Address      NetWork Mask      Ports
-----
192.168.12.0    255.255.255.0     1-24

```



```

Index   Encap.      Protocol Name   Prot  Ports
-----
None

Port associations .. None
Spanning Tree ..... default
Trunk ports ..... None
Mirror port ..... None
Attachments:
Module          Protocol        Format    Discrim    MAC address
-----
GARP            Spanning tree   802.2     42         -
-----

Name ..... B
Identifier ..... 20
Status ..... static
Type ..... Multiple Type
Private ..... No
Nested ..... No
Untagged ports ..... 25-48
Tagged ports ..... None
Associations ..... Port only
Port associations .. 25-48
Spanning Tree ..... default
Trunk ports ..... None
Mirror port ..... None
Attachments:
Module          Protocol        Format    Discrim    MAC address
-----
GARP            Spanning tree   802.2     42         -
-----

Name ..... NB
Identifier ..... 100
Status ..... static
Type ..... Multiple Type
Private ..... No
Nested ..... No
Untagged ports ..... 1-48
Tagged ports ..... None
Associations:
IP Address      NetWork Mask    Ports
-----
None

Index   Encap.      Protocol Name   Prot  Ports
-----
0       SAP        NETBEUI        f0    1-48

```

## SHOW VLAN

```

Port associations .. None
Spanning Tree ..... default
Trunk ports ..... None
Mirror port ..... None
Attachments:
Module          Protocol          Format    Discrim    MAC address
-----
GARP            Spanning tree    802.2     42         -
-----

```

Manager > show vlan

### VLAN Information

```

-----
Name ..... default
Identifier ..... 1
Status ..... static
Type ..... Port-based
Private ..... No
Nested ..... No
Untagged ports ..... 50-52
Tagged ports ..... None
Port associations .. 50-52
Spanning Tree ..... default
Trunk ports ..... None
Mirror port ..... None
Attachments:
Module          Protocol          Format    Discrim    MAC address
-----
GARP            Spanning tree    802.2     42         -
-----

```

```

Name ..... pv
Identifier ..... 2
Status ..... static
Type ..... Multiple Type
Private ..... Yes
Nested ..... No
Untagged ports ..... 1-49
Tagged ports ..... None
Uplink Ports ..... 49
Private Ports ..... 1-48
Associations ..... Port only
Port associations .. 1-49
Spanning Tree ..... default
Trunk ports ..... None
Mirror port ..... None
Attachments:
Module          Protocol          Format    Discrim    MAC address

```

```

-----
GARP                Spanning tree      802.2      42          -
-----

```

Manager > show vlan

#### VLAN Information

```

-----
Name ..... default
Identifier ..... 1
Status ..... static
Type ..... Port-based
Private ..... No
Nested ..... No
Untagged ports ..... 4-46,48-52
Tagged ports ..... None
Port associations .. 4-46,48-52
Spanning Tree ..... default
Trunk ports ..... None
Mirror port ..... None
Attachments:

```

Module	Protocol	Format	Discrim	MAC address
GARP	Spanning tree	802.2	42	-

```

-----
Name ..... Acompaany
Identifier ..... 10
Status ..... static
Type ..... Multiple Type
Private ..... No
Nested ..... Yes
Untagged ports ..... 1
Tagged ports ..... 47
Core ports ..... 47
Customer ports ..... 1
Associations ..... Port only
Port associations .. 1
Spanning Tree ..... default
Trunk ports ..... None
Mirror port ..... None
Attachments:

```

Module	Protocol	Format	Discrim	MAC address
GARP	Spanning tree	802.2	42	-

```

-----
Name ..... Bcompany
Identifier ..... 20

```

## SHOW VLAN

```
Status ..... static
Type ..... Multiple Type
Private ..... No
Nested ..... Yes
Untagged ports ..... 2
Tagged ports ..... 47
Core ports ..... 47
Customer ports ..... 2
Associations ..... Port only
Port associations .. 2
Spanning Tree ..... default
Trunk ports ..... None
Mirror port ..... None
Attachments:
Module          Protocol          Format      Discrim     MAC address
-----
GARP            Spanning tree    802.2      42          -
-----
```

```
Name ..... Ccompany
Identifier ..... 30
Status ..... static
Type ..... Multiple Type
Private ..... No
Nested ..... Yes
Untagged ports ..... 3
Tagged ports ..... 47
Core ports ..... 47
Customer ports ..... 3
Associations ..... Port only
Port associations .. 3
Spanning Tree ..... default
Trunk ports ..... None
Mirror port ..... None
Attachments:
Module          Protocol          Format      Discrim     MAC address
-----
GARP            Spanning tree    802.2      42          -
-----
```

Name	VLAN 名
Identifier	VLAN ID
Status	VLAN のステータス ( static のみ )
Type	VLAN 判定基準の種類。Port-based ( ポートのみ )、Multiple Type ( 複数の基準 ) がある

Nested	ダブルタグ VLAN ( Nested VLAN ) かどうか
Private	マルチプル VLAN ( Private VLAN ) かどうか
Untagged ports	タグなしポート
Tagged ports	タグ付きポート
Core ports	コアポート ( Nested VLAN )
Customer ports	カスタマーポート ( Nested VLAN )
Uplink ports	アップリンクポート ( Private VLAN )
Private ports	プライベートポート ( Private VLAN )
Associations セクション	ポートと IP サブネット、プロトコルの関連付けが表示される
IP Address	IP サブネット VLAN のサブネットアドレス
Network Mask	サブネットマスク
Ports	IP サブネット、プロトコルと関連付けられているポートの一覧
Index	プロトコルのインデックス番号
Encap.	Ethernet のフレームフォーマット ( エンキャプセレーション )
Protocol Name	プロトコル名称
Prot	プロトコル番号
Port associations	ポート VLAN のメンバーポート
Spanning Tree	所属先 STP ドメイン
Trunk ports	トランクポート
Mirror port	ミラーポート
Attachments セクション	VLAN インターフェースにバインドされている上位プロトコルモジュールの情報が表示される
Module	バインドされている上位モジュール名
Protocol	上位モジュールのプロトコル
Format	フレームタイプ
Discrim	上記フレームタイプに対応したプロトコル番号
MAC Address	モジュールが使用する MAC アドレス

表 107:

## 例

すべての VLAN の情報を表示する。

```
SHOW VLAN
```

## 関連コマンド

CREATE VLAN ( 225 ページ )

DESTROY VLAN ( 252 ページ )

## SHOW VLAN PORT

カテゴリー：スイッチング / バーチャル LAN

**SHOW VLAN** [= {*vlanname* | 1..4094 | ALL}] **PORT** [= *port-number*]

*vlanname*: VLAN 名 (1~32 文字。英数字とアンダースコア ( \_ )、ハイフンを使用可能。大文字小文字は区別しない)

*port-number*: スイッチポート番号 (1~)

### 解説

スイッチポートごとの VLAN 所属情報を表示する。

### パラメーター

**VLAN** VLAN 名または VLAN ID。省略時はすべての VLAN が表示される

**PORT** ポート番号。複数指定が可能。省略時はすべてのポートが対象となる

### 入力・出力・画面例

```
Manager > show vlan port=1
```

```
VLAN Port Information
```

```
-----
Port ..... 1
VLAN Name ..... A
Type ..... Multiple Type
Outgoing packets ..... untagged
Associations ..... Port only
Port association ..... Yes
```

```
VLAN Name ..... net11
Type ..... Multiple Type
Outgoing packets ..... untagged
```

```
Associations:
```

```
IP Address          Network Mask
```

```
-----
192.168.11.0        255.255.255.0
```

```
Index  Encapsulation  Protocol  Name
```

```
-----
None
```

```
Port association ..... No
```

```
VLAN Name ..... net12
Type ..... Multiple Type
Outgoing packets ..... untagged
```

```
Associations:
```

```

IP Address      Network Mask
-----
192.168.12.0    255.255.255.0
Index  Encapsulation  Protocol  Name
-----
None
Port association ..... No

VLAN Name ..... NB
Type ..... Multiple Type
Outgoing packets ..... untagged
Associations:
IP Address      Network Mask
-----
None
Index  Encapsulation  Protocol  Name
-----
0      SAP            f0        NETBEUI
Port association ..... No

```

Manager > show vlan port=1

#### VLAN Port Information

```

Port ..... 1
VLAN Name ..... pv
Type ..... Multiple Type
Port Type ..... Private
Outgoing packets ..... untagged
Associations ..... Port only
Port association ..... Yes

```

Manager > show vlan port=5

#### VLAN Port Information

```

Port ..... 5
VLAN Name ..... pv
Type ..... Multiple Type
Port Type ..... Uplink
Outgoing packets ..... untagged
Associations ..... Port only
Port association ..... Yes

```

Manager > show vlan port=1

## VLAN Port Information

```

Port ..... 1
VLAN Name ..... Acompany
Type ..... Multiple Type
Nestedtype ..... CUSTOMER
Outgoing packets ..... untagged
Associations ..... Port only
Port association ..... Yes

```

Manager > show vlan port=47

## VLAN Port Information

```

Port ..... 47
VLAN Name ..... Acompany
Type ..... Multiple Type
Nestedtype ..... CORE
Outgoing packets ..... tagged

VLAN Name ..... Bcompany
Type ..... Multiple Type
Nestedtype ..... CORE
Outgoing packets ..... tagged

VLAN Name ..... Ccompany
Type ..... Multiple Type
Nestedtype ..... CORE
Outgoing packets ..... tagged

```

Port	スイッチポート番号
VLAN Name	VLAN 名
Type	VLAN 判定基準の種類。Port-based ( ポートのみ ) Multiple Type ( 複数の基準 ) がある
Port Type	マルチプル VLAN ( Private VLAN ) のポート種別。Private ( プライベートポート ) Uplink ( アップリンクポート ) のいずれか
Nestedtype	ダブルタグ VLAN ( Nested VLAN ) のポート種別。CUSTOMER ( カスタマーポート ) CORE ( コアポート ) のいずれか
Outgoing packets	送出パケットのタグ付き ( tagged ) タグなし ( untagged )
Associations	受信したパケットを該当 VLAN 所属と判断するための基準。ポート VLAN の場合は Port only と表示される



IP Address	IP サブネット VLAN のサブネットアドレス
Network Mask	サブネットマスク
Index	プロトコルのインデックス番号
Encapsulation	Ethernet のフレームフォーマット (エンキャプセレーション)
Protocol	( プロトコル VLAN の ) プロトコル番号
Name	プロトコル名称
Port association	この VLAN のポート VLAN メンバーに該当ポートが関連付けられているか

表 108:

関連コマンド

- ADD VLAN PORT ( 191 ページ )
- DELETE VLAN PORT ( 239 ページ )
- SET VLAN PORT ( 394 ページ )