

スイッチング

概要・基本設定	8
レイヤー 3 スイッチとしての設定手順	8
ポート	10
ポートの指定方法	10
基本コマンド	10
ポートトラッキング	11
ポートミラーリング	13
基本設定	14
ハードウェア IP フィルターによるミラーリング	15
ポートセキュリティー	17
パケットストームプロテクション	19
ループガード	20
LDF 検出	20
ポート帯域制限機能	23
トリガー	23
LACP (IEEE 802.3ad)	26
基本設定	26
8748SL における制限事項	28
バーチャル LAN	29
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	33
VLAN 間ルーティング	34
Protected VLAN	36
マルチプル VLAN (Private VLAN)	37
基本ルール	37
設定例	38
スパンニングツリープロトコル (STP/RSTP)	41
基本設定	41
マルチプル STP ドメイン	42
スパンニングツリーパラメーターの設定変更	43
マルチプルスパンニングツリープロトコル (MSTP)	46

概要	46
MST インスタンス	46
MST リージョン	47
CIST	50
基本設定	50
ルーティング機能を併用するときの注意事項	55
マルチプルスパニングツリーパラメーターの設定変更	56
フォワーディングデータベース	60
FDB エントリー	60
自動学習とダイナミックエントリー	61
スタティックエントリー	62
QoS	64
プライオリティータグと送信キュー	64
送信キューの重み付けと最大送信遅延時間	65
ハードウェア IP フィルターによる IP ベースの QoS	66
ハードウェア IP フィルター	68
基本動作	68
フィルターの構成	68
フィルター処理の流れ	69
設定手順	72
フィルター（マッチ条件）の作成	72
フィルター番号の確認	74
フィルターエントリーの追加	74
8748SL における制限事項	78
コマンド例	78
設定例	83
特定スイッチポートからのみ外部への UDP 通信を許可	83
TCP 片方向通信	85
「マルチプル VLAN」的構成例	86
IP ベースの QoS	88
ハードウェア IP フィルターによるポートミラーリング	89
ポート認証	92
概要	92
802.1X 認証方式	93
基本設定	93
Authenticator	93
Authenticator（ダイナミック VLAN）	94
Supplicant	97
認証サーバー	97
DHCP Snooping	99
概要	99
登録できるクライアントの数	100

基本設定	100
コマンドリファレンス編	104
機能別コマンド索引	104
ACTIVATE PORTAUTH PORT REAUTHENTICATE	109
ACTIVATE SWITCH PORT AUTONEGOTIATE	110
ACTIVATE SWITCH PORT LOCK	111
ADD DHCP Snooping BINDING	112
ADD LACP PORT	114
ADD MSTP MSTI VLAN	116
ADD STP VLAN	117
ADD SWITCH FILTER	119
ADD SWITCH L3FILTER ENTRY	121
ADD SWITCH L3FILTER MATCH	127
ADD SWITCH TRUNK	131
ADD VLAN PORT	132
CREATE MSTP MSTI	134
CREATE STP	135
CREATE SWITCH TRUNK	136
CREATE VLAN	138
DELETE DHCP Snooping BINDING	140
DELETE LACP PORT	141
DELETE MSTP MSTI VLAN	142
DELETE STP VLAN	143
DELETE SWITCH FILTER	144
DELETE SWITCH L3FILTER	145
DELETE SWITCH L3FILTER ENTRY	146
DELETE SWITCH TRUNK	147
DELETE VLAN PORT	148
DESTROY MSTP MSTI	149
DESTROY STP	150
DESTROY SWITCH TRUNK	151
DESTROY VLAN	152
DISABLE DHCP Snooping	153
DISABLE DHCP Snooping ARPSECURITY	154
DISABLE DHCP Snooping LOG	155
DISABLE DHCP Snooping OPTION82	156
DISABLE LACP	157
DISABLE LACP DEBUG	158
DISABLE MSTP	159
DISABLE MSTP CIST PORT	160
DISABLE MSTP DEBUG MSTI	161
DISABLE MSTP MSTI PORT	162

DISABLE PORTAUTH	163
DISABLE PORTAUTH DEBUG	164
DISABLE PORTAUTH PORT	165
DISABLE STP	166
DISABLE STP DEBUG	167
DISABLE STP PORT	168
DISABLE STP PORT DEBUG	169
DISABLE SWITCH AGEINGTIMER	170
DISABLE SWITCH DEBUG	171
DISABLE SWITCH FILTER VLANSECURE	172
DISABLE SWITCH L3FILTER	173
DISABLE SWITCH LEARNING	174
DISABLE SWITCH LOOPDETECTION	175
DISABLE SWITCH MIRROR	176
DISABLE SWITCH PORT	177
DISABLE SWITCH PORT FLOW	178
DISABLE SWITCH STPFORWARD	179
DISABLE VLAN DEBUG	180
ENABLE DHCP Snooping	181
ENABLE DHCP Snooping ARPSECURITY	182
ENABLE DHCP Snooping LOG	183
ENABLE DHCP Snooping OPTION82	184
ENABLE LACP	185
ENABLE LACP DEBUG	186
ENABLE MSTP	187
ENABLE MSTP CIST PORT	188
ENABLE MSTP DEBUG MSTI	189
ENABLE MSTP MSTI PORT	191
ENABLE PORTAUTH	192
ENABLE PORTAUTH DEBUG	193
ENABLE PORTAUTH PORT	194
ENABLE STP	199
ENABLE STP DEBUG	200
ENABLE STP PORT	201
ENABLE STP PORT DEBUG	202
ENABLE SWITCH AGEINGTIMER	203
ENABLE SWITCH DEBUG	204
ENABLE SWITCH FILTER VLANSECURE	205
ENABLE SWITCH L3FILTER	206
ENABLE SWITCH LEARNING	207
ENABLE SWITCH LOOPDETECTION	208
ENABLE SWITCH MIRROR	210

ENABLE SWITCH PORT	211
ENABLE SWITCH PORT FLOW	212
ENABLE SWITCH STP FORWARD	213
ENABLE VLAN DEBUG	214
PURGE LACP	215
PURGE MSTP	216
PURGE PORTAUTH PORT	217
PURGE STP	218
RESET DHCP Snooping COUNTER	219
RESET LACP PORT COUNTER	220
RESET MSTP COUNTER PORT	221
RESET PORTAUTH PORT	222
RESET PORTAUTH PORT MULTIMIB	223
RESET STP	224
RESET SWITCH	225
RESET SWITCH PORT	226
SET DHCP Snooping CHECKINTERVAL	227
SET DHCP Snooping PORT	228
SET LACP PORT	230
SET LACP PRIORITY	231
SET MSTP	232
SET MSTP CIST	234
SET MSTP CIST PORT	235
SET MSTP MSTI	237
SET MSTP MSTI PORT	238
SET PORTAUTH HYPHEN	239
SET PORTAUTH IDTOGGLE	240
SET PORTAUTH PORT	241
SET PORTAUTH PORT SUPPLICANTMAC	245
SET PORTAUTH USERNAME	248
SET QOS HWPRIORITY	250
SET QOS HWQUEUE	252
SET STP	254
SET STP PORT	256
SET SWITCH AGEINGTIMER	258
SET SWITCH L3AGEINGTIMER	259
SET SWITCH L3FILTER ENTRY	260
SET SWITCH L3FILTER MATCH	265
SET SWITCH LOOPDETECTION	268
SET SWITCH MIRROR	270
SET SWITCH PORT	271
SET SWITCH QOS	274

SET SWITCH TRUNK	276
SET VLAN PORT	277
SHOW DHCP Snooping	278
SHOW DHCP Snooping Counter	280
SHOW DHCP Snooping Database	282
SHOW DHCP Snooping Filter	285
SHOW DHCP Snooping Port	286
SHOW LACP	288
SHOW LACP Port	289
SHOW LACP Trunk	293
SHOW MSTP	295
SHOW MSTP CIST	298
SHOW MSTP CIST Port	301
SHOW MSTP Counter Port	304
SHOW MSTP Debug MSTI	306
SHOW MSTP MSTI	307
SHOW MSTP MSTI Port	310
SHOW PortAuth	312
SHOW PortAuth Counter	316
SHOW PortAuth MultiSupplicant Port	319
SHOW PortAuth Port	323
SHOW PortAuth Timer	329
SHOW QoS HwPriority	333
SHOW QoS HwQueue	334
SHOW STP	335
SHOW STP Counter	339
SHOW STP Debug	341
SHOW STP Port	343
SHOW Switch	346
SHOW Switch Counter	348
SHOW Switch Debug	350
SHOW Switch FDB	351
SHOW Switch Filter	354
SHOW Switch L3Filter	356
SHOW Switch LoopDetection	360
SHOW Switch LoopDetection Counter	363
SHOW Switch Port	365
SHOW Switch Port Counter	369
SHOW Switch Port Intrusion	373
SHOW Switch QoS	374
SHOW Switch Trunk	375
SHOW VLAN	377

SHOW VLAN DEBUG	381
---------------------------	-----

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 (138 ページ) で、ポートの割り当ては ADD VLAN PORT コマンド (132 ページ) で行います。

```
CREATE VLAN=white VID=10 ↵  
CREATE VLAN=orange VID=20 ↵  
ADD VLAN=white PORT=1-12 ↵  
ADD VLAN=orange PORT=13-24 ↵
```

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 288 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 181 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 191 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 (211 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 (177 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 (271 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 ↵
```

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 (110 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 ↵
```

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 (226 ページ) を使います。

```
RESET SWITCH PORT=3,6 ↵
```

ポートの状態を確認するには SHOW SWITCH PORT コマンド (365 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 (369 ページ) を使います。

```
SHOW SWITCH PORT=4 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 (226 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 ↵
```

ポートトランキング

ポート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。

本製品ではトランクグループを 6 つまで作成できます。それぞれのトランクグループには、最大 8 ポートまで所属させることが可能です。ポートは隣接していなくてもかまいません。ただし、同一グループ内に 10/100M ポートと 1000M ポートを混在させることはできません。

ポートトラン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。

- ✎ 8748SL では、1000M ポートのトランキングはできません（8724SL は可能）。
- ✎ 8748SL では、トランクグループがポートグループ「1～24」と「25～48」をまたぐような設定はできません。トランクポートが「1～24」または「25～48」のどちらかのポートグループにすべて入るよう設定してください。
- ✎ 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。
- ✎ トランクグループにポートを追加したあとで、グループ全体あるいはグループ内のポートを所属 VLAN から削除することはできません。VLAN から削除するには、DELETE SWITCH TRUNK コマンド（147 ページ）を使ってあらかじめポートをトランクグループから外しておく必要があります。トランクグループにポートを割り当てた後で、別の VLAN にグループ全体あるいはグループ内のポートを追加することは可能です。
- ✎ ポートトランキングの設定は、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。
- ✎ ポートトラン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（375 ページ）で確認できます。

```
SHOW SWITCH TRUNK=aggr1 ↵
```

送信時のポート選択基準は CREATE SWITCH TRUNK コマンド（136 ページ）、SET SWITCH TRUNK コマンド（276 ページ）の SELECT パラメーターで指定できます。次の例ではトランクグループ「aggr1」のポート選択基準を、送信元 MAC アドレスに変更しています。デフォルトでは、送信元 MAC アドレスと宛先 MAC アドレスの両方（MACBOTH）を使って、トランク内のどのポートを使用するかが決定されます。

```
SET SWITCH TRUNK=aggr1 SELECT=MACSRC ↵
```

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、SELECT パラメーターの設定とは関係なく、常に終点 IP アドレス（IPDEST）に基づいて決定されます（負荷分散されません）。

- ✎ ただし、8748SL では、受信ポートとトランクポートがポートグループ「1～24」と「25～48」をまたいだ場合（たとえば、受信ポート（VLAN1 とします）がポート 47 で、トランクポート（VLAN2 とします）がポート 1～4 の場合）、トランクポートから送信されるパケットの負荷分散が行われません（冗長機能は動作します）。

✎ ソフトウェアルーティングされたパケットは負荷分散の対象になりません。

フラディングパケットは、トランクグループ内で一番最初にリンクが確立されたポートから送出されます。

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。

トランクグループからポートを削除するには DELETE SWITCH TRUNK コマンド (147 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 (151 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 (147 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。

また、ハードウェア IP フィルターを併用することで、IP/TCP/UDP ヘッダー情報をもとに特定のトラフィックだけをミラーポートにコピーするよう設定することも可能です。

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。

- L3 スイッチング (ハードウェアルーティング) される IP パケット (ハードウェア IP フィルターによってミラーリングされたパケットを含む) は、すべてタグ付き状態でミラーポートに出力されます。
- L3 スイッチング (ハードウェアルーティング) される IP パケットは、ルーティング処理後にミラーポートから出力されます。
- ソースポートを複数設定している場合で、かつソースポートにタグ付きとタグなしが混在している場合、送信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。
- ソースポートを複数設定している状態で、あるソースポートから入力されたパケットが、L2 スイッチングされて別のソースポートから出力された場合、ミラーポートにはパケットが 1 個だけ出力されます。
- ソースポートを複数設定している状態で、あるソースポートから入力されたパケットが、L3 スイッチング (ハードウェアルーティング) されて別のソースポートから出力された場合、ミラーポートにはルーティング処理後のパケットが 1 個だけ出力されます。
- ソースポートを複数設定している状態で、あるソースポートから入力されたパケットが、ソフトウェ

ルーティングされて別のソースポートから出力された場合、ミラーポートにはルーティング処理前のパケットとルーティング処理後のパケットの両方が出力されます。また、ルーティング処理後のパケットは、実際の出力ポートのタグ設定にかかわらず、つねにタグなし状態でミラーポートに出力されます。

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。

1. 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 (270 ページ) を実行します。

```
DELETE VLAN=somevlan PORT=1 ↵
```

SET SWITCH MIRROR コマンド (270 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 (271 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。また、複数のソースポートを指定した場合で、かつ指定ポートにタグ付きとタグなしが混在している場合、送信パケットはすべてタグなしとしてミラーリングされます。

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 (346 ページ) を実行します。ミラーポートは SHOW VLAN コマンド (377 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 (365 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 (176 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 (270 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 (271 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 (270 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。

ハードウェア IP フィルターによるミラーリング

ポートミラーリング機能とハードウェア IP フィルターを併用すると、IP アドレスや TCP/UDP のポート番号を基準に、特定の IP トラフィックだけをミラーポートに送るよう設定することができます。

なお、仕様によりハードウェア IP フィルター経由でミラーリングされたパケットは、VLAN タグが付いた状態でミラーポートに出力されます。キャプチャーソフトが VLAN タグを識別できない場合、IP パケットがプロトコルタイプ 0x8100 (802.1Q タグ) として表示される場合がありますのでご注意ください。

ここでは、ハードウェア IP フィルターを使って、サーバー 192.168.10.5 に出入りする IP トラフィックだけをミラーポート (ポート 1) にコピーする設定例を示します。

1. 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 (270 ページ) を実行します。

```
DELETE VLAN=somevlan PORT=1 ↵
```

SET SWITCH MIRROR コマンド (270 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. ミラーリングするパケットの条件を指定するため、ハードウェア IP フィルターを作成します。ここでは 2 つのフィルターを作成し、マッチ条件としてそれぞれ始点 IP アドレスと終点 IP アドレスを指定します。

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=HOST ↓
```

```
ADD SWITCH L3FILTER MATCH=DIPADDR DCLASS=HOST ↓
```

4. 各フィルターにフィルターエントリーを追加して、実際のフィルタリング条件を指定します。ここで対象パケットは「192.168.10.5 (サーバー) が始点となる IP パケット」と「192.168.10.5 が終点となる IP パケット」であり、対象パケットに対するアクションは「SENDMIRROR (ミラーポートに送る)」となります。

```
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.5 ACTION=SENDMIRROR ↓
```

```
ADD SWITCH L3FILTER=2 ENTRY DIPADDR=192.168.10.5 ACTION=SENDMIRROR ↓
```

設定は以上です。

ミラーリング対象パケットに対して他のアクション (TOS 優先度書き換え、プライオリティタグ付与など) を並行して適用したい場合は、手順 4 の ACTION パラメーターにカンマ区切りで複数のアクションを指定してください。

```
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.5 PRIORITY=7
```

```
ACTION=SENDMIRROR,SETPRIORITY ↓
```

```
ADD SWITCH L3FILTER=2 ENTRY DIPADDR=192.168.10.5 PRIORITY=7
```

```
ACTION=SENDMIRROR,SETPRIORITY ↓
```

このように同一エントリーで複数のアクションを指定せず、別のエントリーで他のアクションを指定すると、エントリー番号の大きいエントリー (通常あとから追加したエントリー) で指定されたアクションだけが適用されます。たとえば、上記の手順 1~5 を実行したあとで下のコマンドを入力すると、プライオリティ付与だけが行われミラーポートへの出力は行われなくなります。

```
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.5 PRIORITY=7
```

```
ACTION=SETPRIORITY ↓
```

```
ADD SWITCH L3FILTER=2 ENTRY DIPADDR=192.168.10.5 PRIORITY=7
```

```
ACTION=SETPRIORITY ↓
```

また、一致するエントリーに DENY アクションが含まれている場合は、エントリーの順序に関係なく DENY アクション (破棄) が実行されます。これはハードウェア IP フィルターの仕様です。

ハードウェア IP フィルターの詳細については、「ハードウェア IP フィルター」をご覧ください。

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 (271 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 (271 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 (271 ページ) を使います。たとえば、ポート 3 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=3 LEARN=20 INTRUSIONACTION=DISABLE ↵
```

SET SWITCH PORT コマンド (271 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ー (ダイナミックエントリー) がフォワーディングデータベースから削除され、エントリー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 (271 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)。

- 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。

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」なものと思われ、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 3

Intrusion event.  Disabling port 3
```

学習済みのアドレスを確認するには、SHOW SWITCH FILTER コマンド (354 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=3 ↓
```

ポートセキュリティの設定状況は SHOW SWITCH PORT コマンド (365 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」欄には不正フレーム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=3 ↓
```

不正とみなされた MAC アドレスは SHOW SWITCH PORT INTRUSION コマンド (373 ページ) で確認できます。

```
SHOW SWITCH PORT INTRUSION ↓
SHOW SWITCH PORT=3 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 (111 ページ) を使います。あらかじめ SET SWITCH PORT コマンド (271 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 (119 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=3 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 (144 ページ) で行います。ENTRY 番号は SHOW SWITCH FILTER コマンド (354 ページ) で確認してください。

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

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 (271 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=3 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 (211 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 (271 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=3
```

```
Error (387312): Port 3 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 151 ページ) によって保存されます (SET SWITCH PORT コマンド (271 ページ) の RELEARN パラメーターが OFF の場合)。

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、ポートグループごとにブロードキャスト/マルチキャスト/未学習のユニキャストフレーム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フレームを受信した場合、フレームは破棄されます。本機能はデフォルトではオフになっています。

受信レートは、下記のポートグループ単位で設定します。

機種	ポートグループ
8724SL	ポート 1～8
	ポート 9～16
	ポート 17～24
	ポート 25 (GBIC モジュール)
	ポート 26 (GBIC モジュール)
8748SL	ポート 1～8
	ポート 9～16
	ポート 17～24
	ポート 25～32
	ポート 33～40
	ポート 41～48
	ポート 49 (GBIC モジュール)
	ポート 50 (GBIC モジュール)

表 2: ポートグループ

制限できるのは以下のフレームです。カッコ内は設定パラメーターの名前です。

- ブロードキャストフレーム (BCLIMIT)
- マルチキャストフレーム (MCLIMIT)
- 未学習のユニキャストフレーム (DLFLIMIT)

受信レートの上限値は、1 ポートグループあたり 1 つだけ設定できます。たとえば、ブロードキャストフレームの受信レートを 1000 個/秒に設定した場合、マルチキャストフレームと未学習のユニキャストフレームには、同じ値 (1000 個/秒) を設定するか、上限を設定しないかのどちらかの選択となります。

受信レートの設定は SET SWITCH PORT コマンド (271 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、ブロードキャストフレームの受信レートを 1 秒あたり 1000 個に制限します。

```
SET SWITCH PORT=1-8 BCLIMIT=1000 ↵
```

受信レートの制限を解除するには値として NONE を指定します。

```
SET SWITCH PORT=1-8 BCLIMIT=NONE ↵
```

パケットストームプロテクションの設定状況は SHOW SWITCH PORT コマンド (365 ページ) で確認できます。「Broadcast rate limit」、「Multicast rate limit」、「DLF rate limit」をご覧ください。

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。

- LDF 検出

LDF 検出

LDF 検出は、LDF (Loop Detection Frame) と呼ぶ特殊フレームを利用してネットワーク上のループを検出し、これに対応するための動作を自動的に行う機能です。

- ☞ 配下の HUB やスイッチにて輻輳などにより LDF が消失した場合、ループを検出できない場合があります。

LDF は、特殊な宛先 MAC アドレス (FE-FF-FF-xx-xx-xx。xx-xx-xx はスイッチの MAC アドレス下位 3 オクテット) を持った試験フレームです。

LDF 検出機能を有効にしたポートでは、一定時間ごとに LDF を送出します。

送出した LDF が他の接続機器を経由するなどして戻ってきた場合 (受信した LDF の送信元 MAC アドレスが自身の MAC アドレスと一致した場合) ループ状態と判断し、受信ポートで次のいずれかの動作を行います。

- ☞ SET SWITCH LOOPDETECTION コマンド (268 ページ) で SECURE=ON に設定した場合は、LDF に含まれる ID のチェックも行います。

DISABLEPORT	ポートをディセーブルにする (物理的なリンクはアップ状態のまま)。また、ループ検出時と動作実行時にログ記録を行う。
LINKDOWN	ポートを物理的にリンクダウンさせる。また、ループ検出時と動作実行時にログ記録を行う。
NONE	ループ検出時のログ記録だけを行う。

表 3: LDF によるループ検出時の動作

アクション実行後はタイマーが起動し、指定した時間が経過すると動作実行前の状態に戻ります。

- ☞ ループ検出後のアクションの副次的な作用として、アクションが実行されるときと実行前の状態に戻るときに SNMP のリンクトラップが出力されます。

LDF 検出機能を有効化するには、ENABLE SWITCH LOOPDETECTION コマンド (208 ページ) を実行します。

PORT パラメーターを省略した場合は、すべてのポートで LDF 検出機能が有効になります。

```
ENABLE SWITCH LOOPDETECTION=LDF ↓
```

PORT パラメーターを指定した場合は、指定したポートでのみ LDF 検出機能が有効になります。

```
ENABLE SWITCH LOOPDETECTION=LDF PORT=1-8 ↓
```

ループ検出時の動作設定は SET SWITCH LOOPDETECTION コマンド (268 ページ) の ACTION パラメーターで行います。デフォルトは NONE (ログへの記録のみ) ですが、これを DISABLEPORT (LDF 受信ポートのディセーブル) に変更するには次のようにします。

```
SET SWITCH LOOPDETECTION=LDF ACTION=DISABLEPORT ↓
```

- ループ検出時の動作はシステム全体で1つしか設定できません（ポートごとに異なる動作をさせる設定はできません）。ENABLE SWITCH LOOPDETECTION コマンド（208 ページ）にも ACTION パラメーターがありますが、同コマンドで ACTION パラメーターを指定した場合、PORT パラメーターで対象スイッチポートを限定していても、ACTION パラメーターの設定はシステム全体に適用されますのでご注意ください。

ループ検出後のアクションの持続時間（ループ検出によって動作が実行された後、自動的に実行前の状態に戻るまでの時間）は、SET SWITCH LOOPDETECTION コマンド（268 ページ）の PDTO（Port Disable Time Out）パラメーターで変更できます（デフォルトは 300 秒）。たとえば、持続時間を 60 秒に変更するには次のようにします。

```
SET SWITCH LOOPDETECTION=LDF PDTO=60 ↓
```

LDF の送信間隔は、SET SWITCH LOOPDETECTION コマンド（268 ページ）の LDFINTERVAL パラメーターで変更できます（デフォルトは 120 秒）。たとえば、送信間隔を 90 秒に変更するには、次のようにします。

```
SET SWITCH LOOPDETECTION=LDF LDFINTERVAL=90 ↓
```

LDF 検出機能を無効化するには、DISABLE SWITCH LOOPDETECTION コマンド（175 ページ）を実行します。

PORT パラメーターを省略した場合は、すべてのポートで LDF 検出機能が無効になります。

```
DISABLE SWITCH LOOPDETECTION=LDF ↓
```

PORT パラメーターを指定した場合は、指定したポートでのみ LDF 検出機能が無効になります。

```
DISABLE SWITCH LOOPDETECTION=LDF PORT=1-8 ↓
```

LDF 検出機能の設定や状態、統計情報は SHOW SWITCH LOOPDETECTION コマンド（360 ページ）、SHOW SWITCH LOOPDETECTION COUNTER コマンド（363 ページ）で確認できます。

併用可能な機能と注意事項

スイッチポート単位で設定する機能のうち、同一ポート上で LDF 検出と併用できるのは次の機能に限定されます。

- ポートトラッキング・LACP
- タグ VLAN
- スパニングツリープロトコル（STP/RSTP）
- ポート認証（802.1X 認証、MAC ベース認証）

なお、併用可能な機能についても下記の注意事項があります。

- ポートトラッキング・LACP

- ポートトラッキング・LACP を併用するときは、トラッキンググループの所属ポートすべてに同じ LDF 検出の設定を行ってください。なお、一部の所属ポートにだけ LDF 検出の設定を行っても、すべての所属ポートに同じ LDF 検出設定が自動的に適用されます。
- ポート認証 (802.1X 認証、MAC ベース認証)
 - 802.1X 認証を併用するときは、デフォルトの Single-SupPLICANT モードを使ってください。Multi-SupPLICANT モードは使えません。
(MAC ベース認証には Single-SupPLICANT モード、Multi-SupPLICANT モードの区別がないため、本制限は適用されません)

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、受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 (271 ページ) の INGRESSLIMIT (受信レート)、EGRESSLIMIT (送信レート) パラメーターで行います。ポートの速度 (10/100M か 1000M か) によって指定できる値の範囲と単位が異なるので注意してください。

ポート 1 の受信レートを 20480Kbps (20Mbps) に制限するには、次のようにします。受信レートの上限値は、10/100M ポートの場合は 64 ~ 127000 (Kbps)、1000M ポートの場合は 8 ~ 1016 (Mbps) の範囲で指定します。

```
SET SWITCH PORT=1 INGRESSLIMIT=20480 ↵
```

- 📎 10/100M ポートで指定値が 1000Kbps 未満のとき、実際の受信レート上限値は 64Kbps の倍数になるように切り捨てられます。10/100M ポートで指定値が 1000Kbps 以上のときは、1000Kbps の倍数になるように切り捨てられます。1000M ポートの場合は、8Mbps の倍数になるように切り捨てられます。

ポート 25 (GBIC モジュールを装着しているものと仮定) の送信レートを 500Mbps に制限するには、次のように指定します。送信レートの上限値は、10/100M ポートの場合は 1000 ~ 127000 (Kbps)、1000M ポートの場合は 8 ~ 1016 (Mbps) の範囲で指定します。

```
SET SWITCH PORT=25 EGRESSLIMIT=500 ↵
```

- 📎 10/100M ポートの場合、送信レート上限値の有効範囲 (1000 ~ 127000Kbps) と受信レート上限値の有効範囲 (64 ~ 127000Kbps) が異なるので注意してください。
- 📎 10/100M ポートで指定値が 1000Kbps の倍数でないとき、実際の送信レート上限値は 1000Kbps の倍数になるように切り捨てられます。1000M ポートの場合は、8Mbps の倍数になるように切り捨てられます。

ポートの帯域制限を解除するには値として NONE か 0 を指定します。

```
SET SWITCH PORT=25 EGRESSLIMIT=NONE ↵
```

ポート帯域制限機能の設定状況は SHOW SWITCH PORT コマンド (365 ページ) で確認できます。「Ingress rate limit」、「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 170 ページ）、SET TRIGGER MODULE コマンド（「運用・管理」の 330 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 260 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 6、トランクグループの所属ポート数は最大 8 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。ただし、同一グループ内に 10/100M ポートと 1000M ポートを混在させることはできません。

前記の条件を満たすポートが 9 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 8 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 (136 ページ)、ADD SWITCH TRUNK コマンド (131 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 (185 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 (141 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 8 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 1~10 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=1-10 ↓
```

このように設定すると、通常時はポート 1~8 がメンバーポートに選択され、ポート 9、10 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 9 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 9 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 (288 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 (289 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 (293 ページ) で確認できます。また、SHOW SWITCH TRUNK コマンド (375 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 とポート認証は併用できません (LACP によって生成されたトランクポートでは、ポート認証を使用できません)。

LACP によって生成されたトランクグループから送信されるパケットの送出ポートは、送信元 MAC アドレスと宛先 MAC アドレスの両方に基づいて決定されます。ただし、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、終点 IP アドレスに基づいて決定されます (負荷分散されます)。また、フラディングパケットは、トランクグループ内で一番最初にリンクが確立されたポートから送出されます。

- ✎ ただし、8748SL では、受信ポートとトランクポートがポートグループ「1~24」と「25~48」をまたいだ場合 (たとえば、受信ポート (VLAN1 とします) がポート 47 で、トランクポート (VLAN2 とします) がポート 1~4 の場合) トランクポートから送信されるパケットの負荷分散が行われません (冗長機能は動作します)。
- ✎ ソフトウェアルーティングされたパケットは負荷分散の対象になりません。

8748SL における制限事項

8748SL には、LACP の使用に関して、以下に述べる仕様上の制限事項があります。これらの制限は 8748SL 固有のもので、8724SL にはありません。

8748SL では、1000M ポートのトランキングができないため、1000M ポートでは LACP を無効化し、トランクグループが自動構成されないようにしてください。

```
DELETE LACP PORT=49-50 ↵
```

8748SL では、ポートグループ「1~24」と「25~48」をまたぐトランキングができないため、ポート 1~24 とポート 25~48 にそれぞれ異なるポート鍵を設定し、ポートグループをまたぐトランクグループが自動構成されないようにしてください。ポート鍵 (のもととなる値) は ADD LACP PORT コマンド (114 ページ) SET LACP PORT コマンド (230 ページ) の ADMINKEY パラメーターで設定します (デフォルト値は 1)。

```
SET LACP PORT=1-24 ADMINKEY=10 ↵
SET LACP PORT=25-48 ADMINKEY=20 ↵
```

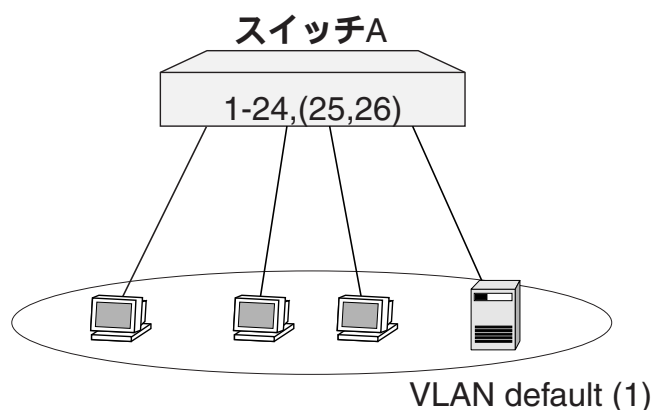
バーチャル LAN

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フレームと、マルチキャスト/ブロードキャストフレーム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。

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。

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。



🔗 GBIC スロットは、GBIC モジュールが装着されていない場合でも、システムからはポートとして認識されます。

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 (138 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、数字だけの文字列と「default」、「ALL」は使用できません) VID は 2~4094 の範囲の任意の数値です (1 は VLAN default のために予約済みです)。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。

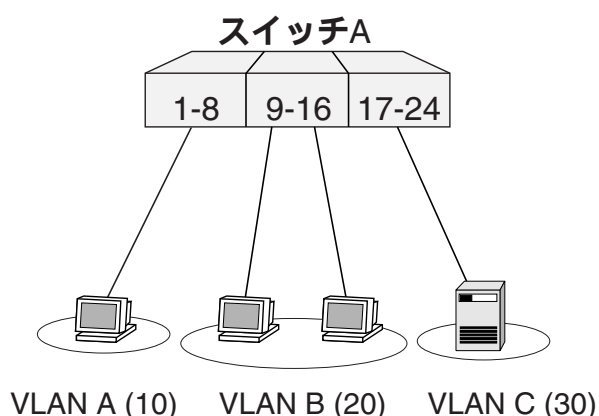
```
CREATE VLAN=A VID=10 ↵
CREATE VLAN=B VID=20 ↵
CREATE VLAN=C VID=30 ↵
```

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 (132 ページ) で VLAN にポートを割り当てます。ここでは、VLAN A にポート 1~8 を、VLAN B にポート 9~16 を、VLAN C にポート 17~24 を割り当てます。

```
ADD VLAN=A PORT=1-8 ↵
ADD VLAN=B PORT=9-16 ↵
ADD VLAN=C PORT=17-24 ↵
```

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。すなわち、上記の設定を終えると VLAN default の所属ポートは、ポート 25 と 26 だけになります (この例では使用しません)。



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 (377 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 (148 ページ) を使います。たとえば、ポート 7 と 8 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=7-8 ↵
```

VLAN を削除するには、DESTROY VLAN コマンド (152 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。

各ポートの VLAN 設定には次のルールが適用されます。

- ポートは、0 ~ 1 つの VLAN にタグなしポート (Untagged Port) として所属できる
- ポートは、0 ~ 複数の VLAN にタグ付きポート (Tagged Port) として所属できる
- ミラーポート以外のポート (通常のポート) は、必ず 1 つ以上の VLAN に所属していなくてはならない

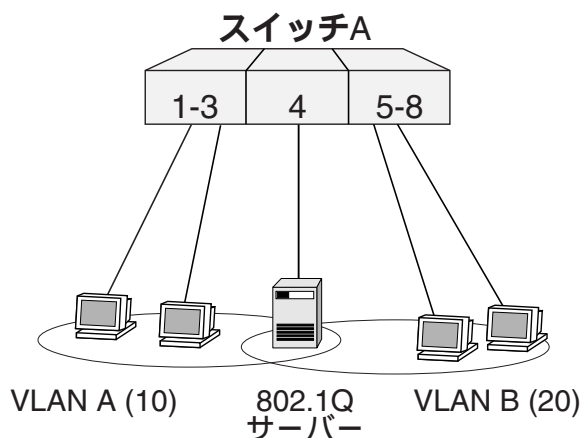
🔑 VLAN タグを使用する場合、接続先機器も VLAN タグ (802.1Q) に対応している必要があります。

🔑 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 (132 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

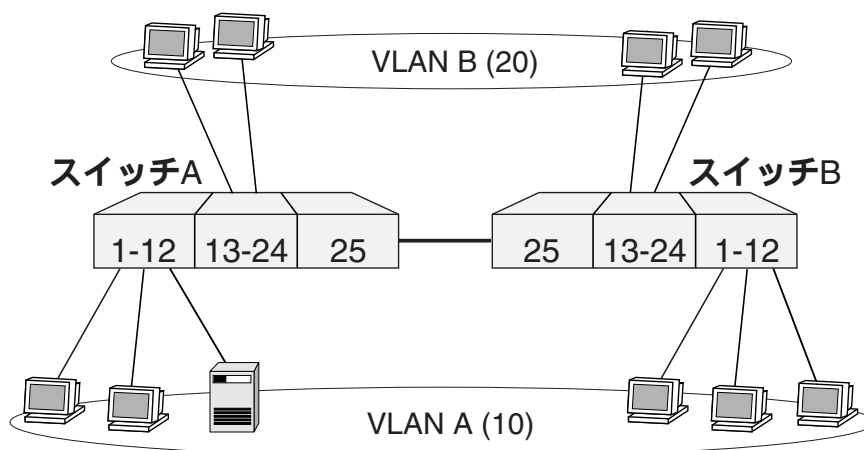
表 4:

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（148 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 25 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 1～12 はタグを使わない通常のポートに設定し、ポート 25 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（132 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=1-12 ↵
```

```
ADD VLAN=A PORT=25 FRAME=TAGGED ↵
```

3. VLAN B にポートを追加します。ポート 13~24 はタグを使わない通常のポートに設定し、ポート 25 はタグを使用するポートとして設定します。

```
ADD VLAN=B PORT=13-24 ↵
```

```
ADD VLAN=B PORT=25 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 (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 25 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 25 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 (148 ページ) を使って、ポート 25 を VLAN default から削除します。

```
DELETE VLAN=default PORT=25 ↵
```

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=1-8 ↵
```

```
ADD VLAN=B PORT=9-16 ↵
```

```
ADD VLAN=C PORT=17-24 ↵
```

3. IP を使用するため、IP ルーティング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 181 ページ) で行います。

```
ADD IP INT=vlan-A IP=192.168.10.1 MASK=255.255.255.0 ↵
```

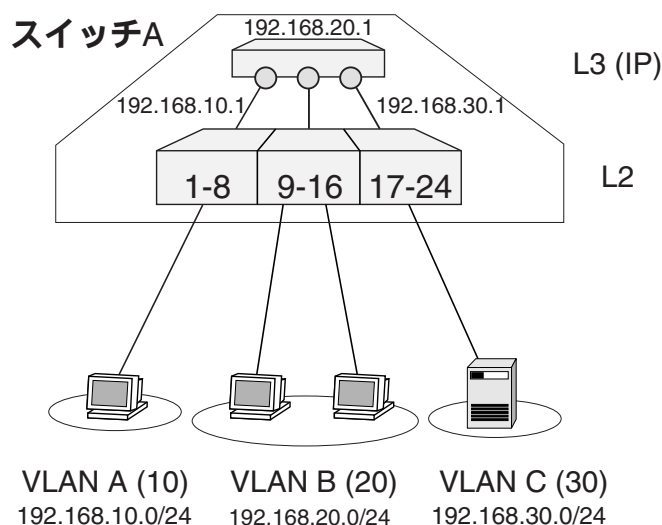
```
ADD IP INT=vlan-B IP=192.168.20.1 MASK=255.255.255.0 ↵
```

```
ADD IP INT=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、一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 名のときとは異なり、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 450 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 191 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 ↵
```

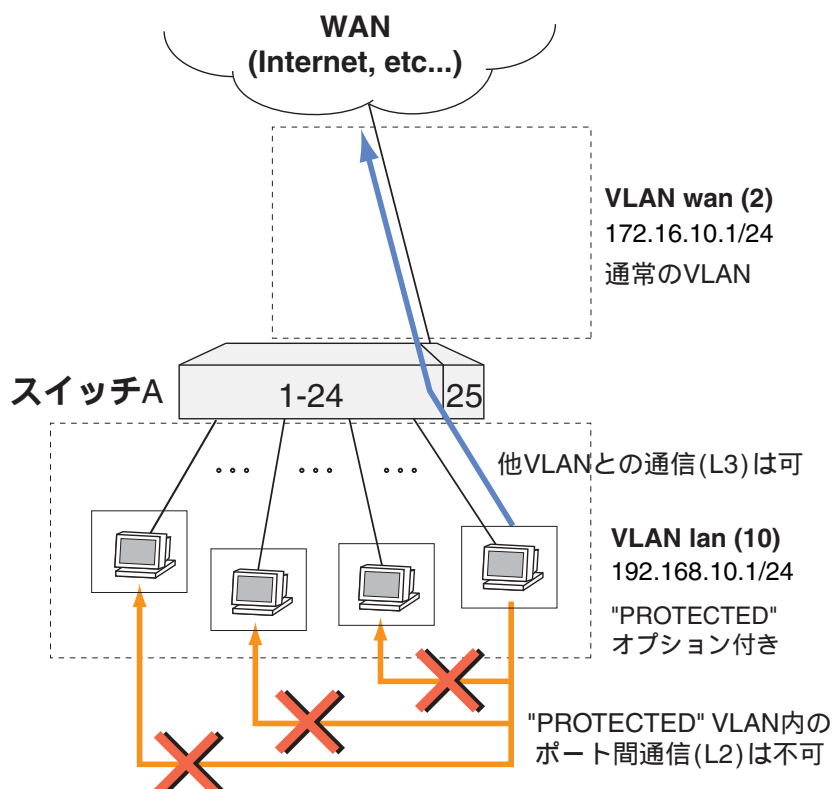
詳細は「IP」の章をご覧ください。

Protected VLAN

CREATE VLAN コマンド（138 ページ）に PROTECTED オプションを付けると、作成した VLAN 内ではポート間のレイヤー 2 通信ができなくなります（レイヤー 3 通信は可能です）。

- Protected VLAN とマルチプル VLAN（Private VLAN）は併用できません。なお、Protected VLAN はレイヤー 3 スイッチとしての機能、Private VLAN はレイヤー 2 スイッチとしての機能です。

次に設定例を示します。



1. 2つの VLAN、wan (VID=2) と lan (VID=10) を作成します。VLAN lan は PROTECTED オプション付きで作成し、Protected VLAN とします。

```
CREATE VLAN=wan VID=2 ↵
CREATE VLAN=lan VID=10 PROTECTED ↵
```

2. 各 VLAN にポートを割り当てます。

```
ADD VLAN=wan PORT=25 ↵
ADD VLAN=lan PORT=1-24 ↵
```

🔗 Protected VLAN の所属ポートは、すべてタグなし (Untagged) に設定してください。

🔗 Protected VLAN 内では、IGMP Snooping を使用できません。

3. IP を有効にします。

```
ENABLE IP ↵
```

4. 各 VLAN に IP アドレスを割り当てます。

```
ADD IP INT=vlan-wan IP=172.16.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-lan IP=192.168.10.1 MASK=255.255.255.0 ↵
```

設定は以上です。

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ートポートという 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原則として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。

なお、本製品の Private VLAN では、プライベートポートをグループ分けすることにより、同一グループ所属のプライベートポート間で通信を可能にすることもできます。

🔗 8748SL では、ポートグループ「1 ~ 24、50」と「25 ~ 48、49」をまたぐプライベートポートグループは作成できません。

🔗 Protected VLAN とマルチプル VLAN (Private VLAN) は併用できません。なお、Protected VLAN はレイヤー 3 スイッチとしての機能、Private VLAN はレイヤー 2 スイッチとしての機能です。

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 つ以上必要。
- 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原則として通信できない。ただし、同一グループに設定されたプライベートポート間では通信可能。
- ルーティングの設定が行われている場合、プライベートポートと別 VLAN のポートとの間の通信は可能。

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、複数設定することが可能。
- 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 との併用が可能。

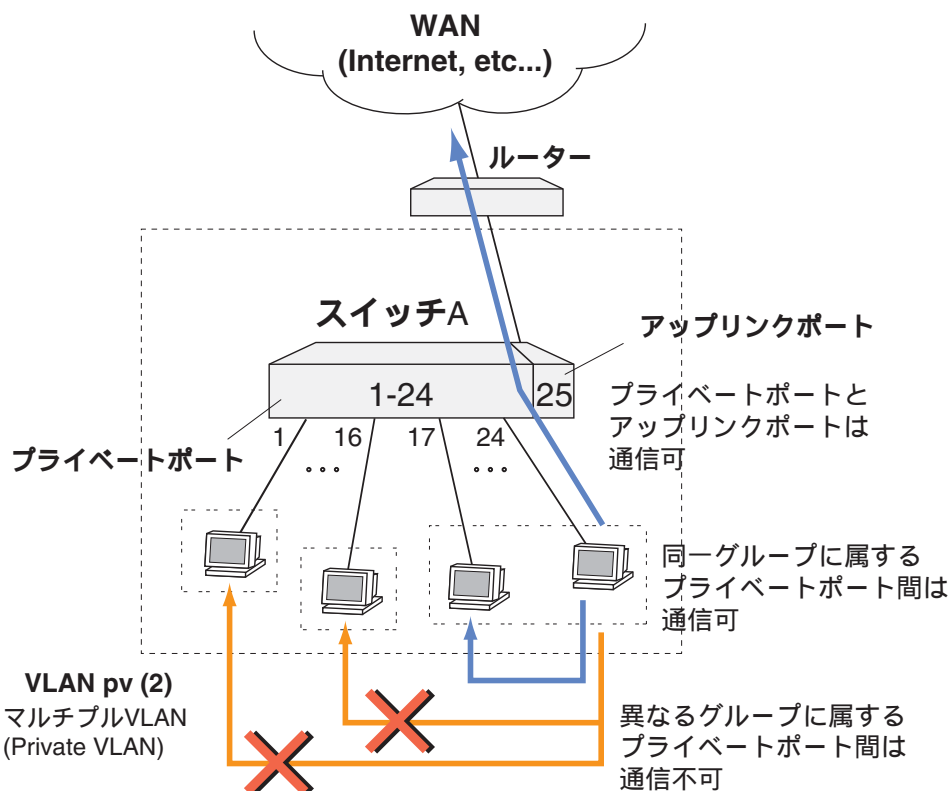
プライベートポートには次のルールが適用されます。

- プライベートポートは、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 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。

設定例

次に Private VLAN の設定例を示します。

ここでは、ポート 25 をアップリンクポートとし、ポート 1～24 をプライベートポートとする Private VLAN 「pv」を作成します。プライベートポートの中でも、ポート 17～24 は 1 つのグループとして互いに通信できるようにします。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 (138 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 (132 ページ) に UPLINK オプションを付けて実行します。

```
ADD VLAN=pv PORT=25 UPLINK ㍿
```

✎ 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 (132 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。最初に、ポート 1~16 を各々独立したプライベートポートとして追加します。これには、ADD VLAN PORT コマンド (132 ページ) をオプションなしで実行します。

```
ADD VLAN=pv PORT=1-16 ↵
```

- ☞ アップリンクポートを割り当てていないと、プライベートポートの追加はできません。Private VLAN の設定をするときは、必ず最初にアップリンクポートを割り当ててください。

4. 次にポート 17～24 を同一グループ所属のプライベートポートとして追加します。この場合は、ADD VLAN PORT コマンド (132 ページ) を GROUP オプション付きで実行します。

```
ADD VLAN=pv PORT=17-24 GROUP ↵
```

- ☞ 8748SL では、ポートグループ「1～24、50」と「25～48、49」をまたぐプライベートポートグループは作成できません。

設定は以上です。

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。

スパニングツリープロトコルにはいくつかの種類がありますが、本製品では以下のバージョンをサポートしています。

名称	略称	対応規格
スパニングツリープロトコル (STANDARD モード)	STP	IEEE 802.1D
スパニングツリープロトコル (RAPID モード)	RSTP (Rapid STP)	IEEE 802.1w
マルチプルスパニングツリープロトコル	MSTP (Multiple STP)	IEEE 802.1s

表 5: スパニングツリープロトコルの種類

この章では、このうちの STP と RSTP の使用方法について説明します。MSTP については、「スイッチング」の「マルチプルスパニングツリープロトコル (MSTP)」をご覧ください。

🔗 STP/RSTP と MSTP を同時に有効化することはできません。

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、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を有効にするには、ENABLE STP コマンド（199 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（166 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 (335 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 (343 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 (339 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。

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。

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 (135 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 (117 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 (143 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 (143 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 (150 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 (143 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 (254 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遷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遷移するまでの時間 (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。
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 6:

STP ドメインのスパン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 (254 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ン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 (256 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)。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 7:

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 8: 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 9: 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 (256 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 (168 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 (201 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 (224 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 (218 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。
- ✎ STP/RSTP と 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。

概要

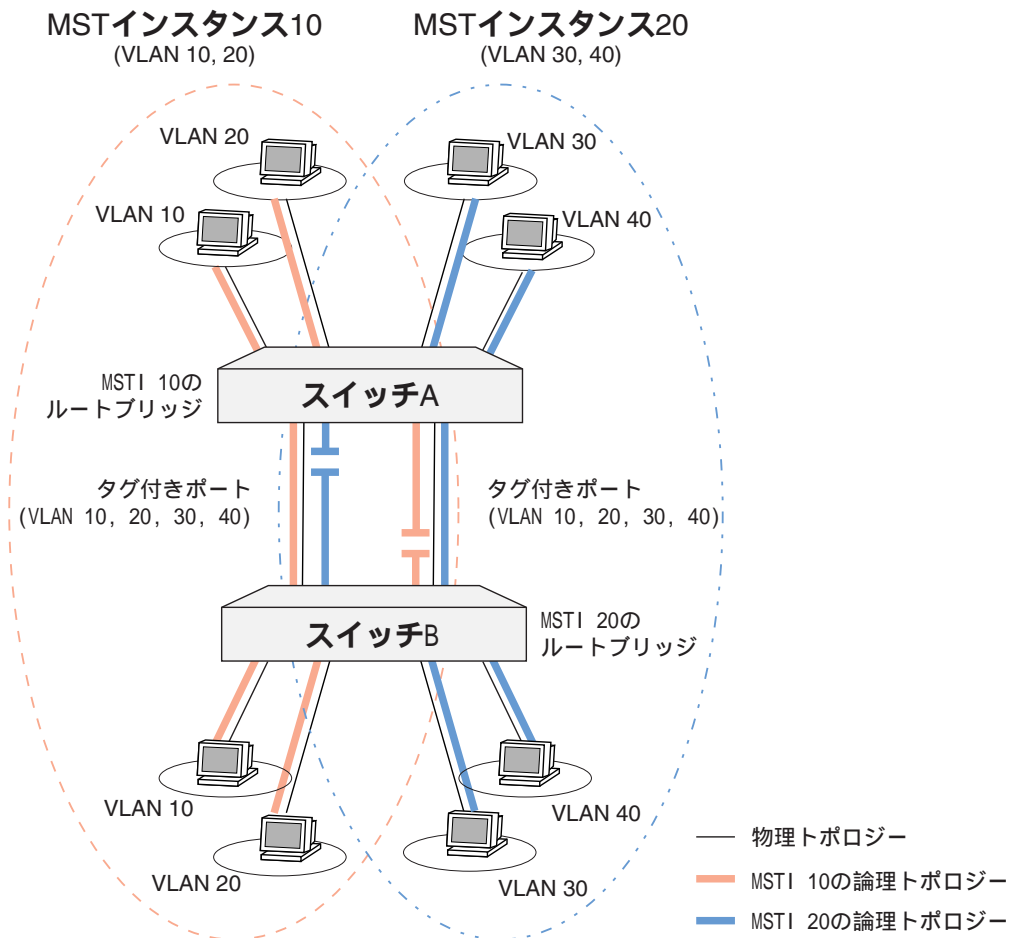
MSTP は、ツリー状の論理経路 (スパニングツリー) を自動的に形成してループを防止する点において、RSTP と同様の動作をします。

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。

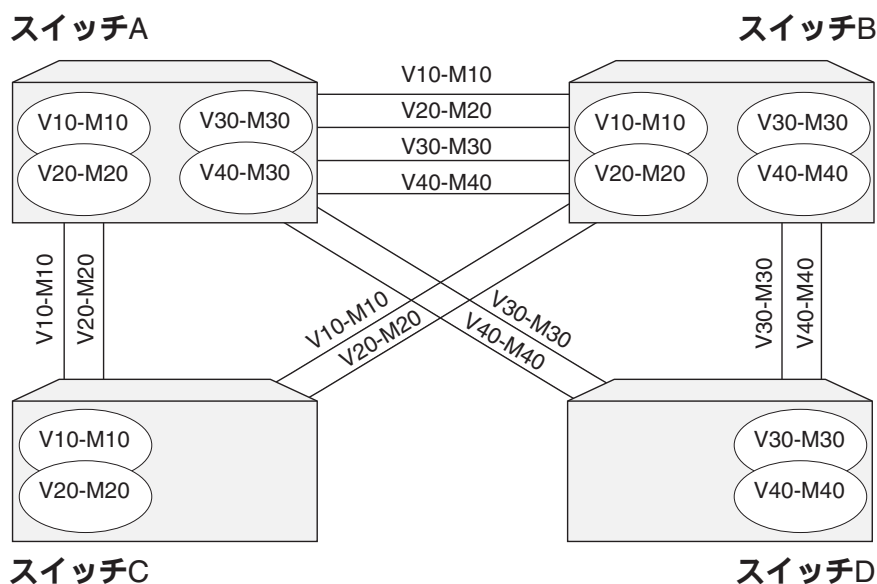
- MST リージョン名
- MST リージョンのリビジョン
- MST インスタンスと VLAN の関連付け (後述)

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 (295 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 (295 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 10: 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 11: MST インスタンスと VLAN の関連付けが同一の例

CIST

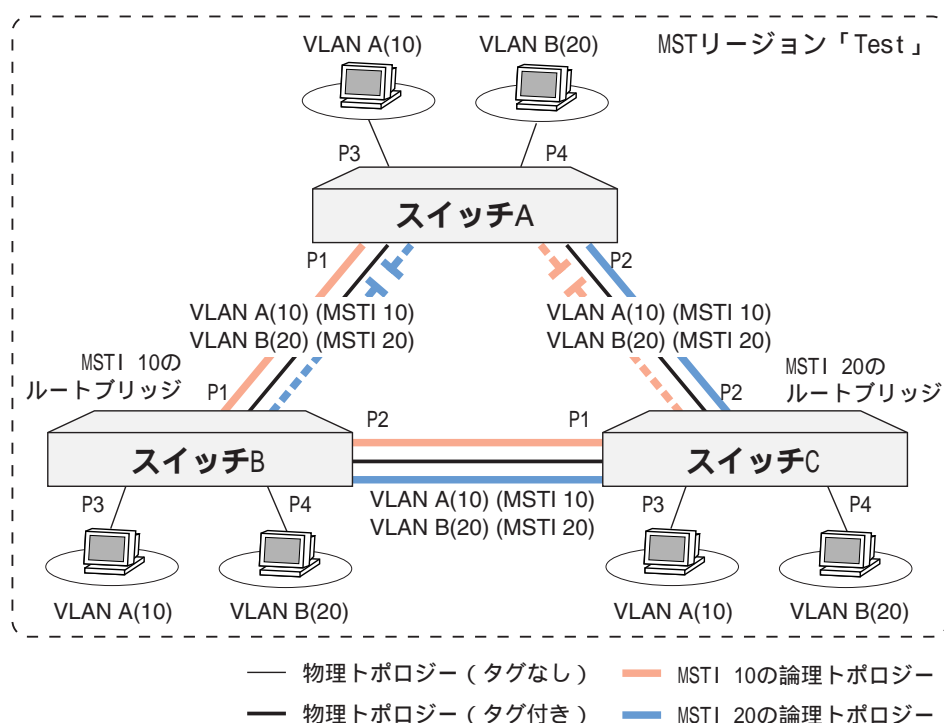
MSTP では、デフォルトで ID=0 の特殊なインスタンスが存在します。これは CIST (Common and Internal Spanning Tree) と呼ばれ、MST リージョン内のすべてのブリッジを接続し、さらには、MST リージョン同士を接続して、ネットワーク全体をカバーするスパンニングツリーを形成します。

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、マルチプルスパン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 (159 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 (142 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 (149 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 (142 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。

マルチプ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 (295 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 (307 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 (310 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 (295 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 (301 ページ) を使います。

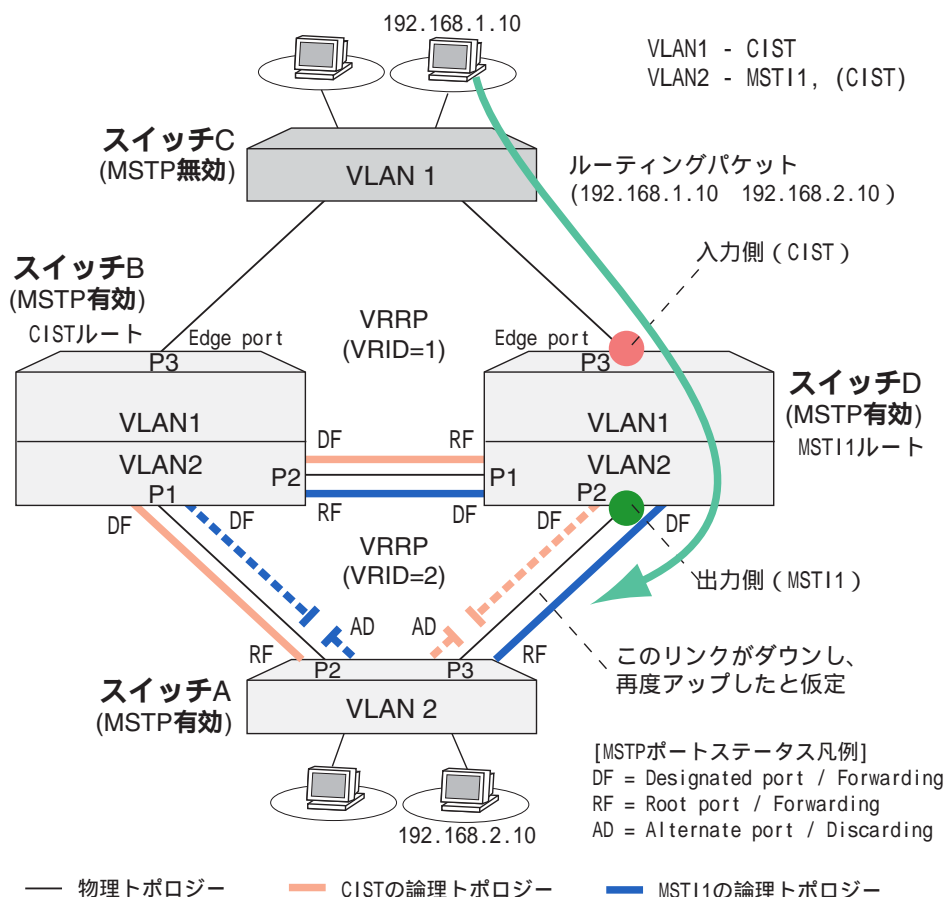
SHOW MSTP CIST PORT=4 ↵

ルーティング機能を併用するときの注意事項

MSTP とルーティング機能を併用する場合は、以下の制限事項があります。

- 以下の 3 条件をすべて満たす構成においてトポロジーチェンジが発生すると、本製品は「フォワードディレイタイム × 2」の間、ルーティング packets を入力ポートで破棄します。
 - ルーティング packets の入力ポート（ルーティング前 VLAN）と出力ポート（ルーティング後 VLAN）で所属先の MST インスタンスが異なる（以下では、それぞれ入力側 MST インスタンス、出力側 MST インスタンスと呼びます）
 - 入力側 MST インスタンスと出力側 MST インスタンスのトポロジー（ルートブリッジ）が異なる
 - 出力ポートにおける MSTP ポートステータスの遷移が遅い

たとえば、次図の構成において、ホスト 192.168.1.10 からホスト 192.168.2.10 へのレイヤー 3 通信が行われていると仮定します。スイッチ B とスイッチ D には 2 つの VLAN が設定されており、VLAN 間ルーティングと VRRP の設定が行われています。MSTP の設定はスイッチ A、B、D に対して行われており、スイッチ B が CIST のルートブリッジ、スイッチ D が MSTI1 のルートブリッジになっています。



ここで、右下のリンク（スイッチ D のポート 2 とスイッチ A のポート 3 を結ぶリンク）がダウンし、再度アップするとトポロジチェンジが発生します。

このとき、スイッチ D のポート 2 の MSTP ポートステータスは、次のように遷移します。

MSTI1 におけるポートステータス	Discarding	Forwarding	の速い遷移
CIST におけるポートステータス	Discarding	Learning	Forwarding の遅い遷移

表 12: スイッチ D のポート 2 の MSTP ポートステータス遷移

CIST においてポート 2 の遷移が遅いのは、同ポートがエッジポートではなく、また、対向ポート（スイッチ A のポート 3）が CIST における Alternate ポートのため、Proposal に対する Agreement を送信してこないことが原因です。

スイッチ D のポート 2 が、CIST において Forwarding 状態に達するまでの間（フォワードディレイタイム × 2）、スイッチ D はポート 3 で受信したルーティングパケットを破棄しつづけます。これは本製品の仕様となります。

この制限を回避するには、次のいずれかの方法をとってください。

- すべての VLAN を 1 つの MST インスタンスに関連付ける
（この例では、VLAN1 を MSTI1 に関連付ける）
- すべての MST インスタンスでトポロジ（ルートブリッジ）が同じになるよう設定する
（この例では、たとえば MSTI2 を新規作成して VLAN1 を関連付け、さらに MSTI1 と MSTI2 のルートブリッジが同じになるよう設定する。あるいは、関連付けはそのまま、CIST と MSTI1 のルートブリッジが同じになるよう設定する）

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（232 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 リージョン設定のリビジョン。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 13:

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 (237 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ーを変更するには、SET MSTP CIST コマンド (234 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 (238 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形成で使用され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 14:

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 15: 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（235 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 内のトポロジ形成で使用され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
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。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 16:

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 17: 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 (235 ページ) の EDGEPORT パラメーターで行います。

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

マルチブル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 MSTP コマンド (216 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してください。

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。本製品は最大 8K 個のアドレスを登録できます。

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 18:

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 19:

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（351 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（225 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（174 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 (207 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 (258 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 (170 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 (203 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 (346 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 (119 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=8 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 (271 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 (354 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 (144 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 (354 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 ↵
```

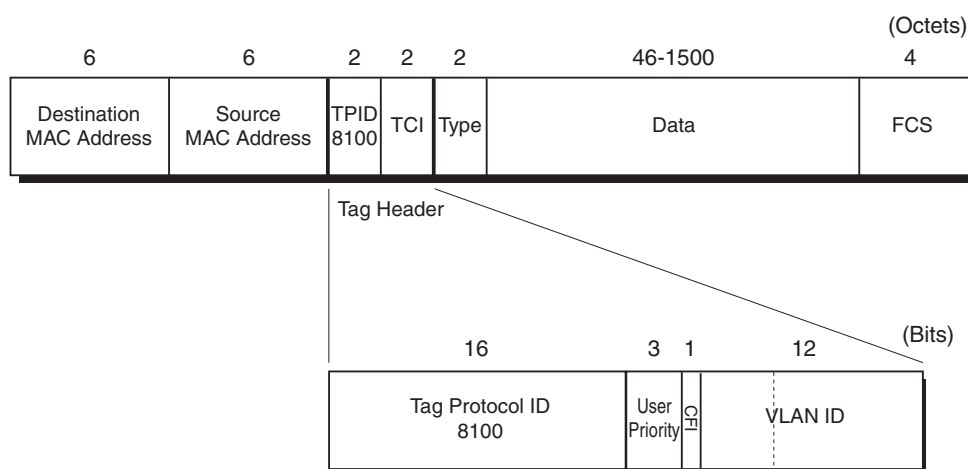
- ✎ エントリーを削除すると、後続のエントリー番号が 1 つずつ前にずれます。

QoS

パケットごとに送信時の優先度を変化させる QoS (Quality of Service) 機能について解説します。本製品は IEEE 802.1p 準拠のプライオリティタグに基づく QoS と、IP ヘッダー等の情報に基づく IP ベースの QoS に対応しています。

プライオリティタグと送信キュー

802.1Q 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、受信フレーム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4レベル(0~3)の送信キューを備えています(キュー3が優先度最高)。フレーム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3とキュー2にフレームが格納されている場合、キュー3が空になるまでキュー2内のフレームは送信されません。割り当てられる帯域は次のようになります(数値は一番左が相対的にもっともレベルの低いキュー、一番右が相対的にもっともレベルの高いキューに割り当てられる帯域(%))を示しています。

- 同時に2つのレベルのキューにパケットがある場合 0 : 100
- 同時に3つのレベルのキューにパケットがある場合 0 : 0 : 100
- 同時に4つのレベルのキューにパケットがある場合 0 : 0 : 0 : 100

受信フレームがどのキューに入れられるかは、ユーザープライオリティ値とキューのマッピング設定によって決まります。デフォルトのマッピングは次のとおりです。VLAN タグ付きのフレームは、このマッピングにしたがって処理されます。

ユーザープライオリティ	キュー番号
0	1
1	0

2	0
3	1
4	2
5	2
6	3
7	3

表 20:

VLAN タグのないフレーム（タグなしフレーム）は、次のように扱われます。

- 宛先 MAC アドレスが本製品の場合 ユーザープライオリティー 4
- 宛先 MAC アドレスが本製品以外の場合 ユーザープライオリティー 0

本製品によってルーティングされる IP、IPv6 パケットは、宛先 MAC アドレスが本製品になるため、プライオリティー 4 で処理されます。一方、本製品によってルーティングされる IP マルチキャストパケットは、宛先 MAC アドレスが本製品ではなく、マルチキャスト MAC アドレスなので、プライオリティー 0 で処理されます。その他のレイヤー 2 スイッチングされるパケットは、プライオリティー 0 で処理されます。

ユーザープライオリティー値とキューのマッピングを変更するには、SET QOS HWPRIORITY コマンド（250 ページ）を使います。たとえば、下図のようなマッピングにするには、次のコマンドを実行します。

```
SET QOS HWPRIORITY QUEUE=0,0,0,1,1,2,2,3 ↵
```

ユーザープライオリティー	キュー番号
0	0
1	0
2	0
3	1
4	1
5	2
6	2
7	3

表 21:

ユーザープライオリティーとキューのマッピングを確認するには SHOW QOS HWPRIORITY コマンド（333 ページ）を使います。

送信キューの重み付けと最大送信遅延時間

特に設定を行わないと、前述の帯域割り当てでも説明したように、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 Priority-based Scheduling）。

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。

これには、次の 2 つの方式があります。

- 送信キューの重み付けを行い、ラウンドロビンで送信していく方式 (Weighted Round-Robin Scheduling)
- 送信キューごとに最大送信遅延時間を保証する方式 (Weighted Round-Robin With Bounded Delay)

✎ 8748SL で以下の設定 (MAXPACKETS、MAXLATENCY) を行った場合は、ポートグループ「1~24、50」と「25~48、49」をまたぐパケットに対して QoS が機能しません。

設定は、SET QOS HWQUEUE コマンド (252 ページ) で行います。送信キューに重み付けを行う場合は、次のように設定します。

```
SET QOS HWQUEUE=3 MAXPACKETS=10 ↓
```

```
SET QOS HWQUEUE=2 MAXPACKETS=5 ↓
```

```
SET QOS HWQUEUE=1 MAXPACKETS=2 ↓
```

```
SET QOS HWQUEUE=0 MAXPACKETS=1 ↓
```

この比率にしたがって、各キューのパケットは順番に送信されます。

✎ 最大送信パケット数を設定して、送信キューに重み付けを行うには、すべてのキューに最大送信パケット数を設定してください。最大送信パケット数が設定されているキューと設定されていないキューがあると、設定されていないキューのパケットが先に送信されます。

最大送信遅延時間を設定するには、次のように設定します。

```
SET QOS HWQUEUE=3 MAXLATENCY=100 ↓
```

```
SET QOS HWQUEUE=2 MAXLATENCY=500 ↓
```

```
SET QOS HWQUEUE=1 MAXLATENCY=700 ↓
```

```
SET QOS HWQUEUE=0 MAXLATENCY=1200 ↓
```

低いレベルのキューに最大送信遅延時間を設定することで、高いレベルのキューのパケット送信中でも、低いレベルのキューの送信が開始されます。また、低い送信レベルのキューに最大送信遅延時間を設定した場合は、高いレベルのキューの最大送信遅延時間を短く設定すれば、待ち時間は短くなります。

送信キューの重み付け、最大送信遅延時間設定は、SHOW QOS HWQUEUE コマンド (334 ページ) で確認できます。

各設定の優先順位は、優先度の高いものから、最大送信遅延時間、送信キューのレベル、最大送信パケット数の順になります。

ハードウェア IP フィルターによる IP ベースの QoS

ハードウェア IP フィルターを利用すると、IP アドレスや 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、受信パケットを送信するときのキューレベルを設定することができます。

ハードウェア IP フィルターによる QoS では、マッチしたパケットに内部的なプライオリティーを付与し、

SET QOS HWPRIORITY コマンド (250 ページ) のマッピングに基づき送信キューレベルを決定します。この場合のプライオリティは仮想的なものであり、受信フレームにプライオリティタグが付いている必要はありません。

ハードウェア IP フィルターを使って特定の packets を任意の送信キューに入れるには、ACTION パラメーターで SENDCOS を指定し、PRIORITY パラメーターで希望するユーザープライオリティを指定します。たとえば、次のようなフィルターを設定すると、始点アドレスが 192.168.10.2 の IP packets に対して、内部的なユーザープライオリティ 7 が付与されます。

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=HOST ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.2 PRIORITY=7
ACTION=SENDCOS ↵
```

パケット送信時には、プライオリティとキューのマッピング設定にしたがい、プライオリティ 7 に対応するキューに該当パケットが入れられます。

次の例では、SSH トラフィックをユーザープライオリティ 5 に相当するキューから送出します。

```
ADD SWITCH L3FILTER MATCH=PROTOCOL,TCPDPORT ↵
ADD SWITCH L3FILTER MATCH=PROTOCOL,TCPSPORT ↵
ADD SWITCH L3FILTER=1 ENTRY PROTOCOL=TCP TCPDPORT=22 PRIORITY=5
ACTION=SENDCOS ↵
ADD SWITCH L3FILTER=2 ENTRY PROTOCOL=TCP TCPSPORT=22 PRIORITY=5
ACTION=SENDCOS ↵
```

ハードウェア IP フィルターの詳細については、「スイッチング」の「ハードウェア IP フィルター」をご覧ください。

ハードウェア IP フィルター

ハードウェア IP フィルターは、ハードウェア (ASIC) レベルで IP トラフィックのフィルタリングを行う機能です。

- ✎ ハードウェア IP フィルターとソフトウェア処理によるフィルター (ソフトウェア IP フィルターとファイアウォール) を同時に使用することはできません。
- ✎ PPP (PPPoE) とハードウェア IP フィルターは併用できません。PPPoE を使用するときは、ハードウェア IP フィルターを使わないでください。

ハードウェア IP フィルターには以下の特長があります。

- ハードウェアで処理するため、ソフトウェア IP フィルターよりも高速
- ポート単位でのフィルタリングが可能 (ソフトウェア IP フィルターは VLAN 単位)
- ルーティングされない IP トラフィック (同一 VLAN 内の IP トラフィック) に対してもフィルタリングが可能 (IP モジュールを有効にしていない状態、すなわちレイヤー 2 スイッチとして使用している場合でも IP のフィルタリングが可能)

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。

- 入出力スイッチポート
- Ethernet ヘッダーのプロトコルタイプ (Ethernet Version 2、802.2 LLC、SNAP の各フレームフォーマットに対応)
- IP ヘッダーの TOS 優先度 (precedence) または DSCP (DiffServ Code Point)、TTL、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、制御フラグ (Syn、Ack、Fin)
- 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) を適用できます (複数の処理を適用することも可能)。一致しなかったパケットは通常通り処理されます。

- 破棄・許可
- 出力スイッチポートの変更
- 出力キューレベルの変更
- VLAN タグフレームの 802.1p ユーザープライオリティーフィールドを書き換え
- IP パケットの TOS 優先度フィールド、または、DSCP フィールドを書き換え
- ミラーポートにパケットをコピー

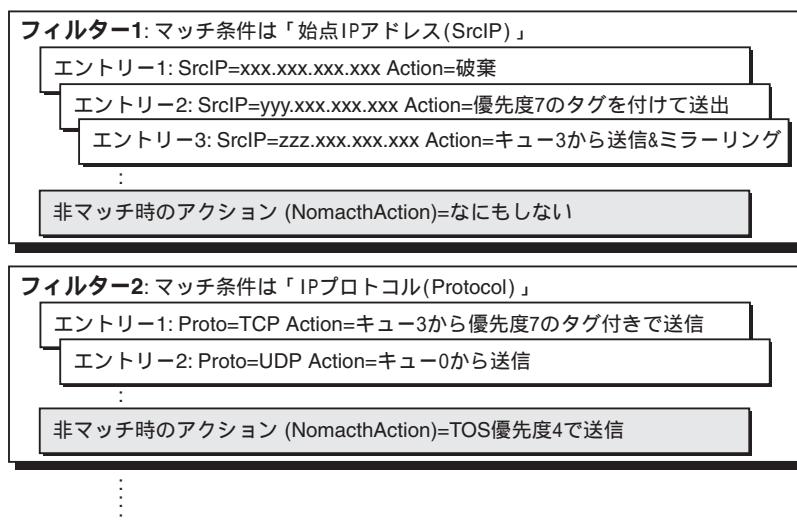
基本動作

ハードウェア IP 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 IP フィルターは、マッチ条件 (フィルター) とフィルターエントリーで構成されます。

- マッチ条件 (フィルター) は、パケットヘッダーのどのフィールドを使ってパケットをふるいわけけるかを指定するもので、ADD SWITCH L3FILTER MATCH コマンド (127 ページ) で作成します。オプションで、どのエントリーにもマッチしなかった場合の処理も指定できます (NOMATCHACTION)。
- フィルターエントリーは、マッチ条件に対して具体的な値を指定し、マッチしたパケットに対して行う処理 (アクション) を指定するもので、ADD SWITCH L3FILTER ENTRY コマンド (121 ページ) で追加します。



作成可能なフィルター数は次のとおりです。

- マッチ条件 (フィルター) はシステム全体で 14 個まで
- フィルターエントリーはシステム全体で 124 個まで

フィルター処理の流れ

ハードウェア IP 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。

- ④ 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. パケットを受信すると、FDB (L2) または L3 テーブル (L3) を参照して出力先 (出力ポート) を決定します。
 2. すべてのフィルター (マッチ条件) すべてのフィルターエントリーをチェックし、受信パケットの入出力スイッチポート、IP、TCP、UDP ヘッダーフィールドと一致するものがあるかどうかを調べていきます。一致するエントリーが 1 つ以上あった場合は、一致したエントリーのアクションをすべて「アクションリスト」にリストアップしておきます。
- ④ NOMATCHACTION が指定されているフィルターの場合、該当フィルターのどのエントリーにもマッチしなかったパケットには、NOMATCHACTION パラメーターで指定されたアクションが適用されます。NOMATCHACTION パラメーターが指定されていない場合は、アクションなしとなります。

3. この時点で「アクションリスト」が空の場合は、フィルター処理を完了し、通常どおりパケットを処理します（パケットを出力）。

☞ タグなしパケットは、宛先 MAC アドレスが本製品ならユーザープライオリティー 4、本製品以外ならユーザープライオリティー 0 として扱われます。そのため、本製品によってルーティングされる IP、IPv6 パケットは、プライオリティー 4 で処理されます。一方、本製品によってルーティングされる IP マルチキャストパケットは、宛先 MAC アドレスが本製品ではないため、プライオリティー 0 で処理されます。その他のレイヤー 2 スイッチングされるパケットは、プライオリティー 0 で処理されます。

4. アクションリストが完成したら、以下の順序でパケットを処理します。フィルター番号順に処理されるのではない点に注意してください。また、以下の各手順では「フィルター処理を終了」と明記していない限り、自動的に次の手順に進みます（パケットに対し、複数のアクションが適用される場合があります）。

- (a) アクションリスト内に「TOS 書き換え系のアクション」(SETTOS、SETIPDSCP、MOVEPRIOTOTOS)があるか調べます。同系のアクションが複数あるときは、フィルター番号のもっとも大きなアクションだけを選択して実行します。したがって、以下の 3 つのうち、どれか 1 つだけが実行されることになります。

- SETTOS アクションの場合は、IP ヘッダーの TOS 優先度 (precedence) フィールドに NEWTOS パラメーターで指定された値を書き込みます。
- SETIPDSCP アクションの場合は、IP ヘッダーの DSCP フィールドに NEWIPDSCP パラメーターで指定された値を書き込みます。
- MOVEPRIOTOTOS アクションの場合は、受信時の 802.1p ユーザープライオリティーフィールドの値を、IP ヘッダーの TOS 優先度 (precedence) フィールドにコピーします。

☞ ここで書き込んだ TOS 優先度値、DSCP 値が、フィルターエントリーの検索に影響することはありません（アクションリストの検証に入った時点で、すでにエントリーの検索が完了しているため）。フィルターエントリー検索時には、パケット受信時の TOS 優先度値、DSCP 値が使われます。

☞ MOVEPRIOTOTOS アクションで使われる 802.1p フィールド値は、パケット受信時の値です。802.1p フィールドを書き換えるアクション (SETPRIORITY、MOVETOSTOPRIO) によって書き換えられた値ではありません。

- (b) アクションリスト内に「802.1p 書き換え系のアクション」(SETPRIORITY、MOVETOSTOPRIO)があるか調べます。同系のアクションが複数あるときは、フィルター番号のもっとも大きなアクションだけを選択して実行します。したがって、以下の 2 つのうち、どれか 1 つだけが実行されることになります。

- SETPRIORITY アクションの場合は、VLAN タグフレームの 802.1p ユーザープライオリティーフィールドに PRIORITY パラメーターで指定された値を書き込みます。
- MOVETOSTOPRIO アクションの場合は、受信時の IP TOS 優先度 (precedence) フィールドの値を、VLAN タグフレームの 802.1p ユーザープライオリティーフィールドにコピーします。

☞ 実際にプライオリティー値がセットされた状態でパケットが出力されるには、出力ポートがタグ付き (TAGGED) に設定されている必要があります。出力ポートがタグなし (UNTAGGED) の場合は、VLAN タグがない状態でパケットが出力されるため、本アクションは実質的な意味を持ちません。

- (c) アクションリスト内に「SENDMIRROR アクション」があるか調べます。SENDMIRROR アクションがある場合は、ミラーポートとして設定されているポートからパケットのコピーを出力します。仕様により、すべてのパケットが VLAN タグ付きでミラーポートから出力されます。

✎ ルーティング対象パケットには、ルーティング先の VLAN タグが付きます。

✎ SENDMIRROR アクションによってミラーされたパケットには、SETTOS、SETIPDSCP、MOVEPRIORITY、SETPRIORITY、MOVETOSTOPRIO アクションによるフィールド書き換えが反映されています。

- (d) アクションリスト内に「破棄・通過系のアクション」(DENY、NODROP)があるか調べます。同系のアクションが複数あるときは、フィルター番号のもっとも大きなアクションだけを選択して実行します。したがって、以下の2つのうち、どれか1つだけが実行されることになります。

- DENY アクションの場合は、パケットを破棄してフィルター処理を終了します。この場合、通常のポートからパケットが出力されることはありません (SENDEPORT、SENDCOS アクションがある場合でもパケットは出力されません)。ただし、ポートミラーリング機能が有効な場合は、ミラーポートからパケットのコピーが出力されます (SENDMIRROR アクションも有効です)。
- NODROP アクションの場合は次のステップに進みます。

- (e) アクションリスト内に「出力ポート変更系のアクション」(SENDEPORT、SENDNONUNICASTTOPORT)があるか調べます。

- パケットがユニキャスト (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以外) で、アクションがSENDEPORTの場合は、パケットの出力先を、FDB や L3 テーブルを参照して決定された出力ポートではなく、PORT パラメーターで指定されたポートに変更します。
- パケットが非ユニキャスト (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) で、アクションがSENDNONUNICASTTOPORTの場合は、パケットの出力先を、同一 VLAN 内の全ポートではなく、PORT パラメーターで指定されたポートだけに変更します。

✎ SENDEPORT、SENDNONUNICASTTOPORT アクションを使う場合は、PORT パラメーターで指定するポート (出力ポート) と入力ポートが同じ VLAN になるよう設定に注意してください。さらに、8748SL では、PORT パラメーターで指定するポート (出力ポート) と入力ポートが、同一ポートグループ「1～24、50」または「25～48、49」に入るようにしてください。また、仕様により、本来なら L3 スイッチング (ルーティング) されるはずのパケットは、出力ポート (PORT) のタグ設定 (タグ付き・タグなし) にかかわらず、本来のルーティング先の VLAN タグが付いた状態で出力されます。

- (f) アクションリスト内に「出力キューレベル変更系のアクション」(SENDCOS、MOVETOSTOPRIO)があるか調べます。同系のアクションが複数あるときは、フィルター番号のもっとも大きなアクションだけを選択して実行します。したがって、以下の2つのうち、どれか1つだけが実行されることになります。

- SENDCOS アクションの場合は、ここまでの手順で確定した出力先ポートの送信キューにパケットを格納し (出力し)、フィルター処理を完了します。このとき、PRIORITY パラメーターで指定されたユーザープライオリティー値に対応するレベルの送信キューを使います。
- MOVETOSTOPRIO アクションの場合は、ここまでの手順で確定した出力先ポートの送信キューにパケットを格納し (出力し)、フィルター処理を完了します。このとき、受信時の

IP TOS 優先度 (precedence) フィールドの値に対応するレベルの送信キューを使います。

- ④ SENDCOS アクションでは、PRIORITY パラメーターを送信キュー選択のためだけに使います。出力するパケットにプライオリティー値をセットするわけではありません(セットするにはSETPRIORITY か MOVETOSTOPRIO アクションを使います)。

(g) アクションリスト内に「出力キューレベル変更系のアクション」(SENDCOS、MOVETOSTOPRIO)がない場合は、ここまでの手順で確定した出力先ポートの送信キューにパケットを格納します。このとき、パケット受信時の 802.1p ユーザープライオリティー値をもとに、どのレベルのキューに入れるかを決定します。

- ④ タグなしパケットは、宛先 MAC アドレスが本製品ならユーザープライオリティー 4、本製品以外ならユーザープライオリティー 0 として扱われます。そのため、本製品によってルーティングされる IP、IPv6 パケットは、プライオリティー 4 で処理されます。一方、本製品によってルーティングされる IP マルチキャストパケットは、宛先 MAC アドレスが本製品ではないため、プライオリティー 0 で処理されます。その他のレイヤー 2 スイッチングされるパケットは、プライオリティー 0 で処理されます。

設定手順

ハードウェア IP フィルターの設定は、次の流れで行います。

1. フィルター (マッチ条件) の作成 (ADD SWITCH L3FILTER MATCH コマンド (127 ページ))
2. フィルター番号の確認 (SHOW SWITCH L3FILTER コマンド (356 ページ))
3. フィルターエントリーの追加 (ADD SWITCH L3FILTER ENTRY コマンド (121 ページ))

以下、各手順について詳しく解説します。

フィルター (マッチ条件) の作成

最初に、ADD SWITCH L3FILTER MATCH コマンド (127 ページ) でフィルター (マッチ条件) を作成し、IP/TCP/UDP ヘッダーのどのフィールドを比較条件として使用するかを指定します。

MATCH パラメーターには、フィルタリング条件として使用するヘッダーフィールドを以下から指定します。複数指定する場合はカンマで区切って指定してください。TCPxxx、UDPxxx を指定する場合は、PROTOCOL も条件として指定し、さらに ADD SWITCH L3FILTER ENTRY コマンド (121 ページ) (後述) でそれぞれ「PROTOCOL=TCP」、「PROTOCOL=UDP」を指定する必要があります。

Ethernet ヘッダー	
TYPE	プロトコルタイプフィールド。他項目との併用は不可
IP ヘッダー	
TOS	TOS オクテットの優先度値 (precedence) フィールド
IPDSCP	TOS オクテットの DSCP (DiffServ Code Point) フィールド
TTL	生存時間 (TTL) フィールド
PROTOCOL	プロトコルフィールド
SIPADDR	始点 IP アドレス (SCLASS も指定すること)

DIPADDR	終点 IP アドレス (DCLASS も指定すること)
TCP ヘッダー	
TCPSPORT	始点ポート (PROTOCOL も指定すること)
TCPDPORT	終点ポート (PROTOCOL も指定すること)
TCPSYN	Syn フラグ (PROTOCOL も指定すること。EMPORT に TRUE を指定しないこと)
TCPACK	Ack フラグ (PROTOCOL も指定すること。EMPORT に TRUE を指定しないこと)
TCPFIN	Fin フラグ (PROTOCOL も指定すること。EMPORT に TRUE を指定しないこと)
UDP ヘッダー	
UDPSPORT	始点ポート (PROTOCOL も指定すること)
UDPDPORT	終点ポート (PROTOCOL も指定すること)

表 22: MATCH パラメーターに指定できる項目

MATCH パラメーターに TYPE を指定した場合は、TYPE パラメーターで Ethernet のフレームフォーマット (エンキャプセレーション) を指定する必要があります。802 (802.2 LLC)、ETHII (Ethernet Version 2)、SNAP (802.2 LLC + SNAP) から選択してください。ADD SWITCH L3FILTER ENTRY コマンド (121 ページ) の TYPE パラメーターには、ここで指定したフレームフォーマットのプロトコル番号を指定します。

- ☞ MATCH パラメーターに TYPE を指定した場合、他のヘッダーフィールドをフィルタリング条件として使うことはできません。また、SETTOS アクションは使用できません。

MATCH パラメーターに SIPADDR か DIPADDR を指定した場合は、SCLASS、DCLASS パラメーターでそれぞれアドレスマスクも指定します。マスク値は、クラス A、B、C の標準マスク (8, 16, 24 ビット長) が単一ホストを対象とする HOST、あるいは、任意のマスク長 (1 ~ 32 ビット) で指定します。ここで指定したマスクは、IP アドレスを実際に指定する際、指定した IP アドレスに対して適用されます。

特定のポートでのみフィルタリングを行うには、IMPORT (入力ポート)、EMPORT (出力ポート) パラメーターに TRUE を指定します。IMPORT、EMPORT パラメーターに TRUE を指定すると、特定のスイッチポートで送受信されるパケットだけがフィルタリングの対象になります。デフォルト (FALSE) では、すべてのポートがフィルタリングの対象になります。なお、具体的なポート番号は、後述する ADD SWITCH L3FILTER ENTRY コマンド (121 ページ) の IPORT、EPORT パラメーターで指定します。

- ☞ EMPORT パラメーターに TRUE を指定した場合は、FDB、L3 テーブルのどちらにも登録されていない MAC アドレス (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) 宛てのパケットがフィルタリング対象にならないという制限があります。TCP 制御フラグによるフィルタリングを行う場合 (マッチ条件に TCPSYN、TCPACK、TCPFIN を指定する場合) および、ブロードキャスト、マルチキャストパケットのフィルタリングを行う場合は、EMPORT に TRUE を指定しないでください。

NOMATCHACTION パラメーターには、オプションとして、どのエントリーともマッチしなかったパケットに適用するアクションを指定できます。指定できるアクションは ADD SWITCH L3FILTER ENTRY コマンド (121 ページ) の ACTION パラメーターと同じです (ただし、NODROP は除く)。また、アクションパラメーターは NOMATCHDSCP、NOMATCHPORT、NOMATCHPRIORITY、NOMATCHTOS で指

定します（それぞれ、ADD SWITCH L3FILTER ENTRY コマンド（121 ページ）の NEWIPDSCP、PORT、PRIORITY、NEWTOS に相当）。

フィルター番号の確認

次に、SHOW SWITCH L3FILTER コマンド（356 ページ）を実行し、手順 1 で作成したフィルター（マッチ条件）の番号を確認します。

- ✎ フィルター番号は、ADD SWITCH L3FILTER MATCH コマンド（127 ページ）実行時にシステムが自動で割り当てます。この番号は可変なので、他のフィルターの削除によって変更される可能性があります。フィルター番号を指定するときは、必ず SHOW SWITCH L3FILTER コマンド（356 ページ）で確認してから指定してください。

フィルターエントリーの追加

次に、ADD SWITCH L3FILTER ENTRY コマンド（121 ページ）を使って、フィルター（マッチ条件）にエントリーを追加します。

フィルターエントリーを追加するには、次の 3 つの情報を入力する必要があります。以下、それぞれについて詳しく解説します。

- フィルター番号
- フィルタリング条件
- マッチ時のアクション

フィルター番号の指定

ADD SWITCH L3FILTER ENTRY コマンド（121 ページ）の L3FILTER パラメーターには、SHOW SWITCH L3FILTER コマンド（356 ページ）で確認したフィルター番号を指定します。

- ✎ エントリー番号は、ADD SWITCH L3FILTER ENTRY コマンド（121 ページ）実行時にシステムが自動で割り当てます。この番号は可変なので、他のエントリーの追加・削除によって変更される可能性があります。エントリー番号を指定するときは、必ず SHOW SWITCH L3FILTER コマンド（356 ページ）に ENTRY パラメーターを付けて実行し、希望するエントリーの番号を確認してから指定してください。

フィルタリング条件の指定

フィルタリング条件は、以下の各パラメーターで指定します。マッチ条件作成時に MATCH パラメーターで指定したすべてのフィールドに対して具体的な値を指定してください。

入出力スイッチポート	
IPORT	入力スイッチポート。指定ポートから入力されたパケットだけがマッチする
EPORT	出力スイッチポート。指定ポートから出力されるパケットだけがマッチする （ただし、若干の制限あり。詳細は後述）

Ethernet ヘッダー	
TYPE	Ethernet フレームのレイヤー 3 プロトコルタイプフィールド値 (16 進数)。ADD SWITCH L3FILTER MATCH コマンドの TYPE パラメーターで指定したフレームフォーマットにおける値を指定する。Ethernet Version 2 と 802.2 LLC(DSAP、SSAP) におけるプロトコルタイプは 2 バイト、SNAP のプロトコルタイプは 5 バイト長
IP ヘッダー	
TOS	TOS 優先度値 (TOS オクテットの precedence フィールド)。有効範囲は 0~7
IPDSCP	DSCP (DiffServ Code Point) フィールド値。有効範囲は 0~63
TTL	生存時間 (TTL) フィールドの値。有効範囲は 0~255
PROTOCOL	IP の上位プロトコル。TCP、UDP などのプロトコル名、または、IP プロトコル番号で指定する
SIPADDR	始点 IP アドレス。パケットマッチング時には、ここで指定したアドレスに対して、ADD SWITCH L3FILTER MATCH コマンドの SCLASS パラメーターで指定したマスクが適用される
DIPADDR	終点 IP アドレス。パケットマッチング時には、ここで指定したアドレスに対して、ADD SWITCH L3FILTER MATCH コマンドの DCLASS パラメーターで指定したマスクが適用される
TCP ヘッダー	
TCPSPORT	始点ポート番号またはサービス名
TCPDPORT	終点ポート番号またはサービス名
TCP SYN	Syn フラグのオン (TRUE) オフ (FALSE)。EPORT パラメーターと併用しないこと
TCP ACK	Ack フラグのオン (TRUE) オフ (FALSE)。EPORT パラメーターと併用しないこと
TCP FIN	Fin フラグのオン (TRUE) オフ (FALSE)。EPORT パラメーターと併用しないこと
UDP ヘッダー	
UDPSPORT	始点ポート番号またはサービス名
UDP DPORT	終点ポート番号またはサービス名

表 23: 条件パラメーター (受信パケットのヘッダーその他とつきあわせるパラメーター)

特定のポートでのみフィルタリングを行いたい場合 (ADD SWITCH L3FILTER MATCH コマンド (127 ページ) で IMPORT=TRUE または EIMPORT=TRUE を指定した場合) は、IPORT (入力ポート)、EPORT (出力ポート) パラメーターでフィルタリングを行うポートの番号を指定してください。IPORT で指定したポートから入力されたパケット、EPORT で指定したポートから出力されるパケットだけが、フィルタリングの対象となります。

- ④ ADD SWITCH L3FILTER MATCH コマンド (127 ページ) で IMPORT=TRUE か EIMPORT=TRUE を指定していながら、IPORT、EPORT パラメーターでポートの番号を指定していないと、フィルタリングが行われません。なお、ポートは一度に 1 つしか指定できないので、複数のポートでフィルタリングを有効にしたい場合は、ポートの数だけエントリーを作成してください。

- ✎ フィルタリング条件として EPORT（出力スイッチポート）を指定した場合、FDB、L3 テーブルのどちらにも登録されていない MAC アドレス（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）宛てのパケットにはフィルターが適用されなくなります。したがって、TCP 制御フラグによるフィルタリング（TCPSYN、TCPACK、TCPFIN パラメーター）を行う場合、および、ブロードキャスト、マルチキャストパケットのフィルタリングを行う場合は、EPORT パラメーターを併用しないでください。

- ✎ 8748SL では、入力ポートと出力ポートがポートグループ「1～24、50」と「25～48、49」をまたいだ場合、たとえば、入力ポートが 1 で出力ポートが 25 の場合や、入力ポートが 49 で出力ポートが 50 の場合に制限があります。詳しくは次節「8748SL における制限事項」をご覧ください。本制限は 8748SL 固有のもので、8724SL にはありません。

TCP の制御フラグはコネクション方向の判別に使用できますが、前述の制限があるため、EPORT パラメーターとは併用しないでください。

アクションの指定

パケットが条件に一致したときのアクションは、ACTION パラメーターで指定します。ACTION はカンマ区切りで複数指定が可能です。

次の表に示すとおり、アクションはいくつかの「カテゴリー」に分類できます。表で（相互排他）と記されているカテゴリーは、パケットが同一カテゴリー内の複数のアクションにマッチした場合に、最後にマッチしたエントリー、すなわち、フィルター番号・エントリー番号のもっとも大きなエントリーのアクションだけが実行されることを示しています。

パケットの破棄・通過を制御するアクション（相互排他）	
DENY	パケットを破棄する。マッチしたエントリーの中に DENY アクションが含まれている場合は、NODROP によって打ち消されない限り、通常のポートからパケットが出力されることはない（SENDEPORT、SENDCOS アクションがある場合でもパケットは出力されない）。ただし、ポートミラーリング機能が有効な場合は、ミラーポートからパケットのコピーが出力される（SENDMIRROR アクションも有効）
NODROP	DENY アクションを打ち消し、本来破棄されるべきパケットを出力する。おもに、デフォルト拒否の設定において、一部のパケットだけを許可したい場合に使う
出力ポートを変更するアクション	
SENDEPORT	ユニキャストパケット（ここでは、ブロードキャスト、マルチキャスト、および、未学習のユニキャストを除くパケットのこと）の出力先を 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）と入力ポートが同じ VLAN でなくてはならないので、設定には注意すること。さらに、8748SL では、入力ポートと出力ポート（PORT）が、同一ポートグループ「1～24、50」または「25～48、49」に入っていないと注意。また、仕様により、本来なら L3 スイッチング（ルーティング）されるはずのパケットは、出力ポート（PORT）のタグ設定（タグ付き・タグなし）にかかわらず、本来のルーティング先の VLAN タグが付いた状態で出力される

SENDNONUNICAST	ユニキャストパケット（ここでは、ブロードキャスト、マルチキャスト、および、未学習のユニキャストのこと）の出力先を PORT パラメーターで指定されたポートだけに変更する。このとき、出力ポート（PORT）と入力ポートが同じ VLAN でなくてはならないので、設定には注意すること。さらに、8748SL では、入力ポートと出力ポート（PORT）が、同一ポートグループ「1～24、50」または「25～48、49」に入っていないと注意
出力キューを変更するアクション（相互排他）	
SEDCOS	パケットを PRIORITY パラメーターで指定されたプライオリティーに対応するレベルの送信キューに入れる
MOVETOSTOPRIO	受信時の IP ヘッダーの TOS 優先度（precedence）フィールドの値を、VLAN タグフレームの 802.1p ユーザープライオリティーフィールドにコピーする。また、コピー後のユーザープライオリティーに対応するレベルの送信キューにパケットを入れる
802.1p プライオリティーを書き換えるアクション（相互排他）	
MOVETOSTOPRIO	受信時の IP ヘッダーの TOS 優先度（precedence）フィールドの値を、VLAN タグフレームの 802.1p ユーザープライオリティーフィールドにコピーする。また、コピー後のユーザープライオリティーに対応するレベルの送信キューにパケットを入れる
SETPRIORITY	VLAN タグフレームの 802.1p ユーザープライオリティーフィールドに、PRIORITY パラメーターで指定された値を書き込む。出力ポートがタグ付きの場合のみ有効。出力ポートがタグなしの場合はパケットにタグが付かないので、本アクションは意味を持たない
IP TOS/DSCP フィールドを書き換えるアクション（相互排他）	
SETTOS	パケットの IP TOS 優先度（precedence）フィールドに、NEWTOS パラメーターで指定された値を書き込む。TYPE パラメーターで IP 以外のプロトコルを指定した場合は無効
MOVEPRIOTOTOS	受信時の VLAN タグフレームの 802.1p ユーザープライオリティーフィールドの値を、IP ヘッダーの TOS 優先度（precedence）フィールドにコピーする
SETIPDSCP	IP ヘッダーの DSCP (DiffServ Code Point) フィールドに、NEWIPDSCP パラメーターで指定された値を書き込む。TYPE パラメーターで IP 以外のプロトコルを指定した場合は無効
その他のアクション	
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、ミラーポートを指定し、ポートミラーリング機能を有効にしておく必要がある。パケットが複数のエントリーにマッチした場合、DENY、NODROP、SEND～を除く他のアクションがすべて適用された状態でパケットがミラーされる。また、DENY 対象のパケットであってもミラーされる。仕様により、すべてのパケットが VLAN タグ付きでミラーポートから出力される。また、ルーティング対象パケットには、ルーティング先の VLAN タグが付く

表 24: ACTION パラメーターに指定できるオプション

- ④ 8748SL では、入力ポートと出力ポートがポートグループ「1～24、50」と「25～48、49」をまたいだ場合、たとえば、入力ポートが 1 で出力ポートが 25 の場合や、入力ポートが 49 で出力ポートが 50 の場合に制限があります。詳しくは次節「8748SL における制限事項」をご覧ください。本制限は 8748SL 固有のもので、8724SL にはありません。

8748SL における制限事項

8748SL には、ハードウェア IP フィルターに関して、以下に述べる仕様上の制限事項があります。これらの制限は 8748SL 固有のもので、8724SL にはありません。

- ポートグループ「1～24、50」と「25～48、49」をまたいで、IPORT と EPORT を同時に設定することはできません。
- 「ACTION=SENDCOS」のエントリーを持つ、あるいは、「NOMACTHACTION=SENDCOS」の指定があるフィルター（マッチ条件）は、合計で 4 つまでしか作れません。
- パケットの入力ポートと出力ポートがポートグループ「1～24、50」と「25～48、49」をまたいだ場合（例：入力ポート「1」、出力ポート「25」の場合など）に、以下の制限があります（SENDEPORT、SENDNONUNICASTTOPORT アクションにおける「出力ポート」は、PORT パラメーターで指定したポートを意味します）。
 - － 以下のアクションが機能しません。
 - * SENDEPORT
 - * SENDNONUNICASTTOPORT
 - － 以下のアクションでは IPORT を指定できません（指定した場合はマッチしません）
 - * SENDCOS
 - － 以下のアクションでは EPORT を指定できません（指定した場合はマッチしません）
 - * NODROP
 - * SETTOS
 - * MOVETOSTOPRIO
 - * MOVEPRIOTOTOS
 - * SETIPDSCP
 - － 以下のアクションは制限なしです。
 - * DENY
 - * SETPRIORITY
 - * SENDMIRROR

- ④ これらの制限を回避するため、8748SL では原則として、入力ポートと出力ポートが「1～24、50」または「25～48、49」のどちらかのポートグループに両方とも入るよう設定することをおすすめします。

コマンド例

次に具体的なコマンド例を示します。

なお、以下の例ではいずれも、フィルター（マッチ条件）を 1 つしか作成していないものと仮定しています。複数のフィルターを作成する場合は、ADD SWITCH L3FILTER ENTRY コマンド（121 ページ）の L3FILTER パラメーターで適切なフィルター番号を指定してください。フィルター番号は SHOW SWITCH L3FILTER コマンド（356 ページ）で確認できます。

ポート 1～3 で受信した 192.168.10.0/24 からの IP パケットを破棄

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=C IMPORT=TRUE ↓
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 IPORT=1 ACTION=DENY ↓
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 IPORT=2 ACTION=DENY ↓
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 IPORT=3 ACTION=DENY ↓
```

192.168.10.100（単一ホスト）からの IP パケットを破棄

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=HOST ↓
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.100 ACTION=DENY ↓
```

ポート 2 から送信される ICMP パケットを破棄

```
ADD SWITCH L3FILTER MATCH=PROTOCOL EXPORT=TRUE ↓
ADD SWITCH L3FILTER=1 ENTRY PROTOCOL=ICMP EPORT=2 ACTION=DENY ↓
```

192.168.10.0/24 からのパケットは原則拒否だが、192.168.10.103 からのパケットだけは許可。NODROP アクションの使用例です。

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=C ↓
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 ACTION=DENY ↓
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=HOST ↓
ADD SWITCH L3FILTER=2 ENTRY SIPADDR=192.168.10.103 ACTION=NODROP ↓
```

telnet パケットをユーザプライオリティ 7 に対応した送信キューに入れる

```
ADD SWITCH L3FILTER MATCH=PROTOCOL,TCPDPORT ↓
ADD SWITCH L3FILTER=1 ENTRY PROTOCOL=TCP TCPDPORT=TELNET PRIORITY=7
ACTION=SEND COS ↓
```

192.168.30.100 への telnet パケットを破棄

```
ADD SWITCH L3FILTER MATCH=DIPADDR, PROTOCOL, TCPDPORT DCLASS=HOST ↵
ADD SWITCH L3FILTER=1 ENTRY DIPADDR=192.168.30.100 PROTOCOL=TCP
TCPDPORT=TELNET ACTION=DENY ↵
```

192.168.10.5 からのパケットの 802.1p ユーザープライオリティーフィールドに 4 をセットして送信

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=HOST ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.5 PRIORITY=4
ACTION=SETPRIORITY ↵
```

受信パケットの IP TOS 優先度が 1 の場合、ユーザープライオリティーを 4 にして送信

```
ADD SWITCH L3FILTER MATCH=TOS ↵
ADD SWITCH L3FILTER=1 ENTRY TOS=1 PRIORITY=4 ACTION=SETPRIORITY ↵
```

192.168.10.100 宛てのパケットをミラーポート 1 から出力。ミラーリングされたパケットには VLAN タグが付いています。

```
SET SWITCH MIRROR=1 ↵
ENABLE SWITCH MIRROR ↵
ADD SWITCH L3FILTER MATCH=DIPADDR DCLASS=HOST ↵
ADD SWITCH L3FILTER=1 ENTRY DIPADDR=192.168.10.100 ACTION=SENDMIRROR ↵
```

192.168.10.100 からの TCP コネクション確立要求を拒否(片方向のみ拒否。他のホストから 192.168.10.100 へはコネクションを張れる)

```
ADD SWITCH L3FILTER MATCH=SIPADDR, PROTOCOL, TCPSYN, TCPACK SCLASS=HOST ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.100 PROTOCOL=TCP
TCPSYN=TRUE TCPACK=FALSE ACTION=DENY ↵
```

192.168.10.0/24 から 192.168.20.0/24 への TCP コネクション確立要求を拒否(片方向のみ拒否。192.168.20.0/24 から 192.168.10.0/24 へはコネクションを張れる)

```
ADD SWITCH L3FILTER MATCH=SIPADDR, DIPADDR, PROTOCOL, TCPSYN, TCPACK SCLASS=C
DCLASS=C ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 DIPADDR=192.168.20.0
PROTOCOL=TCP TCPSYN=TRUE TCPACK=FALSE ACTION=DENY ↵
```

ハードウェア IP フィルターは、ルーティングされない同一 IP ネットワーク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 から他ネットワークへの TCP コネクション確立要求を拒否」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 TCP の通信ができなくなってしまいます。

```
ADD SWITCH L3FILTER MATCH=SIPADDR, PROTOCOL, TCPSYN, TCPACK SCLASS=C ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 PROTOCOL=TCP TCPSYN=TRUE
TCPACK=FALSE ACTION=DENY ↵
```

通常、ネットワーククラス単位でフィルターを設定するとき (SCLASS、DCLASS に A, B, C または 1~32 のマスク長を指定したとき) は、前の例のように送信元 (SIPADDR) と宛先 (DIPADDR) の両方を指定してください。

ある条件を満たしたパケットに対して複数の処理を行いたい場合は、1 つのエントリーで複数のアクションを指定してください。同一フィルター (マッチ条件) 内で、同じフィルタリング条件を持つエントリーを複数作ることはできません。

たとえば、192.168.1.1 からのパケットに対して、TOS precedence の書き換えと送信キューの指定を行いたい場合、次のように設定することはできません。3 行目と 4 行目のエントリーのフィルタリング条件が同じため、4 行目を入力するときにエラーになります。

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=HOST ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.1.1 ACTION=SETTOS NEWTOS=1 ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.1.1 ACTION=SEND COS
PRIORITY=7 ↵
```

このような場合は、次のようにしてください。

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=HOST ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.1.1 ACTION=SETTOS, SEND COS
NEWTOS=1 PRIORITY=7 ↵
```

ハードウェア IP 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 IP 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。

どのようなハードウェア IP フィルター (マッチ条件) が作成されているかを確認するには、SHOW SWITCH L3FILTER コマンド (356 ページ) を使います。

```
Manager > show switch l3filter

Hardware based filtering.... Enabled
Software filtering bypass .. Disabled

Filter ..... 1
Matched fields ..... sip
Type ..... ETH-II
Source address mask .... 255.255.255.0
```

```

Dest. address mask ..... 0.0.0.0
Ingress port mask ..... false
Egress port mask ..... false

Filter ..... 2
Matched fields ..... sip
Type ..... ETH-II
Source address mask .... 255.255.255.255
Dest. address mask ..... 0.0.0.0
Ingress port mask ..... false
Egress port mask ..... false

```

ハードウェア IP フィルターのフィルターエントリーを確認するには、SHOW SWITCH L3FILTER コマンド (356 ページ) に ENTRY オプションを付けます。このときは、フィルター番号を必ず指定しなくてはなりません。

```

Manager > show switch l3filter=2 entry

Hardware based filtering.... Enabled
Software filtering bypass .. Disabled

Filter ..... 2
Matched fields ..... sip
Type ..... ETH-II
Source address mask .... 255.255.255.255
Dest. address mask ..... 0.0.0.0
Ingress port mask ..... false
Egress port mask ..... false
Filter Entries:
-----
Entry ..... 1
Ingress Port ..... None
Egress Port ..... None
Source Address ..... 192.168.10.130
Source Mask ..... 255.255.255.255
Dest Address ..... 0.0.0.0
Dest Mask ..... 0.0.0.0
Protocol ..... 0
TTL ..... 0
TOS ..... 0
IPDSCP ..... 0
Type ..... 0800 (ETH-II)
Action ..... NODROP
-----
Entry ..... 2
Ingress Port ..... None
Egress Port ..... None
Source Address ..... 192.168.10.103
Source Mask ..... 255.255.255.255
Dest Address ..... 0.0.0.0
Dest Mask ..... 0.0.0.0

```

```

Protocol ..... 0
TTL ..... 0
TOS ..... 0
IPDSCP ..... 0
Type ..... 0800 (ETH-II)
Action ..... NODROP
-----

```

```

Entry ..... 3
Ingress Port ..... None
Egress Port ..... None
Source Address ..... 192.168.10.16
Source Mask ..... 255.255.255.255
Dest Address ..... 0.0.0.0
Dest Mask ..... 0.0.0.0
Protocol ..... 0
TTL ..... 0
TOS ..... 0
IPDSCP ..... 0
Type ..... 0800 (ETH-II)
Action ..... NODROP
-----

```

ハードウェア IP フィルターからエントリーを削除するには、DELETE SWITCH L3FILTER コマンド (145 ページ) の ENTRY パラメーターでエントリー番号を指定します。

```
DELETE SWITCH L3FILTER=1 ENTRY=1 ↵
```

- 🔗 エントリー番号は可変です。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してください。コマンド中でエントリー番号を指定するときは、必ず SHOW SWITCH L3FILTER コマンド (356 ページ) に ENTRY パラメーターを付けて実行し、希望のエントリーの番号を確認してから指定してください。

フィルター (マッチ条件) を削除するには、エントリーをすべて削除したあとで次のように実行します。

```
DELETE SWITCH L3FILTER=1 ↵
```

- 🔗 フィルター番号は可変です。フィルター (マッチ条件) を削除すると、後続のフィルター番号が 1 つずつ前にずれるので注意してください。コマンド中でフィルター番号を指定するときは、必ず SHOW SWITCH L3FILTER コマンド (356 ページ) で希望するフィルターの番号を確認してから指定してください。

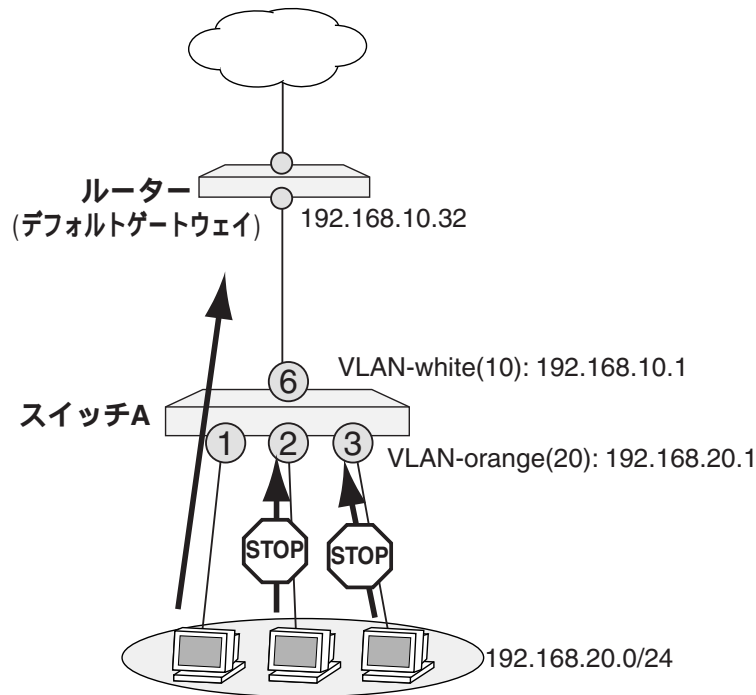
ハードウェア IP フィルターはデフォルトで有効になっています (デフォルト有効の IGMP Snooping がハードウェア IP フィルターを内部的に使用しているため)。無効に設定していた場合は、ENABLE SWITCH L3FILTER コマンド (206 ページ) で有効にしてください。

```
ENABLE SWITCH L3FILTER ↵
```

設定例

特定スイッチポートからのみ外部への UDP 通信を許可

ハードウェア IP フィルターを利用して、VLAN 内の特定ポートからのみ外部への UDP 通信を許可する設定例を示します。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。



ここでは、次のようなフィルタリング条件を考えます。

- VLAN orange から外部への UDP トラフィックは原則として拒否する。
- ただし、ポート 1 から外部へは UDP 通信を許可する。

ポート単位でのフィルタリングには、DHCP クライアントの IP アドレスが変更された場合でも対応できるメリットがあります。

スイッチ A の設定

1. VLAN の設定を行います。

```
CREATE VLAN=white VID=10 ↵
CREATE VLAN=orange VID=20 ↵
ADD VLAN=white PORT=6 ↵
ADD VLAN=orange PORT=1-3 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-white IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-orange IP=192.168.20.1 MASK=255.255.255.0 ↵
```

4. デフォルトルートを設定します。

```
ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0 INT=vlan-white
NEXTTHOP=192.168.10.32 ↵
```

5. ハードウェア IP フィルターの設定を行います。

- フィルターを作成しマッチ条件を指定します。ここでは UDP トラフィックだけを対象とするため、IP プロトコルフィールド (PROTOCOL) を条件として指定します。また、入力ポート単位でフィルタリングを行うため「IMPORT=TRUE」も指定します。

```
ADD SWITCH L3FILTER MATCH=PROTOCOL IMPORT=TRUE ↵
```

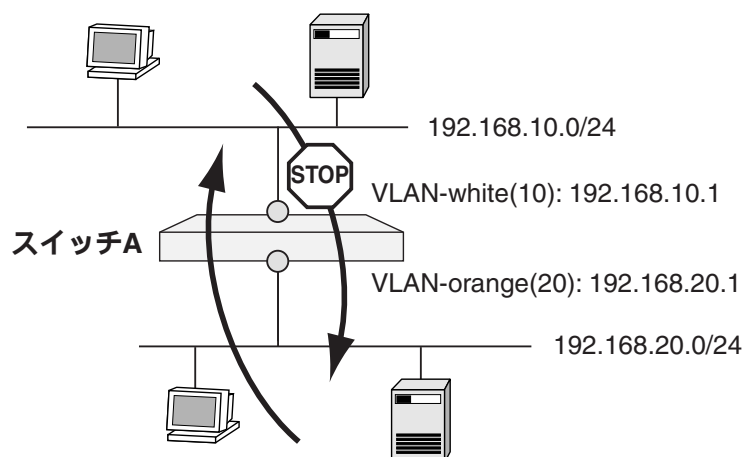
- 具体的な条件値とアクションを指定します。ここではプロトコルが UDP で、受信ポートが 2 か 3 のトラフィックを破棄するよう指定します。

```
ADD SWITCH L3FILTER=1 ENTRY PROTOCOL=UDP IPORT=2 ACTION=DENY ↵
ADD SWITCH L3FILTER=1 ENTRY PROTOCOL=UDP IPORT=3 ACTION=DENY ↵
```

設定は以上です。

TCP 片方向通信

マッチ条件として TCP の制御フラグ Syn と Ack を使用し、片方の VLAN からのみ TCP の通信を開始できるように設定します。



ここでは、次のようなフィルタリング条件を考えます。

- TCP は VLAN orange から white への通信（セッション開始）のみを許可。white から orange への通信は拒否する。
- その他のプロトコルはすべて許可する。

スイッチ A の設定

1. VLAN の設定を行います。

```
CREATE VLAN=white VID=10 ↵
CREATE VLAN=orange VID=20 ↵
ADD VLAN=white PORT=1-12 ↵
ADD VLAN=orange PORT=13-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-white IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-orange IP=192.168.20.1 MASK=255.255.255.0 ↵
```

4. ハードウェア IP フィルターの設定を行います。

- フィルターを作成しマッチ条件を指定します。ここでは IP ヘッダーの始点・終点 IP アドレスとプロトコルフィールド、TCP ヘッダーの Syn、Ack フラグを条件として指定します。サブネット単位でアドレスを指定するため、SCLASS、DCLASS には C（クラス C = 24 ビットマスク）を指定します。

```
ADD SWITCH L3FILTER MATCH=SIPADDR,DIPADDR,PROTOCOL,TCPACK,TCP SYN
SCLASS=C DCLASS=C ↵
```

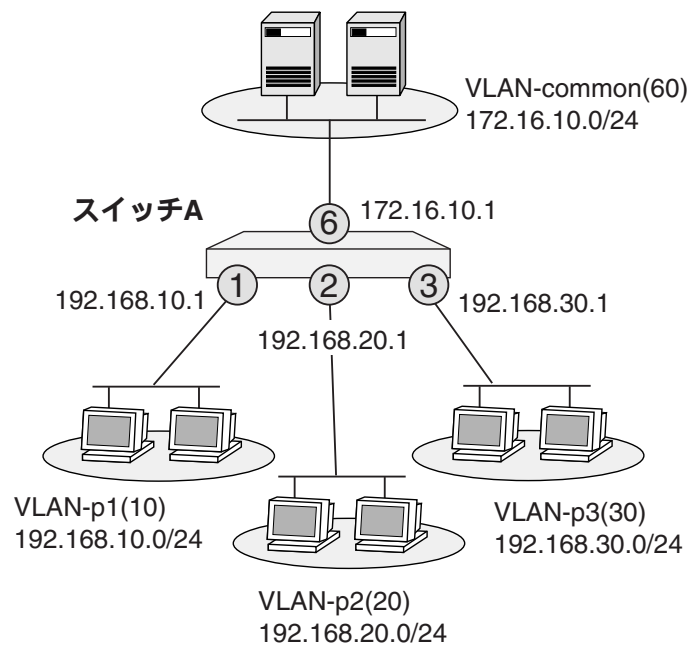
- 具体的な条件値とアクションを指定します。ここでは 192.168.10.0/24 から 192.168.20.0/24 への TCP セッション開始要求（Syn パケット）を破棄するよう設定します。

```
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0
DIPADDR=192.168.20.0 PROTOCOL=TCP TCP SYN=TRUE TCPACK=FALSE
ACTION=DENY ↵
```

設定は以上です。

「マルチプル VLAN」的構成例

ポート 1、2、3 を個別の VLAN とし、VLAN common を共有するよう設定します。個々の VLAN 間の通信は禁止します。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。



スイッチ A の設定

1. VLAN の設定を行います。

```
CREATE VLAN=p1 VID=10 ↵
CREATE VLAN=p2 VID=20 ↵
CREATE VLAN=p3 VID=30 ↵
CREATE VLAN=common VID=60 ↵
ADD VLAN=p1 PORT=1 ↵
ADD VLAN=p2 PORT=2 ↵
ADD VLAN=p3 PORT=3 ↵
ADD VLAN=common PORT=6 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-p1 IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-p2 IP=192.168.20.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-p3 IP=192.168.30.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-common IP=172.16.10.1 MASK=255.255.255.0 ↵
```

4. ハードウェア IP フィルターの設定を行います。

- フィルターを作成しマッチ条件を指定します。ここでは始点・終点 IP アドレスを条件とします。また、SCLASS、DCLASS パラメーターでクラス B マスクを指定し、アドレス指定を簡素化しています。

```
ADD SWITCH L3FILTER MATCH=SIPADDR,DIPADDR SCLASS=B DCLASS=B ↵
```

- 具体的な条件値とアクションを指定します。ここでは始点、終点とも 192.168.0.0/16 となるようなパケットを拒否します。1 ポート 1VLAN なので、同一 VLAN 内のパケットについては考慮しなくてもかまいません。

```
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.0.0
DIPADDR=192.168.0.0 ACTION=DENY ↵
```

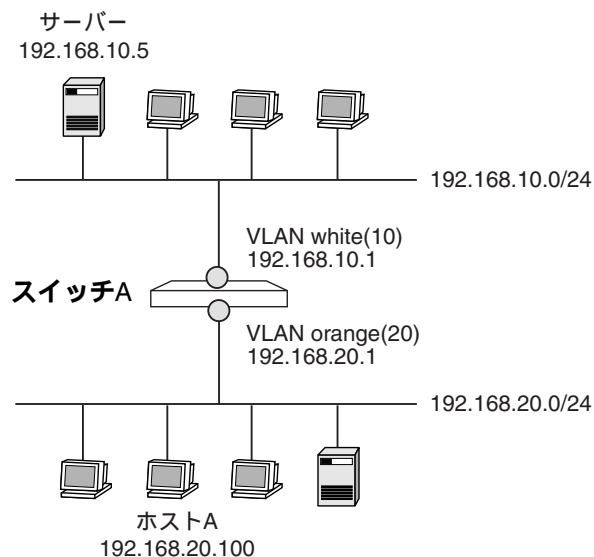
5. 本体への不正アクセスを防ぐため、Telnet サーバーを停止します。

```
DISABLE TELNET SERVER ↵
```

設定は以上です。

IP ベースの QoS

IP アドレスや TCP/UDP ポートに基づきパケット送信時の優先度に差を付ける IP ベース QoS の設定例を示します。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。



ここでは、次のような QoS を設定します。

- ホスト A (192.168.20.100) とサーバー (192.168.10.5) 間の IP トラフィックを最優先で送信する。具体的には最高位の 3 番キューから送信する。
- その他の IP トラフィックは通常の優先度で送信する (0 番キュー)。

- ユーザープライオリティーとキューのマッピングはデフォルト(1,0,0,1,2,2,3,3)とする。詳細は「QoS」および SET QOS HWPRIORITY コマンド (250 ページ) の解説をご覧ください。

スイッチ A の設定

1. VLAN の設定を行います。

```
CREATE VLAN=white VID=10 ↵
CREATE VLAN=orange VID=20 ↵
ADD VLAN=white PORT=1-12 ↵
ADD VLAN=orange PORT=13-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-white IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-orange IP=192.168.20.1 MASK=255.255.255.0 ↵
```

4. ハードウェア IP フィルターの設定を行います。

- マッチ条件 (フィルター) を作成します。ここでは始点・終点 IP アドレスを条件とします。ホスト A・サーバー間の対一通信に対するフィルタリングなので、SCLASS、DCLASS パラメーターには HOST を指定します。

```
ADD SWITCH L3FILTER MATCH=SIPADDR,DIPADDR SCLASS=HOST
DCLASS=HOST ↵
```

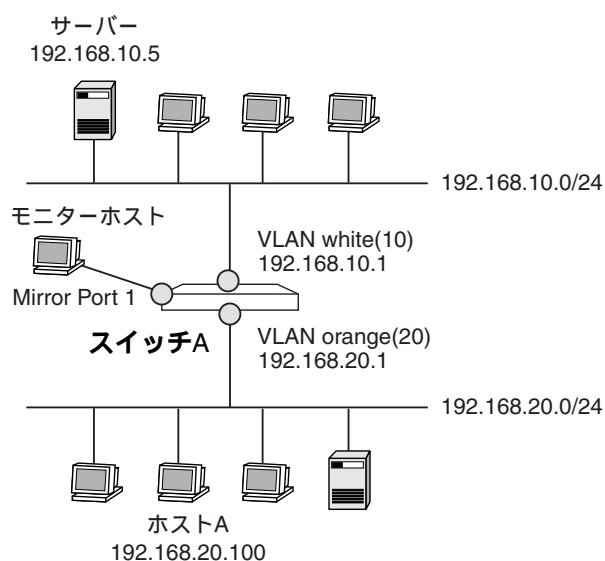
- フィルターエントリーを作成します。ここでは始点がサーバーで終点がホスト A、あるいは、始点がホスト A で終点がサーバーとなる 2 つのエントリーを追加します。アクションに SENDCOS を指定し、PRIORITY でプライオリティーを指定します。デフォルトの QoS マッピングでは、プライオリティー 7 のパケットは最上位の 3 番キューから最優先で送信されます。

```
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.5
DIPADDR=192.168.20.100 ACTION=SENDCOS PRIORITY=7 ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.20.100
DIPADDR=192.168.10.5 ACTION=SENDCOS PRIORITY=7 ↵
```

設定は以上です。

ハードウェア IP フィルターによるポートミラーリング

ハードウェア IP フィルターを用いて、特定の IP パケットだけをミラーポートにコピーする設定例を示します。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。



ここでは、ホスト A (192.168.20.100) とサーバー (192.168.10.5) 間の IP トラフィックだけをミラーポートにコピーするよう設定します。ミラーポートには 1 番ポートを使います。

なお、仕様によりハードウェア IP フィルター経由でミラーリングされたパケットは、VLAN タグが付いた状態でミラーポートに出力されます。キャプチャーソフトが VLAN タグを識別できない場合、IP パケットがプロトコルタイプ 0x8100 (802.1Q タグ) として表示される場合がありますのでご注意ください。

スイッチ A の設定

1. VLAN の設定を行います。

```
CREATE VLAN=white VID=10 ↵
CREATE VLAN=orange VID=20 ↵
ADD VLAN=white PORT=2-12 ↵
ADD VLAN=orange PORT=13-24 ↵
```

2. IP モジュールを有効にします。

```
ENABLE IP ↵
```

3. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-white IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-orange IP=192.168.20.1 MASK=255.255.255.0 ↵
```

4. ミラーポートを設定します。

```
SET SWITCH MIRROR=1 ↵
```

🔧 このときポート 1 が VLAN default 以外に所属しているとエラーになります。その場合は、DELETE

VLAN PORT コマンド (148 ページ) でポートを現在所属中の VLAN から削除した上で、本コマンドを実行してください。

5. ポートミラーリング機能を有効にします。

```
ENABLE SWITCH MIRROR ↵
```

6. ハードウェア IP フィルターの設定を行います。

- マッチ条件 (フィルター) を作成します。ここでは始点・終点 IP アドレスを条件とします。ホスト A・サーバー間の一对一通信に対するフィルタリングなので、SCLASS、DCLASS パラメータには HOST を指定します。

```
ADD SWITCH L3FILTER MATCH=SIPADDR,DIPADDR SCLASS=HOST
DCLASS=HOST ↵
```

- フィルターエントリを作成します。ここでは始点がサーバーで終点がホスト A、あるいは、始点がホスト A で終点がサーバーとなる 2 つのエントリを追加します。アクションに SENDMIRROR を指定し、マッチしたパケットのコピーがミラーポートから出力されるようにします。

```
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.5
DIPADDR=192.168.20.100 ACTION=SENDMIRROR ↵
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.20.100
DIPADDR=192.168.10.5 ACTION=SENDMIRROR ↵
```

設定は以上です。これにより、ホスト A・サーバー間の IP トラフィックだけがミラーポート (ポート 1) にコピーされるようになります。ミラーポートにアナライザーを接続すれば、ホスト A・サーバー間のトラフィックを解析できます。なお、ハードウェア IP フィルターによるミラーリングでは、ミラーされたパケットに VLAN タグが付きます。

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。

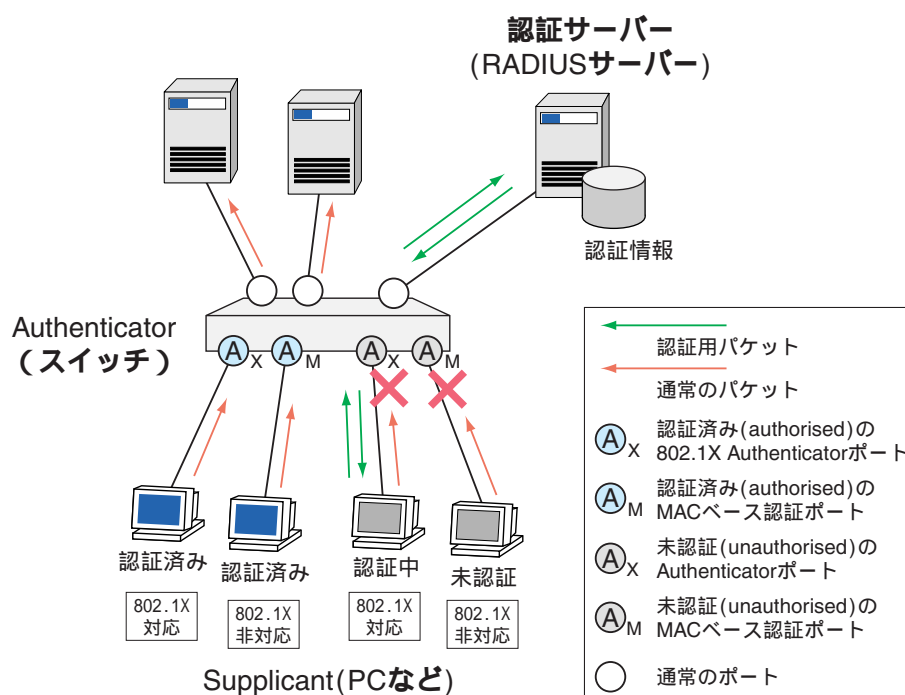
- IEEE 802.1X 認証（以下、802.1X 認証）
- MAC アドレスベース認証（以下、MAC ベース認証）

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。

Authenticator として認証可能な Supplicant は、システム全体で 480 台です (ポートあたりの制限はありません)。

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 (194 ページ) / SET PORTAUTH PORT コマンド (241 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、認証成功后、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 (194 ページ) / SET PORTAUTH PORT コマンド (241 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 (132 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 (132 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 (165 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 (163 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。

- 802.1X 認証モジュールを有効にします。

```
ENABLE PORTAUTH=8021X ↵
```

- 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 25: 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 26: 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 27: ダイナミック VLAN 用の属性

DHCP Snooping

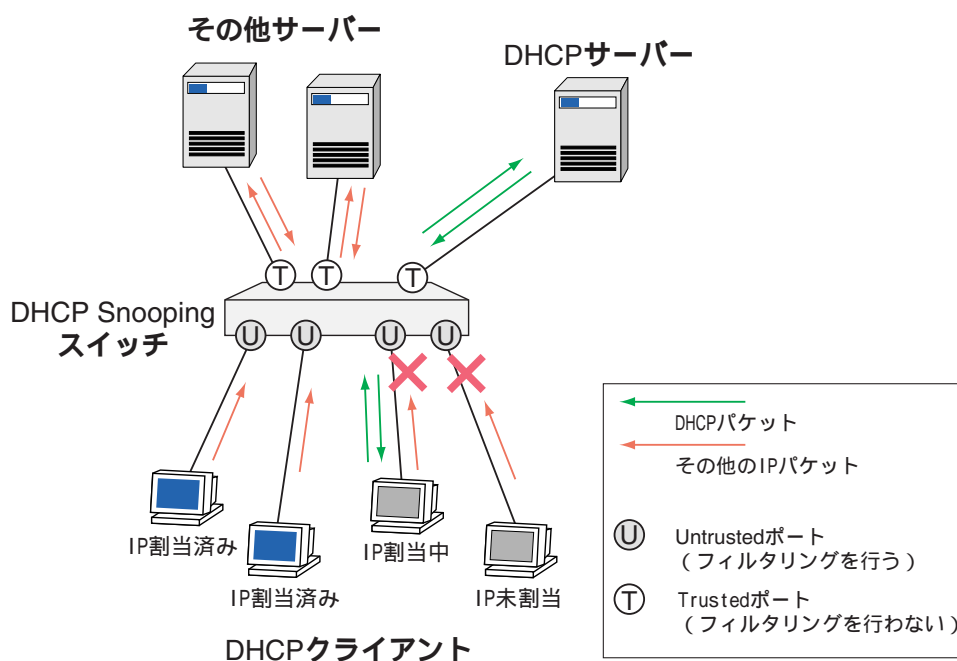
DHCP Snooping は、DHCP サーバー・クライアント間でやりとりされる DHCP メッセージを監視して動的な IP ソースフィルタリングを行う機能です。本機能を利用すれば、DHCP サーバーを用いたネットワーク環境において、正当な DHCP クライアントにだけ IP 通信を許可することができます。

- 🔗 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。

8724SL はポート 1～8、9～16、17～24、25、26 の 5 つ、8748SL はポート 1～8、9～16、17～24、15～32、33～41、42～48、49、50 の 8 つのブロックごとに、それぞれ最大 100 クライアントまで登録できます。システム全体では、最大 500 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 IP フィルター（L3 フィルター）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 IP フィルターの設定可能数が増減します。

DHCP Snooping を有効にすると、ハードウェア IP フィルターのマッチ条件（フィルター）を 2 個消費します。また、オプション機能の ARP セキュリティーを使用すると、さらに 1 個消費します（合計 3 個）。作成可能なマッチ条件はシステム全体で 14 個ですので、ご注意ください。

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、その他のポートには不特定多数の 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 ↓
```

☞ 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。

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）、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。

☞ 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（228 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（228 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（112 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（154 ページ）で無効化できます）。
- 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（228 ページ）の MAXLEASES パラメーターの値を増やす必要があります。

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（182 ページ）で ARP セキュリティーを有効にすると、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 ↓
```

- ④ 本機能は、DHCP Snooping が有効になっていないと動作しません。
- ④ 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ないでください。

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（184 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（228 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 287 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 (227 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 (278 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 (286 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 (282 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 DEBUG	171
DISABLE SWITCH STPFORWARD	179
ENABLE SWITCH DEBUG	204
ENABLE SWITCH STPFORWARD	213
RESET SWITCH	225
SHOW SWITCH	346
SHOW SWITCH COUNTER	348
SHOW SWITCH DEBUG	350

ポート

ACTIVATE SWITCH PORT AUTONEGOTIATE	110
ACTIVATE SWITCH PORT LOCK	111
ADD SWITCH TRUNK	131
CREATE SWITCH TRUNK	136
DELETE SWITCH TRUNK	147
DESTROY SWITCH TRUNK	151
DISABLE SWITCH LOOPDETECTION	175
DISABLE SWITCH MIRROR	176
DISABLE SWITCH PORT	177
DISABLE SWITCH PORT FLOW	178
ENABLE SWITCH LOOPDETECTION	208
ENABLE SWITCH MIRROR	210
ENABLE SWITCH PORT	211
ENABLE SWITCH PORT FLOW	212
RESET SWITCH PORT	226
SET SWITCH LOOPDETECTION	268
SET SWITCH MIRROR	270
SET SWITCH PORT	271
SET SWITCH TRUNK	276
SHOW SWITCH LOOPDETECTION	360
SHOW SWITCH LOOPDETECTION COUNTER	363
SHOW SWITCH PORT	365
SHOW SWITCH PORT COUNTER	369
SHOW SWITCH PORT INTRUSION	373
SHOW SWITCH TRUNK	375

LACP (IEEE 802.3ad)

ADD LACP PORT	114
DELETE LACP PORT	141
DISABLE LACP	157
DISABLE LACP DEBUG	158
ENABLE LACP	185
ENABLE LACP DEBUG	186
PURGE LACP	215
RESET LACP PORT COUNTER	220
SET LACP PORT	230
SET LACP PRIORITY	231
SHOW LACP	288
SHOW LACP PORT	289
SHOW LACP TRUNK	293

バーチャル LAN

ADD VLAN PORT	132
CREATE VLAN	138
DELETE VLAN PORT	148
DESTROY VLAN	152
DISABLE VLAN DEBUG	180
ENABLE VLAN DEBUG	214
SET VLAN PORT	277
SHOW VLAN	377
SHOW VLAN DEBUG	381

スパニングツリープロトコル (STP/RSTP)

ADD STP VLAN	117
CREATE STP	135
DELETE STP VLAN	143
DESTROY STP	150
DISABLE STP	166
DISABLE STP DEBUG	167
DISABLE STP PORT	168
DISABLE STP PORT DEBUG	169
ENABLE STP	199
ENABLE STP DEBUG	200
ENABLE STP PORT	201
ENABLE STP PORT DEBUG	202
PURGE STP	218
RESET STP	224
SET STP	254
SET STP PORT	256
SHOW STP	335

SHOW STP COUNTER	339
SHOW STP DEBUG	341
SHOW STP PORT	343
マルチブルスパニングツリープロトコル (MSTP)	
ADD MSTP MSTI VLAN	116
CREATE MSTP MSTI	134
DELETE MSTP MSTI VLAN	142
DESTROY MSTP MSTI	149
DISABLE MSTP	159
DISABLE MSTP CIST PORT	160
DISABLE MSTP DEBUG MSTI	161
DISABLE MSTP MSTI PORT	162
ENABLE MSTP	187
ENABLE MSTP CIST PORT	188
ENABLE MSTP DEBUG MSTI	189
ENABLE MSTP MSTI PORT	191
PURGE MSTP	216
RESET MSTP COUNTER PORT	221
SET MSTP	232
SET MSTP CIST	234
SET MSTP CIST PORT	235
SET MSTP MSTI	237
SET MSTP MSTI PORT	238
SHOW MSTP	295
SHOW MSTP CIST	298
SHOW MSTP CIST PORT	301
SHOW MSTP COUNTER PORT	304
SHOW MSTP DEBUG MSTI	306
SHOW MSTP MSTI	307
SHOW MSTP MSTI PORT	310
フォワーディングデータベース	
ADD SWITCH FILTER	119
DELETE SWITCH FILTER	144
DISABLE SWITCH AGEINGTIMER	170
DISABLE SWITCH FILTER VLANSECURE	172
DISABLE SWITCH LEARNING	174
ENABLE SWITCH AGEINGTIMER	203
ENABLE SWITCH FILTER VLANSECURE	205
ENABLE SWITCH LEARNING	207
SET SWITCH AGEINGTIMER	258
SET SWITCH L3AGEINGTIMER	259

SHOW SWITCH FDB	351
SHOW SWITCH FILTER	354
QoS	
SET QOS HWPRIORITY	250
SET QOS HWQUEUE	252
SET SWITCH QOS	274
SHOW QOS HWPRIORITY	333
SHOW QOS HWQUEUE	334
SHOW SWITCH QOS	374
ハードウェア IP フィルター	
ADD SWITCH L3FILTER ENTRY	121
ADD SWITCH L3FILTER MATCH	127
DELETE SWITCH L3FILTER	145
DELETE SWITCH L3FILTER ENTRY	146
DISABLE SWITCH L3FILTER	173
ENABLE SWITCH L3FILTER	206
SET SWITCH L3FILTER ENTRY	260
SET SWITCH L3FILTER MATCH	265
SHOW SWITCH L3FILTER	356
ポート認証	
ACTIVATE PORTAUTH PORT REAUTHENTICATE	109
DISABLE PORTAUTH	163
DISABLE PORTAUTH DEBUG	164
DISABLE PORTAUTH PORT	165
ENABLE PORTAUTH	192
ENABLE PORTAUTH DEBUG	193
ENABLE PORTAUTH PORT	194
PURGE PORTAUTH PORT	217
RESET PORTAUTH PORT	222
RESET PORTAUTH PORT MULTIMIB	223
SET PORTAUTH HYPHEN	239
SET PORTAUTH IDTOGGLE	240
SET PORTAUTH PORT	241
SET PORTAUTH PORT SUPPLICANTMAC	245
SET PORTAUTH USERNAME	248
SHOW PORTAUTH	312
SHOW PORTAUTH COUNTER	316
SHOW PORTAUTH MULTISUPPLICANT PORT	319
SHOW PORTAUTH PORT	323
SHOW PORTAUTH TIMER	329

DHCP Snooping

ADD DHCP Snooping BINDING	112
DELETE DHCP Snooping BINDING	140
DISABLE DHCP Snooping	153
DISABLE DHCP Snooping ARPSECURITY	154
DISABLE DHCP Snooping LOG	155
DISABLE DHCP Snooping OPTION82	156
ENABLE DHCP Snooping	181
ENABLE DHCP Snooping ARPSECURITY	182
ENABLE DHCP Snooping LOG	183
ENABLE DHCP Snooping OPTION82	184
RESET DHCP Snooping COUNTER	219
SET DHCP Snooping CHECKINTERVAL	227
SET DHCP Snooping PORT	228
SHOW DHCP Snooping	278
SHOW DHCP Snooping COUNTER	280
SHOW DHCP Snooping DATABASE	282
SHOW DHCP Snooping FILTER	285
SHOW DHCP Snooping PORT	286

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 (192 ページ)

ENABLE PORTAUTH PORT (194 ページ)

SHOW PORTAUTH MULTISUPPLICANT PORT (319 ページ)

SHOW PORTAUTH PORT (323 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 (271 ページ)

SHOW SWITCH PORT (365 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 (271 ページ)

SHOW SWITCH PORT (365 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 (140 ページ)
DISABLE DHCP Snooping ARP Security (154 ページ)
SET DHCP Snooping Port (228 ページ)
SHOW DHCP Snooping Database (282 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。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 (8 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。

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 (141 ページ)

SET LACP PORT (230 ページ)

SHOW LACP PORT (289 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 (134 ページ)

DELETE MSTP MSTI VLAN (142 ページ)

SHOW MSTP (295 ページ)

SHOW MSTP MSTI (307 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。大文字小文字を区別しない)

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
```

関連コマンド

DELETE STP VLAN (143 ページ)

ADD STP VLAN

SHOW STP (335 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。大文字小文字を区別しない)

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 3 (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 ACTION=FORWARD PORT=3
```

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 ACTION=DISCARD PORT=6
```

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 ACTION=FORWARD PORT=2 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 ACTION=FORWARD PORT=5  
VLAN=orange
```

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 (144 ページ)

SET SWITCH PORT (271 ページ)

SHOW SWITCH FILTER (354 ページ)

ADD SWITCH L3FILTER ENTRY

カテゴリー：スイッチング / ハードウェア IP フィルター

```
ADD SWITCH L3FILTER=filter-id ENTRY [TOS=0..7] [IPDSCP=0..63]
[TTL=0..255] [PROTOCOL={TCP|UDP|ICMP|IGMP|protocol}] [SIPADDR=ipadd]
[DIPADDR=ipadd] [TCPSPORT={port|port-name}] [TCPDPORT={port|port-name}]
[TCP SYN={TRUE|FALSE}] [TCPACK={TRUE|FALSE}] [TCPFIN={TRUE|FALSE}]
[TYPE=protocoltype] [UDPSPORT={port|port-name}] [UDPDPOR={port|
port-name}] [I PORT=port-number] [E PORT=port-number] [PRIORITY=0..7]
[PORT=port-number] [NEWTOS=0..7] [NEWIPDSCP=0..63] [ACTION={SETPRIORITY|
SENDCOS|SETTOS|DENY|SENDEPORT|SENDMIRROR|MOVEPRIOTOTOS|MOVETOSTOPRIO|
NODROP|SENDNONUNICASTTOPORT|SETIPDSCP}[ , ... ]]
```

filter-id: フィルター番号 (1~14)

protocol: IP プロトコル番号 (0~255)

ipadd: IP アドレス

port: TCP/UDP ポート番号 (0~65535)

port-name: サービス名

protocoltype: L3 プロトコル番号 (16 進数)

port-number: スイッチポート番号 (1~)

解説

ハードウェア IP フィルターにフィルターエントリを追加する。

ADD SWITCH L3FILTER MATCH コマンドで指定したすべてのパケットフィールドに対して、フィルタリング条件を実際の値で指定し、マッチ時のアクション（複数可）を指定する。

エントリ番号はコマンド実行時にシステムが自動で割り当てる。この番号は可変なので、エントリの追加や削除によって前後にずれる可能性がある。他のコマンドでエントリ番号を指定するときは、必ず SHOW SWITCH L3FILTER コマンドに ENTRY パラメータを付けて実行し、希望するエントリであることを確認してから指定すること。

フィルターエントリは「システム全体」で 124 個まで設定可能。

パラメーター

L3FILTER フィルター（マッチ条件）番号。この番号は可変なので、SHOW SWITCH L3FILTER コマンドで確認してから指定すること

TOS （フィルタリング条件）対象パケットの IP TOS 優先度（TOS オクテットの 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。

IPDSCP （フィルタリング条件）対象パケットの IP DSCP（DiffServ Code Point）フィールド値。有効範囲は 0~63。TOS とは同時に指定できない。

TTL （フィルタリング条件）対象パケットの IP TTL（生存時間）フィールド値。有効範囲は 0~255。

PROTOCOL （フィルタリング条件）対象パケットの IP プロトコルフィールド値。TCP、UDP、ICMP、

- IGMP については名前でも指定できる。その他プロトコルの場合は IP プロトコル番号で指定する。
- SIPADDR** (フィルタリング条件) 対象パケットの始点 IP アドレス。パケットマッチング時には、ここで指定したアドレスに対して ADD SWITCH L3FILTER MATCH コマンドの SCLASS パラメーターで指定したマスクが適用される。ハードウェア IP フィルターはルーティングされない同一 IP ネットワーク内のトラフィックに対しても有効。
- DIPADDR** (フィルタリング条件) 対象パケットの終点 IP アドレス。パケットマッチング時には、ここで指定したアドレスに対して ADD SWITCH L3FILTER MATCH コマンドの DCLASS パラメーターで指定したマスクが適用される。ハードウェア IP フィルターはルーティングされない同一 IP ネットワーク内のトラフィックに対しても有効。
- TCPSPORT** (フィルタリング条件) 対象パケットの TCP 始点ポート。ポート番号かサービス名で指定する。PROTOCOL パラメーターに TCP を指定したときのみ有効。
- TCPDPORT** (フィルタリング条件) 対象パケットの TCP 終点ポート。ポート番号かサービス名で指定する。PROTOCOL パラメーターに TCP を指定したときのみ有効。
- TCP SYN** (フィルタリング条件) 対象パケットの TCP 制御フラグ「Syn」の値 (オン・オフ)。TRUE はフラグが立っていることを、FALSE はフラグが立っていないことを示す。PROTOCOL パラメーターに TCP を指定したときのみ有効。また、EPORT パラメーターとは併用しないこと。
- TCP ACK** (フィルタリング条件) 対象パケットの TCP 制御フラグ「Ack」の値 (オン・オフ)。TRUE はフラグが立っていることを、FALSE はフラグが立っていないことを示す。PROTOCOL パラメーターに TCP を指定したときのみ有効。また、EPORT パラメーターとは併用しないこと。
- TCP FIN** (フィルタリング条件) 対象パケットの TCP 制御フラグ「Fin」の値 (オン・オフ)。TRUE はフラグが立っていることを、FALSE はフラグが立っていないことを示す。PROTOCOL パラメーターに TCP を指定したときのみ有効。また、EPORT パラメーターとは併用しないこと。
- TYPE** (フィルタリング条件) 対象パケット (フレーム) のレイヤー 3 プロトコルタイプフィールド値 (16 進数)。本パラメーターを指定した場合、他のフィルタリング条件パラメーターは無効となる。また、ACTION に SETTOS を指定することはできない。プロトコル番号は、ADD SWITCH L3FILTER MATCH コマンドの TYPE パラメーターで指定したフレームフォーマットにおけるものを指定すること。Ethernet Version 2 と 802.2 LLC (DSAP、SSAP) におけるプロトコルタイプは 2 バイト、SNAP のプロトコルタイプは 5 バイト長で指定する。
- UDPSPORT** (フィルタリング条件) 対象パケットの UDP 始点ポート。ポート番号かサービス名で指定する。PROTOCOL パラメーターに UDP を指定したときのみ有効。
- UDP DPORT** (フィルタリング条件) 対象パケットの UDP 終点ポート。ポート番号かサービス名で指定する。PROTOCOL パラメーターに UDP を指定したときのみ有効。
- IMPORT** (フィルタリング条件) 対象パケットの入力スイッチポート。指定ポートから入力されたパケットだけがフィルタリングの対象となる。ADD SWITCH L3FILTER MATCH コマンドで IMPORT=TRUE を指定した場合にのみ有効。
- EPORT** (フィルタリング条件) 対象パケットの出力スイッチポート。指定ポートから出力されるパケットだけがフィルタリングの対象となる。ADD SWITCH L3FILTER MATCH コマンドで EIMPORT=TRUE を指定した場合にのみ有効。ただし、EPORT パラメーターを指定した場合は、FDB か L3 テーブルに登録されていない MAC アドレス (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) 宛てのパケットにはフィルターが適用されなくなるので注意すること。
- PRIORITY** (アクションパラメーター) 対象パケットに適用する 802.1p ユーザープライオリティ (0 ~ 7) 値。ACTION パラメーターに SETPRIORITY か SENDCOS を指定したときのみ有効。ACTION

に SETPRIORITY を指定したときは、パケットのユーザープライオリティーフィールドに PRIORITY パラメーターで指定した値を書き込んで送出する（出力スイッチポートがタグ付きでないという意味を持たない）。ACTION に SENDCOS を指定したときは、パケットを PRIORITY パラメーターで指定したユーザープライオリティーに対応する送信キューに入れる。省略時は 0。

PORT （アクションパラメーター）対象パケットを出力するスイッチポート。ACTION パラメーターに SENDEPORT か SENDNONUNICASTTOPORT を指定したときのみ有効。このとき、本パラメーターで指定するポート（出力ポート）と入力ポートが同一 VLAN になるよう注意すること。さらに、8748SL では、入力ポートと本パラメーターで指定する出力ポートが、同一ポートグループ「1～24、50」または「25～48、49」に入っていないと注意。

NEWTOS （アクションパラメーター）パケット送信時に IP ヘッダーの TOS 優先度フィールドにセットする値。ACTION に SETTOS を指定した場合のみ有効。

NEWIPDSCP （アクションパラメーター）パケット送信時に IP ヘッダーの DSCP フィールドにセットする値。ACTION に SETIPDSCP を指定した場合のみ有効。

ACTION パケットがフィルターの条件に一致したときのアクション。カンマ区切りで複数のアクションを指定できる。別表に示すとおり、アクションはいくつかの「カテゴリー」に分類できる。表 1 で（相互排他）と記されているカテゴリーは、パケットが同一カテゴリー内の複数のアクションにマッチした場合に、最後にマッチしたエントリー、すなわち、フィルター番号・エントリー番号のもっとも大きなエントリーのアクションだけが実行されることを示している。アクションの詳細は別表を参照のこと。

パケットの破棄・通過を制御するアクション（相互排他）	
DENY	パケットを破棄する。マッチしたエントリーの中に DENY アクションが含まれている場合は、NODROP によって打ち消されない限り、通常のポートからパケットが出力されることはない（SENDEPORT、SENDCOS アクションがある場合でもパケットは出力されない）。ただし、ポートミラーリング機能が有効な場合は、ミラーポートからパケットのコピーが出力される（SENDMIRROR アクションも有効）
NODROP	DENY アクションを打ち消し、本来破棄されるべきパケットを出力する。おもに、デフォルト拒否の設定において、一部のパケットだけを許可したい場合に使う
出力ポートを変更するアクション	
SENDEPORT	ユニキャストパケット（ここでは、ブロードキャスト、マルチキャスト、および、未学習のユニキャストを除くパケットのこと）の出力先を 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）と入力ポートが同じ VLAN でなくてはならないので、設定には注意すること。さらに、8748SL では、入力ポートと出力ポート（PORT）が、同一ポートグループ「1～24、50」または「25～48、49」に入っていないと注意。また、仕様により、本来なら L3 スイッチング（ルーティング）されるはずのパケットは、出力ポート（PORT）のタグ設定（タグ付き・タグなし）にかかわらず、本来のルーティング先の VLAN タグが付いた状態で出力される

SENDNONUNICAST	非ユニキャストパケット（ここでは、ブロードキャスト、マルチキャスト、および、未学習のユニキャストのこと）の出力先を PORT パラメーターで指定されたポートだけに変更する。このとき、出力ポートと入力ポートが同じ VLAN でなくてはならないので、設定には注意すること。さらに、8748SL では、入力ポートと PORT パラメーターで指定する出力ポートが、同一ポートグループ「1～24、50」または「25～48、49」に入っていないと注意
出力キューを変更するアクション（相互排他）	
SEDCOS	パケットを PRIORITY パラメーターで指定されたプライオリティーに対応するレベルの送信キューに入れる
MOVETOSTOPRIO	受信時の IP ヘッダーの TOS 優先度（precedence）フィールドの値を、VLAN タグフレームの 802.1p ユーザープライオリティーフィールドにコピーする。また、コピー後のユーザープライオリティーに対応するレベルの送信キューにパケットを入れる
802.1p プライオリティーを書き換えるアクション（相互排他）	
MOVETOSTOPRIO	受信時の IP ヘッダーの TOS 優先度（precedence）フィールドの値を、VLAN タグフレームの 802.1p ユーザープライオリティーフィールドにコピーする。また、コピー後のユーザープライオリティーに対応するレベルの送信キューにパケットを入れる
SETPRIORITY	VLAN タグフレームの 802.1p ユーザープライオリティーフィールドに、PRIORITY パラメーターで指定された値を書き込む。出力ポートがタグ付きの場合のみ有効。出力ポートがタグなしの場合はパケットにタグが付かないので、本アクションは意味を持たない
IP TOS/DSCP フィールドを書き換えるアクション（相互排他）	
SETTOS	パケットの IP TOS 優先度（precedence）フィールドに、NEWTOS パラメーターで指定された値を書き込む。TYPE パラメーターで IP 以外のプロトコルを指定した場合は無効
MOVEPRIOTOTOS	受信時の VLAN タグフレームの 802.1p ユーザープライオリティーフィールドの値を、IP ヘッダーの TOS 優先度（precedence）フィールドにコピーする
SETIPDSCP	IP ヘッダーの DSCP（DiffServ Code Point）フィールドに、NEWIPDSCP パラメーターで指定された値を書き込む。TYPE パラメーターで IP 以外のプロトコルを指定した場合は無効
その他のアクション	
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、ミラーポートを指定し、ポートミラーリング機能を有効にしておく必要がある。パケットが複数のエントリーにマッチした場合、DENY、NODROP、SEND～を除く他のアクションがすべて適用された状態でパケットがミラーされる。また、DENY 対象のパケットであってもミラーされる

表 28: ACTION パラメーターに指定できるオプション

例

ポート 1～3 で受信した 192.168.10.0/24 からの IP パケットを破棄

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=C IMPORT=TRUE
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 IPORT=1 ACTION=DENY
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 IPORT=2 ACTION=DENY
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 IPORT=3 ACTION=DENY
```

192.168.10.100 からの TCP コネクション確立要求を拒否(片方向のみ拒否。他のホストから 192.168.10.100 へはコネクションを張れる)

```
ADD SWITCH L3FILTER MATCH=SIPADDR, PROTOCOL, TCPSYN, TCPACK SCLASS=HOST
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.100 PROTOCOL=TCP
TCPSYN=TRUE TCPACK=FALSE ACTION=DENY
```

192.168.10.5 からのパケットの 802.1p ユーザープライオリティーフィールドに 4 をセットして送信

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=HOST
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.5 PRIORITY=4
ACTION=SETPRIORITY
```

192.168.10.0/24 からのパケットは原則拒否だが、192.168.10.103 からのパケットだけは許可

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=C
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 ACTION=DENY
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=HOST
ADD SWITCH L3FILTER=2 ENTRY SIPADDR=192.168.10.103 ACTION=NODROP
```

備考・注意事項

フィルタリング条件として EPORT (出力スイッチポート) を指定した場合、FDB、L3 テーブルのどちらにも登録されていない MAC アドレス (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) 宛てのパケットにはフィルターが適用されなくなる。したがって、TCP 制御フラグによるフィルタリング (TCPSYN、TCPACK、TCPFIN パラメーター) を行う場合、および、ブロードキャスト、マルチキャストパケットのフィルタリングを行う場合は、EPORT パラメーターを併用しないこと。

8748SL では、ポートグループ「1～24、50」と「25～48、49」をまたいで、IPORT と EPORT を同時に設定することはできない。

8748SL では、「ACTION=SENDCOS」のエントリーを持つ、あるいは、「NOMACTHACTION=SENDCOS」の指定があるフィルター（マッチ条件）は、合計で 4 つまでしか作れない。

8748SL では、パケットの入力ポートと出力ポートがポートグループ「1～24、50」と「25～48、49」をまたいだ場合に、以下の制限がある（SENDEPORT、SENDNONUNICASTTOPORT アクションにおける「出力ポート」は、PORT パラメーターで指定したポートを意味する）。これらの制限は 8748SL 固有のもので、8724SL にはない。

- ・まったく機能しないアクション：SENDEPORT、SENDNONUNICASTTOPORT
- ・IPOINT を指定できないアクション（指定した場合はマッチしない）：SENDCOS
- ・EPOINT を指定できないアクション（指定した場合はマッチしない）：NODROP、SETTOS、MOVE-TOSTOPRIO、MOVEPRIOTOTOS、SETIPDSCP
- ・制限のないアクション：DENY、SETPRIORITY、SENDMIRROR

前記の制限を回避するため、8748SL では原則として、入力ポートと出力ポートが「1～24、50」または「25～48、49」のどちらかのポートグループに両方とも入るよう設定することをおすすめする。

関連コマンド

DELETE SWITCH L3FILTER ENTRY (146 ページ)

SET SWITCH L3FILTER ENTRY (260 ページ)

SHOW SWITCH L3FILTER (356 ページ)

ADD SWITCH L3FILTER MATCH

カテゴリー：スイッチング / ハードウェア IP フィルター

```
ADD SWITCH L3FILTER MATCH={TOS|IPDSCP|TTL|PROTOCOL|SIPADDR|DIPADDR|
TCPSPORT|TCPPDPORT|TCP SYN|TCPACK|TCPFIN|TYPE|UDPSPORT|UDPDPORT}[,...]
[SCLASS={A|B|C|HOST|1..32}] [DCLASS={A|B|C|HOST|1..32}] [IMPORT={TRUE|
FALSE}] [EXPORT={TRUE|FALSE}] [TYPE={802|ETHII|SNAP}]
[NOMATCHACTION={SETPRIORITY|SENDCOS|SETTOS|DENY|SENDEPORT|SENDMIRROR|
MOVEPRIOTOTOS|MOVETOSTOPRIO|SENDNONUNICASTTOPORT|SETIPDSCP}[,...]]
[NOMATCHDSCP=0..63] [NOMATCHPORT=port-number] [NOMATCHPRIORITY=0..7]
[NOMATCHTOS=0..7]
```

port-number: スイッチポート番号 (1~)

解説

ハードウェア IP フィルター (L3 フィルター) を作成する。

このコマンドでは、どのパケットフィールドをフィルタリング条件 (マッチ条件) として使用するかを指定する。実際のフィルタリング条件 (フィルターエントリー) は ADD SWITCH L3FILTER ENTRY コマンドで指定する。フィルター (マッチ条件) はシステム全体で 14 個まで、フィルターエントリーはシステム全体で 124 個まで設定可能。

フィルター番号はコマンド実行時にシステムが自動で割り当てる。この番号は可変なので、他のフィルターの削除により変更される可能性がある。他のコマンドでフィルター番号を指定するときは、必ず SHOW SWITCH L3FILTER コマンドで確認してから指定すること。

パラメーター

MATCH フィルタリング条件として使用するパケットフィールドを指定する。カンマ区切りで複数指定が可能。詳細は別表を参照。

SCLASS SIPADDR (始点 IP アドレス) のパケットマッチング時に適用するネットマスク。A、B、C はそれぞれクラス A (8 ビット) B (16 ビット) C (24 ビット) の標準マスク。HOST は単一アドレスを示す 32 ビットマスク。あるいは、1~32 の任意長のマスクを指定できる。

DCLASS DIPADDR (終点 IP アドレス) のパケットマッチング時に適用するネットマスク。A、B、C はそれぞれクラス A (8 ビット) B (16 ビット) C (24 ビット) の標準マスク。HOST は単一アドレスを示す 32 ビットマスク。あるいは、1~32 の任意長のマスクを指定できる。

IMPORT 特定のスイッチポートから入力されたパケットだけをフィルタリングの対象にしたい場合に TRUE を指定する。具体的なポート番号は ADD SWITCH L3FILTER ENTRY コマンドの IPORT パラメーターで指定する (指定ポートから入力されたパケットだけがフィルタリングの対象となる)。FALSE のときはすべてのポートでフィルタリングが行われる。デフォルトは FALSE。

EXPORT 特定のスイッチポートから出力されるパケットだけをフィルタリングの対象にしたい場合に TRUE を指定する。具体的なポート番号は ADD SWITCH L3FILTER ENTRY コマンドの EPORT

パラメーターで指定する（指定ポートから出力されるパケットだけがフィルタリングの対象となる。ただし、本パラメーターに TRUE を指定した場合は、FDB か L3 テーブルに登録されていない MAC アドレス宛てのパケットがフィルタリング対象にならないという制限がある。詳細は ADD SWITCH L3FILTER ENTRY コマンドの EPORT パラメーターの説明を参照）。FALSE のときはすべてのポートでフィルタリングが行われる。デフォルトは FALSE。

TYPE フィルタリング条件として TYPE（L3 プロトコルタイプ）を指定した場合に、フレームフォーマット（エンキャプセレーション）を指定する。802（802.2 LLC）、ETHII（Ethernet Version 2）、SNAP（802.2 LLC + SNAP）から選択する。ADD SWITCH L3FILTER ENTRY コマンドの TYPE パラメーターには、ここで指定したフレームフォーマットのプロトコル番号を指定する。

NOMATCHACTION フィルター内のどのエントリーにもマッチしなかったパケットに対するデフォルトのアクション。カンマ区切りで複数のアクションを指定できる。アクションの詳細については、ADD SWITCH L3FILTER ENTRY コマンドの表を参照のこと（ただし、NODROP アクションは指定できない。また、アクションパラメーターの NEWIPDSCP、PORT、PRIORITY、NEWTOS は、それぞれ NOMATCHDSCP、NOMATCHPORT、NOMATCHPRIORITY、NOMATCHTOS となる）。省略時は SENDCOS。

NOMATCHDSCP （どのエントリーにもマッチしなかったパケットに対するアクションパラメーター）パケット送信時に IP ヘッダーの DSCP フィールドにセットする値。NOMATCHACTION に SETIPDSCP を指定した場合のみ有効。

NOMATCHPORT （どのエントリーにもマッチしなかったパケットに対するアクションパラメーター）対象パケットを出力するスイッチポート。NOMATCHACTION パラメーターに SENDEPORT か SENDNONUNICASTTOPORT を指定したときのみ有効。このとき、本パラメーターで指定するポート（出力ポート）と入力ポートが同一 VLAN になるよう注意すること。さらに、8748SL では、入力ポートと本パラメーターで指定する出力ポートが、同一ポートグループ「1～24、50」または「25～48、49」に入っていないと注意。

NOMATCHPRIORITY （どのエントリーにもマッチしなかったパケットに対するアクションパラメーター）対象パケットに適用する 802.1p ユーザープライオリティー（0～7）値。NOMATCHACTION パラメーターに SETPRIORITY か SENDCOS を指定したときのみ有効。NOMATCHACTION に SETPRIORITY を指定したときは、パケットのユーザープライオリティーフィールドに NOMATCHPRIORITY パラメーターで指定した値を書き込んで送出する（出力スイッチポートがタグ付きでないという意味を持たない）。NOMATCHACTION に SENDCOS を指定したときは、パケットを NOMATCHPRIORITY パラメーターで指定したユーザープライオリティーに対応する送信キューに入る。省略時は 0。

NOMATCHTOS （どのエントリーにもマッチしなかったパケットに対するアクションパラメーター）パケット送信時に IP ヘッダーの TOS 優先度フィールドにセットする値。NOMATCHACTION に SETTOS を指定した場合のみ有効。

TOS	IP ヘッダーの TOS オクテットの優先度（precedence）フィールド。IPDSCP とは同時に指定できない
IPDSCP	IP ヘッダーの DSCP（DiffServ Code Point）フィールド。IPTOS とは同時に指定できない

TTL	IP ヘッダーの TTL (生存時間) フィールド
PROTOCOL	IP ヘッダーのプロトコルフィールド
SIPADDR	IP ヘッダーの始点 IP アドレス。本オプションを指定するときは、SCLASS パラメーターの指定も必要。
DIPADDR	IP ヘッダーの終点 IP アドレス。本オプションを指定するときは、DCLASS パラメーターの指定も必要。
TCPSPORT	TCP ヘッダーの始点ポート。本オプションを指定するときは PROTOCOL の指定も必要。
TCPDPORT	TCP ヘッダーの終点ポート。本オプションを指定するときは PROTOCOL の指定も必要。
TCPSYN	TCP ヘッダーの制御フラグ「Syn」。本オプションを指定するときは PROTOCOL の指定も必要。また、EMPORT に TRUE を指定しないこと。
TCPACK	TCP ヘッダーの制御フラグ「Ack」。本オプションを指定するときは PROTOCOL の指定も必要。また、EMPORT に TRUE を指定しないこと。
TCPFIN	TCP ヘッダーの制御フラグ「Fin」。本オプションを指定するときは PROTOCOL の指定も必要。また、EMPORT に TRUE を指定しないこと。
TYPE	Ethernet フレームの L3 プロトコルタイプフィールド。本オプションを指定するときは、TYPE パラメーターでフレームフォーマットも指定する必要がある。他のオプションと併用はできない。
UDPSPORT	UDP ヘッダーの始点ポート。本オプションを指定するときは PROTOCOL の指定も必要。
UDPDPOR	UDP ヘッダーの終点ポート。本オプションを指定するときは PROTOCOL の指定も必要。

表 29: MATCH パラメーターに指定できるオプション

例

ポート 1~3 で受信した 192.168.10.0/24 からの IP パケットを破棄

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=C IMPORT=TRUE
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 IPORT=1 ACTION=DENY
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 IPORT=2 ACTION=DENY
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.0 IPORT=3 ACTION=DENY
```

192.168.10.100 からの TCP コネクション確立要求を拒否(片方向のみ拒否。他のホストから 192.168.10.100 へはコネクションを張れる)

```
ADD SWITCH L3FILTER MATCH=SIPADDR, PROTOCOL, TCPSYN, TCPACK SCLASS=HOST
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.100 PROTOCOL=TCP
TCPSYN=TRUE TCPACK=FALSE ACTION=DENY
```

192.168.10.5 からのパケットの 802.1p ユーザープライオリティーフィールドに 4 をセットして送信

```
ADD SWITCH L3FILTER MATCH=SIPADDR SCLASS=HOST
```

```
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.5 PRIORITY=4  
ACTION=SETPRIORITY
```

NetBEUI パケットをすべて破棄する。

```
ADD SWITCH L3FILTER MATCH=TYPE TYPE=802
```

```
ADD SWITCH L3FILTER=1 ENTRY TYPE=F0F0 ACTION=DENY
```

関連コマンド

ADD SWITCH L3FILTER ENTRY (121 ページ)

DELETE SWITCH L3FILTER (145 ページ)

SET SWITCH L3FILTER MATCH (265 ページ)

SHOW SWITCH L3FILTER (356 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 8 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。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「uplink」にポート 1~4 を追加する。

```
ADD SWITCH TRUNK=uplink PORT=1-4
```

関連コマンド

CREATE SWITCH TRUNK (136 ページ)

DELETE SWITCH TRUNK (147 ページ)

DESTROY SWITCH TRUNK (151 ページ)

SET SWITCH TRUNK (276 ページ)

SHOW SWITCH TRUNK (375 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|GROUP}]

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)

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 にポートを追加する。

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、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 ポートのタグ設定。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。省略時は UNTAGGED。

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。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。

GROUP 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同一グループのプライベートポートになる。なお、VLAN パラメーターでマルチプル VLAN (Private VLAN) を指定した場合で、UPLINK オプションも GROUP オプションも付けずに追加したポートは、単独の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、アップリンクポートになってはならない。8748SL では、ポートグループ「1~24、50」と「25~48、49」をまたぐプライベートポートグループは作成できない。

例

VLAN orange にポート 13~24 を (タグなしポートとして) 割り当てる。

```
ADD VLAN=orange PORT=13-24
```

ポート 25 を VLAN white と orange のタグ付きポートに設定する。

```
ADD VLAN=white PORT=25 FRAME=TAGGED
```

```
ADD VLAN=orange PORT=25 FRAME=TAGGED
```

備考・注意事項

マルチプル VLAN (Private VLAN) のプライベートポートは、アップリンクポートを指定した後でないと追加できない。

8748SL では、ポートグループ「1～24、50」と「25～48、49」をまたぐプライベートポートグループは作成できない。

関連コマンド

DELETE VLAN PORT (148 ページ)

SHOW VLAN (377 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 (116 ページ)

DESTROY MSTP MSTI (149 ページ)

SHOW MSTP (295 ページ)

SHOW MSTP MSTI (307 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。15 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 (150 ページ)

ENABLE STP (199 ページ)

SET STP (254 ページ)

SHOW STP (335 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] [SELECT={MACSRC|MACDEST|
MACBOTH|IPSRC|IPDEST|IPBOTH}] [SPEED={10M|100M|1000M}]
```

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。6 グループまで作成可能。

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 8。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 に所属してはいなくてはならない。

SELECT トランクからパケットを送信するときの選択基準。この基準にしたがって実際の送信に使うポートを選択する。MACSRC (送信元 MAC アドレス)、MACDEST (宛先 MAC アドレス)、MACBOTH (送信元・宛先 MAC アドレス)、IPSRC (始点 IP アドレス)、IPDEST (終点 IP アドレス)、IPBOTH (始点・終点 IP アドレス) から選択する。デフォルトは MACBOTH。

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。デフォルトは 100M。

例

トランクグループ「uplink」を作成する。通信速度は 100M とする。

```
CREATE SWITCH TRUNK=uplink SPEED=100M
```

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、SELECT パラメーターの設定とは関係なく、常に終点 IP アドレス (IPDEST) に基づいて決定される (負荷分散される)。

フラッドパケットは、トランクグループ内で一番最初にリンクが確立されたポートから送出される。

関連コマンド

ADD SWITCH TRUNK (131 ページ)
DELETE SWITCH TRUNK (147 ページ)
DESTROY SWITCH TRUNK (151 ページ)
SET SWITCH TRUNK (276 ページ)
SHOW SWITCH TRUNK (375 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 [{PROTECTED|PRIVATE}]

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)

解説

VLAN を作成する。

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。

PROTECTED 所属ポート間のレイヤー 2 通信を禁止するときに指定するオプション (Protected VLAN)。レイヤー 3 通信は可能。本オプション付きで VLAN を作成した場合、所属ポートは必ずタグなし (Untagged) に設定すること。タグ付き (Tagged) に設定してはならない。また、本オプション付きで作成した VLAN 内では、IGMP Snooping を使用できない。PRIVATE オプション (マルチプル VLAN) との併用は不可。

PRIVATE マルチプル VLAN (Private VLAN) を作成するときに指定する。PROTECTED オプションとの併用は不可。

例

VLAN orange (VLAN ID=20) を作成する。

```
CREATE VLAN=orange VID=20
```

備考・注意事項

VLAN は 254 個 (VLAN default を除く) まで新規作成できるが、IP アドレスを設定できるのは 32 個の VLAN まで。

関連コマンド

ADD VLAN PORT (132 ページ)

DESTROY VLAN (152 ページ)

SHOW VLAN (377 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 (112 ページ)

SHOW DHCP Snooping DATABASE (282 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 (114 ページ)

SET LACP PORT (230 ページ)

SHOW LACP PORT (289 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 (116 ページ)

SHOW MSTP (295 ページ)

SHOW MSTP MSTI (307 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。大文字小文字を区別しない)

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 (117 ページ)

SHOW STP (335 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。カンマ、ハイフン区切りで複数指定が可能)

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。カンマ、ハイフン区切りで複数指定が可能。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 (119 ページ)

SHOW SWITCH FILTER (354 ページ)

DELETE SWITCH L3FILTER

カテゴリー：スイッチング / ハードウェア IP フィルター

DELETE SWITCH L3FILTER=*filter-id*

filter-id: フィルター番号 (1~14)

解説

ハードウェア IP フィルターを削除する。

該当フィルターにエントリーが登録されている場合は削除できない。その場合は、DELETE SWITCH L3FILTER ENTRY コマンドですべてのエントリーを削除してから本コマンドを実行する。

フィルター番号は可変なので、必ず SHOW SWITCH L3FILTER 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、後続のフィルター（削除したフィルターより番号が大きいもの）の番号が1つずつ前にずれるので注意。

パラメーター

L3FILTER フィルター番号。この番号は可変なので、必ず SHOW SWITCH L3FILTER コマンドで確認してから指定すること

関連コマンド

ADD SWITCH L3FILTER MATCH (127 ページ)

SET SWITCH L3FILTER MATCH (265 ページ)

SHOW SWITCH L3FILTER (356 ページ)

DELETE SWITCH L3FILTER ENTRY

カテゴリー：スイッチング / ハードウェア IP フィルター

DELETE SWITCH L3FILTER=*filter-id* **ENTRY=***entry-id*

filter-id: フィルター番号 (1～14)

entry-id: エントリー番号 (1～124)

解説

ハードウェア IP フィルターから指定したフィルターエントリーを削除する。

フィルター番号、エントリー番号は可変なので、必ず SHOW SWITCH L3FILTER コマンドで確認してから指定すること。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

L3FILTER フィルター番号。この番号は可変なので、必ず SHOW SWITCH L3FILTER コマンドで確認してから指定すること

ENTRY エントリー番号。この番号は可変なので、必ず SHOW SWITCH L3FILTER コマンドに ENTRY オプションを付けて実行し、希望のエントリーを確認してから指定すること。

関連コマンド

ADD SWITCH L3FILTER ENTRY (121 ページ)

SET SWITCH L3FILTER ENTRY (260 ページ)

SHOW SWITCH L3FILTER (356 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 (131 ページ)

CREATE SWITCH TRUNK (136 ページ)

DESTROY SWITCH TRUNK (151 ページ)

SET SWITCH TRUNK (276 ページ)

SHOW SWITCH TRUNK (375 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={*vlanname*|1..4094} **PORT**={*port-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

VLAN からポートを削除する。

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。

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。

例

VLAN orange からポート 1 を削除する。

```
DELETE VLAN=orange PORT=1
```

備考・注意事項

ポートは必ずいずれかの VLAN に所属していなくてはならない。そのため、削除するとポートがどの VLAN にも所属しなくなるような指定をすると、本コマンドはエラーになる。

マルチプル VLAN (Private VLAN) のプライベートポートは、グループ単位で削除しなくてはならない。たとえば、ポート 1~8 が同一グループの場合、DELETE VLAN=somevlan PORT=1-8 のように指定すること。

関連コマンド

ADD VLAN PORT (132 ページ)

SHOW VLAN (377 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 (134 ページ)

DELETE MSTP MSTI VLAN (142 ページ)

SHOW MSTP (295 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 (135 ページ)

DISABLE STP (166 ページ)

ENABLE STP (199 ページ)

SET STP (254 ページ)

SHOW STP (335 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 (131 ページ)

CREATE SWITCH TRUNK (136 ページ)

DELETE SWITCH TRUNK (147 ページ)

SET SWITCH TRUNK (276 ページ)

SHOW SWITCH TRUNK (375 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。ただし、「default」は指定できない。大文字小文字を区別しない)

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 VLAN や、他のソフトウェアモジュールとバインドされている VLAN (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。ALL を指定した場合は、VLAN default を除くすべての VLAN が削除される。VLAN default は削除できない。

関連コマンド

CREATE VLAN (138 ページ)

SHOW VLAN (377 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 (181 ページ)

SHOW DHCP Snooping (278 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 (181 ページ)

ENABLE DHCP Snooping ARPSECURITY (182 ページ)

SHOW DHCP Snooping (278 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 (181 ページ)

ENABLE DHCP Snooping ARPSECURITY (182 ページ)

ENABLE DHCP Snooping LOG (183 ページ)

SHOW DHCP Snooping (278 ページ)

SHOW LOG (「運用・管理」の 384 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（181 ページ）

ENABLE DHCP Snooping OPTION82（184 ページ）

SHOW DHCP Snooping（278 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 (185 ページ)

SHOW LACP (288 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 (186 ページ)

SHOW LACP (288 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 (187 ページ)

ENABLE STP (199 ページ)

SHOW MSTP (295 ページ)

DISABLE 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)

DISABLE 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

指定ポートにおいて、CIST (Common and Internal Spanning Tree) に対するマルチプルスパニングツリープロトコル (MSTP) の動作を無効にする。CIST においては、デフォルトですべてのポートで MSTP の動作が有効化されている。

無効にしたポートはディスカードイング状態となり、同ポートではフレームが転送されなくなる。

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ポートが対象となる。

関連コマンド

DISABLE MSTP MSTI PORT (162 ページ)

ENABLE MSTP CIST PORT (188 ページ)

SHOW MSTP CIST (298 ページ)

SHOW MSTP CIST PORT (301 ページ)

DISABLE MSTP DEBUG 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)

DISABLE MSTP DEBUG={MSG|PKT|STATE|ALL} **MSTI**={CIST|*instance*|ALL}
 [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

マルチプルスパニングツリープロトコル (MSTP) のデバッグオプションを無効にする。デフォルトはすべて無効。

パラメーター

DEBUG 無効にするデバッグオプション。MSG (BPDU をデコードして表示)、PKT (BPDU 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。

MSTI デバッグオプション無効化対象の MST インスタンス。ユーザー作成の MST インスタンスの場合は MST インスタンス ID を、CIST (Common and Internal Spanning Tree) の場合はキーワード CIST を指定する。ALL を指定した場合は、すべての MST インスタンスが対象となる。

PORT デバッグオプション無効化対象のポート。

関連コマンド

SHOW MSTP DEBUG MSTI (306 ページ)

SHOW MSTP MSTI (307 ページ)

SHOW MSTP MSTI PORT (310 ページ)

DISABLE 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)

DISABLE 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

指定ポートにおいて、指定した MST インスタンスに対するマルチプルスパニングツリープロトコル (MSTP) の動作を無効にする。各 MST インスタンスにおいては、デフォルトですべてのポートで MSTP の動作が有効化されている。

無効にしたポートはディスカードイング状態となり、同ポートではフレームが転送されなくなる。

パラメーター

MSTI MSI 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。

関連コマンド

DISABLE MSTP CIST PORT (160 ページ)

ENABLE MSTP MSTI PORT (191 ページ)

SHOW MSTP MSTI (307 ページ)

SHOW MSTP MSTI PORT (310 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（165 ページ）

ENABLE PORTAUTH（192 ページ）

ENABLE PORTAUTH PORT（194 ページ）

SHOW PORTAUTH MULTISUPPLICANT PORT（319 ページ）

SHOW PORTAUTH PORT（323 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) \ 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。

関連コマンド

ENABLE PORTAUTH (192 ページ)

ENABLE PORTAUTH DEBUG (193 ページ)

ENABLE PORTAUTH PORT (194 ページ)

SHOW PORTAUTH PORT (323 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 (163 ページ)

ENABLE PORTAUTH (192 ページ)

ENABLE PORTAUTH PORT (194 ページ)

SHOW PORTAUTH PORT (323 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 (135 ページ)
DESTROY STP (150 ページ)
ENABLE STP (199 ページ)
SET STP (254 ページ)
SHOW STP (335 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 (BPDU をデコードして表示)、PKT (BPDU 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 (169 ページ)

ENABLE STP DEBUG (200 ページ)

SHOW STP DEBUG (341 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 BPDU 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 (201 ページ)

SET STP PORT (256 ページ)

SHOW STP PORT (343 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 (BPDU をデコードして表示)、PKT (BPDU 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 (167 ページ)

ENABLE STP DEBUG (200 ページ)

ENABLE STP PORT DEBUG (202 ページ)

SHOW STP DEBUG (341 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 (203 ページ)

SET SWITCH AGEINGTIMER (258 ページ)

SHOW SWITCH (346 ページ)

DISABLE SWITCH DEBUG

カテゴリー：スイッチング / 一般コマンド

DISABLE SWITCH DEBUG={ARL|CMIC|DMA|QOS|S5600|PHY|ALL}

解説

スイッチングモジュールのデバッグオプションを無効にする。

パラメーター

DEBUG デバッグオプション。ARL (FDB)、CMIC (CMIC レイヤー)、DMA (ダイレクトメモリーアクセス)、QOS (QoS)、S5600 (Broadcom チップ)、PHY (PHY)、ALL (すべて) から選択する。

関連コマンド

ENABLE SWITCH DEBUG (204 ページ)

SHOW SWITCH (346 ページ)

DISABLE SWITCH FILTER VLANSECURE

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 FILTER VLANSECURE

解説

FDB スタティックエントリ（スイッチフィルター）が、ルーティングパケットと本体宛てパケットには適用されないようにする。デフォルトは適用される。

本コマンドを実行すると、ACTION=FORWARD のスイッチフィルターは VLAN 内のスイッチングパケットにだけ適用され、スイッチ本体や他 VLAN 宛てのパケットには適用されなくなる。

説明のため、次のスイッチフィルターが設定されていると仮定する。

ADD SWITCH FILTER DESTADDRESS=00-00-00-00-00-01 PORT=13 ACTION=FORWARD

ENABLE SWITCH FILTER VLANSECURE（デフォルト）時、00-00-00-00-00-01 は、

- ・ポート 13 に接続されているときは、同一 VLAN の他ポート、他 VLAN、スイッチ本体のいずれとも通信可能

- ・ポート 13 以外に接続されているときは、他ポートとの通信は一切不可となる。

一方、DISABLE SWITCH FILTER VLANSECURE（本コマンド実行）時、00-00-00-00-00-01 は、

- ・ポート 13 に接続されているときは、同一 VLAN の他ポート、他 VLAN、スイッチ本体のいずれとも通信可能

- ・ポート 13 以外に接続されているときは、同一 VLAN の他ポートとは通信できないが、他 VLAN、スイッチ本体とは通信可能となる。

備考・注意事項

本コマンドは 8724SL のみサポート。8748SL では使用できないので注意。

本コマンドの影響を受けるのは、ACTION=FORWARD のスイッチフィルターだけ。ACTION=DISCARD の動作には影響を与えない。

関連コマンド

ADD SWITCH FILTER（119 ページ）

ENABLE SWITCH FILTER VLANSECURE（205 ページ）

SHOW SWITCH FILTER（354 ページ）

DISABLE SWITCH L3FILTER

カテゴリー：スイッチング / ハードウェア IP フィルター

DISABLE SWITCH L3FILTER

解説

ハードウェア IP フィルター（L3 フィルター）機能を無効にする。デフォルトは有効（デフォルト有効の IGMP Snooping がハードウェア IP フィルターを内部的に使用しているため）。

関連コマンド

ENABLE SWITCH L3FILTER（206 ページ）

SHOW SWITCH L3FILTER（356 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（207 ページ）

SHOW SWITCH（346 ページ）

DISABLE SWITCH LOOPDETECTION

カテゴリー：スイッチング / ポート

DISABLE SWITCH LOOPDETECTION=LDF [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でループガード (LDF 検出) 機能を無効にする。デフォルトは無効。

パラメーター

LOOPDETECTION ループ検出方式。LDF (LDF 検出) しかサポートしていないが省略はできない。

PORT ポート番号。省略時および ALL 指定時はすべてのポートが対象となる。

関連コマンド

ENABLE SWITCH LOOPDETECTION (208 ページ)

SET SWITCH LOOPDETECTION (268 ページ)

SHOW SWITCH LOOPDETECTION (360 ページ)

SHOW SWITCH LOOPDETECTION COUNTER (363 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 (210 ページ)

SET SWITCH MIRROR (270 ページ)

SET SWITCH PORT (271 ページ)

SHOW SWITCH (346 ページ)

SHOW SWITCH PORT (365 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 (10/100Mbps 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 (211 ページ)

SHOW SWITCH PORT (365 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。デフォルトは有効。

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。本製品が PAUSE フレームを送信することはない。

関連コマンド

ENABLE SWITCH PORT FLOW (212 ページ)

SHOW SWITCH PORT (365 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 (213 ページ)

SHOW SWITCH (346 ページ)

DISABLE VLAN DEBUG

カテゴリー：スイッチング / バーチャル LAN

DISABLE VLAN={*vlanname*|1..4094|ALL} **DEBUG**={PKT|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。大文字小文字を区別しない)

解説

VLAN のデバッグオプションを無効にする。デフォルトはすべて無効。

パラメーター

VLAN VLAN 名または VLAN ID

DEBUG デバッグオプション。PKT (パケットを ASCII 表示)、ALL (すべてのデバッグ) から選択する。

関連コマンド

ENABLE VLAN DEBUG (214 ページ)

SHOW VLAN DEBUG (381 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 (153 ページ)

SHOW DHCP Snooping (278 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 (112 ページ)

DISABLE DHCP Snooping (153 ページ)

DISABLE DHCP Snooping ARPSECURITY (154 ページ)

ENABLE DHCP Snooping LOG (183 ページ)

SHOW DHCP Snooping (278 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

DISABLE DHCP Snooping LOG (155 ページ)

ENABLE DHCP Snooping (181 ページ)

ENABLE DHCP Snooping ARPSECURITY (182 ページ)

SHOW DHCP Snooping (278 ページ)

SHOW LOG (「運用・管理」の 384 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 (153 ページ)

DISABLE DHCP Snooping OPTION82 (156 ページ)

SHOW DHCP Snooping (278 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 (114 ページ)

DELETE LACP PORT (141 ページ)

DISABLE LACP (157 ページ)

SHOW LACP (288 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 (158 ページ)

SHOW LACP (288 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。

下記のコマンドを実行するには、あらかじめ本コマンドで MSTP を有効化しておく必要がある。

- ・ ENABLE MSTP CIST PORT コマンド
- ・ DISABLE MSTP CIST PORT コマンド
- ・ ENABLE MSTP MSTI PORT コマンド
- ・ DISABLE MSTP MSTI PORT コマンド

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。

関連コマンド

DISABLE MSTP (159 ページ)

DISABLE STP (166 ページ)

SHOW MSTP (295 ページ)

ENABLE 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)

ENABLE 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

指定ポートにおいて、CIST (Common and Internal Spanning Tree) に対するマルチプルスパニングツリープロトコル (MSTP) の動作を有効にする。CIST においては、デフォルトですべてのポートで MSTP の動作が有効化されている。

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。トランクグループの場合は、マスターポート (トランクグループ内で最初にリンクアップしたポート) を指定する必要がある。

関連コマンド

SHOW MSTP CIST (298 ページ)

SHOW MSTP CIST PORT (301 ページ)

ENABLE MSTP DEBUG 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)

```
ENABLE MSTP DEBUG={MSG|PKT|STATE|ALL} MSTI={CIST|instance|ALL}
[PORT={port-list|ALL}] [STATEMACHINE={PTM|PRX|PPM|PIM|PTX|PRS|PRT|PST|
TCM|ALL}] [OUTPUT={CONSOLE}] [TIMEOUT={1..400000000|NONE}]
```

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

マルチプルスパニングツリープロトコル (MSTP) のデバッグオプションを有効にする。デフォルトはすべて無効。

パラメーター

DEBUG 有効にするデバッグオプション。MSG (BPDU をデコードして表示)、PKT (BPDU を ASCII 表示)、STATE (ポートの状態遷移を表示。STATEMACHINE パラメーターを使えば、表示する情報をより詳しく指定できる)、ALL (すべてのオプション) から選択する。

MSTI デバッグオプション有効化対象の MST インスタンス。ユーザー作成の MST インスタンスの場合は MST インスタンス ID を、CIST (Common and Internal Spanning Tree) の場合はキーワード CIST を指定する。ALL を指定した場合は、すべての MST インスタンスが対象となる。

PORT デバッグオプション有効化対象のポート。

STATEMACHINE DEBUG パラメーターでデバッグオプション STATE を指定したとき、どの状態機械の遷移情報を表示させるかを指定する。詳細は別表を参照。省略時は ALL。

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)。

オプション	説明
PTM	Port timer state machine
PRX	Port receive state machine
PPM	Port protocol migration state machine
PIM	Port information state machine
PTX	Port transmit state machine
PRS	Port role selection state machine
PRT	Port role transitions state machine
PST	Port state transition state machine

TCM	Topology change state machine
ALL	上記すべて

表 30: STATEMACHINE パラメーターのオプション

関連コマンド

DISABLE MSTP DEBUG MSTI (161 ページ)

SHOW MSTP DEBUG MSTI (306 ページ)

ENABLE 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)

ENABLE 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

指定ポートにおいて、指定した MST インスタンスに対するマルチプルスパニングツリープロトコル (MSTP) の動作を有効にする。各 MST インスタンスにおいては、デフォルトですべてのポートで MSTP の動作が有効化されている。

パラメーター

MSTI MSI 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。トランクグループの場合は、マスターポート (トランクグループ内で最初にリンクアップしたポート) を指定する必要がある。

関連コマンド

SHOW MSTP MSTI (307 ページ)

SHOW MSTP MSTI PORT (310 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（163 ページ）
DISABLE PORTAUTH PORT（165 ページ）
ENABLE PORTAUTH PORT（194 ページ）
SHOW PORTAUTH MULTISUPPLICANT PORT（319 ページ）
SHOW PORTAUTH PORT（323 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 (164 ページ)

ENABLE PORTAUTH (192 ページ)

ENABLE PORTAUTH PORT (194 ページ)

SHOW PORTAUTH PORT (323 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}] [AUTOAUTHENTICATE={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)

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。

AUTOAUTHENTICATE (MAC ベース認証ポート) 指定スイッチポートをクリティカルポートとして設定するかどうか。登録済みの RADIUS サーバーがすべて無応答だった場合、通常のポートでは認証失敗となるが、クリティカルポートでは認証成功となる。デフォルトは FALSE (通常のポート)。

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。

AUTOAUTHENTICATE パラメーターの説明における「RADIUS サーバーがすべて無応答」とは、認証期間中にすべての RADIUS サーバーが Dead (使用抑制) 状態になることを意味する。そのため、クリティカルポートを使用する場合は、RADIUS クライアントの動作パラメーターである「DEADTIME」を 1 以上に設定すること。同パラメーターの初期値「0」のままでは、RADIUS サーバーの状態が「Dead」にならないため、クリティカルポートは動作しないので注意。なお、DEADTIME パラメーターの設定は、SET RADIUS コマンドで行う。

クリティカルポートでダイナミック VLAN を使用している場合、RADIUS サーバーが無応答のとき、Supplicant は該当ポート本来の VLAN 所属となる。

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (109 ページ)

ENABLE PORTAUTH (192 ページ)

SET PORTAUTH PORT (241 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (245 ページ)

SHOW PORTAUTH (312 ページ)

SHOW PORTAUTH COUNTER (316 ページ)

SHOW PORTAUTH MULTISUPPLICANT PORT (319 ページ)

SHOW PORTAUTH PORT (323 ページ)

SHOW PORTAUTH TIMER (329 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。

マルチプルスパニングツリープロトコル (MSTP) が有効のときは、スパニングツリープロトコル (STP/RSTP) を有効化できないので、あらかじめ DISABLE MSTP コマンドを実行して MSTP を無効化しておくこと。

パラメーター

STP STP ドメイン名。

関連コマンド

CREATE STP (135 ページ)

DESTROY STP (150 ページ)

DISABLE MSTP (159 ページ)

DISABLE STP (166 ページ)

SET STP (254 ページ)

SHOW STP (335 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 (BPDU をデコードして表示)、PKT (BPDU 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 (167 ページ)

SHOW STP DEBUG (341 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 (168 ページ)

SET STP PORT (256 ページ)

SHOW STP PORT (343 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..400000000|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 (BPDU をデコードして表示) PKT (BPDU 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 (167 ページ)

DISABLE STP PORT DEBUG (169 ページ)

ENABLE STP (199 ページ)

SHOW STP DEBUG (341 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 (170 ページ)

SET SWITCH AGEINGTIMER (258 ページ)

SHOW SWITCH (346 ページ)

ENABLE SWITCH DEBUG

カテゴリー：スイッチング / 一般コマンド

```
ENABLE SWITCH DEBUG={ARL|CMIC|DMA|QOS|S5600|PHY|ALL} [OUTPUT=CONSOLE]
[TIMEOUT={1..4000000000|NONE}]
```

解説

スイッチングモジュール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

DEBUG デバッグオプション。ARL（FDB）、CMIC（CMIC レイヤー）、DMA（ダイレクトメモリアクセス）、QOS（QoS）、S5600（Broadcom チップ）、PHY（PHY）、ALL（すべて）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。

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 SWITCH DEBUG（171 ページ）

SHOW SWITCH（346 ページ）

ENABLE SWITCH FILTER VLANSECURE

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 FILTER VLANSECURE

解説

FDB スタティックエントリー（スイッチフィルター）が、ルーティングパケットと本体宛てパケットにも適用されるよう設定する。デフォルトは適用される。

備考・注意事項

本コマンドは 8724SL のみサポート。

関連コマンド

ADD SWITCH FILTER (119 ページ)

DISABLE SWITCH FILTER VLANSECURE (172 ページ)

SHOW SWITCH FILTER (354 ページ)

ENABLE SWITCH L3FILTER

カテゴリー：スイッチング / ハードウェア IP フィルター

ENABLE SWITCH L3FILTER

解説

ハードウェア IP フィルター（L3 フィルター）機能を有効にする。デフォルトは有効（デフォルト有効の IGMP Snooping がハードウェア IP フィルターを内部的に使用しているため）。

関連コマンド

DISABLE SWITCH L3FILTER（173 ページ）

SHOW SWITCH L3FILTER（356 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（174 ページ）

SHOW SWITCH（346 ページ）

ENABLE SWITCH LOOPDETECTION

カテゴリー：スイッチング / ポート

ENABLE SWITCH LOOPDETECTION=LDF [PORT={*port-list*|ALL}] [ACTION={NONE|
DISABLEPORT|LINKDOWN}]

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ループガード (LDF 検出) 機能を有効にする。デフォルトは無効。

パラメーター

LOOPDETECTION ループ検出方式。LDF (LDF 検出) しかサポートしていないが省略はできない。

PORT ポート番号。省略時および ALL 指定時はすべてのポートが対象となる。

ACTION ループを検出した場合の動作 (アクション)。NONE (ループ検出時のログ記録のみ)、DISABLEPORT (ポートをディセーブルにする。また、ループ検出時と動作実行時にログを記録する)、LINKDOWN (ポートを物理的にリンクダウンさせる。また、ループ検出時と動作実行時にログを記録する) から選択する。これらの動作は、SET SWITCH LOOPDETECTION コマンドの PDTO パラメーターで指定した時間が経過すると自動的にアクション実行前の状態に戻る。また、自動復帰前であっても、ENABLE SWITCH PORT コマンドを用いて任意の時点でアクション実行前の状態に戻すことができる。デフォルトは NONE。

備考・注意事項

- ・ ACTION パラメーターの指定値は、PORT パラメーターの指定値にかかわらずシステム全体 (すべてのポート) に適用される (ループ検出時の動作はシステム全体で 1 つしか設定できないため)。
- ・ ループ検出後のアクションの副次的な作用として、アクションが実行されるときと実行前の状態に戻るときに SNMP のリンクトラップが出力される。
- ・ スイッチポート単位で設定する機能のうち、同一ポート上で LDF 検出と併用できるのは次の機能のみ。なお、これら併用可能な機能にも注意事項がある。詳細は「スイッチング」/「ポート」の解説編を参照。
- ポートランキング・LACP
- タグ VLAN
- スパニングツリープロトコル (STP/RSTP)
- ポート認証 (802.1X 認証、MAC ベース認証)

関連コマンド

DISABLE SWITCH LOOPDETECTION (175 ページ)

ENABLE SWITCH PORT (211 ページ)

SET SWITCH LOOPDETECTION (268 ページ)

SHOW SWITCH LOOPDETECTION (360 ページ)

SHOW SWITCH LOOPDETECTION COUNTER (363 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 (176 ページ)

SET SWITCH MIRROR (270 ページ)

SET SWITCH PORT (271 ページ)

SHOW SWITCH (346 ページ)

SHOW SWITCH PORT (365 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 (177 ページ)

SHOW SWITCH PORT (365 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。デフォルトは有効。

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。本製品が PAUSE フレームを送信することはない。

関連コマンド

DISABLE SWITCH PORT FLOW (178 ページ)

SHOW SWITCH PORT (365 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 (179 ページ)

SHOW SWITCH (346 ページ)

ENABLE VLAN DEBUG

カテゴリー：スイッチング / バーチャル LAN

```
ENABLE VLAN={vlanname|1..4094|ALL} DEBUG={PKT|ALL} [OUTPUT=CONSOLE]
[TIMEOUT={1..4000000000|NONE}]
```

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)

解説

VLAN のデバッグオプションを有効にする。デフォルトはすべて無効。

パラメーター

VLAN VLAN 名または VLAN ID

DEBUG デバッグオプション。PKT (パケットを ASCII 表示)、ALL (すべてのデバッグ) 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 VLAN DEBUG (180 ページ)

SHOW VLAN DEBUG (381 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 (157 ページ)

SHOW LACP (288 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 (295 ページ)

SHOW MSTP MSTI (307 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、指定ポートのポート認証関連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 (163 ページ)

DISABLE PORTAUTH PORT (165 ページ)

SHOW PORTAUTH PORT (323 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 (224 ページ)

SET STP (254 ページ)

SET STP PORT (256 ページ)

SHOW STP (335 ページ)

SHOW STP COUNTER (339 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 (280 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 (215 ページ)

SHOW LACP (288 ページ)

SHOW LACP PORT (289 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 (304 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 (163 ページ)

DISABLE PORTAUTH PORT (165 ページ)

ENABLE PORTAUTH (192 ページ)

ENABLE PORTAUTH PORT (194 ページ)

SHOW PORTAUTH MULTISUPPLICANT PORT (319 ページ)

SHOW PORTAUTH PORT (323 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-Suppliant 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 Suppliant 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-Suppliant 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 (163 ページ)
DISABLE PORTAUTH PORT (165 ページ)
ENABLE PORTAUTH (192 ページ)
ENABLE PORTAUTH PORT (194 ページ)
SET PORTAUTH PORT SUPPLICANTMAC (245 ページ)
SHOW PORTAUTH MULTISUPPLICANT PORT (319 ページ)
SHOW PORTAUTH PORT (323 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 (218 ページ)

SET STP (254 ページ)

SHOW STP (335 ページ)

SHOW STP COUNTER (339 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等、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 (346 ページ)

SHOW SWITCH FDB (351 ページ)

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。

関連コマンド

DISABLE SWITCH PORT (177 ページ)

ENABLE SWITCH PORT (211 ページ)

SHOW SWITCH PORT (365 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（181 ページ）

SHOW DHCP Snooping（278 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 (112 ページ)

ENABLE DHCP Snooping (181 ページ)

ENABLE DHCP Snooping OPTION82 (184 ページ)

SHOW DHCP Snooping (278 ページ)

SHOW DHCP Snooping Port (286 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 (8 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 (114 ページ)

DELETE LACP PORT (141 ページ)

SHOW LACP PORT (289 ページ)

SET LACP PRIORITY

カテゴリー：スイッチング / LACP (IEEE 802.3ad)

SET LACP PRIORITY=0..65535

解説

LACP のシステムプライオリティーを変更する。

パラメーター

PRIORITY LACP システムプライオリティー。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ーとシステム 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。

関連コマンド

SHOW LACP (288 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 (295 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 (295 ページ)

SHOW MSTP CIST (298 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 31: 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 (298 ページ)

SHOW MSTP CIST PORT (301 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 (295 ページ)

SHOW MSTP MSTI (307 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。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 32: 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 (191 ページ)

SHOW MSTP MSTI (307 ページ)

SET PORTAUTH HYPHEN

カテゴリー：スイッチング / ポート認証

SET PORTAUTH [=MACBASED] **HYPHEN**={ON|OFF|YES|NO}

解説

MAC ベース認証において、RADIUS サーバーに認証を要求するときのユーザー名・パスワードにハイフンを含めるかどうかを設定する。

MAC ベース認証では、Supplicant の MAC アドレスをユーザー名・パスワードとして RADIUS サーバーに送信する。送信する MAC アドレスは、ハイフンを含める場合は「00-00-f4-11-22-33」、含めない場合は「0000f4112233」の形式になる。

パラメーター

PORTAUTH 認証メカニズム。本コマンドでは MACBASED (MAC ベース認証) のみ有効。省略時は MACBASED と見なされるため、特に指定する必要はない。

HYPHEN RADIUS サーバーに送信するユーザー名・パスワードにハイフンを含めるかどうか。ON、YES (含める)、OFF、NO (含めない) から選択する。デフォルトは ON。

関連コマンド

SHOW PORTAUTH (312 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}] [AUTOAUTHENTICATE={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）

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。

AUTOAUTHENTICATE (MAC ベース認証ポート) 指定スイッチポートをクリティカルポートとして設定するかどうか。登録済みの RADIUS サーバーがすべて無応答だった場合、通常のポートでは認証失敗となるが、クリティカルポートでは認証成功となる。デフォルトは FALSE (通常のポート)。

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (109 ページ)

ENABLE PORTAUTH (192 ページ)

ENABLE PORTAUTH PORT (194 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (245 ページ)

SHOW PORTAUTH (312 ページ)

SHOW PORTAUTH COUNTER (316 ページ)

SHOW PORTAUTH MULTISUPPLICANT PORT (319 ページ)

SHOW PORTAUTH PORT (323 ページ)

SHOW PORTAUTH TIMER (329 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-Suppliant 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 Suppliant 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-Suppliant 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 Suppliant 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) Suppliant 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) Suppliant の認証に失敗した後、Suppliant 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 (109 ページ)

ENABLE PORTAUTH (192 ページ)

ENABLE PORTAUTH PORT (194 ページ)

SET PORTAUTH PORT (241 ページ)

SHOW PORTAUTH (312 ページ)

SHOW PORTAUTH COUNTER (316 ページ)

SHOW PORTAUTH MULTISUPPLICANT PORT (319 ページ)

SHOW PORTAUTH PORT (323 ページ)

SHOW PORTAUTH TIMER (329 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 (109 ページ)

ENABLE PORTAUTH (192 ページ)

ENABLE PORTAUTH PORT (194 ページ)
SET PORTAUTH PORT (241 ページ)
SET PORTAUTH PORT SUPPLICANTMAC (245 ページ)
SHOW PORTAUTH (312 ページ)
SHOW PORTAUTH COUNTER (316 ページ)
SHOW PORTAUTH MULTISUPPLICANT PORT (319 ページ)
SHOW PORTAUTH PORT (323 ページ)
SHOW PORTAUTH TIMER (329 ページ)

SET QOS HWPRIORITY

カテゴリー：スイッチング / QoS

SET QOS HWPRIORITY QUEUE=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 (0~3。大きいほど優先度が高い)

解説

QoS (Quality of Service) 機能の設定を変更する。
具体的には、プライオリティータグフレームの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。

パラメーター

QUEUE ユーザープライオリティー 0~7 に対応するプライオリティーキューの番号をカンマで区切って指定する。キューはポートごとに 0~3 の 4 つがあり、3 がもっとも優先度が高い。フレーム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る。すなわち、上位のキューに 1 つでもフレームが格納されている場合、それより下位のキューからはフレームは送信されない。タグなしフレームは、宛先 MAC アドレスが本製品ならユーザープライオリティー 4、宛先 MAC アドレスが本製品以外ならユーザープライオリティー 0 と見なされる。p0 から p7 まですべての値を指定すること。デフォルトは別表を参照。

ユーザープライオリティー	キュー番号 (大きいほど優先度が高い)
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

表 33: ユーザープライオリティー値-プライオリティーキューのデフォルトマッピング

例

ユーザープライオリティー 0~7 に対し、送信キュー 0, 0, 0, 1, 1, 2, 2, 3 を割り当てる。

SET QOS HWPRIORITY QUEUE=0,0,0,1,1,2,2,3

関連コマンド

SHOW QOS HWPRIORITY (333 ページ)

SET QOS HWQUEUE

カテゴリー：スイッチング / QoS

```
SET QOS HWQUEUE=queue [MAXPACKETS={NONE|0|1..255}] [MAXLATENCY={NONE|0|16..4080}]
```

queue: 送信キュー（0～3。大きいほど優先度が高い）

解説

送信キューごとに、最大送信パケット数と最大送信遅延時間を設定する。

フレームのユーザプライオリティに対して送信キューの優先度を設定するだけでは、高いレベルのパケットが優先的に処理されてしまい、低いレベルのパケットは処理されない。低いレベルのパケットにも処理の順番を回すための設定。最大送信パケット数と最大送信遅延時間を同時に設定することは可能。

パラメーター

HWQUEUE 送信キュー番号を 0～3 で指定する。大きいほど優先度が高い。

MAXPACKETS 送信キューごとの最大送信パケット数を、1～255 の範囲で指定する。当該キューが空もしくは指定パケット数まで送信すると、次レベルの送信キューに処理が移る。0 または NONE で設定が無効となり、当該キューが空になるまで送信する。デフォルトは NONE。

MAXLATENCY 送信キューごとの最大送信遅延時間を、16～4080（単位は、マイクロ秒）の範囲で指定する。当該キューにキューイングされてから送出されるまでの遅延時間を保証する。高レベルのキューが送信中であっても、本指定時間を経過すると、強制的に当該キューのパケットを送出する。0 または NONE で設定が無効となり、遅延時間は保証されない。デフォルトは NONE。

例

プライオリティキュー 3 に対し、最大送信パケット数 255 を指定する。

```
SET QOS HWQUEUE=3 MAXPACKETS=255
```

備考・注意事項

ここでいうパケットとは、実際のパケット数ではなく、処理上の単位を表す。

8748SL において、MAXPACKETS、または、MAXLATENCY の設定を行った場合、ポートグループ「1～24、50」と「25～48、49」をまたぐパケットに対して QoS が機能しないので注意。

関連コマンド

SHOW QOS HWQUEUE (334 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 (218 ページ)

RESET STP (224 ページ)

SET STP PORT (256 ページ)

SHOW STP (335 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 34: 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 35: 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 (218 ページ)

RESET STP (224 ページ)

SET STP (254 ページ)

SHOW STP (335 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..1000000

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。デフォルトは 300 秒。

関連コマンド

DISABLE SWITCH AGEINGTIMER (170 ページ)

ENABLE SWITCH AGEINGTIMER (203 ページ)

SHOW SWITCH (346 ページ)

SET SWITCH L3AGEINGTIMER

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 L3AGEINGTIMER=30..43200

解説

L3 テーブルのエージングタイムを変更する。

パラメーター

L3AGEINGTIMER エージングタイム。デフォルトは 900 秒。

関連コマンド

SHOW SWITCH (346 ページ)

SET SWITCH L3FILTER ENTRY

カテゴリー：スイッチング / ハードウェア IP フィルター

```
SET SWITCH L3FILTER=filter-id ENTRY=entry-id [TOS=0..7] [IPDSCP=0..63]
[TTL=0..255] [PROTOCOL={TCP|UDP|ICMP|IGMP|protocol}] [SIPADDR=ipadd]
[DIPADDR=ipadd] [TCPSPORT={port|port-name}] [TCPDPORT={port|port-name}]
[TCP SYN={TRUE|FALSE}] [TCPACK={TRUE|FALSE}] [TCPFIN={TRUE|FALSE}]
[TYPE=protocoltype] [UDPSPORT={port|port-name}] [UDPDPOR={port|
port-name}] [I PORT=port-number] [E PORT=port-number] [PRIORITY=0..7]
[P ORT=port-number] [NEWTOS=0..7] [NEWIPDSCP=0..63] [ACTION={SETPRIORITY|
SENDCOS|SETTOS|DENY|SENDEPORT|SENDMIRROR|MOVEPRIOTOTOS|MOVETOSTOPRIO|
NODROP|SENDNONUNICASTTOPORT|SETIPDSCP}[ , ... ]]
```

filter-id: フィルター番号 (1~14)

entry-id: エントリー番号 (1~124)

protocol: IP プロトコル番号 (0~255)

ipadd: IP アドレス

port: TCP/UDP ポート番号 (0~65535)

port-name: サービス名

protocoltype: L3 プロトコル番号 (16 進数)

port-number: スイッチポート番号 (1~)

解説

ハードウェア IP フィルターのフィルターエントリー（フィルタリング条件およびマッチ時のアクション）を変更する。

フィルタリングに使用するパケットフィールドの変更は、SET SWITCH L3FILTER MATCH コマンドで行う。

パラメーター

L3FILTER フィルター番号。この番号は可変なので、必ず SHOW SWITCH L3FILTER コマンドで確認してから指定すること

ENTRY エントリー番号。この番号は可変なので、必ず SHOW SWITCH L3FILTER コマンドに ENTRY パラメーターを付けて実行し、希望のエントリーを確認してから指定すること

TOS （フィルタリング条件）対象パケットの IP TOS 優先度（TOS オクテットの 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。

IPDSCP （フィルタリング条件）対象パケットの IP DSCP（DiffServ Code Point）フィールド値。有効範囲は 0~63。TOS とは同時に指定できない。

TTL （フィルタリング条件）対象パケットの IP TTL（生存時間）フィールド値。有効範囲は 0~255。

PROTOCOL （フィルタリング条件）対象パケットの IP プロトコルフィールド値。TCP、UDP、ICMP、IGMP については名前でも指定できる。その他プロトコルの場合は IP プロトコル番号で指定する。

- SIPADDR** (フィルタリング条件) 対象パケットの始点 IP アドレス。パケットマッチング時には、ここで指定したアドレスに対して ADD SWITCH L3FILTER MATCH コマンドの SCLASS パラメーターで指定したマスクが適用される。ハードウェア IP フィルターはルーティングされない同一 IP ネットワーク内のトラフィックに対しても有効。
- DIPADDR** (フィルタリング条件) 対象パケットの終点 IP アドレス。パケットマッチング時には、ここで指定したアドレスに対して ADD SWITCH L3FILTER MATCH コマンドの DCLASS パラメーターで指定したマスクが適用される。ハードウェア IP フィルターはルーティングされない同一 IP ネットワーク内のトラフィックに対しても有効。
- TCPSPORT** (フィルタリング条件) 対象パケットの TCP 始点ポート。ポート番号かサービス名で指定する。PROTOCOL パラメーターに TCP を指定したときのみ有効。
- TCPDPORT** (フィルタリング条件) 対象パケットの TCP 終点ポート。ポート番号かサービス名で指定する。PROTOCOL パラメーターに TCP を指定したときのみ有効。
- TCPSYN** (フィルタリング条件) 対象パケットの TCP 制御フラグ「Syn」の値 (オン・オフ)。TRUE はフラグが立っていることを、FALSE はフラグが立っていないことを示す。PROTOCOL パラメーターに TCP を指定したときのみ有効。また、EPORT パラメーターとは併用しないこと。
- TCPACK** (フィルタリング条件) 対象パケットの TCP 制御フラグ「Ack」の値 (オン・オフ)。TRUE はフラグが立っていることを、FALSE はフラグが立っていないことを示す。PROTOCOL パラメーターに TCP を指定したときのみ有効。また、EPORT パラメーターとは併用しないこと。
- TCPFIN** (フィルタリング条件) 対象パケットの TCP 制御フラグ「Fin」の値 (オン・オフ)。TRUE はフラグが立っていることを、FALSE はフラグが立っていないことを示す。PROTOCOL パラメーターに TCP を指定したときのみ有効。また、EPORT パラメーターとは併用しないこと。
- TYPE** (フィルタリング条件) 対象パケット (フレーム) のレイヤー 3 プロトコルタイプフィールド値 (16 進数)。本パラメーターを指定した場合、他のフィルタリング条件パラメーターは無効となる。また、ACTION に SETTOS を指定することはできない。プロトコル番号は、ADD SWITCH L3FILTER MATCH コマンドの TYPE パラメーターで指定したフレームフォーマットにおけるものを指定すること。Ethernet Version 2 と 802.2 LLC(DSAP, SSAP) におけるプロトコルタイプは 2 バイト、SNAP のプロトコルタイプは 5 バイト長で指定する。
- UDPSPORT** (フィルタリング条件) 対象パケットの UDP 始点ポート。ポート番号かサービス名で指定する。PROTOCOL パラメーターに UDP を指定したときのみ有効。
- UDPDPOR** (フィルタリング条件) 対象パケットの UDP 終点ポート。ポート番号かサービス名で指定する。PROTOCOL パラメーターに UDP を指定したときのみ有効。
- IPO** (フィルタリング条件) 対象パケットの入力スイッチポート。指定ポートから入力されたパケットだけがフィルタリングの対象となる。ADD SWITCH L3FILTER MATCH コマンドで IMPORT=TRUE を指定した場合にのみ有効。
- EPO** (フィルタリング条件) 対象パケットの出力スイッチポート。指定ポートから出力されるパケットだけがフィルタリングの対象となる。ADD SWITCH L3FILTER MATCH コマンドで EIMPORT=TRUE を指定した場合にのみ有効。ただし、EPORT パラメーターを指定した場合は、FDB か L3 テーブルに登録されていない MAC アドレス (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) 宛てのパケットにはフィルターが適用されなくなるので注意すること。
- PRIORITY** (アクションパラメーター) 対象パケットに適用する 802.1p ユーザープライオリティ (0 ~ 7) 値。ACTION パラメーターに SETPRIORITY か SENDCOS を指定したときのみ有効。ACTION に SETPRIORITY を指定したときは、パケットのユーザープライオリティフィールドに PRIORITY

パラメーターで指定した値を書き込んで送出する（出力スイッチポートがタグ付きでないという意味を持たない）。ACTION に SENDCOS を指定したときは、パケットを PRIORITY パラメーターで指定したユーザープライオリティーに対応する送信キューに入れる。省略時は 0。

PORT （アクションパラメーター）対象パケットを出力するスイッチポート。ACTION パラメーターに SENDEPORT か SENDNONUNICASTTOPORT を指定したときのみに有効。このとき、本パラメーターで指定するポート（出力ポート）と入力ポートが同一 VLAN になるよう注意すること。さらに、8748SL では、入力ポートと本パラメーターで指定する出力ポートが、同一ポートグループ「1～24、50」または「25～48、49」に入っていないくなくてはならないので注意。

NEWTOS （アクションパラメーター）パケット送信時に IP ヘッダーの TOS 優先度フィールドにセットする値。ACTION に SETTOS を指定した場合のみに有効。

NEWIPDSCP （アクションパラメーター）パケット送信時に IP ヘッダーの DSCP フィールドにセットする値。ACTION に SETIPDSCP を指定した場合のみに有効。

ACTION パケットがフィルターの条件に一致したときのアクション。カンマ区切りで複数のアクションを指定できる。別表に示すとおり、アクションはいくつかの「カテゴリー」に分類できる。表 1 で（相互排他）と記されているカテゴリーは、パケットが同一カテゴリー内の複数のアクションにマッチした場合に、最後にマッチしたエントリー、すなわち、フィルター番号・エントリー番号のもっとも大きなエントリーのアクションだけが実行されることを示している。アクションの詳細は別表を参照のこと。

パケットの破棄・通過を制御するアクション（相互排他）	
DENY	パケットを破棄する。マッチしたエントリーの中に DENY アクションが含まれている場合は、NODROP によって打ち消されない限り、通常のポートからパケットが出力されることはない（SENDEPORT、SENDCOS アクションがある場合でもパケットは出力されない）。ただし、ポートミラーリング機能が有効な場合は、ミラーポートからパケットのコピーが出力される（SENDMIRROR アクションも有効）
NODROP	DENY アクションを打ち消し、本来破棄されるべきパケットを出力する。おもに、デフォルト拒否の設定において、一部のパケットだけを許可したい場合に使う
出力ポートを変更するアクション	
SENDEPORT	ユニキャストパケット（ここでは、ブロードキャスト、マルチキャスト、および、未学習のユニキャストを除くパケットのこと）の出力先を 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）と入力ポートが同じ VLAN でなくてはならないので、設定には注意すること。さらに、8748SL では、入力ポートと出力ポート（PORT）が、同一ポートグループ「1～24、50」または「25～48、49」に入っていないくなくてはならないので注意。また、仕様により、本来なら L3 スイッチング（ルーティング）されるはずのパケットは、出力ポート（PORT）のタグ設定（タグ付き・タグなし）にかかわらず、本来のルーティング先の VLAN タグが付いた状態で出力される

SENDNONUNICAST	非ユニキャストパケット（ここでは、ブロードキャスト、マルチキャスト、および、未学習のユニキャストのこと）の出力先を PORT パラメーターで指定されたポートだけに変更する。このとき、出力ポートと入力ポートが同じ VLAN でなくてはならないので、設定には注意すること。さらに、8748SL では、入力ポートと PORT パラメーターで指定する出力ポートが、同一ポートグループ「1～24、50」または「25～48、49」に入っていないと注意
出力キューを変更するアクション（相互排他）	
SEDCOS	パケットを PRIORITY パラメーターで指定されたプライオリティーに対応するレベルの送信キューに入れる
MOVETOSTOPRIO	受信時の IP ヘッダーの TOS 優先度（precedence）フィールドの値を、VLAN タグフレームの 802.1p ユーザープライオリティーフィールドにコピーする。また、コピー後のユーザープライオリティーに対応するレベルの送信キューにパケットを入れる
802.1p プライオリティーを書き換えるアクション（相互排他）	
MOVETOSTOPRIO	受信時の IP ヘッダーの TOS 優先度（precedence）フィールドの値を、VLAN タグフレームの 802.1p ユーザープライオリティーフィールドにコピーする。また、コピー後のユーザープライオリティーに対応するレベルの送信キューにパケットを入れる
SETPRIORITY	VLAN タグフレームの 802.1p ユーザープライオリティーフィールドに、PRIORITY パラメーターで指定された値を書き込む。出力ポートがタグ付きの場合のみ有効。出力ポートがタグなしの場合はパケットにタグが付かないので、本アクションは意味を持たない
IP TOS/DSCP フィールドを書き換えるアクション（相互排他）	
SETTOS	パケットの IP TOS 優先度（precedence）フィールドに、NEWTOS パラメーターで指定された値を書き込む。TYPE パラメーターで IP 以外のプロトコルを指定した場合は無効
MOVEPRIOTOTOS	受信時の VLAN タグフレームの 802.1p ユーザープライオリティーフィールドの値を、IP ヘッダーの TOS 優先度（precedence）フィールドにコピーする
SETIPDSCP	IP ヘッダーの DSCP（DiffServ Code Point）フィールドに、NEWIPDSCP パラメーターで指定された値を書き込む。TYPE パラメーターで IP 以外のプロトコルを指定した場合は無効
その他のアクション	
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、ミラーポートを指定し、ポートミラーリング機能を有効にしておく必要がある。パケットが複数のエントリーにマッチした場合、DENY、NODROP、SEND～を除く他のアクションがすべて適用された状態でパケットがミラーされる。また、DENY 対象のパケットであってもミラーされる

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

フィルタリング条件として EPORT（出力スイッチポート）を指定した場合、FDB、L3 テーブルのどちらにも登録されていない MAC アドレス（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）宛てのパケットにはフィルターが適用されなくなる。したがって、TCP 制御フラグによるフィルタリング（TCPSYN、TCPACK、TCPFIN パラメーター）を行う場合、および、ブロードキャスト、マルチキャストパケットのフィルタリングを行う場合は、EPORT パラメーターを併用しないこと。

8748SL では、ポートグループ「1～24、50」と「25～48、49」をまたいで、IPOINT と EPORT を同時に設定することはできない。

8748SL では、「ACTION=SENDCOS」のエントリを持つ、あるいは、「NOMACTHACTION=SENDCOS」の指定があるフィルター（マッチ条件）は、合計で 4 つまでしか作れない。

8748SL では、パケットの入力ポートと出力ポートがポートグループ「1～24、50」と「25～48、49」をまたいだ場合に、以下の制限がある（SENDEPORT、SENDNONUNICASTTOPORT アクションにおける「出力ポート」は、PORT パラメーターで指定したポートを意味する）。これらの制限は 8748SL 固有のもので、8724SL にはない。

- ・まったく機能しないアクション：SENDEPORT、SENDNONUNICASTTOPORT
- ・IPOINT を指定できないアクション（指定した場合はマッチしない）：SENDCOS
- ・EPORT を指定できないアクション（指定した場合はマッチしない）：NODROP、SETTOS、MOVE-TOSTOPRIO、MOVEPRIOTOTOS、SETIPDSCP
- ・制限のないアクション：DENY、SETPRIORITY、SENDMIRROR

前記の制限を回避するため、8748SL では原則として、入力ポートと出力ポートが「1～24、50」または「25～48、49」のどちらかのポートグループに両方とも入るよう設定することをおすすめする。

関連コマンド

ADD SWITCH L3FILTER ENTRY (121 ページ)
 ADD SWITCH L3FILTER MATCH (127 ページ)
 DELETE SWITCH L3FILTER ENTRY (146 ページ)
 SET SWITCH L3FILTER MATCH (265 ページ)
 SHOW SWITCH L3FILTER (356 ページ)

SET SWITCH L3FILTER MATCH

カテゴリー：スイッチング / ハードウェア IP フィルター

```
SET SWITCH L3FILTER=filter-id MATCH={TOS|IPDSCP|TTL|PROTOCOL|SIPADDR|
DIPADDR|TCPSPORT|TCPDPORT|TCPSYN|TCPACK|TCPFIN|TYPE|UDPSPORT|
UDPDPORT}[,...] [SCLASS={A|B|C|HOST|1..32}] [DCLASS={A|B|C|HOST|1..32}]
[IMPORT={TRUE|FALSE}] [EXPORT={TRUE|FALSE}] [TYPE={802|ETHII|SNAP}]
[NOMATCHACTION={SETPRIORITY|SENDCOS|SETTOS|DENY|SENDEPORT|SENDMIRROR|
MOVEPRIOTOTOS|MOVETOSTOPRIO|SENDNONUNICASTTOPORT|SETIPDSCP}[,...]]
[NOMATCHDSCP=0..63] [NOMATCHPORT=port-number] [NOMATCHPRIORITY=0..7]
[NOMATCHTOS=0..7]
```

filter-id: フィルター番号 (1~14)

port-number: スイッチポート番号 (1~)

解説

ハードウェア IP フィルター (L3 フィルター) の設定を変更する。

本コマンドでは、フィルタリング条件 (マッチ条件) として使用するパケットフィールドの指定を変更できる。具体的な条件値 (エントリー) は SET SWITCH L3FILTER ENTRY コマンドで変更する。

該当フィルターにエントリーが登録されている場合は設定を変更できない。その場合は、DELETE SWITCH L3FILTER ENTRY コマンドですべてのエントリーを削除してから本コマンドを実行し、新しいマッチ条件に適合するよう再度エントリーを登録すること。

パラメーター

L3FILTER フィルター番号。この番号は可変なので、必ず SHOW SWITCH L3FILTER コマンドで確認してから指定すること

MATCH フィルタリング条件として使用するパケットフィールドを指定する。カンマ区切りで複数指定が可能。詳細は別表を参照。

SCLASS SIPADDR (始点 IP アドレス) のパケットマッチング時に適用するネットマスク。A、B、C はそれぞれクラス A (8 ビット)、B (16 ビット)、C (24 ビット) の標準マスク。HOST は単一アドレスを示す 32 ビットマスク。あるいは、1~32 の任意長のマスクを指定できる。

DCLASS DIPADDR (終点 IP アドレス) のパケットマッチング時に適用するネットマスク。A、B、C はそれぞれクラス A (8 ビット)、B (16 ビット)、C (24 ビット) の標準マスク。HOST は単一アドレスを示す 32 ビットマスク。あるいは、1~32 の任意長のマスクを指定できる。

IMPORT 特定のスイッチポートから入力されたパケットだけをフィルタリングの対象にしたい場合に TRUE を指定する。具体的なポート番号は ADD SWITCH L3FILTER ENTRY コマンドの IPORT パラメーターで指定する (指定ポートから入力されたパケットだけがフィルタリングの対象となる)。FALSE のときはすべてのポートでフィルタリングが行われる。デフォルトは FALSE。

EXPORT 特定のスイッチポートから出力されるパケットだけをフィルタリングの対象にしたい場合に

TRUE を指定する。具体的なポート番号は ADD SWITCH L3FILTER ENTRY コマンドの EPORT パラメーターで指定する（指定ポートから出力されるパケットだけがフィルタリングの対象となる。ただし、本パラメーターに TRUE を指定した場合は、FDB か L3 テーブルに登録されていない MAC アドレス宛てのパケットがフィルタリング対象にならないという制限がある。詳細は ADD SWITCH L3FILTER ENTRY コマンドの EPORT パラメーターの説明を参照）。FALSE のときはすべてのポートでフィルタリングが行われる。デフォルトは FALSE。

TYPE フィルタリング条件として TYPE（L3 プロトコルタイプ）を指定した場合に、フレームフォーマット（エンキャプセレーション）を指定する。802（802.2 LLC）、ETHII（Ethernet Version 2）、SNAP（802.2 LLC + SNAP）から選択する。ADD SWITCH L3FILTER ENTRY コマンドの TYPE パラメーターには、ここで指定したフレームフォーマットのプロトコル番号を指定する。

NOMATCHACTION フィルター内のどのエントリーにもマッチしなかったパケットに対するデフォルトのアクション。カンマ区切りで複数のアクションを指定できる。アクションの詳細については、ADD SWITCH L3FILTER ENTRY コマンドの表を参照のこと（ただし、NODROP アクションは指定できない。また、アクションパラメーターの NEWIPDSCP、PORT、PRIORITY、NEWTOS は、それぞれ NOMATCHDSCP、NOMATCHPORT、NOMATCHPRIORITY、NOMATCHTOS となる）。省略時は SENDCOS。

NOMATCHDSCP（どのエントリーにもマッチしなかったパケットに対するアクションパラメーター）パケット送信時に IP ヘッダーの DSCP フィールドにセットする値。NOMATCHACTION に SETIPDSCP を指定した場合のみ有効。

NOMATCHPORT（どのエントリーにもマッチしなかったパケットに対するアクションパラメーター）対象パケットを出力するスイッチポート。NOMATCHACTION パラメーターに SENDEPORT か SENDNONUNICASTTOPORT を指定したときのみ有効。このとき、本パラメーターで指定するポート（出力ポート）と入力ポートが同一 VLAN になるよう注意すること。さらに、8748SL では、入力ポートと本パラメーターで指定する出力ポートが、同一ポートグループ「1～24、50」または「25～48、49」に入っていないと注意。

NOMATCHPRIORITY（どのエントリーにもマッチしなかったパケットに対するアクションパラメーター）対象パケットに適用する 802.1p ユーザープライオリティー（0～7）値。NOMATCHACTION パラメーターに SETPRIORITY か SENDCOS を指定したときのみ有効。NOMATCHACTION に SETPRIORITY を指定したときは、パケットのユーザープライオリティーフィールドに NOMATCHPRIORITY パラメーターで指定した値を書き込んで送出する（出力スイッチポートがタグ付きでないという意味を持たない）。NOMATCHACTION に SENDCOS を指定したときは、パケットを NOMATCHPRIORITY パラメーターで指定したユーザープライオリティーに対応する送信キューに入れる。省略時は 0。

NOMATCHTOS（どのエントリーにもマッチしなかったパケットに対するアクションパラメーター）パケット送信時に IP ヘッダーの TOS 優先度フィールドにセットする値。NOMATCHACTION に SETTOS を指定した場合のみ有効。

TOS	IP ヘッダーの TOS オクテットの優先度（precedence）フィールド。IPDSCP とは同時に指定できない
IPDSCP	IP ヘッダーの DSCP（DiffServ Code Point）フィールド。IPTOS とは同時に指定できない

TTL	IP ヘッダーの TTL (生存時間) フィールド
PROTOCOL	IP ヘッダーのプロトコルフィールド
SIPADDR	IP ヘッダーの始点 IP アドレス。本オプションを指定するときは、SCLASS パラメーターの指定も必要。
DIPADDR	IP ヘッダーの終点 IP アドレス。本オプションを指定するときは、DCLASS パラメーターの指定も必要。
TCPSPORT	TCP ヘッダーの始点ポート。本オプションを指定するときは PROTOCOL の指定も必要。
TCPDPORT	TCP ヘッダーの終点ポート。本オプションを指定するときは PROTOCOL の指定も必要。
TCP SYN	TCP ヘッダーの制御フラグ「Syn」。本オプションを指定するときは PROTOCOL の指定も必要。また、EMPORT に TRUE を指定しないこと。
TCP ACK	TCP ヘッダーの制御フラグ「Ack」。本オプションを指定するときは PROTOCOL の指定も必要。また、EMPORT に TRUE を指定しないこと。
TCP FIN	TCP ヘッダーの制御フラグ「Fin」。本オプションを指定するときは PROTOCOL の指定も必要。また、EMPORT に TRUE を指定しないこと。
TYPE	Ethernet フレームの L3 プロトコルタイプフィールド。本オプションを指定するときは、TYPE パラメーターでフレームフォーマットも指定する必要がある。他のオプションと併用はできない。
UDPSPORT	UDP ヘッダーの始点ポート。本オプションを指定するときは PROTOCOL の指定も必要。
UDP DPORT	UDP ヘッダーの終点ポート。本オプションを指定するときは PROTOCOL の指定も必要。

表 37: MATCH パラメーターに指定できるオプション

関連コマンド

ADD SWITCH L3FILTER ENTRY (121 ページ)
 ADD SWITCH L3FILTER MATCH (127 ページ)
 DELETE SWITCH L3FILTER (145 ページ)
 SET SWITCH L3FILTER ENTRY (260 ページ)
 SHOW SWITCH L3FILTER (356 ページ)

SET SWITCH LOOPDETECTION

カテゴリー：スイッチング / ポート

SET SWITCH LOOPDETECTION=LDF [ACTION={NONE|DISABLEPORT|LINKDOWN}]
[LDFINTERVAL=10..1000000] [PDTO={1..86400|NONE}] [SECURE={ON|OFF}]

解説

ループガード (LDF 検出) 機能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

LOOPDETECTION ループ検出方式。LDF (LDF 検出) しかサポートしていないが省略はできない。

ACTION ループを検出した場合の動作 (アクション)。NONE (ループ検出時のログ記録のみ)、DISABLEPORT (ポートをディセーブルにする。また、ループ検出時と動作実行時にログを記録する)、LINKDOWN (ポートを物理的にリンクダウンさせる。また、ループ検出時と動作実行時にログを記録する) から選択する。これらの動作は、SET SWITCH LOOPDETECTION コマンドの PDTO パラメーターで指定した時間が経過すると自動的にアクション実行前の状態に戻る。また、自動復帰前であっても、ENABLE SWITCH PORT コマンドを用いて任意の時点でアクション実行前の状態に戻すことができる。デフォルトは NONE。

LDFINTERVAL LDF (Loop Detection Frame) の送信間隔 (秒)。一斉送信を避けるため、各ポートはタイミングをずらして LDF を送信する。SECURE オプションを ON にしているときはさらに、この値が LDF の有効時間にもなる。デフォルトは 120。

PDTO ACTION パラメーターで指定した動作が実行された後、自動的に実行前の状態に戻るまでの時間 (秒)。NONE を指定した場合、自動的に実行前の状態には戻らない (ENABLE SWITCH PORT コマンドで復帰可能)。デフォルトは 300。

SECURE 古い LDF を破棄するかどうか。ON の場合、受信した LDF に含まれる ID が、保持している送信済み LDF ID のリストに含まれているかどうかをチェックし、含まれていない場合は該当 LDF を無効と見なして破棄する。ID は LDF を送信するたびに変更されるため、送信した LDF の有効時間は LDF の送信間隔 (LDFINTERVAL パラメーター) の値となる。デフォルトは OFF。

備考・注意事項

- ループ検出後のアクションの副次的な作用として、アクションが実行されるときと実行前の状態に戻るときに SNMP のリンクトラップが出力される。

関連コマンド

ENABLE SWITCH LOOPDETECTION (208 ページ)

ENABLE SWITCH PORT (211 ページ)

SHOW SWITCH LOOPDETECTION (360 ページ)

SHOW SWITCH LOOPDETECTION COUNTER (363 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
- ・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。
- ・複数のソースポートを指定した場合で、かつ指定ポートにタグ付きとタグなしが混在している場合、送信パケットはすべてタグなしとしてミラーリングされる
- ・L3 機能を通じたパケット (ハードウェア IP フィルターによってミラーリングされたパケットを含む) は VLAN タグが付いた状態でミラーポートに出力される

関連コマンド

DISABLE SWITCH MIRROR (176 ページ)

ENABLE SWITCH MIRROR (210 ページ)

SET SWITCH PORT (271 ページ)

SHOW SWITCH (346 ページ)

SHOW SWITCH PORT (365 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|
count}] [DESCRIPTION=string] [DLFLIMIT={NONE|count}] [EGRESSLIMIT={NONE|
0|1000..127000|8..1016}] [INFILTERING={OFF|ON}] [INGRESSLIMIT={NONE|0|
64..127000|8..1016}] [INTRUSIONACTION={DISABLE|DISCARD|TRAP}] [LEARN={0|
1..256}] [RELEARN={ON|OFF}] [MCLIMIT={NONE|count}] [MIRROR={BOTH|NONE|RX|
TX}] [MODE={AUTONEGOTIATE|MASTER|SLAVE}] [SPEED={AUTONEGOTIATE|10MHALF|
10MFULL|100MHALF|100MFULL|1000MFULL}] [IGMPACTION={DENY|REPLACE}]
[IGMPFILTER={NONE|filter-id}] [IGMPMAXGROUP={NONE|1..65535}]
```

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)

count: 個数 (0~262143)

string: 文字列 (1~47 文字)

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。

ミラーソースポート、パケットストームプロテクション、通信モード、受信フレームタイプ (VLAN タグあり・なし) などの設定に使う。

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。パケットストームプロテクションの設定を行うとき (BCLIMIT、DLFLIMIT、MCLIMIT パラメーター) は、1-8、9-16、17-24、25、26 のいずれか (8724SL) または、1-8、9-16、17-24、25-32、33-40、41-48、49、50 のいずれか (8748SL) のポートグループ単位で指定する必要がある。

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 ブロードキャストパケットの受信上限値。1 秒間の最大受信パケット数を指定する。上限を超えたパケットは破棄される。NONE または 0 を指定した場合は、制限なしとなる。デフォルトは NONE。

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。

DLFLIMIT 未学習のユニキャストパケットの受信上限値。1 秒間の最大受信パケット数を指定する。上限を超えたパケットは破棄される。NONE または 0 を指定した場合は、制限なしとなる。デフォルトは NONE。

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、10/100M ポートが 1000～127000Kbps、1000M ポートが 8～1016Mbps。NONE および 0 は制限なし。実際の送信レートは、10/100M ポートでは 1000Kbps の倍数になるよう切り捨てられる。また、1000M ポートでは、8Mbps の倍数になるよう調整される。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）か 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。

INGRESSLIMIT 該当ポートの受信レート上限値（帯域制限機能）。指定可能な値の範囲は、10/100M ポートが 64～127000Kbps、1000M ポートが 8～1016Mbps。NONE および 0 は制限なし。実際の送信レートは、10/100M ポートでは 1000Kbps 未満のときは 64Kbps の倍数に、1000Kbps 以上のときは 1000Kbps の倍数になるよう切り捨てられる。また、1000M ポートでは、8Mbps の倍数になるよう調整される。デフォルトは NONE。

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。

INTRUSIONACTION 未学習の送信元 MAC アドレスを持つフレームを、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。

MCLIMIT マルチキャストパケットの受信上限値。1 秒間の最大受信パケット数を指定する。上限を超えたパケットは破棄される。NONE または 0 を指定した場合は、制限なしとなる。デフォルトは NONE。

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。

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。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。デフォルトは AUTONEGOTIATE（オートネゴシエーション）。

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)。

備考・注意事項

BCLIMIT、DLFLIMIT、MCLIMIT パラメーターに 0/NONE 以外の値を指定する場合は、すべて同じ値を指定しなくてはならない。また、これらのパラメーターを指定する場合は、PORT に 1-8、9-16、17-24、25、26 のいずれか (8724SL) または、1-8、9-16、17-24、25-32、33-40、41-48、49、50 のいずれか (8748SL) を指定する必要がある。

10/100M ポートの場合、送信レート上限値 (EGRESSLIMIT) の有効範囲 (1000 ~ 127000Kbps) と受信レート上限値 (INGRESSLIMIT) の有効範囲 (64 ~ 127000Kbps) が異なるので注意。

関連コマンド

ADD IGMP FILTER (「IP マルチキャスト」の 32 ページ)

CREATE IGMP FILTER (「IP マルチキャスト」の 41 ページ)

DISABLE SWITCH PORT (177 ページ)

ENABLE SWITCH PORT (211 ページ)

SHOW IGMP FILTER (「IP マルチキャスト」の 104 ページ)

SHOW SWITCH PORT (365 ページ)

SET SWITCH QOS

カテゴリー：スイッチング / QoS

SET SWITCH QOS=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 (0~3。大きいほど優先度が高い)

解説

QoS (Quality of Service) 機能の設定を変更する。

具体的には、プライオリティータグフレームの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。

パラメーター

QOS ユーザープライオリティー 0~7 に対応するプライオリティーキューの番号をカンマで区切って指定する。キューはポートごとに 0~3 の 4 つがあり、3 がもっとも優先度が高い。フレーム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る。すなわち、上位のキューに 1 つでもフレームが格納されている場合、それより下位のキューからはフレームは送信されない。タグなしフレームは、宛先 MAC アドレスが本製品ならユーザープライオリティー 4、宛先 MAC アドレスが本製品以外ならユーザープライオリティー 0 と見なされる。p0 から p7 まですべての値を指定すること。デフォルトは別表を参照。

ユーザープライオリティー	キュー番号 (大きいほど優先度が高い)
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

表 38: ユーザープライオリティー値-プライオリティーキューのデフォルトマッピング

例

ユーザープライオリティー 0~7 に対し、送信キュー 0, 0, 0, 1, 1, 2, 2, 3 を割り当てる。

SET SWITCH QOS=0, 0, 0, 1, 1, 2, 2, 3

備考・注意事項

バージョン 2.5.3 より、本コマンドは SET QOS HWPRIORITY コマンドに置き換えられた。本コマンドも後方互換性のために残されているが、設定保存時には SET QOS HWPRIORITY コマンドに自動変換される。

関連コマンド

SHOW SWITCH QOS (374 ページ)

SET SWITCH TRUNK

カテゴリー：スイッチング / ポート

SET SWITCH TRUNK=trunk [SELECT={MACSRC|MACDEST|MACBOTH|IPSRC|IPDEST|
IPBOTH}] [SPEED={10M|100M|1000M}]

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

SELECT トランクからパケットを送信するときの選択基準。この基準にしたがって実際の送信に使うポートを選択する。MACSRC (送信元 MAC アドレス)、MACDEST (宛先 MAC アドレス)、MACBOTH (送信元・宛先 MAC アドレス)、IPSRC (始点 IP アドレス)、IPDEST (終点 IP アドレス)、IPBOTH (始点・終点 IP アドレス) から選択する。デフォルトは MACBOTH。

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。デフォルトは 100M。

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、SELECT パラメーターの設定とは関係なく、常に終点 IP アドレス (IPDEST) に基づいて決定される (負荷分散される)。フラッドパケットは、トランクグループ内で一番最初にリンクが確立されたポートから送出される。

関連コマンド

ADD SWITCH TRUNK (131 ページ)

CREATE SWITCH TRUNK (136 ページ)

DELETE SWITCH TRUNK (147 ページ)

DESTROY SWITCH TRUNK (151 ページ)

SHOW SWITCH TRUNK (375 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={*vlanname*|1..4094} **PORT**={*port-list*|ALL} **FRAME**={UNTAGGED|TAGGED}

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)

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 ポートのタグ設定。TAGGED (タグ付き)、UNTAGGED (タグなし) から選択する。各ポートは、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。

関連コマンド

ADD VLAN PORT (132 ページ)

DELETE VLAN PORT (148 ページ)

SHOW VLAN (377 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 dhcpsnooping

DHCP Snooping Information
-----
DHCP Snooping ..... Enabled
Option 82 status ..... Enabled
Ip Filtering ..... Enabled
ARP security ..... Enabled
ARP security action ..... None
Strict Unicast ..... Disabled
Logging enabled ..... None
XLA ..... Disabled
Block type ..... Block IP traffic
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
ARP security action	未サポート
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
Block type	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 39:

関連コマンド

- ENABLE DHCP Snooping (181 ページ)
- ENABLE DHCP Snooping ARPSECURITY (182 ページ)
- ENABLE DHCP Snooping LOG (183 ページ)
- ENABLE DHCP Snooping OPTION82 (184 ページ)
- SET DHCP Snooping CHECKINTERVAL (227 ページ)
- SET DHCP Snooping PORT (228 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 40:

関連コマンド

ENABLE DHCP Snooping (181 ページ)

ENABLE DHCP Snooping ARP Security (182 ページ)

RESET DHCP Snooping Counter (219 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。起動後 DHCP Snooping を一度も有効にしてい ないときは None、一度でも有効化した後 は CLASSIFIER と表示される
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。Dy- namic (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 41:

関連コマンド

ENABLE DHCP Snooping (181 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/Not specified
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。MAC アドレス無指定エントリーの場合は「Not specified」と表示される

表 42:

関連コマンド

ADD DHCP Snooping BINDING (112 ページ)

ENABLE DHCP Snooping (181 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 43:

関連コマンド

ENABLE DHCP Snooping (181 ページ)

SET DHCP Snooping Port (228 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
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
Actor System	システム ID (MAC アドレス)
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 44:

関連コマンド

DISABLE LACP (157 ページ)

ENABLE LACP (185 ページ)

SET LACP PRIORITY (231 ページ)

SHOW LACP PORT (289 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	Mode	Passive
Periodic	Fast	Periodic	Fast
Individual	No	Individual	Yes
Synchronised	Yes	Synchronised	No
Collecting	No	Collecting	Yes
Distributing	No	Distributing	Yes
Defaulted	Yes	Defaulted	Yes
Expired	No	Expired	No
Actor Churn	No		
Partner Churn	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 45:

関連コマンド

- ADD LACP PORT (114 ページ)
- SET LACP PORT (230 ページ)
- SHOW LACP (288 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イスインデックス）
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 46:

関連コマンド

- ADD LACP PORT（114 ページ）
- SET LACP PORT（230 ページ）
- SET LACP PRIORITY（231 ページ）
- SHOW LACP（288 ページ）

SHOW LACP TRUNK

SHOW LACP PORT (289 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	本機の最大エーゼタイム設定値 (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 47: 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 48: 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 49: TABLE 指定時

関連コマンド

ADD MSTP MSTI VLAN (116 ページ)
 DELETE MSTP MSTI VLAN (142 ページ)
 DISABLE MSTP (159 ページ)
 ENABLE MSTP (187 ページ)
 SET MSTP (232 ページ)
 SET MSTP CIST (234 ページ)
 SET MSTP MSTI (237 ページ)
 SHOW MSTP CIST (298 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 50:

関連コマンド

DISABLE MSTP (159 ページ)

DISABLE MSTP CIST PORT (160 ページ)

ENABLE MSTP (187 ページ)

ENABLE MSTP CIST PORT (188 ページ)

SET MSTP CIST (234 ページ)

SET MSTP CIST PORT (235 ページ)

SHOW MSTP (295 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 51: 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 52: ポート番号指定時

関連コマンド

DISABLE MSTP (159 ページ)

DISABLE MSTP CIST PORT (160 ページ)

ENABLE MSTP (187 ページ)

ENABLE MSTP CIST PORT (188 ページ)

SET MSTP CIST (234 ページ)

SET MSTP CIST PORT (235 ページ)

SHOW MSTP (295 ページ)

SHOW MSTP MSTI PORT (310 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	受信バ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 53:

関連コマンド

DISABLE MSTP (159 ページ)

ENABLE MSTP (187 ページ)

RESET MSTP COUNTER PORT (221 ページ)

SET MSTP CIST (234 ページ)

SHOW MSTP DEBUG 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 DEBUG MSTI={CIST|instance|ALL}

instance: MST インスタンス ID (1 ~ 4094)

解説

各 MST インスタンスで有効になっている MSTP デバッグオプションを表示する。

パラメーター

MSTI MST インスタンス ID または CIST (Common and Internal Spanning Tree)。ALL 指定時はすべての MST インスタンスと CIST が対象となる。

入力・出力・画面例

Manager > show mstp debug msti=cist

MSTP Instance	Port	Debug Modes State Machine Debug Modes	Output	Timeout
CIST	1	STATE PTX	Asyn 0 (16)	None
	2	STATE PTX	Asyn 0 (16)	None
	3	STATE PTX	Asyn 0 (16)	None
	4	STATE PTX	Asyn 0 (16)	None
	5	STATE PTX	Asyn 0 (16)	None
...				

関連コマンド

- DISABLE MSTP (159 ページ)
- DISABLE MSTP DEBUG MSTI (161 ページ)
- ENABLE MSTP (187 ページ)
- ENABLE MSTP DEBUG MSTI (189 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 54: 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 55: MST インスタンス ID 指定時	

関連コマンド

DISABLE MSTP (159 ページ)

ENABLE MSTP (187 ページ)

SET MSTP (232 ページ)

SET MSTP MSTI PORT (238 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、Master 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 56:

関連コマンド

DISABLE MSTP (159 ページ)

DISABLE MSTP MSTI PORT (162 ページ)

ENABLE MSTP (187 ページ)

ENABLE MSTP MSTI PORT (191 ページ)

SET MSTP MSTI (237 ページ)

SET MSTP MSTI PORT (238 ページ)

SHOW MSTP CIST PORT (301 ページ)

SHOW MSTP MSTI (307 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

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)
Use hyphen..... YES

```

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 57: PORTAUTH=8021X のとき

SystemAuthControl	MAC ベース認証機能の有効・無効
Number of 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)
Use hyphen	RADIUS サーバーに認証を要求するときのユーザー名・パスワードにハイフンを含めるかどうか
Port	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

表 58: PORTAUTH=MACBASED のとき

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (109 ページ)

ENABLE PORTAUTH (192 ページ)

ENABLE PORTAUTH PORT (194 ページ)

SET PORTAUTH HYPHEN (239 ページ)

SET PORTAUTH PORT (241 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (245 ページ)

SHOW PORTAUTH COUNTER (316 ページ)

SHOW PORTAUTH MULTISUPPLICANT PORT (319 ページ)

SHOW PORTAUTH PORT (323 ページ)

SHOW PORTAUTH TIMER (329 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 59:

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (109 ページ)

ENABLE PORTAUTH (192 ページ)

ENABLE PORTAUTH PORT (194 ページ)

SET PORTAUTH PORT (241 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (245 ページ)

SHOW PORTAUTH (312 ページ)

SHOW PORTAUTH MULTISUPPLICANT PORT (319 ページ)

SHOW PORTAUTH PORT (323 ページ)

SHOW PORTAUTH TIMER (329 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 multisuppliment 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 60: 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 61: PORTAUTH=MACBASED のとき

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (109 ページ)

ENABLE PORTAUTH (192 ページ)

ENABLE PORTAUTH PORT (194 ページ)

SET PORTAUTH PORT (241 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (245 ページ)

SHOW PORTAUTH (312 ページ)

SHOW PORTAUTH COUNTER (316 ページ)

SHOW PORTAUTH PORT (323 ページ)

SHOW PORTAUTH TIMER (329 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
      Auto Authenticate ..... False
```

```
Manager > show portauth=8021x port=7
```

802.1X Configuration

```
Interface: port7
```

```
PAE Type..... Both
```

Multi-SupPLICANT Authenticator

```
Number of Multi SupPLICANTS... 0
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
Auto Authenticate ..... False
```

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 > show portauth=macbased port=10
```

MAC Based Authentication Configuration

```
Interface: port10
```

```

PAE Status..... Enabled
  Number of Supplicants..... 1
  AuthControlPortControl..... Auto
  quietPeriod..... 60
  reAuthPeriod..... 3600
  reAuthEnabled..... False
  secureVlan..... On
  trap..... None
  mibReset..... Enabled
  vlanAssignment..... Enabled
  Auto Authenticate ..... False

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

Number of Multi Supplicants	Multi-Supplicant モードにおける 802.1X Supplicant の数
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
Auto Authenticate	未サポート
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 62: 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)、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
Auto Authenticate	クリティカルポートに設定されているかどうか

表 63: PORTAUTH=MACBASED のとき

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (109 ページ)

ENABLE PORTAUTH (192 ページ)

ENABLE PORTAUTH PORT (194 ページ)

SET PORTAUTH PORT (241 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (245 ページ)

SHOW PORTAUTH (312 ページ)

SHOW PORTAUTH COUNTER (316 ページ)

SHOW PORTAUTH MULTISUPPLICANT PORT (319 ページ)

SHOW PORTAUTH TIMER (329 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 64: 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 65: PORTAUTH=MACBASE のとき

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (109 ページ)

ENABLE PORTAUTH (192 ページ)

ENABLE PORTAUTH PORT (194 ページ)

SET PORTAUTH PORT (241 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (245 ページ)

SHOW PORTAUTH (312 ページ)

SHOW PORTAUTH COUNTER (316 ページ)

SHOW PORTAUTH MULTISUPPLICANT PORT (319 ページ)

SHOW PORTAUTH PORT (323 ページ)

SHOW QOS HWPRIORITY

カテゴリー：スイッチング / QoS

SHOW QOS HWPRIORITY

解説

QoS 設定（802.1Q/802.1p タグフレームのユーザプライオリティ値とプライオリティキューのマッピング）設定を表示する。

入力・出力・画面例

Manager > show qos hwpriority

QoS Priority Mapping

Priority Value	Egress Queue
P0	1
P1	0
P2	0
P3	1
P4	2
P5	2
P6	3
P7	3

Priority Value	受信フレームのユーザプライオリティ
Egress Queue	プライオリティキュー番号（大きいほど優先度が高い）

表 66:

関連コマンド

SET QOS HWPRIORITY（250 ページ）

SHOW QOS HWQUEUE

カテゴリー：スイッチング / QoS

SHOW QOS HWQUEUE

解説

送信キューごとの最大送信パケット数と最大送信遅延時間の設定情報を表示する。

入力・出力・画面例

Manager > show qos hwqueue

QOS Egress Queue Configuration

Queue Number	Max Packets	Max Latency (microseconds)
0	None	None
1	None	None
2	None	None
3	None	None

Queue Number	キュー番号（0～3。大きいほど優先度が高い）
Max Packets	最大送信パケット数
Max Latency (microseconds)	最大送信遅延時間（単位：マイクロ秒）

表 67:

関連コマンド

SET QOS HWQUEUE（252 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
```

SHOW STP

```
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)
Status ..... ON
Number of Ports ..... 26
    Number Enabled ..... 26
    Number Disabled ..... 0
Bridge Identifier ..... 32768 : 00-00-f4-27-2c-74
Bridge Priority ..... 32768
Root Bridge ..... 32768 : 00-00-cd-24-03-66
Designated Bridge ..... 61440 : 00-00-cd-08-17-0c
Root Port ..... 5
Root Path Cost ..... 220000
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 ..... 2
Time since last TC .... 26
```

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 68:

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 69: SUMMARY オプション指定時

関連コマンド

CREATE STP (135 ページ)

DESTROY STP (150 ページ)

DISABLE STP (166 ページ)

ENABLE STP (199 ページ)

SET STP (254 ページ)

SHOW STP COUNTER (339 ページ)

SHOW STP PORT (343 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:                                Transmit:
Total STP Packets                       0      Total STP Packets                       0
Configuration BPDU                     0      Configuration BPDU                     0
TCN BPDU                               0      TCN BPDU                               0
RSTP TC-Flag                           0      RSTP TC-Flag                           0
RST BPDU                               0      RST BPDU                               0
Invalid BPDU                            0
Discarded:
Port Disabled                           0
Invalid Protocol                        0
Invalid Type                            0
Invalid Message Age                     0
Config BPDU length                      0
TCN BPDU length                         0
RST 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 BPDU (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
RSTP TC-Flag	未サポート
RST BPDU	RSTP BPDU 受信数
Invalid BPDU	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 STP Packets	送信した BPDU (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
RSTP TC-Flag	未サポート
RST BPDU	RSTP 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
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
RST BPDU length	未サポート

表 70:

関連コマンド

RESET STP (224 ページ)

SHOW STP (335 ページ)

SHOW STP PORT (343 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

STP Name	Port	Enabled Debug Modes	Output	Timeout

default	Port1	MSG, PKT, STATE	Asyn 0 (16)	123456
	Port2	STATE	Asyn 0 (16)	123456
	Port3	MSG, PKT	Asyn 0 (16)	123456
	Port4	MSG	Asyn 0 (16)	123456
	Port5	None		
	Port6	None		
	Port7	MSG, PKT, STATE	Asyn 0 (16)	123456
	Port8	MSG, PKT, STATE	Asyn 0 (16)	123456
	Port9	MSG, PKT, STATE	Asyn 0 (16)	123456
	Port10	MSG, PKT, STATE	Asyn 0 (16)	123456
	Port11	MSG, PKT, STATE	Asyn 0 (16)	123456
	Port12	MSG, PKT, STATE	Asyn 0 (16)	123456
	Port13	MSG, PKT, STATE	Asyn 0 (16)	123456
	Port14	MSG, PKT, STATE	Asyn 0 (16)	123456
	Port15	MSG, PKT, STATE	Asyn 0 (16)	123456
	Port16	MSG, PKT, STATE	Asyn 0 (16)	123456
	Port17	MSG, PKT, STATE	Asyn 0 (16)	123456
	Port18	MSG, PKT, STATE	Asyn 0 (16)	123456
	Port19	MSG, PKT, STATE	Asyn 0 (16)	123456
	Port20	MSG, PKT, STATE	Asyn 0 (16)	123456
	Port21	MSG, PKT, STATE	Asyn 0 (16)	123456
	Port22	MSG, PKT, STATE	Asyn 0 (16)	123456
	Port23	MSG, PKT, STATE	Asyn 0 (16)	123456
	Port24	MSG, PKT, STATE	Asyn 0 (16)	123456
	Port25	None		
	Port26	None		

STP Name	STP ドメイン名
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 (BPDU をデコードして表示)、PKT (BPDU を ASCII 表示)、STATE (ポートの状態遷移を表示)、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 71:

関連コマンド

DISABLE STP DEBUG (167 ページ)

ENABLE STP DEBUG (200 ページ)

SHOW STP COUNTER (339 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 ..... 100 (auto configured)
  Designated Root ..... 32768 : 00-00-f4-27-2c-74
  Designated Cost ..... 0
  Designated Bridge ... 32768 : 00-00-f4-27-2c-74
  Designated Port ..... 8001
  VLAN membership ..... 1
  Send RSTP BPDU ..... TRUE
-----

Manager > show stp port=5

STP Port Information
-----
STP ..... default
  STP Status ..... ON

Port ..... 5

```

```

RSTP Port Role ..... Root
State ..... Forwarding
Point To Point ..... Yes (Auto)
Port Priority ..... 128
Port Identifier ..... 8005
Pathcost ..... 200000 (auto configured)
Designated Root ..... 32768 : 00-00-cd-24-03-66
Designated Cost ..... 20000
Designated Bridge ... 61440 : 00-00-cd-08-17-0c
Designated Port ..... 8008
EdgePort ..... No
VLAN membership ..... 1
Send RSTP BPDU ..... TRUE
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
VLAN membership	所属 VLAN の数

Send RSTP BPDU	未サポート
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 72:

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最初にリンクアップしたポート、「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 (254 ページ)
- SET STP PORT (256 ページ)
- SHOW STP (335 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

スイッチングモジュール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-f4-27-2c-74
Learning ..... ON
Ageing Timer ..... ON
Number of Fixed Ports ..... 26
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
Number of WAN Interfaces ... 0
Name of Interface(s) ..... -
Ageingtime ..... 300
L3 Ageingtime ..... 900
UpTime ..... 00:00:25
STP Forwarding ..... DISABLED
-----
```

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
Number of Fixed Ports	固定 Ethernet ポートの数
Number of Uplink Ports	アップリンク Ethernet 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
Number of WAN Interfaces	WAN インターフェース数
Name of Interface(s)	WAN インターフェース名
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)
L3 Ageingtime	L3 テーブルのエージングタイム
Uptime	再起動後の経過時間 (時:分:秒の形式)。MIB-II オブジェクト sysUp-Time と同じ。
STP Forwarding	BPDU フォワーディングの有効・無効

表 73:

関連コマンド

RESET SWITCH (225 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        ErrorResets                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ーが表示される
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
ErrorResets	未サポート
General counters セクション	一般的なカウンターが表示される。
Resets	エラーによる DMA チャンネルのリセット回数

表 74:

関連コマンド

RESET SWITCH (225 ページ)

SHOW SWITCH (346 ページ)

SHOW SWITCH DEBUG

カテゴリー：スイッチング / 一般コマンド

SHOW SWITCH DEBUG

解説

スイッチングモジュールのデバッグオプションに関する情報を表示する。

入力・出力・画面例

Enabled Switch Debug Modes	Output	Timeout
-----	-----	-----
ARL, DMA	16	12345
-----	-----	-----

Enabled Switch Debug Modes	現在有効になっているデバッグオプション。ARL (FDB)、CMIC (CMIC レイヤー)、DMA (ダイレクトメモリアクセス)、QOS (QoS)、S5600 (Broadcom チップ)、PHY (PHY)、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 75:

関連コマンド

DISABLE SWITCH DEBUG (171 ページ)

ENABLE SWITCH DEBUG (204 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 [= {SW|HW}] [ADDRESS=macadd] [DISCARD={SOURCE|
DESTINATION}] [HIT={YES|NO}] [L3={YES|NO}] [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。大文字小文字を区別しない)

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

- FDB** ソフト (SW) ハード (HW) のどちらが保持している FDB を表示するかを指定する。FDB はハードウェア内部に保持され、そのコピーがソフトウェアによって保持されている。通常両者は同一の内容となる。デフォルトは SW
- ADDRESS** 指定したアドレスのエントリーだけを表示する。
- DISCARD** アクションとして DISCARD が指定されているアドレスの破棄基準。送信元アドレス (SOURCE) か宛先アドレス (DESTINATION) のどちらかを指定する。
- HIT** エージングタイム内に受信されたかどうかを指定する。
- L3** レイヤー 3 インターフェースの設定時に登録されたアドレスかどうかを指定する。
- PORT** アドレスを学習したポート。あるいはスタティック登録時に指定した出力ポートを指定する。
- STATUS** 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)

VLAN	MAC Address	Port	Status	Discard	L3	Hit	QOS	QSD
1	00-00-cd-00-8b-00	17	dynamic	-	n	y	0:0	dest
1	00-00-f4-90-19-9b	17	dynamic	-	n	y	0:0	dest

1	00-00-f4-95-3f-07	17	dynamic	-	n	y	0:0	dest
1	00-00-f4-95-9c-96	17	dynamic	-	n	y	0:0	dest
1	00-00-f4-95-9f-31	17	dynamic	-	n	y	0:0	dest
1	00-00-f4-c3-02-cf	17	dynamic	-	n	y	0:0	dest
1	00-05-02-04-41-0d	17	dynamic	-	n	y	0:0	dest
1	00-05-02-69-a0-49	17	dynamic	-	n	y	0:0	dest
1	00-05-02-d1-af-6b	17	dynamic	-	n	y	0:0	dest
1	00-0a-27-ae-59-70	17	dynamic	-	n	y	0:0	dest
1	00-90-27-92-63-22	17	dynamic	-	n	y	0:0	dest
1	00-90-99-1b-65-c7	17	dynamic	-	n	y	0:0	dest
1	00-90-99-38-00-2f	17	dynamic	-	n	y	0:0	dest
1	00-a0-c9-5a-b3-33	17	dynamic	-	n	y	0:0	dest
1	02-41-f4-02-c2-4b	17	dynamic	-	n	y	0:0	dest
1	08-00-2b-e7-fe-1f	17	dynamic	-	n	y	0:0	dest

VLAN	VLAN ID
MAC Address	MAC アドレス
Port	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)
Discard	パケットを破棄するフィルターが設定されている場合、送信元・宛先のどちらのアドレスを基準に破棄するかを示す。source (送信元) destination (宛先) - (破棄しない) のいずれか。
L3	レイヤー 3 インターフェースで登録されたエントリーかどうかを示す。y (yes) か n (no)
Hit	エージングタイム期間内に該当するパケットを受信したかどうか。y (yes) か n (no) で示される。エージングタイマーが有効なときは、n のエントリーは削除される。
QoS	QoS 値。左側の値は送信元アドレスに基づく QoS 値、右側は宛先アドレスに基づく QoS 値。
QSD	プライオリティー情報を持たないフレームを受信したときに、宛先・送信元のどちらを基準にプライオリティーを設定するかどうか。source (送信元) か dest (宛先) で表示される。

表 76:

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 (207 ページ)

SHOW SWITCH (346 ページ)

SHOW SWITCH FILTER (354 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。大文字小文字を区別しない)

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
```

```
VlanSecure ..... ENABLED
```

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

VlanSecure	アクションが Forward（転送）のスタティックエントリーを、ルーティングパケットと本体宛てパケットにも適用するかどうか。ENABLED（適用する）、DISABLED（適用しない）のいずれか（8724SL のみサポート）
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 パラメーターを指定した場合も 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 77:

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（119 ページ）

DELETE SWITCH FILTER（144 ページ）

SET SWITCH MIRROR（270 ページ）

SHOW SWITCH L3FILTER

カテゴリー：スイッチング / ハードウェア IP フィルター

SHOW SWITCH L3FILTER [=*filter-id* [ENTRY [=*entry-id*]]]

filter-id: フィルター番号 (1~14)

entry-id: エントリー番号 (1~124)

解説

ハードウェア IP フィルター (L3 フィルター) の設定内容を表示する。

パラメーター

L3FILTER フィルター番号。番号を省略した場合は、フィルターの一覧が表示される。

ENTRY エントリー番号。番号を省略した場合は、L3FILTER パラメーターで指定したフィルター内の全エントリーが表示される。本パラメーターを指定するときは、L3FILTER パラメーターでフィルター番号を指定しなくてはならない。

入力・出力・画面例

```
Manager > show switch l3filter

Hardware based filtering.... Enabled
Software filtering bypass .. Disabled

Filter ..... 1
Matched fields ..... sip
Type ..... ETH-II
Source address mask .... 255.255.255.0
Dest. address mask ..... 0.0.0.0
Ingress port mask ..... false
Egress port mask ..... false

Filter ..... 2
Matched fields ..... sip
Type ..... ETH-II
Source address mask .... 255.255.255.255
Dest. address mask ..... 0.0.0.0
Ingress port mask ..... false
Egress port mask ..... false

Manager > show switch l3filter=2 entry
```

```
Hardware based filtering.... Enabled
Software filtering bypass .. Disabled
```

```
Filter ..... 2
Matched fields ..... sip
Type ..... ETH-II
Source address mask .... 255.255.255.255
Dest. address mask ..... 0.0.0.0
Ingress port mask ..... false
Egress port mask ..... false
Filter Entries:
```

```
-----
Entry ..... 1
Ingress Port ..... None
Egress Port ..... None
Source Address ..... 192.168.10.130
Source Mask ..... 255.255.255.255
Dest Address ..... 0.0.0.0
Dest Mask ..... 0.0.0.0
Protocol ..... 0
TTL ..... 0
TOS ..... 0
IPDSCP ..... 0
Type ..... 0800 (ETH-II)
Action ..... NODROP
-----
```

```
Entry ..... 2
Ingress Port ..... None
Egress Port ..... None
Source Address ..... 192.168.10.103
Source Mask ..... 255.255.255.255
Dest Address ..... 0.0.0.0
Dest Mask ..... 0.0.0.0
Protocol ..... 0
TTL ..... 0
TOS ..... 0
IPDSCP ..... 0
Type ..... 0800 (ETH-II)
Action ..... NODROP
-----
```

```
Entry ..... 3
Ingress Port ..... None
Egress Port ..... None
Source Address ..... 192.168.10.16
Source Mask ..... 255.255.255.255
Dest Address ..... 0.0.0.0
Dest Mask ..... 0.0.0.0
Protocol ..... 0
TTL ..... 0
TOS ..... 0
IPDSCP ..... 0
```

```
Type ..... 0800 (ETH-II)
Action ..... NODROP
-----
```

Hardware based filtering	ハードウェア IP フィルターの有効・無効
Software filtering bypass	未サポート
Filter	フィルター番号
Matched fields	フィルタリング条件として用いるパケットフィールドの一覧。tos (TOS) \ ipds (IPDSCP) \ ttl (TTL) \ prot (PROTOCOL) \ sip (SIPADDR) \ dip (DIPADDR) \ tcpsp (TCPSPORT) \ tcpd (TCPDPORT) \ tcpsy (TCPSYN) \ tcpa (TCPACK) \ tcpf (TCPFIN) \ udps (UDPSPORT) \ udpd (UDPDPORT) \ type (TYPE) の組み合わせ。
Type	フレームフォーマット
Source address mask	始点 IP アドレスのマッチング時に適用するアドレスマスク
Dest. address mask	終点 IP アドレスのマッチング時に適用するアドレスマスク
Ingress port mask	入力パケットに対するフィルタリングを指定ポートだけに限定するかどうか。
Egress port mask	出力パケットに対するフィルタリングを指定ポートだけに限定するかどうか。
Entry	フィルターエントリー番号
Ingress Port	フィルタリングを適用する入力ポート
Egress Port	フィルタリングを適用する出力ポート
Source Address	始点 IP アドレス
Source Mask	始点マスク
Dest Address	終点 IP アドレス
Dest Mask	終点マスク
Protocol	IP プロトコル番号
TTL	TTL (生存時間) フィールド値
TOS	TOS (サービスタイプ) 優先度 (precedence) 値
IPDSCP	DSCP (DiffServ Code Point) 値
Type	プロトコルタイプ (フレームフォーマット)
TCP Flags	TCP 制御フラグ。左から順に Syn/Ack/Fin
TCP S-Port	TCP 始点ポート
TCP D-Port	TCP 終点ポート
UDP S-Port	UDP 始点ポート
UDP D-Port	UDP 終点ポート
Action	マッチ時のアクション。DENY、SETPRIORITY、SENDCOS、SETTOS、SENDEPORT、SENDMIRROR、NODROP、SENDNONUNICASTTO-PORT、MOVEPRIOTOTOS、MOVETOSTOPRIO、SETIPDSCP がある

Port	マッチしたパケットの送出先ポート
New IP TOS	マッチしたパケットに設定する TOS 優先度値
New IP DSCP	マッチしたパケットに設定する DSCP 値
Priority	マッチしたパケットに設定する 802.1p ユーザープライオリティー
Syn/Ack/Fin	TCP 制御フラグ値

表 78:

関連コマンド

ADD SWITCH L3FILTER ENTRY (121 ページ)
 ADD SWITCH L3FILTER MATCH (127 ページ)
 DELETE SWITCH L3FILTER (145 ページ)
 DELETE SWITCH L3FILTER ENTRY (146 ページ)
 DISABLE SWITCH L3FILTER (173 ページ)
 ENABLE SWITCH L3FILTER (206 ページ)
 SET SWITCH L3FILTER ENTRY (260 ページ)
 SET SWITCH L3FILTER MATCH (265 ページ)

SHOW SWITCH LOOPDETECTION

カテゴリー：スイッチング / ポート

SHOW SWITCH LOOPDETECTION=LDF [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

ループガード (LDF 検出) 機能のグローバル設定と各ポートの状態を表示する。

パラメーター

PORT ポート番号。省略時および ALL 指定時はすべてのポートが対象となる。

入力・出力・画面例

```
Manager > show switch loopdetection=ldf
```

```
Switch Loop Detection
```

```
LDF Method
```

```
Action ..... Disable port
```

```
Secure ..... OFF
```

```
LDF interval ..... 120 sec
```

```
Port disabled timeout ..... 300 sec
```

Rx port	In loop	Disabled	Re-enabling in	Tx port	Debug mode
1	No	No	-	-	None
2	No	No	-	-	None
3	No	No	-	-	None
4	Yes	Yes	253	3	None
5	No	No	-	-	None
6	No	No	-	-	None
7	No	No	-	-	None
8	No	No	-	-	None
...					

Action	ループ検出時の動作（アクション）
Secure	古い LDF を破棄するかどうか
LDF interval	LDF の送信間隔
Port disable timeout	ループ検出時のアクションによってディセーブルまたはリンクダウン状態にされたポートが、復帰するまでの時間

Rx port	ポート番号
In loop	該当ポートでループを検出しているかどうか
Disabled	該当ポートが、ループ検出時のアクションによってディセーブルまたはリンクダウン状態にされているかどうか
Re-enabling in	該当ポートが、ループ検出時のアクションによってディセーブルまたはリンクダウン状態にされている場合、復帰するまでの残り時間（秒）
Tx port	該当ポートでループを検出している場合、受信した LDF の送信元ポート番号
Debug mode	未サポート

表 79:

関連コマンド

ENABLE SWITCH LOOPDETECTION (208 ページ)

ENABLE SWITCH PORT (211 ページ)

SET SWITCH LOOPDETECTION (268 ページ)

SHOW SWITCH LOOPDETECTION COUNTER (363 ページ)

SHOW SWITCH LOOPDETECTION COUNTER

カテゴリー：スイッチング / ポート

SHOW SWITCH LOOPDETECTION COUNTER [PORT={*port-list*|ALL}]

解説

ループガード（LDF 検出）機能に関するポートごとの統計情報と状態を表示する。

パラメーター

PORT ポート番号。省略時および ALL 指定時はすべてのポートが対象となる。

入力・出力・画面例

```

Manager > show switch loopdetection counter

Switch Loop Detection Counter
-----
LDF Method

Port          Date/Time          Tx          Rx          Status
-----
1              -              0           0          Enabled
2              -              0           0          Enabled
3              -              1           0          Enabled
4      28-Dec-2009 14:12:58      0           1          Enabled
5              -              0           0          Enabled
6              -              0           0          Enabled
...

```

Port	ポート番号
Date/Time	最後にループを検出した日時
Tx	LDF の送信数
Rx	LDF の受信数
Status	ループガード（LDF 検出）機能の有効・無効

表 80:

関連コマンド

ENABLE SWITCH LOOPDETECTION (208 ページ)

ENABLE SWITCH PORT (211 ページ)

SET SWITCH LOOPDETECTION (268 ページ)

SHOW SWITCH LOOPDETECTION (360 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 ..... Up
  UpTime ..... 00:01:11
  Port Media Type ..... ETHERNET CSMACD
  Configured speed/duplex ..... Autonegotiate
  Actual speed/duplex ..... 10 Mbps, half duplex
  Configured master/slave mode .. Not applicable
  Actual master/slave mode ..... Not applicable
  Acceptable Frame Types ..... Admit All Frames
  Broadcast rate limit ..... -
  Multicast rate limit ..... -
  DLF rate limit ..... -
  Ingress rate limit ..... -
  Egress rate limit ..... -
  Learn limit ..... -
  Intrusion action ..... Discard
  Current learned, lock state ... -, not locked
  Relearn ..... OFF
  Mirroring ..... None
  Is this port mirror port ..... No
  Enabled flow control(s) ..... Pause
  Send tagged pkts for VLAN(s) .. -
  Port-based VLAN ..... default (1)
```

```

Ingress Filtering ..... OFF
Trunk Group ..... -
STP ..... default
IGMP Filter ..... None
Max-groups/Joined ..... Undefined/0
IGMP Max-groups Action ..... Deny
Multicast filtering mode ..... (B) Forward all unregister groups
-----

```

Manager > show switch port=25

Switch Port Information

```

Port ..... 25
Description ..... -
Status ..... ENABLED
Link State ..... Down
UpTime ..... -
Port Media Type ..... ETHERNET CSMACD
Configured speed/duplex ..... Autonegotiate
Actual speed/duplex ..... -
Configured master/slave mode .. Autonegotiate
Actual master/slave mode ..... -
Acceptable Frame Types ..... Admit All Frames
Broadcast rate limit ..... -
Multicast rate limit ..... -
DLF rate limit ..... -
Ingress rate limit ..... -
Egress rate limit ..... -
Learn limit ..... -
Intrusion action ..... Discard
Current learned, lock state ... -, not locked
Relearn ..... OFF
Mirroring ..... None
Is this port mirror port ..... No
Enabled flow control(s) ..... Pause
Send tagged pkts for VLAN(s) .. -
Port-based VLAN ..... default (1)
Ingress Filtering ..... OFF
Trunk Group ..... -
STP ..... default
IGMP Filter ..... None
Max-groups/Joined ..... Undefined/0
IGMP Max-groups Action ..... Deny
Multicast filtering mode ..... (B) Forward all unregister groups

GBIC vendor name ..... AGILENT
GBIC part number ..... HFBR-5601
GBIC vendor SN ..... 0204010732020196
GBIC date code ..... 02040100
-----

```

Port	ポート番号
Description	ポート名称 (メモ)
Status	ポートのステータス。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、10Mbps、100Mbps、1000Mbps/half duplex、Full duplex で表示される
Actual speed/duplex	実際の通信モード
Configured master/slave mode	1000BASE-T ポートのマスター/スレーブ設定値。その他のポートの場合は、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
Broadcast rate limit	ブロードキャストパケットの 1 秒当たり最大受信数
Multicast rate limit	マルチキャストパケットの 1 秒当たり最大受信数
DLF rate limit	DLF (Destination Lookup Failure) パケットの 1 秒当たり最大受信数
Ingress rate limit	受信レート上限値 (帯域制限機能)
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) で表示される
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。None、Rx、TX、Both のいずれか。Rx、Tx、Both のときは、「frames mirrored to Port 24」のようにミラーポートも表示される。ミラーポートが設定されていないときは、「no Mirror Port set」と表示される

Is this port mirror port	ミラーポートに設定されているかどうか
Enabled flow control(s)	有効なフロー制御方式。Pause (IEEE 802.3x PAUSE) のみサポート
Send tagged pkts for VLAN(s)	ポートが所属するタグ VLAN 名 (VID)
Port-based VLAN	ポートが所属するポートベース VLAN 名 (VID)
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
Multicast filtering mode	未サポート
GBIC vendor name	GBIC ベンダー名 (GBIC ポートのみ)
GBIC part number	GBIC の製品名または型番 (GBIC ポートのみ)
GBIC vendor SN	GBIC のベンダーシリアル番号 (GBIC ポートのみ)
GBIC date code	GBIC の日付コード (GBIC ポートのみ)

表 81:

関連コマンド

SET SWITCH PORT (271 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. Fast Ethernet MAC counters:
Combined receive/transmit packets by size (octets) counters:
  64                               476 512 - 1023                0
  65 - 127                         485 1024 - MaxPktSz          0
  128 - 255                        99 1519 - 1522              0
  256 - 511                        14                          0

General Counters:
Receive                               Transmit
Octets                               92316 Octets                3520
Pkts                                 1019 Pkts                    55
FCSErrors                           0 FCSErrors                  0
MulticastPkts                       316 MulticastPkts           0
BroadcastPkts                       339 BroadcastPkts           0
PauseMACCtrlFrms                    0 PauseMACCtrlFrm           0
OversizePkts                        0 OversizePkts              0
Fragments                           0 Fragments                  0
Jabbers                             0 Jabbers                    0
MACControlFrms                      0
UnsupportOpcode                     0
AlignmentErrors                     0
OutOfRngeLenFld                     0
SymErDurCarrier                     0
CarrierSenseErr                     0

```

UndersizePkts	0		
	PauseCtrlFrms		0
	FrameWDeferdTx		0
	FrmWExcesDefer		0
	SingleCollsnFrm		0
	MultCollsnFrm		0
	LateCollsns		0
	ExcessivCollsns		0
	CollisionFrames		0
Layer 3 Counters:			
ifInUcastPkts	0	ifOutUcastPkts	0
ifInDiscards	0	ifOutErrors	0
ipInHdrErrors	0		
Miscellaneous Counters:			
DropEvents	0		
ifOutDiscards	0		
taggedPktTx	0		
totalPktTxAbort	0		
HW Multicasting Counters:			
TTL expired	0		
Bridged Frames	0		
Routed Frames	0		
Receive Drops	0		
Transmit Drops	0		

Combined receive/transmit packets by size (octets) counters	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 オクテット ~ 最大サイズ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	一般的な送受信カウンター
Receive	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
PauseMACCtl-Frms	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。
MACControlFrms	MAC 制御フレーム受信数 (PAUSE フレームと未サポートのフレームの合計)
Unsupport-Opcode	未サポートの MAC 制御フレーム受信数 (PAUSE フレーム以外の制御フレーム)
AlignmentErrors	アライメントエラーフレーム受信数。フレーム長がオクテットの整数倍でないフレームの数
OutOfRngeLenFld	長さフィールドの値が範囲外のフレーム受信数
SymErDurCarrier	不正なデータシンボルを持つフレームの受信数
CarrierSenseErr	フレーム間の搬送波にエラーがあった回数
UndersizePkts	アンダーサイズフレーム数。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	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	送信対象フレームのうち FCS エラーがあったものの数
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
PauseMACCtl-Frms	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。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送信数。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	ジャバーフレーム送信数。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。
PauseCtrlFrms	PAUSE フレーム数
FrameWDeferrd-Tx	キャリア検出による送信動作の延期が 1 回あった後、コリジョンを発生せずに正常送信されたフレーム数
FrmWExcesDefer	キャリア検出による送信動作の延期が続いたため送信が中止されたフレーム数
SingleCollsnFrm	1 回だけコリジョンを発生したフレームの数

MultCollsnFrm	2～15 回コリジョンを発生したフレームの数（レートコリジョンを含む）
LateCollsns	レートコリジョンを発生したフレームの数
ExcessivCollsns	16 回コリジョンを発生したため送信が中止されたフレームの数
CollisionFrames	コリジョンフレーム総数
Layer 3 Counters	レイヤー 3 スイッチングカウンター（CPU で処理されたフレームは除く）ifIn-UcastPkts
ifInDiscards	レイヤー 3 インターフェースで破棄された受信パケット数
ipInHdrErrors	IP ヘッダーエラーにより破棄された受信パケット数
ifOutUcastPkts	レイヤー 3 でスイッチングされた送信ユニキャストパケット数
ifOutErrors	レイヤー 3 インターフェースからの送出時に破棄されたパケット数
Miscellaneous Counters	その他のカウンター
DropEvents	受信ポートでとりこぼされたパケットの数
ifOutDiscards	エージングのため送信前に破棄されたパケットの数
taggedPktTx	VLAN タグ付きパケット送信数
totalPktTxAbort	送信されずに破棄されたレイヤー 2/3 パケット数
HW Multicasting Counters	マルチキャストパケット関連カウンター
TTL expired	生存時間（TTL）超過により破棄されたパケットの数
Bridged Frames	該当ポートで受信したパケットのうち、他ポートに L2 スイッチング（ブリッジング）されたものの数
Routed Frames	該当ポートで受信したパケットのうち、他ポートに L3 スイッチング（ルーティング）されたものの数。ただし、8748SL では、受信ポートと送信ポートが異なるポートグループ（「1～24、50」または「25～48、49」）になる場合、本カウンターはカウントされない。
Receive Drops	該当ポートで受信したパケットのうち、受信時に破棄されたものの数
Transmit Drops	該当ポートで受信したパケットのうち、送信時に破棄されたものの数

表 82:

関連コマンド

SET SWITCH PORT (271 ページ)

SHOW SWITCH COUNTER (348 ページ)

SHOW SWITCH PORT (365 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-list* | ALL}] **INTRUSION**

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。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=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 (271 ページ)

SHOW SWITCH QOS

カテゴリー：スイッチング / QoS

SHOW SWITCH QOS

解説

QoS 設定（802.1Q/802.1p タグフレームのユーザプライオリティ値とプライオリティキューのマッピング）設定を表示する。

入力・出力・画面例

```
Manager > show switch qos

Priority Level      QOS egress queue
-----
0 ..... 1
1 ..... 0
2 ..... 0
3 ..... 1
4 ..... 2
5 ..... 2
6 ..... 3
7 ..... 3
```

Priority level	受信フレームのユーザプライオリティ
QOS egress queue	プライオリティキュー番号（大きいほど優先度が高い）

表 83:

備考・注意事項

バージョン 2.5.3 より、本コマンドはSHOW QOS HWPRIORITY コマンドに置き換えられた。本コマンドも後方互換性のために残されている。表示形式は若干異なるが、内容は同じ。

関連コマンド

SET SWITCH QOS (274 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 ..... uplink
Speed ..... 1000 Mbps
Select ..... source and destination mac address
Ports ..... 25-26
-----
```

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。
Selection criterion	送出ポートの選択基準
Ports	所属ポート

表 84:

関連コマンド

- ADD SWITCH TRUNK (131 ページ)
- CREATE SWITCH TRUNK (136 ページ)
- DELETE SWITCH TRUNK (147 ページ)
- DESTROY SWITCH TRUNK (151 ページ)

SET SWITCH TRUNK (276 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。大文字小文字を区別しない)

解説

VLAN 情報を表示する。

パラメーター

VLAN VLAN 名または VLAN ID。省略時および ALL を指定した場合は、すべての VLAN の情報が表示される。

入力・出力・画面例

```
Manager > show vlan
```

```
VLAN Information
```

```
-----
Name ..... default
Identifier ..... 1
Status ..... static
Private VLAN ..... No
Admin Active ..... No
Protected ..... No
Untagged ports ..... 25-26
Tagged ports ..... None
Disabled Ports ..... None
Spanning Tree ..... default
Trunk ports ..... None
Mirror port ..... None
Attached to Bridge . No
```

```
Attachments:
```

Module	Protocol	Format	Discrim	MAC address
GARP	Spanning tree	802.2	42	-

```
-----
Name ..... white
Identifier ..... 10
Status ..... static
Private VLAN ..... No
Admin Active ..... No
```

SHOW VLAN

```

Protected ..... No
Untagged ports ..... 1-8
Tagged ports ..... None
Disabled Ports ..... None
Spanning Tree ..... default
Trunk ports ..... None
Mirror port ..... None
Attached to Bridge . No
Attachments:
Module          Protocol      Format      Discrim      MAC address
-----
GARP            Spanning tree  802.2       42           -
IP              IP            Ethernet    0800         -
IP              ARP           Ethernet    0806         -
-----

```

```

Name ..... orange
Identifier ..... 20
Status ..... static
Private VLAN ..... No
Admin Active ..... No
Protected ..... No
Untagged ports ..... 9-24
Tagged ports ..... None
Disabled Ports ..... None
Spanning Tree ..... default
Trunk ports ..... None
Mirror port ..... None
Attached to Bridge . No
Attachments:
Module          Protocol      Format      Discrim      MAC address
-----
GARP            Spanning tree  802.2       42           -
IP              IP            Ethernet    0800         -
IP              ARP           Ethernet    0806         -
-----

```

Manager > show vlan=apriv

VLAN Information

```

-----
Name ..... apriv
Identifier ..... 10
Status ..... static
Private VLAN ..... Yes
Admin Active ..... No
Protected ..... No
Untagged ports ..... 1-26
Tagged ports ..... None
Associations ..... Port only
Disabled Ports ..... None

```

```

Spanning Tree ..... default
Trunk ports ..... 25-26
Mirror port ..... None
Attached to Bridge . No
Attachments:
Module          Protocol          Format      Discrim      MAC address
-----
GARP             Spanning tree      802.2       42           -
-----

Private Uplink:
Uplink ports ..... 25
Uplink ports ..... 26

Private Groups:
Group ports ..... 1-8
Group ports ..... 9-16
Group ports ..... 17-24
-----

```

Name	VLAN 名
Identifier	VLAN ID
Status	VLAN のステータス (static のみ)
Private VLAN	マルチプル VLAN (Private VLAN) かどうか
Admin Active	未サポート
Protected	Protected VLAN (所属ポート間のレイヤー 2 通信が禁止されている) かどうか
Untagged ports	タグなしポート
Tagged ports	タグ付きポート
Disabled Ports	ディセーブル状態のポート
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
Attached to Bridge	未サポート
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	フレームフォーマット
Discrim	上記フレームフォーマットに対応したプロトコル ID
MAC Address	モジュールが使用する MAC アドレス
Uplink ports	アップリンクポート (Private VLAN)
Group ports	プライベートポート (Private VLAN)。グループごとに表示される

表 85:

関連コマンド

CREATE VLAN (138 ページ)

DESTROY VLAN (152 ページ)

SHOW VLAN DEBUG

カテゴリー：スイッチング / バーチャル LAN

SHOW VLAN DEBUG

解説

VLAN のデバッグオプションを表示する。

入力・出力・画面例

Manager > show vlan debug

Vlan	Enabled Debug Modes	Output	Timeout
Vlan1	PKT	16	NONE
Vlan	Enabled Debug Modes	Output	Timeout
Vlan1000	None		

VLAN	VLAN 名称。接頭辞「Vlan」に VLAN ID をつなげた形式で表示される。
Enabled Debug Modes	現在有効になっているデバッグオプション。PKT か None。
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 86:

関連コマンド

DISABLE VLAN DEBUG（180 ページ）

ENABLE VLAN DEBUG（214 ページ）