スイッチング

概要・基本設定 7
レイヤー 3 スイッチとしての設定手順 7
ポート 9
ポートの指定方法 9
基本コマンド 9
ポートトランキング 10
ポートミラーリング 11
基本設定 12
ポートセキュリティー 13
ポート帯域制限機能 16
トリガー 16
バーチャル LAN 19
VLAN の種類 19
ポートと VLAN 20
デフォルト VLAN 21
ポート VLAN 21
VLAN タギング 23
IP サブネット VLAN 26
プロトコル VLAN 28
MAC アドレス VLAN 29
リミテッドプロトコル VLAN 30
VLAN 間ルーティング 32
パケットストームプロテクション 34
スパニングツリープロトコル 35
基本設定 35
マルチプル STP ドメイン 36
スパニングツリーパラメーターの設定変更 37
フォワーディングデータベース 40
FDB エントリー 40
自動学習とダイナミックエントリー 41
スタティックエントリー 42
クラシファイア 44
クラシファイアの構成 44
基本設定 44

クラシファイアの使用 45
クラシファイア使用時の注意 46
ポリシーベース QoS 47
概要 47
構成要素 47
スイッチポート 48
QoS ポリシー 48
トラフィッククラス 49
フローグループ 49
クラシファイア 49
パケットの照合順序について 50
基本設定 53
QoS ポリシーとスイッチポート 53
トラフィッククラス 54
フローグループ 55
クラシファイア 57
詳細設定 57
帯域制御 57
DSCP フィールドの書き換え 62
RED アルゴリズム 62
設定例 64
最小帯域保証 64
DiffServ 67
ハードウェアパケットフィルター 74
基本動作 74
フィルターの構成 74
フィルター処理の流れ 75
設定手順 75
コマンド例 76
注意事項 79
DPORT 指定について 79
本体宛てのパケットと本体発のパケット 80
DVLAN、SVLAN について 80
包含関係にあるネットワークアドレスについて 81
802.1X 認証 83
概要 83
要件 84
基本設定 84
Authenticator 84
Supplicant 85
コマンドリファレンス編 86
機能別コマンド索引 86

ACTIVATE PORTAUTH PORT REAUTHENTICATE 90
ACTIVATE SWITCH PORT AUTONEGOTIATE 91
ACTIVATE SWITCH PORT LOCK 92
ADD QOS FLOWGROUP 93
ADD QOS POLICY 94
ADD QOS TRAFFICCLASS 95
ADD STP VLAN 96
ADD SWITCH FILTER 98
ADD SWITCH HWFILTER 100
ADD SWITCH TRUNK 102
ADD VLAN ADDRESS 103
ADD VLAN LIMITEDPROTOCOL 105
ADD VLAN PORT 107
ADD VLAN PROTOCOL 110
ADD VLAN SUBNET 113
CREATE CLASSIFIER 114
CREATE QOS FLOWGROUP 119
CREATE QOS POLICY 120
CREATE QOS RED 122
CREATE QOS TRAFFICCLASS 124
CREATE STP 126
CREATE SWITCH TRUNK 127
CREATE VLAN 128
DELETE QOS FLOWGROUP 132
DELETE QOS POLICY 133
DELETE QOS TRAFFICCLASS 134
DELETE STP VLAN 135
DELETE SWITCH FILTER 136
DELETE SWITCH HWFILTER 137
DELETE SWITCH TRUNK 139
DELETE VLAN ADDRESS 140
DELETE VLAN LIMITEDPROTOCOL 141
DELETE VLAN PORT 142
DELETE VLAN PROTOCOL 145
DELETE VLAN SUBNET 146
DESTROY CLASSIFIER 147
DESTROY QOS FLOWGROUP 148
DESTROY QOS POLICY 149
DESTROY QOS RED 150
DESTROY QOS TRAFFICCLASS 151
DESTROY STP 152
DESTROY SWITCH TRUNK 153

DESTROY VLAN 154
DISABLE PORTAUTH 155
DISABLE PORTAUTH DEBUG 156
DISABLE PORTAUTH PORT 157
DISABLE QOS DEBUG 158
DISABLE QOS VLANPRIORITYREMAPPING 159
DISABLE STP 160
DISABLE STP DEBUG 161
DISABLE STP PORT 162
DISABLE STP PORT DEBUG 163
DISABLE SWITCH AGEINGTIMER 164
DISABLE SWITCH DEBUG 165
DISABLE SWITCH HASH 166
DISABLE SWITCH LEARNING 167
DISABLE SWITCH MIRROR 168
DISABLE SWITCH PORT 169
DISABLE SWITCH PORT FLOW 170
DISABLE SWITCH STPFORWARD 171
DISABLE VLAN DEBUG 172
DISABLE VLAN STORMPROTECT 173
ENABLE PORTAUTH 174
ENABLE PORTAUTH DEBUG 175
ENABLE PORTAUTH PORT 178
ENABLE QOS DEBUG 181
ENABLE QOS VLANPRIORITYREMAPPING 182
ENABLE STP 183
ENABLE STP DEBUG 184
ENABLE STP PORT 185
ENABLE STP PORT DEBUG 186
ENABLE SWITCH AGEINGTIMER 187
ENABLE SWITCH DEBUG 188
ENABLE SWITCH HASH 189
ENABLE SWITCH LEARNING 190
ENABLE SWITCH MIRROR 191
ENABLE SWITCH PORT 192
ENABLE SWITCH PORT FLOW 193
ENABLE SWITCH STPFORWARD 194
ENABLE VLAN DEBUG 195
ENABLE VLAN STORMPROTECT 196
PURGE PORTAUTH PORT 197
PURGE QOS 198
PURGE STP 199

RESET PORTAUTH PORT 200
RESET STP 201
RESET SWITCH 202
RESET SWITCH PORT 203
SET CLASSIFIER 204
SET PORTAUTH PORT 207
SET PORTAUTH USERNAME 210
SET QOS FLOWGROUP 212
SET QOS POLICY 213
SET QOS PORT 214
SET QOS RED 215
SET QOS TRAFFICCLASS 216
SET QOS VLANREMAP 218
SET STP 219
SET STP PORT 221
SET SWITCH AGEINGTIMER 223
SET SWITCH MIRROR 224
SET SWITCH PORT 225
SET SWITCH TRUNK 227
SET VLAN 228
SET VLAN PORT 229
SHOW CLASSIFIER 230
SHOW PORTAUTH 234
SHOW PORTAUTH COUNTER 236
SHOW PORTAUTH PORT 239
SHOW PORTAUTH TIMER 244
SHOW QOS FLOWGROUP 246
SHOW QOS POLICY 248
SHOW QOS RED 250
SHOW QOS TRAFFICCLASS 252
SHOW QOS VLANPRIORITYREMAPPING 254
SHOW STP 255
SHOW STP COUNTER 258
SHOW STP DEBUG 260
SHOW STP PORT 261
SHOW SWITCH 263
SHOW SWITCH COUNTER 265
SHOW SWITCH DEBUG 268
SHOW SWITCH FDB 269
SHOW SWITCH FILTER 272
SHOW SWITCH HWFILTER 274
SHOW SWITCH PORT 276

SHOW SWITCH PORT COUNTER 280
SHOW SWITCH PORT INTRUSION 283
SHOW SWITCH TRUNK 284
SHOW VLAN 285
SHOW VLAN DEBUG 289
SHOW VLAN PORT 290

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（128 ページ）で、ポートの割り当ては ADD VLAN PORT コマンド（107 ページ）で行います。

   ```
   CREATE VLAN=white VID=10 ↵
   CREATE VLAN=orange VID=20 ↵
   ADD VLAN=white PORT=1-6 ↵
   ADD VLAN=orange PORT=7-12 ↵
   ```

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 197 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 125 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 129 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（192 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（169 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（225 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（91 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（203 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（276 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（280 ページ）を使います。

```
SHOW SWITCH PORT=12 COUNTER ↵
```

■ ポートの統計カウンターをクリアするには RESET SWITCH PORT コマンド（203 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。トランクグループは、VLAN 内でも単一ポートとして認識されます。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。
作成できるトランクグループの数は最大 16、トランクグループの所属ポート数も最大 16 となります。グループ内のポートは隣接していなくてもかまいません。
ポートトラ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「quad1000」を作成します。グループ名は自由につけられます。

   ```
   CREATE SWITCH TRUNK=quad1000 ↵
   ```

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=quad1000 PORT=1-4 ↵
   ```

基本設定は以上です。

✎ トランクグループの所属ポートは、すべて同一の VLAN 設定である必要があります。すべての所属ポートは、同一 VLAN の所属で、同一のタグ設定（TAGGED か UNTAGGED）にする必要があります。VLAN への追加・削除は、トランクグループの所属ポートすべてを一単位として行ってください。所属ポートのタグ設定を変更するときも同様です。

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

✎ ポートトランキングの設定は、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。

■ トランクグループの情報は SHOW SWITCH TRUNK コマンド（284 ページ）で確認できます。

```
SHOW SWITCH TRUNK=quad1000 ↵
```

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

■ トランクグループ内のどのポートからパケットを送出するかは、L2、L3、L4 ヘッダーの情報に基づいて決定されます。ENABLE SWITCH HASH コマンド（189 ページ）、DISABLE SWITCH HASH コマンド（166 ページ）を使うと、送出ポート決定に使うヘッダー情報を制御できます。
たとえば、L4 のヘッダー情報を使わないようにするには、次のようにします。デフォルトでは、L2 と L4 のヘッダー情報を使って送出ポートを決定します。

```
DISABLE SWITCH HASH=L4 ↵
```

■ 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（139 ページ）を使います。

```
DELETE SWITCH TRUNK=quad1000 PORT=4 ↵
```

■ トランクグループを削除するには DESTROY SWITCH TRUNK コマンド（153 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（139 ページ）で所属ポートを削除してください。

```
DELETE SWITCH TRUNK=quad PORT=ALL ↵
DESTROY SWITCH TRUNK=quad ↵
```

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。

✎ 本製品は送信パケットのミラーリングには対応していません。

基本設定

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

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（224 ページ）を実行します。

   ```
   DELETE VLAN=somevlan PORT=1 ↵
   ```

   SET SWITCH MIRROR コマンド（224 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 で受信した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=RX ↵
   ```

   ✎ 本製品は送信パケットのミラーリングには対応していません。

   ✎ 複数のポートをミラーしたいときは、SET SWITCH PORT コマンド（225 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。

   ✎ 不正なパケット（エラーパケットなど）はミラーされません。

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（263 ページ）を実行します。ミ

ラーポートはSHOW VLAN コマンド（285 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（276 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（168 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（224 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（225 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（224 ページ）を実行した時点で、ミラーポートはいずれのVLAN にも所属していない状態となります。

ポートセキュリティー

ポートセキュリティーは、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（225 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みなし、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（225 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。
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（225 ページ）を使います。たとえば、ポート11 のMAC アドレス学習数の上限を20 個、アクションをDISABLE に設定するには次のようにします。

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

SET SWITCH PORT コマンド（225 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（225 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ー）、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ー）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ーが有効なポートでは、802.1X 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」なものと見なされ、INTRUSIONACTION で指定したアクションが実行されます。
たとえば、アクションが「DISABLE」に設定されているときに不正パケットを受信すると、トラップ送信とポートのディセーブルが実行され、コンソール画面に次のように表示されます。

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

Intrusion event.  Disabling port 11
```

■ 学習済みのアドレスを確認するには、SHOW SWITCH FILTER コマンド（272 ページ）を使います。ポートセキュリティーがオンのポートで学習されたアドレスは、Source 欄に「Learn」と表示されます。

```
SHOW SWITCH FILTER ↵
SHOW SWITCH FILTER PORT=11 ↵
```

■ ポートセキュリティーの設定状況は SHOW SWITCH PORT コマンド（276 ページ）で確認できます。「Learn limit」欄には現在設定されている上限が、「Intrusion action」欄には不正パケット受信時のアクションが表示されます。また、「Current learned, lock state」欄には、現在までに学習したアドレスの数と、ポートがロック（これ以上学習しない状態のこと）されているかどうかが表示されます。「Relearn」欄には、LEARN パラメーターを設定した場合に、学習した MAC アドレスがエージングの対象であるかどうかが表示されます。

```
SHOW SWITCH PORT ↵
SHOW SWITCH PORT=11 ↵
```

■ 不正とみなされた MAC アドレスは SHOW SWITCH PORT INTRUSION コマンド（283 ページ）で確認できます。

```
SHOW SWITCH PORT INTRUSION ↵
SWOW SWITCH PORT=11 INTRUSION ↵
```

■ 学習済みアドレス数が上限に達する前に手動でポートをロックするには ACTIVATE SWITCH PORT LOCK コマンド（92 ページ）を使います。あらかじめ SET SWITCH PORT コマンド（225 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ーがオンのポート（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（98 ページ）に LEARN オプションを付けて実行します。すでに上限に達している場合であっても、本コマンドで手動追加した場合は上限値が引き上げられます。

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

✎ LEARN オプションを付け忘れると通常のスタティックエントリーとなり、ポートセキュリティー機能における「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ーの削除は DELETE SWITCH FILTER コマンド（136 ページ）で行います。ENTRY 番号は SHOW SWITCH FILTER コマンド（272 ページ）で確認してください。

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

■ ポートのロックを解除する、あるいはポートセキュリティー機能をオフにするには、SET SWITCH PORT コマンド（225 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ーがオンのときに学習されたエントリーは、システムの再起動とともにデータベースから削除されます。

```
SET SWITCH PORT=11 LEARN=0 ↵
```

■ ポートセキュリティー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（192 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（225 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ーをオフにすると、イネーブルに戻ります。

```
Manager > enable switch port=11

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

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

■ ポートセキュリティーの設定（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 133 ページ）によって保存されます。

ポート帯域制限機能

本製品は、スイッチポートごとに送信レートを制限することができます。

✎ ポート帯域制限機能は、ポリシーベース QoS の帯域制御機能と同時に使用しないでください。

帯域制限の設定は SET SWITCH PORT コマンド（225 ページ）の EGRESSLIMIT（送信レート）パラメーターで行います。

■ ポート 1 の送信レートを 500Mbps に制限するには、次のように指定します。EGRESSLIMIT の単位は Kbps です。

```
SET SWITCH PORT=1 EGRESSLIMIT=500000 ↵
```

✎ EGRESSLIMIT パラメーターに指定できる値の範囲は 0〜16000063Kbps ですが、64 の倍数になるよう切り捨てが行われるので注意してください。たとえば、EGRESSLIMIT に 63 を指定しても、64 に満たないため切り捨てにより 0 として扱われます。

✎ EGRESSLIMIT=0 は、EGRESSLIMIT=NONE（制限なし）と同じ意味になります。

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

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

■ ポート帯域制限機能の設定状況は SHOW SWITCH PORT コマンド（276 ページ）で確認できます。「Egress rate limit」をご覧ください。

トリガー

トリガー機能を使用すると、スイッチポートのリンクアップ、リンクダウン時に任意のスクリプトを実行させることができます。
スイッチポートのリンクアップ、リンクダウンは、スイッチングモジュール固有のモジュールトリガーを使って捕捉します。
CREATE TRIGGER MODULE コマンド（「運用・管理」の 147 ページ）、SET TRIGGER MODULE コマンド（「運用・管理」の 294 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 233 ページ）を使って管理者で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んでいるものと仮定します。IP の設定については「IP」の章を、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
```

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ちますが、未学習の宛先 MAC アドレスを持つユニキャストパケットと、マルチキャスト / ブロードキャストパケットは全ポートに出力します。VLAN を作成して、頻繁に通信を行うホスト同士をグループ化することにより、不要なトラフィックの影響を受ける範囲を限定し、帯域をより有効に活用できるようになります。

VLAN の種類

本製品がサポートする VLAN は次の 5 種類です。

- ポート VLAN（タグ VLAN を含む）
- IP サブネット VLAN
- プロトコル VLAN
- MAC アドレス VLAN
- リミテッドプロトコル VLAN

ただし、すべての種類を同時に使用することはできません。使用可能な VLAN 種別に関する基本ルールは次のとおりです。

- ポート VLAN（タグ VLAN を含む）はつねに使用できます。
- 残りの 4 種類は次の 2 グループに分けられます。同時に使用できるのはどちらか 1 グループのみです。
  - IP サブネット VLAN、プロトコル VLAN
  - MAC アドレス VLAN、リミテッドプロトコル VLAN
- どの種類の VLAN を使用できるかは、ポート VLAN 以外の VLAN を最初に作成したときに決まります。ご購入時のように VLAN default だけが定義されている状態では、使用可能な VLAN 種別は未確定です。
  - 最初に作成したポート VLAN 以外の VLAN が IP サブネット VLAN かプロトコル VLAN ならば、使用可能な VLAN 種別は「IP サブネット VLAN、プロトコル VLAN、ポート VLAN」となります。
  - 最初に作成したポート VLAN 以外の VLAN が MAC アドレス VLAN かリミテッドプロトコル VLAN ならば、使用可能な VLAN 種別は「MAC アドレス VLAN、リミテッドプロトコル VLAN、ポート VLAN」となります。
- 使用できる VLAN の種類が確定したあとで、異なるグループの種類の VLAN を作成することはできません。つまり、IP サブネット VLAN と MAC アドレス VLAN を同時に使用することはできません。使用できる VLAN の種類を変更するには、VLAN default 以外の VLAN をすべて削除し、使用可能な VLAN 種別を「未確定」な状態に戻す必要があります。
- 現在使用可能な VLAN 種別は、SHOW SWITCH コマンド（263 ページ）で表示される「VLAN classification」欄で確認できます。「IP subnet, Protocol, Port」は「IP サブネット VLAN、プロトコル VLAN、ポート VLAN」を使用可能、「MAC address, Limited Protocol, Port」は「MAC アドレス VLAN、リミテッドプロトコル VLAN、ポート VLAN」を使用可能なことを示します。「To

be defined」は、ポート VLAN 以外の VLAN をまだ作成していないため、使用できる VLAN 種別が確定していないことを示します。

ポートと VLAN

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

- ポート VLAN（タグなしポート）：1 つの VLAN にだけ所属できる
- ポート VLAN（タグ付きポート）：複数の VLAN に所属できる
- IP サブネット VLAN（タグなしポート）：複数の VLAN に所属できる
- プロトコル VLAN（タグなしポート）：複数の VLAN に所属できる
- MAC アドレス VLAN（タグなしポート）：複数の VLAN に所属できる
- リミテッドプロトコル VLAN（タグなしポート）：複数の VLAN に所属できる

ただし、上記の基本ルールには、「VLAN の種類」で述べた「同時に使用可能な VLAN 種別」の制限が加わります。したがって、あるポートを IP サブネット VLAN と MAC アドレス VLAN に所属させることはできません。

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

■ ポートが複数の VLAN に所属している場合、受信パケットの所属先は次の基準にしたがって決定されます。スイッチポートがどの VLAN に所属しているかは、SHOW VLAN PORT コマンド（290 ページ）で確認できます。

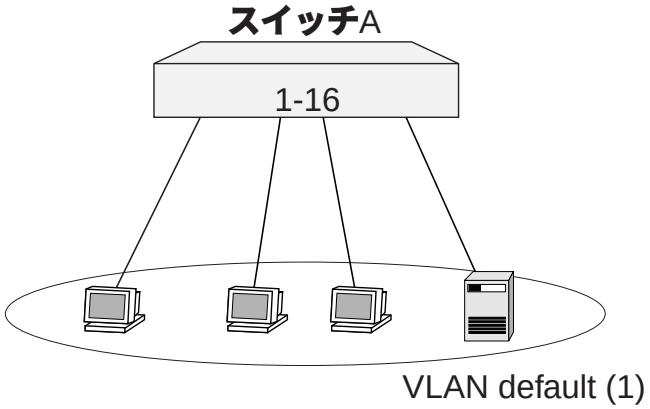
- 使用可能な VLAN 種別が「IP サブネット VLAN、プロトコル VLAN、ポート VLAN」のとき
  - パケットが IP サブネット VLAN のサブネット範囲に合致する場合、IP サブネット VLAN の所属と判断します。
  - パケットがプロトコル VLAN の対象プロトコルに合致する場合、プロトコル VLAN の所属と判断します。
  - 上記の基準に当てはまらないパケットは、ポート VLAN の所属と判断します。
- 使用可能な VLAN 種別が「MAC アドレス VLAN、リミテッドプロトコル VLAN、ポート VLAN」のとき
  - パケットが MAC アドレス VLAN のメンバーアドレスに合致する場合、MAC アドレス VLAN の所属と判断します。
  - パケットがリミテッドプロトコル VLAN の対象プロトコルに合致する場合、リミテッドプロトコル VLAN の所属と判断します。
  - 上記の基準に当てはまらないパケットは、ポート VLAN の所属と判断します。
- 使用可能な VLAN 種別が「未確定」のときは、システム上にポート VLAN しか存在しないため、すべてのパケットがポート VLAN の所属になります。

以下の各節では、上記をふまえ、最初にもっとも基本的な VLAN であるポート VLAN とタグ VLAN につ

いて説明したのち、その他の VLAN について簡単に説明します。

デフォルト VLAN

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



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

- VLAN default は削除できません。
- ポートが VLAN default にしか所属していない場合、同ポートを VLAN default から削除することはできません。ただし同ポートを、ユーザー定義のポート VLAN にタグなしポートとして割り当てると、該当ポートは自動的に VLAN default から削除されます。
- ユーザー定義 VLAN のポート VLAN メンバーからタグなしポートを削除すると、該当ポートは自動的に VLAN default のタグなしポートに戻ります。
- VLAN default は「default STP」以外の STP ドメインに参加できません。
- VLAN default の VLAN 種別（TYPE）は、ポート VLAN 以外の VLAN を最初に作成したときに決まります。最初に作成したポート VLAN 以外の VLAN が IP サブネット VLAN かプロトコル VLAN ならば、VLAN default は IP サブネット VLAN になります。また、最初に作成したポート VLAN 以外の VLAN が MAC アドレス VLAN かリミテッドプロトコル VLAN ならば、VLAN default は MAC アドレス VLAN になります。

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（128 ページ）を使います。VLAN 作成時には、VLAN 名と VLAN ID（VID）を割り当てる必要があります。VLAN 名は任意の文字列（ただし、先頭文字は数字以外）、VID は 2〜4090 の範囲の任意の数値です（1 は VLAN default に割り

当てられているため使用できません)。3 つの VLAN、A（VID=10)、B（VID=20)、C（VID=30）を作成するには次のようにします。

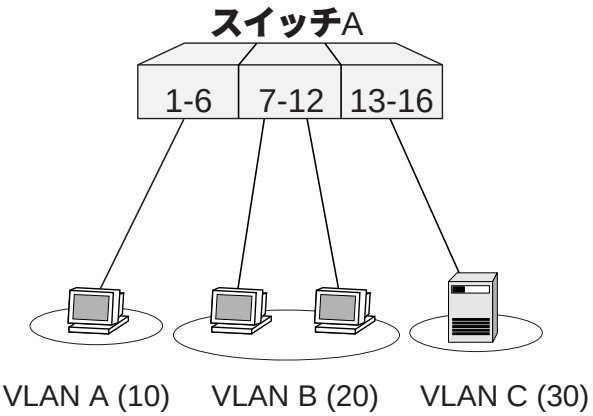
```
CREATE VLAN=A VID=10 ↵
CREATE VLAN=B VID=20 ↵
CREATE VLAN=C VID=30 ↵
```

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

2. VLAN を作成したら、ADD VLAN PORT コマンド（107 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 1〜6 を、VLAN B にポート 7〜12 を、VLAN C にポート 13〜16 を割り当てます。

```
ADD VLAN=A PORT=1-6 ↵
ADD VLAN=B PORT=7-12 ↵
ADD VLAN=C PORT=13-16 ↵
```

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 には所属ポートが 1 つもない状態になります。



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

■ VLAN の情報を確認するには、SHOW VLAN コマンド（285 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（142 ページ）を使います。たとえば、ポート 5 と 6 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=5-6 ↵
```

■ VLAN を削除するには、DESTROY VLAN コマンド（154 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。

VLAN タギング

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

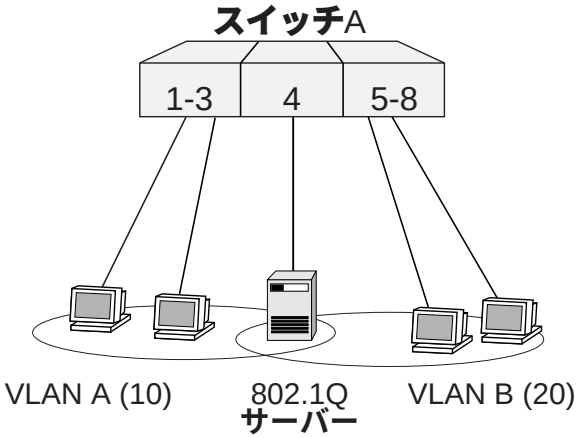
✎ VLAN 内に、複数 VLAN に所属するポートが 1 つでも含まれている場合、その VLAN を default 以外の STP ドメインに参加させることはできません。そうした VLAN では、default STP を使ってください（VLAN はデフォルトで default STP 所属となります）。

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 からも 802.1Q 対応サーバーにアクセスできるようにします。

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

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（107 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

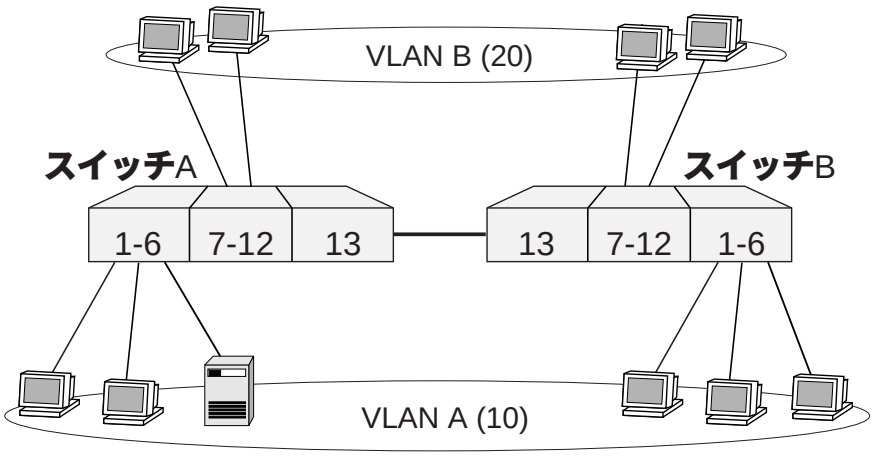
表 2:

■ 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（142 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 13 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. VLANA、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 1〜6 はタグを使わない通常のポートに設定し、ポート 13 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（107 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=1-6 ↵
   ADD VLAN=A PORT=13 FRAME=TAGGED ↵
   ```

3. VLAN B にポートを追加します。ポート 7〜12 はタグを使わない通常のポートに設定し、ポート 13 はタグを使用するポートとして設定します。

   ```
   ADD VLAN=B PORT=7-12 ↵
   ADD VLAN=B PORT=13 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いてもかまい

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 13 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 13 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（142 ページ）を使って、ポート 13 を VLAN default から削除します。

```
DELETE VLAN=default PORT=13 ↵
```

IP サブネット VLAN

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

✎ IP サブネット VLAN の対象となるプロトコルは IP だけです。ARP パケットのグルーピングにはプロトコル VLAN を利用してください。

■ IP サブネット VLAN を作成するには、CREATE VLAN コマンド（128 ページ）の TYPE パラメーターに SUBNET を指定します。また、SUBNET および MASK パラメーターでサブネットの範囲を指定します。MASK パラメーターを省略した場合は、SUBNET パラメーターで指定したアドレスのクラス標準マスクが使用されます。

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

また、サブネットの範囲は ADD VLAN SUBNET コマンド（113 ページ）を使って後から追加することもできます。

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

✎ 作成した VLAN の種類を変更することはできません。変更したい場合は、DESTROY VLAN コマンド（154 ページ）で VLAN を削除したのち、別の種類で新規作成してください。

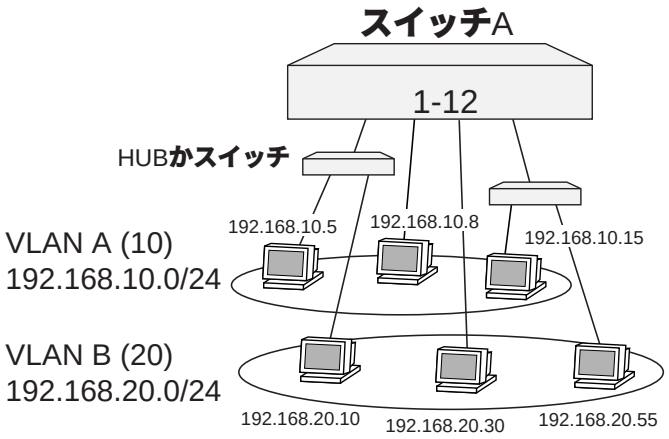
✎ IP サブネット VLAN にサブネット範囲を複数設定する場合、および、IP サブネット VLAN を複数作成する場合、サブネットのアドレス範囲が重複するような設定はできません。たとえば、VLAN A のサブネット範囲を「172.16.10.0/24」（172.16.10.0〜172.16.10.255）に設定した場合、VLAN B のサブネット範囲として「172.16.0.0/16」（172.16.0.0〜172.16.255.255）を指定することはできません。

■ IP サブネット VLAN を作成し、サブネットの範囲を指定したら、ADD VLAN PORT コマンド（107 ページ）でタグなしポートを IP サブネット VLAN に関連付けます。

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

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

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




```
CREATE VLAN=A VID=10 TYPE=SUBNET SUBNET=192.168.10.0 MASK=255.255.255.0 ↵
CREATE VLAN=B VID=20 TYPE=SUBNET SUBNET=192.168.20.0 MASK=255.255.255.0 ↵
ADD VLAN=A PORT=1-12 SUBNET=192.168.10.0 ↵
ADD VLAN=B PORT=1-12 SUBNET=192.168.20.0 ↵
```

これにより、ポート 1〜12 で受信したパケットのうち、始点アドレスが 192.168.10.0 / 24 の範囲におさまるものは VLAN A、192.168.20.0 / 24 の範囲におさまるものは VLAN B の所属として扱われます。
また、その他のパケット（始点アドレスが上記以外、あるいは、IP でないパケット）は、受信ポートが所属しているポート VLAN の所属になります。上記の例で VLAN A、B 以外にユーザー定義の VLAN がないと仮定すると、その他のパケットは VLAN default の所属として扱われます。
ポート 1〜12 以外のポートにも機器が接続されている場合、それらの機器が送信したパケットは VLAN default 所属となるため、ポート 1〜12 にもパケットが出力される可能性があります。これを避けるには、ポート 1〜12 を VLAN default 以外のポート VLAN に所属させるか、ポート 1〜12 以外を VLAN default 以外のポート VLAN に所属させます。前者の設定は次のとおりです。

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

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

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

詳細は「VLAN 間ルーティング」をご覧ください。

プロトコル VLAN

プロトコル VLAN では、受信したタグなしパケットの L2 プロトコルタイプフィールドに特定の値が格納されているパケットを VLAN メンバーと見なします。プロトコル VLAN は、他の種類の VLAN（ポート VLAN など）と組み合わせて使うケースがよくあります。

■ プロトコル VLAN を作成するには、CREATE VLAN コマンド（128 ページ）の TYPE パラメーターに PROTOCOL を指定します。また、PROTOCOL パラメーターでプロトコルを指定します。プロトコルは、定義済みのプロトコル名（ADD VLAN PROTOCOL コマンド（110 ページ）の表を参照）か 16 進表記（「0x」を前置）のプロトコル番号で指定します。
プロトコル名で指定する場合は次のようにします。

```
CREATE VLAN=nw VID=100 TYPE=PROTOCOL PROTOCOL="IPX 802.2" ↵
```

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

```
CREATE VLAN=nw VID=100 TYPE=PROTOCOL PROTOCOL=0xe0 ↵
```

また、プロトコルは ADD VLAN PROTOCOL コマンド（110 ページ）を使って後から追加することもできます。

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

✎ 作成した VLAN の種類を変更することはできません。変更したい場合は、DESTROY VLAN コマンド（154 ページ）で VLAN を削除したのち、別の種類で新規作成してください。

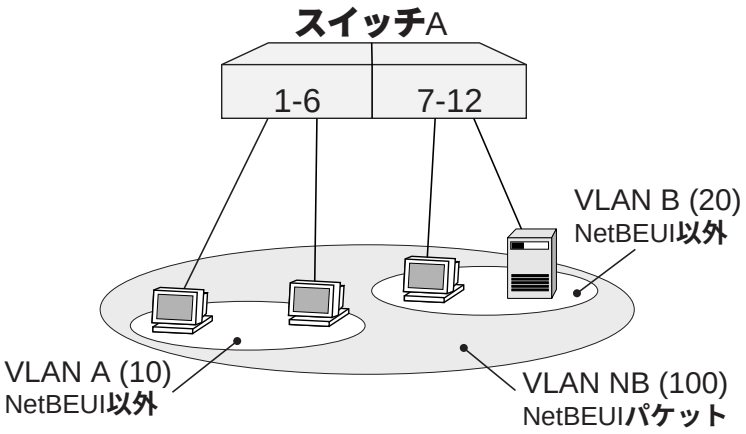
■ プロトコル VLAN を作成し、対象プロトコルを指定したら、ADD VLAN PORT コマンド（107 ページ）でタグなしポートをプロトコル VLAN に関連付けます。

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

これにより、ポート 1〜6 で受信したパケットのうち、フレームタイプ 802.2 の IPX パケット（DSAP =

0xe0）が VLAN nw の所属として扱われます。

■ 2 つのポート VLAN A と B を包含するプロトコル VLAN NB を作成します。ポート 1〜12 で受信した NetBEUI パケットは VLAN NB 所属と見なされます。それ以外のパケットは、受信ポートが 1〜6 なら VLAN A、7〜12 なら VLAN B 所属として扱われます。




```
CREATE VLAN=A VID=10 ↵
CREATE VLAN=B VID=20 ↵
CREATE VLAN=NB VID=100 TYPE=PROTOCOL PROTOCOL=NetBEUI ↵
ADD VLAN=A PORT=1-6 ↵
ADD VLAN=B PORT=7-12 ↵
ADD VLAN=NB PORT=1-12 PROTOCOL=NetBEUI ↵
```

MAC アドレス VLAN

MAC アドレス VLAN では、受信したタグなしパケットの送信元 MAC アドレスが特定のアドレスだった場合に、これを VLAN メンバーと見なします。

■ MAC アドレス VLAN を作成するには、CREATE VLAN コマンド（128 ページ）の TYPE パラメーターに MACADDRESS を指定します。また、ADDRESS（および ENDADDRESS）パラメーターでメンバーとみなす MAC アドレスを指定します。MAC アドレスは「xx-xx-xx-xx-xx-xx」の形式で、ユニキャストアドレスのみ有効です。アドレスを 1 個だけ指定するときは、ADDRESS パラメーターに指定します。連続するアドレスを一度に指定するには、ADDRESS に先頭アドレスを、ENDADDRESS に終了アドレスを指定します。
アドレスを 1 個だけ指定する場合は次のようにします。

```
CREATE VLAN=private VID=10 TYPE=MACADDRESS ADDRESS=00-00-f4-12-34-56 ↵
```

連続するアドレスを複数指定する場合は次のようにします。

```
CREATE VLAN=private VID=10 TYPE=MACADDRESS ADDRESS=00-00-f4-12-34-56
  ENDADDRESS=00-00-f4-12-34-ff ↵
```

✎ アドレスを範囲指定する場合、1 回のコマンド実行で追加できるアドレスは 1024 個までです。必要であれば複数回コマンドを実行してください。

また、MAC アドレスは ADD VLAN ADDRESS コマンド（103 ページ）を使って後から追加することもできます。

```
CREATE VLAN=private VID=10 TYPE=MACADDRESS ↵
ADD VLAN=private ADDRESS=00-00-f4-ab-cd-ef ↵
ADD VLAN=private ADDRESS=00-00-f4-ff-00-00 ENDADDRESS=00-00-f4-ff-03-ff ↵
```

✎ 作成した VLAN の種類を変更することはできません。変更したい場合は、DESTROY VLAN コマンド（154 ページ）で VLAN を削除したのち、別の種類で新規作成してください。

■ MAC アドレス VLAN を作成し、メンバーアドレスを指定したら、ADD VLAN PORT コマンド（107 ページ）でタグなしポートを MAC アドレス VLAN に関連付けます。ADDRESS パラメーターには通常 ALL を指定して、すべての MAC アドレスが対象になるようにします。

```
ADD VLAN=private PORT=1-6 ADDRESS=ALL ↵
```

これにより、ポート 1〜6 で受信したパケットのうち、送信元 MAC アドレスが登録済みのメンバーアドレスと合致するパケットが VLAN private の所属として扱われます。

リミテッドプロトコル VLAN

リミテッドプロトコル VLAN は、指定できるプロトコルが IP、IPX、それ以外の原則 3 種に限定されたプロトコル VLAN です。通常のプロトコル VLAN を併用できない MAC アドレス VLAN 使用時に使います。

■ リミテッドプロトコル VLAN を作成するには、CREATE VLAN コマンド（128 ページ）の TYPE パラメーターに LIMITEDPROTOCOL を指定します。また、LIMITEDPROTOCOL パラメーターでプロトコルを指定します。LIMITEDPROTOCOL には、定義済みのプロトコル名「IP」、「IPX」、「OTHER」か、プロトコル番号「0x0800」、「0xE0」、「0x8137」、「0xFFFF」、「0x0000008137」を指定します。IPX か OTHER を指定した場合は、ENCAPSULATION パラメーターでフレームタイプも指定する必要があります。

✎ 定義済みのプロトコル名「IP」に ARP は含まれません。ARP は「OTHER」に含まれています。

Ethernet2 の IP パケットだけを対象とするリミテッドプロトコル VLAN「ipp」を作成します。

```
CREATE VLAN=ipp VID=20 TYPE=LIMITEDPROTOCOL LIMITEDPROTOCOL=IP ↵
```

または

```
CREATE VLAN=ipp VID=20 TYPE=LIMITEDPROTOCOL LIMITEDPROTOCOL=0x0800 ↵
```

すべての IPX パケットを対象とするリミテッドプロトコル VLAN「allipx」を作成します。

```
CREATE VLAN=allipx VID=30 TYPE=LIMITEDPROTOCOL LIMITEDPROTOCOL=IPX
  ENCAPSULATION=ALL ↵
```

また、プロトコルは ADD VLAN LIMITEDPROTOCOL コマンド（105 ページ）を使って後から追加することもできます。

```
CREATE VLAN=ipp VID=20 TYPE=LIMITEDPROTOCOL ↵
ADD VLAN=ipp LIMITEDPROTOCOL=IP ↵
```

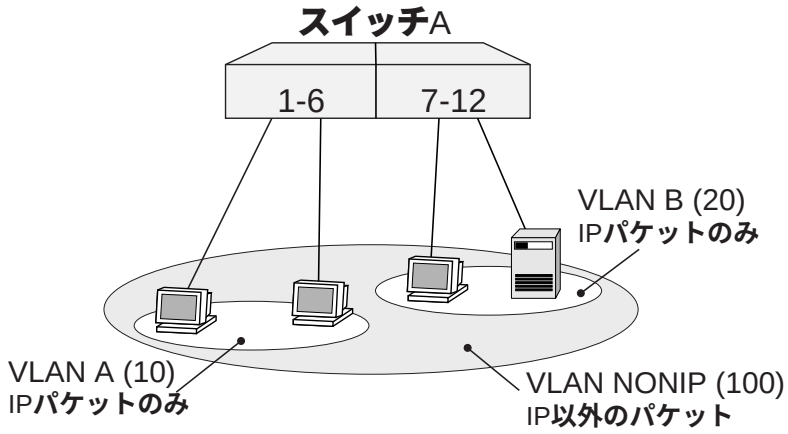
✎ 作成した VLAN の種類を変更することはできません。変更したい場合は、DESTROY VLAN コマンド（154 ページ）で VLAN を削除したのち、別の種類で新規作成してください。

■ リミテッドプロトコル VLAN を作成し、対象プロトコルを指定したら、ADD VLAN PORT コマンド（107 ページ）でタグなしポートをリミテッドプロトコル VLAN に関連付けます。

```
ADD VLAN=ipp PORT=1-6 LIMITEDPROTOCOL=IP ↵
```

これにより、ポート 1〜6 で受信したパケットのうち、IP パケット（Ethertype = 0x0800）が VLAN ipp の所属として扱われます。

■ リミテッドプロトコル VLAN を使って、IP とそれ以外のプロトコル（OTHER）を分ける場合は、IP 用の VLAN を単なるポート VLAN とせず、「LIMITEDPROTOCOL=IP」を明示的に指定したリミテッドプロトコル VLAN にしてください。



```
CREATE VLAN=A VID=10 TYPE=LIMITEDPROTOCOL ↵
CREATE VLAN=B VID=20 TYPE=LIMITEDPROTOCOL ↵
CREATE VLAN=NONIP VID=100 TYPE=LIMITEDPROTOCOL ↵
ADD VLAN=A PORT=1-6 LIMITEDPROTOCOL=IP ↵
ADD VLAN=B PORT=7-12 LIMITEDPROTOCOL=IP ↵
ADD VLAN=NONIP PORT=1-12 LIMITEDPROTOCOL=OTHER ↵
```

VLAN A、B の設定を次のようにすると（通常のポート VLAN として設定すると）、VLAN 間の IP 通信ができなくなりますのでご注意ください。

```
CREATE VLAN=A VID=10 ↵
CREATE VLAN=B VID=20 ↵
CREATE VLAN=NONIP VID=100 TYPE=LIMITEDPROTOCOL ↵
ADD VLAN=A PORT=1-6 ↵
ADD VLAN=B PORT=7-12 ↵
ADD VLAN=NONIP PORT=1-12 LIMITEDPROTOCOL=OTHER ↵
```

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=1-6 ↵
   ADD VLAN=B PORT=7-12 ↵
   ADD VLAN=C PORT=13-16 ↵
   ```

3. IP を使用するため、IP モジュールを有効にします。

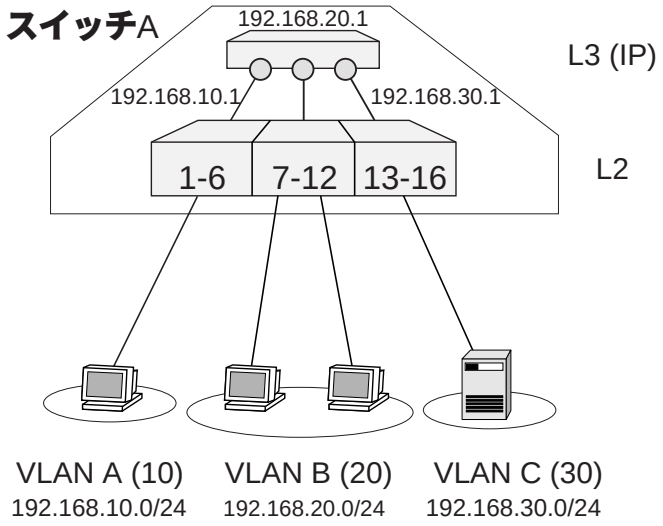
   ```
   ENABLE IP ↵
   ```

4. 各 VLAN（VLAN インターフェース）に IP アドレスを割り当てます。IP アドレスの設定は ADD IP

INTERFACE コマンド（「IP」の 125 ページ）で行います。

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

設定は以上です。
これにより、VLAN 間で IP がルーティングされるようになります。VLAN 間ルーティングは、同じプロトコルのレイヤー 3 インターフェースを 2 つ作成した時点で自動的に有効になります。
次の図は、この状態を概念的に示したものです。VLAN 分けにより分割された仮想的なスイッチ 3 台の上位に、仮想的なルーターを設置したものと考えることができます。実際にはこれらのスイッチやルーターの機能は、1 台の筐体内で実現されています。



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

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

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

- VLAN ID（VID）による指定
  VID が 10 ならば、vlan10 のように「vlan」+VID のように指定します。VLAN 名のときとは異なり、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 314 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 129 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。

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、VLAN ごとにレイヤー 2 のブロードキャストパケット、マルチキャストパケットの送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。これらのパケットの送信レートが設定値を上回った場合、パケットは破棄されます。本機能はデフォルトではオフになっています。
制限できるのは以下のパケットです。かっこ内は設定パラメーターの名前です。

- ブロードキャストパケット（BCLIMIT）
- マルチキャストパケット（MCLIMIT）

送信レートの上限値は、ブロードキャストパケット、マルチキャストパケットのそれぞれについて、16 個 / 秒～1048560 個 / 秒の範囲で指定できます。ただし、実際の設定値は、16 の倍数になるよう切り捨てられます。

■ 送信レートの設定は SET VLAN コマンド（228 ページ）で行います。ここでは、VLAN orange に対して、ブロードキャストパケットの送信レートを 1 秒あたり 1000 個、マルチキャストパケットの送信レートを 1 秒あたり 1500 個に制限します。

```
SET VLAN=orange BCLIMIT=1000 MCLIMIT=1500 ↵
```

> ✎ パケットストームプロテクションは、64 個のカウンターによって実現されています。BCLIMIT、MCLIMIT パラメーターに NONE 以外の値を設定すると、パラメーター 1 個あたりカウンター 1 個が消費されます。たとえば、VLAN orange に BCLIMIT と MCLIMIT の両方を設定した場合、カウンターは 2 個消費されます。したがって、パケットストームプロテクションを利用できる VLAN の数は最大 64 個、最小 32 個となります。

■ 送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 VLAN=orange BCLIMIT=NONE MCLIMIT=NONE ↵
```

■ パケットストームプロテクションの設定状況は SHOW VLAN コマンド（285 ページ）で確認できます。「Broadcast limit」、「Multicast limit」をご覧ください。

スパニングツリープロトコル

スパニングツリープロトコル（STP）は、スイッチ（ブリッジ）ネットワークにおいて、冗長経路（複数経路）の設定を可能とし、ネットワークの耐障害性を高めるプロトコルです。
ネットワーク上に複数の経路を設定し、障害発生時に迂回路を使えるようにすることは自然な発想ですが、Ethernet ではループ状の経路がブロードキャストストームによるネットワーク停止を招くため、そのままでは複数経路の設定自体ができません。
スパニングツリープロトコルを使用すると、ブリッジ同士がメッセージを交換し合うことにより、すべてのブリッジを含むツリー状の論理経路（スパニングツリー）が自立的に構築されます。物理的にループが存在しても、ツリーを構成しないポートは自動的にブロックされるため、パケットがループすることはありません。また、障害が発生して一部の経路が不通になったときは、ツリーの再計算が行われ、自動的に新しい経路に切り替わる冗長機能も備えています。

基本設定

本製品は、VLAN グループ（1 つ以上の VLAN で構成）ごとに個別のスパニングツリーを構成するマルチプル STP ドメインに対応していますが、デフォルトの設定では VLAN default、ユーザー定義の VLAN とも、すべての VLAN がデフォルトの STP ドメイン「default」所属となります。
以下、スパニングツリープロトコルの基本設定コマンドについて解説します。

■ 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（183 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（160 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（255 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（261 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（258 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
- 各ポートが所属できる STP ドメインは 1 つ。VLAN 内に、複数 VLAN に所属するポートが 1 つでも含まれている場合、その VLAN を default 以外の STP ドメインに参加させることはできません。そうした VLAN では、default STP を使ってください（VLAN はデフォルトで default STP 所属となります）

なお、通常の環境では複数の 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（126 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（96 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（135 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（135 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（152 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（135 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や複数 STP ドメインの作成方法など、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（219 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、ディスカーディ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 3:

■ STP ドメインのスパニングツリーパラメーター（MODE と RSTPTYPE を除く）をデフォルト値に戻したいときは、SET STP コマンド（219 ページ）の DEFAULT オプションを使います。

```
SET STP=default DEFAULT ↵
SET STP=ALL DEFAULT ↵
```

■ スイッチポートのスパニングツリーパラメーターを変更するには、SET STP PORT コマンド（221 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 4:

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 5: 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 6: 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（221 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（162 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（185 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（201 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（199 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。

フォワーディングデータベース

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

FDB エントリー

FDB 内の各エントリーは次のようなフィールドで構成されています。

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

表 7:

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（フラッディング）。

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ー（learn）エントリー	ポートセキュリティー機能の「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しないかを設定できる。ポートセキュリティー機能をオフにする、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ー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ー機能は、SET SWITCH PORT コマンドの LEARN パラメーターで設定する

表 8:

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（269 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（202 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、ポートやカウンター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（167 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（190 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（223 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（164 ページ）を実行します。これにより、ダイナミックエントリー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（187 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（263 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ー

手動で FDB エントリーを追加するには ADD SWITCH FILTER コマンド（98 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ーだけでなく、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ーも作成できます。また、ポートセキュリティー機能の「学習済みアドレス」としてカウントされるエントリーも登録できます。
FDB エントリーは 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ーを追加します。

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

■ タグ付きポートにスタティックエントリーを追加するときは、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ー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ー機能は SET SWITCH PORT コマンド（225 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ー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ー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（272 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（136 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（272 ページ）で確認してから指定してください。例のように、ENTRY パラメーターには複数のエントリーを指定できます。

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

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

クラシファイア

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

クラシファイアの構成

クラシファイアは、下記の条件に基づいてパケットをフローに分類します。

項目名	説明
	レイヤー 2
MACTYPE	（Ethernet）レイヤー 2 アドレス種別。L2UCAST（ユニキャスト）、L2MCAST（マルチキャスト）、L2BCAST（ブロードキャスト）、ANY（すべて）のいずれか
ETHFORMAT	（Ethernet）フレームフォーマット（エンキャプセレーション）
PROTOCOL	（Ethernet）プロトコルタイプ
SVLAN	入力 VLAN（DVLAN とは同時に指定できない）
DVLAN	出力 VLAN（SVLAN とは同時に指定できない）
	レイヤー 3
IPSADDR	（IP ヘッダー）始点アドレス/マスク長
IPDADDR	（IP ヘッダー）終点アドレス/マスク長
IPDSCP	（IP ヘッダー）DSCP（DiffServ Code Point）
IPTOS	（IP ヘッダー）TOS 優先度（precedence）
IPPROTOCOL	（IP ヘッダー）プロトコルタイプ（レイヤー 4 プロトコルタイプ）
IPXDADDR	（IPX ヘッダー）終点ネットワーク番号
IPXSSOCKET	（IPX ヘッダー）始点ソケット（レイヤー 4 プロトコルタイプ）
IPXDSOCKET	（IPX ヘッダー）終点ソケット（レイヤー 4 プロトコルタイプ）
	レイヤー 4
TCPSPORT	（TCP ヘッダー）始点ポート
TCPDPORT	（TCP ヘッダー）終点ポート
UDPSPORT	（UDP ヘッダー）始点ポート
UDPDPORT	（UDP ヘッダー）終点ポート

表 9: 条件パラメーター

基本設定

■ クラシファイアを作成するには、CREATE CLASSIFIER コマンド（114 ページ）を使います。CLASSIFIER パラメーターに指定するのは、各クラシファイアを識別するための番号です。この番号は単なる識別子であり、値の大小は意味を持ちません。

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

✎ クラシファイアの設定において、ファイアウォールポリシーに追加されたインターフェース（VLAN）を SVLAN に指定しないでください。指定した場合、そのクラシファイアは、ルーティングパケットに対しては機能しません（スイッチングパケットに対しては機能します）。この現象は、ファイアウォール機能が無効であっても発生するのでご注意ください。

■ 作成済みのクラシファイアを変更するには、SET CLASSIFIER コマンド（204 ページ）を使います。

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

■ クラシファイアを削除するには、DESTROY CLASSIFIER コマンド（147 ページ）を使います。ハードウェアパケットフィルターや QoS ポリシー（厳密にはフローグループ）に関連付けられているクラシファイアは削除できません。先に関連付けを削除してから DESTROY CLASSIFIER コマンド（147 ページ）を実行してください。
クラシファイア番号は、カンマ、ハイフンを使って複数指定が可能です。

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

■ クラシファイアの一覧は SHOW CLASSIFIER コマンド（230 ページ）で確認できます。

```
SHOW CLASSIFIER ↵
```

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

```
SHOW CLASSIFIER=1 ↵
SHOW CLASSIFIER=ALL ↵
```

クラシファイアの使用

前述のとおり、クラシファイアはパケットをフローに分類するメカニズムを提供するだけです。実際に使用するには、QoS ポリシーかハードウェアパケットフィルターと関連付ける必要があります。

■ ポリシーベース QoS 機能では、パケットをフローグループに分類するためにクラシファイアを使います。フローグループにクラシファイアを関連付けるには、ADD QOS FLOWGROUP コマンド（93 ページ）を使います。

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

■ ハードウェアパケットフィルター機能では、クラシファイアとマッチ時のアクション、および、送出ポートの 3 つ 1 組でフィルターエントリーを構成します。ハードウェアパケットフィルターにエントリーを追加するには、ADD SWITCH HWFILTER コマンド（100 ページ）を使います。

```
ADD SWITCH HWFILTER=1 CLASSIFIER=10-12 ACTION=DISCARD DPORT=1-4 ↵
```

この例では、スイッチポート 1〜4 から送出されるパケットのうち、クラシファイア「10」、「11」、「12」のいずれかにマッチするパケットを破棄します。
ポリシーベース QoS、ハードウェアパケットフィルターの詳細については、それぞれ「スイッチング」の「QoS」、「ハードウェアパケットフィルター」をご覧ください。

クラシファイア使用時の注意

IPDADDR/IPXDADDR を条件に含むクラシファイアは、適用ポートの数だけ内部テーブルエントリーを消費します。IPDADDR/IPXDADDR 用の内部エントリー容量は 62 個なので、適用ポートを限定するなどして（例：「DPORT=ALL」の指定を避ける）、エントリー消費数が 62 個以内におさまるよう工夫してください。

> ✎ ここでの適用ポートとは、ハードウェアパケットフィルターの DPORT パラメーターに指定するポート、および、QoS ポリシーの SET QOS PORT コマンド（214 ページ）で指定するポートのことです。

■ 一例として、次のようなハードウェアパケットフィルターを定義したとします。

```
CREATE CLASSIFIER=1 IPDADDR=10.1.2.0/24
ADD SWITCH HWFILTER=1 CLASSIFIER=1 ACTION=DISCARD DPORT=ALL
```

クラシファイア「1」は IPDADDR を条件に含んでいるため、適用ポート数分の内部エントリーを消費します。ここでは、「DPORT=ALL」が指定されているため、適用ポート数は 16 となり、結果的に内部エントリーを 16 個も消費してしまいます。
回避策としては、DPORT に ALL ではなく本当に必要なポートだけを指定します。たとえば、10.1.2.0/24 のネットワークがポート 1〜3 に接続されているなら、DPORT の指定を次のように変更することで、消費エントリー数を 3 個にまで減らせます。

```
CREATE CLASSIFIER=1 IPDADDR=10.1.2.0/24
ADD SWITCH HWFILTER=1 CLASSIFIER=1 ACTION=DISCARD DPORT=1-3
```

ポリシーベース QoS

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

✎ IEEE 802.1p 準拠のプライオリティータグに基づく QoS はサポートしておりません。

✎ ポリシーベース QoS の帯域制御機能とスイッチポートの帯域制限機能（SET SWITCH PORT コマンド（225 ページ）の EGRESSLIMIT パラメーター）は併用できません。

概要

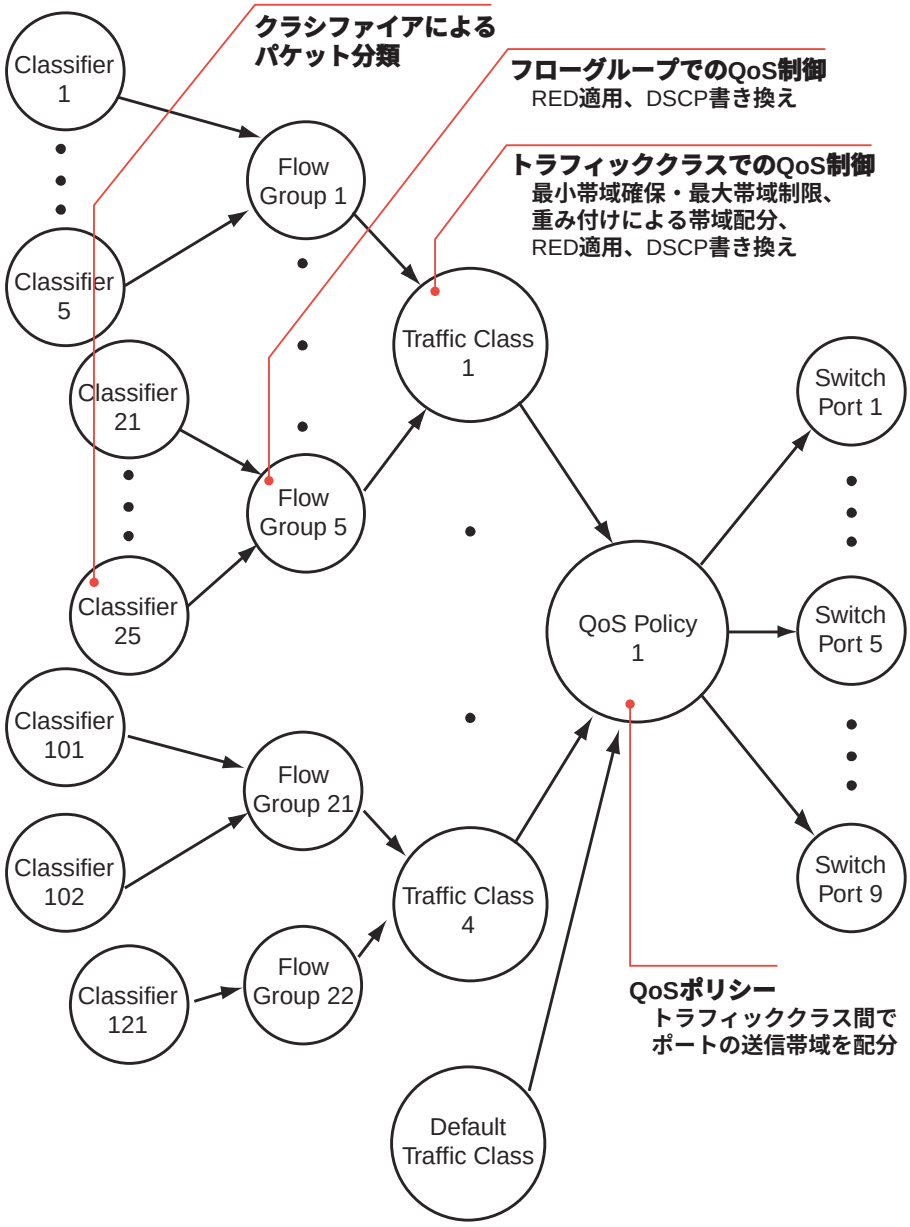
ポリシーベース QoS では、クラシファイアと呼ばれる汎用のパケットフィルターを用いてパケットを分類し、クラスごとに帯域を割り当てます。
ポリシーベース QoS を使うと、次のことが可能です。

- 帯域保証：特定のトラフィッククラスに対し、一定の帯域を保証します。
- 帯域制限：特定のトラフィッククラスに与える帯域を、一定値までに制限します。
- 帯域配分：複数のトラフィッククラス間で、「重み付け」を考慮しつつ帯域を均等に配分します。
- DiffServ：IP ヘッダーの DSCP（DiffServ Code Point）フィールド値による帯域制御が可能です。また、送信時に DSCP フィールドを書き換えることができます。
- 輻輳制御：RED（Random Early Detection / Discard）アルゴリズムを用いて、トラフィック量を段階的に制御します。動作パラメーターは、トラフィッククラスまたはフローグループ単位で設定できます。

構成要素

本製品のポリシーベース QoS 機能は、以下の基本要素から成り立っています。

- スイッチポート
- QoS ポリシー
- トラフィッククラス
- フローグループ
- クラシファイア



以下、各要素について説明します。

スイッチポート

本製品の QoS 機能は、スイッチポート（出力ポート）ごとに設定します。これは、後述する QoS ポリシーをスイッチポートに割り当てることで行います。
本製品は、ポートを通過するパケットをトラフィッククラスに分類し、各クラスの設定に基づいて送信帯域や送信順序を制御します。

QoS ポリシー

QoS ポリシーは、スイッチポートからパケットを出力するときに帯域制御を行うためのメカニズムで、ポリシーベース QoS の中心となる構成要素です。QoS ポリシーは、トラフィッククラスの集合として定義します。通常、QoS ポリシーは、ユーザー定義のトラフィッククラス（複数）とデフォルトトラフィッククラス（1 つ）から構成されます。
QoS ポリシーをスイッチポートに関連付けると、ポートから出力されるトラフィックに対して、該当するトラフィッククラスで定められた最大・最小帯域と帯域配分時の優先度（重み）が割り当てられます。
QoS ポリシーは、スイッチポートの帯域をどのように配分すべきか定義するものと言えます。

トラフィッククラス

トラフィッククラスは、同等の QoS（帯域）を与えるべきパケットフローをひとまとめにしたものです。トラフィッククラスはフローグループの集合として定義します。帯域割り当てや帯域配分時の優先度など、QoS パラメーターの多くはトラフィッククラス単位で設定します。QoS ポリシー内のトラフィッククラスは、各クラスの設定に基づき、ポート帯域を分け合うことになります。
ポリシーベース QoS では、トラフィッククラスごとに送信時の最小帯域幅（保証帯域）、最大帯域幅、帯域配分時の優先度（重み：Weight）などを設定できます。
たとえば、トラフィッククラス「TCP」とトラフィッククラス「UDP」を定義し、TCP にポート帯域の 70%、UDP に 20%、その他（デフォルトトラフィッククラス）に 10%を割り当てるようなことができます。

> ✎ 実際のトラフィッククラスは「TCP」「UDP」のような名前ではなく、番号で識別します。ただし、覚え書きとして文字列を割り当てることはできます（DESCRIPTION パラメーター）。

トラフィッククラスは、QoS ポリシーに割り当てて使います。なお、QoS ポリシーには、ユーザー定義のトラフィッククラスに加え、暗黙のデフォルトトラフィッククラスが存在します。ユーザー定義のトラフィッククラスに分類されないトラフィックは、自動的にデフォルトトラフィッククラスの所属として処理されます。

フローグループ

フローグループは、同等な性格を持つパケットのフロー（流れ）をグループ化したものです（アプリケーションの「行き」と「戻り」など）。QoS パラメーターの多くはトラフィッククラスのレベルで設定しますが、トラフィッククラスに割り当てられた帯域の中でより細かい制御を行いたい場合は、フローグループごとに帯域制御の方法を微調整することができます。
たとえば、前述のトラフィッククラス「TCP」に対し、「Web」、「FTP」、「その他」という 3 つのフローグループを定義し、「FTP」、「Web」、「その他」のそれぞれに対して異なる RED カーブを適用することができます。

> ✎ 実際のフローグループは「Web」「FTP」「その他」のような名前ではなく、番号で識別します。ただし、覚え書きとして文字列を割り当てることはできます（DESCRIPTION パラメーター）。

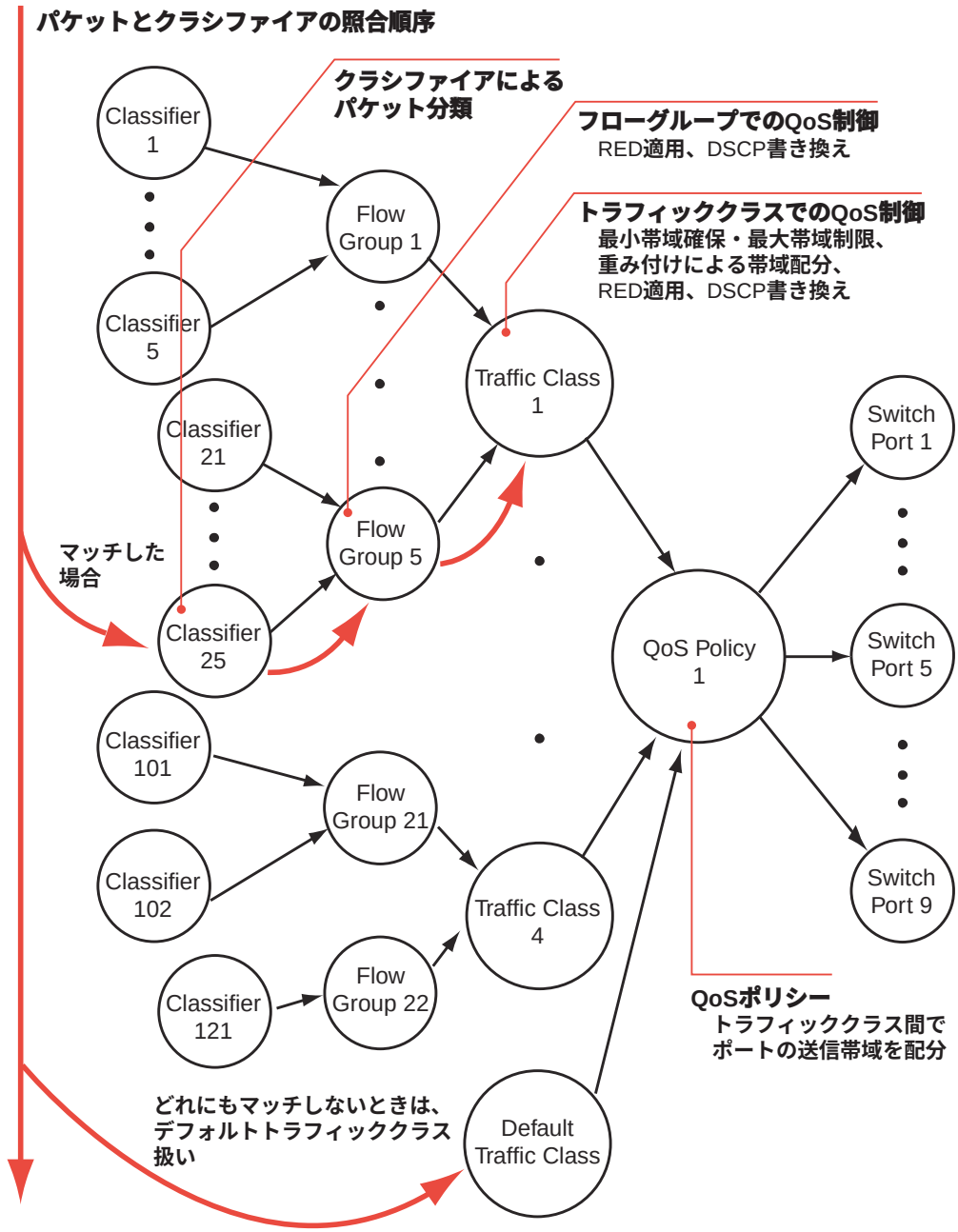
パケットフローは、クラシファイアと呼ばれる汎用のパケットフィルターによって定義します。したがって、フローグループはクラシファイアの集合として定義します。また、フローグループは、トラフィッククラスに割り当てて使います。
フローグループは、QoS パラメーターの最小設定単位です。

クラシファイア

クラシファイアは、IP アドレス、ポート、プロトコルなど、さまざまな条件に基づいてパケットを「フロー」に分類する汎用のパケットフィルターです。本製品では、ハードウェアパケットフィルターとポリシーベース QoS の両機能でクラシファイアを使用しています。
ポリシーベース QoS では、クラシファイアを使ってパケットを「フロー」に分類します。ただし、QoS パラメーターの設定は、フローを束ねた「フローグループ」またはフローグループを束ねた「トラフィッククラス」を単位として行います。

パケットの照合順序について

パケットとクラシファイアの照合は、次の順序でおこなわれます。
図中のトラフィッククラス、フローグループ、クラシファイアは、いずれも番号の小さいものから大きなものの順に上位のオブジェクトに追加されたものと仮定しています。
なお、ここでの「上位のオブジェクト」とは、トラフィッククラスに対する QoS ポリシー、フローグループに対するトラフィッククラス、クラシファイアに対するフローグループを意味しています。



次に例をあげて解説します。下記のコマンドを実行し、QoS ポリシー「1」を ポート「1」に適用するとします。

```
### QOS ポリシーの作成とポートへの割り当て (1)
create qos policy=1
set qos port=1 policy=1

### トラフィッククラスの作成とポリシーへの割り当て (2)
create qos trafficclass=1
create qos trafficclass=2
add qos policy=1 trafficclass=1
```

```
add qos policy=1 trafficclass=2

### フローグループの作成とトラフィッククラスへの割り当て (3)
create qos flowgroup=11
create qos flowgroup=12
create qos flowgroup=21
add qos trafficclass=1 flowgroup=11
add qos trafficclass=1 flowgroup=12
add qos trafficclass=2 flowgroup=21

### クラシファイアの作成とフローグループへの割り当て (4)
create classifier=111 <フィルター条件は割愛（以下同じ）>...
create classifier=112 ...
create classifier=113 ...
add qos flowgroup=11 classifier=111
add qos flowgroup=11 classifier=112
add qos flowgroup=11 classifier=113

create classifier=121 ...
create classifier=122 ...
add qos flowgroup=12 classifier=121
add qos flowgroup=12 classifier=122

create classifier=211 ...
create classifier=212 ...
create classifier=213 ...
add qos flowgroup=21 classifier=211
add qos flowgroup=21 classifier=212
add qos flowgroup=21 classifier=213
```

この場合、パケットとクラシファイアの照合は、クラシファイア 111, 112, 113, 121, 122, 211, 212, 213 の順に行われます。

ここで注意すべきことがあります。照合順序を決めるのはトラフィッククラス、フローグループ、クラシファイアの ID（番号）ではなく、それらを上位のオブジェクトに追加した順序だということです。

例では、ID 順 ＝ 追加順となるように設定しているため見落としがちですが、照合順序は ID 順ではなく追加（ADD）順によって決まります。

たとえば、上記設定例の (2) の部分を次のように変更した場合（3、4 行目を入れ替えた）、照合順序は 211, 212, 213, 111, 112, 113, 121, 122 となります。

```
### トラフィッククラスの作成とポリシーへの割り当て (2)
create qos trafficclass=1
create qos trafficclass=2
add qos policy=1 trafficclass=2
add qos policy=1 trafficclass=1
```

なお、追加順序の確認は下記のコマンドで行います。

■ トラフィッククラスの追加順は、SHOW QOS POLICY コマンド（248 ページ）の Trafficclasses または TCs Assigned で確認できます。

次の出力例では、トラフィッククラス 2, 1 の順に、ポリシーへの追加が行われていることがわかります。

```
Manager > show qos policy

QOS Policy Information
Id    Description     Trafficclasses      Ports Assigned to
-------------------------------------------------------------------------
1                     2,1                 Port: 1

Manager > show qos policy=1

Identifier ............... 1
Description ...............
TCs Assigned ............. 2,1
Port Assigned to .......... 1
Default Traffic Class
Percent ................ 20
```

■ 同様に、フローグループの追加順は SHOW QOS TRAFFICCLASS コマンド（252 ページ）の FlowGroups または Flow Groups で確認できます。

■ 同様に、クラシファイアの追加順は SHOW QOS FLOWGROUP コマンド（246 ページ）の Classifiers で確認できます。

基本設定

ポリシーベース QoS の設定は、QoS ポリシーを作成し、スイッチポートに関連付けることによって行います。QoS ポリシーは前図のような階層構造になっているため、ポリシーの作成はこの階層を形づくる作業と言えます。

✎ ポリシーベース QoS の帯域制御機能とスイッチポートの帯域制限機能（SET SWITCH PORT コマンド（225 ページ）の EGRESSLIMIT パラメーター）は併用できません。どちらか一方だけを使用するようにしてください。

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

1. QoS ポリシーを作成する
2. QoS ポリシーをスイッチポートに関連付ける
3. トラフィッククラスを作成する
4. トラフィッククラスを QoS ポリシーに割り当てる
5. フローグループを作成する
6. フローグループをトラフィッククラスに割り当てる
7. クラシファイアを作成する
8. クラシファイアをフローグループに割り当てる

以下、QoS ポリシーの基本的な設定項目について解説します。ポリシーの詳細設定については、次節「詳細設定」をご覧ください。また、全体的な設定例については、次々節「設定例」をご覧ください。

QoS ポリシーとスイッチポート

ポリシーベース QoS の基本要素は QoS ポリシーです。本製品では、スイッチポートに QoS ポリシーを関連付けることで、該当ポートからパケットを送信するときの動作を制御します。

■ QoS ポリシーを作成するには、CREATE QOS POLICY コマンド（120 ページ）を使います。DTCPERCENT パラメーターには、デフォルトトラフィッククラスに割り当てる帯域（最小かつ最大帯域）を、ポートの帯域に対するパーセンテージで指定します。省略時は 20%です。
次の例では、デフォルトトラフィッククラスにポート帯域の 15%を割り当てています。

```
CREATE QOS POLICY=1 DTCPERCENT=15 ↵
```

✎ DTCPERCENT は最小保証帯域である同時に最大帯域（使用可能な帯域の上限）でもあります。

✎ ポリシーベース QoS の帯域制御機能とスイッチポートの帯域制限機能（SET SWITCH PORT コマンド（225 ページ）の EGRESSLIMIT パラメーター）は併用できません。どちらか一方だけを使用するようにしてください。

■ QoS ポリシーをスイッチポートに割り当てるには、SET QOS PORT コマンド（214 ページ）を使います。これにより、該当ポートから送出されるパケットに QoS ポリシーが適用されます。

```
SET QOS PORT=1-4 POLICY=1 ↵
```

✎ スイッチポートには、QoS ポリシーを 1 つだけ割り当てることができます。

✎ QoS ポリシーは、複数のスイッチポートに割り当てることができます。また、QoS ポリシーには、複数のトラフィッククラスを割り当てることができます。

✎ QoS 設定パラメーター（帯域設定など）のエラーチェックは、「トラフィッククラス割り当て済みのポリシーをスイッチポートに関連付けたとき」あるいは「スイッチポートに関連付けられた QoS ポリシーにトラフィッククラスやフローグループを追加したとき」に行われます。したがって、QoS の設定では、最初に QoS ポリシーを作成しスイッチポートに割り当てたあとで、トラフィッククラスやフローグループの設定をすることをおすすめします。

■ ポートから QoS ポリシーを削除（関連付けを削除）するには、SET QOS PORT コマンド（214 ページ）の POLICY パラメーターに NONE を指定します。

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

トラフィッククラス

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

■ トラフィッククラスを作成するには、CREATE QOS TRAFFICCLASS コマンド（124 ページ）を使います。

```
CREATE QOS TRAFFICCLASS=1 ↵
```

■ トラフィッククラスに割り当てる最小帯域（保証帯域）、最大帯域（上限値）、RED アルゴリズム（後述）の使用・不使用、DSCP フィールドの書き換え設定（後述）は、それぞれ MINBANDWIDTH、MAXBANDWIDTH、RED、MARKVALUE パラメーターで指定します。

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

✎ MINBANDWIDTH、MAXBANDWIDTH は、内部キューからデータを送り出すときの送信レートを示しています。回線（ケーブル）上での送信レートとは異なるので注意してください。パケットが回線上に出力されるときは、フレーム間ギャップ（IFG）やプリアンブルが付加されるため、実際の送信レートはこれらのパラメーターで指定した値よりも小さくなります。なお、パケットサイズが大きいほど IFG やプリアンブルの割合（オーバーヘッド）が減るので、実際の送信レートがパラメーター指定値に近づきます。

■ 作成したトラフィッククラスの設定を変更するには、SET QOS TRAFFICCLASS コマンド（216 ページ）を使います。

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

■ トラフィッククラスを QoS ポリシーに割り当てるには、ADD QOS POLICY コマンド（94 ページ）を使います。パケットのチェック（クラシファイアとの照合）は、ポリシー内のトラフィッククラス追加順、トラフィッククラス内のフローグループ追加順、フローグループ内のクラシファイア追加順に行われます（前掲の図を参照）。

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

✎ QoS ポリシーには複数のトラフィッククラスを割り当てることができます。

✎ トラフィッククラスは、1 つの QoS ポリシーにしか割り当てることができません。あるポリシーに割り当てたトラフィッククラスは、別のポリシーでは使用できません。

✎ トラフィッククラスには、複数のフローグループを割り当てることができます。

フローグループ

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

フローグループは、クラシファイアによって分類された「フロー」をグループ化したものです。同じ性格を持つフロー（特定アプリケーションの「行き」と「戻り」など）を束ねたものと言えます。フローグループは、複数のクラシファイアで構成されます。
トラフィッククラスに割り当てられた帯域の中で、より細かい制御を行いたい場合は、フローグループごとに帯域制御の方法を微調整することができます。

■ フローグループを作成するには、CREATE QOS FLOWGROUP コマンド（119 ページ）を使います。

```
CREATE QOS FLOWGROUP=1 ↵
```

■ パケットがどのフローグループに所属するかを決定するのは、汎用のパケットフィルターであるクラシファイアです。クラシファイアは CREATE CLASSIFIER コマンド（114 ページ）で作成します。たとえば、Web トラフィック（HTTP と HTTPS）に対応するクラシファイアは次のようになります。

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

■ フローグループにクラシファイアを関連付けるには、ADD QOS FLOWGROUP コマンド（93 ページ）を使います。クラシファイアのチェックは、本コマンドで追加した順番で行われます。

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

■ 通常、QoS パラメーター（最大・最小帯域、RED カーブ、DSCP 値）はトラフィッククラス単位で設定しますが、RED カーブ、DSCP 値はフローグループ単位で設定することもできます。これらは、CREATE QOS FLOWGROUP コマンド（119 ページ）、SET QOS FLOWGROUP コマンド（212 ページ）の RED、MARKVALUE パラメーターで指定します。

```
SET QOS FLOWGROUP=1 RED=2 ↵
```

RED カーブや DSCP 値がフローグループとトラフィッククラスの両方に設定されている場合は、フローグループの設定が使用されます。フローグループで設定されていないパラメーターについては、トラフィッククラスの設定が使用されます。

■ フローグループは、トラフィッククラスに割り当てて使います。フローグループをトラフィッククラスに割り当てるには、ADD QOS TRAFFICCLASS コマンド（95 ページ）を使います。パケットのチェック（クラシファイアとの照合）は、ポリシー内のトラフィッククラス追加順、トラフィッククラス内のフローグループ追加順、フローグループ内のクラシファイア追加順に行われます（前掲の図を参照）。

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

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

クラシファイア

ポリシーベース QoS 機能の中心要素が QoS ポリシーだとすると、末端の要素はクラシファイアです。クラシファイアは、ハードウェアパケットフィルターでも用いられる汎用のパケットフィルターで、アドレス、プロトコルなどをもとにパケットを「フロー」に分類する働きを持ちます。
ポリシーベース QoS では、パケットをフローグループやトラフィッククラスに分類して、グループやクラスごとに処理を行いますが、これらの分類の第一歩はクラシファイアによって行われます。

■ クラシファイアは CREATE CLASSIFIER コマンド（114 ページ）で作成します。クラシファイアの詳細については、「スイッチング」の「クラシファイア」をご覧ください。

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

✎ クラシファイアの設定において、ファイアウォールポリシーに追加されたインターフェース（VLAN）を SVLAN に指定しないでください。指定した場合、そのクラシファイアは、ルーティングパケットに対しては機能しません（スイッチングパケットに対しては機能します）。この現象は、ファイアウォール機能が無効であっても発生するのでご注意ください。

■ フローグループはクラシファイアの集合として定義します。フローグループにクラシファイアを割り当てるには、ADD QOS FLOWGROUP コマンド（93 ページ）を使います。クラシファイアのチェックは、本コマンドで追加した順番で行われます。

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

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

詳細設定

ここでは、より詳細な QoS 設定に必要となる設定項目について解説します。

帯域制御

ポリシーベース QoS では、トラフィッククラスごとにポート帯域の割り当てが可能です。トラフィッククラス 1〜n を定義している場合、スイッチポートの送信帯域は次のクラス間で配分されます。

- トラフィッククラス 1
- トラフィッククラス 2
- ...
- トラフィッククラス n

- デフォルトトラフィッククラス

クラス間の帯域配分は、以下の設定要素に基づいて行われます。

- デフォルトトラフィッククラスの帯域（DTCPERCENT）
- 各トラフィッククラスの最小帯域（MINBANDWIDTH）
- 各トラフィッククラスの最大帯域（MAXBANDWIDTH）
- 各トラフィッククラスの重み付け（WEIGHT）

以下、それぞれの設定について解説します。

デフォルトトラフィッククラス

デフォルトトラフィッククラスは、QoS ポリシーを作成したときに自動的に作られる暗黙のトラフィッククラスです。ユーザー定義のトラフィッククラスに分類されないトラフィックは、すべてデフォルトトラフィッククラスの所属として扱われます。
デフォルトトラフィッククラスには、CREATE QOS POLICY コマンド（120 ページ）、SET QOS POLICY コマンド（213 ページ）の DTCPERCENT パラメーターで指定したパーセンテージのポート帯域が割り当てられます。
たとえば、QoS ポリシー「5」を次のようにして作成した場合、デフォルトトラフィッククラスにはポート帯域の 10%が割り当てられます。

```
CREATE QOS POLICY=5 DTCPERCENT=10 ↵
```

デフォルトトラフィッククラスには、DTCPERCENT の帯域が保証されますが、DTCPERCENT を超える帯域は割り当てられません。
デフォルト以外のトラフィッククラスが利用できる帯域は、ポート帯域から DTCPERCENT 分を差し引いた量になります。

最小帯域（帯域保証）

デフォルト以外のトラフィッククラスには、それぞれ最小帯域（最低限確保する帯域）を設定できます。特に設定しなかった場合の最小帯域は 64Kbps（ほぼ 0 に近い）になります。

✎ デフォルトトラフィッククラスの最小帯域は、ポート帯域× DTCPERCENT ÷ 100 となります。これは同時に最大帯域でもあります。

■ 最小帯域は CREATE QOS TRAFFICCLASS コマンド（124 ページ）、SET QOS TRAFFICCLASS コマンド（216 ページ）の MINBANDWIDTH パラメーターで設定します。単位としては K（Kbps）、M（Mbps = 1000Kbps）、G（Gbps = 1000000Kbps）を指定できます。単位を省略した場合は Kbps となります。

```
CREATE QOS TRAFFICCLASS=10 MINBANDWIDTH=256K ↵
```

✎ MINBANDWIDTH は、内部キューからデータを送り出すときの送信レートを示しています。回線（ケーブル）上での送信レートとは異なるので注意してください。パケットが回線上に出力されるときは、フレーム間ギャッ

プ（IFG）やプリアンブルが付加されるため、実際の送信レートは MINBANDWIDTH で指定した値よりも小さくなります。なお、パケットサイズが大きいほど IFG やプリアンブルの割合（オーバーヘッド）が減るので、実際の送信レートが MINBANDWIDTH の値に近づきます。

同じ QoS ポリシーに属するトラフィッククラスは、スイッチポートの送信帯域を分け合いますが、デフォルトトラフィッククラスに DTCPERCENT 分の帯域が割り当てられるため、通常トラフィッククラスの MINBANDWIDTH の合計は、ポート帯域から DTCPERCENT 分を引いた値以下でなくてはなりません。

```
sum(MINBANDWIDTH) <= ポート帯域 - (ポート帯域 * (DTCPERCENT / 100))
```

✎ ここで、sum(MINBANDWIDTH）は、全トラフィッククラスの MINBANDWIDTH の合計を示しています。

たとえば、100M でリンクアップしているポート 4 に QoS ポリシー「1」を関連付けたとします。QoS ポリシーの DTCPERCENT パラメーターが 25 に設定されている場合、同ポリシーのデフォルトトラフィッククラスには 25Mbps の送信帯域が保証されます。したがって、ユーザー定義のトラフィッククラスには 75Mbps の帯域が残ります。
ポリシーが 3 つのトラフィッククラス（1、2、3）を持つとすると、帯域設定の可否は次のようになります。

- 設定可能（最小帯域の合計が 75Mbps 以下）

```
CREATE QOS TRAFFICCLASS=1 MINBANDWIDTH=10M ↵
CREATE QOS TRAFFICCLASS=2 MINBANDWIDTH=20M ↵
CREATE QOS TRAFFICCLASS=3 MINBANDWIDTH=30M ↵
```

- 設定不可（最小帯域の合計が 75Mbps を超える）

```
CREATE QOS TRAFFICCLASS=1 MINBANDWIDTH=20M ↵
CREATE QOS TRAFFICCLASS=2 MINBANDWIDTH=30M ↵
CREATE QOS TRAFFICCLASS=3 MINBANDWIDTH=40M ↵
```

✎ QoS 設定パラメーター（帯域設定など）のエラーチェックは、トラフィッククラス割り当て済みのポリシーをスイッチポートに関連付けたとき、あるいは、スイッチポートに関連付けられた QoS ポリシーにトラフィッククラスやフローグループを追加したとき、に行われます。したがって、QoS の設定では、最初に QoS ポリシーを作成しスイッチポートに割り当てたあとで、トラフィッククラスやフローグループの設定をすることをおすすめします。

各トラフィッククラスの最小帯域の合計を超える帯域については、トラフィッククラスごとの「重み付け」（WEIGHT パラメーター）に基づいて、トラフィッククラス間で均等配分されます。ただし、各トラフィッククラスの最大帯域を超えるような割り当ては行いません。詳しくは「重み付けに基づく帯域配分」をご覧ください。

最大帯域（帯域制限）

デフォルト以外のトラフィッククラスには、それぞれ最大帯域（割り当てる帯域の上限値）を設定できます。特に設定しなかった場合の最大帯域は 16Gbps（事実上無制限）になります。

✎ デフォルトトラフィッククラスの最大帯域は、ポート帯域× DTCPERCENT ÷ 100 となります。これは同時に最小帯域でもあります。

■ 最大帯域は CREATE QOS TRAFFICCLASS コマンド（124 ページ）、SET QOS TRAFFICCLASS コマンド（216 ページ）の MAXBANDWIDTH パラメーターで設定します。単位としては K（Kbps）、M（Mbps = 1000Kbps）、G（Gbps = 1000000Kbps）を指定できます。単位を省略した場合は Kbps となります。

```
SET QOS TRAFFICCLASS=10 MAXBANDWIDTH=512K ↵
```

✎ MAXBANDWIDTH は、内部キューからデータを送り出すときの送信レートを示しています。回線（ケーブル）上での送信レートとは異なるので注意してください。パケットが回線上に出力されるときは、フレーム間ギャップ（IFG）やプリアンブルが付加されるため、実際の送信レートは MAXBANDWIDTH で指定した値よりも小さくなります。なお、パケットサイズが大きいほど IFG やプリアンブルの割合（オーバーヘッド）が減るので、実際の送信レートが MAXBANDWIDTH の値に近づきます。

重み付けに基づく帯域配分

各トラフィッククラスの最小帯域の合計を超える帯域（余剰帯域）については、トラフィッククラスごとの重み付け（WEIGHT パラメーター）に基づいて、トラフィッククラス間で均等配分されます。ただし、各トラフィッククラスの最大帯域を超えるような割り当ては行いません。

■ トラフィッククラスの重み付けは CREATE QOS TRAFFICCLASS コマンド（124 ページ）、SET QOS TRAFFICCLASS コマンド（216 ページ）の WEIGHT パラメーターで行います。トラフィッククラスのデフォルト WEIGHT は 1、すなわちすべてのトラフィッククラスが平等です。

```
SET QOS TRAFFICCLASS=1 WEIGHT=1 ↵
SET QOS TRAFFICCLASS=2 WEIGHT=2 ↵
SET QOS TRAFFICCLASS=3 WEIGHT=4 ↵
```

WEIGHT に指定できる値は、以下の通りです。

```
1、2、3、4、5、6、7、8、10、12、14、16、20、24、28、32、40、48、56、64、80、96、112、
128、160、192、224、256、320、384、448、512、640、768、896、1024
```

■ 重み付けに基づく余剰帯域の配分方法は次のとおりです。ここではトラフィッククラス 1〜n が存在すると仮定し、次の記号を用いて説明します。

- pbw：スイッチポートの送信帯域（bps）
- dtc：デフォルトトラフィッククラスに割り当てた最小かつ最大帯域（pbw に対するパーセンテージ）
- bw：一時変数
- min1, min2...minn：各トラフィッククラスの最小保証帯域（bps）

- wei1, wei2...wein：各トラフィッククラスの「重み付け」（WEIGHT）
- sum_of_1_wei：「重み付け値の逆数」の合計
- alc1, alc2...alcn：各トラフィッククラスに追加配分される帯域（bps）
- bw1, bw2...bwn：各トラフィッククラスに実際に割り当てられる帯域（bps）

1. ポートの送信帯域から、デフォルトトラフィッククラスに割り当てた帯域（DTCPERCENT）分を差し引きます（bw）。

   ```
   bw = pbw - pbw * dtc / 100
   ```

2. さらに、各トラフィッククラスの最小保証帯域を差し引きます（bw）。

   ```
   bw = bw - (min1 + min2 + ...  + minn)
   ```

3. 残りの帯域（bw）を各トラフィッククラスの「重み付け」値に基づいて配分します。最初にそれぞれの「重み付け値の逆数」を求め、「重み付け値の逆数の合計」を求めます。

   ```
   sum_of_1_wei = (1/wei1 + 1/wei2 + ...  + 1/wein)
   ```

4. トラフィッククラスごとに残り帯域×「重み付け値の逆数」÷「重み付け値の逆数の合計」を求めます。これが各トラフィッククラスに追加配分される帯域です。

   ```
   alc1 = bw * 1 / wei1 / sum_of_1_wei
   alc2 = bw * 1 / wei2 / sum_of_1_wei
   ...
   alcn = bw * 1 / wein / sum_of_1_wei
   ```

5. 各トラフィッククラスの最小保証帯域に手順 4 で求めた追加配分帯域を足したものが、該当トラフィッククラスに割り当てられる実際の帯域幅になります。

   ```
   bw1 = min1 + alc1
   bw2 = min2 + alc2
   ...
   bwn = minn + alcn
   ```

■ 次に重み付けに基づく帯域配分の例を示します。ここでは、4 つのトラフィッククラス 1、2、3、4 にそれぞれ 1、2、4、8 という WEIGHT を設定すると仮定します。その場合の余剰帯域配分比率は、下記のとおりとなります。

トラフィッククラス	WEIGHT	1/WEIGHT	**配分比率**	**計算式**
Class 1	1	1	0.5333	= 1 / 1.875

Class 2	2	0.5	0.2667	= 0.5 / 1.875
Class 3	4	0.25	0.1333	= 0.25 / 1.875
Class 4	8	0.125	0.0667	= 0.125 / 1.875
合計		1.875	1.000	

表 10: 重み付けに基づく帯域配分の例

■ すべてのトラフィッククラスに帯域を均等に割り当てるには、各トラフィッククラスの MAXBANDWIDTH、MINBANDWIDTH、WEIGHT パラメーターを同じ値に設定します。デフォルト（前記のパラメーターを指定しなかった場合）では、このような設定になっています。

DSCP フィールドの書き換え

DiffServ（Differentiated Service）ドメインを運用する場合、IP パケットの DSCP（DiffServ Code Point）フィールドに基づいて QoS を割り当てたり、DSCP フィールドを書き換えたりする機能が必要になります。ポリシーベース QoS では、トラフィッククラスまたはフローグループ単位で、DSCP フィールドの書き換え設定が可能です。この機能は、おもに DiffServ ドメインのエッジルーター（スイッチ）で使います。

■ トラフィッククラスに所属するパケットの DSCP フィールドを書き換えるには、CREATE QOS TRAFFICCLASS コマンド（124 ページ）、SET QOS TRAFFICCLASS コマンド（216 ページ）の MARKVALUE パラメーターを使います。DSCP 値の有効範囲は 0〜63 です。MARKVALUE パラメーターを指定しなかった場合、あるいは、NONE を指定した場合は DSCP を書き換えません。
たとえば、トラフィッククラス「2」のパケットに DSCP 値 20 を設定するには次のようにします。

```
SET QOS TRAFFICCLASS=2 MARKVALUE=20 ↵
```

■ フローグループに所属するパケットの DSCP フィールドを書き換えるには、CREATE QOS FLOWGROUP コマンド（119 ページ）、SET QOS FLOWGROUP コマンド（212 ページ）の MARKVALUE パラメーターを使います。DSCP 値の有効範囲は 0〜63 です。MARKVALUE パラメーターを指定しなかった場合、あるいは、NONE を指定した場合は DSCP を書き換えません。
たとえば、フローグループ「10」のパケットに DSCP 値 25 を設定するには次のようにします。

```
SET QOS FLOWGROUP=10 MARKVALUE=25 ↵
```

なお、フローグループに MARKVALUE が設定されている場合は、該当フローグループの MARKVALUE に基づいて DSCP フィールドの書き換えが行われます。フローグループに MARKVALUE が設定されていない場合は、トラフィックグループの MARKVALUE が使用されます。

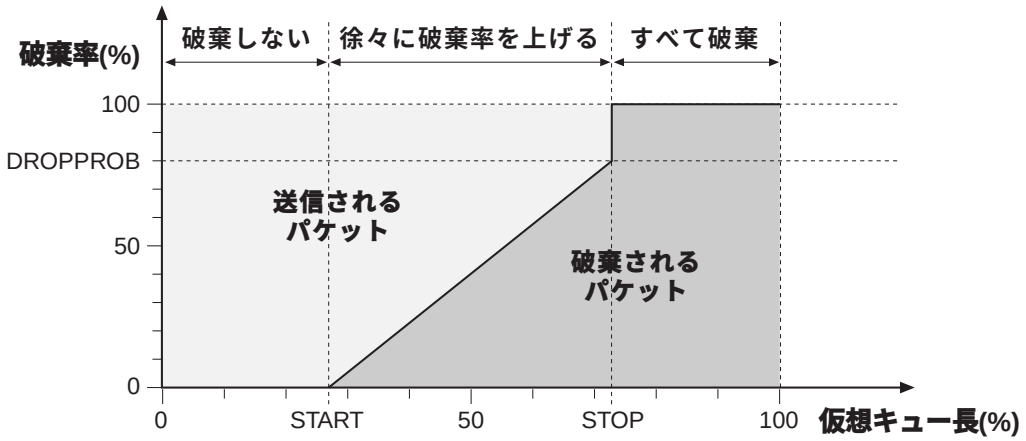
RED アルゴリズム

本製品は、トラフィッククラスごとに仮想的なキュー（仮想キュー）を保持しています。通常は、仮想キューの長さがトラフィッククラスに割り当てられた最大帯域を超えると、超過分のパケットを破棄します（ドロップテイル「drop-tail」アルゴリズム）。
これに対し、RED（Random Early Detection / Discard）は、仮想キュー長が上限に達する前にパケットを

徐々に破棄していくことで、キューの枯渇を予防したり、トランスポート層の輻輳回避メカニズムを有効に機能させたりするためのアルゴリズムです。RED を使用すれば、より細やかな帯域制御を実現できます。RED アルゴリズムの設定は、仮想キュー長とパケット破棄率の関係を示す「RED カーブ」を定義し、これをトラフィッククラスかフローグループに割り当てることによって行います。
RED カーブは以下のパラメーターによって定義します。

- START：パケットを破棄し始めるポイント
- STOP：パケットを完全に破棄するポイント
- DROPPROB：キュー長が STOP のときに破棄するパケットの割合

各パラメーターを図示すると次のようになります。仮想キュー長が START から STOP の間にある場合、パケットは 0 から DROPPROB の間の確率でランダムに破棄されます。パケットの破棄率はキュー長が STOP に近づくにつれ高くなっていき、STOP のとき DROPPROB となります。キュー長が STOP を超えると、すべてのパケットが破棄されます。キュー長が START 以下のときはパケットは破棄されません。



デフォルトでは、次に示す 5 つの RED カーブが定義されています。これらは変更したり、削除したりすることはできません。これらの 5 つに加え、43 個の RED カーブを定義することができます。

RED **カーブ番号**	0	1	2	3	4
名称（DESCRIPTION）	Aggressive	Med-Aggressive	Medium	Med-Passive	Passive
START	15	25	35	45	55
STOP	30	50	65	80	95
DROPPROB	50	70	80	90	100

表 11: デフォルト RED カーブ

■ RED カーブの作成例を示します。

```
CREATE QOS RED=5 DESCRIPTION="Sample RED curve" START=30 STOP=90
  DROPPROB=30 ↵
```

■ トラフィッククラスに RED カーブを適用するには、CREATE QOS TRAFFICCLASS コマンド（124 ページ）か SET QOS TRAFFICCLASS コマンド（216 ページ）の RED パラメーターを使います。

```
SET QOS TRAFFICCLASS=1 RED=3 ↵
```

■ フローグループごとに異なる RED カーブを適用することもできます。フローグループに RED カーブを適用するには、CREATE QOS FLOWGROUP コマンド（119 ページ）か SET QOS FLOWGROUP コマンド（212 ページ）の RED パラメーターを使います。

```
SET QOS FLOWGROUP=1 RED=1 ↵
```

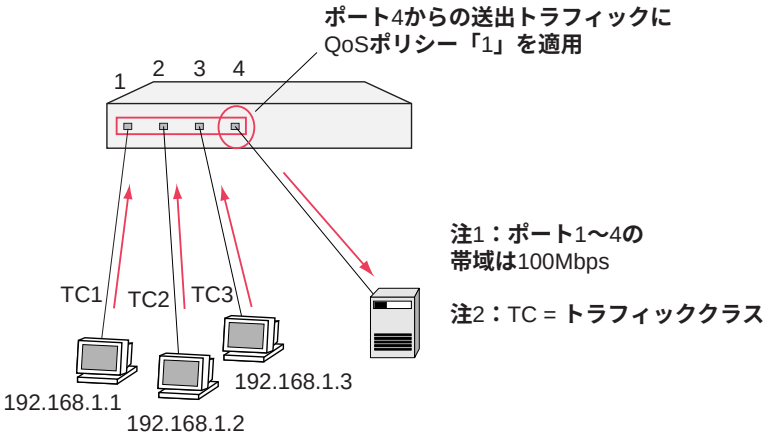
フローグループとトラフィッククラスの両方に RED カーブが適用されている場合は、フローグループの設定が使用されます。フローグループに RED カーブが適用されていない場合は、トラフィッククラスの設定が使用されます。
なお、RED アルゴリズムは流量制御や輻輳回避の機能を持つ TCP トラフィックに対してもっとも効果を発揮します。UDP や ICMP のように流量制御を行わないプロトコルに対しては、逆効果になる場合がありますのでご注意ください。

設定例

ここでは、ポリシーベース QoS の基本的な設定方法について説明します。
QoS 機能を使用すると、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、パケット送信時の最大・最小帯域を設定することができます。
最初に必要なのは「ポリシー」を設計することです。どのトラフィックにどの程度の QoS を提供するのかをよく考えてください。

最小帯域保証

入力ポートから出力ポートに向けて、出力ポートの帯域以上にパケットが流入すると、出力キューにパケットがたまりはじめます。このとき、出力キューがあふれると、QoS ポリシーで最小帯域を保証するよう設定していても、パケットが破棄されてしまいます。
ここでは、RED アルゴリズムの設定によって、出力キューでのパケット破棄を制御し、特定のトラフィックに対して最小帯域を保証する設定例を示します。
最初に、前提条件として次のような構成を考えます。



ポート 1〜3 にはそれぞれ 1 台ずつクライアントが接続されており、ポート 4 のサーバーに向けて大量のトラフィックを送信しているものとします。ポート 1〜4 の帯域はいずれも 100Mbps であると仮定します。この構成では、サーバーへのトラフィックが集中するスイッチポート 4 で輻輳が発生しがちです。
ここでは、スイッチポート 4 に QoS ポリシーを適用し、ポート 1 のクライアントに 80Mpbs の最小帯域を保証するよう設定します。他のクライアントからのトラフィックには RED アルゴリズムを適用し、輻輳発生時にこれらのトラフィックが段階的に破棄されるようにします。
ここでは、3 つのトラフィッククラスを持つ QoS ポリシーを作成します。

	条件	最小帯域	最大帯域	RED カーブ
1	SrcIP = 192.168.1.1	80Mbps	無制限	適用せず
2	SrcIP = 192.168.1.2	無制限	無制限	RED カーブ「5」
3	SrcIP = 192.168.1.3	無制限	無制限	RED カーブ「6」

表 12: トラフィッククラスの設定

以下、設定内容を示します。

1. QoS ポリシー「1」を作成します。

   ```
   CREATE QOS POLICY=1 ↵
   ```

2. QoS ポリシー「1」を出力スイッチポートである 4 に関連付けます。

   ```
   SET QOS PORT=4 POLICY=1 ↵
   ```

3. トラフィッククラス「2」「3」に適用する RED カーブ「5」「6」を作成します。

   ```
   CREATE QOS RED=5 START=80 STOP=90 DROPPROB=50 ↵
   CREATE QOS RED=6 START=40 STOP=50 DROPPROB=95 ↵
   ```

✎ RED カーブ「0」〜「4」はデフォルトで定義済みです。

4. 各クライアントに対応する 3 つのトラフィッククラスを作成し、それぞれに最大・最小帯域を割り当て、重み付けを設定します。

```
CREATE QOS TRAFFICCLASS=1 MINBANDWIDTH=80000 WEIGHT=1 ↵
CREATE QOS TRAFFICCLASS=2 MINBANDWIDTH=0 WEIGHT=10 ↵
CREATE QOS TRAFFICCLASS=3 MINBANDWIDTH=0 WEIGHT=1024 ↵
```

   重み付けの設定により、出力ポートの帯域 100Mbps から最低保証帯域 80Mbps を引いた残りの 20Mbps は、トラフィッククラス 1、2、3 の優先順位で配分されます。

5. 最小帯域を保証するトラフィッククラス「1」以外に RED カーブを適用します。

```
SET QOS TRAFFICCLASS=2 RED=5 ↵
SET QOS TRAFFICCLASS=3 RED=6 ↵
```

   RED カーブの設定ポリシーは次のとおりです。
   - 輻輳発生時には、最初にトラフィッククラス「3」を破棄します。
   - それでも輻輳が軽減されないときは、トラフィッククラス「2」を破棄して、トラフィッククラス「1」の帯域を確保しようとします。

6. QoS ポリシーにトラフィッククラスを割り当てます。

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

7. 各トラフィッククラスに対応する 3 つのフローグループを作成します。

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

8. トラフィッククラスにフローグループを割り当てます。

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

9. 各クライアントからのパケットに対応するクラシファイアを定義します。

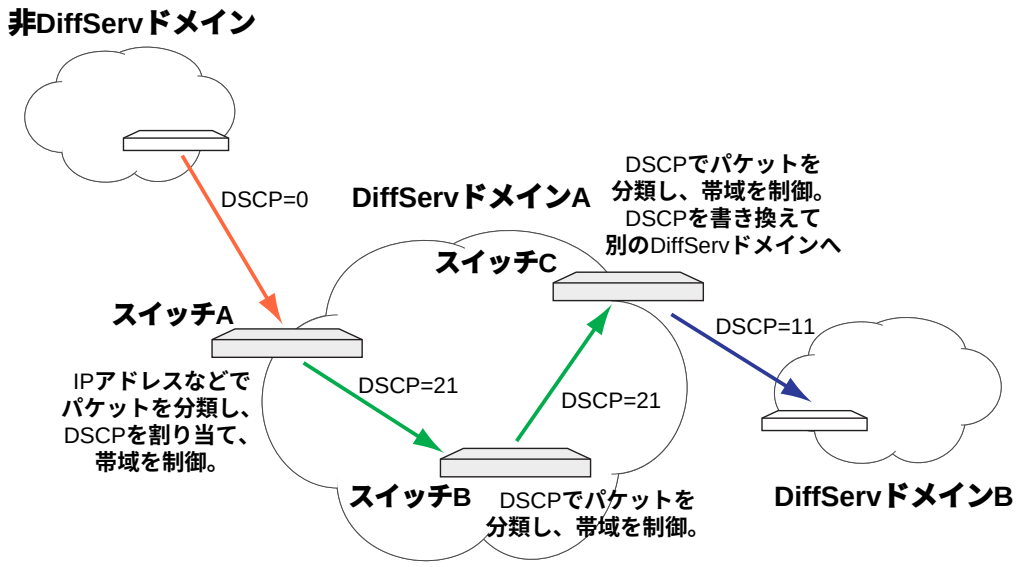
```
CREATE CLASSIFIER=1 IPSADDR=192.168.1.1/32 ↵
CREATE CLASSIFIER=2 IPSADDR=192.168.1.2/32 ↵
CREATE CLASSIFIER=3 IPSADDR=192.168.1.3/32 ↵
```

10. フローグループにクラシファイアを割り当てます。

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

DiffServ

DiffServ（Differentiated Service）は、ネットワーク境界（エッジ）で流入トラフィックをクラス分け・マーキングし、ネットワーク内部ではマーカーだけを見て QoS を適用できるようにする技術です。
DiffServ では、マーキング用に IP ヘッダーの TOS オクテットを再定義しています。従来、TOS オクテットは 3 ビットの優先度フィールドと、3 または 4 ビットの TOS フラグフィールド、および予約済みフィールドで構成されていましたが、DiffServ では先頭 6 ビットを DSCP（DiffServ Code Point）として定義しなおしています。DSCP フィールドは 0〜63 の値をとるマーカーフィールドであり、各値の意味は個々のネットワーク主体（DiffServ ドメイン）が独自に定義します。たとえば、DSCP=20 は低遅延・狭帯域、DSCP=21 は中遅延・広帯域などといった定義が可能です。



ここでは、スイッチ A、B、C の DiffServ 設定を示します。
スイッチ A の設定

1. QoS ポリシー「1」を作成します。

   ```
   CREATE QOS POLICY=1 ↵
   ```

2. QoS ポリシー「1」をスイッチポートに関連付けます。

```
SET QOS PORT=8 POLICY=1 ↵
```

3. 8 つのトラフィッククラス「1」～「8」を定義し、それぞれに最小帯域を割り当てます。また、各クラスに対し、DSCP 値「21」～「28」を付加するよう設定します。

```
CREATE QOS TRAFFICCLASS=1 MINBANDWIDTH=20M MARKVALUE=21 ↵
CREATE QOS TRAFFICCLASS=2 MINBANDWIDTH=10M MARKVALUE=22 ↵
CREATE QOS TRAFFICCLASS=3 MINBANDWIDTH=5M MARKVALUE=23 ↵
CREATE QOS TRAFFICCLASS=4 MINBANDWIDTH=3M MARKVALUE=24 ↵
CREATE QOS TRAFFICCLASS=5 MINBANDWIDTH=1M MARKVALUE=25 ↵
CREATE QOS TRAFFICCLASS=6 MINBANDWIDTH=1M MARKVALUE=26 ↵
CREATE QOS TRAFFICCLASS=7 MINBANDWIDTH=1M MARKVALUE=27 ↵
CREATE QOS TRAFFICCLASS=8 MINBANDWIDTH=1M MARKVALUE=28 ↵
```

4. トラフィッククラス「1」～「8」を QoS ポリシー「1」に割り当てます。

```
ADD QOS POLICY=1 TRAFFICCLASS=1-8 ↵
```

5. トラフィックグループ「1」～「8」と 1 対 1 で対応するフローグループ「1」～「8」を作成します。

```
CREATE QOS FLOWGROUP=1 ↵
CREATE QOS FLOWGROUP=2 ↵
CREATE QOS FLOWGROUP=3 ↵
CREATE QOS FLOWGROUP=4 ↵
CREATE QOS FLOWGROUP=5 ↵
CREATE QOS FLOWGROUP=6 ↵
CREATE QOS FLOWGROUP=7 ↵
CREATE QOS FLOWGROUP=8 ↵
```

6. トラフィッククラス「1」～「8」にフローグループ「1」～「8」を割り当てます。

```
ADD QOS TRAFFICCLASS=1 FLOWGROUP=1 ↵
ADD QOS TRAFFICCLASS=2 FLOWGROUP=2 ↵
ADD QOS TRAFFICCLASS=3 FLOWGROUP=3 ↵
ADD QOS TRAFFICCLASS=4 FLOWGROUP=4 ↵
ADD QOS TRAFFICCLASS=5 FLOWGROUP=5 ↵
ADD QOS TRAFFICCLASS=6 FLOWGROUP=6 ↵
ADD QOS TRAFFICCLASS=7 FLOWGROUP=7 ↵
ADD QOS TRAFFICCLASS=8 FLOWGROUP=8 ↵
```

7. ヘッダー情報に基づいてパケットを分類するクラシファイアを作成します。

```
CREATE CLASSIFIER=1 TCPSPORT=80 ↵
CREATE CLASSIFIER=2 TCPSPORT=20 ↵
CREATE CLASSIFIER=3 TCPSPORT=25 ↵
CREATE CLASSIFIER=4 IPPROTOCOL=TCP ↵
CREATE CLASSIFIER=5 UDPSPORT=53 ↵
CREATE CLASSIFIER=6 UDPDPORT=53 ↵
CREATE CLASSIFIER=7 IPPROTOCOL=UDP ↵
CREATE CLASSIFIER=8 IPPROTOCOL=ICMP ↵
```

✎ 本例はあくまでも説明のためのサンプルです。トラフィッククラスは綿密な計画とテストに基づいて作成してください。

8. フローグループにクラシファイアを割り当てます。

```
ADD QOS FLOWGROUP=1 CLASSIFIER=1 ↵
ADD QOS FLOWGROUP=2 CLASSIFIER=2 ↵
ADD QOS FLOWGROUP=3 CLASSIFIER=3 ↵
ADD QOS FLOWGROUP=4 CLASSIFIER=4 ↵
ADD QOS FLOWGROUP=5 CLASSIFIER=5 ↵
ADD QOS FLOWGROUP=6 CLASSIFIER=6 ↵
ADD QOS FLOWGROUP=7 CLASSIFIER=7 ↵
ADD QOS FLOWGROUP=8 CLASSIFIER=8 ↵
```

スイッチ B の設定

1. QoS ポリシー「1」を作成します。

```
CREATE QOS POLICY=1 ↵
```

2. QoS ポリシー「1」をスイッチポートに関連付けます。

```
SET QOS PORT=8 POLICY=1 ↵
```

3. DSCP 値「21」～「28」に対応する 8 つのトラフィッククラスを定義し、それぞれに最小帯域を割り当てます。

```
CREATE QOS TRAFFICCLASS=1 MINBANDWIDTH=20M ↵
CREATE QOS TRAFFICCLASS=2 MINBANDWIDTH=10M ↵
CREATE QOS TRAFFICCLASS=3 MINBANDWIDTH=5M ↵
CREATE QOS TRAFFICCLASS=4 MINBANDWIDTH=3M ↵
CREATE QOS TRAFFICCLASS=5 MINBANDWIDTH=1M ↵
CREATE QOS TRAFFICCLASS=6 MINBANDWIDTH=1M ↵
CREATE QOS TRAFFICCLASS=7 MINBANDWIDTH=1M ↵
CREATE QOS TRAFFICCLASS=8 MINBANDWIDTH=1M ↵
```

4. トラフィッククラス「1」～「8」を QoS ポリシー「1」に割り当てます。

```
ADD QOS POLICY=1 TRAFFICCLASS=1-8 ↵
```

5. トラフィックグループ「1」～「8」と 1 対 1 で対応するフローグループ「1」～「8」を作成します。

```
CREATE QOS FLOWGROUP=1 ↵
CREATE QOS FLOWGROUP=2 ↵
CREATE QOS FLOWGROUP=3 ↵
CREATE QOS FLOWGROUP=4 ↵
CREATE QOS FLOWGROUP=5 ↵
CREATE QOS FLOWGROUP=6 ↵
CREATE QOS FLOWGROUP=7 ↵
CREATE QOS FLOWGROUP=8 ↵
```

6. トラフィッククラス「1」～「8」にフローグループ「1」～「8」を割り当てます。

```
ADD QOS TRAFFICCLASS=1 FLOWGROUP=1 ↵
ADD QOS TRAFFICCLASS=2 FLOWGROUP=2 ↵
ADD QOS TRAFFICCLASS=3 FLOWGROUP=3 ↵
ADD QOS TRAFFICCLASS=4 FLOWGROUP=4 ↵
ADD QOS TRAFFICCLASS=5 FLOWGROUP=5 ↵
ADD QOS TRAFFICCLASS=6 FLOWGROUP=6 ↵
ADD QOS TRAFFICCLASS=7 FLOWGROUP=7 ↵
ADD QOS TRAFFICCLASS=8 FLOWGROUP=8 ↵
```

7. IP ヘッダーの DSCP 値によってパケットを分類するクラシファイアを作成します。

```
CREATE CLASSIFIER=1 IPDSCP=21 ↵
CREATE CLASSIFIER=2 IPDSCP=22 ↵
CREATE CLASSIFIER=3 IPDSCP=23 ↵
CREATE CLASSIFIER=4 IPDSCP=24 ↵
CREATE CLASSIFIER=5 IPDSCP=25 ↵
CREATE CLASSIFIER=6 IPDSCP=26 ↵
CREATE CLASSIFIER=7 IPDSCP=27 ↵
CREATE CLASSIFIER=8 IPDSCP=28 ↵
```

8. フローグループにクラシファイアを割り当てます。

```
ADD QOS FLOWGROUP=1 CLASSIFIER=1 ↵
ADD QOS FLOWGROUP=2 CLASSIFIER=2 ↵
ADD QOS FLOWGROUP=3 CLASSIFIER=3 ↵
ADD QOS FLOWGROUP=4 CLASSIFIER=4 ↵
ADD QOS FLOWGROUP=5 CLASSIFIER=5 ↵
ADD QOS FLOWGROUP=6 CLASSIFIER=6 ↵
ADD QOS FLOWGROUP=7 CLASSIFIER=7 ↵
ADD QOS FLOWGROUP=8 CLASSIFIER=8 ↵
```

スイッチ C の設定

1. QoS ポリシー「1」を作成します。

```
CREATE QOS POLICY=1 ↵
```

2. QoS ポリシー「1」をスイッチポートに関連付けます。

```
SET QOS PORT=8 POLICY=1 ↵
```

3. DSCP 値「21」～「28」に対応する 8 つのトラフィッククラスを定義し、それぞれに最小帯域を割り当てます。また、各クラスに対し、DSCP 値を「11」～「18」に書き換えるよう設定します。

```
CREATE QOS TRAFFICCLASS=1 MINBANDWIDTH=20M MARKVALUE=11 ↵
CREATE QOS TRAFFICCLASS=2 MINBANDWIDTH=10M MARKVALUE=12 ↵
CREATE QOS TRAFFICCLASS=3 MINBANDWIDTH=5M MARKVALUE=13 ↵
CREATE QOS TRAFFICCLASS=4 MINBANDWIDTH=3M MARKVALUE=14 ↵
CREATE QOS TRAFFICCLASS=5 MINBANDWIDTH=1M MARKVALUE=15 ↵
CREATE QOS TRAFFICCLASS=6 MINBANDWIDTH=1M MARKVALUE=16 ↵
CREATE QOS TRAFFICCLASS=7 MINBANDWIDTH=1M MARKVALUE=17 ↵
CREATE QOS TRAFFICCLASS=8 MINBANDWIDTH=1M MARKVALUE=18 ↵
```

4. トラフィッククラス「1」～「8」を QoS ポリシー「1」に割り当てます。

```
ADD QOS POLICY=1 TRAFFICCLASS=1-8 ↵
```

5. トラフィックグループ「1」～「8」と 1 対 1 で対応するフローグループ「1」～「8」を作成します。

```
CREATE QOS FLOWGROUP=1 ↵
CREATE QOS FLOWGROUP=2 ↵
CREATE QOS FLOWGROUP=3 ↵
CREATE QOS FLOWGROUP=4 ↵
CREATE QOS FLOWGROUP=5 ↵
CREATE QOS FLOWGROUP=6 ↵
CREATE QOS FLOWGROUP=7 ↵
CREATE QOS FLOWGROUP=8 ↵
```

6. トラフィッククラス「1」～「8」にフローグループ「1」～「8」を割り当てます。

```
ADD QOS TRAFFICCLASS=1 FLOWGROUP=1 ↵
ADD QOS TRAFFICCLASS=2 FLOWGROUP=2 ↵
ADD QOS TRAFFICCLASS=3 FLOWGROUP=3 ↵
ADD QOS TRAFFICCLASS=4 FLOWGROUP=4 ↵
ADD QOS TRAFFICCLASS=5 FLOWGROUP=5 ↵
ADD QOS TRAFFICCLASS=6 FLOWGROUP=6 ↵
ADD QOS TRAFFICCLASS=7 FLOWGROUP=7 ↵
ADD QOS TRAFFICCLASS=8 FLOWGROUP=8 ↵
```

7. IP ヘッダーの DSCP 値によってパケットを分類するクラシファイアを作成します。

```
CREATE CLASSIFIER=1 IPDSCP=21 ↵
CREATE CLASSIFIER=2 IPDSCP=22 ↵
CREATE CLASSIFIER=3 IPDSCP=23 ↵
CREATE CLASSIFIER=4 IPDSCP=24 ↵
CREATE CLASSIFIER=5 IPDSCP=25 ↵
CREATE CLASSIFIER=6 IPDSCP=26 ↵
CREATE CLASSIFIER=7 IPDSCP=27 ↵
CREATE CLASSIFIER=8 IPDSCP=28 ↵
```

8. フローグループにクラシファイアを割り当てます。

```
ADD QOS FLOWGROUP=1 CLASSIFIER=1 ↵
ADD QOS FLOWGROUP=2 CLASSIFIER=2 ↵
ADD QOS FLOWGROUP=3 CLASSIFIER=3 ↵
ADD QOS FLOWGROUP=4 CLASSIFIER=4 ↵
ADD QOS FLOWGROUP=5 CLASSIFIER=5 ↵
ADD QOS FLOWGROUP=6 CLASSIFIER=6 ↵
ADD QOS FLOWGROUP=7 CLASSIFIER=7 ↵
ADD QOS FLOWGROUP=8 CLASSIFIER=8 ↵
```

ハードウェアパケットフィルター

ハードウェアパケットフィルターは、ハードウェア（ASIC）レベルでパケットをフィルタリング（許可・拒否）する機能です。

✎ ファイアウォールとハードウェアパケットフィルターは併用可能です。ただしその場合、ハードウェアパケットフィルターはスイッチングされるパケットにだけ適用され、ルーティングされるパケットには適用されません。なお、ファイアウォール機能が無効であっても、ファイアウォールポリシーにインターフェース（VLAN）を追加すると、本件においてはファイアウォールを併用していることになりますのでご注意ください。なお、ファイアウォールポリシーに追加されたインターフェース（VLAN）経由の通信（ルーティング）はソフトウェア処理となります。

ハードウェアパケットフィルターには以下の特長があります。

- ハードウェアで処理するため、ソフトウェア処理のファイアウォールよりも高速
- 出力ポート単位でフィルタリングが可能（ファイアウォールは VLAN 単位）
- ルーティングされないトラフィック（同一 VLAN 内のトラフィック）に対してもフィルタリングが可能（たとえば、IP モジュールを有効にしていない状態、すなわちレイヤー 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。フィルタリング条件は、汎用のパケットフィルターであるクラシファイアによって定義します。クラシファイアの詳細については「スイッチング」の「クラシファイア」をご覧ください。

- 出力スイッチポート
- 入力 VLAN、出力 VLAN
- Ethernet のフレームフォーマット、プロトコルタイプ
- レイヤー 2 アドレス種別（ユニキャストとそれ以外）
- IP ヘッダーの TOS 優先度（precedence）、DSCP（DiffServ Code Point）、プロトコル、始点・終点 IP アドレス
- IPX ヘッダーの終点ネットワーク、始点・終点ソケット
- TCP ヘッダーの始点・終点ポート
- UDP ヘッダーの始点・終点ポート

条件に一致したパケットに対しては、以下の処理（アクション）が可能です。アクションは最初に一致したエントリーで適用されます。どのエントリーにも一致しなかったパケットは通常通り処理（転送）されます。

- 転送（Forward）
- 破棄（Discard）

✎ ハードウェアパケットフィルターの設定コマンド（ADD SWITCH HWFILTER コマンド（100 ページ））には、転送、破棄以外にデバッグ用のアクションが存在しますが、通常の運用では使わないためここでは触れません。

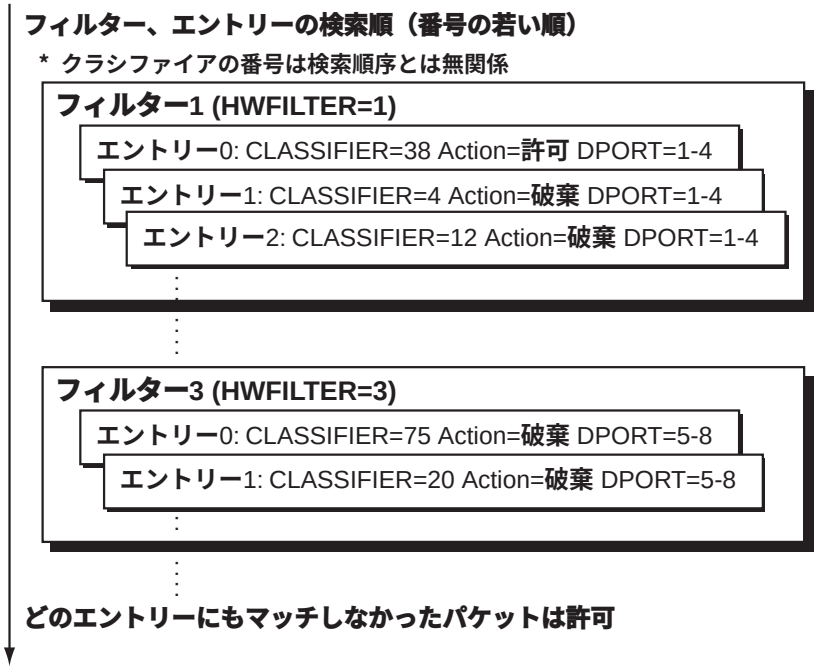
基本動作

ハードウェアパケットフィルターの基本動作について説明します。

フィルターの構成

ハードウェアパケットフィルターは、複数のエントリーをリストとして保持する「フィルター」と、個々の「エントリー」から構成されます。エントリーは、クラシファイア（汎用パケットフィルター）とアクション、および適用対象のスイッチポート（送出ポート）で構成されます。

✎ スイッチ本体宛てのパケット、および、スイッチ本体から送信されるパケットへの適用条件については、本章の「本体宛てのパケットと本体発のパケット」をご覧ください。



フィルター処理の流れ

ハードウェアパケットフィルターの処理は、パケット送信時に、おおむね次の手順にしたがって行われます。

✎ 以下の説明は、設定上の便宜を最優先して書いたものであり、実際の内部動作を正確に記述したものではありません。あらかじめご了承ください。

1. ハードウェアパケットフィルターが 1 つでも定義されている場合、送信パケットとフィルターエントリーを、フィルター番号の小さい順、エントリー番号の小さい順に照合します。
2. 一致するエントリーが見つかった場合は、その場でアクション（破棄か転送）を実行し、フィルターの処理を完了します。
3. 一致するエントリーがなかった場合はフィルター処理を完了し、通常どおりパケットを出力します。

設定手順

ハードウェアパケットフィルターの設定は、次の流れで行います。

1. クラシファイアの作成（CREATE CLASSIFIER コマンド（114 ページ））
2. フィルターエントリーの追加（ADD SWITCH HWFILTER コマンド（100 ページ））

以下、各手順について詳しく解説します。
ここでは例として、ホスト 192.168.100.38 から、ポート 8 に接続されているサーバー 192.168.10.5 宛てのパケットを遮断するよう設定します。

1. クラシファイアを作成します。詳細は「スイッチング」の「クラシファイア」をご覧ください。

   ```
   CREATE CLASSIFIER=1 IPDADDR=192.168.10.5 IPSADDR=192.168.100.38 ↵
   ```

   ✎ クラシファイアの設定において、ファイアウォールポリシーに追加されたインターフェース（VLAN）を SVLAN に指定しないでください。指定した場合、そのクラシファイアは、ルーティングパケットに対しては機能しません（スイッチングパケットに対しては機能します）。この現象は、ファイアウォール機能が無効であっても発生するのでご注意ください。

2. ハードウェアパケットフィルターにエントリーを追加します。エントリーを追加するには、クラシファイア、マッチ時のアクション（転送か破棄）、エントリーを適用する送出ポートの指定が必要です。

   ```
   ADD SWITCH HWFILTER=1 CLASSIFIER=1 ACTION=DISCARD DPORT=8 ↵
   ```

✎ DPORT（送出スイッチポート）には、可能な限り、フィルターを適用したいポートだけを指定するようにしてください。CREATE CLASSIFIER コマンド（114 ページ）で IPDADDR、IPXDADDR を指定している場合、ADD SWITCH HWFILTER コマンド（100 ページ）の DPORT パラメーターに指定したポートの数だけ内部テーブル領域が消費されます。ADD SWITCH HWFILTER コマンド（100 ページ）の実行時に「Insufficient space in the hardware packet classifier tables.」というエラーメッセージが表示されたときは、DPORT パラメーターに指定するポートを限定できないか確認してください。特に「DPORT=ALL」は、本当に必要なとき以外使わないでください。詳しくは本章の「DPORT 指定に関する注意」をご参照ください。

✎ DPORT に ALL 以外を指定した場合、複数ポートへ出力されるブロードキャスト、マルチキャスト、未学習ユニキャストパケットはフィルターの適用対象になりません。

✎ スイッチ本体宛てのパケット、および、スイッチ本体から送信されるパケットへの適用条件については、本章の「本体宛てのパケットと本体発のパケット」をご覧ください。

基本設定は以上です。

コマンド例

次に具体的なコマンド例を示します。

■ グローバルネットワークに出すべきでないパケット（始点がプライベート、ループバック、マルチキャスト、実験用アドレスのもの）を遮断する。ここでは、ポート 12 がグローバルネットワークに接続されているものと仮定している。

```
CREATE CLASSIFIER=1 IPSADDR=10.0.0.0/8 ↵
CREATE CLASSIFIER=2 IPSADDR=127.0.0.0/8 ↵
CREATE CLASSIFIER=3 IPSADDR=169.254.0.0/16 ↵
CREATE CLASSIFIER=4 IPSADDR=172.16.0.0/12 ↵
CREATE CLASSIFIER=5 IPSADDR=192.168.0.0/16 ↵
CREATE CLASSIFIER=6 IPSADDR=224.0.0.0/3 ↵
CREATE CLASSIFIER=7 IPSADDR=0.0.0.0/8 ↵
ADD SWITCH HWFILTER=1 CLASSIFIER=1-7 ACTION=DISCARD DPORT=12 ↵
```

■ 192.168.10.100 から 192.168.20.0/24 への IP パケットを破棄。ここでは、192.168.20.0/24 がスイッチポート 5-8 に接続されていると仮定している。

```
CREATE CLASSIFIER=1 IPSADDR=192.168.10.100/32 IPDADDR=192.168.20.0/24 ↵
ADD SWITCH HWFILTER=1 CLASSIFIER=1 ACTION=DISCARD DPORT=5-8 ↵
```

■ ポート 2 から送信される ICMP パケットを破棄

```
CREATE CLASSIFIER=1 IPPROTOCOL=ICMP ↵
ADD SWITCH HWFILTER=1 CLASSIFIER=1 ACTION=DISCARD DPORT=2 ↵
```

■ 192.168.30.100 への telnet パケットを破棄。ここでは、192.168.30.100 がスイッチポート 4 に接続されていると仮定している。

```
CREATE CLASSIFIER=1 IPDADDR=192.168.30.100/32 TCPDPORT=23 ↵
ADD SWITCH HWFILTER=1 CLASSIFIER=1 ACTION=DISCARD DPORT=4 ↵
```

■ ハードウェアパケットフィルターは、ルーティングされない同一 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 IP 通信を拒否」するつもりで次のような設定を行うと、192.168.10.0/24 内でも IP 通信ができなくなってしまいます。

```
CREATE CLASSIFIER=1 IPSADDR=192.168.10.0/24 ↵
ADD SWITCH HWFILTER=1 CLASSIFIER=1 ACTION=DISCARD DPORT=ALL ↵
```

通常、ネットワーク単位でフィルターを設定するときは、次の例のように、フィルターエントリーを適用する送出ポート（DPORT）を限定してください。ここでは、192.168.10.0/24 がスイッチポート 1-4 に接続されていると仮定しています。

```
CREATE CLASSIFIER=1 IPSADDR=192.168.10.0/24 ↵
ADD SWITCH HWFILTER=1 CLASSIFIER=1 ACTION=DISCARD DPORT=5-12 ↵
```

✎ DPORT（送出スイッチポート）には、可能な限り、フィルターを適用したいポートだけを指定するようにしてください。CREATE CLASSIFIER コマンド（114 ページ）で IPDADDR、IPXDADDR を指定している場合、ADD SWITCH HWFILTER コマンド（100 ページ）の DPORT パラメーターに指定したポートの数だけ内部テーブル領域が消費されます。ADD SWITCH HWFILTER コマンド（100 ページ）の実行時に「Insufficient space in the hardware packet classifier tables.」というエラーメッセージが表示されたときは、DPORT パラメーターに指定するポートを限定できないか確認してください。特に「DPORT=ALL」は、本当に必要なとき以外使わないでください。詳しくは本章の「DPORT 指定に関する注意」をご参照ください。

✎ ハードウェアパケットフィルターでは、最初にマッチしたエントリーのアクションが実行されます。デフォルト拒否の設定を行うには、最初に許可するエントリーを並べた上で、最後にすべてを破棄するエントリーを設定します。また、デフォルト許可に設定する場合は、拒否するエントリーだけを並べていきます。ハードウェアパケットフィルター自体は、デフォルト許可です。

■ ハードウェアパケットフィルターを使用するために、必ずしも IP モジュールを有効にする必要はありません。純粋なレイヤー 2 スイッチとして本製品を使用する場合であっても、ハードウェアパケットフィルターを使えば、IP アドレスやプロトコルに応じたフィルタリングが可能です。

■ ハードウェアパケットフィルターの一覧を表示するには、SHOW SWITCH HWFILTER コマンド（274 ページ）を使います。

```
SHOW SWITCH HWFILTER ↵
```

■ クラシファイアの一覧を表示するには、SHOW CLASSIFIER コマンド（230 ページ）を実行します。CLASSIFIER パラメーターに番号を指定すれば、該当するクラシファイアの詳細なパラメーターが表示されます。

```
SHOW CLASSIFIER ↵
SHOW CLASSIFIER=1-3 ↵
SHOW CLASSIFIER=ALL ↵
```

■ ハードウェアパケットフィルターからエントリーを削除するには、DELETE SWITCH HWFILTER コマンド（137 ページ）を使います。
次のようにクラシファイア番号だけを指定したときは、該当する番号のクラシファイアを持つエントリーがすべて削除されます。同じクラシファイアを複数のエントリーで使用している場合、該当するすべてのエントリーが削除されます。

```
DELETE SWITCH HWFILTER=1 CLASSIFIER=2 ↵
DELETE SWITCH HWFILTER=1 CLASSIFIER=5-8 ↵
```

次のようにクラシファイア番号とエントリー番号（エントリー位置を示す番号）を指定すれば、同じクラシファイアを複数回使用している場合でも、特定のエントリーだけを削除できます。

```
DELETE SWITCH HWFILTER=1 CLASSIFIER=3 RULEPOS=4 ↵
```

✎ 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 HWFILTER コマンド（274 ページ）を実行し、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。

■ ハードウェアパケットフィルター全体を削除するには、DELETE SWITCH HWFILTER コマンド（137 ページ）にフィルター番号だけを指定します。これにより、フィルター内の全エントリーが削除されます。また、CLASSIFIER パラメーターに ALL を指定しても同じことができます。

```
DELETE SWITCH HWFILTER=1 ↵
DELETE SWITCH HWFILTER=1 CLASSIFIER=ALL ↵
```

✎ ハードウェアパケットフィルターやエントリーを削除しても、クラシファイアは削除されません。ハードウェアパケットフィルターとクラシファイアの関連付けが削除されるだけです。クラシファイアを削除するには、DESTROY CLASSIFIER コマンド（147 ページ）を使います。

注意事項

ここでは、設定時に注意が必要なハードウェアパケットフィルターの仕様について解説します。

DPORT 指定について

IPDADDR / IPXDADDR を条件に含むクラシファイアは、適用ポート（DPORT）の数だけ内部テーブルエントリーを消費します。IPDADDR / IPXDADDR 用の内部エントリー容量は 62 個なので、適用ポートを限定するなどして（例：「DPORT=ALL」の指定を避ける）、エントリー消費数が 62 個以内におさまるよう工夫してください。

■ 一例として、次のようなハードウェアパケットフィルターを定義したとします。

```
CREATE CLASSIFIER=1 IPDADDR=10.1.2.0/24
ADD SWITCH HWFILTER=1 CLASSIFIER=1 ACTION=DISCARD DPORT=ALL
```

クラシファイア「1」は IPDADDR を条件に含んでいるため、適用ポート数分の内部エントリーを消費します。ここでは、「DPORT=ALL」が指定されているため、適用ポート数は 16 となり、結果的に内部エントリーを 16 個も消費してしまいます。
回避策としては、DPORT に ALL ではなく本当に必要なポートだけを指定します。たとえば、10.1.2.0 / 24 のネットワークがポート 1〜3 に接続されているなら、DPORT の指定を次のように変更することで、消費エントリー数を 3 個にまで減らせます。

```
CREATE CLASSIFIER=1 IPDADDR=10.1.2.0/24
ADD SWITCH HWFILTER=1 CLASSIFIER=1 ACTION=DISCARD DPORT=1-3
```

本体宛てのパケットと本体発のパケット

本体（CPU）宛てのパケットと本体から送信されるパケットに対して、ハードウェアパケットフィルターは次のように適用されます。

本体宛てのパケット

スイッチ本体（CPU）宛てのパケットに対し、ハードウェアパケットフィルターは次のように動作します。

- DPORT=ALL を指定した場合、このフィルターはすべての CPU 宛てパケットに適用されます。
- DPORT に上記以外を指定した場合、このフィルターは CPU 宛てパケットには適用されません。

本体発のパケット

スイッチ本体（CPU）から送信されるパケットに対し、ハードウェアパケットフィルターは次のように動作します。レイヤー 2 のアドレス種別によって、動作が異なります。

- CPU 発のユニキャストパケットには、原則として通常どおりフィルターが適用されます。たとえば、DPORT=5 のフィルターは、ポート 5 から送信される CPU 発パケットに適用されます。
- CPU 発のマルチキャストパケットには、いっさいフィルターが適用されません。
- CPU 発のブロードキャストパケットには、下記のいずれかの条件を満たすフィルターだけが適用されます。いずれの条件も満たさないフィルターは適用されません。
  - DPORT=ALL が指定されている
  - DPORT に指定したポートの所属インスタンス内に、同一 VLAN 所属の他のポートが存在しない場合
  - DPORT に指定したポートの所属インスタンス内に、同一 VLAN 所属で、なおかつ、リンクアップしている他のポートが存在しない場合

DVLAN、SVLAN について

DVLAN を条件とするエントリーと SVLAN を条件とするエントリーがある場合、DVLAN と SVLAN の両方にマッチするパケットには、エントリーの順序とは関係なく、DISCARD アクションのエントリーが優先的に適用されます。
たとえば、次のようなフィルターを設定した場合、

```
CREATE CLASSIFIER=10 DVLAN=30 ↵
CREATE CLASSIFIER=20 SVLAN=10 ↵
ADD SWITCH HWFILTER=10 CLASSIFIER=20 ACTION=FORWARD DPORT=3 (1) ↵
ADD SWITCH HWFILTER=10 CLASSIFIER=10 ACTION=DISCARD DPORT=3 (2) ↵
```

VLAN 10 から VLAN 30 宛てのパケットは、1 つ目のエントリー (1) にマッチするためフォワードされると予測できますが、実際には 2 つ目のエントリー (2) が適用され破棄されてしまいます。2 つのエントリーの順番を入れ替えても同じ動作になります。

包含関係にあるネットワークアドレスについて

IPSADDR と IPDADDR の両方を指定した FORWARD エントリーが複数存在しており、なおかつ、これらのエントリーの IPSADDR が、後続する DISCARD エントリーの IPSADDR に包含されている場合、特定のパケットが意図したとおりに破棄されないことがあります。
たとえば、次の 3 つのフィルターエントリーが定義されている状況を考えます。

1. AS ＞ AD Forward
2. BS ＞ BD Forward
3. ZS ＞ ZD Discard

ここでは説明を簡単にするため、フィルターの条件とアクションを 1 行で表しています。「AS ＞ BS Forward」は AS から BS へのパケットを許可する、「ZS ＞ ZD Discard」は ZS から ZD へのパケットを破棄する、の意味になります。また、AS, BS, ZS, AD, BD, ZD は IP アドレスを示しています。先頭の番号はエントリー番号です。
このとき、アドレス ZS が AS と BS を包含していると（例：ZS = 192.168.0.0 / 16, AS = 192.168.10.0 / 24, BS = 192.168.20.0 / 24）、次の IP 通信が意図したとおりに破棄されません。

- AS ＞ BD
- BS ＞ AD

このようなときは、AS ＞ BD, BS ＞ AD を破棄するエントリーを明示的に追加してください。具体的には次の 3、4 番を追加します。

1. AS ＞ AD Forward
2. BS ＞ BD Forward
3. AS ＞ BD Discard
4. BS ＞ AD Discard
5. ZS ＞ ZD Discard

最後の DISCARD エントリーの IPSADDR（例では ZS）に包含されるアドレスが 2 個より多い場合も同様です。たとえば、次の 4 つのフィルターエントリーが定義されている状況を考えます。

1. AS ＞ AD Forward
2. BS ＞ BD Forward
3. CS ＞ CD Forward

4. ZS > ZD Discard

このとき、アドレス ZS が AS、BS、CS を包含していると、次の IP 通信が意図したとおりに破棄されません。

- AS > BD, AS > CD
- BS > AD, BS > CD
- CS > AD, CS > BD

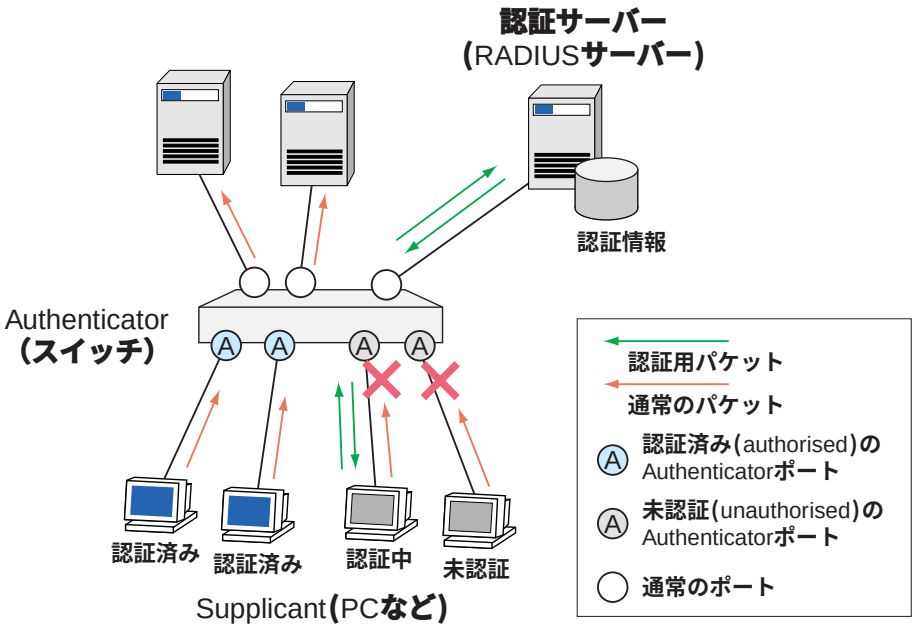
このようなときは、先ほどの例と同様に、AS > BD, AS > CD, BS > AD, BS > CD, CS > AD, CS > BD を破棄するエントリーを明示的に追加してください。

802.1X 認証

本製品は、ポート単位で LAN 上の機器を認証する IEEE 802.1X 認証（以下、802.1X 認証）に対応しています。
本機能を使用することにより、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、本製品が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

802.1X 認証のシステムは、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。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。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。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。

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。

要件

本製品を使って 802.1X 認証のシステムを運用する場合は、以下の要件を満たしている必要があります。

- 認証サーバー：本製品で 802.1X を運用する場合、認証方式「EAP-MD5」または「EAP-OTP（MD4/MD5）」に対応した RADIUS サーバーを用意する必要があります。
- Supplicant：本製品を Authenticator として使用する場合、Supplicant は認証方式「EAP-MD5」または「EAP-OTP（MD4/MD5）」に対応している必要があります。
- Authenticator：本製品を Supplicant として使用する場合、Authenticator は認証方式「EAP-MD5」または「EAP-OTP（MD4/MD5）」に対応している必要があります。

基本設定

本製品を使って 802.1X 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、認証方式として「EAP-MD5」を使うものと仮定します。

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。ここでは、ポート 5 で認証を行うものとします。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。

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。最初に 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 認証モジュールを有効にします。

   ```
   ENABLE PORTAUTH ↵
   ```

4. ポート 5 で認証を行うよう設定します。「TYPE=AUTHENTICATOR」の指定により、ポート 5 は Authenticator ポートとなります。

```
ENABLE PORTAUTH PORT=5 TYPE=AUTHENTICATOR ↵
```

✎ Authenticator ポートには、Supplicant を 1 台だけ接続してください。同一ポート下における複数 Supplicant の認証には対応していません。

✎ Authenticator ポートでは、ポートトランキング、スパニングツリープロトコル、ポートセキュリティーを使用できません。また、Authenticator 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（178 ページ）/SET PORTAUTH PORT コマンド（207 ページ）の CONTROL パラメーターを AUTHORISED に設定してください。

Supplicant

本製品を Supplicant として使用する場合の基本設定を示します。ここでは、ポート 1 が認証を受けるものとします。Supplicant としての動作においては、IP の設定は必須ではありません。

1. 802.1X 認証モジュールを有効にします。

   ```
   ENABLE PORTAUTH ↵
   ```

2. ポート 1 で認証を受けるよう設定します。認証を受けるためのユーザー名とパスワードを指定してください。「TYPE=SUPPLICANT」の指定により、ポート 1 は Supplicant ポートとなります。

   ```
   ENABLE PORTAUTH PORT=1 TYPE=SUPPLICANT USERNAME=atswitch
     PASSWORD=atpasswd ↵
   ```

✎ Supplicant ポートでは、ポートトランキング、スパニングツリープロトコル、ポートセキュリティーを使用できません。

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 165
DISABLE SWITCH STPFORWARD 171
ENABLE SWITCH DEBUG 188
ENABLE SWITCH STPFORWARD 194
RESET SWITCH 202
SHOW SWITCH 263
SHOW SWITCH COUNTER 265
SHOW SWITCH DEBUG 268

ポート

ACTIVATE SWITCH PORT AUTONEGOTIATE 91
ACTIVATE SWITCH PORT LOCK 92
ADD SWITCH TRUNK 102
CREATE SWITCH TRUNK 127
DELETE SWITCH TRUNK 139
DESTROY SWITCH TRUNK 153
DISABLE SWITCH HASH 166
DISABLE SWITCH MIRROR 168
DISABLE SWITCH PORT 169
DISABLE SWITCH PORT FLOW 170
ENABLE SWITCH HASH 189
ENABLE SWITCH MIRROR 191
ENABLE SWITCH PORT 192
ENABLE SWITCH PORT FLOW 193
RESET SWITCH PORT 203
SET SWITCH MIRROR 224
SET SWITCH PORT 225
SET SWITCH TRUNK 227
SHOW SWITCH PORT 276
SHOW SWITCH PORT COUNTER 280
SHOW SWITCH PORT INTRUSION 283
SHOW SWITCH TRUNK 284

バーチャル LAN

ADD VLAN ADDRESS 103
ADD VLAN LIMITEDPROTOCOL 105
ADD VLAN PORT 107

ADD VLAN PROTOCOL 110
ADD VLAN SUBNET 113
CREATE VLAN 128
DELETE VLAN ADDRESS 140
DELETE VLAN LIMITEDPROTOCOL 141
DELETE VLAN PORT 142
DELETE VLAN PROTOCOL 145
DELETE VLAN SUBNET 146
DESTROY VLAN 154
DISABLE VLAN DEBUG 172
DISABLE VLAN STORMPROTECT 173
ENABLE VLAN DEBUG 195
ENABLE VLAN STORMPROTECT 196
SET VLAN 228
SET VLAN PORT 229
SHOW VLAN 285
SHOW VLAN DEBUG 289
SHOW VLAN PORT 290

スパニングツリープロトコル

ADD STP VLAN 96
CREATE STP 126
DELETE STP VLAN 135
DESTROY STP 152
DISABLE STP 160
DISABLE STP DEBUG 161
DISABLE STP PORT 162
DISABLE STP PORT DEBUG 163
ENABLE STP 183
ENABLE STP DEBUG 184
ENABLE STP PORT 185
ENABLE STP PORT DEBUG 186
PURGE STP 199
RESET STP 201
SET STP 219
SET STP PORT 221
SHOW STP 255
SHOW STP COUNTER 258
SHOW STP DEBUG 260
SHOW STP PORT 261

フォワーディングデータベース

ADD SWITCH FILTER 98

DELETE SWITCH FILTER 136
DISABLE SWITCH AGEINGTIMER 164
DISABLE SWITCH LEARNING 167
ENABLE SWITCH AGEINGTIMER 187
ENABLE SWITCH LEARNING 190
SET SWITCH AGEINGTIMER 223
SHOW SWITCH FDB 269
SHOW SWITCH FILTER 272

クラシファイア

CREATE CLASSIFIER 114
DESTROY CLASSIFIER 147
SET CLASSIFIER 204
SHOW CLASSIFIER 230

ポリシーベース QoS

ADD QOS FLOWGROUP 93
ADD QOS POLICY 94
ADD QOS TRAFFICCLASS 95
CREATE QOS FLOWGROUP 119
CREATE QOS POLICY 120
CREATE QOS RED 122
CREATE QOS TRAFFICCLASS 124
DELETE QOS FLOWGROUP 132
DELETE QOS POLICY 133
DELETE QOS TRAFFICCLASS 134
DESTROY QOS FLOWGROUP 148
DESTROY QOS POLICY 149
DESTROY QOS RED 150
DESTROY QOS TRAFFICCLASS 151
DISABLE QOS DEBUG 158
DISABLE QOS VLANPRIORITYREMAPPING 159
ENABLE QOS DEBUG 181
ENABLE QOS VLANPRIORITYREMAPPING 182
PURGE QOS 198
SET QOS FLOWGROUP 212
SET QOS POLICY 213
SET QOS PORT 214
SET QOS RED 215
SET QOS TRAFFICCLASS 216
SET QOS VLANREMAP 218
SHOW QOS FLOWGROUP 246
SHOW QOS POLICY 248

SHOW QOS RED 250
SHOW QOS TRAFFICCLASS 252
SHOW QOS VLANPRIORITYREMAPPING 254

ハードウェアパケットフィルター

ADD SWITCH HWFILTER 100
DELETE SWITCH HWFILTER 137
SHOW SWITCH HWFILTER 274

802.1X 認証

ACTIVATE PORTAUTH PORT REAUTHENTICATE 90
DISABLE PORTAUTH 155
DISABLE PORTAUTH DEBUG 156
DISABLE PORTAUTH PORT 157
ENABLE PORTAUTH 174
ENABLE PORTAUTH DEBUG 175
ENABLE PORTAUTH PORT 178
PURGE PORTAUTH PORT 197
RESET PORTAUTH PORT 200
SET PORTAUTH PORT 207
SET PORTAUTH USERNAME 210
SHOW PORTAUTH 234
SHOW PORTAUTH COUNTER 236
SHOW PORTAUTH PORT 239
SHOW PORTAUTH TIMER 244

ACTIVATE PORTAUTH PORT REAUTHENTICATE

カテゴリー：スイッチング / 802.1X 認証

ACTIVATE PORTAUTH PORT={***port-list***|**ALL**} **REAUTHENTICATE**

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、Supplicant を再認証する。

パラメーター

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、Authenticator として設定されているポート（TYPE=AUTHENTICATOR または TYPE=BOTH）でのみ、認証プロセスが再実行される。

例

■ポート 5 で Supplicant を再認証する。

```
ACTIVATE PORTAUTH PORT=5 REAUTHENTICATE
```

関連コマンド

ENABLE PORTAUTH（174 ページ）
ENABLE PORTAUTH PORT（178 ページ）
SHOW PORTAUTH PORT（239 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（225 ページ）
SHOW SWITCH PORT（276 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ー機能）。
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ー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（225 ページ）
SHOW SWITCH PORT（276 ページ）

ADD QOS FLOWGROUP

カテゴリー：スイッチング / ポリシーベース QoS

ADD QOS FLOWGROUP=*flow-id* CLASSIFIER=*rule-list*

flow-id: フローグループ番号（0〜1023）
rule-list: クラシファイア番号（1〜9999。ハイフン、カンマを使った複数指定も可能）

解説

フローグループにクラシファイア（汎用パケットフィルター）を割り当てる。

パラメーター

FLOWGROUP　フローグループ番号
CLASSIFIER　クラシファイア番号。複数指定も可能。クラシファイアは、本コマンドで追加した順序で照合される。

例

■フローグループ「100」にクラシファイア「1」「5」「6」をこの順序で追加する。

```
ADD QOS FLOWGROUP=100 CLASSIFIER=1,5-6
```

関連コマンド

CREATE QOS FLOWGROUP（119 ページ）
DELETE QOS FLOWGROUP（132 ページ）
DESTROY QOS FLOWGROUP（148 ページ）
SET QOS FLOWGROUP（212 ページ）
SHOW QOS FLOWGROUP（246 ページ）

ADD QOS POLICY

カテゴリー：スイッチング / ポリシーベース QoS

ADD QOS POLICY=*qos-id* TRAFFICCLASS=*tc-list*

qos-id: QoS ポリシー番号（0〜255）
tc-list: トラフィッククラス番号（0〜511。ハイフン、カンマを使った複数指定も可能）

解説

QoS ポリシーにトラフィッククラスを割り当てる。

パラメーター

POLICY　QoS ポリシー番号

TRAFFICCLASS　トラフィッククラス番号。複数指定が可能。クラシファイアの照合は、ポリシー内のトラフィッククラス順、トラフィッククラス内のフローグループ順、フローグループ内のクラシファイア順に行われる。トラフィッククラスの順番は、本コマンドでポリシーに追加した順序となる。

例

■QoS ポリシー「10」にトラフィッククラス「1」「2」「3」をこの順序で追加する。

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

関連コマンド

CREATE QOS POLICY（120 ページ）
DELETE QOS POLICY（133 ページ）
DESTROY QOS POLICY（149 ページ）
SET QOS POLICY（213 ページ）
SET QOS PORT（214 ページ）
SHOW QOS POLICY（248 ページ）

ADD QOS TRAFFICCLASS

カテゴリー：スイッチング / ポリシーベース QoS

ADD QOS TRAFFICCLASS=*tc-id* FLOWGROUP=*flow-list*

tc-id: トラフィッククラス番号（0〜511）
flow-list: フローグループ番号（0〜1023。ハイフン、カンマを使った複数指定も可能）

解説

トラフィッククラスにフローグループを割り当てる。

パラメーター

TRAFFICCLASS　トラフィッククラス番号

FLOWGROUP　フローグループ番号。複数指定が可能。クラシファイアの照合は、ポリシー内のトラフィッククラス順、トラフィッククラス内のフローグループ順、フローグループ内のクラシファイア順に行われる。フローグループの順番は、本コマンドでトラフィッククラスに割り当てた順序となる。

例

■トラフィッククラス「20」にフローグループ「1」「3」をこの順序で割り当てる。

```
ADD QOS TRAFFICCLASS=20 FLOWGROUP=1,3
```

関連コマンド

CREATE QOS TRAFFICCLASS（124 ページ）
DELETE QOS TRAFFICCLASS（134 ページ）
DESTROY QOS TRAFFICCLASS（151 ページ）
SET QOS TRAFFICCLASS（216 ページ）
SHOW QOS TRAFFICCLASS（252 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

ADD STP=*stpname* VLAN={*vlanname*|*2..4090*}

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（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。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。
・スイッチポートは複数の STP ドメインに所属することはできない。VLAN 内に、複数 VLAN に所属するポートが 1 つでも含まれている場合、その VLAN を default 以外の STP ドメインに参加させることはできない。そうした VLAN では、default STP を使う必要がある（VLAN はデフォルトで default STP 所属となる）。

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 に戻したいときは、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（135 ページ）
SHOW STP（255 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..4090*}]

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（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。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ーの学習済み 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ー機能は、SET SWITCH PORT コマンドの LEARN パラメーターで設定する。

VLAN　VLAN 名か VLAN ID（VID）。出力ポートに VLAN タグが設定されている場合に指定する。省略時は該当ポートのタグなし VLAN を指定したものと見なされる。そのため、ポートがタグ付き VLAN にしか所属していないとき（タグなし VLAN に所属していないとき）は省略できない。出力ポートがタグなしの場合は不要。

例

■ポート 10（タグなし）配下のステーションを FDB に登録する。

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

■ポート 6（タグなし）配下のステーション 00-00-f4-ab-cd-ef 宛てのフレームを破棄する。

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

■ポート 2（タグなし）配下のステーション 00-00-f4-c9-73-ff をポートセキュリティーの学習済みアドレスとして追加する。

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

■ポート 5（タグ付き）配下のステーションを FDB に登録する。所属 VLAN は orange。

```
ADD SWITCH FILTER DEST=00-00-f4-11-11-11 PORT=5 VLAN=orange
  ACTION=FORWARD
```

備考・注意事項

スタティックエントリーの出力ポートが指定 VLAN から削除された場合、同エントリーも自動的に削除される。

関連コマンド

DELETE SWITCH FILTER（136 ページ）
SET SWITCH PORT（225 ページ）
SHOW SWITCH FILTER（272 ページ）

ADD SWITCH HWFILTER

カテゴリー：スイッチング / ハードウェアパケットフィルター

ADD SWITCH HWFILTER=*filter-id* CLASSIFIER=*rule-list* ACTION={FORWARD|DISCARD|COPY|COPY,DISCARD} DPORT={*port-list*|ALL} [RULEPOS=*pos*]

filter-id: フィルター番号（1〜999）
rule-list: クラシファイア番号（1〜9999。ハイフン、カンマを使った複数指定も可能）
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）
pos: エントリー番号（0〜）

解説

ハードウェアパケットフィルターにフィルターエントリーを追加する。
パケットをフィルタリングするためのパラメーター（IP アドレス、ポート番号など）は、汎用のパケットフィルターであるクラシファイア（CREATE CLASSIFIER コマンドで作成）で定義する。本コマンドでは、クラシファイア番号とマッチ時のアクションを一組のエントリーとしてフィルターに追加する。
ハードウェアパケットフィルターは番号の小さい順に検索される。また、フィルター内のエントリーも番号の小さい順に検索される。アクションは最初にマッチしたエントリーで実行される。

パラメーター

HWFILTER フィルター番号。ハードウェアパケットフィルターの検索は番号の小さい順に行われる。番号は固定なので、他のフィルターを削除しても変更されることはない。また、番号に空きがあってもよい

CLASSIFIER クラシファイア番号。ハイフン、カンマを使って複数指定することも可能。複数指定した場合は、クラシファイアの数だけ（同じアクションの）エントリーが作成される。単一のフィルター内で同一のクラシファイアを複数回使用したり、複数のフィルターで同一のクラシファイアを使うことも可能だが、その場合は DPORT パラメーターで指定するポートが重ならないようにすること

ACTION パケットがクラシファイアに一致したときのアクション。FORWARD（転送）、DISCARD（破棄）、COPY（CPU にコピー）、COPY,DISCARD（CPU にコピー＋破棄）から選択する。COPY と COPY,DISCARD はフィルターのデバッグ用で、ENABLE IP DEBUG コマンドの PACKET オプションと組み合わせて使うことを想定している。通常は FORWARD と DISCARD だけを使うこと

DPORT 出力スイッチポート。本エントリーは、DPORT で指定したポートから出力されるパケットにだけ適用される。ALL はすべてのスイッチポートを意味する。また、DPORT に ALL 以外を指定したときは、複数ポートへ出力されるブロードキャスト、マルチキャスト、未学習ユニキャストパケットは、フィルターの適用対象にならない

RULEPOS 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。「0」を指定した場合は、エントリーリストの先頭に挿入される。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 CLASSIFIER パラメーターで指定したクラシファイアの数だけ後ろにずれる

例

■ホスト 192.168.20.200 からネットワーク 192.168.10.0 / 24 宛ての IP パケットを破棄。ここでは、192.168.10.0 / 24 がスイッチポート 1-4 に接続されている

```
CREATE CLASSIFIER=11 IPSADDR=192.168.20.200 IPDADDR=192.168.10.0/24
ADD SWITCH HWFILTER=1 CLASSIFIER=11 ACTION=DISCARD DPORT=1-4
```

備考・注意事項

DPORT には、可能な限り、フィルターを適用したいポートだけを指定すること。CREATE CLASSIFIER コマンドで IPDADDR、IPXDADDR を指定している場合、ADD SWITCH HWFILTER コマンドの DPORT パラメーターに指定したポートの数だけ内部テーブル領域が消費される。ADD SWITCH HWFILTER コマンドの実行時に「Insufficient space in the hardware packet classifier tables.」というエラーメッセージが表示されたときは、DPORT パラメーターに指定するポートを限定できないか検討してみるとよい。特に「DPORT=ALL」は、本当に必要なとき以外使わないこと。
DPORT に ALL 以外を指定した場合、複数ポートへ出力されるブロードキャスト、マルチキャスト、未学習ユニキャストパケットには、ハードウェアパケットフィルターが適用されない。
スイッチ本体宛てのパケット、および、スイッチ本体から送信されるパケットへの適用条件については、解説編の「本体宛てのパケットと本体発のパケット」を参照。その他、注意すべき各種仕様については解説編を参照。

関連コマンド

CREATE CLASSIFIER（114 ページ）
DELETE SWITCH HWFILTER（137 ページ）
SHOW SWITCH HWFILTER（274 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 16 ポートまで所属可能。ミラーポートをトランクグループに参加させることはできない。また、他のトランクグループに所属しているポートは指定できない。トランクポートは同一 VLAN に所属している必要がある。

例

■トランクグループ「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（127 ページ）
DELETE SWITCH TRUNK（139 ページ）
DESTROY SWITCH TRUNK（153 ページ）
ENABLE SWITCH HASH（189 ページ）
SET SWITCH TRUNK（227 ページ）
SHOW SWITCH TRUNK（284 ページ）

ADD VLAN ADDRESS

カテゴリー：スイッチング / バーチャル LAN

ADD VLAN={***vlanname***|***1..4090***} **ADDRESS=***macadd* [ENDADDRESS=*macadd*]

vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。大文字小文字を区別しない）
macadd: MAC アドレス（xx-xx-xx-xx-xx-xx の形式）

解説

MAC アドレス VLAN にメンバーの MAC アドレスを追加する。
追加した MAC アドレスは、ADD VLAN PORT コマンドでタグなしポートと関連付ける必要がある。

パラメーター

VLAN VLAN 名または VLAN ID（VID）。VLAN default（VID=1）を指定した場合で、かつ、VLAN default の種別（Type）がポート VLAN（Port-based）の場合、本コマンドの実行により VLAN default は MAC アドレス VLAN となる。また、使用可能な VLAN 種別も「MAC address, Limited Protocol, Port」となる

ADDRESS MAC アドレス。ユニキャストアドレスのみ有効。連続するアドレスを範囲指定するには、本パラメーターで先頭アドレスを指定し、ENDADDRESS で終了アドレスを指定する。

ENDADDRESS MAC アドレスを範囲指定する場合の終了 MAC アドレス。ユニキャストアドレスのみ有効。ADDRESS よりも大きい値でなくてはならない。範囲指定する場合、1 回のコマンド実行で追加できるアドレスは 1024 個まで

例

■VLAN bw に MAC アドレス「00-90-99-42-00-f2」を割り当てる。

```
ADD VLAN=bw ADDRESS=00-90-99-42-00-f2
```

■VLAN bw に MAC アドレス「00-00-f4-00-00-00」〜「00-00-f4-00-03-ff」を割り当てる。

```
ADD VLAN=bw ADDRESS=00-00-f4-00-00-00 ENDADDRESS=00-00-f4-00-03-ff
```

備考・注意事項

本コマンドで追加した MAC アドレスは、これ以降インデックス番号で指定することができる。インデックス番号を確認するには SHOW VLAN コマンドを使う。なお、インデックス番号は可変（追加、削除により番号がずれる）なので、インデックス番号を指定するときは、必ず SHOW VLAN コマンドで確認すること。

関連コマンド

ADD VLAN PORT（107 ページ）
DELETE VLAN ADDRESS（140 ページ）
DELETE VLAN PORT（142 ページ）
SHOW VLAN（285 ページ）

ADD VLAN LIMITEDPROTOCOL

カテゴリー：スイッチング / バーチャル LAN

ADD VLAN={***vlanname***|***1..4090***} **LIMITEDPROTOCOL=**{**IP**|***0x0800***|**0xE0**|***0x8137***|
0xFFFF|***0x0000008137***}
ADD VLAN={***vlanname***|***1..4090***} **LIMITEDPROTOCOL=IPX**
ENCAPSULATION={***802.2***|**ETHII**|**NETWARERAW**|**SNAP**|**ALL**}
ADD VLAN={***vlanname***|
1..4090} **LIMITEDPROTOCOL=OTHER ENCAPSULATION=**{***802.2***|**ETHII**|**SNAP**|**ALL**}

vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。大文字小文字を区別しない）

解説

MAC アドレス VLAN またはリミテッドプロトコル VLAN にプロトコルを追加する。LIMITEDPROTOCOL の名前が示すとおり、本コマンドで指定できるプロトコルは、原則として IP、IPX、IP・IPX 以外の 3 通りのみ。
追加したプロトコルは、ADD VLAN PORT コマンドでタグなしポートと関連付ける必要がある。

パラメーター

VLAN　VLAN 名または VLAN ID（VID）。VLAN default（VID=1）を指定した場合で、かつ、VLAN default の種別（Type）がポート VLAN（Port-based）の場合、本コマンドの実行により VLAN default は MAC アドレス VLAN となる。また、使用可能な VLAN 種別も「MAC address, Limited Protocol, Port」となる

LIMITEDPROTOCOL　プロトコル。原則として IP、IPX（各フレームタイプ）、OTHER（IP・IPX 以外の意味）しか指定できない。ただし、IPX、OTHER を指定した場合は ENCAPSULATION（フレームタイプ）も指定する必要がある。16 進表記のプロトコル番号で指定した場合は、ENCAPSULATION の指定は不要。

ENCAPSULATION　フレームタイプ（エンキャプセレーション）。LIMITEDPROTOCOL に IPX か OTHER を指定した場合の必須パラメーター

LIMITEDPROTOCOL	ENCAPSULATION	**該当プロトコル（フレームタイプ）**
IP	指定不要	IP（ETHII）
0x0800	指定不要	IP（ETHII）
0xE0	指定不要	IPX（802.2）
0x8137	指定不要	IPX（ETHII）
0xFFFF	指定不要	IPX（802.3 raw）

0x0000008137	指定不要	IPX（SNAP）
IPX	802.2	IPX（802.2）
IPX	ETHII	IPX（ETHII）
IPX	NETWARERAW	IPX（802.3 raw）
IPX	SNAP	IPX（SNAP）
IPX	ALL	IPX（すべて）
OTHER	802.2	IP・IPX 以外（802.2）
OTHER	ETHII	IP・IPX 以外（ETHII）
OTHER	SNAP	IP・IPX 以外（SNAP）
OTHER	ALL	IP・IPX 以外（すべて）

表 13: プロトコル指定

例

■VLAN beige に IP（Ethernet II）を追加する。

```
ADD VLAN=beige LIMITEDPROTOCOL=IP
```

■VLAN orange に IPX（802.3 raw）を追加する。

```
ADD VLAN=orange LIMITEDPROTOCOL=IPX ENCAPSULATION=NETWARERAW
```

■VLAN black に「IP・IPX 以外の全プロトコル」を追加する。

```
ADD VLAN=black LIMITEDPROTOCOL=OTHER ENCAPSULATION=ALL
```

備考・注意事項

本コマンドで追加したプロトコルは、これ以降インデックス番号で指定することができる。インデックス番号を確認するには SHOW VLAN コマンドを使う。なお、インデックス番号は可変（追加、削除により番号がずれる）なので、インデックス番号を指定するときは、必ず SHOW VLAN コマンドで確認すること。

関連コマンド

ADD VLAN PORT（107 ページ）
DELETE VLAN LIMITEDPROTOCOL（141 ページ）
DELETE VLAN PORT（142 ページ）
SHOW VLAN（285 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..4090***} **PORT=**{***port-list***|**ALL**} [FRAME={TAGGED|UNTAGGED}]
ADD VLAN={***vlanname***|***1..4090***} **PORT=**{***port-list***|**ALL**}
SUBNET={***ipadd***|**ALL**}
ADD VLAN={***vlanname***|***1..4090***} **PORT=**{***port-list***|**ALL**}
PROTOCOL={***protocoltype***|***index-list***|**ALL**}
ADD VLAN={***vlanname***|***1..4090***}
PORT={***port-list***|**ALL**} **ADDRESS=***macadd* [ENDADDRESS=*macadd*]
ADD
VLAN={***vlanname***|***1..4090***} **PORT=**{***port-list***|**ALL**} **ADDRESS=**{***index-list***|**ALL**}
ADD VLAN={***vlanname***|***1..4090***} **PORT=**{***port-list***|**ALL**}
LIMITEDPROTOCOL={**IP**|***0x0800***|**0xE0**|***0x8137***|**0xFFFF**|***0x0000008137***|***index-list***|**ALL**}
ADD VLAN={***vlanname***|***1..4090***} **PORT=**{***port-list***|**ALL**}
LIMITEDPROTOCOL=IPX ENCAPSULATION={***802***.2**|**ETHII**|**NETWARERAW**|**SNAP**|**ALL**}
ADD
VLAN={***vlanname***|***1..4090***} **PORT=**{***port-list***|**ALL**} **LIMITEDPROTOCOL=OTHER ENCAPSULATION=**{***802***.2**|**ETHII**|**SNAP**|**ALL**}

vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。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）
ipadd: IP アドレス
protocoltype: L3 プロトコル番号（16 進数。「0x」を前置すること）
index-list: インデックス番号（0〜。ハイフン、カンマを使った複数指定も可能）
macadd: MAC アドレス（xx-xx-xx-xx-xx-xx の形式）

解説

VLAN にポートを追加する。
VLAN と PORT 以外のパラメーターを指定しなかった場合は、該当 VLAN のタグなし（Untagged）ポート VLAN メンバーに追加される。VLAN、PORT と FRAME=TAGGED を指定した場合は、該当 VLAN のタグ付き（Tagged）ポート VLAN メンバーに追加される。
VLAN、PORT に加え、SUBNET、PROTOCOL、ADDRESS（および ENDADDRESS）、LIMITEDPROTOCOL（ENCAPSULATION）のいずれかを指定した場合は、それぞれ該当 VLAN のサブネット VLAN メンバー、プロトコル VLAN メンバー、MAC アドレス VLAN メンバー、リミテッドプロトコル VLAN メンバーに追加される。
ポートをサブネット VLAN、プロトコル VLAN、MAC アドレス VLAN、リミテッドプロトコル VLAN

のいずれかに追加する場合、該当ポートをあらかじめ任意のポート VLAN にタグなしポートとして参加させておく必要がある。

パラメーター

VLAN　VLAN 名または VLAN ID（VID）

PORT　ポート番号。複数指定が可能。ALL を指定した場合はすべてのスイッチポートが対象となる。各ポートは、ポート VLAN のタグなしポートとしては 1 つの VLAN だけに、タグ付きポートとしては複数の VLAN に所属できる。ミラーポートを VLAN に追加することはできない。

FRAME　該当 VLAN のタグ設定。TAGGED（タグ付き）、UNTAGGED（タグなし）から選択する。UNTAGGED を指定する場合、該当ポートがすでに default 以外の VLAN にタグなしポートとして所属しているときは、同 VLAN から削除した上で本コマンドを実行する必要がある。ポートが VLAN default に所属している状態で UNTAGGED を指定して別の VLAN に追加すると、自動的に VLAN default から削除される。デフォルトは UNTAGGED。

SUBNET　サブネットアドレス。ポートをサブネット VLAN に追加するときに指定する。

PROTOCOL　プロトコル。ポートをプロトコル VLAN に追加するときに指定する。プロトコルは、定義済みのプロトコル名（ADD VLAN PROTOCOL コマンドの表を参照）か、16 進表記（「0x」を前置すること）のプロトコル番号で指定する。あるいは、SHOW VLAN コマンドで表示されるインデックス番号（複数指定可）で指定することもできる。

ADDRESS　MAC アドレス。ポートを MAC アドレス VLAN に追加するときに指定する。通常は ALL（すべて）を指定する。連続するアドレスを範囲指定するには、本パラメーターで先頭アドレスを指定し、ENDADDRESS で終了アドレスを指定する。あるいは、SHOW VLAN コマンドで表示されるインデックス番号（複数指定可）で指定することもできる。

ENDADDRESS　範囲指定時の終了 MAC アドレス

LIMITEDPROTOCOL　プロトコル。ポートをリミテッドプロトコル VLAN に追加するときに指定する。プロトコルは、定義済みのプロトコル名（ADD VLAN LIMITEDPROTOCOL コマンドの表を参照）か、16 進表記のプロトコル番号で指定する。あるいは、SHOW VLAN コマンドで表示されるインデックス番号（複数指定可）で指定することもできる。IPX か OTHER を指定した場合は ENCAPSULATION パラメーターも必須

ENCAPSULATION　フレームタイプ（エンキャプセレーション）。LIMITEDPROTOCOL に IPX か OTHER を指定した場合の必須パラメーター

例

■ポート 1〜4 を VLAN orange のポート VLAN メンバー（タグなしポート）に追加する。

```
ADD VLAN=orange PORT=1-4
```

■ポート 12 を VLAN white と orange のタグ付きポートに設定する。

```
ADD VLAN=white PORT=12 FRAME=TAGGED
ADD VLAN=orange PORT=12 FRAME=TAGGED
```

■ポート 1〜2 を VLAN orange のサブネット VLAN メンバー（サブネット 192.168.10.0）に追加する。

```
ADD VLAN=orange PORT=1-2 SUBNET=192.168.10.0
```

■ポート 4〜8 を VLAN beige のプロトコル VLAN メンバー（プロトコル NetBEUI）に追加する。

```
ADD VLAN=beige PORT=4-8 PROTOCOL=NetBEUI
```

■ポート 9〜12 を VLAN black の MAC アドレス VLAN メンバー（MAC アドレス インデックス 0〜255）に追加する。

```
ADD VLAN=black PORT=9-12 ADDRESS=0-255
```

備考・注意事項

スイッチポートを複数の STP ドメインに所属させることはできない。ポートを複数の VLAN に所属させる場合、これらの VLAN はすべて、デフォルトの STP ドメイン「default」所属のまま使用しなくてはならない。

関連コマンド

ADD VLAN ADDRESS（103 ページ）
ADD VLAN LIMITEDPROTOCOL（105 ページ）
ADD VLAN PROTOCOL（110 ページ）
ADD VLAN SUBNET（113 ページ）
DELETE VLAN PORT（142 ページ）
SET VLAN PORT（229 ページ）
SHOW VLAN（285 ページ）
SHOW VLAN PORT（290 ページ）

ADD VLAN PROTOCOL

カテゴリー：スイッチング / バーチャル LAN

ADD VLAN={***vlanname***|***1..4090***} **PROTOCOL=***protocoltype*

vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。大文字小文字を区別しない）
protocoltype: L3 プロトコル番号（16 進数。「0x」を前置すること）

解説

IP サブネット VLAN またはプロトコル VLAN にプロトコルを追加する。
追加したプロトコルは、ADD VLAN PORT コマンドでタグなしポートと関連付ける必要がある。

パラメーター

VLAN　VLAN 名または VLAN ID（VID）。VLAN default（VID=1）を指定した場合で、かつ、VLAN default の種別（Type）がポート VLAN（Port-based）の場合、本コマンドの実行により VLAN default は IP サブネット VLAN となる。また、使用可能な VLAN 種別も「IP subnet, Protocol, Port」となる

PROTOCOL　プロトコル。定義済みのプロトコル名（別表を参照）か、16 進表記（「0x」を前置すること）のプロトコル番号で指定する。プロトコル番号で指定する場合、802.2 なら 1 バイト（DSAP のみ）で、Ethernet Version 2 なら 2 バイトで、SNAP なら 5 バイトの 16 進数で指定する

SAP（Service Access Point）	
IPX 802.2	0xE0（SAP）
NetBEUI	0xF0（SAP）
SNA Path Control	0x04（SAP）
PROWAY-LAN	0x0E（SAP）
EIA-RS	0x4E（SAP）
PROWAY	0x8E（SAP）
ISO CLNS IS	0xFE（SAP）
Ethernet Version 2	
IP ETHII	0x0800（Ethernet Version 2）
X.75 Internet	0x0801（Ethernet Version 2）
NBS Internet	0x0802（Ethernet Version 2）
ECMA Internet	0x0803（Ethernet Version 2）
Chaosnet	0x0804（Ethernet Version 2）
X.25 Level 3	0x0805（Ethernet Version 2）

ARP	0x0806（Ethernet Version 2）
XNS Compat	0x0807（Ethernet Version 2）
Banyan Systems	0x0BAD（Ethernet Version 2）
BBN Simnet	0x5208（Ethernet Version 2）
DEC MOP Dump/Ld	0x6001（Ethernet Version 2）
DEC MOP Rem Cons	0x6002（Ethernet Version 2）
DEC DECNET	0x6003（Ethernet Version 2）
DEC LAT	0x6004（Ethernet Version 2）
DEC Diagnostic	0x6005（Ethernet Version 2）
DEC Customer	0x6006（Ethernet Version 2）
DEC LAVC	0x6007（Ethernet Version 2）
RARP	0x8035（Ethernet Version 2）
DEC LANBridge	0x8038（Ethernet Version 2）
DEC Encryption	0x803D（Ethernet Version 2）
Appletalk	0x809B（Ethernet Version 2）
IBM SNA	0x80D5（Ethernet Version 2）
AppleTalk AARP	0x80F3（Ethernet Version 2）
IPX EthII	0x8137（Ethernet Version 2）
SNMP	0x814C（Ethernet Version 2）
IPv6	0x86DD（Ethernet Version 2）
IPX 802.3	0xFFFF（NetWare 802.3 raw）
SNAP（Sub-Network Access Protocol）	
ETHERTALK 2	0x080007809B（SNAP）
ETHERTALK 2 AARP	0x00000080F3（SNAP）
IPX SNAP	0x0000008137（SNAP）

表 14: 定義済みのプロトコル名一覧

例

■VLAN sales にプロトコル IPX 802.2（802.2 の IPX）を追加する。

```
ADD VLAN=sales PROTOCOL="IPX 802.2"
```

■VLAN mktg にプロトコル NetBEUI を追加する。

```
ADD VLAN=mktg PROTOCOL="NetBEUI"
```

備考・注意事項

本コマンドで追加したプロトコルは、これ以降インデックス番号で指定することができる。インデックス番

号を確認するには SHOW VLAN コマンドを使う。なお、インデックス番号は可変（追加、削除により番号がずれる）なので、インデックス番号を指定するときは、必ず SHOW VLAN コマンドで確認すること。

関連コマンド

ADD VLAN PORT（107 ページ）
DELETE VLAN PORT（142 ページ）
DELETE VLAN PROTOCOL（145 ページ）
SHOW VLAN（285 ページ）

ADD VLAN SUBNET

カテゴリー：スイッチング / バーチャル LAN

ADD VLAN={***vlanname***|***1..4090***} **SUBNET=***ipadd* [MASK=*ipadd*]

vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。大文字小文字を区別しない）
ipadd: IP アドレスまたはネットマスク

解説

IP サブネット VLAN に IP サブネットを追加する。
追加したサブネットは、ADD VLAN PORT コマンドでタグなしポートと関連付ける必要がある。

パラメーター

VLAN　VLAN 名または VLAN ID（VID）。VLAN default（VID=1）を指定した場合で、かつ、VLAN default の種別（Type）がポート VLAN（Port-based）の場合、本コマンドの実行により VLAN default は IP サブネット VLAN となる。また、使用可能な VLAN 種別も「IP subnet, Protocol, Port」となる
SUBNET　サブネットアドレス。アドレス範囲が他のサブネット VLAN と重なるような設定はできない
MASK　SUBNET に対するネットマスク。省略時はサブネットアドレスのクラス標準マスクが適用される

例

■VLAN yomo にサブネット 172.16.56.0/24 を追加する。

```
ADD VLAN=yomo SUBNET=172.16.56.0 MASK=255.255.255.0
```

関連コマンド

ADD VLAN PORT（107 ページ）
DELETE VLAN PORT（142 ページ）
DELETE VLAN SUBNET（146 ページ）
SHOW VLAN（285 ページ）

CREATE CLASSIFIER

カテゴリー：スイッチング / クラシファイア

CREATE CLASSIFIER=*rule-id* [SVLAN={*vlanname*|*1..4090*|ANY}]
[DVLAN={*vlanname*|*1..4090*|ANY}] [ETHFORMAT={*802.2*|ETHII|NETWARERAW|SNAP|ANY}] [PROTOCOL={*protocoltype*|IP|IPX|NONIPIPX|ANY}] [MACTYPE={L2UCAST|L2MCAST|L2BCAST|ANY}] [IPSADDR={*ipadd*[*/masklen*]|ANY}] [IPDADDR={*ipadd*[*/masklen*]|ANY}] [IPDSCP={*0..63*|ANY}] [IPTOS={*0..7*|ANY}] [IPPROTOCOL={TCP|UDP|ICMP|IGMP|*protocol*|ANY|NONTCPUDP}] [IPXDADDR={*ipxnet*|ANY}] [IPXSSOCKET={NCP|SAP|RIP|NNB|DIAG|NLSP|IPXWAN|*socket*|ANY}] [IPXDSOCKET={NCP|SAP|RIP|NNB|DIAG|NLSP|IPXWAN|*socket*|ANY}] [TCPSPORT={*port*|ANY}] [TCPDPORT={*port*|ANY}] [UDPSPORT={*port*|ANY}] [UDPDPORT={*port*|ANY}]

rule-id: クラシファイア番号（1〜9999）
vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。大文字小文字を区別しない）
protocoltype: L3 プロトコル番号（16 進数）
ipadd: IP アドレス
masklen: マスク長（0〜32）
protocol: IP プロトコル番号（0〜255）
ipxnet: IPX ネットワーク番号（32 ビット長。16 進数最大 8 文字。先頭の 0 は省略可能）
socket: IPX ソケット番号（16 ビット長。16 進数最大 4 文字）
port: TCP / UDP ポート番号（0〜65535）

解説

クラシファイア（汎用パケットフィルター）を作成する。
クラシファイアはパケットを分類（Classify = クラス分け）するための条件を定義するもの。ハードウェアパケットフィルターとポリシーベース QoS の両方で共通に用いられる。
クラシファイアを作成しただけでは何も行われないことに注意。クラシファイアは、ハードウェアパケットフィルターか、QoS ポリシーのフローグループに割り当てて初めて効果を発揮する。

パラメーター

CLASSIFIER　クラシファイア番号。この番号は単なる識別子であり、番号の大小は意味を持たない。番号は固定なので、他のクラシファイアを削除しても変更されることはない。また、番号に空きがあってもよい

SVLAN　入力 VLAN。パケットの入力元が指定した VLAN のときだけマッチする。省略時は ANY。DVLAN とは同時に指定できない

DVLAN　出力 VLAN。パケットの出力先が指定した VLAN のときだけマッチする。省略時は ANY。SVLAN とは同時に指定できない

ETHFORMAT Ethernet のフレームフォーマット（エンキャプセレーション）。802.2（802.2 LLC）、ETHII（Ethernet Version 2）、NETWARERAW（Novell 802.3 raw）、SNAP（802.2 LLC + SNAP）から選択する。PROTOCOL パラメーターには、ここで指定したフレームタイプのプロトコル番号を指定する。 省略時は ANY。ETHII、802.2、SNAP を指定した場合は、PROTOCOL パラメーターも必須。ETHFORMAT と PROTOCOL パラメーターは、組み合わせによって入力できないもの（エラーになるもの）と、コマンドは受け付けるが ASIC チップ上エラーとなり無効になるものがあるので注意。詳細は別表を参照のこと

PROTOCOL レイヤー 3 プロトコルタイプフィールド値。特殊なプロトコル名（IP、IPX、NONIPIPX、ANY。別表を参照）か、定義済みのプロトコル名（別表を参照）、または、16 進表記のプロトコル番号で指定する。プロトコル番号で指定する場合、802.2 なら 1 バイト（DSAP のみ）で、Ethernet Version 2 なら 2 バイトで、SNAP なら 5 バイトの 16 進数で指定する。ただし、SNAP の場合は下位 2 バイトしかパケットマッチングに使用されない（例：「xxxxxxABCD」を指定した場合、「ABCD」の部分だけがマッチングに使われる）。なお、定義済みのプロトコル名とプロトコル番号は、フレームフォーマット（ETHFORMAT）ごとに最大 3 個までしか使用できない。本パラメーターは、ETHFORMAT に ETHII、802.2、SNAP のいずれかを指定した場合は必須。

MACTYPE レイヤー 2 アドレス種別。L2UCAST（ユニキャスト）、L2MCAST（マルチキャスト）、L2BCAST（ブロードキャスト）、ANY（すべて）から選択する。本パラメーターは、ハードウェアパケットフィルターの DPORT パラメーターに ALL を指定したときだけ有効。省略時は ANY

IPSADDR 始点 IP アドレス。IP アドレス / マスク長の形式で指定する。マスク長を省略した場合は、32 ビットマスク（ホストアドレス）と見なされる。省略時は ANY

IPDADDR 終点 IP アドレス。IP アドレス / マスク長の形式で指定する。マスク長を省略した場合は、32 ビットマスク（ホストアドレス）と見なされる。省略時は ANY

IPDSCP IP ヘッダーの DSCP（DiffServ Code Point）フィールド値。有効範囲は 0〜63。IPTOS とは同時に指定できない。省略時は ANY

IPTOS IP ヘッダーの TOS 優先度（precedence）フィールド値。有効範囲は 0〜7。IPDSCP とは同時に指定できない。省略時は ANY

IPPROTOCOL IP ヘッダーのプロトコルタイプフィールド値。定義済みのプロトコル名（TCP、UDP、ICMP、IGMP、NONTCPUDP）か 10 進表記のプロトコル番号で指定する。本パラメーターに指定できるプロトコル番号は、システム全体で 29 種類まで（ただし、TCP、UDP、IGMP、NONTCPUDP、ANY は数えない）。なお、TCPSPORT、TCPDPORT パラメーターを使っている場合は、本パラメーターに TCP を指定したものと見なされる（他の値は指定できない）。また、UDPSPORT、UDPDPORT パラメーターを使っている場合は、本パラメーターに UDP を指定したものと見なされる（他の値は指定できない）。省略時は ANY

IPXDADDR 終点 IPX ネットワーク番号。省略時は ANY

IPXSSOCKET 始点 IPX ソケット。定義済みのソケット名か 16 進表記のソケット番号で指定する。本パラメーターに指定できるソケット番号は、システム全体で 7 種類まで（ANY は数えない）。省略時は ANY

IPXDSOCKET 終点 IPX ソケット。定義済みのソケット名か 16 進表記のソケット番号で指定する。本パラメーターに指定できるソケット番号は、システム全体で 7 種類まで（ANY は数えない）。省略時は ANY

TCPSPORT TCP 始点ポート。本パラメーターに指定できるポート番号は、システム全体で 15 種類まで。省略時は ANY

TCPDPORT　TCP 終点ポート。本パラメーターに指定できるポート番号は、システム全体で 15 種類まで。省略時は ANY

UDPSPORT　UDP 始点ポート。本パラメーターに指定できるポート番号は、システム全体で 15 種類まで。省略時は ANY

UDPDPORT　UDP 終点ポート。本パラメーターに指定できるポート番号は、システム全体で 15 種類まで。省略時は ANY

ETHFORMAT	PROTOCOL	**コマンド入力上**	ASIC **チップ上**
ETHII	無指定	OK	無効
	ANY	OK	無効
	NONIPIPX	OK	無効
	IP（0800 と同等）	OK	有効
	IPX（8137 と同等）	OK	有効
	プロトコル番号	OK	有効
NETWARERAW	無指定（”IPX 802.3”と同等）	OK	有効
	ANY（”IPX 802.3”と同等）	OK	有効
	NONIPIPX	エラー	無効
	IP	エラー	無効
	IPX（”IPX 802.3”と同等）	OK	有効
	”IPX 802.3”	OK	有効
	プロトコル番号	エラー	無効
SNAP	無指定	OK	無効
	ANY	OK	無効
	NONIPIPX	OK	無効
	IP	エラー	無効
	IPX（E0 と同等）	OK	有効
	プロトコル番号	OK	有効

表 15: ETHFORMAT と PROTOCOL の組み合わせと有効・無効

IP	すべての IP（ETHII、SNAP）
IPX	すべての IPX（ETHII、NETWARERAW、802.2、SNAP）
NONIPIPX	IP（ETHII、SNAP）、IPX（ETHII、NETWARERAW、802.2、SNAP）以外
ANY	すべてのプロトコル。つまり、プロトコルタイプには関知しないということ

表 16: 特殊なプロトコル名一覧

SAP（Service Access Point）	
IPX 802.2	E0（SAP）
NetBEUI	F0（SAP）
SNA Path Control	04（SAP）

PROWAY-LAN	0E（SAP）
EIA-RS	4E（SAP）
PROWAY	8E（SAP）
ISO CLNS IS	FE（SAP）
Ethernet Version 2	
IP ETHII	0800（Ethernet Version 2）
X.75 Internet	0801（Ethernet Version 2）
NBS Internet	0802（Ethernet Version 2）
ECMA Internet	0803（Ethernet Version 2）
Chaosnet	0804（Ethernet Version 2）
X.25 Level 3	0805（Ethernet Version 2）
ARP	0806（Ethernet Version 2）
XNS Compat	0807（Ethernet Version 2）
Banyan Systems	0BAD（Ethernet Version 2）
BBN Simnet	5208（Ethernet Version 2）
DEC MOP Dump/Ld	6001（Ethernet Version 2）
DEC MOP Rem Cons	6002（Ethernet Version 2）
DEC DECNET	6003（Ethernet Version 2）
DEC LAT	6004（Ethernet Version 2）
DEC Diagnostic	6005（Ethernet Version 2）
DEC Customer	6006（Ethernet Version 2）
DEC LAVC	6007（Ethernet Version 2）
RARP	8035（Ethernet Version 2）
DEC LANBridge	8038（Ethernet Version 2）
DEC Encryption	803D（Ethernet Version 2）
Appletalk	809B（Ethernet Version 2）
IBM SNA	80D5（Ethernet Version 2）
AppleTalk AARP	80F3（Ethernet Version 2）
IPX EthII	8137（Ethernet Version 2）
SNMP	814C（Ethernet Version 2）
IPv6	86DD（Ethernet Version 2）
IPX 802.3	FFFF（NetWare 802.3 raw）
SNAP（Sub-Network Access Protocol）	
ETHERTALK 2	080007809B（SNAP）
ETHERTALK 2 AARP	00000080F3（SNAP）
IPX SNAP	0000008137（SNAP）

表 17: 定義済みのプロトコル名一覧

例

■SSH サーバー宛てのパケットにマッチするクラシファイア「100」を作成する。

```
CREATE CLASSIFIER=100 TCPDPORT=22
```

■IPv6 パケットにマッチするクラシファイア「201」を作成する。

```
CREATE CLASSIFIER=201 PROTOCOL="IPv6"
```

■サブネット 172.16.10.128/28 からの UDP パケットにマッチするクラシファイア「10」を作成する。

```
CREATE CLASSIFIER=10 IPSADDR=172.16.10.128/28 IPPROTOCOL=UDP
```

■すべてのパケットにマッチするクラシファイア「9999」を作成する。

```
CREATE CLASSIFIER=9999
```

備考・注意事項

クラシファイアの設定において、ファイアウォールポリシーに追加されたインターフェース（VLAN）を SVLAN に指定すると、そのクラシファイアは、ルーティングパケットに対しては機能しなくなる（スイッチングパケットに対しては機能する）。この現象は、ファイアウォール機能が無効であっても発生するので注意。

関連コマンド

ADD QOS FLOWGROUP（93 ページ）
ADD SWITCH HWFILTER（100 ページ）
DELETE QOS FLOWGROUP（132 ページ）
DELETE SWITCH HWFILTER（137 ページ）
DESTROY CLASSIFIER（147 ページ）
SET CLASSIFIER（204 ページ）
SHOW CLASSIFIER（230 ページ）

CREATE QOS FLOWGROUP

カテゴリー：スイッチング / ポリシーベース QoS

```
CREATE QOS FLOWGROUP=flow-list [RED={red-id|NONE}] [MARKVALUE={0..63|
   NONE}] [DESCRIPTION=string]
```

flow-list: フローグループ番号（0〜1023。ハイフン、カンマを使った複数指定も可能）
string: 文字列（1〜15 文字。空白を含む場合はダブルクォートで囲む）
red-id: RED カーブ番号（0〜47）

解説

フローグループを作成する。
フローグループは、クラシファイア（汎用パケットフィルター）を用いて、パケットを一連の「フロー」として定義するもの。トラフィッククラスよりも細かい QoS 制御を行いたい場合は、フローグループごとに RED カーブを設定することができる。

パラメーター

FLOWGROUP　フローグループ番号
RED　RED カーブ番号。トラフィッククラスの RED カーブよりも優先される。省略時は NONE
MARKVALUE　IP ヘッダーの DSCP（DiffServ Code Point）フィールドに書き込む値。トラフィッククラスの MARKVALUE よりも優先される。省略時は NONE
DESCRIPTION　フローグループの説明（メモとして使う）

例

■フローグループ「50」を作成する。

```
CREATE QOS FLOWGROUP=50 DESCRIPTION="Sample Flow Group"
```

関連コマンド

ADD QOS FLOWGROUP（93 ページ）
DELETE QOS FLOWGROUP（132 ページ）
DESTROY QOS FLOWGROUP（148 ページ）
SET QOS FLOWGROUP（212 ページ）
SHOW QOS FLOWGROUP（246 ページ）

CREATE QOS POLICY

カテゴリー：スイッチング / ポリシーベース QoS

CREATE QOS POLICY=*qos-list* [DESCRIPTION=*string*] [DTCPERCENT=*1..100*]

qos-list: QoS ポリシー番号（0〜255。ハイフン、カンマを使った複数指定も可能）
string: 文字列（1〜15 文字。空白を含む場合はダブルクォートで囲む）

解説

QoS ポリシーを作成する。
QoS ポリシーはパケット出力時に帯域制御を行うためのメカニズムで、ユーザー定義のトラフィッククラス（複数）とデフォルトトラフィッククラス（1 つ）から構成される。
QoS ポリシーをスイッチポートに関連付けると、送出トラフィックに対して、該当するトラフィッククラスで定められた最大・最小帯域が割り当てられる。

パラメーター

POLICY　QoS ポリシー番号
DESCRIPTION　ポリシーの説明（メモとして使う）。POLICY パラメーターに複数の番号を指定した場合は、すべてのポリシーに同じメモ文字列が設定される
DTCPERCENT　本ポリシーのデフォルトトラフィッククラスに割り当てる帯域幅。スイッチポートの帯域幅に対する割合（%）で指定する。デフォルトトラフィッククラスには、本パラメーターで指定した割合の帯域が保証される。また、デフォルトトラフィッククラスの帯域は本パラメーターで指定した割合までに制限される。省略時は 20%

例

■QoS ポリシー「10」を作成する。

```
CREATE QOS POLICY=10
```

備考・注意事項

スイッチポートの帯域制限機能（SET SWITCH PORT コマンドの EGRESSLIMIT パラメーター）とポリシーベース QoS の帯域制御機能は併用できない。どちらか一方だけを使うこと

関連コマンド

ADD QOS POLICY（94 ページ）
DELETE QOS POLICY（133 ページ）

DESTROY QOS POLICY（149 ページ）
SET QOS POLICY（213 ページ）
SET QOS PORT（214 ページ）
SHOW QOS POLICY（248 ページ）

CREATE QOS RED

カテゴリー：スイッチング / ポリシーベース QoS

```
CREATE QOS RED=red-id [START=0..100] [STOP=0..100] [DROPPROB=0..100]
   [DESCRIPTION=string]
```

red-id: RED カーブ番号（5〜47）
string: 文字列（1〜15 文字。空白を含む場合はダブルクォートで囲む）

解説

RED（Random Early Detection / Discard）アルゴリズムの動作を規定する RED カーブを定義する。
本製品は、トラフィッククラスごとに仮想的なキュー（仮想キュー）を保持している。通常は、仮想キューの長さがトラフィッククラスの最大帯域（MAXBANDWIDTH）を超えると超過分のパケットを破棄する（ドロップテイルアルゴリズム）。
RED（Random Early Detection / Discard）は、仮想キューの長さが最大帯域に達しないうちに、徐々にパケット破棄率を高くしていくことで、輻輳回避やより細やかな帯域制御を実現するアルゴリズム。
RED の設定は、仮想キュー長とパケット破棄率の関係を示す「RED カーブ」を定義することによって行う。詳細は解説編を参照のこと。

パラメーター

RED　RED カーブ番号。0〜4 は定義済みの RED カーブが使っているため指定できない
START　パケットを破棄し始めるポイント。トラフィッククラスの最大帯域幅に対する仮想キュー長の割合（%）で指定する。仮想キュー長がこのポイントを超えると、徐々にパケットの破棄率が高くなり、STOP に達したときに破棄率が DROPPROB%となる。
STOP　パケットを完全に破棄し始めるポイント。トラフィッククラスの最大帯域幅に対する仮想キュー長の割合（%）で指定する。仮想キュー長がこのポイントを超えると、すべてのパケットが破棄されるようになる。
DROPPROB　仮想キュー長が STOP のときのパケット破棄率
DESCRIPTION　RED カーブの説明（メモとして使う）

例

■仮想キューの長さが最大帯域の 30%に達したらランダムにパケットを破棄しはじめ、90%を超えたらすべてのパケットを破棄する RED カーブ「5」を定義する。パケットの破棄率は、仮想キュー長が 30%〜90%のとき、0%〜30%の範囲で段階的に高くなっていく。

```
CREATE QOS RED=5 DESCRIPTION="Sample RED curve" START=30 STOP=90
  DROPPROB=30
```

関連コマンド

DESTROY QOS RED（150 ページ）
SET QOS RED（215 ページ）
SHOW QOS RED（250 ページ）

CREATE QOS TRAFFICCLASS

カテゴリー：スイッチング / ポリシーベース QoS

CREATE QOS TRAFFICCLASS=*tc-list* [MINBANDWIDTH=*bandwidth*]
[MAXBANDWIDTH=*bandwidth*] [WEIGHT=*weight*] [RED={*red-id*|NONE}]
[MARKVALUE={*0..63*|NONE}] [NUMHASHEDFLOWS={NONE|*1*|*2*|*8*|*32*|*64*|*128*|*256*|*512*}]
[FAIRHASHLIMIT={LOW|MODLOW|MODHIGH|HIGH}] [DESCRIPTION=*string*]

tc-list: トラフィッククラス番号（0〜511。ハイフン、カンマを使った複数指定も可能）
bandwidth: 帯域幅（0〜16000000Kbps）
weight: 帯域配分用の重み付け値
red-id: RED カーブ番号（0〜47）
string: 文字列（1〜15 文字。空白を含む場合はダブルクォートで囲む）

解説

トラフィッククラスを作成する。
トラフィッククラスは、同等の QoS（帯域）を与えるべきフローグループをひとまとめにしたもの。トラフィッククラスは、複数のフローグループで構成される。
ポリシーベース QoS では、トラフィッククラスごとに送信時の最大帯域幅、最小帯域幅を設定する。トラフィッククラスは、QoS ポリシーに割り当てることによって効果を発揮する。QoS ポリシーには、ユーザー定義のトラフィッククラスに加え、暗黙のデフォルトトラフィッククラスが存在する。

パラメーター

TRAFFICCLASS　トラフィッククラス番号

MINBANDWIDTH　トラフィッククラスに割り当てる最小帯域幅（Kbps）。該当クラスには、ここで指定した帯域が確保される。この値は、パケットをスイッチ内部のキューから送り出すときのレートを示す。数値だけで指定する場合の単位は Kbps。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「× 1」、「× 1000」、「× 1000000」の意味になる。有効範囲は Kbps 換算で 0〜16000000。ただし、指定値が 64Kbps の倍数でない場合は切り捨てが行われる（63Kbps を指定した場合は 0Kbps となる）。0 は帯域ゼロの意味。「M」、「G」を指定する場合は、「2.256G」や「128.4M」のように小数を指定することもできる（小数点以下は 3 桁目まで有効）。省略時は 64Kbps

MAXBANDWIDTH　トラフィッククラスに割り当てる最大帯域幅（Kbps）。該当クラスに割り当てる帯域は、ここで指定した値までに制限される。この値は、パケットをスイッチ内部のキューから送り出すときのレートを示す。数値だけで指定する場合の単位は Kbps。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「× 1」、「× 1000」、「× 1000000」の意味になる。有効範囲は Kbps 換算で 0〜16000000。ただし、指定値が 64Kbps の倍数でない場合は切り捨てが行われる（63Kbps を指定した場合は 0Kbps となる）。0 は帯域ゼロの意味。「M」、「G」を指定する場合は、「2.256G」や「128.4M」のように小数を指定することもできる（小数点以下は 3 桁目まで有効）。省略時は 16Gbps

WEIGHT　同一 QoS ポリシー所属のトラフィッククラス間で帯域を配分するときに用いる重み付け値。この値が小さいほど多くの帯域が割り当てられる。有効な値は、1、2、3、4、5、6、7、8、10、12、14、

16、20、24、28、32、40、48、56、64、80、96、112、128、160、192、224、256、320、384、448、512、640、768、896、1024。詳細は解説編を参照のこと。省略時は 1

RED 本トラフィッククラスに適用する RED（Random Early Detection / Discard）カーブの番号。NONE は RED アルゴリズムを使用せずに、帯域オーバー分を単純に破棄するアルゴリズムを使用することを示す。省略時は NONE

MARKVALUE IP ヘッダーの DSCP（DiffServ Code Point）フィールドに書き込む値。NONE は値を書き換えないことを示す。省略時は NONE

NUMHASHEDFLOWS 同一トラフィックグループ所属のフローグループ間で、どの程度均等に帯域を配分するかを指定するパラメーター（FAIRHASHLIMIT も参照）。フローグループはハッシュアルゴリズムによって NUMHASHEDFLOWS 個のグループ（Hashed Flowgroup）にハッシュ（分類）され、グループごとに帯域が配分される。本パラメーターの値が大きいほど、フローグループ間で帯域が均等に配分される。NONE を指定した場合は、フローグループ間での帯域均等配分は行われない。省略時は NONE

FAIRHASHLIMIT 同一トラフィックグループ所属のフローグループ間で、どの程度均等に帯域を配分するかを指定するパラメーター（NUMHASHEDFLOWS も参照）。LOW、MODLOW、MODHIGH、HIGH の順に均等さが増す（HIGH がもっとも均等）。省略時は MODHIGH

DESCRIPTION トラフィッククラスの説明（メモとして使う）。TRAFFICCLASS パラメーターに複数の番号を指定した場合は、すべてのトラフィッククラスに同じメモ文字列が設定される

備考・注意事項

スイッチポートの帯域制限機能（SET SWITCH PORT コマンドの EGRESSLIMIT パラメーター）とポリシーベース QoS の帯域制御機能は併用できない。どちらか一方だけを使うこと

MINBANDWIDTH、MAXBANDWIDTH は、内部キューからデータを送り出すときの送信レートを示している。回線（ケーブル）上での送信レートとは異なるので注意すること。パケットが回線上に出力されるときは、フレーム間ギャップ（IFG）やプリアンブルが付加されるため、実際の送信レートはこれらのパラメーターで指定した値よりも小さくなる。なお、パケットサイズが大きいほど IFG やプリアンブルの割合（オーバーヘッド）が減るので、実際の送信レートがパラメーター指定値に近づく。

関連コマンド

ADD QOS TRAFFICCLASS（95 ページ）
DESTROY QOS TRAFFICCLASS（151 ページ）
SET QOS TRAFFICCLASS（216 ページ）
SHOW QOS TRAFFICCLASS（252 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

CREATE STP=*stpname*

stpname: STP ドメイン名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。大文字小文字を区別しない）

解説

STP ドメインを作成する。STP ドメインは「default」を含め 8 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（152 ページ）
ENABLE STP（183 ページ）
SET STP（219 ページ）
SHOW STP（255 ページ）

CREATE SWITCH TRUNK

カテゴリー：スイッチング / ポート

CREATE SWITCH TRUNK=*trunk* [PORT=*port-list*] [SPEED={10M|100M|1000M}]

trunk: トランクグループ名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。大文字小文字を区別しない）
port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）

解説

トランクグループを作成する。
トランクグループは 16 個まで作成可能。また、トランクグループの所属ポート数は最大 16 ポート。

パラメーター

TRUNK　トランクグループ名
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 16。他のトランクグループに所属するポートやミラーポートは追加できない。また、トランクポートは同じ VLAN に所属していなくてはならない。
SPEED　トランクポートの通信速度。トランクグループに参加したポートは、ここで指定した速度のオートネゴシエーション（AUTONEGOTIATE）となる

例

■トランクグループ「uplink」を作成する。

```
CREATE SWITCH TRUNK=uplink
```

関連コマンド

ADD SWITCH TRUNK（102 ページ）
DELETE SWITCH TRUNK（139 ページ）
DESTROY SWITCH TRUNK（153 ページ）
ENABLE SWITCH HASH（189 ページ）
SET SWITCH TRUNK（227 ページ）
SHOW SWITCH TRUNK（284 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..4090*
CREATE VLAN=*vlanname* VID=*2..4090*
TYPE=SUBNET [SUBNET=*ipadd*] [MASK=*ipadd*]
CREATE VLAN=*vlanname* VID=*2..4090*
TYPE=PROTOCOL [PROTOCOL=*protocoltype*]
CREATE VLAN=*vlanname* VID=*2..4090*
TYPE=MACADDRESS [ADDRESS=*macadd*] [ENDADDRESS=*macadd*]
CREATE
VLAN=*vlanname* VID=*2..4090* TYPE=LIMITEDPROTOCOL [LIMITEDPROTOCOL={IP|*0x0800*|0xE0|*0x8137*|0xFFFF|*0x0000008137*}]
CREATE VLAN=*vlanname*
VID=*2..4090* TYPE=LIMITEDPROTOCOL [LIMITEDPROTOCOL=IPX]
[ENCAPSULATION={*802.*2|ETHII|NETWARERAW|SNAP|ALL}]
CREATE VLAN=*vlanname*
VID=*2..4090* TYPE=LIMITEDPROTOCOL [LIMITEDPROTOCOL=OTHER]
[ENCAPSULATION={*802.*2|ETHII|SNAP|ALL}]

vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。大文字小文字を区別しない）
ipadd: IP アドレスまたはネットマスク
protocoltype: L3 プロトコル番号（16 進数。「0x」を前置すること）
macadd: MAC アドレス（xx-xx-xx-xx-xx-xx の形式）

解説

VLAN を作成する。
本製品がサポートする VLAN は次の 5 種類。
・ポート VLAN（タグ VLAN を含む）
・IP サブネット VLAN
・プロトコル VLAN
・MAC アドレス VLAN
・リミテッドプロトコル VLAN
ただし、すべての種類を同時に使用することはできない。使用可能な VLAN 種別に関する基本ルールは次のとおり。
・ポート VLAN（タグ VLAN を含む）はつねに使用できる。
・残りの 4 種類は、「IP サブネット VLAN、プロトコル VLAN」と「MAC アドレス VLAN、リミテッドプロトコル VLAN」の 2 グループに分けられる。同時に使用できるのはどちらか 1 グループのみ。
・どの種類の VLAN を使用できるかは、ポート VLAN 以外の VLAN を最初に作成したときに決まる。購入直後のように VLAN default だけが定義されている状態では、使用可能な VLAN 種別は未確定。

(1) 最初に作成したポート VLAN 以外の VLAN が IP サブネット VLAN かプロトコル VLAN ならば、使用可能な VLAN 種別は「IP サブネット VLAN、プロトコル VLAN、ポート VLAN」となる。
(2) 最初に作成したポート VLAN 以外の VLAN が MAC アドレス VLAN かリミテッドプロトコル VLAN ならば、使用可能な VLAN 種別は「MAC アドレス VLAN、リミテッドプロトコル VLAN、ポート VLAN」となる。
・使用できる VLAN の種類が確定したあとで、異なるグループの種類の VLAN を作成することはできない。つまり、IP サブネット VLAN と MAC アドレス VLAN を同時に使用することはできない。使用できる VLAN の種類を変更するには、VLAN default 以外の VLAN をすべて削除し、使用可能な VLAN 種別を「未確定」な状態に戻す必要がある。
・現在使用可能な VLAN 種別は、SHOW SWITCH コマンドで表示される「VLAN classification」欄で確認できる。「IP subnet, Protocol, Port」は「IP サブネット VLAN、プロトコル VLAN、ポート VLAN」を使用可能、「MAC address, Limited Protocol, Port」は「MAC アドレス VLAN、リミテッドプロトコル VLAN、ポート VLAN」を使用可能なことを示す。また、「To be defined」は、ポート VLAN 以外の VLAN をまだ作成していないため、使用できる VLAN 種別が確定していないことを示す。
また、VLAN default の VLAN 種別も、ポート VLAN 以外の VLAN を最初に作成したときに決まる。最初に作成したポート VLAN 以外の VLAN が IP サブネット VLAN かプロトコル VLAN ならば、VLAN default は IP サブネット VLAN になる。また、最初に作成したポート VLAN 以外の VLAN が MAC アドレス VLAN かリミテッドプロトコル VLAN ならば、VLAN default は MAC アドレス VLAN になる。

パラメーター

VLAN　VLAN 名。この名前はコマンドでの指定を簡単にするためのもので、スイッチの外に送られることはない。

VID　VLAN ID。タグ付きポートでは、この値を元に VLAN を識別する。ポート VLAN の場合は単なる識別子として使われる。1 は VLAN default に割り当て済み。

TYPE　VLAN の種類。現在使用可能な VLAN 種別（SHOW SWITCH コマンドで表示される「VLAN classification」を参照）によって選択できる種類が異なる。省略時は PORT（ポート VLAN）と見なされる。作成した VLAN の種類を変更することはできない。変更したいときは、いったん VLAN を削除したのち、別の種類で新規に作成すること。

SUBNET　サブネット VLAN のサブネットアドレス。MASK と組み合わせて指定する。TYPE に SUBNET を指定したときだけ有効。サブネットは、ADD VLAN SUBNET コマンドを使って後から追加することも可能

MASK　サブネット VLAN の所属サブネットアドレスに対するマスク。省略時は SUBNET で指定したアドレスのクラス標準マスクが使われる

PROTOCOL　プロトコル VLAN の対象プロトコル。TYPE に PROTOCOL を指定したときだけ有効。定義済みのプロトコル名（ADD VLAN PROTOCOL コマンドの表を参照）か、16 進表記（「0x」を前置すること）のプロトコル番号で指定する。プロトコル番号で指定する場合、802.2 なら 1 バイト（DSAP のみ）で、Ethernet Version 2 なら 2 バイトで、SNAP なら 5 バイトの 16 進数で指定する。プロトコルは、ADD VLAN PROTOCOL コマンドを使って後から追加することも可能

ADDRESS　MAC アドレス VLAN のメンバー MAC アドレス。複数アドレスを範囲指定するときは本パラメーターで先頭アドレスを指定し、ENDADDRESS で終了アドレスを指定する。TYPE に MACADDRESS を指定したときだけ有効。MAC アドレスは、ADD VLAN ADDRESS コマンドを

使って後から追加することも可能

ENDADDRESS MAC アドレスを範囲指定するときの終了 MAC アドレス

LIMITEDPROTOCOL リミテッドプロトコル VLAN の対象プロトコル。TYPE に LIMITEDPROTOCOL を指定したときだけ有効。原則として IP、IPX（各フレームタイプ）、OTHER（IP・IPX 以外の意味）しか指定できない。ただし、IPX、OTHER を指定した場合は ENCAPSULATION（フレームタイプ）も指定する必要がある。16 進のプロトコル番号で指定した場合は、ENCAPSULATION の指定は不要。プロトコルは、ADD VLAN LIMITEDPROTOCOL コマンドを使って後から追加することも可能

ENCAPSULATION LIMITEDPROTOCOL に IPX か OTHER を指定した場合にフレームタイプ（エンキャプセレーション）を指定する

IP サブネット VLAN	IP サブネット（SUBNET）
	プロトコル（PROTOCOL）
	ポート（PORT）
プロトコル VLAN	プロトコル（PROTOCOL）
	ポート（PORT）
MAC アドレス VLAN	MAC アドレス（ADDRESS, ENDADDRESS）
	プロトコル（LIMITEDPROTOCOL）
	ポート（PORT）
リミテッドプロトコル VLAN	プロトコル（LIMITEDPROTOCOL）
	ポート（PORT）
ポート VLAN	ポート（PORT）

表 18: VLAN の種類と使用できるパケット分類基準（カッコ内はパラメーター名）

例

■ポート VLAN「orange」（VLAN ID=20）を作成する。

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

■プロトコル VLAN「NetWare」（VLAN ID=100）を作成する。

```
CREATE VLAN=NetWare VID=100 TYPE=PROTOCOL PROTOCOL="IPX 802.2"
```

■リミテッドプロトコル VLAN「ippp」（VLAN ID=1000）を作成する。

```
CREATE VLAN=ippp VID=1000 TYPE=LIMITEDPROTOCOL LIMITEDPROTOCOL=IP
```

備考・注意事項

VLAN は 2048 個（VLAN default を含む）まで作成できるが、IP アドレスを設定できるのは 64 個まで。
作成した直後の VLAN はデフォルトの STP ドメイン「default」に所属している。

関連コマンド

ADD VLAN ADDRESS（103 ページ）
ADD VLAN LIMITEDPROTOCOL（105 ページ）
ADD VLAN PROTOCOL（110 ページ）
ADD VLAN SUBNET（113 ページ）
DESTROY VLAN（154 ページ）
SHOW SWITCH（263 ページ）
SHOW VLAN（285 ページ）

DELETE QOS FLOWGROUP

カテゴリー：スイッチング / ポリシーベース QoS

DELETE QOS FLOWGROUP=*flow-id* CLASSIFIER={***rule-list***|**ALL**}**

flow-id: フローグループ番号（0〜1023）
rule-list: クラシファイア番号（1〜9999。ハイフン、カンマを使った複数指定も可能）

解説

フローグループからクラシファイア（汎用パケットフィルター）を削除する。

パラメーター

FLOWGROUP　フローグループ番号
CLASSIFIER　クラシファイア番号

関連コマンド

ADD QOS FLOWGROUP（93 ページ）
CREATE QOS FLOWGROUP（119 ページ）
DESTROY QOS FLOWGROUP（148 ページ）
SET QOS FLOWGROUP（212 ページ）
SHOW QOS FLOWGROUP（246 ページ）

DELETE QOS POLICY

カテゴリー：スイッチング / ポリシーベース QoS

DELETE QOS POLICY=*qos-id* TRAFFICCLASS={***tc-list***|ALL}

qos-id: QoS ポリシー番号（0〜255）
tc-list: トラフィッククラス番号（0〜511。ハイフン、カンマを使った複数指定も可能）

解説

QoS ポリシーからトラフィッククラスを削除する。

パラメーター

POLICY　QoS ポリシー番号
TRAFFICCLASS　トラフィッククラス番号

関連コマンド

ADD QOS POLICY（94 ページ）
CREATE QOS POLICY（120 ページ）
DESTROY QOS POLICY（149 ページ）
SET QOS POLICY（213 ページ）
SET QOS PORT（214 ページ）
SHOW QOS POLICY（248 ページ）

DELETE QOS TRAFFICCLASS

カテゴリー：スイッチング / ポリシーベース QoS

DELETE QOS TRAFFICCLASS=*tc-id* FLOWGROUP={***flow-list***|**ALL**}**

tc-id: トラフィッククラス番号（0〜511）
flow-list: フローグループ番号（0〜1023。ハイフン、カンマを使った複数指定も可能）

解説

トラフィッククラスからフローグループを削除する。

パラメーター

TRAFFICCLASS　トラフィッククラス番号
FLOWGROUP　フローグループ番号

関連コマンド

ADD QOS TRAFFICCLASS（95 ページ）
CREATE QOS TRAFFICCLASS（124 ページ）
DESTROY QOS TRAFFICCLASS（151 ページ）
SET QOS TRAFFICCLASS（216 ページ）
SHOW QOS TRAFFICCLASS（252 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

DELETE STP=*stpname* VLAN={***vlanname***|***2..4090***|**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（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。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（96 ページ）
SHOW STP（255 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（98 ページ）
SHOW SWITCH FILTER（272 ページ）

DELETE SWITCH HWFILTER

カテゴリー：スイッチング / ハードウェアパケットフィルター

```
DELETE SWITCH HWFILTER=filter-list
DELETE SWITCH HWFILTER=filter-id
   CLASSIFIER=rule-id [RULEPOS=pos]
DELETE SWITCH HWFILTER=filter-id
   CLASSIFIER=rule-list
DELETE SWITCH HWFILTER=filter-id CLASSIFIER=ALL
```

filter-list: フィルター番号（1〜999。ハイフン、カンマを使った複数指定も可能）
filter-id: フィルター番号（1〜999）
rule-id: クラシファイア番号（1〜9999）
rule-list: クラシファイア番号（1〜9999。ハイフン、カンマを使った複数指定も可能）
pos: エントリー番号（0〜）

解説

ハードウェアパケットフィルターからフィルターエントリー（クラシファイアとアクションのペア）を削除する。
本コマンドは、ハードウェアパケットフィルターとクラシファイアの関連付けを削除するだけで、クラシファイアそのものを削除するわけではない。クラシファイアの削除は DESTROY CLASSIFIER コマンドで行う。

パラメーター

HWFILTER　フィルター番号。他のパラメーターを指定しない場合は、複数のフィルター番号を指定可能。この場合、指定したフィルターが（エントリーも含めて）すべて削除される。他のパラメーターを指定する場合は、フィルター番号は 1 つしか指定できない

CLASSIFIER　フィルターから削除するクラシファイアの番号。複数指定も可能。複数のクラシファイア番号を指定した場合、指定した番号のクラシファイアを持つエントリーはすべて削除される。クラシファイア番号を 1 つしか指定しない場合は、RULEPOS パラメーターでエントリー番号を指定することもできる。この場合は、複数のエントリーで同じクラシファイアを使っていても、エントリー番号が一致するものだけが削除される

RULEPOS　エントリー番号。指定した番号のエントリーだけを削除する。CLASSIFIER パラメーターに単一のクラシファイア番号を指定した場合のみ有効

例

■ハードウェアパケットフィルター「39」と「96」を削除する。

```
DELETE SWITCH HWFILTER=39,96
```

■ハードウェアパケットフィルター「24」からクラシファイア「100」と「101」のエントリーを削除する。

```
DELETE SWITCH HWFILTER=24 CLASSIFIER=100-101
```

■ハードウェアパケットフィルター「2」からエントリー番号「3」のクラシファイア「52」を削除する。

```
DELETE SWITCH HWFILTER=2 CLASSIFIER=52 RULEPOS=3
```

関連コマンド

ADD SWITCH HWFILTER（100 ページ）
CREATE CLASSIFIER（114 ページ）
SHOW SWITCH HWFILTER（274 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（102 ページ）
CREATE SWITCH TRUNK（127 ページ）
DESTROY SWITCH TRUNK（153 ページ）
SET SWITCH TRUNK（227 ページ）
SHOW SWITCH TRUNK（284 ページ）

DELETE VLAN ADDRESS

カテゴリー：スイッチング / バーチャル LAN

DELETE VLAN={***vlanname***|***1..4090***} **ADDRESS=*macadd*** [ENDADDRESS=*macadd*]
DELETE
VLAN={***vlanname***|***1..4090***} **ADDRESS=**{***index-list***|**ALL**}

vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。大文字小文字を区別しない）
macadd: MAC アドレス（xx-xx-xx-xx-xx-xx の形式）
index-list: インデックス番号（0〜。ハイフン、カンマを使った複数指定も可能）

解説

MAC アドレス VLAN から MAC アドレスを削除する。
タグなしポートと関連付けられているアドレスは削除できない。その場合は、最初に DELETE VLAN PORT コマンドでポートと MAC アドレスの関連付けを削除してから、本コマンドでアドレスを削除する。

パラメーター

VLAN　VLAN 名または VLAN ID

ADDRESS　MAC アドレスまたは MAC アドレスのインデックス番号（SHOW VLAN コマンドで確認可能）。連続するアドレスを範囲指定するには、先頭・終了アドレスを ADDRESS と ENDADDRESS で指定するか、インデックス番号で範囲指定する。

ENDADDRESS　MAC アドレスを範囲指定する場合の終了 MAC アドレス。ADDRESS よりも大きい値でなくてはならない

備考・注意事項

MAC アドレスをインデックス番号で指定するときは、あらかじめ SHOW VLAN コマンドで番号を確認してから指定すること。アドレスを追加・削除するとインデックス番号がずれる可能性がある。

関連コマンド

ADD VLAN ADDRESS（103 ページ）
ADD VLAN PORT（107 ページ）
DELETE VLAN PORT（142 ページ）
SHOW VLAN（285 ページ）

DELETE VLAN LIMITEDPROTOCOL

カテゴリー：スイッチング / バーチャル LAN

DELETE VLAN={***vlanname***|***1..4090***} **LIMITEDPROTOCOL=**{**IP**|***0x0800***|**0xE0**|***0x8137***|
0xFFFF|***0x0000008137***|***index-list***|**ALL**}
DELETE VLAN={***vlanname***|***1..4090***}
LIMITEDPROTOCOL=IPX ENCAPSULATION={***802.2***|**ETHII**|**NETWARERAW**|**SNAP**|
ALL}
DELETE VLAN={***vlanname***|***1..4090***} **LIMITEDPROTOCOL=OTHER**
ENCAPSULATION={***802.2***|**ETHII**|**SNAP**|**ALL**}

vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。大文字小文字を区別しない）
index-list: インデックス番号（0〜。ハイフン、カンマを使った複数指定も可能）

解説

リミテッドプロトコル VLAN からプロトコルを削除する。

パラメーター

VLAN　VLAN 名または VLAN ID
LIMITEDPROTOCOL　プロトコルまたはインデックス番号（SHOW VLAN コマンドで確認可能）。IPX、OTHER を指定した場合は ENCAPSULATION（フレームタイプ）も指定する必要がある
ENCAPSULATION　フレームタイプ（エンキャプセレーション）。LIMITEDPROTOCOL に IPX か OTHER を指定した場合の必須パラメーター

関連コマンド

ADD VLAN LIMITEDPROTOCOL（105 ページ）
ADD VLAN PORT（107 ページ）
DELETE VLAN PORT（142 ページ）
SHOW VLAN（285 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..4090} PORT={port-list|ALL}
DELETE
   VLAN={vlanname|1..4090} PORT={port-list|ALL} SUBNET={ipadd|ALL}
DELETE
   VLAN={vlanname|1..4090} PORT={port-list|ALL} PROTOCOL={protocoltype|
   index-list|ALL}
DELETE VLAN={vlanname|1..4090} PORT={port-list|ALL}
   ADDRESS=macadd [ENDADDRESS=macadd]
DELETE VLAN={vlanname|1..4090}
   PORT={port-list|ALL} ADDRESS={index-list|ALL}
DELETE VLAN={vlanname|
   1..4090} PORT={port-list|ALL} LIMITEDPROTOCOL={IP|0x0800|0xE0|0x8137|
   0xFFFF|0x0000008137|index-list|ALL}
DELETE VLAN={vlanname|1..4090}
   PORT={port-list|ALL} LIMITEDPROTOCOL=IPX ENCAPSULATION={802.2|ETHII|
   NETWARERAW|SNAP|ALL}
DELETE VLAN={vlanname|1..4090} PORT={port-list|ALL}
   LIMITEDPROTOCOL=OTHER ENCAPSULATION={802.2|ETHII|SNAP|ALL}
```

vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。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）
ipadd: IP アドレス
protocoltype: L3 プロトコル番号（16 進数。「0x」を前置すること）
index-list: インデックス番号（0〜。ハイフン、カンマを使った複数指定も可能）
macadd: MAC アドレス（xx-xx-xx-xx-xx-xx の形式）

解説

VLAN からポートを削除する。または、ポートとプロトコル、リミテッドプロトコル、IP サブネット、MAC アドレスとの関連付けを削除する。
VLAN と PORT パラメーターだけを指定した場合は、指定した VLAN のポート VLAN メンバーから指定ポートを削除する。
VLAN、PORT パラメーターに加え、SUBNET、PROTOCOL、ADDRESS（および ENDADDRESS）、LIMITEDPROTOCOL（および ENCAPSULATION）のいずれかを指定した場合は、それぞれ指定 VLAN のサブネット VLAN メンバー、プロトコル VLAN メンバー、MAC アドレス VLAN メンバー、リミテッドプロトコル VLAN メンバーから指定ポートを削除する。

パラメーター

VLAN　VLAN 名または VLAN ID。VLAN default にのみ所属しているポートを VLAN default から削除することはできない。

PORT　削除するポートの一覧。ALL を指定した場合は、該当 VLAN の所属ポートがすべて削除される。

SUBNET　サブネットアドレス。サブネット VLAN からポートを削除するときに指定する。

PROTOCOL　プロトコル。プロトコル VLAN からポートを削除するときに指定する。プロトコルは、定義済みのプロトコル名（ADD VLAN PROTOCOL コマンドの表を参照）か、16 進表記（「0x」を前置すること）のプロトコル番号で指定する。あるいは、SHOW VLAN コマンドで表示されるインデックス番号（複数指定可）で指定することもできる。

ADDRESS　MAC アドレス。MAC アドレス VLAN からポートを削除するときに指定する。連続するアドレスを範囲指定するには、本パラメーターで先頭アドレスを指定し、ENDADDRESS で終了アドレスを指定する。あるいは、SHOW VLAN コマンドで表示されるインデックス番号（複数指定可）で指定することもできる。

ENDADDRESS　範囲指定時の終了 MAC アドレス

LIMITEDPROTOCOL　プロトコル。リミテッドプロトコル VLAN からポートを削除するときに指定する。プロトコルは、定義済みのプロトコル名（ADD VLAN LIMITEDPROTOCOL コマンドの表を参照）か、16 進表記のプロトコル番号で指定する。あるいは、SHOW VLAN コマンドで表示されるインデックス番号（複数指定可）で指定することもできる。IPX か OTHER を指定した場合は ENCAPSULATION パラメーターも必須

ENCAPSULATION　フレームタイプ（エンキャプセレーション）。LIMITEDPROTOCOL に IPX か OTHER を指定した場合の必須パラメーター

例

■VLAN orange からポート 2 を削除する。

```
DELETE VLAN=orange PORT=2
```

■VLAN net10 のサブネット VLAN メンバー（所属サブネット 192.168.10.0/24）からポート 1〜4 を削除する。

```
DELETE VLAN=net10 PORT=1-4 SUBNET=192.168.10.0
```

■VLAN nw のプロトコル VLAN メンバー（所属プロトコル IPX 802.2）からポート 3 と 5 を削除する。

```
DELETE VLAN=nw PORT=3,5 PROTOCOL="IPX 802.2"
```

■VLAN private の MAC アドレス VLAN メンバー（所属アドレス範囲 00-00-f4-00-00-00〜00-00-f4-00-03-ff）からポート 2、4〜6 を削除する。

```
DELETE VLAN=private PORT=2,4-6 ADDRESS=00-00-f4-00-00-00
  ENDADDRESS=00-00-f4-00-03-ff
```

■VLAN private のリミテッドプロトコル VLAN メンバー（所属プロトコル IPX（802.3 raw））からポート 5 を削除する。

```
DELETE VLAN=private PORT=5 LIMITEDPROTOCOL=IPX ENCAPSULATION=NETWARERAW
```

関連コマンド

ADD VLAN PORT（107 ページ）
ADD VLAN SUBNET（113 ページ）
DELETE VLAN ADDRESS（140 ページ）
DELETE VLAN LIMITEDPROTOCOL（141 ページ）
DELETE VLAN PROTOCOL（145 ページ）
DELETE VLAN SUBNET（146 ページ）
SHOW VLAN（285 ページ）

DELETE VLAN PROTOCOL

カテゴリー：スイッチング / バーチャル LAN

DELETE VLAN={***vlanname***|***1..4090***} **PROTOCOL=**{***protocoltype***|***index-list***|**ALL**}

vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。大文字小文字を区別しない）
protocoltype: L3 プロトコル番号（16 進数。「0x」を前置すること）
index-list: インデックス番号（0〜。ハイフン、カンマを使った複数指定も可能）

解説

プロトコル VLAN からプロトコルを削除する。

パラメーター

VLAN　VLAN 名または VLAN ID
PROTOCOL　プロトコルまたはインデックス番号（SHOW VLAN コマンドで確認可能）

関連コマンド

ADD VLAN PORT（107 ページ）
ADD VLAN PROTOCOL（110 ページ）
DELETE VLAN PORT（142 ページ）
SHOW VLAN（285 ページ）

DELETE VLAN SUBNET

カテゴリー：スイッチング / バーチャル LAN

DELETE VLAN={***vlanname***|***1..4090***} **SUBNET=**{***ipadd***|**ALL**}

vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。大文字小文字を区別しない）
ipadd: IP アドレス

解説

IP サブネット VLAN から IP サブネットを削除する。

パラメーター

VLAN　VLAN 名または VLAN ID
SUBNET　サブネットアドレス

関連コマンド

ADD VLAN PORT（107 ページ）
ADD VLAN PROTOCOL（110 ページ）
DELETE VLAN PORT（142 ページ）
SHOW VLAN（285 ページ）

DESTROY CLASSIFIER

カテゴリー：スイッチング / クラシファイア

DESTROY CLASSIFIER={***rule-list***|**ALL**}

rule-list: クラシファイア番号（1〜9999。ハイフン、カンマを使った複数指定も可能）

解説

クラシファイア（汎用パケットフィルター）を削除する。
ハードウェアパケットフィルターや QoS フローグループに関連付けられているクラシファイアは削除できない。

パラメーター

CLASSIFIER　クラシファイア番号。ALL を指定した場合は、すべてのクラシファイアが削除される

例

■クラシファイア「10」「12」「13」を削除する。

```
DESTROY CLASSIFIER=10,12-13
```

■すべてのクラシファイアを削除する。

```
DESTROY CLASSIFIER=ALL
```

関連コマンド

CREATE CLASSIFIER（114 ページ）
SET CLASSIFIER（204 ページ）
SHOW CLASSIFIER（230 ページ）

DESTROY QOS FLOWGROUP

カテゴリー：スイッチング / ポリシーベース QoS

DESTROY QOS FLOWGROUP={***flow-list***|**ALL**}

flow-list: フローグループ番号（0〜1023。ハイフン、カンマを使った複数指定も可能）

解説

フローグループを削除する。

パラメーター

FLOWGROUP　フローグループ番号

関連コマンド

ADD QOS POLICY（94 ページ）
CREATE QOS FLOWGROUP（119 ページ）
DELETE QOS POLICY（133 ページ）
SET QOS POLICY（213 ページ）
SET QOS PORT（214 ページ）
SHOW QOS POLICY（248 ページ）

DESTROY QOS POLICY

カテゴリー：スイッチング / ポリシーベース QoS

DESTROY QOS POLICY={***qos-list***|**ALL**}

qos-list: QoS ポリシー番号（0〜255。ハイフン、カンマを使った複数指定も可能）

解説

QoS ポリシーを削除する。

パラメーター

POLICY　QoS ポリシー番号

関連コマンド

ADD QOS POLICY（94 ページ）
CREATE QOS FLOWGROUP（119 ページ）
DELETE QOS POLICY（133 ページ）
SET QOS POLICY（213 ページ）
SET QOS PORT（214 ページ）
SHOW QOS POLICY（248 ページ）

DESTROY QOS RED

カテゴリー：スイッチング / ポリシーベース QoS

DESTROY QOS RED={***red-list***|**ALL**}

red-list: RED 番号（5〜47。ハイフン、カンマを使った複数指定も可能）

解説

RED（Random Early Detection / Discard）カーブを削除する。

パラメーター

RED　RED カーブ番号

関連コマンド

CREATE QOS RED（122 ページ）
SET QOS RED（215 ページ）
SHOW QOS RED（250 ページ）

DESTROY QOS TRAFFICCLASS

カテゴリー：スイッチング / ポリシーベース QoS

DESTROY QOS TRAFFICCLASS={***tc-list***|**ALL**}

tc-list: トラフィッククラス番号（0〜511。ハイフン、カンマを使った複数指定も可能）

解説

トラフィッククラスを削除する。

パラメーター

TRAFFICCLASS　トラフィッククラス番号

関連コマンド

ADD QOS TRAFFICCLASS（95 ページ）
CREATE QOS TRAFFICCLASS（124 ページ）
DELETE QOS TRAFFICCLASS（134 ページ）
SET QOS TRAFFICCLASS（216 ページ）
SHOW QOS TRAFFICCLASS（252 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

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（126 ページ）
DISABLE STP（160 ページ）
ENABLE STP（183 ページ）
SET STP（219 ページ）
SHOW STP（255 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（102 ページ）
CREATE SWITCH TRUNK（127 ページ）
DELETE SWITCH TRUNK（139 ページ）
SET SWITCH TRUNK（227 ページ）
SHOW SWITCH TRUNK（284 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..4090***|**ALL**}

vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。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。VLAN default は削除できない。

関連コマンド

CREATE VLAN（128 ページ）
SHOW VLAN（285 ページ）

DISABLE PORTAUTH

カテゴリー：スイッチング / 802.1X 認証

DISABLE PORTAUTH

解説

802.1X 認証モジュールを無効にする。デフォルトは無効。

関連コマンド

DISABLE PORTAUTH PORT（157 ページ）
ENABLE PORTAUTH（174 ページ）
ENABLE PORTAUTH PORT（178 ページ）
SHOW PORTAUTH PORT（239 ページ）

DISABLE PORTAUTH DEBUG

カテゴリー：スイッチング / 802.1X 認証

DISABLE PORTAUTH 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、802.1X 認証モジュール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

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。

PORT　スイッチポート。複数指定が可能。

関連コマンド

ENABLE PORTAUTH（174 ページ）
ENABLE PORTAUTH DEBUG（175 ページ）
ENABLE PORTAUTH PORT（178 ページ）
SHOW PORTAUTH PORT（239 ページ）

DISABLE PORTAUTH PORT

カテゴリー：スイッチング / 802.1X 認証

DISABLE PORTAUTH 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、802.1X 認証機能を無効にする。デフォルトは全ポート無効。

パラメーター

PORT　スイッチポート。複数指定が可能。

関連コマンド

DISABLE PORTAUTH（155 ページ）
ENABLE PORTAUTH（174 ページ）
ENABLE PORTAUTH PORT（178 ページ）
SHOW PORTAUTH PORT（239 ページ）

DISABLE QOS DEBUG

カテゴリー：スイッチング / ポリシーベース QoS

DISABLE QOS DEBUG={**COMMAND**|**DETAIL**|**TRACE**|**ALL**}

解説

QoS 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　無効にするデバッグオプション。デフォルトはすべて無効

関連コマンド

ENABLE QOS DEBUG（181 ページ）

DISABLE QOS VLANPRIORITYREMAPPING

カテゴリー：スイッチング / ポリシーベース QoS

DISABLE QOS VLANPRIORITYREMAPPING

解説

802.1p タグプライオリティー書き換え機能を無効にする。デフォルトは無効。

関連コマンド

ENABLE QOS VLANPRIORITYREMAPPING（182 ページ）
SET QOS VLANREMAP（218 ページ）
SHOW QOS VLANPRIORITYREMAPPING（254 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

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（126 ページ）
DESTROY STP（152 ページ）
ENABLE STP（183 ページ）
SET STP（219 ページ）
SHOW STP（255 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

DISABLE STP={***stpname***|**ALL**} **DEBUG=**{**MSG**|**PKT**|**STATE**|**ALL**}

stpname: STP ドメイン名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。大文字小文字を区別しない）

解説

STP ドメインのデバッグオプションを無効にする。

パラメーター

STP STP ドメイン名。

DEBUG 無効にするデバッグオプション。MSG（STP パケットをデコードして表示）、PKT（STP パケットを ASCII 表示）、STATE（ポートの状態遷移を表示）、ALL（すべてのオプション）から選択する。

関連コマンド

DISABLE STP PORT DEBUG（163 ページ）
ENABLE STP DEBUG（184 ページ）
SHOW STP DEBUG（260 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

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でいうディセーブル状態となり、同ポートでは STP パケットの送受信が行われなくなる。

パラメーター

PORT　ポート番号。複数指定が可能。ALL を指定した場合はすべてのスイッチポートでスパニングツリープロトコルを無効にする。

関連コマンド

ENABLE STP PORT（185 ページ）
SET STP PORT（221 ページ）
SHOW STP PORT（261 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

DISABLE STP PORT={***port-list***|**ALL**} **DEBUG=**{**MSG**|**PKT**|**STATE**|**ALL**}

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）

解説

STP ポートのデバッグオプションを無効にする。

パラメーター

PORT　ポート番号。複数指定が可能。

DEBUG　無効にするデバッグオプション。MSG（STP パケットをデコードして表示）、PKT（STP パケットを ASCII 表示）、STATE（ポートの状態遷移を表示）、ALL（すべてのオプション）から選択する。

関連コマンド

DISABLE STP DEBUG（161 ページ）
ENABLE STP DEBUG（184 ページ）
ENABLE STP PORT DEBUG（186 ページ）
SHOW STP DEBUG（260 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（187 ページ）
SET SWITCH AGEINGTIMER（223 ページ）
SHOW SWITCH（263 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={**DMA**|**QOS**|**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。DMA（ダイレクトメモリーアクセス）、QOS（QoS）、PHY（PHY）、ALL（すべて）から選択する。

関連コマンド

ENABLE SWITCH DEBUG（188 ページ）
SHOW SWITCH（263 ページ）

DISABLE SWITCH HASH

カテゴリー：スイッチング / ポート

DISABLE SWITCH HASH={**L2**|**L3**|**L4**}**[,...]**

解説

ポートトランキングの送出ポート決定アルゴリズムにおいて、指定した種類のヘッダー情報を使わないよう設定する。
デフォルトでは、L2 と L4 のヘッダー情報を使用して送出ポートを決定する。

パラメーター

HASH　送出ポート決定アルゴリズムで使用しないヘッダー情報の種別。L2（送信元・宛先 MAC アドレス）、L3（始点・終点 IP アドレス）、L4（始点・終点ポート）から選択する。カンマ区切りで複数指定が可能。

関連コマンド

ADD SWITCH TRUNK（102 ページ）
CREATE SWITCH TRUNK（127 ページ）
ENABLE SWITCH HASH（189 ページ）
SHOW SWITCH（263 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（190 ページ）
SHOW SWITCH（263 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（191 ページ）
SET SWITCH MIRROR（224 ページ）
SET SWITCH PORT（225 ページ）
SHOW SWITCH（263 ページ）
SHOW SWITCH PORT（276 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**}

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

関連コマンド

ENABLE SWITCH PORT（192 ページ）
SHOW SWITCH PORT（276 ページ）

DISABLE SWITCH PORT FLOW

カテゴリー：スイッチング / ポート

DISABLE SWITCH PORT={***port-list***|**ALL**} **FLOW=**{**PAUSE**}

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）

解説

指定したスイッチポートでフローコントロール（802.3x PAUSE）を無効にする。デフォルトは無効。

パラメーター

PORT　ポート番号

FLOW　フロー制御方式。PAUSE（802.3x PAUSE。オートネゴシエーションによる Full Duplex 接続時）のみサポート。

備考・注意事項

本製品の実装では PAUSE フレームの受信（受信により送信を一時停止）のみをサポート。PAUSE フレームの送信についてはサポート対象外。

関連コマンド

ENABLE SWITCH PORT FLOW（193 ページ）
SHOW SWITCH PORT（276 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（194 ページ）
SHOW SWITCH（263 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..4090***|**ALL**} **DEBUG=**{**PKT**|**ALL**}

vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。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（195 ページ）
SHOW VLAN DEBUG（289 ページ）

DISABLE VLAN STORMPROTECT

カテゴリー：スイッチング / バーチャル LAN

DISABLE VLAN={***vlanname***|***1..4090***|**ALL**} **STORMPROTECT=**{**BC**|**MC**}[,...]

vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。大文字小文字を区別しない）

解説

指定した VLAN でパケットストームプロテクションを無効にする。
デフォルトでは、すべての VLAN でパケットストームプロテクションが無効に設定されている（BCLIMIT、MCLIMIT ともに NONE）。SET VLAN コマンドで BCLIMIT か MCLIMIT を NONE 以外に設定すると、該当 VLAN のパケットストームプロテクションが自動的に有効化される。

パラメーター

VLAN　VLAN 名または VLAN ID

STORMPROTECT　ストームプロテクションを無効にするパケットタイプ。BC（ブロードキャスト）、MC（マルチキャスト）から選択する。カンマ区切りで複数指定が可能。

関連コマンド

ENABLE VLAN STORMPROTECT（196 ページ）
SET VLAN（228 ページ）
SHOW VLAN（285 ページ）

ENABLE PORTAUTH

カテゴリー：スイッチング / 802.1X 認証

ENABLE PORTAUTH

解説

802.1X 認証モジュールを有効にする。デフォルトは無効。
802.1X 認証を使用するためには、使用するスイッチポートでもポート認証を有効にする必要がある（ENABLE PORTAUTH PORT コマンド）。

関連コマンド

DISABLE PORTAUTH（155 ページ）
DISABLE PORTAUTH PORT（157 ページ）
ENABLE PORTAUTH PORT（178 ページ）
SHOW PORTAUTH PORT（239 ページ）

ENABLE PORTAUTH DEBUG

カテゴリー：スイッチング / 802.1X 認証

ENABLE PORTAUTH 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、802.1X 認証モジュール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

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。

PORT　スイッチポート。複数指定が可能。

入力・出力・画面例

```
Manager > ena portauth port=7 type=authenticator

PORTAUTH : Int=port7     Authenticator Pae State Change
           From : INITIALISE       To : INITIALISE

PORTAUTH : Int=port7     Authenticator Pae State Change
           From : INITIALISE       To : DISCONNECTED
EAPOL Auth Tx: ifIndex=7 ver=1 type=EAP len=4
   EAP Auth Tx: code=FAILURE id=0 length=4

PORTAUTH : Int=port7     Authenticator Pae State Change
           From : DISCONNECTED     To : CONNECTING

EAPOL Auth Tx: ifIndex=7 ver=1 type=EAP len=5
   EAP Auth Tx: code=REQUEST type=IDENTITY id=1 length=5

PORTAUTH : Int=port7     Backend Authentication State Change
           From : INITIALISE       To : IDLE

Info (1118003): Operation successful.

Manager >
PORTAUTH : Int=port7     Authenticator Pae State Change
           From : CONNECTING       To : CONNECTING
EAPOL Auth Tx: ifIndex=7 ver=1 type=EAP len=5
   EAP Auth Tx: code=REQUEST type=IDENTITY id=1 length=5
```

```
Manager >
PORTAUTH : Int=port7     Authenticator Pae State Change
           From : CONNECTING       To : CONNECTING
EAPOL Auth Tx: ifIndex=7 ver=1 type=EAP len=5
   EAP Auth Tx: code=REQUEST type=IDENTITY id=1 length=5

PORTAUTH : Int=port7     Authenticator Pae State Change
           From : CONNECTING       To : DISCONNECTED
EAPOL Auth Tx: ifIndex=7 ver=1 type=EAP len=4
   EAP Auth Tx: code=FAILURE id=1 length=4

PORTAUTH : Int=port7     Authenticator Pae State Change
           From : DISCONNECTED     To : CONNECTING
EAPOL Auth Tx: ifIndex=7 ver=1 type=EAP len=5
   EAP Auth Tx: code=REQUEST type=IDENTITY id=2 length=5

Manager > EAPOL Auth Rx: ifIndex=7 src=00-00-e2-59-56-48 ver=1 type=EAP len=9
   EAP Auth Rx: ifIndex=7 code=RESPONSE type=IDENTITY id=2 length=9

PORTAUTH : Int=port7     Authenticator Pae State Change
           From : CONNECTING       To : AUTHENTICATING

PORTAUTH : Int=port7     Backend Authentication State Change
           From : IDLE             To : RESPONSE

EAP Auth Tx: code=RESPONSE type=IDENTITY id=2 length=9
EAP Auth Rx: ifIndex=7 code=REQUEST type=MD5 id=3 length=22

PORTAUTH : Int=port7     Backend Authentication State Change
           From : RESPONSE         To : REQUEST
EAPOL Auth Tx: ifIndex=7 ver=1 type=EAP len=22
   EAP Auth Tx: code=REQUEST type=MD5 id=3 length=22
EAPOL Auth Rx: ifIndex=7 src=00-00-e2-59-56-48 ver=1 type=EAP len=26
   EAP Auth Rx: ifIndex=7 code=RESPONSE type=MD5 id=3 length=26

PORTAUTH : Int=port7     Backend Authentication State Change
           From : REQUEST          To : RESPONSE
EAP Auth Tx: code=RESPONSE type=MD5 id=3 length=26
EAP Auth Rx: ifIndex=7 code=SUCCESS id=3 length=4

PORTAUTH : Int=port7     Backend Authentication State Change
           From : RESPONSE         To : SUCCESS
EAPOL Auth Tx: ifIndex=7 ver=1 type=EAP len=4
   EAP Auth Tx: code=SUCCESS id=3 length=4

PORTAUTH : Int=port7     Authenticator Pae State Change
           From : AUTHENTICATING   To : AUTHENTICATED

PORTAUTH : Int=port7     Backend Authentication State Change
           From : SUCCESS          To : IDLE
```

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（156 ページ）
ENABLE PORTAUTH（174 ページ）
ENABLE PORTAUTH PORT（178 ページ）
SHOW PORTAUTH PORT（239 ページ）

ENABLE PORTAUTH PORT

カテゴリー：スイッチング / 802.1X 認証

```
ENABLE PORTAUTH PORT={port-list|ALL} TYPE=AUTHENTICATOR
   [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]
ENABLE PORTAUTH PORT={port-list|ALL} TYPE=BOTH
   [AUTHPERIOD=1..60] [CONTROL={AUTHORISED|UNAUTHORISED|AUTO}]
   [HELDPERIOD=0..65535] [MAXREQ=1..10] [MAXSTART=1..10]
   [QUIETPERIOD=0..65535] [REAUTHENABLED={TRUE|FALSE}] [REAUTHMAX=1..10]
   [REAUTHPERIOD=1..86400] [SERVERTIMEOUT=1..60] [STARTPERIOD=1..60]
   [SUPPTIMEOUT=1..60] [TXPERIOD=1..65535] [USERNAME=login-name
   PASSWORD=password [METHOD={OTP [ENCRYPTION={MD4|MD5}]|STANDARD}]]
ENABLE
   PORTAUTH 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}]]
```

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）
login-name: ログイン名（1〜64 文字。英数字のみ使用可能）
password: パスワード（1〜64 文字。英数字のみ使用可能）

解説

指定ポートで、802.1X 認証機能を有効にする。各ポートは、Authenticator、Supplicant、Authenticator かつ Supplicant 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

PORT　スイッチポート。複数指定が可能。

TYPE　スイッチポートのタイプ（802.1X における役割）。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。

CONTROL　（Authenticator 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　（Authenticator ポート）Supplicant に対する EAPOL-Request パケットの最大再送回数。デ

フォルトは 2 回

QUIETPERIOD （Authenticator 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 EAPOL パケットをすべて破棄する。デフォルトは 60 秒。

REAUTHENABLED （Authenticator 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 （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 （Authenticator ポート）Supplicant の再認証間隔（秒）。デフォルトは 3600 秒。

SERVERTIMEOUT （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 （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 （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。

AUTHPERIOD （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 （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 （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、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 （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 （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 （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 （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 （Supplicant ポート）ワンタイムパスワードの生成アルゴリズム。MD4、MD5 から選択する。デフォルトは MD5。METHOD パラメーターに OTP を指定した場合の必須パラメーター。

備考・注意事項

802.1X 認証を有効にしたポート（Authenticator、Supplicant とも）では、ポートトランキング、スパニングツリープロトコル、ポートセキュリティーを使用できない。また、Authenticator ポートをタグ付きに設定することはできない。

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE（90 ページ）
ENABLE PORTAUTH（174 ページ）
ENABLE PORTAUTH PORT（178 ページ）
SET PORTAUTH PORT（207 ページ）
SHOW PORTAUTH（234 ページ）
SHOW PORTAUTH COUNTER（236 ページ）
SHOW PORTAUTH PORT（239 ページ）
SHOW PORTAUTH TIMER（244 ページ）

ENABLE QOS DEBUG

カテゴリー：スイッチング / ポリシーベース QoS

ENABLE QOS DEBUG={**COMMAND**|**DETAIL**|**TRACE**|**ALL**}

解説

QoS モジュールのデバッグオプションを有効にする。

パラメーター

DEBUG　有効にするデバッグオプション。デフォルトはすべて無効

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 QOS DEBUG（158 ページ）

ENABLE QOS VLANPRIORITYREMAPPING

カテゴリー：スイッチング / ポリシーベース QoS

ENABLE QOS VLANPRIORITYREMAPPING

解説

802.1p タグプライオリティー書き換え機能を有効にする。デフォルトは無効。

関連コマンド

DISABLE QOS VLANPRIORITYREMAPPING（159 ページ）
SET QOS VLANREMAP（218 ページ）
SHOW QOS VLANPRIORITYREMAPPING（254 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

ENABLE STP{**=***stpname*|**ALL**}

stpname: STP ドメイン名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。大文字小文字を区別しない）

解説

STP ドメイン、あるいは、スイッチ全体でスパニングツリープロトコルを有効にする。デフォルトはどちらも無効。

パラメーター

STP　STP ドメイン名。

関連コマンド

CREATE STP（126 ページ）
DESTROY STP（152 ページ）
DISABLE STP（160 ページ）
SET STP（219 ページ）
SHOW STP（255 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

ENABLE STP={***stpname***|**ALL**} **DEBUG=**{**MSG**|**PKT**|**STATE**|**ALL**} [OUTPUT=CONSOLE]
[TIMEOUT={*1..4000000000*|NONE}]

stpname: STP ドメイン名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。大文字小文字を区別しない）

解説

指定した STP ドメインのデバッグオプションを有効にする。
デバッグをオンにすると、端末（コンソールや Telnet クライアント）画面に大量のデバッグ情報が出力されるため注意が必要。

パラメーター

STP　STP ドメイン名。
DEBUG　デバッグオプション。MSG（STP パケットをデコードして表示）、PKT（STP パケットを ASCII 表示）、STATE（ポートの状態遷移を表示）、ALL（すべてのオプション）から選択する。
OUTPUT　デバッグ情報の出力先を指定する。CONSOLE（コンソール）のみ指定可能。省略時はコマンドを投入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（161 ページ）
SHOW STP DEBUG（260 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

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（162 ページ）
SET STP PORT（221 ページ）
SHOW STP PORT（261 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

ENABLE STP PORT={***port-list***|**ALL**} **DEBUG=**{**MSG**|**PKT**|**STATE**|**ALL**}
[OUTPUT=CONSOLE] [TIMEOUT={*1..4000000000*|NONE}]

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）

解説

STP ポートのデバッグオプションを有効にする。

パラメーター

PORT ポート番号。複数指定が可能。

DEBUG デバッグオプション。MSG（STP パケットをデコードして表示）、PKT（STP パケットを ASCII 表示）、STATE（ポートの状態遷移を表示）、ALL（すべてのオプション）から選択する。

OUTPUT デバッグ情報の出力先を指定する。CONSOLE（コンソール）のみ指定可能。省略時はコマンドを投入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（161 ページ）
DISABLE STP PORT DEBUG（163 ページ）
ENABLE STP（183 ページ）
SHOW STP DEBUG（260 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（164 ページ）
SET SWITCH AGEINGTIMER（223 ページ）
SHOW SWITCH（263 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={**DMA**|**QOS**|**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。DMA（ダイレクトメモリーアクセス）、QOS（QoS）、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投入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（165 ページ）
SHOW SWITCH（263 ページ）

ENABLE SWITCH HASH

カテゴリー：スイッチング / ポート

ENABLE SWITCH HASH={**L2**|**L3**|**L4**}**[,...]**

解説

ポートトランキングの送出ポート決定アルゴリズムにおいて、指定した種類のヘッダー情報を使うよう設定する。
デフォルトでは、L2 と L4 のヘッダー情報を使用して送出ポートを決定する。

パラメーター

HASH　送出ポート決定アルゴリズムで使用するヘッダー情報の種別。L2（送信元・宛先 MAC アドレス）、L3（始点・終点 IP アドレス）、L4（始点・終点ポート）から選択する。カンマ区切りで複数指定が可能。

関連コマンド

ADD SWITCH TRUNK（102 ページ）
CREATE SWITCH TRUNK（127 ページ）
DISABLE SWITCH HASH（166 ページ）
SHOW SWITCH（263 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（167 ページ）
SHOW SWITCH（263 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。

備考・注意事項

本製品では受信パケットのミラーリングだけが可能。送信パケットのミラーリングには対応していない。

関連コマンド

DISABLE SWITCH MIRROR（168 ページ）
SET SWITCH MIRROR（224 ページ）
SET SWITCH PORT（225 ページ）
SHOW SWITCH（263 ページ）
SHOW SWITCH PORT（276 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ー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ーをオフにする必要がある。

関連コマンド

DISABLE SWITCH PORT（169 ページ）
SHOW SWITCH PORT（276 ページ）

ENABLE SWITCH PORT FLOW

カテゴリー：スイッチング / ポート

ENABLE SWITCH PORT={***port-list***|**ALL**} **FLOW=**{**PAUSE**}

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）

解説

指定したスイッチポートでフローコントロール（802.3x PAUSE）を有効にする。デフォルトは無効。
有効に設定している場合は、オートネゴシエーション時に AS/SY ビットをオンにして、フローコントロール動作可であることを対向機器に通知する（無効のときは AS/SY ビットオフ）。

パラメーター

PORT　ポート番号
FLOW　フロー制御方式。PAUSE（802.3x PAUSE。オートネゴシエーションによる Full Duplex 接続時）のみサポート。

備考・注意事項

本製品の実装では PAUSE フレームの受信（受信により送信を一時停止）のみをサポート。PAUSE フレームの送信についてはサポート対象外。

関連コマンド

DISABLE SWITCH PORT FLOW（170 ページ）
SHOW SWITCH PORT（276 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（171 ページ）
SHOW SWITCH（263 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..4090***|**ALL**} **DEBUG=**{**PKT**|**ALL**} [OUTPUT=CONSOLE]
[TIMEOUT={*1..4000000000*|NONE}]

vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。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投入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（172 ページ）
SHOW VLAN DEBUG（289 ページ）

ENABLE VLAN STORMPROTECT

カテゴリー：スイッチング / バーチャル LAN

ENABLE VLAN={***vlanname***|***1..4090***|**ALL**} **STORMPROTECT=**{**BC**|**MC**}**[,...]**

vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。大文字小文字を区別しない）

解説

指定した VLAN でパケットストームプロテクションを有効にする。
デフォルトでは、すべての VLAN でパケットストームプロテクションが無効に設定されている（BCLIMIT、MCLIMIT ともに NONE）。SET VLAN コマンドで BCLIMIT か MCLIMIT を NONE 以外に設定すると、該当 VLAN のパケットストームプロテクションが自動的に有効化される。

パラメーター

VLAN　VLAN 名または VLAN ID

STORMPROTECT　ストームプロテクションを有効にするパケットタイプ。BC（ブロードキャスト）、MC（マルチキャスト）から選択する。カンマ区切りで複数指定が可能。

関連コマンド

DISABLE VLAN STORMPROTECT（173 ページ）
SET VLAN（228 ページ）
SHOW VLAN（285 ページ）

PURGE PORTAUTH PORT

カテゴリー：スイッチング / 802.1X 認証

PURGE PORTAUTH 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 認証設定をすべて削除する。

パラメーター

PORT　スイッチポート。複数指定が可能。

備考・注意事項

ランタイムメモリー上にある、指定ポートの 802.1X 関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意すること。

関連コマンド

DISABLE PORTAUTH（155 ページ）
DISABLE PORTAUTH PORT（157 ページ）
SHOW PORTAUTH PORT（239 ページ）

PURGE QOS

カテゴリー：スイッチング / ポリシーベース QoS

PURGE QOS

解説

ポリシーベース QoS の設定をすべて削除する。

備考・注意事項

ランタイムメモリー上にあるポリシーベース QoS 関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意すること。

関連コマンド

SHOW QOS POLICY（248 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

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（201 ページ）
SET STP（219 ページ）
SET STP PORT（221 ページ）
SHOW STP（255 ページ）
SHOW STP COUNTER（258 ページ）

RESET PORTAUTH PORT

カテゴリー：スイッチング / 802.1X 認証

RESET PORTAUTH 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、802.1X 認証機能の状態をリセットする。

パラメーター

PORT　スイッチポート。複数指定が可能。

関連コマンド

DISABLE PORTAUTH（155 ページ）
DISABLE PORTAUTH PORT（157 ページ）
ENABLE PORTAUTH（174 ページ）
ENABLE PORTAUTH PORT（178 ページ）
SHOW PORTAUTH PORT（239 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

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（199 ページ）
SET STP（219 ページ）
SHOW STP（255 ページ）
SHOW STP COUNTER（258 ページ）

RESET SWITCH

カテゴリー：スイッチング / 一般コマンド

RESET SWITCH

解説

スイッチングモジュールをリセットする。
すべてのスイッチポートがリセットされ、FDB のダイナミックエントリーなど、動的に取得した情報はすべてクリアされる。また、スイッチングに関するタイマーと統計カウンターもクリアされる。

関連コマンド

SHOW SWITCH（263 ページ）
SHOW SWITCH FDB（269 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。

備考・注意事項

本コマンドは、GBIC ポートおよび（GBIC でない）1000BASE-SX ポートに対しては機能しない。

関連コマンド

DISABLE SWITCH PORT（169 ページ）
ENABLE SWITCH PORT（192 ページ）
SHOW SWITCH PORT（276 ページ）

SET CLASSIFIER

カテゴリー：スイッチング / クラシファイア

SET CLASSIFIER=*rule-id* [SVLAN={*vlanname*|*1..4090*|ANY}] [DVLAN={*vlanname*|*1..4090*|ANY}] [ETHFORMAT={*802.2*|ETHII|NETWARERAW|SNAP|ANY}] [PROTOCOL={*protocoltype*|IP|IPX|NONIPIPX|ANY}] [MACTYPE={L2UCAST|L2MCAST|L2BCAST|ANY}] [IPSADDR={*ipadd*[*/masklen*]|ANY}] [IPDADDR={*ipadd*[*/masklen*]|ANY}] [IPDSCP={*0..63*|ANY}] [IPTOS={*0..7*|ANY}] [IPPROTOCOL={TCP|UDP|ICMP|IGMP|*protocol*|ANY|NONTCPUDP}] [IPXDADDR={*ipxnet*|ANY}] [IPXSSOCKET={NCP|SAP|RIP|NNB|DIAG|NLSP|IPXWAN|*socket*|ANY}] [IPXDSOCKET={NCP|SAP|RIP|NNB|DIAG|NLSP|IPXWAN|*socket*|ANY}] [TCPSPORT={*port*|ANY}] [TCPDPORT={*port*|ANY}] [UDPSPORT={*port*|ANY}] [UDPDPORT={*port*|ANY}]

rule-id: クラシファイア番号（1〜9999）
vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。大文字小文字を区別しない）
protocoltype: L3 プロトコル番号（16 進数）
ipadd: IP アドレス
masklen: マスク長（0〜32）
protocol: IP プロトコル番号（0〜255）
ipxnet: IPX ネットワーク番号（32 ビット長。16 進数最大 8 文字。先頭の 0 は省略可能）
socket: IPX ソケット番号（16 ビット長。16 進数最大 4 文字）
port: TCP / UDP ポート番号（0〜65535）

解説

クラシファイア（汎用パケットフィルター）の設定を変更する。

パラメーター

CLASSIFIER　クラシファイア番号。この番号は単なる識別子であり、番号の大小は意味を持たない。番号は固定なので、他のクラシファイアを削除しても変更されることはない。また、番号に空きがあってもよい

SVLAN　入力 VLAN。パケットの入力元が指定した VLAN のときだけマッチする。省略時は ANY。DVLAN とは同時に指定できない

DVLAN　出力 VLAN。パケットの出力先が指定した VLAN のときだけマッチする。省略時は ANY。SVLAN とは同時に指定できない

ETHFORMAT　Ethernet のフレームフォーマット（エンキャプセレーション）。802.2（802.2 LLC）、ETHII（Ethernet Version 2）、NETWARERAW（Novell 802.3 raw）、SNAP（802.2 LLC + SNAP）から選択する。PROTOCOL パラメーターには、ここで指定したフレームタイプのプロトコル番号を指定する。 省略時は ANY。ETHII、802.2、SNAP を指定した場合は、PROTOCOL パラメーターも必須。ETHFORMAT と PROTOCOL パラメーターは、組み合わせによって入力できないもの（エラー

になるもの）と、コマンドは受け付けるが ASIC チップ上エラーとなり無効になるものがあるので注意。詳細は CREATE CLASSIFIER コマンドの表を参照のこと

PROTOCOL レイヤー 3 プロトコルタイプフィールド値。特殊なプロトコル名（IP、IPX、NONIPIPX、ANY。CREATE CLASSIFIER コマンドの表を参照）か、定義済みのプロトコル名（CREATE CLASSIFIER コマンドの表を参照）、または、16 進表記のプロトコル番号で指定する。プロトコル番号で指定する場合、802.2 なら 1 バイト（DSAP のみ）で、Ethernet Version 2 なら 2 バイトで、SNAP なら 5 バイトの 16 進数で指定する。ただし、SNAP の場合は下位 2 バイトしかパケットマッチングに使用されない（例：「xxxxxxABCD」を指定した場合、「ABCD」の部分だけがマッチングに使われる）。なお、定義済みのプロトコル名とプロトコル番号は、フレームフォーマット（ETHFORMAT）ごとに最大 3 個までしか使用できない。本パラメーターは、ETHFORMAT に ETHII、802.2、SNAP のいずれかを指定した場合は必須。

MACTYPE レイヤー 2 アドレス種別。L2UCAST（ユニキャスト）、L2MCAST（マルチキャスト）、L2BCAST（ブロードキャスト）、ANY（すべて）から選択する。本パラメーターは、ハードウェアパケットフィルターの DPORT パラメーターに ALL を指定したときだけ有効。省略時は ANY

IPSADDR 始点 IP アドレス。IP アドレス/マスク長の形式で指定する。マスク長を省略した場合は、32 ビットマスク（ホストアドレス）と見なされる。省略時は ANY

IPDADDR 終点 IP アドレス。IP アドレス/マスク長の形式で指定する。マスク長を省略した場合は、32 ビットマスク（ホストアドレス）と見なされる。省略時は ANY

IPDSCP IP ヘッダーの DSCP（DiffServ Code Point）フィールド値。有効範囲は 0〜63。IPTOS とは同時に指定できない。省略時は ANY

IPTOS IP ヘッダーの TOS 優先度（precedence）フィールド値。有効範囲は 0〜7。IPDSCP とは同時に指定できない。省略時は ANY

IPPROTOCOL IP ヘッダーのプロトコルタイプフィールド値。定義済みのプロトコル名（TCP、UDP、ICMP、IGMP、NONTCPUDP）か 10 進表記のプロトコル番号で指定する。本パラメーターに指定できるプロトコル番号は、システム全体で 29 種類まで（ただし、TCP、UDP、IGMP、NONTCPUDP、ANY は数えない）。なお、TCPSPORT、TCPDPORT パラメーターを使っている場合は、本パラメーターに TCP を指定したものと見なされる（他の値は指定できない）。また、UDPSPORT、UDPDPORT パラメーターを使っている場合は、本パラメーターに UDP を指定したものと見なされる（他の値は指定できない）。省略時は ANY

IPXDADDR 終点 IPX ネットワーク番号。省略時は ANY

IPXSSOCKET 始点 IPX ソケット。定義済みのソケット名か 16 進表記のソケット番号で指定する。本パラメーターに指定できるソケット番号は、システム全体で 7 種類まで（ANY は数えない）。省略時は ANY

IPXDSOCKET 終点 IPX ソケット。定義済みのソケット名か 16 進表記のソケット番号で指定する。本パラメーターに指定できるソケット番号は、システム全体で 7 種類まで（ANY は数えない）。省略時は ANY

TCPSPORT TCP 始点ポート。本パラメーターに指定できるポート番号は、システム全体で 15 種類まで。省略時は ANY

TCPDPORT TCP 終点ポート。本パラメーターに指定できるポート番号は、システム全体で 15 種類まで。省略時は ANY

UDPSPORT UDP 始点ポート。本パラメーターに指定できるポート番号は、システム全体で 15 種類まで。省略時は ANY

UDPDPORT　UDP 終点ポート。本パラメーターに指定できるポート番号は、システム全体で 15 種類まで。省略時は ANY

関連コマンド

CREATE CLASSIFIER（114 ページ）
DESTROY CLASSIFIER（147 ページ）
SHOW CLASSIFIER（230 ページ）

SET PORTAUTH PORT

カテゴリー：スイッチング / 802.1X 認証

```
SET PORTAUTH PORT={port-list|ALL} TYPE=AUTHENTICATOR
   [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]
SET PORTAUTH PORT={port-list|ALL} TYPE=BOTH
   [AUTHPERIOD=1..60] [CONTROL={AUTHORISED|UNAUTHORISED|AUTO}]
   [HELDPERIOD=0..65535] [MAXREQ=1..10] [MAXSTART=1..10]
   [QUIETPERIOD=0..65535] [REAUTHENABLED={TRUE|FALSE}] [REAUTHMAX=1..10]
   [REAUTHPERIOD=1..86400] [SERVERTIMEOUT=1..60] [STARTPERIOD=1..60]
   [SUPPTIMEOUT=1..60] [TXPERIOD=1..65535] [USERNAME=login-name
   PASSWORD=password [METHOD={OTP [ENCRYPTION={MD4|MD5}]|STANDARD}]]
SET
   PORTAUTH 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}]]
```

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）
login-name: ログイン名（1〜64 文字。英数字のみ使用可能）
password: パスワード（1〜64 文字。英数字のみ使用可能）

解説

指定ポートの 802.1X 認証設定を変更する。

パラメーター

PORT　スイッチポート。複数指定が可能。

TYPE　スイッチポートのタイプ（802.1X における役割）。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。

CONTROL　（Authenticator 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　（Authenticator ポート）Supplicant に対する EAPOL-Request パケットの最大再送回数。デフォルトは 2 回

QUIETPERIOD （Authenticator 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 EAPOL パケットをすべて破棄する。デフォルトは 60 秒。

REAUTHENABLED （Authenticator 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 （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 （Authenticator ポート）Supplicant の再認証間隔（秒）。デフォルトは 3600 秒。

SERVERTIMEOUT （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 （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 （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。

AUTHPERIOD （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 （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 （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、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 （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 （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 （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 （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 （Supplicant ポート）ワンタイムパスワードの生成アルゴリズム。MD4、MD5 から選択する。デフォルトは MD5。METHOD パラメーターに OTP を指定した場合の必須パラメーター。

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE（90 ページ）

ENABLE PORTAUTH（174 ページ）
ENABLE PORTAUTH PORT（178 ページ）
SET PORTAUTH PORT（207 ページ）
SHOW PORTAUTH（234 ページ）
SHOW PORTAUTH COUNTER（236 ページ）
SHOW PORTAUTH PORT（239 ページ）
SHOW PORTAUTH TIMER（244 ページ）

SET PORTAUTH USERNAME

カテゴリー：スイッチング / 802.1X 認証

SET PORTAUTH 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。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

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（90 ページ）
ENABLE PORTAUTH（174 ページ）
ENABLE PORTAUTH PORT（178 ページ）
SET PORTAUTH PORT（207 ページ）
SHOW PORTAUTH（234 ページ）

SHOW PORTAUTH COUNTER（236 ページ）
SHOW PORTAUTH PORT（239 ページ）
SHOW PORTAUTH TIMER（244 ページ）

SET QOS FLOWGROUP

カテゴリー：スイッチング / ポリシーベース QoS

SET QOS FLOWGROUP=*flow-list* [RED={*red-id*|NONE}] [MARKVALUE={*0..63*|NONE}]
[DESCRIPTION=*string*]

flow-list: フローグループ番号（0〜1023。ハイフン、カンマを使った複数指定も可能）
string: 文字列（1〜15 文字。空白を含む場合はダブルクォートで囲む）
red-id: RED カーブ番号（0〜47）

解説

フローグループの設定を変更する。

パラメーター

FLOWGROUP フローグループ番号
RED RED カーブ番号。トラフィッククラスの RED カーブよりも優先される
MARKVALUE IP ヘッダーの DSCP（DiffServ Code Point）フィールドに書き込む値。トラフィッククラスの MARKVALUE よりも優先される
DESCRIPTION フローグループの説明（メモとして使う）

関連コマンド

ADD QOS FLOWGROUP（93 ページ）
CREATE QOS FLOWGROUP（119 ページ）
DELETE QOS FLOWGROUP（132 ページ）
DESTROY QOS FLOWGROUP（148 ページ）
SHOW QOS FLOWGROUP（246 ページ）

SET QOS POLICY

カテゴリー：スイッチング / ポリシーベース QoS

SET QOS POLICY=*qos-list* [DESCRIPTION=*string*] [DTCPERCENT=*1..100*]

qos-list: QoS ポリシー番号（0〜255。ハイフン、カンマを使った複数指定も可能）
string: 文字列（1〜15 文字。空白を含む場合はダブルクォートで囲む）

解説

QoS ポリシーの設定を変更する。

パラメーター

POLICY　QoS ポリシー番号

DESCRIPTION　ポリシーの説明（メモとして使う）。POLICY パラメーターに複数の番号を指定した場合は、すべてのポリシーに同じメモ文字列が設定される

DTCPERCENT　本ポリシーのデフォルトトラフィッククラスに割り当てる帯域幅。スイッチポートの帯域幅に対する割合（%）で指定する。デフォルトトラフィッククラスには、本パラメーターで指定した割合の帯域が保証される。省略時は 20%

関連コマンド

ADD QOS POLICY（94 ページ）
CREATE QOS POLICY（120 ページ）
DELETE QOS POLICY（133 ページ）
DESTROY QOS POLICY（149 ページ）
SET QOS PORT（214 ページ）
SHOW QOS POLICY（248 ページ）

SET QOS PORT

カテゴリー：スイッチング / ポリシーベース QoS

SET QOS PORT={***port-list***|**ALL**} **POLICY=**{***qos-id***|**NONE**}

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）
qos-id: QoS ポリシー番号（0〜255）

解説

スイッチポートに QoS ポリシーを割り当てる。

パラメーター

PORT　スイッチポート番号
POLICY　QoS ポリシー番号

関連コマンド

SHOW QOS POLICY（248 ページ）

SET QOS RED

カテゴリー：スイッチング / ポリシーベース QoS

SET QOS RED=*red-id* [START=*0..100*] [STOP=*0..100*] [DROPPROB=*0..100*]
[DESCRIPTION=*string*]

red-id: RED カーブ番号（5〜47）
string: 文字列（1〜15 文字。空白を含む場合はダブルクォートで囲む）

解説

RED（Random Early Detection / Discard）カーブの設定を変更する。

パラメーター

RED RED カーブ番号。0〜4 は定義済みの RED カーブが使っているため指定できない
START パケットを破棄し始めるポイント。トラフィッククラスの最大帯域幅に対する仮想キュー長の割合（パーセンテージ）で指定する。仮想キュー長がこのポイントを超えると、徐々にパケットの破棄率が高くなり、STOP に達したときに破棄率が DROPPROB%となる。
STOP パケットを完全に破棄し始めるポイント。トラフィッククラスの最大帯域幅に対する仮想キュー長の割合（パーセンテージ）で指定する。仮想キュー長がこのポイントを超えると、すべてのパケットが破棄されるようになる。
DROPPROB 仮想キュー長が STOP のときのパケット破棄率
DESCRIPTION RED カーブの説明（メモとして使う）

関連コマンド

CREATE QOS RED（122 ページ）
DESTROY QOS RED（150 ページ）
SHOW QOS RED（250 ページ）

SET QOS TRAFFICCLASS

カテゴリー：スイッチング / ポリシーベース QoS

SET QOS TRAFFICCLASS=*tc-list* [MINBANDWIDTH=*bandwidth*]
[MAXBANDWIDTH=*bandwidth*] [WEIGHT=*weight*] [RED={*red-id*|NONE}]
[MARKVALUE={*0..63*|NONE}] [NUMHASHEDFLOWS={NONE|*1*|*2*|*8*|*32*|*64*|*128*|*256*|*512*}]
[FAIRHASHLIMIT={LOW|MODLOW|MODHIGH|HIGH}] [DESCRIPTION=*string*]

tc-list: トラフィッククラス番号（0〜511。ハイフン、カンマを使った複数指定も可能）
bandwidth: 帯域幅（0〜16000000Kbps）
weight: 帯域配分用の重み付け値
red-id: RED カーブ番号（0〜47）
string: 文字列（1〜15 文字。空白を含む場合はダブルクォートで囲む）

解説

トラフィッククラスの設定を変更する。

パラメーター

TRAFFICCLASS　トラフィッククラス番号

MINBANDWIDTH　トラフィッククラスに割り当てる最小帯域幅（Kbps）。該当クラスには、ここで指定した帯域が確保される。この値は、パケットをスイッチ内部のキューから送り出すときのレートを示す。数値だけで指定する場合の単位は Kbps。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「× 1」、「× 1000」、「× 1000000」の意味になる。有効範囲は Kbps 換算で 0〜16000000。ただし、指定値が 64Kbps の倍数でない場合は切り捨てが行われる（63Kbps を指定した場合は 0Kbps となる）。0 は帯域ゼロの意味。「M」、「G」を指定する場合は、「2.256G」や「128.4M」のように小数を指定することもできる（小数点以下は 3 桁目まで有効）。省略時は 64Kbps

MAXBANDWIDTH　トラフィッククラスに割り当てる最大帯域幅（Kbps）。該当クラスに割り当てる帯域は、ここで指定した値までに制限される。この値は、パケットをスイッチ内部のキューから送り出すときのレートを示す。数値だけで指定する場合の単位は Kbps。ただし、数値のあとに「K」、「M」、「G」をつけると、それぞれ「× 1」、「× 1000」、「× 1000000」の意味になる。有効範囲は Kbps 換算で 0〜16000000。ただし、指定値が 64Kbps の倍数でない場合は切り捨てが行われる（63Kbps を指定した場合は 0Kbps となる）。0 は帯域ゼロの意味。「M」、「G」を指定する場合は、「2.256G」や「128.4M」のように小数を指定することもできる（小数点以下は 3 桁目まで有効）。省略時は 16Gbps

WEIGHT　同一 QoS ポリシー所属のトラフィッククラス間で帯域を配分するときに用いる重み付け値。この値が小さいほど多くの帯域が割り当てられる。有効な値は、1、2、3、4、5、6、7、8、10、12、14、16、20、24、28、32、40、48、56、64、80、96、112、128、160、192、224、256、320、384、448、512、640、768、896、1024。WEIGHT と配分される帯域の関係については解説編を参照のこと。省略時は 1

RED　本トラフィッククラスに適用する RED（Random Early Detection / Discard）カーブの番号。NONE は RED アルゴリズムを使用せずに、帯域オーバー分を単純に破棄するアルゴリズムを使用すること

を示す。省略時は NONE

MARKVALUE　IP ヘッダーの DSCP（DiffServ Code Point）フィールドに書き込む値。NONE は値を書き換えないことを示す。省略時は NONE

NUMHASHEDFLOWS　同一トラフィックグループ所属のフローグループ間で、どの程度均等に帯域を配分するかを指定するパラメーター（FAIRHASHLIMIT も参照）。フローグループはハッシュアルゴリズムによって NUMHASHEDFLOWS 個のグループ（Hashed Flowgroup）にハッシュ（分類）され、グループごとに帯域が配分される。本パラメーターの値が大きいほど、フローグループ間で帯域が均等に配分される。NONE を指定した場合は、フローグループ間での帯域均等配分は行われない。省略時は NONE

FAIRHASHLIMIT　同一トラフィックグループ所属のフローグループ間で、どの程度均等に帯域を配分するかを指定するパラメーター（NUMHASHEDFLOWS も参照）。LOW、MODLOW、MODHIGH、HIGH の順に均等さが増す（HIGH がもっとも均等）。省略時は MODHIGH

DESCRIPTION　トラフィッククラスの説明（メモとして使う）。TRAFFICCLASS パラメーターに複数の番号を指定した場合は、すべてのトラフィッククラスに同じメモ文字列が設定される

関連コマンド

ADD QOS TRAFFICCLASS（95 ページ）
CREATE QOS TRAFFICCLASS（124 ページ）
DESTROY QOS TRAFFICCLASS（151 ページ）
SHOW QOS TRAFFICCLASS（252 ページ）

SET QOS VLANREMAP

カテゴリー：スイッチング / ポリシーベース QoS

SET QOS VLANREMAP=*p0*,p1,*p2*,p3,*p4*,p5,*p6*,p7

p0*〜*7: 受信パケットのユーザープライオリティー 0〜7 に対応する送信時のユーザープライオリティー（0〜7）

解説

802.1p タグプライオリティー書き換え機能のマッピング設定を変更する。
具体的には、受信時のユーザープライオリティーと送信時のユーザープライオリティーのマッピングを行う。
デフォルトでは、受信時と送信時でプライオリティーが同じになるような設定になっている（タグを書き換えない）。
タグプライオリティー書き換え機能はデフォルト無効なので、別途 ENABLE QOS VLANPRIORITYREMAPPING コマンドで有効にする必要がある。

パラメーター

VLANREMAP　受信パケットのユーザープライオリティー 0〜7 に対応する送信時のユーザープライオリティー値をカンマ区切りで指定する。デフォルトは 0,1,2,3,4,5,6,7、すなわちプライオリティーを書き換えない設定。

備考・注意事項

タグなしの受信パケットは、送出パケットがタグつきであっても、常にプライオリティー 0 で送出される。

関連コマンド

DISABLE QOS VLANPRIORITYREMAPPING（159 ページ）
ENABLE QOS VLANPRIORITYREMAPPING（182 ページ）
SHOW QOS VLANPRIORITYREMAPPING（254 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

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、ディスカーディ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。

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）。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（199 ページ）
RESET STP（201 ページ）
SET STP PORT（221 ページ）
SHOW STP（255 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

SET STP PORT={***port-list***|**ALL**} [PATHCOST={*1..1000000*|*1..200000000*}]
[PORTPRIORITY=*0..255*] [EDGEPORT={YES|NO}] [PTP={AUTO|YES|NO}] [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）

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

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 19: 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 20: 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

関連コマンド

PURGE STP（199 ページ）
RESET STP（201 ページ）
SET STP（219 ページ）
SHOW STP（255 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ーは削除される。デフォルトは 300 秒。

関連コマンド

DISABLE SWITCH AGEINGTIMER（164 ページ）
ENABLE SWITCH AGEINGTIMER（187 ページ）
SHOW SWITCH（263 ページ）

SET SWITCH MIRROR

カテゴリー：スイッチング / ポート

SET SWITCH MIRROR={**NONE**|***port-number***}

port-number: スイッチポート番号（1〜）

解説

ミラーポートの設定および解除を行う。
ソースポートと対象トラフィックは、SET SWITCH PORT コマンドの MIRROR パラメーターで指定する。

パラメーター

MIRROR　ミラーポートとして使用するポートを指定する。VLAN default 以外に所属しているポートはミラーポートに設定できない。また、トランクポートも不可。本コマンド実行時に別のポートがミラーポートとして設定されていた場合、先に設定されていたポートはミラーポートでなくなり、VLAN default 所属のタグなしポートとなる。ミラーポートになったポートは、どの VLAN にも所属しない。ミラーポートを削除するには NONE を指定する。

備考・注意事項

ミラーポートとして設定されたポートは通常のスイッチポートとしては機能しない。また、ポートトランキングの所属ポートをミラーポートに設定することはできない。

関連コマンド

DISABLE SWITCH MIRROR（168 ページ）
ENABLE SWITCH MIRROR（191 ページ）
SET SWITCH PORT（225 ページ）
SHOW SWITCH（263 ページ）
SHOW SWITCH PORT（276 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}]
   [DESCRIPTION=string] [EGRESSLIMIT={NONE|0..16000063}]
   [INTRUSIONACTION={DISABLE|DISCARD|TRAP}] [LEARN={0|1..256] [RELEARN={ON|
   OFF}] [MIRROR={NONE|RX}] [MODE={AUTONEGOTIATE|MASTER|SLAVE}]
   [SPEED={AUTONEGOTIATE|10MHALF|10MFULL|100MHALF|100MFULL|1000MFULL}]
```

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）
string: 文字列（1〜47 文字）

解説

スイッチポートの各種設定を行う。

パラメーター

PORT　ポート番号。複数指定が可能。ALL を指定した場合はすべてのポートが対象となる。

ACCEPTABLE　受信可能なフレームタイプ。VLAN（VLAN タグ付きフレームのみ。VID=0 のプライオリティータグフレームは破棄）か ALL（すべて）から選択する。タグなし VLAN 所属ポートのデフォルトは ALL。タグ VLAN にしか所属していないポートでは、自動的に本パラメーターが VLAN に設定され変更できない。

DESCRIPTION　ポート名称。SHOW SWITCH PORT コマンドなどで表示されるもので、メモ的に使用する。

EGRESSLIMIT　該当ポートの送信レート上限値(帯域制限機能)。指定可能な値の範囲は 0〜16000063Kbps。ただし、指定値が 64 の倍数でない場合は切り捨てが行われる（63 を指定した場合は 0 となる)。NONE および 0 は帯域を制限しないの意味になる。EGRESSLIMIT の値は、パケットをスイッチ内部のキューから送り出すときのデータレートであり、フレームヘッダーやトレーラーは含まない。デフォルトは NONE。本機能はポリシーベース QoS の帯域制御機能とは併用できない。

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ーをオフにする)。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ーオフ）

RELEARN　ポートセキュリティーの動作モード。OFF を指定した場合、ポートセキュリティーエントリー（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ー)。本パラメーターは、ポートセキュリティーが有効でないとき（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 アドレスを持つパケットを、LEARN パラメーターで指定した制限値を超えて受信した場合のアクション。DISCARD（受信パケットを破棄する)、TRAP（受

信パケットを破棄した後、SNMP トラップを送信する。トラップは 1 秒単位で送信)、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。

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。RX（受信パケット)、NONE（ミラーリングしない）から選択する。デフォルトは NONE。送信パケットのミラーリングはサポート対象外。

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（別表を参照)。トランクグループ所属ポートに対して本コマンドで SPEED オプションを変更した場合、ポートレベルの設定値は変更されるが、実際の値はトランクグループ全体の設定値のまま変化しない。同ポートをトランクグループから除外した時点で設定値が有効になる。デフォルトは AUTONEGOTIATE（オートネゴシエーション)。なお、1000BASE-T ポートの MDI / MDI-X 自動切替は、オートネゴシエーションが有効のときだけ使用可能。

AUTONEGOTIATE	オートネゴシエーション
10MHALF	10M Half Duplex 固定
10MFULL	10M Full Duplex 固定
100MHALF	100M Half Duplex 固定
100MFULL	100M Full Duplex 固定
1000MFULL	1000M Full Duplex 固定（ただし、1000BASE-T インターフェースの場合は、オートネゴシエーションで 1000M Full Duplex を通知するという動作になる）

表 21: SPEED パラメーターの設定

備考・注意事項

スイッチポートの帯域制限機能（EGRESSLIMIT）とポリシーベース QoS の帯域制御機能は併用できない。どちらか一方だけを使うこと

関連コマンド

DISABLE SWITCH PORT（169 ページ）
ENABLE SWITCH PORT（192 ページ）
SHOW SWITCH PORT（276 ページ）

SET SWITCH TRUNK

カテゴリー：スイッチング / ポート

SET SWITCH TRUNK=*trunk* [SPEED={10M|100M|1000M}]

trunk: トランクグループ名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。大文字小文字を区別しない）

解説

トランクグループの設定を変更する。

パラメーター

TRUNK　トランクグループ名

SPEED　トランクポートの通信速度。トランクグループに参加したポートは、ここで指定した速度のオートネゴシエーション（AUTONEGOTIATE）となる

関連コマンド

ADD SWITCH TRUNK（102 ページ）
CREATE SWITCH TRUNK（127 ページ）
DELETE SWITCH TRUNK（139 ページ）
DESTROY SWITCH TRUNK（153 ページ）
SHOW SWITCH TRUNK（284 ページ）

SET VLAN

カテゴリー：スイッチング / バーチャル LAN

SET VLAN={***vlanname***|***1..4090***} [BCLIMIT={NONE|*count*}] [MCLIMIT={NONE|*count*}]

vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。大文字小文字を区別しない）
count: 個数（16〜1048560）

解説

パケットストームプロテクションの設定を行う。

パラメーター

VLAN　VLAN 名または VLAN ID

BCLIMIT　ブロードキャストパケットの送信レート上限値。1 秒間に送信する L2 ブロードキャストパケットの最大数を指定する。上限を超えたパケットは送信されずに破棄される。NONE を指定した場合は制限なしとなる。デフォルトは NONE。

MCLIMIT　マルチキャストパケットの送信レート上限値。1 秒間に送信する L2 マルチキャストパケットの最大数を指定する。上限を超えたパケットは送信されずに破棄される。NONE を指定した場合は制限なしとなる。デフォルトは NONE。

備考・注意事項

BCLIMIT、MCLIMIT パラメーターの指定値は、内部的には 16 の倍数になるよう切り捨てられる。

関連コマンド

DISABLE VLAN STORMPROTECT（173 ページ）
ENABLE VLAN STORMPROTECT（196 ページ）
SHOW VLAN（285 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..4090***} **PORT=**{***port-list***|**ALL**} **FRAME=**{**UNTAGGED**|**TAGGED**}

vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。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　該当 VLAN のタグ設定。TAGGED（タグ付き）、UNTAGGED（タグなし）から選択する。

関連コマンド

ADD VLAN PORT（107 ページ）
DELETE VLAN PORT（142 ページ）
SHOW VLAN（285 ページ）

SHOW CLASSIFIER

カテゴリー：スイッチング / クラシファイア

SHOW CLASSIFIER[={*rule-list*|ALL}] [SVLAN={*vlanname*|*1..4090*|ANY}]
[DVLAN={*vlanname*|*1..4090*|ANY}] [ETHFORMAT={*802.2*|ETHII|NETWARERAW|SNAP|ANY}] [PROTOCOL={*protocoltype*|IP|IPX|NONIPIPX|ANY}] [MACTYPE={L2UCAST|L2MCAST|L2BCAST|ANY}] [IPSADDR={*ipadd*/masklen|ANY}]
[IPDADDR={*ipadd*/masklen|ANY}] [IPDSCP={*0..63*|ANY}] [IPTOS={*0..7*|ANY}]
[IPPROTOCOL={TCP|UDP|ICMP|IGMP|*protocol*|ANY}] [IPXDADDR={*ipxnet*|ANY}]
[IPXSSOCKET={NCP|SAP|RIP|NNB|DIAG|NLSP|IPXWAN|*socket*|ANY}]
[IPXDSOCKET={NCP|SAP|RIP|NNB|DIAG|NLSP|IPXWAN|*socket*|ANY}]
[TCPSPORT={*port*|ANY}] [TCPDPORT={*port*|ANY}] [UDPSPORT={*port*|ANY}]
[UDPDPORT={*port*|ANY}]

rule-list: クラシファイア番号（1〜9999。ハイフン、カンマを使った複数指定も可能）
vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。大文字小文字を区別しない）
protocoltype: L3 プロトコル番号（16 進数）
ipadd: IP アドレス
masklen: マスク長（0〜32）
protocol: IP プロトコル番号（0〜255）
ipxnet: IPX ネットワーク番号（32 ビット長。16 進数最大 8 文字。先頭の 0 は省略可能）
socket: IPX ソケット番号（16 ビット長。16 進数最大 4 文字）
port: TCP / UDP ポート番号（0〜65535）

解説

クラシファイア（汎用パケットフィルター）の設定内容を表示する。

パラメーター

CLASSIFIER　クラシファイア番号。番号を指定した場合は該当するクラシファイアのパラメーターがすべて表示される。ALL を指定した場合はすべてのクラシファイアのパラメーターが表示される。値を指定しなかった場合は、クラシファイアの一覧が簡潔に表示される。本パラメーターになんらかの値を指定した場合は、以下の各パラメーターを使って表示するクラシファイアの絞り込みが可能。本パラメーターに値を指定しなかった場合は、以下の各パラメーターは無効

SVLAN　入力 VLAN

DVLAN　出力 VLAN

ETHFORMAT　Ethernet のフレームフォーマット（エンキャプセレーション）

PROTOCOL　レイヤー 3 プロトコルタイプフィールド値

MACTYPE　レイヤー 2 アドレス種別

IPSADDR　始点 IP アドレス

IPDADDR　終点 IP アドレス

IPDSCP IP ヘッダーの DSCP（DiffServ Code Point）フィールド値
IPTOS IP ヘッダーの TOS 優先度（precedence）フィールド値
IPPROTOCOL IP ヘッダーのプロトコルタイプフィールド値
IPXDADDR 終点 IPX ネットワーク番号
IPXSSOCKET 始点 IPX ソケット
IPXDSOCKET 終点 IPX ソケット
TCPSPORT TCP 始点ポート
TCPDPORT TCP 終点ポート
UDPSPORT UDP 始点ポート
UDPDPORT UDP 終点ポート

入力・出力・画面例

```
Manager > show classifier

 Classifier General Info
--------------------------------------------------------------------------------
 Total number of rules .... 7

 Rule ..................... 1
   Related module(s) ...... None

 Rule ..................... 101
   Related module(s) ...... L3 switch
                            QOS

 Rule ..................... 102
   Related module(s) ...... QOS

 Rule ..................... 103
   Related module(s) ...... L3 switch

 Rule ..................... 104
   Related module(s) ...... L3 switch

 Rule ..................... 105
   Related module(s) ...... L3 switch

 Rule ..................... 106
   Related module(s) ...... QOS

--------------------------------------------------------------------------------

Manager > show classifier=103

 Classifier Rules
--------------------------------------------------------------------------------
 Rule .................. 103
```

```
  S-VLAN ............... ANY
  D-VLAN ............... ANY
  M-Type ............... ANY
  E-Format ............. ANY
  Protocol ............. IP
  S-IP Address ......... ANY
  D-IP Address ......... ANY
  IP Protocol .......... TCP
  TOS/DSCP ............. ANY
  S-TCP Port ........... 22
  D-TCP Port ........... ANY

------------------------------------------------------------------------------
```

Total number of rules	クラシファイアの総数
Rule	クラシファイア番号
Related module(s)	クラシファイアを使用している上位モジュール。L3 switch（ハードウェアパケットフィルター）か QOS（ポリシーベース QoS）

表 22: パラメーター無指定時

Rule	クラシファイア番号
S-VLAN	入力 VLAN。カッコ内は VLAN ID
D-VLAN	出力 VLAN。カッコ内は VLAN ID
M-Type	レイヤー 2 アドレス種別
E-Format	レイヤー 2 フレームタイプ（エンキャプセレーション）
Protocol	プロトコルタイプ。カッコ内は定義済みのプロトコル名
S-IP Address	始点 IP アドレス/マスク
D-IP Address	終点 IP アドレス/マスク
IP Protocol	IP プロトコルタイプ
TOS/DSCP	TOS または DSCP 値
S-TCP Port	TCP 始点ポート
D-TCP Port	TCP 終点ポート
S-UDP Port	UDP 始点ポート
D-UDP Port	UDP 終点ポート
D-IPX Address	終点 IPX ネットワーク番号
D-IPX Socket	終点 IPX ソケット
S-IPX Socket	始点 IPX ソケット

表 23: CLASSIFIER パラメーター指定時（表示項目はクラシファイアの設定により異なる）

例

■クラシファイアの一覧を表示する。

```
SHOW CLASSIFIER
```

■IP プロトコルとして UDP を含むクラシファイアの詳細を表示する。

```
SHOW CLASSIFIER=ALL IPPROTOCOL=UDP
```

関連コマンド

CREATE CLASSIFIER（114 ページ）
DESTROY CLASSIFIER（147 ページ）
SET CLASSIFIER（204 ページ）

SHOW PORTAUTH

カテゴリー：スイッチング / 802.1X 認証

SHOW PORTAUTH

解説

802.1X 認証モジュールの全般的な設定と状態を表示する。

入力・出力・画面例

```
Manager > show portauth

802.1X System
-------------------------------------------------------------------------------
  SystemAuthControl............ ENABLED
  Global Username.............. portAuthPortAuth
  Global Password.............. portAuthPortAuth
  Global Encryption Method..... Standard


  Port                PAE Capabilities                Protocol Version

  port1               None                            1
  port2               None                            1
  port3               None                            1
  port4               None                            1
  port5               Authenticator                   1
  port6               None                            1
  port7               None                            1
  port8               None                            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
```

SystemAuthControl	802.1X 認証モジュールの有効・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
Port	スイッチポートのインターフェース名
PAE Capabilities	スイッチポートのタイプ（802.1X における役割）。Authenticator、Supplicant、Both、None のいずれか
Protocol Version	EAPOL プロトコルバージョン

表 24:

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE（90 ページ）
ENABLE PORTAUTH（174 ページ）
ENABLE PORTAUTH PORT（178 ページ）
SET PORTAUTH PORT（207 ページ）
SHOW PORTAUTH（234 ページ）
SHOW PORTAUTH COUNTER（236 ページ）
SHOW PORTAUTH PORT（239 ページ）
SHOW PORTAUTH TIMER（244 ページ）

SHOW PORTAUTH COUNTER

カテゴリー：スイッチング / 802.1X 認証

SHOW PORTAUTH 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

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	スイッチポートのタイプ（802.1X における役割）。Authenticator、Supplicant、Both のいずれか
	Authenticator としての設定
Last EAPOL Frame Version	
Last EAPOL Frame Source	
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 25:

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE（90 ページ）
ENABLE PORTAUTH（174 ページ）
ENABLE PORTAUTH PORT（178 ページ）
SET PORTAUTH PORT（207 ページ）
SHOW PORTAUTH（234 ページ）
SHOW PORTAUTH COUNTER（236 ページ）
SHOW PORTAUTH PORT（239 ページ）
SHOW PORTAUTH TIMER（244 ページ）

SHOW PORTAUTH PORT

カテゴリー：スイッチング / 802.1X 認証

SHOW PORTAUTH 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 設定を表示する。

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 portauth port=5

802.1X Configuration
--------------------------------------------------------------------------------
Interface: port5
  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 (not supported)
          keyTransmissionEnabled........ False (not supported)
          adminControlledDirections..... Both (not supported)

Manager > show portauth port=7

802.1X Configuration
--------------------------------------------------------------------------------
Interface: port7
  PAE Type.............. Both
```

```
Multi-Supplicant Authenticator
  Default Settings
        AuthControlPortControl........ Auto
        quietPeriod................... 60
        txPeriod...................... 30
        suppTimeout................... 30
        serverTimeout................. 30
        maxReq........................ 2
        reAuthMax..................... 2
        reAuthPeriod.................. 3600
        reAuthEnabled................. False

  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)

  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.................. 3600
        reAuthEnabled................. False
        keyTransmissionEnabled........ False (not supported)
        operControlledDirections...... False (not supported)

Supplicant
        heldPeriod.................... 60
        authPeriod.................... 30
        startPeriod................... 30
        maxStart...................... 3
```

```
        Supplicant PAE State.......... CONNECTING
```

Interface	スイッチポートのインターフェース名
PAE Type	スイッチポートのタイプ（802.1X における役割）。Authenticator、Supplicant、Both のいずれか
	Authenticator としての設定
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	802.1X におけるポートの状態。unauthorised（未認証）か authorised（認証済み）
Backend Authenticator State	認証機構の状態。IDLE（アイドル）、INITIALISE（初期化）、RESPONSE（Supplicant から応答受信）、REQUEST（認証サーバーに要求送信）、SUCCESS（認証成功）、FAIL（認証失敗）、TIMEOUT（タイムアウト）のいずれか
AuthControlPortControl	手動設定によるポート状態。Auto（認証結果に応じて変動。通常の設定）、forceUnauthorised（未認証に固定）、forceAuthorised（認証済みに固定）のいずれか
quietPeriod	認証失敗後、Supplicant との通信を拒否する期間（秒）
txPeriod	Supplicant に EAPOL パケットを再送信する間隔（秒）
suppTimeout	Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間（秒）
serverTimeout	RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間（秒）
maxReq	Supplicant に対する EAPOL-Request パケットの最大再送回数
reAuthMax	再認証時における EAPOL-Request パケットの最大再送回数
reAuthPeriod	Supplicant を再認証する間隔（秒）
reAuthEnabled	再認証の有効・無効
piggyBack	未サポート
keyTransmissionEnabled	未サポート
adminControlledDirections	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、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 26:

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE（90 ページ）
ENABLE PORTAUTH（174 ページ）
ENABLE PORTAUTH PORT（178 ページ）
SET PORTAUTH PORT（207 ページ）
SHOW PORTAUTH（234 ページ）
SHOW PORTAUTH COUNTER（236 ページ）
SHOW PORTAUTH PORT（239 ページ）
SHOW PORTAUTH TIMER（244 ページ）

SHOW PORTAUTH TIMER

カテゴリー：スイッチング / 802.1X 認証

SHOW PORTAUTH 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、802.1X 認証機能の各種タイマー（残り時間）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 portauth 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 timer port=7
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
```

Interface	スイッチポートのインターフェース名
PAE Type	スイッチポートのタイプ（802.1X における役割）。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）。TX-PERIOD 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 27:

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE（90 ページ）
ENABLE PORTAUTH（174 ページ）
ENABLE PORTAUTH PORT（178 ページ）
SET PORTAUTH PORT（207 ページ）
SHOW PORTAUTH（234 ページ）
SHOW PORTAUTH COUNTER（236 ページ）
SHOW PORTAUTH PORT（239 ページ）
SHOW PORTAUTH TIMER（244 ページ）

SHOW QOS FLOWGROUP

カテゴリー：スイッチング / ポリシーベース QoS

SHOW QOS FLOWGROUP[={*flow-id*|ALL}]

flow-id: フローグループ番号（0〜1023）

解説

フローグループの設定内容を表示する。

パラメーター

FLOWGROUP　フローグループ番号

入力・出力・画面例

```
Manager > show qos flowgroup

Flow Group Information
 Id    Description     Assigned TC   Classifiers
--------------------------------------------------------------------------------
 1     to/from host200 1             1-2
 2     others          2             3

Manager > show qos flowgroup=1

Identifier ................ 1
Description ............... to/from host200
TC Assigned to ............ 1
Classifiers ............... 1-2
Priority .................. None
Red Curve ................. None
Mark Value ................ None
```

Id	フローグループ番号
Description	説明（メモ）
Assigned TC	割り当て先のトラフィッククラス
Classifiers	割り当てられているクラシファイア

表 28: 番号省略時

Identifier	フローグループ番号
Description	説明（メモ）
TC Assigned to	割り当て先のトラフィッククラス
Classifiers	割り当てられているクラシファイア
Priority	優先度（未サポート）
Red Curve	RED カーブ番号
Mark Value	DSCP フィールドに書き込む値

表 29: 番号指定時

関連コマンド

ADD QOS FLOWGROUP（93 ページ）
CREATE QOS FLOWGROUP（119 ページ）
DELETE QOS FLOWGROUP（132 ページ）
DESTROY QOS FLOWGROUP（148 ページ）
SET QOS FLOWGROUP（212 ページ）

SHOW QOS POLICY

カテゴリー：スイッチング / ポリシーベース QoS

SHOW QOS POLICY[={*qos-id*|ALL}]

qos-id: QoS ポリシー番号（0〜255）

解説

QoS ポリシーの設定内容を表示する。

パラメーター

POLICY　QoS ポリシー番号

入力・出力・画面例

```
Manager > show qos policy

QOS Policy Information
 Id    Description     Trafficclasses      Ports Assigned to
 ------------------------------------------------------------------------------
 1     Host-based      1-2                 Port: 1-4
 2     App-based       None                None
 3     Proto-based     None                None

Manager > show qos policy=1

Identifier ................ 1
Description ............... Host-based
TCs Assigned .............. 1-2
Port Assigned to .......... 1-4
Default Traffic Class
   Percent ................ 20
```

Id	QoS ポリシー番号
Description	説明（メモ）
Trafficclasses	割り当てられているトラフィッククラス
Ports Assigned to	割り当て先のスイッチポート

表 30: 番号省略時

Identifier	QoS ポリシー番号
Description	説明（メモ）
TCs Assigned	割り当てられているトラフィッククラス
Port Assigned to	割り当て先のスイッチポート
Percent	デフォルトトラフィッククラスに割り当てる帯域（ポート帯域に対するパーセンテージ）

表 31: 番号指定時

関連コマンド

ADD QOS POLICY（94 ページ）
CREATE QOS POLICY（120 ページ）
DELETE QOS POLICY（133 ページ）
DESTROY QOS POLICY（149 ページ）
SET QOS POLICY（213 ページ）
SET QOS PORT（214 ページ）

SHOW QOS RED

カテゴリー：スイッチング / ポリシーベース QoS

SHOW QOS RED[={*red-id*|ALL}]

red-id: RED カーブ番号（0〜47）

解説

RED（Random Early Detection / Discard）カーブの設定内容を表示する。

パラメーター

RED RED カーブ番号。指定した場合は該当 RED カーブの詳細設定を表示する。番号を指定しなかった場合は、RED カーブの一覧を表示する。

入力・出力・画面例

```
Manager > show qos red

Random Early Detection Information
 Id   Description     Assigned TCs        Assigned Flow Groups
------------------------------------------------------------------------------
 0    Aggressive      None                None
 1    Med-Aggressive  None                None
 2    Medium          None                None
 3    Med-Passive     None                None
 4    Passive         1                   None
 10   Very Aggressive None                None

Manager > show qos red=4

Identifier ............... 4
Description ............... Passive
TCs Assigned to ........... 1
FlowGroups Assigned to .... None
Start ..................... 55
Stop ...................... 95
Drop Probability .......... 100
```

Id	RED カーブ番号
Description	説明（メモ）
Assigned TCs	割り当て先のトラフィッククラス

Assigned Flow Groups	割り当て先のフローグループ

表 32: 番号省略時

Identifier	RED カーブ番号
Description	説明（メモ）
TCs Assigned to	割り当て先のトラフィッククラス
FlowGroups Assigned to	割り当て先のフローグループ
Start	パケットを破棄しはじめるポイント。最大帯域に対する仮想キュー長の割合（%）で表す
Stop	パケットを完全に破棄するポイント。最大帯域に対する仮想キュー長の割合（%）で表す
Drop Probability	仮想キュー長が Stop%のときのパケット破棄率（%）

表 33: 番号指定時

関連コマンド

CREATE QOS RED（122 ページ）
DESTROY QOS RED（150 ページ）
SET QOS RED（215 ページ）

SHOW QOS TRAFFICCLASS

カテゴリー：スイッチング / ポリシーベース QoS

SHOW QOS TRAFFICCLASS[={*tc-id*|ALL}]

tc-id: トラフィッククラス番号（0〜511）

解説

トラフィッククラスの設定内容を表示する。

パラメーター

TRAFFICCLASS　トラフィッククラス番号

入力・出力・画面例

```
Manager > show qos trafficclass

QOS Traffic Class Information
 Id    Description      Policy   FlowGroups
-------------------------------------------------------------------------------
 1     MAX 128Kbps      1        1
 2     MAX 256Kbps      1        2

Manager > show qos trafficclass=1

Identifier ................ 1
Description ............... MAX 128Kbps
Policy Assigned to ........ 1
Flow Groups ............... 1
Min Bandwidth ............. 0.000kbps
Max Bandwidth ............. 128.000kbps
Weight .................... 1
Priority .................. None
Red Curve ................. None
Mark Value ................ None
Stats ..................... ACCEPT
Num Hashed Flows .......... None
Fair Hash Limit ........... MODHIGH
```

Id	トラフィッククラス番号
Description	説明（メモ）

Policy	割り当て先の QoS ポリシー
FlowGroups	割り当てられているフローグループ

表 34: 番号省略時

Identifier	トラフィッククラス番号
Description	説明（メモ）
Policy Assigned to	割り当て先の QoS ポリシー
Flow Groups	割り当てられているフローグループ
Min Bandwidth	最小帯域
Max Bandwidth	最大帯域
Weight	重み付け値
Priority	優先度（未サポート）
Red Curve	RED カーブ
Mark Value	DSCP フィールドに書き込む値
Num Hashed Flows	フローグループをいくつにハッシュするか
Fair Hash Limit	フローグループ間での帯域配分をどのくらい均等にするか

表 35: 番号指定時

関連コマンド

ADD QOS TRAFFICCLASS（95 ページ）
CREATE QOS TRAFFICCLASS（124 ページ）
DELETE QOS TRAFFICCLASS（134 ページ）
DESTROY QOS TRAFFICCLASS（151 ページ）
SET QOS TRAFFICCLASS（216 ページ）

SHOW QOS VLANPRIORITYREMAPPING

カテゴリー：スイッチング / ポリシーベース QoS

SHOW QOS VLANPRIORITYREMAPPING

解説

802.1p タグプライオリティー書き換え機能の設定を表示する。

入力・出力・画面例

```
Manager > show qos vlanprioritymapping

QOS VLAN Tag User Priority Remapping
--------------------------------------------------------------------------------
VLAN Tag User Priority Remapping .......... ENABLED
 ------------------------------------------------------------------------------
VLAN Priority Remap

 In VTUP   |   Out VTUP
 ----------------------
     0     |     0
     1     |     1
     2     |     2
     3     |     3
     4     |     4
     5     |     5
     6     |     6
     7     |     7
--------------------------------------------------------------------------------
```

VLAN Tag User Priority Remapping	802.1p タグプライオリティー書き換え機能の有効（ENABLED）・無効（DISABLED）
In VTUP	受信パケットの VLAN タグユーザープライオリティー値
Out VTUP	書き換え後の VLAN タグユーザープライオリティー値

表 36:

関連コマンド

DISABLE QOS VLANPRIORITYREMAPPING（159 ページ）
ENABLE QOS VLANPRIORITYREMAPPING（182 ページ）
SET QOS VLANREMAP（218 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

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
 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
 Designated Root ....... 32768 : 00-90-99-40-4f-00
 Root Port ............. (n/a)
 Root Path Cost ........ 0
 Max Age ............... 20
 Hello Time ............ 2
 Forward Delay ......... 15
 Switch Max Age ........ 20
 Switch Hello Time ..... 2
 Switch Forward Delay .. 15
 Hold Time ............. 1

--------------------------------------------------------------------------------
```

```
Manager > show stp summary

 STP Name          Mode       Ports Enabled   Ports Disabled   Bridge Role
-------------------------------------------------------------------------
 default           Standard             22                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。かっこ内は 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ーと MAC アドレスで構成される
Bridge Priority	ブリッジプライオリティー
Designated Root	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
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。

表 37:

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 38: SUMMARY オプション指定時

関連コマンド

CREATE STP（126 ページ）
DESTROY STP（152 ページ）
DISABLE STP（160 ページ）
ENABLE STP（183 ページ）
SET STP（219 ページ）
SHOW STP COUNTER（258 ページ）
SHOW STP PORT（261 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

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              351      Total STP Packets              544
  Configuration BPDU             351      Configuration BPDU             544
  TCN BPDU                         0      TCN 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

-------------------------------------------------------------------------
```

STP Name	STP ドメイン名
Receive セクション	受信パケット数が表示される
Total STP Packets	受信した STP パケット（Configuration BPDU と Topology Change Notification BPDU）の総数

Configuration BPDU	Configuration BPDU 受信数
TCN BPDU	Topology Change Notification BPDU 受信数
Invalid BPDU	無効な STP パケット受信数
Transmit セクション	送信パケット数が表示される
Total STP Packets	送信した STP パケット（Configuration BPDU と Topology Change Notification BPDU）の総数
Configuration BPDU	Configuration BPDU 送信数
TCN BPDU	Topology Change Notification BPDU 送信数
Discarded セクション	破棄されたパケット数が表示される
Port Disabled	受信ポートがディセーブル状態だったために破棄された BPDU の数
Invalid Protocol	プロトコル ID フィールドかプロトコルバージョン ID フィールドの値が無効であったため破棄された STP パケット数
Invalid Type	Type フィールドの値が無効であったため破棄された STP パケット数
Invalid Message Age	メッセージエージが無効であったため破棄された STP パケット数
Config BPDU length	長さが無効だった Configuration BPDU の数
TCN BPDU length	長さが無効だった Topology Change Notification BPDU の数

表 39:

関連コマンド

RESET STP（201 ページ）
SHOW STP（255 ページ）
SHOW STP PORT（261 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

SHOW STP DEBUG

解説

各ポートで有効になっている STP デバッグオプションを表示する。

入力・出力・画面例

```
Manager >  show stp debug

  Port    Enabled Debug Modes         Output     Timeout
  ------------------------------------------------------------------------------
  Port1   MSG, PKT, STATE             16         NONE
  ------------------------------------------------------------
  Port    Enabled Debug Modes         Output     Timeout
  ------------------------------------------------------------
  Port2   STATE                       16         12345
  ------------------------------------------------------------
  Port    Enabled Debug Modes         Output     Timeout
  ------------------------------------------------------------
  Port3   None
  ------------------------------------------------------------
```

Port	ポート番号
Enabled Debug Modes	現在有効になっている STP デバッグオプション。MSG（STP パケットをデコードして表示）、PKT（STP パケットを ASCII 表示）、STATE（ポートの状態遷移を表示）、ALL（すべてのオプション）がある
Output	デバッグ情報の出力先（仮想端末（TTY）番号）
Timeout	デバッグオプションの残り有効期間（秒）

表 40:

関連コマンド

DISABLE STP DEBUG（161 ページ）
ENABLE STP DEBUG（184 ページ）
SHOW STP COUNTER（258 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

SHOW STP PORT[={*port-list*|ALL}]

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）

解説

各ポートの STP 情報を表示する。

パラメーター

PORT　ポート番号

入力・出力・画面例

```
Manager > show stp port=1

 STP Port Information
--------------------------------------------------------------------------------
 STP ..................... default
   STP Status ............ OFF
   Port .................. 1
     State ............... Disabled
     Port Priority ....... 128
     Port Identifier ..... 8001
     Pathcost ............ 4 (auto configured)
     Designated Root ..... 32768 : 00-00-cd-08-17-0c
     Designated Cost ..... 0
     Designated Bridge ... 32768 : 00-00-cd-08-17-0c
     Designated Port ..... 8001

--------------------------------------------------------------------------------
```

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ー
Port Identifier	ポート識別子
Pathcost	パスコスト
Designated Root	ルートブリッジのブリッジ識別子
Designated Cost	ポートの代表コスト
Designated Bridge	代表ブリッジのブリッジ識別子
Designated Port	代表ポート。代表ブリッジが BPDU を送信するポートのポート識別子
EdgePort	ポートがエッジポートかどうか。Yes、No のいずれか。Rapid モードのときだけ表示される
Counters/Loopback Disabled	ループ検出によりポートをディセーブルにした回数。Rapid モードのときだけ表示される

表 41:

関連コマンド

SET STP（219 ページ）
SET STP PORT（221 ページ）
SHOW STP（255 ページ）

SHOW SWITCH

カテゴリー：スイッチング / 一般コマンド

SHOW SWITCH

解説

スイッチ機能の全般的情報を表示する。

入力・出力・画面例

```
Manager > show switch

 Switch Configuration
------------------------------------------------------------------------------
 CAM size ( entries ) ....... 237568
 Switch Address ............. 00-00-cd-08-17-0c
 Learning ................... ON
 Ageing Timer ............... ON
 Number of Fixed Ports ...... 16
 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
 VLAN classification ........ To be defined
 STP Forwarding ............. Disabled
 UpTime ..................... 13:59:04
 Hashingfield ............... L2 L3 L4
 ------------------------------------------------------------------------------
```

CAM size (entries)	フォワーディングデータベースサイズ
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	固定ポートの数
Number of Uplink Ports	拡張ポートの数
Mirroring	ポートミラーリング機能の状態。Enabled か Disabled

Mirror port	ミラーポート
Ports mirroring on Rx	受信トラフィックだけをミラーリングしているソースポート
Ports mirroring on Tx	送信トラフィックだけをミラーリングしているソースポート
Ports mirroring on Both	送受信両方のトラフィックをミラーリングしているソースポート
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）
VLAN classification	現在使用可能な VLAN 種別。「To be defined」（未決定）、「IP subnet, Protocol, Port」、「MAC address, Limited Protocol, Port」のいずれか
STP Forwarding	BPDU フォワーディングの有効・無効
Uptime	再起動後の経過時間（時:分:秒の形式）。MIB-II オブジェクト sysUpTime と同じ
Hashingfield	ポートトランキングの送出ポート決定アルゴリズムが使用するヘッダー情報の種類

表 42:

関連コマンド

RESET SWITCH（202 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

スイッチング機能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                          8     Packets                         39
  Discards                         0     Discards                         0
  TooFewBuffers                    0     Aborts                           0
  DescriptorsExhausteds            0     DescriptorAreaFilleds            0
  QueueLength                      0     QueueLength                      0

PCI bus counters:
  ParityErrors                     0     ErrorChannel                     0
  FatalErrors                      0

General counters:
  Resets                           0

...
  ...
  ...
-------------------------------------------------------------------------------
```

Packet DMA counters セクション	DMA に関するカウンターが表示される
Receive サブセクション	受信パケットに関する統計が表示される
Packets	スイッチチップから CPU に渡されたパケットの数
Discards	スイッチチップから受け取ったパケットのうち、受信キューが 4096 を超えたか、空きバッファー容量が 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、空きバッファー容量が BufferLevel3 を下回ったために破棄されたものの数
DescriptorsExhausteds	受信バッファー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ーへの 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
DescriptorAreaFilleds	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ーエラーの発生回数（スイッチチップが報告したもの）
FatalErrors	PCI バス上のデータ転送における致命的エラーの発生回数（スイッチチップが報告したもの）
ErrorChannel	データ転送中にエラーが発生した DMA チャンネル
General counters セクション	一般的なカウンターが表示される
Resets	エラーによる DMA チャンネルのリセット回数

表 43:

関連コマンド

RESET SWITCH（202 ページ）
SHOW SWITCH（263 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

```
Manager > show switch debug

 Enabled Switch Debug Modes              Output     Timeout
-------------------------------------------------------------------------------
 QOS                                     16         None
-------------------------------------------------------------------------------
```

Enabled Switch Debug Modes	現在有効になっているデバッグオプション。DMA（ダイレクトメモリーアクセス）、QOS（QoS）、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 44:

関連コマンド

DISABLE SWITCH DEBUG（165 ページ）
ENABLE SWITCH DEBUG（188 ページ）

SHOW SWITCH FDB

カテゴリー：スイッチング / フォワーディングデータベース

SHOW SWITCH FDB [ADDRESS=*macadd*] [PORT={*port-list*|ALL}] [STATUS={STATIC|DYNAMIC}] [VLAN={*vlanname*|*1..4090*}]

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（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。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

ADDRESS　指定したアドレスと一致するエントリーだけを表示する
PORT　指定したポートと一致するエントリーだけを表示する
STATUS　表示するエントリー種別。STATIC（スタティックエントリー）か DYNAMIC（ダイナミックエントリー）を指定する。DYNAMIC にはポートセキュリティー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 (hardware)
------------------------------------------------------------------------------
 VLAN MAC Address         Port  Status    Hit
------------------------------------------------------------------------------
 1    00-00-cd-08-17-0c   CPU   static    y
 10   00-00-cd-08-17-0c   CPU   static    y
 20   00-00-cd-08-17-0c   CPU   static    y
 100  00-00-cd-08-17-0c   CPU   static    y
 10   00-00-cd-08-17-0c   CPU   static    n
 20   00-00-cd-08-17-0c   CPU   static    n
 100  00-00-cd-08-17-0c   CPU   static    n
 100  02-41-f4-02-c5-4b   9     dynamic   n
 10   00-00-f4-c4-04-63   1     dynamic   n
 100  00-00-f4-95-9f-31   9     dynamic   n
 100  00-90-99-1b-65-c7   9     dynamic   n
```

```
100  00-90-27-92-63-22   9     dynamic   n
100  00-50-e4-fa-02-4a   9     dynamic   n
10   00-90-99-42-00-f2   1     dynamic   n
100  08-00-2b-e7-05-8b   9     dynamic   n
100  00-00-f4-97-00-19   9     dynamic   n
100  00-00-f4-90-19-9b   9     dynamic   n
100  00-06-5b-88-80-41   9     dynamic   n
100  00-80-92-35-5e-dc   9     dynamic   n
100  00-e0-18-8a-2a-92   9     dynamic   n
100  00-03-93-ac-75-ec   9     dynamic   n
100  00-00-f4-63-1a-32   9     dynamic   n
100  00-00-f4-95-d3-78   9     dynamic   n
100  00-00-f4-95-3e-33   9     dynamic   n
100  00-00-f4-c3-02-cf   9     dynamic   n
100  00-03-93-0c-fe-f0   9     dynamic   n
100  00-30-65-bd-00-7a   9     dynamic   n
100  00-50-e4-1e-f1-4a   9     dynamic   n
100  00-90-99-00-00-14   9     dynamic   n
100  00-90-99-15-07-fd   9     dynamic   n
100  00-03-93-8c-4a-3c   9     dynamic   n
100  00-00-f4-95-30-6a   9     dynamic   n
100  00-90-99-7e-65-e7   9     dynamic   n
100  00-50-56-47-36-81   9     dynamic   n
100  00-90-99-15-08-fc   9     dynamic   n
100  00-90-99-15-07-2f   9     dynamic   n
```

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）
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

表 45:

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（190 ページ）
SHOW SWITCH（263 ページ）
SHOW SWITCH FILTER（272 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..4090}]
```

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（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。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
--------------------------------------------------------------------------
 Entry             VLAN         Destination Address   Port  Action  Source
--------------------------------------------------------------------------
     0           white (10)     00-00-f4-12-12-12     8     Forward Static
     1           white (10)     00-00-f4-12-12-13     8     Forward Learn
     2           white (10)     00-00-f4-12-12-14     8     Forward Learn

     0           orange (20)    00-00-f4-01-01-01     11    Forward Static
--------------------------------------------------------------------------
```

Entry	スタティックエントリーの番号
Destination Address	宛先 MAC アドレス

VLAN	VLAN 名と VLAN ID
Port	マッチしたパケットの出力先ポート
Action	マッチしたパケットに適用するアクション。Forward（転送）か Discard（破棄）
Source	エントリーのタイプ。Static は通常のスタティックエントリー。Learn はポートセキュリティー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 46:

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（98 ページ）
DELETE SWITCH FILTER（136 ページ）
SET SWITCH MIRROR（224 ページ）

SHOW SWITCH HWFILTER

カテゴリー：スイッチング / ハードウェアパケットフィルター

SHOW SWITCH HWFILTER[=*filter-list*]

filter-list: フィルター番号（1〜999。ハイフン、カンマを使った複数指定も可能）

解説

ハードウェアパケットフィルターの情報を表示する。
クラシファイアの設定は SHOW CLASSIFIER コマンドで確認できる。

パラメーター

HWFILTER　フィルター番号。省略時はすべてのフィルターの情報が簡潔に表示される

入力・出力・画面例

```
Manager > show switch hwfilter

Switch Hardware Filter Summary Information
------------------------------------------------------------------------------
Number of Filters ..... 1
Status ................. ENABLED

Filter ................. 1
  Classifier ........... 102

  Classifier ........... 103

  Classifier ........... 104

------------------------------------------------------------------------------

Manager > show switch hwfilter=1

 Hardware-based Packet Filters
------------------------------------------------------------------------------
 Filter ................. 1
   Rule Position ......... 0
   Classifier ............ 102
   Action ................ FORWARD
   D-Port ................ 1-4

   Rule Position ......... 1
```

```
   Classifier ............ 103
   Action ................ FORWARD
   D-Port ................ 1-4

   Rule Position ......... 2
   Classifier ............ 104
   Action ................ DISCARD
   D-Port ................ 1-4

------------------------------------------------------------------------
```

Number of Filters	定義されているフィルターの数
Status	ハードウェアパケットフィルターの状態。常に ENABLED
Filter	フィルター番号
Classifier	クラシファイア（汎用パケットフィルター）番号

表 47: HWFILTER 無指定時

Filter	フィルター番号
Rule Position	エントリー番号
Classifier	クラシファイア（汎用パケットフィルター）番号
Action	アクション
D-Port	出力スイッチポート

表 48: HWFILTER 指定時

関連コマンド

ADD SWITCH HWFILTER（100 ページ）
SHOW CLASSIFIER（230 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=5

 Switch Port Information
--------------------------------------------------------------------------------
 Port ........................... 5
   Description ................... -
   Status ........................ ENABLED
   Link State .................... Up
   UpTime ........................ 00:00:32
   Port Media Type ............... ISO8802-3 CSMACD
   Configured speed/duplex ....... Autonegotiate
   Actual speed/duplex ........... 100 Mbps, full duplex
   Configured master/slave mode .. Autonegotiate
   Actual master/slave mode ...... Not applicable
   Acceptable Frames Type ........ Admit All Frames
   Egress rate limit ............  -
   Learn limit ................... -
   Intrusion action .............. Discard
   Current learned, lock state ... 0, not locked
   Relearn ....................... OFF
   Mirroring ..................... Disabled
   Is this port mirror port ...... No
   Enabled flow control(s) ....... Pause
   Port-based VLAN(s) ............ default (1)
   Advanced Flow Control length .. -
   Jumbo Packets ................. Off
   Trunk Group ................... -
   STP ........................... default
--------------------------------------------------------------------------------
```

```
Manager > show switch port=3

 Switch Port Information
--------------------------------------------------------------------------------
 Port ........................... 3
   Description ................... -
   Status ........................ ENABLED
   Link State .................... Down
   UpTime ........................ -
   Port Media Type ............... ISO8802-3 CSMACD
   Configured speed/duplex ....... Autonegotiate
   Actual speed/duplex ........... -
   Configured master/slave mode .. Not applicable
   Actual master/slave mode ...... -
   Acceptable Frames Type ........ Admit All Frames
   Egress rate limit ............  -
   Learn limit ................... -
   Intrusion action .............. Discard
   Current learned, lock state ... 0, not locked
   Relearn ....................... OFF
   Mirroring ..................... Disabled
   Is this port mirror port ...... No
   Enabled flow control(s) ....... Pause
   Port-based VLAN(s) ............ default (1)
   Advanced Flow Control length .. -
   Jumbo Packets ................. Off
   Trunk Group ................... -
   STP ........................... default

   GBIC vendor name .............. AGILENT
   GBIC part number .............. HFBR-5601
   GBIC vendor SN ................ 0201091421522381
   GBIC date code ................ 02010900
--------------------------------------------------------------------------------
```

Port	ポート番号
Description	ポート名称（メモ）
Status	ポートの管理ステータス。ENABLED か DISABLED
Link State	ポートのリンクステータス。Up か Down
UpTime	ポートがリセット（初期化）されてから現在までの経過時間（hh:mm:ss の形式）
Port Media Type	MIB-II オブジェクト ifType で定義される物理層インターフェースタイプ
Configured speed / duplex	通信モードの設定値。Autonegotiate または速度 10Mbps、100Mbps とデュプレックスモード half duplex、full duplex の組み合わせで表示される。また、オートネゴシエーションで特定の通信モードを使うよう設定されているときは、「(by autonegotiation)」という文字列も表示される
Actual speed / duplex	実際の通信モード。速度 10 Mbps、100 Mbps、1000 Mbps とデュプレックスモード half duplex、full duplex の組み合わせで表示される。通信モードが固定に設定されている場合は、Configured speed / duplex と同じ。ポートがオートネゴシエーションに設定されている場合は、ネゴシエーションで決定された通信モードが表示される。ポートがリンクアップしていない場合は「-」（未決定）と表示される
Configured master / slave mode	1000BASE-T ポートのマスター / スレーブ設定値。Autonegotiate、Master、Slave のいずれか。1000BASE-T 以外のポートでは、Not applicable と表示される
Actual master / slave mode	1000BASE-T ポートの実際のマスター / スレーブ。その他のポートの場合は、Not applicable と表示される
Acceptable Frames Type	受信可能なフレームタイプ。Admit All Frames か Admit Only VLAN-tagged Frames
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ーの動作モード。OFF（スタティック）、ON（ダイナミック）のどちらか
Mirroring	ミラーリング対象パケットの向きとミラーポート。「Disabled」、「Rx, frames mirrored to Port X」、「TX, frames mirrored to Port X」、「Both, frames mirrored to Port X」のいずれか
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
IP subnet-based VLAN(s)	ポートが所属する IP サブネット VLAN 名（VID）
Protocol-based VLAN(s)	ポートが所属するプロトコル VLAN 名（VID）
MAC address-based VLAN(s)	ポートが所属する MAC アドレス VLAN 名（VID）
Limited protocol-based VLAN(s)	ポートが所属するリミテッドプロトコル VLAN 名（VID）
Port-based VLAN(s)	ポートが所属するポート VLAN 名（VID）
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
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 49:

関連コマンド

SET SWITCH PORT（225 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=9 counter

 Switch Port Counters
------------------------------------------------------------------------------

Port 9. Fast Ethernet MAC counters:
 Combined receive/transmit packets by size (octets) counters:
  64                              122 512 - 1023                          1
  65 - 127                      16341 1024 - 1518                         0
  128 - 255                        46 1519 - MaxPktSz                     0
  256 - 511                        10

 General Counters:
 Receive                           Transmit
  Octets                       851898 Octets                        831907
  Pkts                           8371 Pkts                            8149
  FCSErrors                         0
  MulticastPkts                    66 MulticastPkts                      0
  BroadcastPkts                   132 BroadcastPkts                      3
  PauseCtrlFrms                     0 PauseCtrlFrms                      0
  OversizePkts                      0
  Fragments                         0
  Jabbers                           0
  AlignmentErrors                   0
  CarrierSenseErr                   0
  UndersizePkts                     0
                                      FrameWDeferrdTx 0
                                      SingleCollsnFrm 0
                                      MultCollsnFrm   0
```

```
                                        LateCollsns     0
                                        ExcessivCollsns 0
------------------------------------------------------------------------------
```

Combined receive/transmit packets by size (octets) counters セクション	フレームサイズ別送受信数分布
64	64 オクテット長のフレーム送受信数
65 - 127	65～127 オクテット長のフレーム送受信数
128 - 255	128～255 オクテット長のフレーム送受信数
256 - 511	256～511 オクテット長のフレーム送受信数
512 - 1023	512～1023 オクテット長のフレーム送受信数
1024 - 1518	1024～1518 オクテット長のフレーム送受信数
1519 - MaxPktSz	1519 オクテット～最大サイズのフレーム送受信数
General Counters セクション	一般的な送受信カウンター
Receive サブセクション	受信トラフィックカウンターが表示される
Octets	受信オクテット数
Pkts	受信パケット数
FCSErrors	FCS エラーフレーム受信数
MulticastPkts	マルチキャストフレーム受信数
BroadcastPkts	ブロードキャストフレーム受信数
PauseCtrlFrms	有効な PAUSE フレーム受信数
OversizePkts	オーバーサイズフレーム受信数。正しい形式であるが、長さが 1518 オクテットより長いパケットの総数
Fragments	フラグメントフレーム受信数。不正な FCS を持ち、なおかつ、長さが 64 オクテットより短いフレームの総数。アライメントエラーを含む
Jabbers	ジャバーフレーム受信数。1518 オクテットより長いフレームのうち、不正な FCS を持つものの総数。アライメントエラーパケットも含む
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
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 サブセクション	送信トラフィックカウンターが表示される
Octets	送信オクテット数
Pkts	送信パケット数

MulticastPkts	マルチキャストフレーム送信数
BroadcastPkts	ブロードキャストフレーム送信数
PauseCtrlFrms	有効な PAUSE フレーム送信数
FrameWDeferrdTx	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
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

表 50:

関連コマンド

SET SWITCH PORT（225 ページ）
SHOW SWITCH COUNTER（265 ページ）
SHOW SWITCH PORT（276 ページ）

SHOW SWITCH PORT INTRUSION

カテゴリー：スイッチング / ポート

SHOW SWITCH PORT=*port-number* INTRUSION

port-number: スイッチポート番号（1〜）

解説

ポートセキュリティー機能がオンのポート（LEARN パラメーターが 0 以外に設定されているポート）において、学習済み MAC アドレス数が上限に達した後で受信した未学習の MAC アドレス（INTRUSIONACTION の対象となったアドレス）の一覧を表示する。

パラメーター

PORT　ポート番号

入力・出力・画面例

```
Manager > show switch port=11 intrusion

 Switch Port Information
--------------------------------------------------------------------------------
Port 11 -    1 intrusion(s) detected
    00-00-f4-1e-e0-0a
--------------------------------------------------------------------------------
```

関連コマンド

SET SWITCH PORT（225 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 ..................... quad1000
   Speed ............................... 1000 Mbps
   Ports ............................... 1-4
--------------------------------------------------------------------------------
```

Trunk group name	トランクグループ名
Speed	トランクポートの通信速度。10Mbps、100Mbps、1000Mbps、-（未設定）のいずれか
Ports	所属ポート

表 51:

関連コマンド

ADD SWITCH TRUNK（102 ページ）
CREATE SWITCH TRUNK（127 ページ）
DELETE SWITCH TRUNK（139 ページ）
DESTROY SWITCH TRUNK（153 ページ）
SET SWITCH TRUNK（227 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..4090*|ALL}]
SHOW VLAN[=ALL] [TYPE={PORT|SUBNET|
PROTOCOL|LIMITEDPROTOCOL|MACADDRESS|ALL}]

vlanname: VLAN 名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、先頭は数字以外。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。省略時はすべての VLAN が表示される
TYPE　VLAN 種別。特定の種類の VLAN だけを表示させたいときに指定する

入力・出力・画面例

```
Manager > show vlan

 VLAN Information
--------------------------------------------------------------------------------
 Name ............... default
 Identifier ......... 1
 Status ............. static
 Type ............... IP subnet-based
 Untagged ports ..... None
 Tagged ports ....... None
 Associations ....... Port only
 Port associations .. None
 Spanning Tree ...... default
 Trunk ports ........ None
 Mirror port ........ None
 Broadcast limit .... None
 Multicast limit .... None
 Attachments:
 Module           Protocol         Format    Discrim     MAC address
 ------------------------------------------------------------------
 GARP             Spanning tree    802.2     42              -
 ------------------------------------------------------------------

 Name ............... a
```

```
Identifier ......... 10
Status ............. static
Type ............... Port-based
Untagged ports ..... 1-8
Tagged ports ....... None
Port associations .. 1-8
Spanning Tree ...... default
Trunk ports ........ None
Mirror port ........ None
Broadcast limit .... None
Multicast limit .... None
Attachments:
Module           Protocol         Format    Discrim     MAC address
-------------------------------------------------------------------
GARP             Spanning tree    802.2     42              -
-------------------------------------------------------------------

Name ............... b
Identifier ......... 20
Status ............. static
Type ............... Port-based
Untagged ports ..... 9-16
Tagged ports ....... None
Port associations .. 9-16
Spanning Tree ...... default
Trunk ports ........ None
Mirror port ........ None
Broadcast limit .... None
Multicast limit .... None
Attachments:
Module           Protocol         Format    Discrim     MAC address
-------------------------------------------------------------------
GARP             Spanning tree    802.2     42              -
-------------------------------------------------------------------

Name ............... nb
Identifier ......... 100
Status ............. static
Type ............... Protocol-based
Untagged ports ..... 1-16
Tagged ports ....... None
Associations:
Index   Encap.       Protocol Name     Prot  Ports
-------------------------------------------------------------------
   0    SAP          NETBEUI           f0    1-16

Port associations .. None
Spanning Tree ...... default
Trunk ports ........ None
Mirror port ........ None
Broadcast limit .... None
```

```
Multicast limit .... None
Attachments:
Module           Protocol         Format    Discrim     MAC address
-------------------------------------------------------------------
GARP             Spanning tree    802.2     42              -
-------------------------------------------------------------------


-------------------------------------------------------------------------
```

Name	VLAN 名
Identifier	VLAN ID
Status	VLAN のステータス（static のみ）
Type	VLAN の種類（Port-based、Protocol-based、IP subnet-based、MAC address-based、Limited protocol-based）
Untagged ports	タグなしポート
Tagged ports	タグ付きポート
Ports associations	ポート VLAN のメンバーポート
Associations セクション	ポートと IP サブネット、プロトコル、MAC アドレスの関連付けが表示される
IP Address	IP サブネット VLAN のサブネットアドレス
Network Mask	サブネットマスク
Ports	IP サブネット、プロトコル、MAC アドレスと関連付けられているポートの一覧
Index	プロトコル、MAC アドレスのインデックス番号
MAC address	MAC アドレス VLAN のメンバーアドレス
Encap.	Ethernet のフレームフォーマット（エンキャプセレーション）
Protocol Name	プロトコル名称
Prot	プロトコル番号
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
Broadcast limit	ブロードキャストパケットの送信レート上限値
Multicast limit	マルチキャストパケットの送信レート上限値
Attachments セクション	VLAN インターフェースにバインドされている上位プロトコルモジュールの情報が表示される
Module	バインドされている上位モジュール名
Protocol	上位モジュールのプロトコル
Format	フレームタイプ
Discrim	上記フレームタイプに対応したプロトコル番号
MAC Address	モジュールが使用する MAC アドレス

表 52:

例

■すべての VLAN の情報を表示する。

```
SHOW VLAN
```

■プロトコル VLAN の情報をだけを表示する。

```
SHOW VLAN TYPE=PROTOCOL
```

関連コマンド

CREATE VLAN（128 ページ）
DESTROY VLAN（154 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 53:

関連コマンド

DISABLE VLAN DEBUG（172 ページ）
ENABLE VLAN DEBUG（195 ページ）

SHOW VLAN PORT

カテゴリー：スイッチング / バーチャル LAN

SHOW VLAN PORT[=*port-number*]

port-number: スイッチポート番号（1〜）

解説

スイッチポートごとの VLAN 所属情報を表示する。

パラメーター

PORT　ポート番号。複数指定が可能。省略時はすべてのポートが対象となる

入力・出力・画面例

```
Manager > show vlan port=8-9

 VLAN Port Information
--------------------------------------------------------------------------------
 Port ........................... 8
   VLAN Name ..................... IP10
   Type .......................... Port-based
   Outgoing packets .............. untagged
   Associations .................. Port only
   Port association .............. Yes

   VLAN Name ..................... NetWare
   Type .......................... Protocol-based
   Outgoing packets .............. untagged
   Associations:
   Index   Encapsulation     Protocol     Name
   ------------------------------------------------------
      0    SAP               e0           IPX 802.2
   Port association .............. No

 Port ........................... 9
   VLAN Name ..................... IP20
   Type .......................... Port-based
   Outgoing packets .............. untagged
   Associations .................. Port only
   Port association .............. Yes

   VLAN Name ..................... NetWare
   Type .......................... Protocol-based
```

```
   Outgoing packets .............. untagged
   Associations:
   Index   Encapsulation     Protocol     Name
   ------------------------------------------------------
      0    SAP               e0           IPX 802.2
   Port association ............... No

-------------------------------------------------------------------------
```

Port	スイッチポート番号
VLAN Name	VLAN 名
Type	VLAN の種類（Port-based、Protocol-based、IP subnet-based、MAC address-based、Limited protocol-based）
Outgoing packets	送出パケットのタグ付き（tagged）、タグなし（untagged）
Associations	受信したパケットを該当 VLAN 所属と判断するための基準。ポート VLAN の場合は Port only と表示される
IP Address	IP サブネット VLAN のサブネットアドレス
Network Mask	サブネットマスク
MAC Address	MAC アドレス VLAN のメンバーアドレス
Index	プロトコル、MAC アドレスのインデックス番号
Encapsulation	Ethernet のフレームフォーマット（エンキャプセレーション）
Protocol	（プロトコル VLAN の）プロトコル番号
Limited Protocol	（リミテッドプロトコル VLAN の）プロトコル番号
Name	プロトコル名称
Port association	この VLAN にポートが関連付けられているか

表 54:

関連コマンド

ADD VLAN PORT（107 ページ）
DELETE VLAN PORT（142 ページ）
SET VLAN PORT（229 ページ）