スイッチング

概要・基本設定

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。

■ 1 つのポートを指定

```
ENABLE SWITCH PORT=2 ↵
```

■ 連続するポート番号をハイフン区切りで指定

```
ADD VLAN=black PORT=3-7 ↵
```

■ 連続していないポート番号をカンマ区切りで指定

```
SHOW SWITCH PORT=2,4,8 ↵
```

■ カンマとハイフンの組み合わせ指定

```
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（104 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（83 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（138 ページ）の SPEED パラメーターを使います。デフォルトは AUTONEGOTIATE です。

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

■ 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（118 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（194 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（200 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（118 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 ↵
```

■ デフォルトでは、すべてのポートで MDI/MDI-X 自動切り替えが有効になっています。MDI/MDI-X 自動切り替えを無効にするには、DISABLE SWITCH PORT AUTOMDI コマンド（84 ページ）を実行します。

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

■ MDI/MDI-X 自動切り替えを無効にした直後のポートは、MDI-X 固定になります。MDI/MDI-X 自動切り替えが無効なポートで MDI/MDI-X を変更するには、SET SWITCH PORT コマンド（138 ページ）の POLARITY パラメーターを使います。

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

ポートトランキング

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。

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

本製品ではトランクグループを 6 つまで作成できます。それぞれのトランクグループには、最大 8 ポートまで所属させることが可能です。ポートは隣接していなくてもかまいません。ただし、同一グループ内に 10/100M ポートと 1000M ポートを混在させることはできません。
ポートトランキングを使用するために最低限必要な設定について説明します。ここでは、ポート 1-4 を束ねて使用するものとします。

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

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

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=uplink 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。

✎ トランクグループにポートを追加したあとで、グループ全体あるいはグループ内のポートを所属 VLAN から削除することはできません。VLAN から削除するには、DELETE SWITCH TRUNK コマンド（69 ページ）を使ってあらかじめポートをトランクグループから外しておく必要があります。トランクグループにポートを割り当てた後で、別の VLAN にグループ全体あるいはグループ内のポートを追加することは可能です。

✎ ポートトランキングの設定は、トランクポートによって接続される両方のスイッチで行う必要があります。

✎ ポートトランキングとイングレスフィルタリング、ポートトランキングとポート認証は併用できません（トランクポートでは、イングレスフィルタリング、ポート認証を使用できません）。

■ トランクグループの情報は SHOW SWITCH TRUNK コマンド（206 ページ）で確認できます。

```
SHOW SWITCH TRUNK=uplink ↵
```

■ 送信時のポート選択基準は CREATE SWITCH TRUNK コマンド（64 ページ）、SET SWITCH TRUNK コマンド（143 ページ）の SELECT パラメーターで指定できます。次の例ではトランクグループ「uplink」のポート選択基準を、送信元 MAC アドレスに変更しています。デフォルトでは、送信元 MAC アドレスと宛先 MAC アドレスの両方（MACBOTH）を使って、トランク内のどのポートを使用するかが決定されます。

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

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

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

■ トランクグループからポートを削除するには DELETE SWITCH TRUNK コマンド（69 ページ）を使い

ます。

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

■ トランクグループを削除するには DESTROY SWITCH TRUNK コマンド（71 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（69 ページ）で所属ポートを削除します。

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

ポートミラーリング

ポートミラーリングは、特定のポートを通過するトラフィックをあらかじめ指定したミラーポートにコピーする機能です。パケットを必要なポートにだけ出力するスイッチではパケットキャプチャーなどが困難ですが、ポートミラーリングを利用すれば、任意のポートのトラフィックをミラーポートでキャプチャーすることができます。
また、ハードウェアパケットフィルターを併用することで、Ethernet ヘッダー情報や、IP/TCP/UDP ヘッダー情報を元に特定のトラフィックだけをミラーポートにコピーするよう設定することも可能です。
なお、ポートミラーリング機能の仕様は以下のようになっています。

- ミラーポートは 1 つ、ソースポートは 3 つまで指定可能
- ハードウェアパケットフィルターによってミラーリングされたパケットは、すべて VLAN タグが付いた状態でミラーポートに出力されます。
- ソースポートを複数設定している状態で、あるソースポートから入力されたパケットが、L2 スイッチングされて別のソースポートから出力された場合、ミラーポートにはパケットが 1 個だけ出力されます。

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（137 ページ）を実行します。

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

   SET SWITCH MIRROR コマンド（137 ページ）を実行すると、指定ポートはミラーポートとして設定され、どの VLAN にも属していない状態となります。

```
SET SWITCH MIRROR=1 ↵
```

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

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

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

2. ポートミラーリング機能を有効にします。

```
ENABLE SWITCH MIRROR ↵
```

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

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

✎ 複数のポートをミラーしたいときは、SET SWITCH PORT コマンド（138 ページ）を複数回実行してください（最大 3 ポートまで指定可能）。ただし、ミラーリング対象ポートを増やすことはパフォーマンス低下につながりますのでご注意ください。また、複数のソースポートを指定した場合で、かつ指定ポートにタグ付きとタグなしが混在している場合、送信パケットはすべてタグなしとしてミラーリングされます。

設定は以上です。

■ ポートミラーリングの設定を確認するには SHOW SWITCH コマンド（187 ページ）を実行します。ミラーポートは SHOW VLAN コマンド（「バーチャル LAN」の 19 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（194 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（82 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（137 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（138 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（137 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。

■ 次の条件の場合、ソースポートから入力されたタグ付きパケットがタグなしパケットとして、またタグなしパケットがタグ付きパケットとして、ミラーポートから出力されます。

- タグなしのソースポートから入力したタグ付きのパケットで、タグの VLAN ID が機器に存在しない場合は、タグなしでミラーポートから出力されます。
- タグ付きのソースポートから入力したタグ付きパケットで、ソースポートの受信可能なフレームタイプが Acceptable All Frames（すべて）に設定されていて、かつ、タグの VLAN ID が機器に存在しない場合は、タグなしでミラーポートから出力されます。
- タグ付きのソースポートから入力したタグなしパケットで、ソースポートの受信可能なフレームタイプが Admit Only Vlan-tagged Frames（VLAN タグ付きフレームのみ）に設定されている場合は、タグ付きでミラーポートから出力されます。

ハードウェアパケットフィルターによるミラーリング

ポートミラーリング機能とハードウェアパケットフィルターを併用すると、IP アドレスや TCP/UDP のポート番号を基準に、特定の IP トラフィックだけをミラーポートに送るよう設定することができます。
なお、仕様によりハードウェアパケットフィルター経由でミラーリングされたパケットは、VLAN タグが付いた状態でミラーポートに出力されます。キャプチャーソフトが VLAN タグを識別できない場合、IP パケットがプロトコルタイプ 0x8100（802.1Q タグ）として表示される場合がありますのでご注意ください。
ここでは、ハードウェアパケットフィルターを使って、サーバー 192.168.10.5 に出入りする IP トラフィックだけをミラーポート（ポート 1）にコピーする設定例を示します。

1. ミラーポートを指定します。指定できるのは VLAN default 所属のポートだけです。ミラーポートに指定したいポートが VLAN default 以外に所属している場合は、最初に現在所属の VLAN から削除し VLAN default の所属に戻した上で、SET SWITCH MIRROR コマンド（137 ページ）を実行します。

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

   SET SWITCH MIRROR コマンド（137 ページ）を実行すると、指定ポートはミラーポートとして設定され、どの VLAN にも属していない状態となります。

   ```
   SET SWITCH MIRROR=1 ↵
   ```

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

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

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

2. ポートミラーリング機能を有効にします。

   ```
   ENABLE SWITCH MIRROR ↵
   ```

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

を指定します。

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

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

```
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.5 ACTION=SENDMIRROR ↵
ADD SWITCH L3FILTER=2 ENTRY DIPADDR=192.168.10.5 ACTION=SENDMIRROR ↵
```

設定は以上です。

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

```
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.5 PRIORITY=7
  ACTION=SENDMIRROR,SETPRIORITY ↵
ADD SWITCH L3FILTER=2 ENTRY DIPADDR=192.168.10.5 PRIORITY=7
  ACTION=SENDMIRROR,SETPRIORITY ↵
```

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

```
ADD SWITCH L3FILTER=1 ENTRY SIPADDR=192.168.10.5 PRIORITY=7
  ACTION=SETPRIORITY ↵
ADD SWITCH L3FILTER=2 ENTRY DIPADDR=192.168.10.5 PRIORITY=7
  ACTION=SETPRIORITY ↵
```

また、一致するエントリーに DENY アクションが含まれている場合は、エントリーの順序に関係なく DENY アクション（破棄）が実行されます。これはハードウェアパケットフィルターの仕様です。
ハードウェアパケットフィルターの詳細については、「ハードウェアパケットフィルター」をご覧ください。

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フレーム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（138 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（0〜256 個）を設定することによって有効になります。LEARN パラメーターに 0 を設定するか、学習済みの MAC アドレスが制限値に達すると、学習機能を停止（ポートロック状態）し、それ以降に受信した未学習の送信元 MAC アドレスを持つフレーム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（138 ページ）の INTRUSIONACTION パラメーターで指定）

アクション名	動作
DISCARD	不正なフレームを破棄する。
TRAP	不正なフレームを破棄し、SNMP トラップを送信する。
DISABLE	不正なフレームを破棄し、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。
LOG	不正なフレームを破棄し、ログに記録する。
TRAPCONTINUE	SNMP トラップ通知済みの不正 MAC アドレスを検知すると再度 SNMP トラップを通知する。
LOGCONTINUE	ログ保存済みの不正 MAC アドレスを検知すると再度ログに記憶する。

表 1:

■ ポートに学習可能な MAC アドレスの最大数と不正フレーム受信時のアクションを設定するには、SET SWITCH PORT コマンド（138 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 ↵
```

✎ ポートに学習可能な MAC アドレスの最大数と不正フレーム受信時のアクションを設定した場合は、ポートに接続されているデバイスを別のポートに移動させないでください。

✎ TRAP/TRAPCONTINUE と LOG/LOGCONTINUE は、カンマで区切って同時に指定することができます。ただし、TRAP と TRAPCONTINUE、LOG と LOGCONTINUE は同時に指定することはできません。

SET SWITCH PORT コマンド（138 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（138 ページ）の RELEARN パラメーターの設定により異なります。デフォルトでは、OFF に設定されています。

- 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、ポート認証を使用できません。

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フレームは「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フレームを受信すると、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 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（「フォワーディングデータベース」の 25 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（194 ページ）に SECURITY オプションを指定して確認します。「Learn」欄には学習可能な MAC アドレス最大数 (0〜256、セキュリティーオフ時は「-」)、「Relearn」欄にはポートセキュリティーモードの動作モード (Off か On のいずれか)、「Learned」欄は MAC アドレスの登録数 (0〜256、セキュリティーオフ時は「-」)、「Locked」欄はポートロック状態 (Off か On のいずれか、セキュリティーオフ時は「-」、ACTIVATE SWITCH PORT LOCK コマンド (54 ページ）によるロック時は「#」が付与されます)、「IntrusionAction」欄はロック状態で未学習の MAC アドレスを受信したときのアクション (Disable、Discard、Trap、Log、TrapContinue、LogContinue のいずれか) が表示されます。

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

■ 不正とみなされた MAC アドレスは SHOW SWITCH PORT INTRUSION コマンド（205 ページ）で確認できます（SET SWITCH PORT コマンド（138 ページ）の INTRUSIONACTION に DISABLE、TRAP、LOG、TRAPCONTINUE、LOGCONTINUE を指定した場合）。

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

■ 学習済みアドレス数が上限に達する前に手動でポートをロックするには ACTIVATE SWITCH PORT LOCK コマンド（54 ページ）を使います。あらかじめ SET SWITCH PORT コマンド（138 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（「フォワーディングデータベース」の 8 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 ACTION=FORWARD PORT=11
  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（「フォワーディングデータベース」の 12 ページ）で行います。ENTRY 番号は SHOW SWITCH FILTER コマンド（「フォワーディングデータベース」の 25 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（138 ページ）でアドレス学習の上限値（LEARN パラメーター）に NONE 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データベースから削除されます。

```
SET SWITCH PORT=11 LEARN=NONE ↵
```

■ 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（104 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（138 ページ）の LEARN パラメーターに NONE 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 (3087312): Port 11 has been disabled by the Port Security feature.
```

■ 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 129 ページ）によって保存されます（SET SWITCH PORT コマンド（138 ページ）の RELEARN パラメーターが OFF の場合）。

パケットストームプロテクション

パケットストームプロテクションは、ポートグループごとにブロードキャスト/マルチキャスト/未学習のユニキャストフレームの受信レートに上限を設定し、パケットストームを防止するための機能です。設定値を上回るレートでこれらのフレームを受信した場合、フレームは破棄されます。本機能はデフォルトではオフ

になっています。
受信レートは、下記のポートグループ単位で設定します。

機種	ポートグループ
8424TX/XL	ポート 1〜8
	ポート 9〜16
	ポート 17〜24
8424XL	ポート 25（拡張モジュール）
	ポート 26（拡張モジュール）

表 2: ポートグループ

制限できるのは以下のフレームです。かっこ内は設定パラメーターの名前です。

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

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

✎ 受信レートの上限値は、ポートグループ単位での設定になりますが、1 ポートあたりの上限値として動作します。

■ 受信レートの設定は SET SWITCH PORT コマンド（138 ページ）で行います。ここでは、ポートグループ 1-8 に対して、ブロードキャストフレームの受信レートを 1 秒あたり 1000 個に制限します。

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

■ 受信レートの制限を解除するには値として NONE か 0 を指定します。

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

■ パケットストームプロテクションの設定状況は SHOW SWITCH PORT コマンド（194 ページ）で確認できます。「Broadcast rate limit」、「Multicast rate limit」、「DLF rate limit」をご覧ください。

ループガード

本製品ではループガードとして以下の 2 つをサポートしています。
ループ検出したポート番号をログ、トラップで管理者に通知することにより、ループの原因特定、対策が容易になります。設定方法については、「運用・管理」/「ログ」、「運用・管理」/「SNMP」をご覧ください。

- LDF 検出
- MAC アドレススラッシングプロテクション

LDF 検出

LDF（Loop Detection Frame）とは、特殊な宛先 MAC アドレス（00-00-F4-27-71-01）を持った試験フレームです。
LDF 検出機能を有効にしたポートでは、一定時間ごとに LDF を送出します。
送出した LDF が他の接続機器を経由するなどして戻ってきた場合、以下の条件をすべて満たす場合に、ループ状態と判断されます。

- LDF の送信元 MAC アドレスと機器自身の MAC アドレスが一致すること
- 装置で保持している送信済み LDF の情報（LDF ID）と、LDF フレーム内の LDF ID の情報が一致すること
- その他、受信した LDF のフレームサイズやフィールドの一部をチェックした結果、本製品から送信した LDF と仕様が一致すること

LDF 検出の仕様は、次のとおりです。

- アクション終了時の FDB 全クリアは実施しない。
- トランクポートに対して LDF 検出機能を有効にするよう指定した場合、トランクグループの全ポートについて機能が有効になる。
- LDF を送信したポートの VLAN ID と受信したポートの VLAN ID が異なる場合もループ状態と判定する。(VLANDISABLE を除く)

ループ状態と判断された場合、受信ポートで以下のアクションのうちいずれかを行います。

PORTDISABLE	ポートをディセーブルにする：デフォルト
VLANDISABLE	ループが発生した VLAN に対してのみポートをディセーブルにする
LINKDOWN	ポートを物理的にリンクダウンさせる
LOGONLY	ポートの制御は行わず、ログへの記録と SNMP トラップの送信のみを行う
NONE	動作を行わず、LDF の送受信およびカウンター処理のみを行う

表 3: LDF によるループ検出時のアクション

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

■ ポート 2 の LDF 検出機能を有効にするには ENABLE SWITCH LOOPDETECTION コマンド（101 ページ）を使用します。

```
ENABLE SWITCH LOOPDETECTION PORT=2 ↵
```

■ ポート 2 の LDF 検出時のアクションを LINKDOWN（ポートを物理的にリンクダウンさせる）、アクションからの復帰時間を 60 秒に設定するには SET SWITCH PORT コマンド（138 ページ）を使用します。

```
SET SWITCH PORT=2 LOOPACTION=LINKDOWN BLOCKTIMEOUT=60 ↵
```

■ LDF の送出間隔を 60 秒に設定するには SET SWITCH LOOPDETECTION コマンド（136 ページ）を使用します。

```
SET SWITCH LOOPDETECTION INTERVAL=60 ↵
```

■ ポート 2 の LDF 検出機能の設定情報や状態を表示するには SHOW SWITCH LOOPDETECTION コマ

ンド（191 ページ）を使用します。

```
SHOW SWITCH LOOPDETECTION PORT=2 ↵
```

■ ポート 2 の LDF 検出機能のカウンターの情報を表示するには SHOW SWITCH LOOPDETECTION コマンド（191 ページ）を使用します。

```
SHOW SWITCH LOOPDETECTION COUNTER PORT=2 ↵
```

併用可能な機能と注意事項

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

- ポートトランキング・LACP
- MAC アドレススラッシングプロテクション
- タグ VLAN
- マルチプル VLAN（Protected Port VLAN）
- スパニングツリープロトコル（STP/RSTP）
- ポート認証（802.1X 認証、MAC ベース認証）

なお、併用可能な機能についても下記の注意事項があります。

- ポートトランキング・LACP
  - ポートトランキング・LACP を併用するときは、トランクグループの所属ポートすべてに CREATE SWITCH TRUNK コマンド（64 ページ）、SET SWITCH TRUNK コマンド（143 ページ）または SET LACP コマンド（123 ページ）で指定された LDF 検出の設定が適用されます。トランクグループの所属ポートに対する SET SWITCH PORT コマンド（138 ページ）によるポート個別の設定は無効となります。なお、一部の所属ポートにだけ LDF 検出の設定を行っても、すべての所属ポートに同じ LDF 検出設定が自動的に適用されます。
- MAC アドレススラッシングプロテクション
  - MAC アドレススラッシングプロテクションは LDF 検出と目的が同じであるため、同一装置上で併用（同時使用）することは推奨しません。（ループ検出に時間がかかることがあります。）併用を行う場合は、MAC アドレススラッシングプロテクションと LDF 検出のアクションを一致させてください。
  - 初期状態では MAC アドレススラッシングプロテクションが有効なため、LDF 検出のみを使う場合は、全ポートで MAC アドレススラッシングプロテクションを無効化（SET SWITCH PORT=ALL THRASHACTION=NONE を指定）、トランキングを使用している場合はトランク名ごとに無効化（SET SWITCH TRUNK=trunk THRASHACTION=NONE を指定）、LACP を使用している場合は LACP 全体で無効化（SET LACP THRASHACTION=NONE を指定）してから、LDF 検出を有効化してください。
- ポート認証（802.1X 認証、MAC ベース認証）
  - LDF 検出とポート認証を併用した場合、アクションのうち VLANDISABLE は使用できません。（ポート認証とタグ VLAN が併用できないためです。）

MAC アドレススラッシングプロテクション

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

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

表 4: MAC アドレススラッシング検出時の動作

■ ポート単位での動作設定は SET SWITCH PORT コマンド（138 ページ）で行います。ここでは、ポートグループ 1-8 に対して、MAC アドレススラッシング検出時に、スラッシングが発生した VLAN に対してのみポートをディセーブルにするよう設定します。

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

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

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

■ スタティックなトランクグループへの動作設定は、SET SWITCH TRUNK コマンド（143 ページ）で行います。また、新規にトランクグループを作成する際に、あわせて設定することも可能です。ここでは、既存のトランクグループ「uplink」に対して設定を行います。

```
SET SWITCH TRUNK=uplink THRASHACTION=LEARNDISABLE THRASHTIMEOUT=1 ↵
```

■ LACP によって自動生成されるトランクグループへの動作設定は、SET LACP コマンド（123 ページ）で行います。ここでは、LACP によって自動生成されるトランクグループに対して設定を行います。

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

■ 本製品全体に対する MAC アドレススラッシングの検出しきい値の設定は、SET SWITCH THRASHLIMIT コマンド（142 ページ）で行います。ここでは、1 秒間に 10 回以上の変更を検出した場合にスラッシングと見なすよう設定します。

```
SET SWITCH THRASHLIMIT=10 ↵
```

ポート帯域制限機能

本製品では、スイッチポートごとに送信レート、受信レートを制限することができます。
帯域制限の設定は SET SWITCH PORT コマンド（138 ページ）の INGRESSLIMIT（受信レート）、EGRESSLIMIT（送信レート）パラメーターで行います。ポートの速度（10/100M か 1000M か）によって指定できる値の範囲と単位が異なるので注意してください。

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

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

✎ 10/100M ポートで指定値が 1000Kbps の倍数でないとき、実際の受信レート上限値は 1000Kbps の倍数になるように切り上げられます。1000M ポートの場合は、8Mbps の倍数になるように切り上げられます。

✎ スイッチポートに受信レート上限値（INGRESSLIMIT）を設定している場合、同ポートを経由した TCP の通信では、TCP データのスループットが設定した上限値よりも低くなります（低下の度合いは通信状況に依存します）。これは TCP プロトコルの特性として、帯域制限機能によって破壊されたパケットの再送処理などが発生するためです。また、TCP 以外においても、同様の再送処理を行うプロトコルでは、この現象が発生する可能性があります。

✎ ポート帯域制限機能の受信レート上限値（INGRESSLIMIT）とハードウェアパケットフィルターを併用している場合、ハードウェアパケットフィルターの NODROP エントリーにマッチしたパケットに対して、受信レート上限値が適用されないことがあります。これを回避するには、EDIT コマンド（「運用・管理」の 198 ページ）で設定ファイルを開き、受信レート上限値の設定コマンド（SET SWITCH PORT=x INGRESSLIMIT=x）がハードウェアパケットフィルター設定コマンドの後にくるよう編集するか、あるいは、次のような再起動トリガーを定義して、起動時に受信レート上限値の設定が自動的に再入力されるようにしてください。

- 再起動トリガーの設定例

```
ENABLE TRIGGER ↵
CREATE TRIGGER=1 REBOOT=ALL SCRIPT=INGRESS.SCP ↵
```

- トリガースクリプト INGRESS.SCP の例

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

■ 拡張スロットに 1000M 拡張モジュールを装着している場合（ポート 25 またはポート 26）の送信レートを 500Mbps に制限するには、次のように指定します。送信レートの上限値は、10/100M ポートの場合は 1000～127000（Kbps）、1000M ポートの場合は 8～1016（Mbps）の範囲で指定します。

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

✎ 10/100M ポートで指定値が 1000Kbps の倍数でないとき、実際の送信レート上限値は 1000Kbps の倍数になるように切り上げられます。1000M ポートの場合は、8Mbps の倍数になるように切り上げられます。

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

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

■ ポート帯域制限機能の設定状況は SHOW SWITCH PORT コマンド（194 ページ）で確認できます。「Ingress rate limit」、「Egress rate limit」をご覧ください。

トリガー

トリガー機能を使用すると、スイッチポートのリンクアップ、リンクダウン時に任意のスクリプトを実行させることができます。
スイッチポートのリンクアップ、リンクダウンは、スイッチングモジュール固有のモジュールトリガーを使って捕捉します。
CREATE TRIGGER MODULE コマンド（「運用・管理」の 144 ページ）、SET TRIGGER MODULE コマンド（「運用・管理」の 293 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 229 ページ）を使って管理者にメールで通知するようにします。
なお、IP やメールの設定はす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.mydomain.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.mydomain.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.mydomain.com
To: <admin@is.mydomain.com>
Date: Thu, 22 Sep 2005 19:02:41

22-Sep-2005 19:02:41 ud-sw(SN:1193046) Port 3 linkdown
```

省電力モード

省電力モードは、リンクしていないスイッチポートへの電力供給を制限し、消費電力を抑える機能です。本機能の設定は、スイッチポート別ではなく、装置全体に対して機能します。本機能は、デフォルトで無効に設定されています。

■ 本製品の省電力モードを有効にするには、ENABLE SWITCH POWERSAVE コマンド（108 ページ）を使います。

```
ENABLE SWITCH POWERSAVE ↵
```

LACP（IEEE 802.3ad）

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

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

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

LACP によって自動設定されたトランクグループは、手動設定したトランクグループと同じように、論理的に 1 本のポートとして扱われます。また、トランクグループ内のポートに障害が発生しても残りのポートで通信が継続できるため、信頼性の向上にも貢献します。
LACP では、次の条件をすべて満たすポート群が同一のトランクグループを構成する候補となります。

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

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

作成できるトランクグループの数は最大 6（手動で設定したトランクグループを含む）、トランクグループの所属ポート数は最大 8 となります。グループ内のポートは隣接していなくてもかまいません。
前記の条件を満たすポートが 9 ポート以上ある場合は、以下の基準にしたがってメンバーポートが 8 ポート選択されます。

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

選択されなかったポートはスタンバイ状態となり、メンバーポートがリンクダウンしたときに備えて待機します。メンバーポートがリンクダウンしたときはスタンバイ状態のポートが自動的に昇格し、リンクダウンしていた旧メンバーポートが再度リンクアップしたときは、旧メンバーポートがメンバーに復帰します。
なお、以下のポートでは LACP を使用できません。これらのポートは、自動的に LACP の管理下から除外されます。

- 手動設定したトランクポート（CREATE SWITCH TRUNK コマンド（64 ページ）、ADD SWITCH TRUNK コマンド（61 ページ））
- Half Duplex で動作しているポート

基本設定

■ LACP を使用するには、ENABLE LACP コマンド（94 ページ）を実行して LACP モジュールを有効にします（デフォルトは無効）。デフォルトでは、すべてのポートが LACP の管理下に置かれているため、

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

```
ENABLE LACP ↵
```

■ 前述のとおり、デフォルトではすべてのポートで LACP が有効になっていますが、通常は特定のポートでのみ LACP を有効化して使います。たとえば、ポート 1〜4 でのみ LACP を有効化するには、DELETE LACP PORT コマンド（68 ページ）を使って、それ以外のポートを LACP の管理下から外します。

```
DELETE LACP PORT=5-16 ↵
```

あるいは、もう少し直感的な方法として、次のように指定することもできます。

```
DELETE LACP PORT=ALL ↵
ADD LACP PORT=1-4 ↵
```

■ 1 つのトランクグループで同時に使用できるポート数は最大 8 ポートですが、より多くのポートで LACP を有効化しておくことにより、冗長性をさらに高めることが可能です。たとえば、ポート 1〜10 で LACP を有効化するには次のようにします。

```
DELETE LACP PORT=ALL ↵
ADD LACP PORT=1-10 ↵
```

このように設定すると、通常時はポート 1〜8 がメンバーポートに選択され、ポート 9、10 はスタンバイ状態となります。ここでポート 1 に障害が発生すると、ポート 9 がメンバーに選択されます。ポート 1 が復帰すると、再びポート 1 がメンバーに選択され、ポート 9 はスタンバイ状態に戻ります。

■ LACP モジュールの状態は、SHOW LACP コマンド（160 ページ）で確認できます。

```
SHOW LACP ↵
```

■ LACP の管理下にあるポートの情報は、SHOW LACP PORT コマンド（162 ページ）で確認できます。

```
SHOW LACP PORT ↵
SHOW LACP PORT=1 ↵
```

■ LACP によって自動生成されたトランクグループの情報は、SHOW LACP TRUNK コマンド（166 ページ）で確認できます。また、SHOW SWITCH TRUNK コマンド（206 ページ）でも確認できます。

```
SHOW LACP TRUNK ↵
SHOW SWITCH TRUNK ↵
```

✎ LACP の設定は、対向する両方のスイッチで行う必要があります。

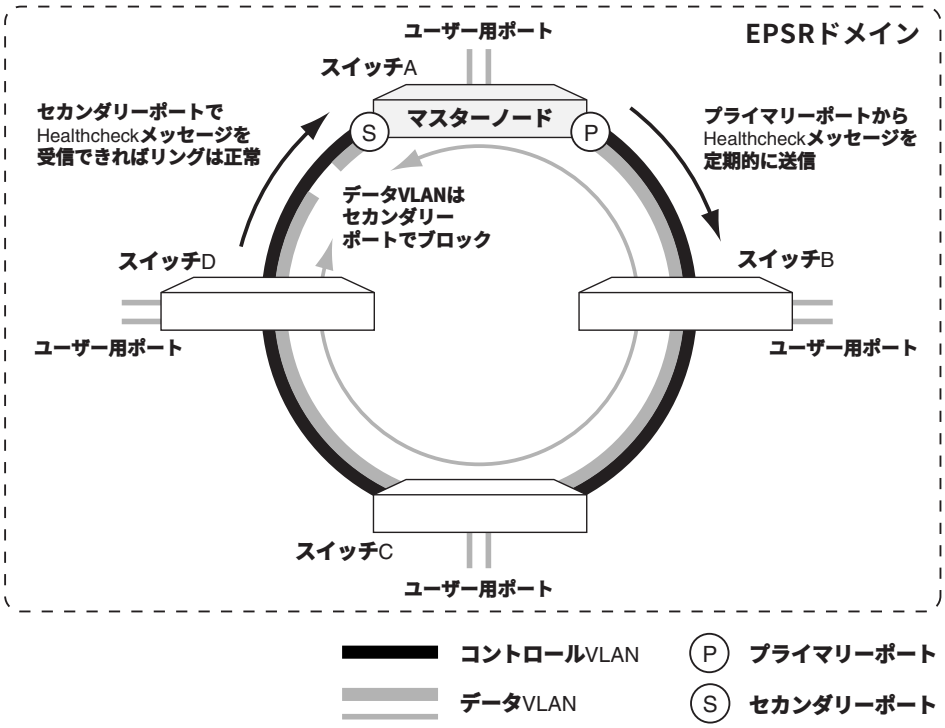
✎ LACP と EPSR、LACP とポート認証は併用できません（LACP によって生成されたトランクポートでは、EPSR、ポート認証を使用できません）。

EPSR アウェア

イーサネットリングプロテクション（EPSR = Ethernet Protected Switched Ring）は、リング構成の Ethernet ネットワークに特化したレイヤー 2 のループ防止・冗長化機能（RFC3619）です。
EPSR は、トポロジーをリング構成に限定し、各スイッチの役割をあらかじめ固定しておくことで、障害の検出と経路の切り替えをより高速に行います（最短 50 ミリ秒未満）。
本製品は、EPSR リングを構成するノードのうち、アウェア機能を実装したトランジットノードとして機能することができます。
この章では、EPSR の概要と使用方法について説明します。

概要

EPSR は、リング構成の Ethernet ネットワークでのみ動作します。
EPSR リングは複数のスイッチ（ノード）で構成され、そのうちの 1 台はリングの動作を制御するマスターノードとして、その他はトランジットノードとして機能します。
各スイッチは 2 つのポートで Ethernet リングに接続します。マスターノード上のポートは、一方をプライマリーポート、もう一方をセカンダリーポートとして設定します。データトラフィックに対し、プライマリーポートは常時フォワーディング状態ですが、セカンダリーポートは通常ブロッキング状態であり、リングに障害が発生したときだけフォワーディング状態に切り替わります。障害から回復したときは再度ブロッキング状態に戻ります。
次にリングの基本的な構成を示します。



EPSR ドメイン

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

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

ノードの種類

EPSR ドメインを構成するリング上の各スイッチは、役割上マスターノードとトランジットノードに分類されます。マスターノードは、該当 EPSR ドメインの動作を制御するスイッチで、各ドメインに 1 台だけ設定できます。その他のスイッチはトランジットノードになります。
トランジットノードは、マスターノードの指示によりリングの切り替えに対応し、自らのポート制御を行います。
また、障害時のリング切り替えの対応に特化した「スヌーピング機能」、リングの切り替えに加えて自ら検出した障害をマスターノードに通知することができる「アウェア機能」に限定したものもあり、本製品は「アウェア機能」を実装しています。
いずれのタイプのトランジットノードも同じ EPSR ドメインに複数存在でき、それぞれの機能の特徴は以下のようになります。

トランジットノードの機能	フル実装	アウェア機能	スヌーピング機能
EPSR ドメイン状態の表示	○	○	×
マスターノードの指示による FDB/ARP クリア	○	○	○
自ポートのリンクダウン通知	○	○	×
Double Fail 回復時の対応	○	○	×
プリフォワーディング状態での障害回復ポートのブロッキング	○	×	×
Trap 送信機能	○	×	×
ログ機能	○	○	×
デバッグ表示機能	○	○	×

表 5: トランジットノードの機能

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

コントロール VLAN とデータ VLAN

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

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

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

制御メッセージ

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

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

表 6: EPSR 制御メッセージ

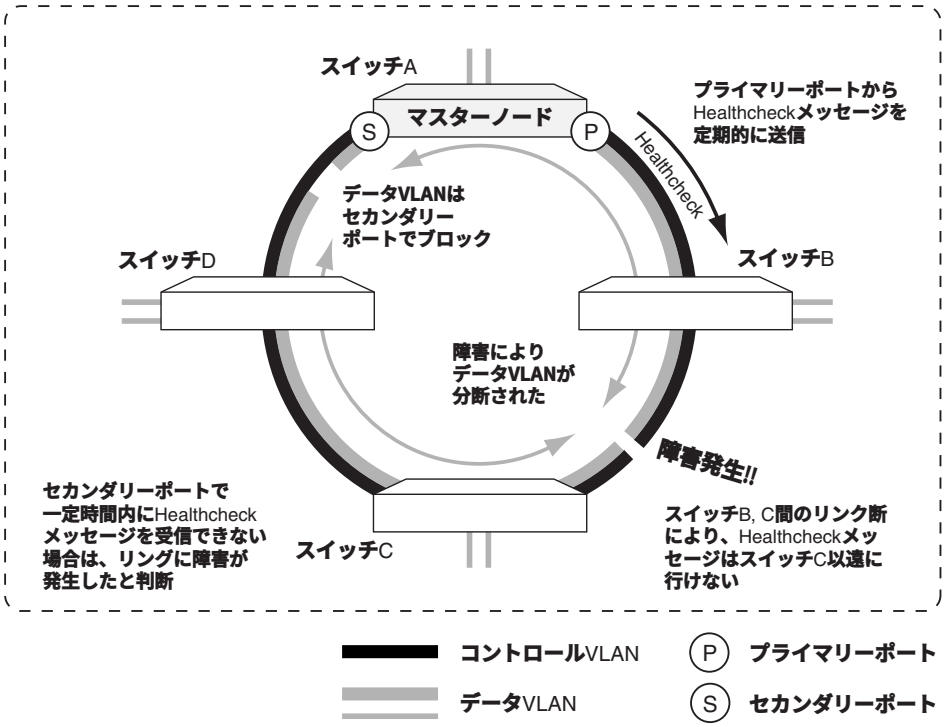
障害検出機能

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

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

Healthcheck メッセージ

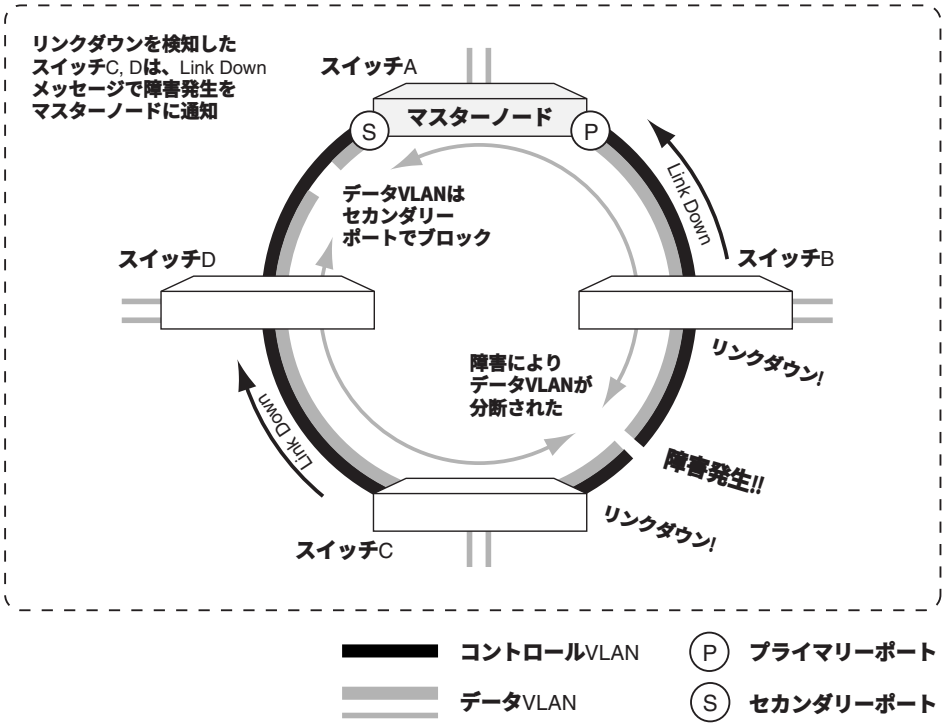
マスターノードは、コントロール VLAN 上において、プライマリーポートから Healthcheck メッセージを定期的に送出します。一定の時間内にセカンダリーポートで Healthcheck メッセージを受信できなかった場合は、リングに障害が発生したと判断します。
マスターノードは、障害発生中も Healthcheck メッセージを送出し続け、セカンダリーポートで再び受信できるようになると、リングが障害から回復したと判断します。



Link Down メッセージ

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

メッセージがタイムアウトしたときと同様のアクションをとります。



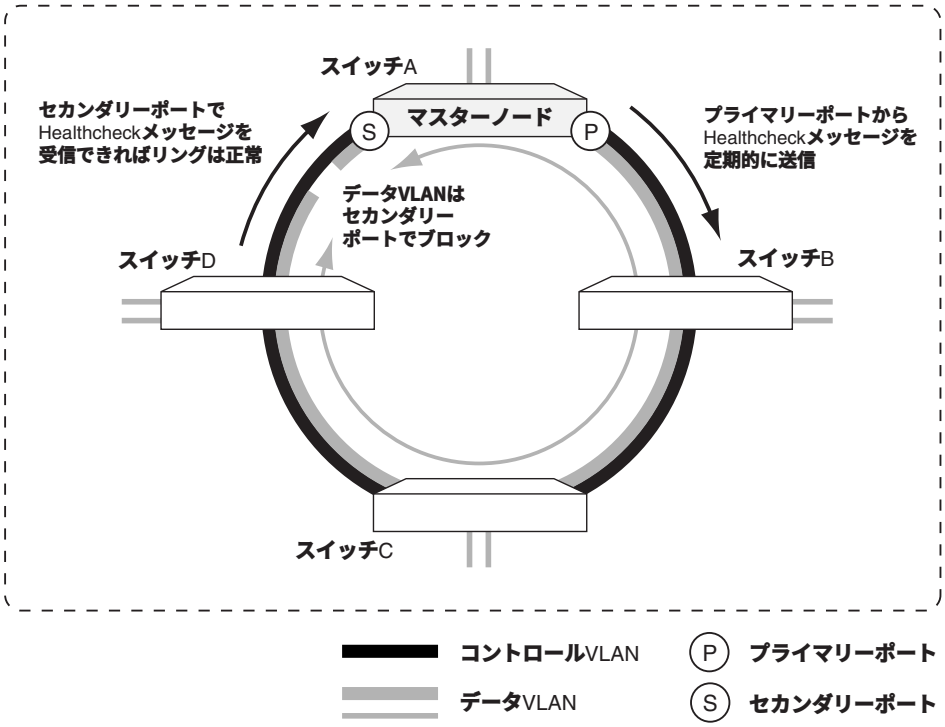
✎ トランジットノードがスヌーピング機能にのみ対応している場合は、Link Down メッセージの送出は行いません。

基本動作

次に、EPSR の基本的な動作について説明します。

正常動作時

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

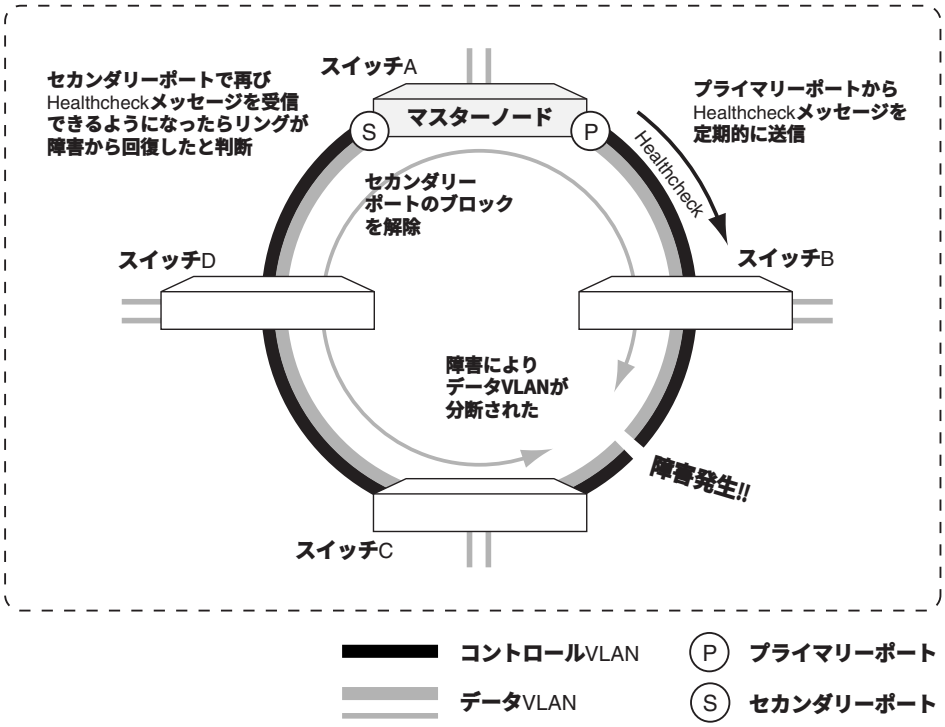


障害発生時

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

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

さらに、マスターノードは Ring Down メッセージをすべてのノードに送信して、FDB をクリアするよう指示します。これにより、リング上での通信が回復します。



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

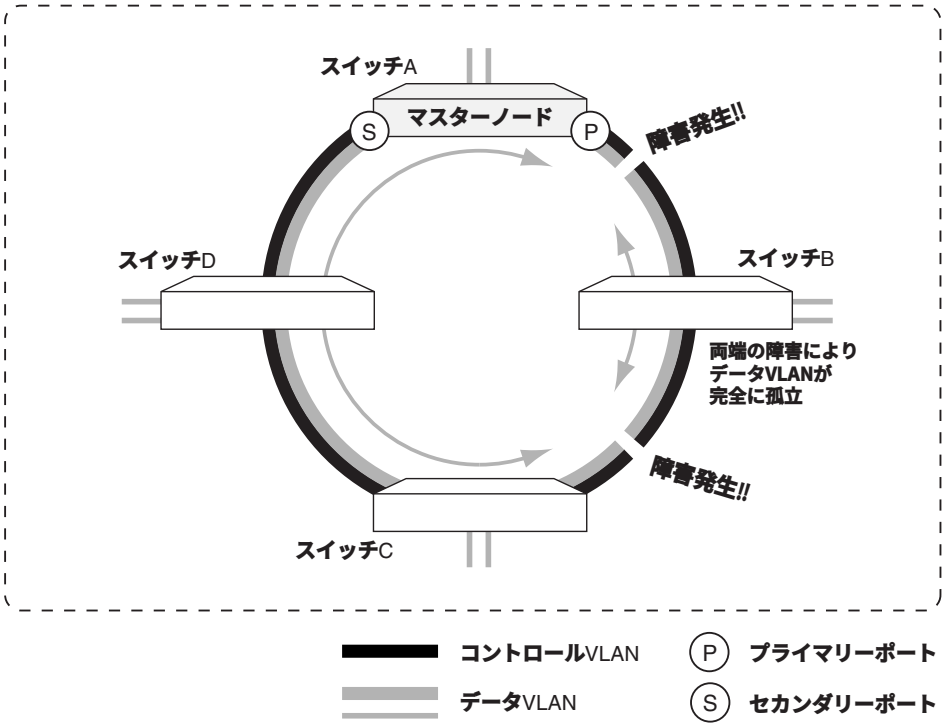
障害回復時

障害が回復すると、マスターノードはセカンダリーポートで再び Healthcheck メッセージを受信できるようになります。
この場合、マスターノードはリングを「Complete」状態に復帰させ、データ VLAN に対してセカンダリーポートを再度ブロックします。また FDB をクリアして MAC アドレスを再学習します。
さらに、マスターノードは Ring Up メッセージをすべてのノードに送信して、FDB をクリアするよう指示します。これにより、リング上での通信が正常時の動作に回復します。
なお、障害発生箇所に接続されているトランジットノードは、リング接続用ポートのリンクアップにより障害の回復を検知できますが、このとき、回復したポートをデータ VLAN に対してただちにフォワーディング状態に戻すとループが起こる可能性があるため、該当ポートを一時的にプリフォワーディング状態に遷移させ、マスターノードから Ring Up メッセージが届くのを待って、FDB をクリアし、該当ポートをフォワーディング状態に戻します。
アウェア機能、またはスヌーピング機能にのみ対応したトランジットノードでは、プリフォワーディング状態でもポートはブロックされず、ただちに通信を再開します。

Double Fail への対応

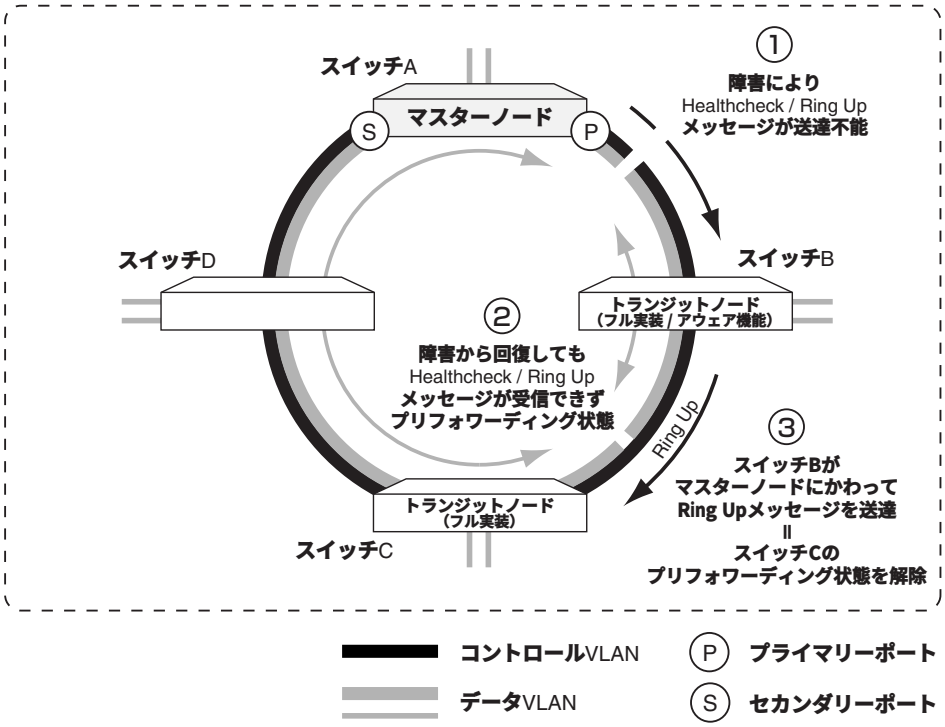
あるノードの両端のリンクに障害が発生している状態を Double Fail と呼びます。
下図のように、Double Fail が発生したノードであるスイッチ B の下流側（マスターノードのセカンダリー

ポートに近い側）のリンクが回復した場合、回復したリンクの下流ノードにあたるスイッチ C では両方のポートがリンクアップし、プリフォワーディング状態に移行します。



スイッチ C がフル実装のトランジットノードである場合、プリフォワーディング状態に遷移したポートは、上流（マスターノードのプライマリーポートに近い側）のスイッチ B から Ring Up メッセージが届くまでの間、通信をブロックします。

しかし、スイッチ B ではもう一方のポートが依然ダウンしているため、下流のスイッチ C にはマスターノードからの Ring Up メッセージが到達しません。このような場合、スイッチ C は、プリフォワーディング状態からフォワーディング状態に移行できず、スイッチ B-C 間のデータ VLAN のリンクがブロックされたままになります。結果、単純な 1 リンクの障害発生時と同じリンク状態にもかかわらず、スイッチ B の一方はダウン、もう一方はブロックされ、EPSR ドメインから孤立した状態となります。



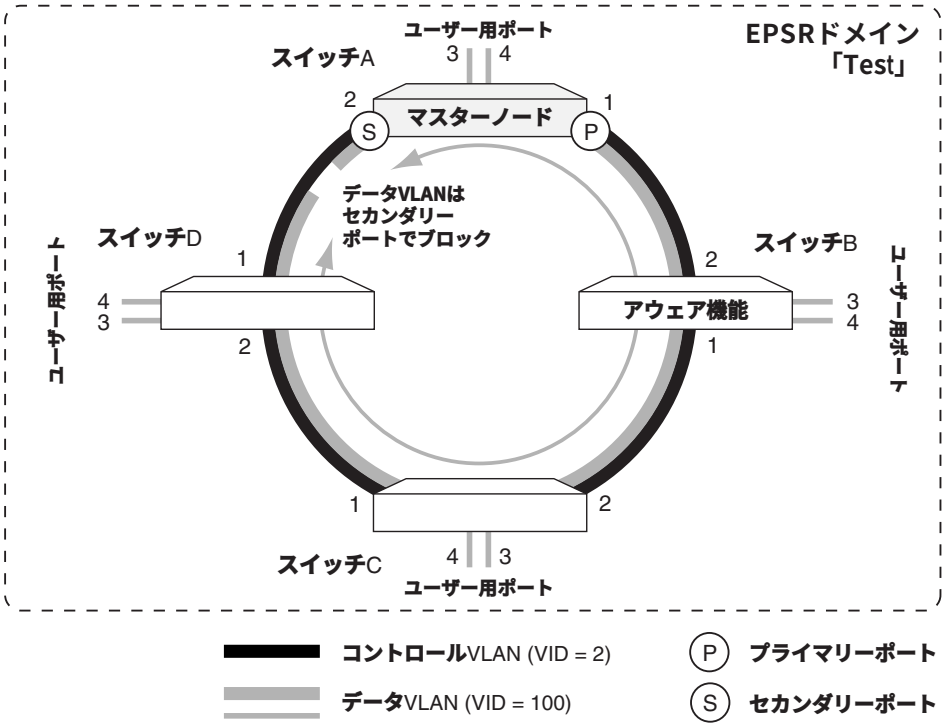
この問題を解決するため、スイッチ B は、片方のポートがリンクアップしてから 4 秒経過してももう一方のポートがリンクアップしない場合、マスターノードの代わりに Ring Up メッセージを送出してスイッチ C をフォワーディング状態に遷移させます。

✎ スイッチ B のトランジットノードがスヌーピング機能にのみ対応している場合は、EPSR 制御メッセージを送出しないため、Double Fail に対応できません。

✎ Double Fail が発生したノードの下流のトランジットノードがアウェア機能、またはスヌーピング機能にのみ対応している場合は、ノード間のリンクが障害から回復した際、ポートはブロックされず、ただちに通信を再開します。

基本設定

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



本製品はアウェア機能にのみ対応していますので、ここではスイッチ B の設定のみ説明します。マスターノードをはじめ、他のノードには、すでに同様の VLAN および EPSR ドメインの設定がされているものとします。

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

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

   ✎ コントロール VLAN には IP アドレスの設定などを行わないでください。コントロール VLAN はリングを構成・制御するためだけに存在する VLAN です。

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

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

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

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

4. EPSR ドメイン「Test」を作成します。動作モードは AWARE を指定します。アウェア機能を持ったトランジットノードでは、コントロール VLAN だけを指定します。

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

5. EPSR ドメイン「Test」のデータ VLAN を指定します。

```
ADD EPSR=Test DATAVLAN=data ↵
```

6. EPSR ドメイン「Test」を有効にします。

```
ENABLE EPSR=Test ↵
```

以上で設定は完了です。

ポート認証

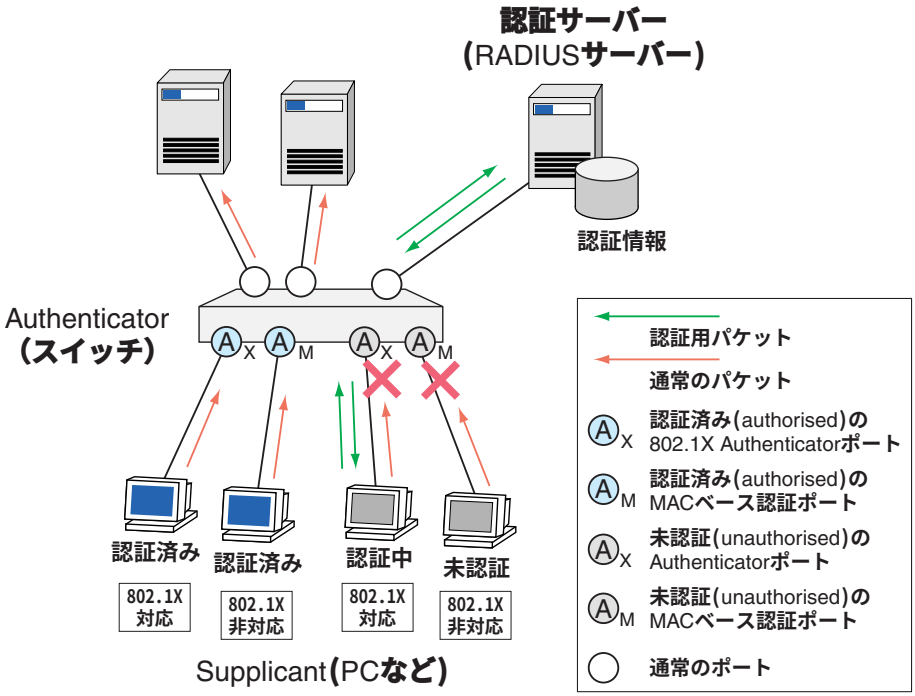
本製品は、スイッチポート単位で LAN 上のユーザーや機器を認証するポート認証機能を実装しています。ポートに接続された機器（および機器を使用するユーザー。以下同様）の認証方法としては、大きく分けて次の 2 種類をサポートしています。

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

802.1X 認証は、EAP（Extensible Authentication Protocol）というプロトコルを使って、ユーザー単位で認証を行うしくみです。802.1X 認証を利用するには、認証する側と認証される側の両方が 802.1X に対応している必要があります。
一方、MAC ベース認証は、機器の MAC アドレスに基づいて機器単位で認証を行うしくみです。認証される側に特殊な機能を必要としないため、802.1X 認証の環境に 802.1X 非対応の機器（例：ネットワークプリンター）を接続したい場合などに利用できます。おもに、802.1X 認証を補完するものとして利用されます。
802.1X および MAC ベースのポート認証機能を使用すれば、スイッチポートに接続された機器を認証し、認証に成功したときだけ同機器からの通信、および、同機器への通信を許可するよう設定できます。また、認証に成功した機器を特定の VLAN にアサインすることも可能です（ダイナミック VLAN）。さらに、本製品は Supplicant 機能にも対応しているため、他の機器から認証を受けるよう設定することもできます。

概要

ポート認証のシステムは、下記の 3 要素から成り立っています。



- Authenticator（認証者）：ポートに接続してきたSupplicant（クライアント）を認証する機器またはソフトウェア。802.1X認証ではEAPメッセージの交換によってSupplicantを認証する（ユーザー認証）。また、MACベース認証ではSupplicantのMACアドレスによって認証を行う（機器認証）。認証に成功した場合はポート経由の通信を許可、失敗した場合はポート経由の通信を拒否する。認証処理そのものは、認証サーバー（RADIUSサーバー）に依頼する（Supplicantの情報を認証サーバーに中継して、認証結果（成功・失敗）を受け取る）。
- 認証サーバー（RADIUSサーバー）：Authenticatorの要求に応じて、Supplicantを認証する機器またはソフトウェア。ユーザー名、パスワード、MACアドレス、所属VLANなどの認証情報を一元管理している。Authenticatorとの間の認証情報の受け渡しにはRADIUSプロトコルを用いる。
- Supplicant（クライアント）：ポートへの接続時にAuthenticatorから認証を受ける機器またはソフトウェア。802.1Xの認証を受けるためには、802.1X Supplicantの機能を備えている必要がある。802.1X Supplicant機能は、一部のOSに標準装備されているほか、単体のクライアントソフトウェアとして用意されていることもある。一方、MACベースの認証を受けるために特殊な機能は必要ない。

本製品の各スイッチポートは、上記のうち、AuthenticatorとSupplicantになることができます（Authenticatorであると同時にSupplicantでもあるような設定も可能）。認証サーバー（RADIUSサーバー）は別途用意する必要があります。

802.1X 認証方式

802.1X認証では、EAP-MD5、EAP-TLS、EAP-TTLS、EAP-PEAPなど様々な認証方式が使用されています。このうち、本製品の802.1X認証モジュールが現在サポートしているEAP認証方式は以下のとおりです。

- Authenticator時：EAP-MD5、EAP-TLS、EAP-TTLS、EAP-PEAP、EAP-OTP(MD4/MD5)
- Supplicant時：EAP-MD5、EAP-TLS、EAP-OTP(MD4/MD5)

基本設定

本製品を使ってポート認証のシステムを運用するための基本的な設定例を示します。以下の例では、メインの認証方式として802.1X認証を使用し、これを補うためにMACベース認証を併用します。

Authenticator

本製品をAuthenticatorとして使用する場合の基本設定を示します。Authenticatorとしての動作には、IPの設定とRADIUSサーバーの指定が必須です。
ここでは、すべてのポートがVLAN defaultに所属していることを前提に、ポート1〜8で802.1X認証を、ポート9〜15でMACベース認証を行うものとします。また、RADIUSサーバーはポート16（通常のポート）に接続されているものとします。

1. 802.1XではRADIUSサーバーを使って認証を行うため、最初にRADIUSサーバーと通信するための設定をします。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認証機能を有効にします。

```
ENABLE PORTAUTH=8021X ↵
```

4. ポート1〜8で802.1X認証を行うよう設定します。「TYPE=AUTHENTICATOR」の指定により、ポート1〜8はAuthenticatorポートとなります。

```
ENABLE PORTAUTH=8021X PORT=1-8 TYPE=AUTHENTICATOR ↵
```

5. MACベース認証機能を有効にします。

```
ENABLE PORTAUTH=MACBASED ↵
```

6. ポート9〜15でMACベース認証を行うよう設定します。

```
ENABLE PORTAUTH=MACBASED PORT=9-15 ↵
```

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

✎ RADIUSサーバーを接続するポートは、Authenticatorポートにしないでください。Authenticatorポートにする場合は、ENABLE PORTAUTH PORTコマンド（96ページ）/SET PORTAUTH PORTコマンド（127ページ）のCONTROLパラメーターをAUTHORISEDに設定してください。

Authenticator（ダイナミックVLAN）

ダイナミックVLAN（Dynamic VLAN Assignemnt）は、RADIUSサーバーから受け取った認証情報に基づいてポートの所属VLANを動的に変更する機能です。802.1X認証、MACベース認証のどちらでも利

用可能です。
以下、本製品を Authenticator として使用し、さらにダイナミック VLAN 機能を利用する場合の基本設定を示します。Authenticator としての動作には、IP の設定と RADIUS サーバーの指定が必須です。
ここでは、利用者機器のために 3 つの VLAN「A」、「B」、「C」を用意します。また、RADIUS サーバーを接続するための VLAN「R」も作成します。各ポートに接続された機器は、認証成功後、RADIUS サーバー側から返された VLAN（「A」、「B」、「C」のどれか）に自動的にアサインされます。
ここでは、ポート 1〜8 で 802.1X 認証を、ポート 9〜15 で MAC ベース認証を行うものとします。また、RADIUS サーバーは、VLAN「R」所属のポート 16（通常のポート）に接続されているものとします。

1. VLAN を作成します。

```
CREATE VLAN=A VID=10 ↵
CREATE VLAN=B VID=20 ↵
CREATE VLAN=C VID=30 ↵
CREATE VLAN=R VID=1000 ↵
```

2. RADIUS サーバーを接続するポート 16 を VLAN「R」に割り当てます。

```
ADD VLAN=R PORT=16 ↵
```

3. 802.1X では RADIUS サーバーを使って認証を行うため、最初に RADIUS サーバーと通信するための設定をします。IP モジュールを有効にし、VLAN「R」に IP アドレスを設定します。

```
ENABLE IP ↵
ADD IP INT=vlan-R IP=192.168.10.5 MASK=255.255.255.0 ↵
```

4. RADIUS サーバーの IP アドレスと UDP ポート、共有パスワードを指定します。

```
ADD RADIUS SERVER=192.168.10.130 PORT=1812 ACCPORT=1813
  SECRET=himitsu ↵
```

5. 802.1X 認証機能を有効にします。

```
ENABLE PORTAUTH=8021X ↵
```

6. ポート 1〜8 で 802.1X 認証を行うよう設定します。「TYPE=AUTHENTICATOR」の指定により、ポート 1〜8 は Authenticator ポートとなります。また、「VLANASSIGNMENT=ENABLED」の指定により、ダイナミック VLAN を有効にします。

```
ENABLE PORTAUTH=8021X PORT=1-8 TYPE=AUTHENTICATOR
  VLANASSIGNMENT=ENABLED ↵
```

7. MAC ベース認証機能を有効にします。

```
ENABLE PORTAUTH=MACBASED ↵
```

8. ポート 9〜15 で MAC ベース認証を行うよう設定します。また、「VLANASSIGNMENT=ENABLED」の指定により、ダイナミック VLAN を有効にします。

```
ENABLE PORTAUTH=MACBASED PORT=9-15 VLANASSIGNMENT=ENABLED ↵
```

✎ 802.1X 認証の Authenticator ポートと MAC ベース認証ポートでは、ポートトランキング、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、802.1X 認証の Authenticator ポートと MAC ベース認証ポートをタグ付きに設定することはできません。

✎ RADIUS サーバーを接続するポートは、Authenticator ポートにしないでください。Authenticator ポートにする場合は、ENABLE PORTAUTH PORT コマンド（96 ページ）/SET PORTAUTH PORT コマンド（127 ページ）の CONTROL パラメーターを AUTHORISED に設定してください。

■ ダイナミック VLAN の動作仕様は次のとおりです。

- Supplicant の認証に失敗した場合、ポートは本来の VLAN（ADD VLAN PORT コマンド（「バーチャル LAN」の 12 ページ）で指定した VLAN）の所属となります。ポート越えの通信は不可能です。
- RADIUS サーバーから有効な VLAN の情報が返ってきた場合、ポートはその VLAN の所属となります。認証に成功すれば、ポート越えの通信も可能です。
- RADIUS サーバーから無効な VLAN の情報が返ってきた場合、ポートは本来の VLAN 所属となります。また、認証も失敗となるため、ポート越えの通信は不可能です。
- RADIUS サーバーから VLAN の情報が返ってこなかった場合、ポートは本来の VLAN 所属となります。認証に成功すれば、ポート越えの通信も可能です。
- 該当ポートまたはシステム全体でポート認証が無効に設定された場合、ポートは本来の VLAN 所属となります。ポート認証が無効なので、ポート越えの通信に関する制限はありません。
- 未認証のポート、および、CONTROL=UNAUTHORISED（未認証固定）または CONTROL=AUTHORISED（認証済み固定）に設定されたポートは、本来の VLAN 所属となります。

■ ポートがダイナミック VLAN にアサインされているときは、ADD VLAN PORT コマンド（「バーチャル LAN」の 12 ページ）で該当ポートの所属 VLAN を変更しても、設定変更は直ちには反映されません。ポートがダイナミック VLAN から本来の VLAN に戻るのは、次のときです。

- 認証済みの Supplicant がいなくなったとき。
- リンクがダウンしたとき。
- ポート上でポート認証が無効にされたとき（DISABLE PORTAUTH PORT コマンド（79 ページ））。
- システム上でポート認証が無効にされたとき（DISABLE PORTAUTH コマンド（78 ページ））。

Supplicant

本製品を 802.1X Supplicant として使用する場合の基本設定を示します。ここでは、ポート 1 が認証を受けるものとします。Supplicant としての動作においては、IP の設定は必須ではありません。

1. 802.1X 認証モジュールを有効にします。

```
ENABLE PORTAUTH=8021X ↵
```

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

```
ENABLE PORTAUTH=8021X PORT=1 TYPE=SUPPLICANT USERNAME=atswitch
  PASSWORD=atpasswd ↵
```

✎ 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。

認証サーバー

ポート認証機能を利用するために必要な認証サーバー（RADIUS サーバー）の設定項目について簡単に説明します。

✎ 認証サーバーの詳細な設定方法については、ご使用のサーバー製品のマニュアルをご参照ください。

- 802.1X 認証において、ダイナミック VLAN を使用しないときは、ユーザーごとに下記の属性を定義してください。

属性名	属性値	備考
User-Name	ユーザー名	認証対象のユーザー名（例：”user1”, ”userB”）
User-Password	パスワード	（EAP-MD5、PEAP(EAP-MSCHAPv2)、TTLS 使用時）ユーザー名に対応するパスワード（例：”dbf8a9hve”, ”h1mi2uDa4o”）。EAP-TLS 使用時は不要（別途、ユーザー電子証明書の用意が必要）

表 7: 802.1X 認証（ダイナミック VLAN なし）

✎ 認証方式として EAP-TLS を使う場合は、RADIUS サーバーの電子証明書と各ユーザーの電子証明書を用意し、各コンピューター上に適切にインストールしておく必要があります。認証方式として EAP-PEAP、EAP-TTLS を使う場合は、RADIUS サーバーの電子証明書を用意し、各コンピューター上に適切にインストールしておく必要があります。詳細は RADIUS サーバーおよび Supplicant（OS や専用ソフトウェアなど）のマニュアルをご参照ください。

- MAC ベース認証において、ダイナミック VLAN を使用しないときは、機器ごとに下記の属性を定義してください。

属性名	属性値	備考
User-Name	MAC アドレス	認証対象機器の MAC アドレス（例：”00-00-f4-11-22-33”）。a〜f は小文字で指定
User-Password	MAC アドレス	認証対象機器の MAC アドレス。User-Name と同じ値を指定すること

表 8: 802.1X 認証（ダイナミック VLAN なし）

- また、802.1X 認証、MAC ベース認証でダイナミック VLAN を使用するときは、前述の諸属性に加え、下記の 3 属性を追加設定してください。

属性名	属性値	備考
Tunnel-Type	VLAN (13)	固定値。指定方法はサーバーに依存
Tunnel-Medium-Type	IEEE-802 (6)	固定値。指定方法はサーバーに依存
Tunnel-Private-Group-ID	VLAN 名か VLAN ID	認証対象のユーザーや機器が認証をパスした後に所属させる VLAN の名前か VLAN ID（例：”sales”, 10）

表 9: ダイナミック VLAN 用の属性

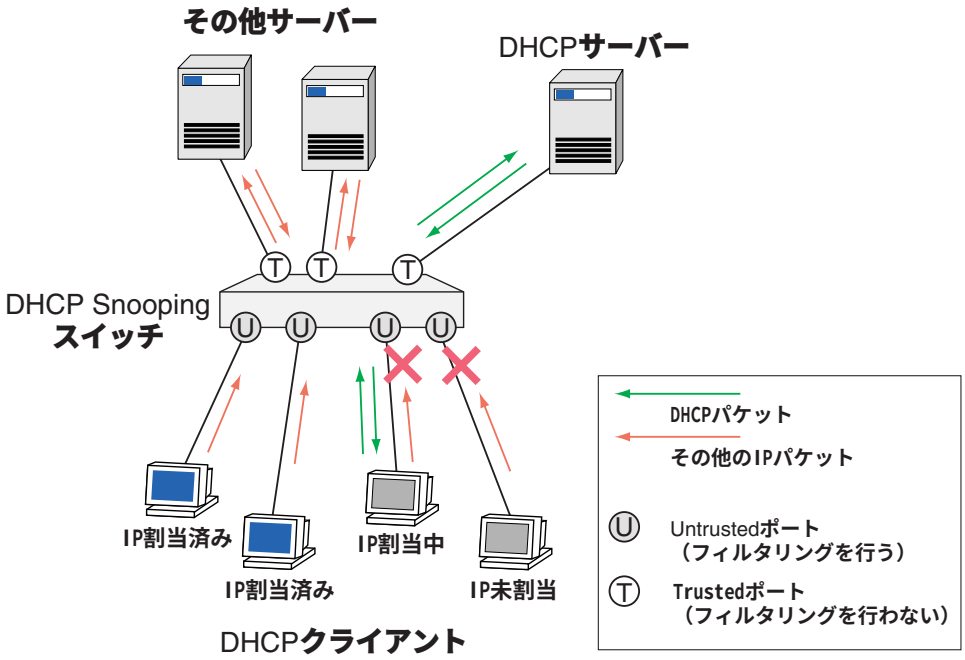
DHCP Snooping

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

- 本機能はレイヤー 2 の機能であるため、IP の設定などをしていなくても使用できます。
- DHCP クライアント機能と DHCP Snooping は併用できません。
- DHCP サーバー機能と DHCP Snooping は併用できません。

概要

DHCP Snooping では、DHCP メッセージのやりとりを監視して DHCP クライアントがどのポート配下に存在するかを追跡し、その情報に基づいて IP パケットのフィルタリングを行います。
DHCP Snooping を利用する場合は、次の図のように本製品を DHCP サーバーと DHCP クライアントの間に配置します。このとき、本製品が DHCP/BOOTP リレーエージェントとして動作していてもかまいません。



DHCP Snooping では、スイッチポートを次の 2 つに分類・設定します。デフォルトではすべてのポートが Untrusted ポートとして設定されています。

- Trusted ポート：DHCP Snooping によるフィルタリングが無効なポート。Trusted ポートでは、パケットに対して特別な処理を行わず、すべてのパケットを通過させます。ネットワーク機器やサーバーのように常時接続で信頼のおける装置を接続するポートは通常 Trusted ポートに設定します。DHCP サーバーを接続するポートも Trusted ポートに設定してください。
- Untrusted ポート：DHCP Snooping によるフィルタリングが有効なポート。Untrusted ポートでは、DHCP サーバーから IP アドレスの割り当てを受けたクライアントからの IP パケットだけを通過させ、その他の IP パケットは破棄します（DHCP のクライアントパケットを除く）。クライアント PC のように不特定多数の必ずしも信頼のおけない装置を接続するポートは Untrusted ポートに設定します（デフォルトではすべてのポートが Untrusted になります）。

DHCP Snooping を有効にすると、本製品は DHCP サーバー・クライアント間で交換される DHCP メッセージを監視するようになります。
Untrusted ポートに接続されているクライアントが DHCP サーバーから IP アドレスの割り当てを受けると、本製品はクライアントの IP アドレスや MAC アドレス、ポート番号などを DHCP Snooping テーブル（バインディングデータベース）に登録します。
Untrusted ポートでは、バインディングデータベースに登録されているクライアントからの IP パケットだけを許可し、その他の IP パケットは破棄します。これにより、不正に接続されたクライアントがポートを越えてネットワークにアクセスすることを防ぐことができます。

✎ デフォルト設定では、Untrusted ポートには DHCP クライアントを 1 台しか接続できません。クライアントを複数接続した場合、最初に IP アドレスを割り当てられたクライアントだけが通信できます。

一方、Trusted ポートでは特別な処理を行いません。Trusted ポートで受信したパケットは（他のフィルタリング機能によって破棄されないかぎり）通常どおり転送されます。

登録できるクライアントの数

8424TX はポート 1〜8、9〜16、17〜24 の 3 つ、8424XL はポート 1〜8、9〜16、17〜24、25、26 の 5 つのブロックごとに、それぞれ最大 100 クライアントまで登録できます。装置全体では、8424TX は最大 300 クライアント、8424XL は最大 500 クライアントまで登録できます。
なお、本機能はハードウェアパケットフィルターと記憶領域を共有しているため、本機能の使用によって、ハードウェアパケットフィルターの最大エントリー数が増減します。

- DHCP Snooping 機能を有効にすると、10/100M ポートのブロック（1〜8、9〜16、17〜24）では 10 エントリー分、1000M ポートのブロック（25、26）では 3 エントリー分のフィルターエントリーを消費します。
- DHCP クライアントを 1 クライアント登録するごとに、1 エントリー分のフィルターエントリーを消費します。

基本設定

DHCP Snooping を使用するための基本的な設定手順は次のとおりです。
ここでは、ポート 1 に DHCP サーバーが接続されており、ポート 2〜24 には不特定多数の DHCP クライアントが接続されるものと仮定します。

1. DHCP Snooping を有効にします。

   ```
   ENABLE DHCPSNOOPING ↵
   ```

2. DHCP サーバーが接続されているポートを Trusted ポートに設定します。

   ```
   SET DHCPSNOOPING PORT=1 TRUSTED=YES ↵
   ```

基本設定は以上です。
デフォルトではすべてのポートが Untrusted ポートに設定されているため、手順 2 で Trusted ポートに設定した DHCP サーバーの接続ポートを除き、他のすべてのポートで IP パケット（DHCP のクライアントパケットを除く）が破棄されます。
Untrusted ポートにおいて、DHCP クライアントが DHCP サーバーから IP アドレスを割り当てられたことを検知すると（DHCPACK をクライアントに転送すると）、そのポートでは該当クライアントからの IP パケットを通過させるようになります。

■ ネットワーク機器やサーバーなど、DHCP Snooping の対象外にしたい装置を接続しているポートは、Trusted ポートに設定します。Trusted ポートでは DHCP Snooping によるフィルタリングが行われず、原則的にすべての受信パケットが転送されます。

✎ DHCP サーバーを接続するポートは Trusted ポートに設定してください。

ポート種別の設定は、SET DHCPSNOOPING PORT コマンド（121 ページ）の TRUSTED パラメーターで行います。たとえば、DHCP サーバーがポート 1 に接続されている場合は、次のようにして該当ポートを Trusted ポートに設定します。

```
SET DHCPSNOOPING PORT=1 TRUSTED=YES ↵
```

■ デフォルト設定では、Untrusted ポートには DHCP クライアントを 1 台しか接続できません。クライアントを複数接続した場合、最初に IP アドレスを割り当てられたクライアントだけが通信できます。
複数のクライアントを接続したい場合は、SET DHCPSNOOPING PORT コマンド（121 ページ）の MAXLEASES パラメーターで接続台数を 1〜100 の範囲で指定します。

```
SET DHCPSNOOPING PORT=1 MAXLEASES=5 ↵
```

■ IP アドレスを固定設定している装置（DHCP クライアント機能を無効化している装置や DHCP クライアント機能を持たない装置など）を Untrusted ポートで利用したい場合は、バインディングデータベースにクライアント情報をスタティック登録します。
クライアントの登録は ADD DHCPSNOOPING BINDING コマンド（56 ページ）で行います。登録には、IP アドレス、MAC アドレス、所属 VLAN、接続ポートの情報が必要です。

```
ADD DHCPSNOOPING BINDING=00-00-00-00-00-01 INTERFACE=vlan-default
  IP=192.168.10.5 PORT=5 ↵
```

✎ デフォルト設定では、ポートあたり 1 つしかスタティックエントリーを登録できません。1 つのポートに複数のスタティックエントリーを登録したいときは、SET DHCPSNOOPING PORT コマンド（121 ページ）の MAXLEASES パラメーターの値を増やす必要があります。

■ DHCP Snooping では、IP パケットだけでなく、ARP パケットに対してもフィルタリングを行うことができます。
ENABLE DHCPSNOOPING ARPSECURITY コマンド（90 ページ）で ARP セキュリティーを有効にすると、Untrusted ポートにおいて、登録済み DHCP クライアントからの ARP パケットだけを他ポートに転送し、その他の ARP パケットは転送せずに破棄するようになります。

```
ENABLE DHCPSNOOPING ARPSECURITY ↵
```

✎ 本機能は、DHCP Snooping が有効になっていないと動作しません。

■ DHCP Snooping では、監視している DHCP メッセージに対して、リレーエージェント情報オプション（オプションコード 82）の付加と削除を行うことも可能です。
ENABLE DHCPSNOOPING OPTION82 コマンド（91 ページ）でリレーエージェント情報オプションの付加・検査・削除を有効にすると、Untrusted ポートに接続されたクライアントからの DHCP/BOOTP パケットを転送するときに、リレーエージェント情報オプションを挿入するようになります。また、サーバーからの戻りパケットを Untrusted ポートに直接接続されたクライアントに転送するときは同オプションを削除するようになります。

```
ENABLE DHCPSNOOPING OPTION82 ↵
```

SET DHCPSNOOPING PORT コマンド（121 ページ）の SUBSCRIBERID パラメーターを利用すれば、リレーエージェント情報オプションに Subscriber-ID サブオプションを含めるかどうか（含めるならばその内容も）をスイッチポートごとに設定することができます。

```
SET DHCPSNOOPING PORT=5 SUBSCRIBERID="ud-mahahiha" ↵
```

✎ 本機能は、DHCP Snooping が有効になっていないと動作しません。

■ DHCP Snooping 有効時は、バインディングデータベースの内容を定期的にチェックして、IP アドレスの使用期限が切れたクライアントの情報をデータベースから削除します。デフォルトのチェック間隔は 60 秒です。

✎ スタティック登録したクライアントの情報は削除されません。

チェック間隔は、SET DHCPSNOOPING CHECKINTERVAL コマンド（119 ページ）で変更できます。有効範囲は 1〜3600 秒です。

```
SET DHCPSNOOPING CHECKINTERVAL=120 ↵
```

また、チェックの際、IP アドレスの使用期限が切れている場合に加えて、クライアントが条件を満たした場合にクライアントの情報をデータベースから削除するよう設定できます。設定には、SET DHCPSNOOPING CHECKOPTIONS コマンド（120 ページ）を使います。

```
SET DHCPSNOOPING CHECKOPTIONS=DHCPRELEASE,LINKDOWN ↵
```

本製品は、バインディングデータベースをチェックするたびに、その時点で有効な（ダイナミック登録された）クライアントの情報を bindings.dsn ファイルに書き込みます。DHCP Snooping を無効から有効に変更したときは、最初にこのファイルを読み込み、その時点でまだ有効なクライアントがあれば、それをバインディングデータベースに登録します。

■ DHCP Snooping の全般的な情報を確認するには、SHOW DHCPSNOOPING コマンド（145 ページ）を使います。

```
SHOW DHCPSNOOPING ↵
```

■ ポートごとの DHCP Snooping 設定を確認するには、SHOW DHCPSNOOPING PORT コマンド（153 ページ）を使います。

```
SHOW DHCPSNOOPING PORT ↵
SHOW DHCPSNOOPING PORT=1 ↵
```

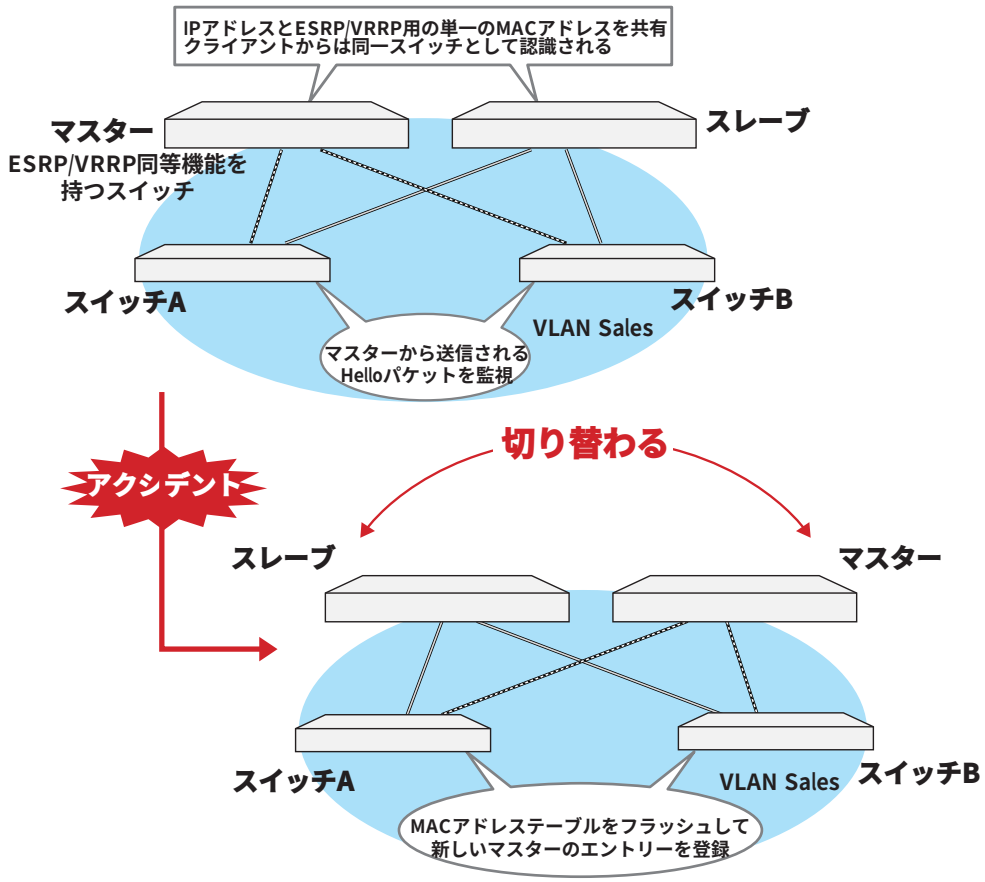
■ バインディングデータベースの内容を確認するには、SHOW DHCPSNOOPING DATABASE コマンド（149 ページ）を使います。

```
SHOW DHCPSNOOPING DATABASE ↵
```

RRP Snooping

RRP Snooping（Router Redundancy Protocol Snooping）は、ESRP/VRRP および同等機能を持つ製品の下位に本製品を配置し、高速な冗長性を実現するための機能です。

ポートに RRP Snooping を設定すると、本製品はマスタールーターから定期的に送信される Hello パケット（VRRP アドバタイズメント・パケット）を VLAN ごとに監視し、どのポートがマスターかを記憶します。マスタールーターに障害が発生して、スレーブに切り替わると、マスタールーターが接続されたポートでの対象 VLAN 所属の MAC アドレスをフラッシュしてスレーブルーターのエントリーがすぐに登録されるようにします。これによって、ESRP/VRRP に対応していないスイッチを下位に接続するよりも、はるかに短い時間で通信を再開することができます。



上記の例は、VLAN Sales 内において、本製品を ESRP イネーブルな 2 台のスイッチに対して、それぞれ RRP Snooping を設定したポートを用いて接続した例です。

2 台のスイッチは互いに ESRP Hello パケット（実際は、規定の送信元 MAC アドレス）を交換し、どちらがマスターになるかを決定します。マスターになったスイッチは VLAN Sales に対してスイッチング（ルーティング）のサービスを提供します。一方、スタンバイ（スレーブ）側のスイッチはまったくパケットの転送を行わず、これによりブリッジループを回避します。

本製品はスイッチの間で交換される ESRP Hello パケットを監視し、マスターの障害発生を検知するとただちに自らの MAC アドレステーブルをフラッシュして、新しいマスターのエントリーがすぐに登録されるよ

うにします。これにより 4 秒程度という高速な切り替えを実現します。
この機能は VRRP（Virtual Router Redundant Protocol）にも対応しています。
本製品がスヌーピングする Hello パケット（VRRP アドバタイズメント・パケット）の送信元 MAC アドレスは下記のとおりです。

- 00:e0:2b:00:00:80～9F (ESRP)
- 00:a0:d2:eb:ff:80
- 00:00:5e:00:01:00～FF (VRRP)

上記の例は 1 つの VLAN に対する多重化の例ですが、複数の VLAN に対して RRP Snooping を設定することも可能です。

■ RRP Snooping を有効にするには、ENABLE RRPSNOOPING コマンド（100 ページ）を使います。

```
ENABLE RRPSNOOPING ↵
```

■ RRP Snooping を無効にするには、DISABLE RRPSNOOPING コマンド（80 ページ）を使います。

```
DISABLE RRPSNOOPING ↵
```

■ RRP Snooping に関する設定を表示するには、SHOW RRPSNOOPING コマンド（186 ページ）を使います。

```
SHOW RRPSNOOPING ↵
```

RRP Snooping を有効にすると、学習機能により登録されていた Hello パケット（VRRP アドバタイズメント・パケット）の送信元 MAC アドレスは、フォワーディングデータベースから削除されます。

✎ ポートセキュリティーが有効なポート、または、Authenticator/Supplicant ポートでは RRP Snooping 機能は無効です。

✎ ミラーリング設定のミラーポートでは RRP Snooping 機能は無効です。

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

ポート

DHCP Snooping

RRP Snooping

ACTIVATE PORTAUTH PORT REAUTHENTICATE

カテゴリー：スイッチング / ポート認証

ACTIVATE PORTAUTH[={8021X|MACBASED}] **PORT=**{***port-list***|**ALL**} **REAUTHENTICATE**
[SUPPLICANTMAC=*macadd*]

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）
macadd: MAC アドレス（xx-xx-xx-xx-xx-xx の形式）

解説

指定ポートにおいて、Supplicant を再認証する。

パラメーター

PORTAUTH　認証メカニズム。8021X（802.1X 認証）、MACBASED（MAC ベース認証）から選択する。省略時は 8021X と見なされる。

PORT　ポート番号。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。

SUPPLICANTMAC　スイッチポートが Multi-Supplicant モードに設定されている場合、対象 Supplicant の MAC アドレスを指定する。

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（95 ページ）
ENABLE PORTAUTH PORT（96 ページ）
SHOW PORTAUTH MULTISUPPLICANT PORT（173 ページ）
SHOW PORTAUTH PORT（177 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 アドレスを持つフレームを受信した場合は、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。
SET SWITCH PORT コマンドの LEARN パラメーターに NONE を指定することでポートロックは解除される。

パラメーター

PORT　ポート番号。複数指定が可能。

入力・出力・画面例

```
Manager > set switch port=1 learn=10 intrusionaction=discard

Info (1087003): Operation successful.

Manager > ACTIVATE SWITCH PORT=1 LOCK

Info (1087003): Operation successful.
```

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 NONE 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（138 ページ）
SHOW SWITCH PORT（194 ページ）

ADD DHCPSNOOPING BINDING

カテゴリー：スイッチング / DHCP Snooping

ADD DHCPSNOOPING BINDING=*macadd* INTERFACE=*vlan-if* IP=*ipadd*
PORT=*port-number*

macadd: MAC アドレス（xx-xx-xx-xx-xx-xx の形式）
vlan-if: VLAN インターフェース（VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID）
ipadd: IP アドレス
port-number: スイッチポート番号（1〜）

解説

DHCP Snooping テーブル（バインディングデータベース）にスタティックエントリー（IP アドレスを固定的に設定しているクライアントの情報）を追加する。

パラメーター

BINDING　クライアントの MAC アドレス
INTERFACE　クライアントの所属 VLAN
IP　クライアントの IP アドレス
PORT　クライアントが接続されているスイッチポート

例

■IP アドレス 192.168.10.5、MAC アドレス 00-00-00-00-00-01 のクライアントをバインディングデータベースにスタティック登録する。所属 VLAN は「default」、接続するスイッチポートは 5 とする。

```
ADD DHCPSNOOPING BINDING=00-00-00-00-00-01 INTERFACE=vlan-default
  IP=192.168.10.5 PORT=5
```

備考・注意事項

デフォルト設定では、ポートあたり 1 つしかスタティックエントリーを登録できない。1 つのポートに複数のスタティックエントリーを登録したいときは、SET DHCPSNOOPING PORT コマンドの MAXLEASES パラメーターの値を増やす必要がある。

関連コマンド

DELETE DHCPSNOOPING BINDING（66 ページ）
DISABLE DHCPSNOOPING ARPSECURITY（73 ページ）

SET DHCPSNOOPING PORT（121 ページ）
SHOW DHCPSNOOPING DATABASE（149 ページ）

ADD EPSR DATAVLAN

カテゴリー：スイッチング / EPSR アウェア

ADD EPSR=*epsrname* DATAVLAN={***vlanname***|***1..4094***}

epsrname: EPSR ドメイン名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。大文字小文字を区別しない）
vlanname: VLAN 名（1〜32 文字。英数字とアンダースコア（_）、ハイフンを使用可能。大文字小文字は区別しない）

解説

EPSR ドメインにデータ VLAN（保護対象の VLAN）を追加する。
本コマンド実行時は、次のルールが適用される。
・1 つの EPSR ドメインに追加できるデータ VLAN の数は 512 個まで
・データ VLAN、コントロール VLAN を問わず、追加対象の EPSR ドメインにすでに追加されている VLAN は指定できない
・他の EPSR ドメインにコントロール VLAN として追加されている VLAN は指定できない
・他の EPSR ドメインにデータ VLAN として追加されている VLAN を指定するときは、リング接続用のポートが EPSR ドメイン間で重複しないようにする必要がある
・EPSR ドメインに VLAN を追加するとき、あらかじめ VLAN にメンバーポートを割り当てておく必要はない（ループを避ける意味ではそのほうが望ましい場合もある）

パラメーター

EPSR　EPSR ドメイン名
DATAVLAN　データ VLAN。VLAN 名または VLAN ID（VID）で指定する。

例

■EPSR ドメイン「blues」に VLAN skyblue をデータ VLAN として追加する。

```
ADD EPSR=blues DATAVLAN=skyblue
```

関連コマンド

CREATE EPSR（62 ページ）
CREATE VLAN（「バーチャル LAN」の 14 ページ）
DELETE EPSR DATAVLAN（67 ページ）
SHOW EPSR（155 ページ）

ADD LACP PORT

カテゴリー：スイッチング / LACP（IEEE 802.3ad）

ADD LACP PORT={***port-list***|**ALL**} [ADMINKEY=*0..65535*] [PRIORITY=*0..65535*]
[MODE={ACTIVE|PASSIVE}] [PERIODIC={FAST|SLOW}]

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）

解説

指定したスイッチポートを LACP の管理下に置く（該当ポートで LACP を有効にする）。
ただし、手動設定したトランクポート（CREATE SWITCH TRUNK コマンド、ADD SWITCH TRUNK コマンド）と Half Duplex で動作しているポートでは LACP を使用できないため、これらのポートは（本コマンドで指定したとしても）自動的に LACP の管理下から外される。
なお、デフォルトでは、すべてのスイッチポートが LACP の管理下に置かれている。

パラメーター

PORT　ポート番号。

ADMINKEY　LACP ポート鍵の元となる値を指定する（ポート鍵の値そのものではない）。LACP では、対向機器、所属 VLAN、通信速度、ポート鍵のすべてが等しいポート群で 1 つのトランクグループを構成する。したがって、本来なら 1 つのトランクグループを構成するポート群を複数のグループに分けたい場合は、グループごとに異なる ADMINKEY を設定すればよい。なお、ADMINKEY は自機内でのみ意味を持つ（対向機器と同じに設定する必要はない）。デフォルトは 1。

PRIORITY　LACP ポートプライオリティー。小さいほど優先度が高い。使用可能な LACP ポートの数がトランクグループの最大ポート数（8 ポート）よりも多い場合、本パラメーターの小さいポートほどメンバーに選ばれる可能性が高くなる。なお、ポートプライオリティーが等しい場合は、ポート番号の小さいほうが優先的に使用される。また、メンバーに選ばれなかったポートはスタンバイ状態となり、現行のメンバーポートがリンクダウンするときに備えて待機する。デフォルトは 32768。

MODE　LACP ポートの動作モード。ACTIVE（PERIODIC パラメーターで設定した間隔で LACP パケットを自発的に送信する）、PASSIVE（対向ポートから LACP パケットを受信したときだけ LACP パケットを送信する）から選択する。デフォルトは ACTIVE。

PERIODIC　ACTIVE モード時の LACP パケットの送信間隔。FAST（1 秒）、SLOW（30 秒）から選択する。デフォルトは FAST。

例

■ポート 1〜4 を LACP の管理下に置く。

```
ADD LACP PORT=1-4
```

関連コマンド

DELETE LACP PORT（68 ページ）
SET LACP PORT（125 ページ）
SHOW LACP PORT（162 ページ）

ADD SWITCH TRUNK

カテゴリー：スイッチング / ポート

ADD SWITCH TRUNK=*trunk* PORT=*port-list*

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

解説

既存のトランクグループにポートを追加する。

パラメーター

TRUNK　トランクグループ名
PORT　ポート番号。複数指定が可能。トランクグループには、最大 8 ポートまで所属可能。ミラーポートをトランクグループに参加させることはできない。トランクポートは同一 VLAN に所属している必要がある。

例

■トランクグループ「uplink」にポート 1〜4 を追加する。

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

備考・注意事項

トランクポートを MDI/MDI-X 自動切替無効に設定できない。ただし、MDI/MDI-X 自動切替無効のポートをトランクグループに追加することは可能。

関連コマンド

CREATE SWITCH TRUNK（64 ページ）
DELETE SWITCH TRUNK（69 ページ）
DESTROY SWITCH TRUNK（71 ページ）
SET SWITCH TRUNK（143 ページ）
SHOW SWITCH TRUNK（206 ページ）

CREATE EPSR

カテゴリー：スイッチング / EPSR アウェア

CREATE EPSR=*epsrname* MODE=AWARE CONTROLVLAN={*vlanname*|*1..4094*}

epsrname: EPSR ドメイン名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。ただし、「ALL」は指定できない。大文字小文字を区別しない）
vlanname: VLAN 名（1〜32 文字。英数字とアンダースコア（_）、ハイフンを使用可能。大文字小文字は区別しない）

解説

EPSR ドメインを作成する。
本コマンド実行時は、次のルールが適用される。
・1 台のスイッチ上に作成できる EPSR ドメインは最大 16 個
・コントロール VLAN の所属ポートはちょうど 2 ポートでなくてはならない（ただし、トランクグループは全体で 1 ポートと見なす）。また、これらのポートはタグ付き設定でなくてはならない。
・データ VLAN、コントロール VLAN を問わず、他の EPSR ドメインに追加されている VLAN はコントロール VLAN として指定できない
・トランクポートは、グループ内のポートが 1 つでもリンクアップしていれば全体としてリンクアップのステータスとなる。また、SNMP トラップでトランクポートのポート番号を通知するときは、トランクグループ内でポート番号のもっとも小さいポートの番号が使われる。
・LACP、スパニングツリープロトコル（STP/RSTP）、ダイナミック VLAN（ポート認証）が有効なポートは EPSR ドメインに追加できない。

パラメーター

EPSR　EPSR ドメイン名
MODE　EPSR ドメインにおける役割。AWARE（アウェア機能を持つトランジットノード）のみ。
CONTROLVLAN　コントロール VLAN。VLAN 名または VLAN ID（VID）で指定する。

例

■EPSR ドメイン「blues」を作成し、アウェア機能を持つトランジットノードとして動作するよう設定する。コントロール VLAN には VLAN「blues_control」を指定する。

```
CREATE EPSR=blues MODE=AWARE CONTROLVLAN=blues_control
```

備考・注意事項

EPSR が使用するスイッチポートでは、自動的にイングレスフィルタリング（SET SWITCH PORT コマン

ドの INFILTERING パラメーター）が有効になる。同パラメーターは、EPSR ドメインを削除して該当ポートを EPSR で使用されないようにするまで変更できない。
コントロール VLAN にはレイヤー 3 以上の設定（IP アドレスの設定など）を行わないこと（コントロール VLAN はリングを構成・制御するためだけに存在する）。
EPSR ドメインの状態変化を知らせる SNMP トラップを利用するためには、SNMPv2c のトラップホストまたは SNMPv3 のターゲットを設定する必要がある。SNMPv1 トラップホストの設定だけでは、EPSR の SNMP トラップは利用できないので注意。

関連コマンド

ADD EPSR DATAVLAN（58 ページ）
CREATE VLAN（「バーチャル LAN」の 14 ページ）
DESTROY EPSR（70 ページ）
ENABLE EPSR（92 ページ）
SHOW EPSR（155 ページ）

CREATE SWITCH TRUNK

カテゴリー：スイッチング / ポート

CREATE SWITCH TRUNK=*trunk* [PORT=*port-list*] [SELECT={MACSRC|MACDEST|MACBOTH|IPSRC|IPDEST|IPBOTH}] [SPEED={10M|100M|1000M}] [THRASHACTION={NONE|LEARNDISABLE|PORTDISABLE|VLANDISABLE|LINKDOWN}] [THRASHTIMEOUT={NONE|*1..86400*}] [LOOPACTION={PORTDISABLE|VLANDISABLE|LINKDOWN|LOGONLY|NONE}] [BLOCKTIMEOUT={NONE|*1..86400*}]

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

解説

トランクグループを作成する。6 グループまで作成可能。

パラメーター

TRUNK　トランクグループ名

PORT　トランクに所属するポートの一覧。グループあたりの最大ポート数は 8。他のトランクグループに所属するポートやミラーポートは追加できない。また、トランクポートは同じ VLAN に所属していなくてはならない。

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

SPEED　トランクポートの通信速度。トランクグループに参加したポートは、ここで指定した速度のオートネゴシエーション（AUTONEGOTIATE）となる。デフォルトは 100M。実際の通信速度は 10M に設定した場合は 10MFULL Autonegotiate、100M に設定した場合は 100MFULL Autonegotiate、1000M に設定した場合は 1000MFULL Autonegotiate で動作する。

THRASHACTION　該当トランクグループで MAC アドレススラッシング（同一 MAC アドレスの登録ポートが頻繁に変更されること）を検出した場合の動作。NONE（なにもしない）、LEARNDISABLE（トランクグループ内の全ポートで MAC アドレスの学習を停止する）、PORTDISABLE（トランクグループ内の全ポートをディセーブルにする）、VLANDISABLE（スラッシングが発生した VLAN に対してのみトランクグループ内の全ポートをディセーブルにする）、LINKDOWN（トランクグループ内の全ポートを物理的にリンクダウンさせる）から選択する。これらの動作は、THRASHTIMEOUT パラメーターで指定した時間が経過すると終了する（通常のポート動作に戻る）。ただし、PORTDISABLE、LINKDOWN の場合は、ENABLE SWITCH PORT コマンドにより手動で動作を終了させられる。また、VLANDISABLE の場合は、ENABLE SWITCH PORT VLAN コマンドにより手動で動作を終了させられる。LINKDOWN は 10/100Mbps ポートのみリンクダウンさせる。拡張モジュールに

対してはポートをディセーブルにするのみ。デフォルトは LEARNDISABLE。

THRASHTIMEOUT　MAC アドレススラッシング検出時の動作の持続時間（秒）。NONE は無期限を示す。THRASHACTION パラメーターに LEARNDISABLE を指定している場合、本パラメーターを NONE に変更することはできない。また、本パラメーターを NONE に設定している状態で、THRASHACTION パラメーターの値を LEARNDISABLE に変更した場合、本パラメーターの値は自動的に 1 に変更される。デフォルトは 1 秒。

LOOPACTION　該当トランクグループでループを検出した場合の動作。PORTDISABLE（トランクグループ内の全ポートをディセーブルにする）、VLANDISABLE（ループが発生した VLAN に対してのみトランクグループ内の全ポートをディセーブルにする）、LINKDOWN（トランクグループ内の全ポートを物理的にリンクダウンさせる）、LOGONLY（ポートの制御は行わず、ログへの記録と SNMP トラップの送信のみを行う）、NONE（動作を行わず、LDF の送受信およびカウンター処理のみを行う）のいずれか。これらの動作は、BLOCKTIMEOUT パラメーターで指定した時間が経過すると終了する（通常のポート動作に戻る）。PORTDISABLE または LINKDOWN の場合は、ENABLE SWITCH PORT コマンドにより手動で動作を終了させられる。また、VLANDISABLE の場合は、ENABLE SWITCH PORT VLAN コマンドにより手動で動作を終了させられる。LINKDOWN は 10/100Mbps ポートのみリンクダウンさせる。拡張モジュールに対してはポートをディセーブルにするのみ。デフォルトは PORTDISABLE。

BLOCKTIMEOUT　対象トランクグループで LDF 検出機能がループを検出した場合の動作の持続時間（秒）。NONE は無期限を示す。デフォルトは 7。

例

■トランクグループ「uplink」を作成する。通信速度は 100M とする。

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

備考・注意事項

THRASHACTION/LOOPACTION パラメーターの値を VLANDISABLE に変更すると、トランクグループ内の全ポートで自動的にイングレスフィルタリング（SET SWITCH PORT コマンドの INFILTERING パラメーター）が有効になる。また、VLANDISABLE からそれ以外に変更すると、イングレスフィルタリングが無効になる。

関連コマンド

ADD SWITCH TRUNK（61 ページ）
DELETE SWITCH TRUNK（69 ページ）
DESTROY SWITCH TRUNK（71 ページ）
SET SWITCH TRUNK（143 ページ）
SHOW SWITCH TRUNK（206 ページ）

DELETE DHCPSNOOPING BINDING

カテゴリー：スイッチング / DHCP Snooping

DELETE DHCPSNOOPING BINDING=*macadd*

macadd: MAC アドレス（xx-xx-xx-xx-xx-xx の形式）

解説

DHCP Snooping テーブル（バインディングデータベース）からスタティックエントリー（IP アドレスを固定的に設定しているクライアントの情報）を削除する。

パラメーター

BINDING　クライアントの MAC アドレス

関連コマンド

ADD DHCPSNOOPING BINDING（56 ページ）
SHOW DHCPSNOOPING DATABASE（149 ページ）

DELETE EPSR DATAVLAN

カテゴリー：スイッチング / EPSR アウェア

DELETE EPSR=*epsrname* DATAVLAN={***vlanname***|***1..4094***|**ALL**}**

epsrname: EPSR ドメイン名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。大文字小文字を区別しない）
vlanname: VLAN 名（1〜32 文字。英数字とアンダースコア（_）、ハイフンを使用可能。大文字小文字は区別しない）

解説

EPSR ドメインからデータ VLAN を削除する。
本コマンドを実行する前には、次のいずれかの手順をとる必要がある。
・DISABLE SWITCH PORT コマンドで該当 VLAN のリング接続用ポートをディセーブルにする
・該当 VLAN のリング接続用ポートからケーブルを抜く

パラメーター

EPSR　EPSR ドメイン名
DATAVLAN　データ VLAN。VLAN 名または VLAN ID（VID）で指定する。ALL を指定した場合は該当 EPSR ドメインに所属しているすべてのデータ VLAN が対象となる。

関連コマンド

ADD EPSR DATAVLAN（58 ページ）
CREATE EPSR（62 ページ）
DELETE VLAN PORT（「バーチャル LAN」の 16 ページ）
DISABLE SWITCH PORT（83 ページ）
SHOW EPSR（155 ページ）

DELETE LACP PORT

カテゴリー：スイッチング / LACP（IEEE 802.3ad）

DELETE LACP PORT=*port-list*

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）

解説

指定したスイッチポートを LACP の管理下から除外する（該当ポートで LACP を無効にする）。
なお、デフォルトでは、すべてのスイッチポートが LACP の管理下に置かれている。

パラメーター

PORT　ポート番号。

例

■ポート 4 を LACP の管理下から外す。

```
DELETE LACP PORT=4
```

関連コマンド

ADD LACP PORT（59 ページ）
SET LACP PORT（125 ページ）
SHOW LACP PORT（162 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（61 ページ）
CREATE SWITCH TRUNK（64 ページ）
DESTROY SWITCH TRUNK（71 ページ）
SET SWITCH TRUNK（143 ページ）
SHOW SWITCH TRUNK（206 ページ）

DESTROY EPSR

カテゴリー：スイッチング / EPSR アウェア

DESTROY EPSR={***epsrname***|**ALL**}

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

解説

EPSR ドメインを削除する。
本コマンドを実行する前には、次のいずれかの手順をとる必要がある。
・DISABLE SWITCH PORT コマンドで該当 VLAN のリング接続用ポートをディセーブルにする
・該当 VLAN のリング接続用ポートからケーブルを抜く

パラメーター

EPSR　EPSR ドメイン名。ALL を指定した場合は、すべての EPSR ドメインが対象となる。

備考・注意事項

EPSR が使用するスイッチポートでは、自動的にイングレスフィルタリング（SET SWITCH PORT コマンドの INFILTERING パラメーター）が有効になる。その反対に、EPSR ドメインを削除すると、EPSR で使用されなくなったスイッチポートでは、自動的にイングレスフィルタリングが無効になる。

関連コマンド

CREATE EPSR（62 ページ）
DELETE EPSR DATAVLAN（67 ページ）
DELETE VLAN PORT（「バーチャル LAN」の 16 ページ）
DISABLE EPSR（75 ページ）
DISABLE SWITCH PORT（83 ページ）
SHOW EPSR（155 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（61 ページ）
CREATE SWITCH TRUNK（64 ページ）
DELETE SWITCH TRUNK（69 ページ）
SET SWITCH TRUNK（143 ページ）
SHOW SWITCH TRUNK（206 ページ）

DISABLE DHCPSNOOPING

カテゴリー：スイッチング / DHCP Snooping

DISABLE DHCPSNOOPING

解説

DHCP Snooping を無効にする。デフォルトは無効。

関連コマンド

ENABLE DHCPSNOOPING（89 ページ）
SHOW DHCPSNOOPING（145 ページ）

DISABLE DHCPSNOOPING ARPSECURITY

カテゴリー：スイッチング / DHCP Snooping

DISABLE DHCPSNOOPING ARPSECURITY

解説

DHCP Snooping のオプション機能である ARP セキュリティーを無効にする。デフォルトは無効。

関連コマンド

ENABLE DHCPSNOOPING（89 ページ）
ENABLE DHCPSNOOPING ARPSECURITY（90 ページ）
SHOW DHCPSNOOPING（145 ページ）

DISABLE DHCPSNOOPING OPTION82

カテゴリー：スイッチング / DHCP Snooping

DISABLE DHCPSNOOPING OPTION82

解説

DHCP Snooping のオプション機能であるリレーエージェント情報オプション（オプションコード 82）の処理機能を無効にする。デフォルトは無効。

関連コマンド

ENABLE DHCPSNOOPING（89 ページ）
SHOW DHCPSNOOPING（145 ページ）

DISABLE EPSR

カテゴリー：スイッチング / EPSR アウェア

DISABLE EPSR={***epsrname***|**ALL**}

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

解説

EPSR ドメインを無効化する。
本コマンドを実行する前には、次のいずれかの手順をとる必要がある。
・DISABLE SWITCH PORT コマンドで該当 VLAN のリング接続用ポートをディセーブルにする
・該当 VLAN のリング接続用ポートからケーブルを抜く

パラメーター

EPSR　EPSR ドメイン名。ALL を指定した場合は、すべての EPSR ドメインが対象となる。

関連コマンド

CREATE EPSR（62 ページ）
DELETE VLAN PORT（「バーチャル LAN」の 16 ページ）
DISABLE SWITCH PORT（83 ページ）
ENABLE EPSR（92 ページ）
SHOW EPSR（155 ページ）

DISABLE EPSR DEBUG

カテゴリー：スイッチング / EPSR アウェア

DISABLE EPSR={***epsrname***|**ALL**} **DEBUG=**{**INFO**|**MSG**|**PKT**|**STATE**|**ALL**}

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

解説

EPSR ドメインのデバッグオプションを無効化する。デフォルトはすべて無効。

パラメーター

EPSR　EPSR ドメイン名。ALL を指定した場合は、すべての EPSR ドメインが対象となる。

DEBUG　無効にするデバッグオプション。INFO（EPSR に関する全般的情報を表示）、MSG（EPSR パケットをデコードして表示）、PKT（EPSR パケットを ASCII 表示）、STATE（EPSR の状態遷移を表示）、ALL（すべてのオプション）から選択する。

関連コマンド

CREATE EPSR（62 ページ）
ENABLE EPSR DEBUG（93 ページ）
SHOW EPSR DEBUG（159 ページ）

DISABLE LACP

カテゴリー：スイッチング / LACP（IEEE 802.3ad）

DISABLE LACP

解説

LACP モジュールを無効にする。デフォルトは無効。
LACP を無効にしても、各ポートの LACP 関連設定は保持される。

関連コマンド

ENABLE LACP（94 ページ）
SHOW LACP（160 ページ）

DISABLE PORTAUTH

カテゴリー：スイッチング / ポート認証

DISABLE PORTAUTH[={8021X|MACBASED}]

解説

ポート認証機能（802.1X 認証または MAC ベース認証）を無効にする。デフォルトはどちらとも無効。

パラメーター

PORTAUTH　認証メカニズム。8021X（802.1X 認証）、MACBASED（MAC ベース認証）から選択する。省略時は 8021X と見なされる。

関連コマンド

DISABLE PORTAUTH PORT（79 ページ）
ENABLE PORTAUTH（95 ページ）
ENABLE PORTAUTH PORT（96 ページ）
SHOW PORTAUTH MULTISUPPLICANT PORT（173 ページ）
SHOW PORTAUTH PORT（177 ページ）

DISABLE PORTAUTH PORT

カテゴリー：スイッチング / ポート認証

DISABLE PORTAUTH[=8021X|MACBASED] **PORT=**{***port-list***|**ALL**}

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）

解説

指定ポートで、ポート認証機能（802.1X 認証または MAC ベース認証）を無効にする。デフォルトは全ポート無効。

パラメーター

PORTAUTH　認証メカニズム。8021X（802.1X 認証）、MACBASED（MAC ベース認証）から選択する。省略時は 8021X と見なされる。

PORT　スイッチポート。複数指定が可能。

関連コマンド

DISABLE PORTAUTH（78 ページ）
ENABLE PORTAUTH（95 ページ）
ENABLE PORTAUTH PORT（96 ページ）
SHOW PORTAUTH PORT（177 ページ）

DISABLE RRPSNOOPING

カテゴリー：スイッチング / RRP Snooping

DISABLE RRPSNOOPING

解説

RRP Snooping を無効にする。デフォルトは無効。

関連コマンド

ENABLE RRPSNOOPING（100 ページ）
SHOW RRPSNOOPING（186 ページ）

DISABLE SWITCH LOOPDETECTION

カテゴリー：スイッチング / ポート

DISABLE SWITCH LOOPDETECTION 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

LDF 検出機能を無効にする。デフォルトは無効

パラメーター

PORT　ポート番号または ALL を指定する

例

■ポート 2 の LDF 検出機能を無効にする

```
DISABLE SWITCH LOOPDETECTION PORT=2
```

備考・注意事項

すべてのポートで機能を無効にした場合、ハードウェアパケットフィルターから登録を解除した旨のメッセージ「INFO: LDF is inactive, L3FILT is deleted」が表示される。

関連コマンド

ENABLE SWITCH LOOPDETECTION（101 ページ）
RESET SWITCH LOOPDETECTION COUNTER（117 ページ）
SET SWITCH LOOPDETECTION（136 ページ）
SHOW SWITCH LOOPDETECTION（191 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（103 ページ）
SET SWITCH MIRROR（137 ページ）
SET SWITCH PORT（138 ページ）
SHOW SWITCH（187 ページ）
SHOW SWITCH PORT（194 ページ）

DISABLE SWITCH PORT

カテゴリー：スイッチング / ポート

DISABLE SWITCH PORT={***port-list***|**ALL**} [LINK={DISABLE|ENABLE}]

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能)

解説

スイッチポートを無効にする。デフォルトは有効。

パラメーター

PORT ポート番号。複数指定が可能。

LINK （10/100Mbps ポートのみ）ポートを物理的にリンクダウンさせるかどうか。DISABLE（物理的にリンクダウンさせる)、ENABLE（物理的にはリンクアップのまま）から選択する。省略時はENABLE。

関連コマンド

ENABLE SWITCH PORT（104 ページ）
SHOW SWITCH PORT（194 ページ）

DISABLE SWITCH PORT AUTOMDI

カテゴリー：スイッチング / ポート

DISABLE SWITCH PORT={***port-list***|**ALL**} **AUTOMDI**

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能)

解説

MDI/MDI-X 自動切り替え機能を無効にする。デフォルトは有効。
本コマンド実行後のスイッチポートは、MDI/MDI-X 自動切り替え機能を有効にする前の設定に戻る。デフォルトは MDI-X。スイッチポートの MDI/MDI-X 設定は SET SWITCH PORT コマンドの POLARITY パラメーターで設定変更が可能。

パラメーター

PORT　ポート番号。複数指定が可能。

備考・注意事項

トランクポートを MDI/MDI-X 自動切替無効に設定できない。ただし、MDI/MDI-X 自動切替無効のポートをトランクグループに追加することは可能。

関連コマンド

ENABLE SWITCH PORT AUTOMDI（105 ページ）
SET SWITCH PORT（138 ページ）
SHOW SWITCH PORT（194 ページ）

DISABLE SWITCH PORT FLOW

カテゴリー：スイッチング / ポート

DISABLE SWITCH PORT={***port-list***|**ALL**} **FLOW=**{**PAUSE**}

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能)

解説

指定したスイッチポートでフローコントロール（802.3x PAUSE）を無効にする。デフォルトは有効。

パラメーター

PORT　ポート番号。複数指定が可能。
FLOW　フロー制御方式。PAUSE（802.3x PAUSE。Full-Duplex 時）のみサポート。

備考・注意事項

本製品の実装では、100Mbps、Full-Duplex 時の PAUSE フレームの受信（受信により送信を一時停止）のみをサポート。本製品が PAUSE フレームを送信することはない。

関連コマンド

ENABLE SWITCH PORT FLOW（106 ページ）
SHOW SWITCH PORT（194 ページ）

DISABLE SWITCH PORT VLAN

カテゴリー：スイッチング / ポート

DISABLE SWITCH PORT={***port-list***|**ALL**} **VLAN**[={*vlanname*|*1..4094*|ALL}]

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）
vlanname: VLAN 名（1〜32 文字。英数字とアンダースコア（_）、ハイフンを使用可能。大文字小文字は区別しない）

解説

指定した VLAN においてのみ、スイッチポートをディセーブルにする。

パラメーター

PORT　ポート番号
VLAN　VLAN 名または VLAN ID（VID）。省略時および ALL 指定時は、該当ポートが所属しているすべての VLAN が対象になる。

備考・注意事項

本コマンドを実行すると、該当ポートでは自動的にイングレスフィルタリング（SET SWITCH PORT コマンドの INFILTERING パラメーター）が有効になる。

関連コマンド

ENABLE SWITCH PORT VLAN（107 ページ）
SET SWITCH PORT（138 ページ）
SHOW SWITCH PORT（194 ページ）

DISABLE SWITCH POWERSAVE

カテゴリー：スイッチング / 一般コマンド

DISABLE SWITCH POWERSAVE

解説

省電力モードを無効にする。デフォルトは無効

備考・注意事項

省電力モードの設定は、装置全体に対して機能する。

関連コマンド

ENABLE SWITCH POWERSAVE（108 ページ）
SHOW SWITCH（187 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 透過機能を無効にする。デフォルトは無効。

関連コマンド

ENABLE SWITCH STPFORWARD（109 ページ）
SHOW SWITCH（187 ページ）

ENABLE DHCPSNOOPING

カテゴリー：スイッチング / DHCP Snooping

ENABLE DHCPSNOOPING

解説

DHCP Snooping を有効にする。デフォルトは無効。

関連コマンド

DISABLE DHCPSNOOPING（72 ページ）
SHOW DHCPSNOOPING（145 ページ）

ENABLE DHCPSNOOPING ARPSECURITY

カテゴリー：スイッチング / DHCP Snooping

ENABLE DHCPSNOOPING ARPSECURITY

解説

DHCP Snooping のオプション機能である ARP セキュリティーを有効にする。デフォルトは無効。

備考・注意事項

本機能は、DHCP Snooping が有効になっていないと動作しない。

関連コマンド

ADD DHCPSNOOPING BINDING（56 ページ）
DISABLE DHCPSNOOPING（72 ページ）
DISABLE DHCPSNOOPING ARPSECURITY（73 ページ）
SHOW DHCPSNOOPING（145 ページ）

ENABLE DHCPSNOOPING OPTION82

カテゴリー：スイッチング / DHCP Snooping

ENABLE DHCPSNOOPING OPTION82

解説

DHCP Snooping のオプション機能であるリレーエージェント情報オプション（オプションコード 82）の付加・検査・削除を有効にする。デフォルトは無効。
本機能を有効にした場合、Untrusted ポートで受信したクライアントからの DHCP/BOOTP パケットを転送するときに、リレーエージェント情報オプションを挿入する。同オプションには次の情報が含まれる。
・Remote-ID: 本製品の MAC アドレス
・Circuit-ID: クライアントパケットを受信したスイッチポートと VLAN ID
・Subscriber-ID:（オプション）任意の文字列（SET DHCPSNOOPING PORT コマンドの SUBSCRIBERID パラメーターで設定した場合のみ含める）
受信した DHCP/BOOTP パケットにリレーエージェント情報オプションがすでに付加されていた場合の動作は、受信ポートの DHCP Snooping ポート種別によって異なる。なお、このときの動作は、本機能の有効・無効とは関係なくつねに同じとなる。
・Untrusted ポートでは破棄
・Trusted ポートでは変更せずにそのまま転送
本機能が有効のとき、サーバーからの戻りパケットを Untrusted ポート配下のクライアントに転送するときは、クライアントが Untrusted ポートに直接接続されている場合にかぎって同オプションを削除する。

備考・注意事項

本機能は、DHCP Snooping が有効になっていないと動作しない。

関連コマンド

DISABLE DHCPSNOOPING（72 ページ）
DISABLE DHCPSNOOPING OPTION82（74 ページ）
SHOW DHCPSNOOPING（145 ページ）

ENABLE EPSR

カテゴリー：スイッチング / EPSR アウェア

ENABLE EPSR={***epsrname***|**ALL**}

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

解説

EPSR ドメインを有効化する。

パラメーター

EPSR　EPSR ドメイン名。ALL を指定した場合は、すべての EPSR ドメインが対象となる。

関連コマンド

CREATE EPSR（62 ページ）
DISABLE EPSR（75 ページ）
SHOW EPSR（155 ページ）

ENABLE EPSR DEBUG

カテゴリー：スイッチング / EPSR アウェア

ENABLE EPSR={***epsrname***|**ALL**} **DEBUG=**{**INFO**|**MSG**|**PKT**|**STATE**|**ALL**}
[OUTPUT=CONSOLE] [TIMEOUT={*1..4000000000*|NONE}]

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

解説

EPSR ドメインのデバッグオプションを有効化する。デフォルトはすべて無効。

パラメーター

EPSR　EPSR ドメイン名。ALL を指定した場合は、すべての EPSR ドメインが対象となる。

DEBUG　有効にするデバッグオプション。INFO（EPSR に関する全般的情報を表示）、MSG（EPSR パケットをデコードして表示）、PKT（EPSR パケットを ASCII 表示）、STATE（EPSR の状態遷移を表示）、ALL（すべてのオプション）から選択する。

OUTPUT　デバッグ情報の出力先を指定する。CONSOLE（コンソール）のみ指定可能。省略時はコマンドを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。

関連コマンド

CREATE EPSR（62 ページ）
DISABLE EPSR DEBUG（76 ページ）
SHOW EPSR DEBUG（159 ページ）

ENABLE LACP

カテゴリー：スイッチング / LACP（IEEE 802.3ad）

ENABLE LACP

解説

LACP モジュールを有効にする。デフォルトは無効。
なお、デフォルトでは、すべてのスイッチポートが LACP の管理下に置かれている。

関連コマンド

ADD LACP PORT（59 ページ）
DELETE LACP PORT（68 ページ）
DISABLE LACP（77 ページ）
SHOW LACP（160 ページ）

ENABLE PORTAUTH

カテゴリー：スイッチング / ポート認証

ENABLE PORTAUTH[={8021X|MACBASED}]

解説

ポート認証機能（802.1X 認証または MAC ベース認証）を有効にする。デフォルトはどちらも無効。
ポート認証を使用するためには、個々のスイッチポートでもポート認証機能を有効にする必要がある（ENABLE PORTAUTH PORT コマンド）。

パラメーター

PORTAUTH　認証メカニズム。8021X（802.1X 認証）、MACBASED（MAC ベース認証）から選択する。省略時は 8021X と見なされる。

関連コマンド

DISABLE PORTAUTH（78 ページ）
DISABLE PORTAUTH PORT（79 ページ）
SHOW PORTAUTH MULTISUPPLICANT PORT（173 ページ）
SHOW PORTAUTH PORT（177 ページ）

ENABLE PORTAUTH PORT

カテゴリー：スイッチング / ポート認証

ENABLE PORTAUTH[=8021X] **PORT=**{***port-list***|**ALL**} **TYPE=AUTHENTICATOR**
[CONTROL={AUTHORISED|AUTO|UNAUTHORISED}] [MAXREQ=*1..10*] [MODE={MULTI|SINGLE}] [PIGGYBACK={TRUE|FALSE}] [QUIETPERIOD=*0..65535*] [REAUTHENABLED={TRUE|FALSE}] [REAUTHMAX=*1..10*] [REAUTHPERIOD=*1..86400*] [SERVERTIMEOUT=*1..60*] [SUPPTIMEOUT=*1..60*] [TXPERIOD=*1..65535*] [GUESTVLAN={*vlanname*|*1..4094*|NONE}] [SECUREVLAN={ON|OFF}] [VLANASSIGNMENT={ENABLED|DISABLED}] [MIBRESET={ENABLED|DISABLED}] [TRAP={SUCCESS|FAILURE|BOTH|NONE}]

ENABLE PORTAUTH[=8021X] **PORT=**{***port-list***|**ALL**} **TYPE=BOTH**
[CONTROL={AUTHORISED|UNAUTHORISED|AUTO}] [MAXREQ=*1..10*] [MODE=SINGLE] [PIGGYBACK={TRUE|FALSE}] [QUIETPERIOD=*0..65535*] [REAUTHENABLED={TRUE|FALSE}] [REAUTHMAX=*1..10*] [REAUTHPERIOD=*1..86400*] [SERVERTIMEOUT=*1..60*] [SUPPTIMEOUT=*1..60*] [TXPERIOD=*1..65535*] [GUESTVLAN={*vlanname*|*1..4094*|NONE}] [VLANASSIGNMENT={ENABLED|DISABLED}] [MIBRESET={ENABLED|DISABLED}] [TRAP={SUCCESS|FAILURE|BOTH|NONE}] [AUTHPERIOD=*1..60*] [HELDPERIOD=*0..65535*] [MAXSTART=*1..10*] [STARTPERIOD=*1..60*] [USERNAME=*login-name* PASSWORD=*password* [METHOD={OTP [ENCRYPTION={MD4|MD5}]|STANDARD}]]

ENABLE PORTAUTH[=8021X] **PORT=**{***port-list***|**ALL**} **TYPE=SUPPLICANT**
[AUTHPERIOD=*1..60*] [HELDPERIOD=*0..65535*] [MAXSTART=*1..10*] [STARTPERIOD=*1..60*] [USERNAME=*login-name* PASSWORD=*password* [METHOD={OTP [ENCRYPTION={MD4|MD5}]|STANDARD}]]

ENABLE PORTAUTH=MACBASED PORT={***port-list***|**ALL**} [CONTROL={AUTHORISED|AUTO|UNAUTHORISED}] [QUIETPERIOD=*0..65535*] [SECUREVLAN={ON|OFF}] [VLANASSIGNMENT={ENABLED|DISABLED}] [MIBRESET={ENABLED|DISABLED}] [TRAP={SUCCESS|FAILURE|BOTH|NONE}]

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）
vlanname: VLAN 名（1〜32 文字。英数字とアンダースコア（_）、ハイフンを使用可能。大文字小文字を区別しない）
login-name: ログイン名（1〜64 文字。英数字のみ使用可能）
password: パスワード（1〜64 文字。英数字のみ使用可能）

解説

指定ポートで、ポート認証機能（802.1X 認証または MAC ベース認証）を有効にする。各ポートでは、802.1X

認証か MAC ベース認証のどちらか一方だけを使用できる。また、802.1X 認証を使用する場合は、各ポートを Authenticator、Supplicant、Authenticator かつ Supplicant (Both) のいずれかに設定できる。デフォルトは全ポート無効。

パラメーター

PORTAUTH　認証メカニズム。8021X（802.1X 認証）、MACBASED（MAC ベース認証）から選択する。省略時は 8021X と見なされる。

PORT　スイッチポート。複数指定が可能。

TYPE　（802.1X ポート）802.1X 認証におけるスイッチポートの役割。AUTHENTICATOR（Authenticator ポート）、SUPPLICANT（Supplicant ポート）、BOTH（Authenticator ポートかつ Supplicant ポート）のいずれかを指定する。なお、Multi-Supplicant モード（MODE=MULTI）を使用する場合、TYPE=BOTH は指定できない。TYPE=AUTHENTICATOR を指定すること。

CONTROL　（802.1X Authenticator ポート、MAC ベース認証ポート）手動設定による Authenticator ポートの状態。AUTO（認証結果に応じて変動）、UNAUTHORISED（未認証固定）、AUTHORISED（認証済み固定）から選択する。デフォルトは AUTO。通常は AUTO のままでよい。ただし、RADIUS サーバーの接続先ポートを Authenticator に設定している場合は、本パラメーターを AUTHORISED に設定する必要がある。

MAXREQ　（802.1X Authenticator ポート）Supplicant に対する EAPOL-Request パケットの最大再送回数。デフォルトは 2 回。

MODE　（802.1X Authenticator ポート）Authenticator ポートのモード。Supplicant が 1 台だけ接続されていることを想定した Single-Supplicant モード（MODE=SINGLE）と、Supplicant が複数台接続されていることを想定した Multi-Supplicant モード（MODE=MULTI）がある。Single-Supplicant モードでは、該当ポート配下に最初に接続された Supplicant だけが認証対象となる（その他の Supplicant からの通信を許可するかどうかは、PIGGYBACK パラメーターで制御可能）。Multi-Supplicant モードでは、該当ポート配下に接続された個々の Supplicant を識別し、個別に認証を行う。なお、Multi-Supplicant モードを使用する場合、TYPE パラメーターには BOTH を指定できない。AUTHENTICATOR を指定すること。デフォルトは SINGLE。

PIGGYBACK　（802.1X Single-Supplicant Authenticator ポート）Single-Supplicant モード（MODE=SINGLE）において、最初に接続された Supplicant の認証に成功した後、他のデバイスからのパケットも許可するかどうかを指定する。TRUE なら許可、FALSE なら拒否。デフォルトは TRUE。

QUIETPERIOD　（802.1X Authenticator ポート、MAC ベース認証ポート）Supplicant の認証に失敗した後、Supplicant との通信を拒否する期間（秒）。この期間中は受信したパケットをすべて破棄する。デフォルトは 60 秒。

REAUTHENABLED　（802.1X Authenticator ポート）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。MAC ベース認証ポートでは TRUE は動作しない。デフォルトは FALSE。

REAUTHMAX　（802.1X Authenticator ポート）再認証時における EAPOL-Request パケットの最大再送回数。デフォルトは 2 回。

REAUTHPERIOD　（802.1X Authenticator ポート）Supplicant の再認証間隔（秒）。デフォルトは 3600 秒。

SERVERTIMEOUT　（802.1X Authenticator ポート）RADIUS サーバーに Access-Request を送信した

後、RADIUS サーバーからの応答を待つ時間（秒）。デフォルトは 30 秒。

SUPPTIMEOUT （802.1X Authenticator ポート）Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間（秒）。デフォルトは 30 秒。

TXPERIOD （802.1X Authenticator ポート）Supplicant に EAPOL パケットを再送信する間隔（秒）。デフォルトは 30 秒。

GUESTVLAN （802.1X Single-Supplicant Authenticator ポート）ゲスト VLAN を指定する。装置上に設定されている VLAN の名前か VLAN ID を指定すること。NONE はゲスト VLAN を使用しないことを意味する。EAPOL パケットをまだ受信していないとき、該当ポートはゲスト VLAN の所属となる。最初の EAPOL パケットを受信すると、該当ポートはゲスト VLAN から削除され、本来の所属 VLAN に復帰する。本パラメーターは、Single-Supplicant モード（MODE=SINGLE）でのみ有効。デフォルトは NONE。

SECUREVLAN （802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート）802.1X 認証の Multi-Supplicant モード（MODE=MULTI）か MAC ベース認証でダイナミック VLAN を使用しているとき、2 番目以降の Supplicant の認証方法を指定する。本パラメーターに ON を指定した場合は、2 番目以降の Supplicant は、最初に認証を通った Supplicant と同じ VLAN でないと認証されない。一方、OFF を指定した場合は、有効な VLAN でありさえすれば認証をパスする。ただし、2 番目以降の Supplicant は、実際には最初に認証をパスした Supplicant と同じ VLAN の所属となる。本パラメーターは、Multi-Supplicant モード（MODE=MULTI）のポートか、MAC ベース認証のポートでのみ使用可能。デフォルトは ON。

VLANASSIGNMENT （802.1X Authenticator ポート、MAC ベース認証ポート）ダイナミック VLAN の有効・無効。有効時は、RADIUS サーバーが返してきた Tunnel-Private-Group-ID の値をもとに、指定ポートの所属 VLAN を動的に変更する。デフォルトは ENABLED。

MIBRESET （802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート）802.1X 認証の Multi-Supplicant モード（MODE=MULTI）か MAC ベース認証を使用しているポートにおいて、古い Supplicant 情報をエージアウトするかどうか。デフォルトは ENABLED。

TRAP （802.1X Authenticator ポート、MAC ベース認証ポート）ポート認証機能に関する SNMP トラップを送信するかどうか。SUCCESS を指定した場合は、Supplicant の認証に成功したときと、認証情報が時間切れになったときに SNMP トラップを送信する。FAILURE を指定した場合は、Supplicant の認証に失敗したときに SNMP トラップを送信する。BOTH を指定したときは、SUCCESS と FAILURE の両方の場合に SNMP トラップを送信する。NONE はトラップを送信しない。デフォルトは NONE。

AUTHPERIOD （802.1X Supplicant ポート）Authenticator に EAP-Response パケットを送信した後、Authenticator からの応答を待つ時間（秒）。デフォルトは 30 秒。

HELDPERIOD （802.1X Supplicant ポート）認証失敗後、Authenticator との通信を試みない期間（秒）。デフォルトは 60 秒。

MAXSTART （802.1X Supplicant ポート）EAPOL-Start パケットの最大送信回数。Supplicant ポートは、EAPOL-Start パケットを MAXSTART 回送信しても応答がない場合、Authenticator が存在しておらずポート認証の必要はないと判断する。デフォルトは 3 回。

STARTPERIOD （802.1X Supplicant ポート）Authenticator に EAPOL-Start パケットを再送信する間隔（秒）。デフォルトは 30 秒。

USERNAME （802.1X Supplicant ポート）指定スイッチポートが Supplicant として動作する場合に使うユーザー名。必ず PASSWORD パラメーターと組で指定すること。本パラメーターを設定した場

合、該当ポートでは、SET PORTAUTH USERNAME コマンドで設定するグローバルなユーザー名・パスワード・暗号化方式ではなく、本コマンドで設定した値が使用される。

PASSWORD （802.1X Supplicant ポート）指定スイッチポートが Supplicant として動作する場合に使うパスワード。必ず USERNAME パラメーターと組で指定すること。METHOD パラメーターに STANDARD を指定した場合、または、METHOD パラメーターを省略した場合は、6〜63 文字の文字列を指定する。METHOD パラメーターに OTP を指定した場合は、10〜63 文字の文字列（認証サーバー上で設定した OTP Initialisation Password と同じ値）を指定する。本パラメーターを設定した場合、該当ポートでは、SET PORTAUTH USERNAME コマンドで設定するグローバルなユーザー名・パスワード・暗号化方式ではなく、本コマンドで設定した値が使用される。

METHOD （802.1X Supplicant ポート）パスワード送信時の暗号化方式。STANDARD（EAP-MD5）または OTP（One-Time Password）から選択する。OTP を指定した場合は、ENCRYPTION パラメーターでワンタイムパスワードの生成アルゴリズムも指定する必要がある。デフォルトは STANDARD。

ENCRYPTION （802.1X Supplicant ポート）ワンタイムパスワードの生成アルゴリズム。MD4、MD5 から選択する。デフォルトは MD5。METHOD パラメーターに OTP を指定した場合の必須パラメーター。

備考・注意事項

802.1X 認証を有効にしたポート（Authenticator、Supplicant とも）、MAC ベース認証ポートでは、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ない。また、Authenticator ポート、MAC ベース認証ポートをタグ付きに設定することはできない。

Multi-Supplicant モード（MODE=MULTI）は 802.1X 規格に準拠しておらず、セキュリティー上のリスクがあるため、通常は Single-Supplicant モード（MODE=SINGLE）のまま使用すること。

MAC ベース認証ポートにおいて、SECUREVLAN パラメーターの設定を変更しても、ポートに接続してきた Supplicant の MAC アドレスの設定には反映されない。SET PORTAUTH PORT SUPPLICANTMAC コマンドで、Supplicant の MAC アドレスを指定して、SECUREVLAN パラメーターの設定を行うことで、設定は反映される。

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE（53 ページ）
ENABLE PORTAUTH（95 ページ）
SET PORTAUTH PORT（127 ページ）
SET PORTAUTH PORT SUPPLICANTMAC（131 ページ）
SHOW PORTAUTH（167 ページ）
SHOW PORTAUTH COUNTER（170 ページ）
SHOW PORTAUTH MULTISUPPLICANT PORT（173 ページ）
SHOW PORTAUTH PORT（177 ページ）
SHOW PORTAUTH TIMER（183 ページ）

ENABLE RRPSNOOPING

カテゴリー：スイッチング / RRP Snooping

ENABLE RRPSNOOPING

解説

RRP Snooping を有効にする。デフォルトは無効。

関連コマンド

DISABLE RRPSNOOPING（80 ページ）
SHOW RRPSNOOPING（186 ページ）

ENABLE SWITCH LOOPDETECTION

カテゴリー：スイッチング / ポート

ENABLE SWITCH LOOPDETECTION 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

LDF 検出機能を有効にする。デフォルトは無効

パラメーター

PORT　ポート番号または ALL を指定する。指定したポートがトランクポートの一部であった場合、そのトランクグループに所属しているすべてのポートに対して機能が有効になる。

例

■ポート 2 の LDF 検出機能を有効にする

```
ENABLE SWITCH LOOPDETECTION PORT=2
```

備考・注意事項

装置で最初に機能を有効にした場合のみ、ハードウェアパケットフィルターを使用する旨のメッセージ「INFO: LDF is active, L3FILT is activated」が表示される。
機能を有効にしなかったポートでは LDF の送出及び受信は行わない。
指定したポートがトランクポートの一部であった場合、そのトランクグループに所属しているすべてのポートで機能を有効にする。
LDF 検出と MAC アドレススラッシングプロテクションは目的が同じであるため、同一装置上で併用（同時使用）することは推奨しない。（ループ検出に時間がかかることがある。）併用を行う場合は、MAC アドレススラッシングプロテクションと LDF 検出のアクションを一致させること。
初期状態では MAC アドレススラッシングプロテクションが有効なため、LDF 検出のみを使う場合は、全ポートで MAC アドレススラッシングプロテクションを無効化（SET SWITCH PORT=ALL THRASHACTION=NONE を指定）、トランキングを使用している場合はトランク名ごとに無効化（SET SWITCH TRUNK=trunk THRASHACTION=NONE を指定）、LACP を使用している場合は LACP 全体で無効化（SET LACP THRASHACTION=NONE を指定）してから、LDF 検出を有効化すること。

関連コマンド

DISABLE SWITCH LOOPDETECTION（81 ページ）
RESET SWITCH LOOPDETECTION COUNTER（117 ページ）
SET SWITCH LOOPDETECTION（136 ページ）
SHOW SWITCH LOOPDETECTION（191 ページ）

ENABLE SWITCH MIRROR

カテゴリー：スイッチング / ポート

ENABLE SWITCH MIRROR

解説

ポートミラーリング機能を有効にする。ミラーポートの設定は変化しない。デフォルトは無効。

関連コマンド

DISABLE SWITCH MIRROR（82 ページ）
SET SWITCH MIRROR（137 ページ）
SET SWITCH PORT（138 ページ）
SHOW SWITCH（187 ページ）
SHOW SWITCH PORT（194 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

スイッチポートを有効にする。デフォルトは有効。

パラメーター

PORT　ポート番号。複数指定が可能。

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 NONE 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（83 ページ）
SHOW SWITCH PORT（194 ページ）

ENABLE SWITCH PORT AUTOMDI

カテゴリー：スイッチング / ポート

ENABLE SWITCH PORT={***port-list***|**ALL**} **AUTOMDI**

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能)

解説

MDI/MDI-X 自動切り替え機能を有効にする。デフォルトは有効。

パラメーター

PORT　ポート番号。複数指定が可能。

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

DISABLE SWITCH PORT AUTOMDI（84 ページ）
SET SWITCH PORT（138 ページ）
SHOW SWITCH PORT（194 ページ）

ENABLE SWITCH PORT FLOW

カテゴリー：スイッチング / ポート

ENABLE SWITCH PORT={***port-list***|**ALL**} **FLOW=**{**PAUSE**}

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能)

解説

指定したスイッチポートでフローコントロール（802.3x PAUSE）を有効にする。デフォルトは有効。

パラメーター

PORT　ポート番号。複数指定が可能。
FLOW　フロー制御方式。PAUSE（802.3x PAUSE。Full-Duplex 時）のみサポート。

備考・注意事項

本製品の実装では、100Mbps、Full-Duplex 時の PAUSE フレームの受信（受信により送信を一時停止）のみをサポート。本製品が PAUSE フレームを送信することはない。

関連コマンド

DISABLE SWITCH PORT FLOW（85 ページ）
SHOW SWITCH PORT（194 ページ）

ENABLE SWITCH PORT VLAN

カテゴリー：スイッチング / ポート

ENABLE SWITCH PORT={***port-list***|**ALL**} **VLAN**[={*vlanname*|*1..4094*|ALL}]

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）
vlanname: VLAN 名（1〜32 文字。英数字とアンダースコア（_）、ハイフンを使用可能。大文字小文字は区別しない）

解説

指定した VLAN においてのみ、スイッチポートをイネーブルにする。

パラメーター

PORT　ポート番号
VLAN　VLAN 名または VLAN ID（VID）。省略時および ALL 指定時は、該当ポートが所属しているすべての VLAN が対象になる。

備考・注意事項

本コマンドを実行すると、該当ポートでは自動的にイングレスフィルタリング（SET SWITCH PORT コマンドの INFILTERING パラメーター）が無効になる（ただし、該当ポートがまだ特定の VLAN に対してディセーブル状態にある場合、および、手動で該当ポートのイングレスフィルタリングを有効化していた場合は除く）。

関連コマンド

DISABLE SWITCH PORT VLAN（86 ページ）
SET SWITCH PORT（138 ページ）
SHOW SWITCH PORT（194 ページ）

ENABLE SWITCH POWERSAVE

カテゴリー：スイッチング / 一般コマンド

ENABLE SWITCH POWERSAVE

解説

省電力モードを有効にする。省電力モードを有効にすると、リンクしていないスイッチポートへの電力供給を制限し、自動的に消費電力を抑える。デフォルトは無効

備考・注意事項

省電力モードの設定は、装置全体に対して機能する。
省電力モードを有効にすると、リンクアップ時に 0〜2 秒程度の遅延が伴う。

関連コマンド

DISABLE SWITCH POWERSAVE（87 ページ）
SHOW SWITCH（187 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 透過機能を有効にする。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 透過機能を有効化できない。
また、BPDU 透過機能有効時に、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 透過機能は無効化される。
BPDU 透過機能無効時は、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。

備考・注意事項

パケットの送信先 MAC アドレスが BPDU のアドレスになっていても、DSAP（Destination Service Access Point）/SSAP（Source Service Access Point）に「0x42」が指定されていなければ、BPDU 透過機能の対象にはならない。

関連コマンド

DISABLE SWITCH STPFORWARD（88 ページ）
SHOW SWITCH（187 ページ）

PURGE EPSR

カテゴリー：スイッチング / EPSR アウェア

PURGE EPSR

解説

EPSR（Ethernet Protected Switching Ring）の設定をデフォルト状態に戻す。
EPSR ドメインはすべて削除され、各種タイマーはデフォルト値に戻る。
本コマンドを実行する前には、次のいずれかの手順をとる必要がある。
・DISABLE SWITCH PORT コマンドで該当 VLAN のリング接続用ポートをディセーブルにする
・該当 VLAN のリング接続用ポートからケーブルを抜く

備考・注意事項

ランタイムメモリー上にある EPSR 関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意すること。

関連コマンド

CREATE EPSR（62 ページ）
SHOW EPSR（155 ページ）

PURGE LACP

カテゴリー：スイッチング / LACP（IEEE 802.3ad）

PURGE LACP

解説

LACP の設定情報をすべて削除する。

備考・注意事項

ランタイムメモリー上にある LACP 関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意すること。

関連コマンド

DISABLE LACP（77 ページ）
SHOW LACP（160 ページ）

PURGE PORTAUTH PORT

カテゴリー：スイッチング / ポート認証

PURGE PORTAUTH[={8021X|MACBASED}] **PORT=**{***port-list***|**ALL**}

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）

解説

指定ポートにおけるポート認証機能（802.1X 認証、MAC ベース認証）の設定をすべて削除する。

パラメーター

PORTAUTH　認証メカニズム。8021X（802.1X 認証）、MACBASED（MAC ベース認証）から選択する。省略時は 8021X と見なされる。

PORT　スイッチポート。複数指定が可能。

備考・注意事項

ランタイムメモリー上にある、指定ポートの 802.1X 関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意すること。

関連コマンド

DISABLE PORTAUTH（78 ページ）
DISABLE PORTAUTH PORT（79 ページ）
SHOW PORTAUTH PORT（177 ページ）

RESET LACP PORT COUNTER

カテゴリー：スイッチング / LACP（IEEE 802.3ad）

RESET LACP PORT[={*port-list*|ALL}] **COUNTER**

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）

解説

スイッチポートの LACP 関連統計カウンターをクリアする。

パラメーター

PORT　ポート番号。

関連コマンド

PURGE LACP（111 ページ）
SHOW LACP（160 ページ）
SHOW LACP PORT（162 ページ）

RESET PORTAUTH PORT

カテゴリー：スイッチング / ポート認証

RESET PORTAUTH[={8021X|MACBASED}] **PORT=**{***port-list***|**ALL**}
[SUPPLICANTMAC=*macadd*]

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）
macadd: MAC アドレス（xx-xx-xx-xx-xx-xx の形式）

解説

指定ポートにおけるポート認証機能（802.1X 認証、MAC ベース認証）の状態をリセットする。

パラメーター

PORTAUTH　認証メカニズム。8021X（802.1X 認証）、MACBASED（MAC ベース認証）から選択する。省略時は 8021X と見なされる。

PORT　スイッチポート。複数指定が可能。

SUPPLICANTMAC　Supplicant の MAC アドレス。本パラメーターは、Multi-Supplicant モード（MODE=MULTI）のポートか、MAC ベース認証のポートでのみ使用可能。

関連コマンド

DISABLE PORTAUTH（78 ページ）
DISABLE PORTAUTH PORT（79 ページ）
ENABLE PORTAUTH（95 ページ）
ENABLE PORTAUTH PORT（96 ページ）
SHOW PORTAUTH MULTISUPPLICANT PORT（173 ページ）
SHOW PORTAUTH PORT（177 ページ）

RESET PORTAUTH PORT MULTIMIB

カテゴリー：スイッチング / ポート認証

RESET PORTAUTH[={8021X|MACBASED}] **PORT=**{***port-list***|**ALL**} **MULTIMIB**

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）

解説

Multi-Supplicant モードの Authenticator ポートにおいて、未認証かつ SET PORTAUTH PORT SUPPLICANTMAC コマンドで設定していない Supplicant の情報をクリアする。

パラメーター

PORTAUTH　認証メカニズム。8021X（802.1X 認証）、MACBASED（MAC ベース認証）から選択する。省略時は 8021X と見なされる。

PORT　スイッチポート。複数指定が可能。本コマンドは、Multi-Supplicant モード（MODE=MULTI）のポートか、MAC ベース認証のポートでのみ使用可能。

関連コマンド

DISABLE PORTAUTH（78 ページ）
DISABLE PORTAUTH PORT（79 ページ）
ENABLE PORTAUTH（95 ページ）
ENABLE PORTAUTH PORT（96 ページ）
SET PORTAUTH PORT SUPPLICANTMAC（131 ページ）
SHOW PORTAUTH MULTISUPPLICANT PORT（173 ページ）
SHOW PORTAUTH PORT（177 ページ）

RESET SWITCH

カテゴリー：スイッチング / 一般コマンド

RESET SWITCH

解説

スイッチングモジュールをリセットする。
すべてのスイッチポートがリセットされ、FDB のダイナミックエントリー等、動的に取得した情報はすべてクリアされる。また、スイッチングに関するタイマーと統計カウンターもクリアされる。

関連コマンド

SHOW SWITCH（187 ページ）
SHOW SWITCH FDB（「フォワーディングデータベース」の 22 ページ）

RESET SWITCH LOOPDETECTION COUNTER

カテゴリー：スイッチング / ポート

RESET SWITCH LOOPDETECTION 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

LDF 検出機能のカウンター情報をリセット (クリア) する

パラメーター

PORT　ポート番号または ALL を指定する

例

■ポート 1,2 の LDF 検出機能のカウンターをリセットする

```
RESET SWITCH LOOPDETECTION COUNTER PORT=1,2
```

備考・注意事項

DISABLE SWITCH LOOPDETECTION コマンドでは、LDF 検出機能のカウンター情報はリセットされない。本コマンド、または RESET SWITCH PORT コマンドを使用することで指定したポートについてリセットされる。また、RESET SWITCH コマンドではすべてのポートについてリセットされる。

関連コマンド

DISABLE SWITCH LOOPDETECTION（81 ページ）
ENABLE SWITCH LOOPDETECTION（101 ページ）
SET SWITCH LOOPDETECTION（136 ページ）
SHOW SWITCH LOOPDETECTION（191 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。複数指定が可能。
COUNTER　統計カウンターだけをリセットしたいときに指定する。

関連コマンド

DISABLE SWITCH PORT（83 ページ）
ENABLE SWITCH PORT（104 ページ）
SHOW SWITCH PORT（194 ページ）

SET DHCPSNOOPING CHECKINTERVAL

カテゴリー：スイッチング / DHCP Snooping

SET DHCPSNOOPING CHECKINTERVAL=*1..3600*

解説

DHCP Snooping テーブル（バインディングデータベース）のチェック間隔を変更する。
デフォルトでは、60 秒間隔でテーブル内のダイナミックエントリーをチェックし、IP アドレスの使用期限が切れたクライアントの情報をデータベースから削除する。スタティックエントリーはチェックされない（削除されない）。

パラメーター

CHECKINTERVAL　チェック間隔（秒）。デフォルトは 60 秒。

備考・注意事項

本製品は、バインディングデータベースをチェックするたびに、その時点で有効な（ダイナミック登録された）クライアントの情報を bindings.dsn ファイルに書き込む。DHCP Snooping を無効から有効に変更したときは、最初にこのファイルを読み込み、その時点でまだ有効なクライアントがあれば、それをバインディングデータベースに登録する。

関連コマンド

ENABLE DHCPSNOOPING（89 ページ）
SHOW DHCPSNOOPING（145 ページ）

SET DHCPSNOOPING CHECKOPTIONS

カテゴリー：スイッチング / DHCP Snooping

SET DHCPSNOOPING CHECKOPTIONS={**NONE**|**DHCPRELEASE**|**LINKDOWN**}[,...]

解説

DHCP Snooping テーブル（バインディングデータベース）から DHCP クライアント情報を削除する条件を追加する。
設定すると、すべての Untrusted ポートに設定が反映される。
装置全体に同じ設定が適用され、ポート毎に変更することはできない。

パラメーター

CHECKOPTIONS　クライアント情報を削除する条件。リース満了以外のダイナミックエントリーの削除条件を、DHCPRELEASE（DHCP RELEASE パケットを受信した場合）、LINKDOWN（クライアントが所属するポートがリンクダウンした場合）、または NONE（リース満了時のみ）で指定する。カンマ区切りによる複数指定が可能で（順不同、NONE を除く）、指定されたいずれかの条件が満たされた場合にクライアント情報を削除する。同じ条件を複数指定した場合、または NONE とその他の条件を同時に指定した場合はエラーになる。なお、スタティックエントリーは削除されない。デフォルトは NONE。

例

■DHCP Snooping テーブルの削除条件を、リース満了、DHCP RELEASE パケット受信時、クライアント所属ポートリンクダウン時のいずれかを満たす場合に設定する

```
SET DHCPSNOOPING CHECKOPTIONS=DHCPRELEASE,LINKDOWN
```

関連コマンド

SHOW DHCPSNOOPING（145 ページ）

SET DHCPSNOOPING PORT

カテゴリー：スイッチング / DHCP Snooping

SET DHCPSNOOPING PORT={***port-list***|**ALL**} [MAXLEASES=*0..100*]
[SUBSCRIBERID=*string*] [TRUSTED={YES|NO|ON|OFF|TRUE|FALSE}]

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）
string: 文字列（0〜50 文字。英数字と空白のみ使用可能。空白を含む場合はダブルクォートで囲む）

解説

指定したスイッチポートにおける DHCP Snooping の動作を変更する。

パラメーター

PORT　スイッチポート。複数指定が可能。

MAXLEASES　指定ポート経由の IP 通信を許可するクライアントの数（ダイナミック（DHCP クライアント）、スタティック（IP 固定設定クライアント）の合計）。0 が指定されている場合は、指定ポート経由の IP 通信を許可しない。デフォルトは 1。

SUBSCRIBERID　指定ポートの Subscriber-ID を指定する。DHCP Snooping のオプション機能であるリレーエージェント情報オプション（オプションコード 82）の付加・検査・削除機能が有効化されている場合、本パラメーターに 1 文字以上の文字列が指定されているときは、リレーエージェント情報オプションに Subscriber-ID サブオプションを含める。本パラメーターが指定されていない、あるいは、空文字列（長さが 0 の文字列）が指定されている場合は、Subscriber-ID サブオプションを含めない。デフォルトは指定なし（Subscriber-ID サブオプションを含めない）。

TRUSTED　DHCP Snooping におけるポート種別。YES、ON、TRUE を指定した場合、DHCP Snooping によるフィルタリングが行われない Trusted ポートとなる（サーバーなどの接続用）。NO、OFF、FALSE を指定した場合は、DHCP Snooping によるフィルタリングが行われる Untrusted ポートとなる（不特定多数のクライアント接続用）。デフォルトは NO（Untrusted ポート）。

備考・注意事項

MAXLEASES パラメーターは、ダイナミックエントリー（DHCP クライアント）だけでなく、ADD DHCPSNOOPING BINDING コマンドで登録するスタティックエントリー（IP 固定設定のクライアント）の数にも影響する（デフォルトでは、ポートあたり 1 つしかスタティックエントリーを登録できない）。

関連コマンド

ADD DHCPSNOOPING BINDING（56 ページ）
ENABLE DHCPSNOOPING（89 ページ）
ENABLE DHCPSNOOPING OPTION82（91 ページ）

SHOW DHCPSNOOPING（145 ページ）
SHOW DHCPSNOOPING PORT（153 ページ）

SET LACP

カテゴリー：スイッチング / LACP（IEEE 802.3ad）

```
SET LACP [PRIORITY=0..65535] [THRASHACTION={NONE|LEARNDISABLE|
    PORTDISABLE|VLANDISABLE|LINKDOWN}] [THRASHTIMEOUT={NONE|1..86400}]
    [LOOPACTION={PORTDISABLE|VLANDISABLE|LINKDOWN|LOGONLY|NONE}]
    [BLOCKTIMEOUT={NONE|1..86400}]
```

解説

LACP のグローバル設定パラメーターを変更する。

パラメーター

PRIORITY　LACP システムプライオリティー。小さいほど優先度が高い。相互接続された LACP システムは、システムプライオリティーとシステム ID（MAC アドレス）を組み合わせた値（System priority data identifier）を互いに比較し、値の小さいほうにリンクの制御権を付与する。デフォルトは 32768。

THRASHACTION　LACP によって自動生成されたトランクグループで MAC アドレススラッシング（同一 MAC アドレスの登録ポートが頻繁に変更されること）を検出した場合の動作。NONE（なにもしない）、LEARNDISABLE（トランクグループ内の全ポートで MAC アドレスの学習を停止する）、PORTDISABLE（トランクグループ内の全ポートをディセーブルにする）、VLANDISABLE（スラッシングが発生した VLAN に対してのみトランクグループ内の全ポートをディセーブルにする）、LINKDOWN（トランクグループ内の全ポートを物理的にリンクダウンさせる）から選択する。これらの動作は、THRASHTIMEOUT パラメーターで指定した時間が経過すると終了する（通常のポート動作に戻る）。ただし、PORTDISABLE、LINKDOWN の場合は、ENABLE SWITCH PORT コマンドにより手動で動作を終了させられる。また、VLANDISABLE の場合は、ENABLE SWITCH PORT VLAN コマンドにより手動で動作を終了させられる。LINKDOWN は 10/100Mbps ポートのみリンクダウンさせる。拡張モジュールに対してはポートをディセーブルにするのみ。デフォルトは LEARNDISABLE。

THRASHTIMEOUT　MAC アドレススラッシング検出時の動作の持続時間（秒）。NONE は無期限を示す。THRASHACTION パラメーターに LEARNDISABLE を指定している場合、本パラメーターを NONE に変更することはできない。また、本パラメーターを NONE に設定している状態で、THRASHACTION パラメーターの値を LEARNDISABLE に変更した場合、本パラメーターの値は自動的に 1 に変更される。デフォルトは 1 秒。

LOOPACTION　LACP によって自動生成されたトランクグループでループを検出した場合の動作。PORTDISABLE（トランクグループ内の全ポートをディセーブルにする）、VLANDISABLE（ループが発生した VLAN に対してのみトランクグループ内の全ポートをディセーブルにする）、LINKDOWN（トランクグループ内の全ポートを物理的にリンクダウンさせる）、LOGONLY（ポートの制御は行わず、ログへの記録と SNMP トラップの送信のみを行う）、NONE（動作を行わず、LDF の送受

信およびカウンター処理のみを行う）のいずれか。これらの動作は、BLOCKTIMEOUT パラメーターで指定した時間が経過すると終了する（通常のポート動作に戻る）。PORTDISABLE または LINKDOWN の場合は、ENABLE SWITCH PORT コマンドにより手動で動作を終了させられる。また、VLANDISABLE の場合は、ENABLE SWITCH PORT VLAN コマンドにより手動で動作を終了させられる。LINKDOWN は 10/100Mbps ポートのみリンクダウンさせる。拡張モジュールに対してはポートをディセーブルにするのみ。デフォルトは PORTDISABLE。

BLOCKTIMEOUT　対象トランクグループで LDF 検出機能がループを検出した場合の動作の持続時間（秒）。NONE は無期限を示す。デフォルトは 7。

備考・注意事項

THRASHACTION/LOOPACTION パラメーターの値を VLANDISABLE に変更すると、トランクグループ内の全ポートで自動的にイングレスフィルタリング（SET SWITCH PORT コマンドの INFILTERING パラメーター）が有効になる。また、VLANDISABLE からそれ以外に変更すると、イングレスフィルタリングが無効になる。

関連コマンド

SET SWITCH THRASHLIMIT（142 ページ）
SHOW LACP（160 ページ）

SET LACP PORT

カテゴリー：スイッチング / LACP（IEEE 802.3ad）

SET LACP PORT={***port-list***|**ALL**} [ADMINKEY=*0..65535*] [PRIORITY=*0..65535*]
[MODE={ACTIVE|PASSIVE}] [PERIODIC={FAST|SLOW}]

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）

解説

指定したスイッチポートの LACP 関連パラメーターを変更する。

パラメーター

PORT　ポート番号。

ADMINKEY　LACP ポート鍵の元となる値を指定する（ポート鍵の値そのものではない）。LACP では、対向機器、所属 VLAN、通信速度、ポート鍵のすべてが等しいポート群で 1 つのトランクグループを構成する。したがって、本来なら 1 つのトランクグループを構成するポート群を複数のグループに分けたい場合は、グループごとに異なる ADMINKEY を設定すればよい。なお、ADMINKEY は自機内でのみ意味を持つ（対向機器と同じに設定する必要はない）。デフォルトは 1。

PRIORITY　LACP ポートプライオリティー。小さいほど優先度が高い。使用可能な LACP ポートの数がトランクグループの最大ポート数（8 ポート）よりも多い場合、本パラメーターの小さいポートほどメンバーに選ばれる可能性が高くなる。なお、ポートプライオリティーが等しい場合は、ポート番号の小さいほうが優先的に使用される。また、メンバーに選ばれなかったポートはスタンバイ状態となり、現行のメンバーポートがリンクダウンするときに備えて待機する。デフォルトは 32768。

MODE　LACP ポートの動作モード。ACTIVE（PERIODIC パラメーターで設定した間隔で LACP パケットを自発的に送信する）、PASSIVE（対向ポートから LACP パケットを受信したときだけ LACP パケットを送信する）から選択する。デフォルトは ACTIVE。

PERIODIC　ACTIVE モード時の LACP パケットの送信間隔。FAST（1 秒）、SLOW（30 秒）から選択する。デフォルトは FAST。

関連コマンド

ADD LACP PORT（59 ページ）
DELETE LACP PORT（68 ページ）
SHOW LACP PORT（162 ページ）

SET PORTAUTH IDTOGGLE

カテゴリー：スイッチング / ポート認証

SET PORTAUTH[=8021X] **IDTOGGLE=**{**ON**|**OFF**}

解説

802.1X Multi-Supplicant モードで動作している Authenticator ポートにおいて、EAP パケットの Identifier フィールドに値をどのようにセットするかを指定する。
Supplicant として Windows XP SP2 ホストを使用している場合は、IDTOGGLE=ON に設定することで、ログインプロンプトが正しく表示されるようになる。

パラメーター

PORTAUTH　認証メカニズム。本コマンドでは 8021X（802.1X 認証）のみ有効。省略時は 8021X と見なされるため、特に指定する必要はない。

IDTOGGLE　EAP パケットの Identifier フィールドに値をどのようにセットするか。ON を指定した場合は 0 と 1 を交互にセットする。OFF を指定した場合は常に 0 をセットする。デフォルトは OFF。

備考・注意事項

IDTOGGLE=ON に設定すると、ポート認証を必要としない Windows XP ホストが同一ポートに接続されている場合、同ホスト上でログインプロンプトが常に表示されてしまうという弊害がある。

SET PORTAUTH PORT

カテゴリー：スイッチング / ポート認証

SET PORTAUTH[=8021X] **PORT=**{***port-list***|**ALL**} **TYPE=AUTHENTICATOR**
[CONTROL={AUTHORISED|AUTO|UNAUTHORISED}] [MAXREQ=*1..10*] [MODE={MULTI|SINGLE}] [PIGGYBACK={TRUE|FALSE}] [QUIETPERIOD=*0..65535*] [REAUTHENABLED={TRUE|FALSE}] [REAUTHMAX=*1..10*] [REAUTHPERIOD=*1..86400*] [SERVERTIMEOUT=*1..60*] [SUPPTIMEOUT=*1..60*] [TXPERIOD=*1..65535*] [GUESTVLAN={*vlanname*|*1..4094*|NONE}] [SECUREVLAN={ON|OFF}] [VLANASSIGNMENT={ENABLED|DISABLED}] [MIBRESET={ENABLED|DISABLED}] [TRAP={SUCCESS|FAILURE|BOTH|NONE}]

SET PORTAUTH[=8021X] **PORT=**{***port-list***|**ALL**} **TYPE=BOTH** [CONTROL={AUTHORISED|UNAUTHORISED|AUTO}] [MAXREQ=*1..10*] [MODE=SINGLE] [PIGGYBACK={TRUE|FALSE}] [QUIETPERIOD=*0..65535*] [REAUTHENABLED={TRUE|FALSE}] [REAUTHMAX=*1..10*] [REAUTHPERIOD=*1..86400*] [SERVERTIMEOUT=*1..60*] [SUPPTIMEOUT=*1..60*] [TXPERIOD=*1..65535*] [GUESTVLAN={*vlanname*|*1..4094*|NONE}] [VLANASSIGNMENT={ENABLED|DISABLED}] [MIBRESET={ENABLED|DISABLED}] [TRAP={SUCCESS|FAILURE|BOTH|NONE}] [AUTHPERIOD=*1..60*] [HELDPERIOD=*0..65535*] [MAXSTART=*1..10*] [STARTPERIOD=*1..60*] [USERNAME=*login-name* PASSWORD=*password* [METHOD={OTP [ENCRYPTION={MD4|MD5}]|STANDARD}]]

SET PORTAUTH[=8021X] **PORT=**{***port-list***|**ALL**} **TYPE=SUPPLICANT**
[AUTHPERIOD=*1..60*] [HELDPERIOD=*0..65535*] [MAXSTART=*1..10*] [STARTPERIOD=*1..60*] [USERNAME=*login-name* PASSWORD=*password* [METHOD={OTP [ENCRYPTION={MD4|MD5}]|STANDARD}]]

SET PORTAUTH=MACBASED PORT={***port-list***|**ALL**} [CONTROL={AUTHORISED|AUTO|UNAUTHORISED}] [QUIETPERIOD=*0..65535*] [SECUREVLAN={ON|OFF}] [VLANASSIGNMENT={ENABLED|DISABLED}] [MIBRESET={ENABLED|DISABLED}] [TRAP={SUCCESS|FAILURE|BOTH|NONE}]

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）
vlanname: VLAN 名（1〜32 文字。英数字とアンダースコア（_）、ハイフンを使用可能。大文字小文字を区別しない）
login-name: ログイン名（1〜64 文字。英数字のみ使用可能）
password: パスワード（1〜64 文字。英数字のみ使用可能）

解説

指定ポートにおけるポート認証機能（802.1X 認証または MAC ベース認証）の設定を変更する。

パラメーター

PORTAUTH　認証メカニズム。8021X（802.1X 認証）、MACBASED（MAC ベース認証）から選択する。省略時は 8021X と見なされる。

PORT　スイッチポート。複数指定が可能。

TYPE　（802.1X ポート）802.1X 認証におけるスイッチポートの役割。AUTHENTICATOR（Authenticator ポート）、SUPPLICANT（Supplicant ポート）、BOTH（Authenticator ポートかつ Supplicant ポート）のいずれかを指定する。なお、Multi-Supplicant モード（MODE=MULTI）を使用する場合、TYPE=BOTH は指定できない。TYPE=AUTHENTICATOR を指定すること。

CONTROL　（802.1X Authenticator ポート、MAC ベース認証ポート）手動設定による Authenticator ポートの状態。AUTO（認証結果に応じて変動）、UNAUTHORISED（未認証固定）、AUTHORISED（認証済み固定）から選択する。デフォルトは AUTO。通常は AUTO のままでよい。ただし、RADIUS サーバーの接続先ポートを Authenticator に設定している場合は、本パラメーターを AUTHORISED に設定する必要がある。

MAXREQ　（802.1X Authenticator ポート）Supplicant に対する EAPOL-Request パケットの最大再送回数。デフォルトは 2 回。

MODE　（802.1X Authenticator ポート）Authenticator ポートのモード。Supplicant が 1 台だけ接続されていることを想定した Single-Supplicant モード（MODE=SINGLE）と、Supplicant が複数台接続されていることを想定した Multi-Supplicant モード（MODE=MULTI）がある。Single-Supplicant モードでは、該当ポート配下に最初に接続された Supplicant だけが認証対象となる（その他の Supplicant からの通信を許可するかどうかは、PIGGYBACK パラメーターで制御可能）。Multi-Supplicant モードでは、該当ポート配下に接続された個々の Supplicant を識別し、個別に認証を行う。なお、Multi-Supplicant モードを使用する場合、TYPE パラメーターには BOTH を指定できない。AUTHENTICATOR を指定すること。デフォルトは SINGLE。

PIGGYBACK　（802.1X Single-Supplicant Authenticator ポート）Single-Supplicant モード（MODE=SINGLE）において、最初に接続された Supplicant の認証に成功した後、他のデバイスからのパケットも許可するかどうかを指定する。TRUE なら許可、FALSE なら拒否。デフォルトは TRUE。

QUIETPERIOD　（802.1X Authenticator ポート、MAC ベース認証ポート）Supplicant の認証に失敗した後、Supplicant との通信を拒否する期間（秒）。この期間中は受信したパケットをすべて破棄する。デフォルトは 60 秒。

REAUTHENABLED　（802.1X Authenticator ポート）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。MAC ベース認証ポートでは TRUE は動作しない。デフォルトは FALSE。

REAUTHMAX　（802.1X Authenticator ポート）再認証時における EAPOL-Request パケットの最大再送回数。デフォルトは 2 回。

REAUTHPERIOD　（802.1X Authenticator ポート）Supplicant の再認証間隔（秒）。デフォルトは 3600 秒。

SERVERTIMEOUT　（802.1X Authenticator ポート）RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間（秒）。デフォルトは 30 秒。

SUPPTIMEOUT　（802.1X Authenticator ポート）Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間（秒）。デフォルトは 30 秒。

TXPERIOD　（802.1X Authenticator ポート）Supplicant に EAPOL パケットを再送信する間隔（秒）。

デフォルトは 30 秒。

GUESTVLAN （802.1X Single-Supplicant Authenticator ポート）ゲスト VLAN を指定する。装置上に設定されている VLAN の名前か VLAN ID を指定すること。NONE はゲスト VLAN を使用しないことを意味する。EAPOL パケットをまだ受信していないとき、該当ポートはゲスト VLAN の所属となる。最初の EAPOL パケットを受信すると、該当ポートはゲスト VLAN から削除され、本来の所属 VLAN に復帰する。本パラメーターは、Single-Supplicant モード（MODE=SINGLE）でのみ有効。デフォルトは NONE。

SECUREVLAN （802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート）802.1X 認証の Multi-Supplicant モード（MODE=MULTI）か MAC ベース認証でダイナミック VLAN を使用しているとき、2 番目以降の Supplicant の認証方法を指定する。本パラメーターに ON を指定した場合は、2 番目以降の Supplicant は、最初に認証を通った Supplicant と同じ VLAN でないと認証されない。一方、OFF を指定した場合は、有効な VLAN でありさえすれば認証をパスする。ただし、2 番目以降の Supplicant は、実際には最初に認証をパスした Supplicant と同じ VLAN の所属となる。本パラメーターは、Multi-Supplicant モード（MODE=MULTI）のポートか、MAC ベース認証のポートでのみ使用可能。デフォルトは ON。

VLANASSIGNMENT （802.1X Authenticator ポート、MAC ベース認証ポート）ダイナミック VLAN の有効・無効。有効時は、RADIUS サーバーが返してきた Tunnel-Private-Group-ID の値をもとに、指定ポートの所属 VLAN を動的に変更する。デフォルトは ENABLED。

MIBRESET （802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート）802.1X 認証の Multi-Supplicant モード（MODE=MULTI）か MAC ベース認証を使用しているポートにおいて、古い Supplicant 情報をエージアウトするかどうか。デフォルトは ENABLED。

TRAP （802.1X Authenticator ポート、MAC ベース認証ポート）ポート認証機能に関する SNMP トラップを送信するかどうか。SUCCESS を指定した場合は、Supplicant の認証に成功したときと、認証情報が時間切れになったときに SNMP トラップを送信する。FAILURE を指定した場合は、Supplicant の認証に失敗したときに SNMP トラップを送信する。BOTH を指定したときは、SUCCESS と FAILURE の両方の場合に SNMP トラップを送信する。NONE はトラップを送信しない。デフォルトは NONE。

AUTHPERIOD （802.1X Supplicant ポート）Authenticator に EAP-Response パケットを送信した後、Authenticator からの応答を待つ時間（秒）。デフォルトは 30 秒。

HELDPERIOD （802.1X Supplicant ポート）認証失敗後、Authenticator との通信を試みない期間（秒）。デフォルトは 60 秒。

MAXSTART （802.1X Supplicant ポート）EAPOL-Start パケットの最大送信回数。Supplicant ポートは、EAPOL-Start パケットを MAXSTART 回送信しても応答がない場合、Authenticator が存在しておらずポート認証の必要はないと判断する。デフォルトは 3 回。

STARTPERIOD （802.1X Supplicant ポート）Authenticator に EAPOL-Start パケットを再送信する間隔（秒）。デフォルトは 30 秒。

USERNAME （802.1X Supplicant ポート）指定スイッチポートが Supplicant として動作する場合に使うユーザー名。必ず PASSWORD パラメーターと組で指定すること。本パラメーターを設定した場合、該当ポートでは、SET PORTAUTH USERNAME コマンドで設定するグローバルなユーザー名・パスワード・暗号化方式ではなく、本コマンドで設定した値が使用される。

PASSWORD （802.1X Supplicant ポート）指定スイッチポートが Supplicant として動作する場合に使うパスワード。必ず USERNAME パラメーターと組で指定すること。METHOD パラメーターに

STANDARD を指定した場合、または、METHOD パラメーターを省略した場合は、6〜63 文字の文字列を指定する。METHOD パラメーターに OTP を指定した場合は、10〜63 文字の文字列（認証サーバー上で設定した OTP Initialisation Password と同じ値）を指定する。本パラメーターを設定した場合、該当ポートでは、SET PORTAUTH USERNAME コマンドで設定するグローバルなユーザー名・パスワード・暗号化方式ではなく、本コマンドで設定した値が使用される。

METHOD （802.1X Supplicant ポート）パスワード送信時の暗号化方式。STANDARD（EAP-MD5）または OTP（One-Time Password）から選択する。OTP を指定した場合は、ENCRYPTION パラメーターでワンタイムパスワードの生成アルゴリズムも指定する必要がある。デフォルトは STANDARD。

ENCRYPTION （802.1X Supplicant ポート）ワンタイムパスワードの生成アルゴリズム。MD4、MD5 から選択する。デフォルトは MD5。METHOD パラメーターに OTP を指定した場合の必須パラメーター。

備考・注意事項

802.1X Multi-Supplicant モードで動作している Authenticator ポート、または、MAC ベース認証ポートに対し、特定の MAC アドレスを持つ Supplicant 固有の設定を行う場合は、SET PORTAUTH PORT SUPPLICANTMAC コマンドを使用する。

MAC ベース認証ポートにおいて、SECUREVLAN パラメーターの設定を変更しても、ポートに接続してきた Supplicant の MAC アドレスの設定には反映されない。SET PORTAUTH PORT SUPPLICANTMAC コマンドで、Supplicant の MAC アドレスを指定して、SECUREVLAN パラメーターの設定を行うことで、設定は反映される。

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE（53 ページ）
ENABLE PORTAUTH（95 ページ）
ENABLE PORTAUTH PORT（96 ページ）
SET PORTAUTH PORT SUPPLICANTMAC（131 ページ）
SHOW PORTAUTH（167 ページ）
SHOW PORTAUTH COUNTER（170 ページ）
SHOW PORTAUTH MULTISUPPLICANT PORT（173 ページ）
SHOW PORTAUTH PORT（177 ページ）
SHOW PORTAUTH TIMER（183 ページ）

SET PORTAUTH PORT SUPPLICANTMAC

カテゴリー：スイッチング / ポート認証

SET PORTAUTH[=8021X] **PORT=**{***port-list***|**ALL**} **SUPPLICANTMAC=*macadd***
[CONTROL={AUTHORISED|AUTO|UNAUTHORISED}] [MAXREQ=*1..10*]
[QUIETPERIOD=*0..65535*] [REAUTHENABLED={TRUE|FALSE}] [REAUTHMAX=*1..10*]
[REAUTHPERIOD=*1..86400*] [SERVERTIMEOUT=*1..60*] [SUPPTIMEOUT=*1..60*]
[TXPERIOD=*1..65535*] [SECUREVLAN={ON|OFF}] [VLANASSIGNMENT={ENABLED|
DISABLED}] [MIBRESET={ENABLED|DISABLED}] [TRAP={SUCCESS|FAILURE|BOTH|
NONE}] [DEFAULT]

SET PORTAUTH=MACBASED PORT={***port-list***|**ALL**} **SUPPLICANTMAC=*macadd***
[CONTROL={AUTHORISED|AUTO|UNAUTHORISED}] [QUIETPERIOD=*0..65535*]
[SECUREVLAN={ON|OFF}] [VLANASSIGNMENT={ENABLED|DISABLED}]
[MIBRESET={ENABLED|DISABLED}] [TRAP={SUCCESS|FAILURE|BOTH|NONE}]
[DEFAULT]

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）
macadd: MAC アドレス（xx-xx-xx-xx-xx-xx の形式）

解説

802.1X Multi-Supplicant モードで動作している Authenticator ポート、または、MAC ベース認証ポートに対し、特定の MAC アドレスを持つ Supplicant 固有のパラメーターを設定する。

パラメーター

PORTAUTH　認証メカニズム。8021X（802.1X 認証）、MACBASED（MAC ベース認証）から選択する。省略時は 8021X と見なされる。

PORT　スイッチポート。複数指定が可能。本コマンドは、Multi-Supplicant モード（MODE=MULTI）のポートか、MAC ベース認証のポートでのみ使用可能。

SUPPLICANTMAC　Supplicant の MAC アドレス。

CONTROL　（802.1X Authenticator ポート、MAC ベース認証ポート）手動設定による Authenticator ポートの状態。AUTO（認証結果に応じて変動）、UNAUTHORISED（未認証固定）、AUTHORISED（認証済み固定）から選択する。デフォルトは AUTO。通常は AUTO のままでよい。ただし、RADIUS サーバーの接続先ポートを Authenticator に設定している場合は、本パラメーターを AUTHORISED に設定する必要がある。

MAXREQ　（802.1X Authenticator ポート）Supplicant に対する EAPOL-Request パケットの最大再送回数。デフォルトは 2 回。

QUIETPERIOD　（802.1X Authenticator ポート、MAC ベース認証ポート）Supplicant の認証に失敗した後、Supplicant との通信を拒否する期間（秒）。この期間中は受信したパケットをすべて破棄する。

デフォルトは 60 秒。

REAUTHENABLED （802.1X Authenticator ポート）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。MAC ベース認証ポートでは TRUE は動作しない。デフォルトは FALSE。

REAUTHMAX （802.1X Authenticator ポート）再認証時における EAPOL-Request パケットの最大再送回数。デフォルトは 2 回。

REAUTHPERIOD （802.1X Authenticator ポート）Supplicant の再認証間隔（秒）。デフォルトは 3600 秒。

SERVERTIMEOUT （802.1X Authenticator ポート）RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間（秒）。デフォルトは 30 秒。

SUPPTIMEOUT （802.1X Authenticator ポート）Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間（秒）。デフォルトは 30 秒。

TXPERIOD （802.1X Authenticator ポート）Supplicant に EAPOL パケットを再送信する間隔（秒）。デフォルトは 30 秒。

SECUREVLAN （802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート）802.1X 認証の Multi-Supplicant モード（MODE=MULTI）か MAC ベース認証でダイナミック VLAN を使用しているとき、2 番目以降の Supplicant の認証方法を指定する。本パラメーターに ON を指定した場合は、2 番目以降の Supplicant は、最初に認証を通った Supplicant と同じ VLAN でないと認証されない。一方、OFF を指定した場合は、有効な VLAN でありさえすれば認証をパスする。ただし、2 番目以降の Supplicant は、実際には最初に認証をパスした Supplicant と同じ VLAN の所属となる。本パラメーターは、Multi-Supplicant モード（MODE=MULTI）のポートか、MAC ベース認証のポートでのみ使用可能。デフォルトは ON。

VLANASSIGNMENT （802.1X Authenticator ポート、MAC ベース認証ポート）ダイナミック VLAN の有効・無効。有効時は、RADIUS サーバーが返してきた Tunnel-Private-Group-ID の値をもとに、指定ポートの所属 VLAN を動的に変更する。デフォルトは ENABLED。

MIBRESET （802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート）802.1X 認証の Multi-Supplicant モード（MODE=MULTI）か MAC ベース認証を使用しているポートにおいて、古い Supplicant 情報をエージアウトするかどうか。デフォルトは ENABLED。

TRAP （802.1X Authenticator ポート、MAC ベース認証ポート）ポート認証機能に関する SNMP トラップを送信するかどうか。SUCCESS を指定した場合は、Supplicant の認証に成功したときと、認証情報が時間切れになったときに SNMP トラップを送信する。FAILURE を指定した場合は、Supplicant の認証に失敗したときに SNMP トラップを送信する。BOTH を指定したときは、SUCCESS と FAILURE の両方の場合に SNMP トラップを送信する。NONE はトラップを送信しない。デフォルトは NONE。

DEFAULT 指定した Supplicant 固有のポート認証設定を破棄するときに指定する。

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE（53 ページ）
ENABLE PORTAUTH（95 ページ）
ENABLE PORTAUTH PORT（96 ページ）
SET PORTAUTH PORT（127 ページ）

SHOW PORTAUTH（167 ページ）
SHOW PORTAUTH COUNTER（170 ページ）
SHOW PORTAUTH MULTISUPPLICANT PORT（173 ページ）
SHOW PORTAUTH PORT（177 ページ）
SHOW PORTAUTH TIMER（183 ページ）

SET PORTAUTH USERNAME

カテゴリー：スイッチング / ポート認証

SET PORTAUTH[=8021X] **USERNAME=*login-name* PASSWORD=*password*** [METHOD={OTP [ENCRYPTION={MD4|MD5}]|STANDARD}]

login-name: ログイン名（1〜64 文字。英数字のみ使用可能。大文字小文字を区別しない）
password: パスワード（文字数は認証方式によって異なる。英数字のみ使用可能。大文字小文字を区別する）

解説

Supplicant 時に使用するグローバルなユーザー名、パスワード、パスワード暗号化方式およびアルゴリズムを設定する。
本コマンドで設定するのは、Supplicant ポート固有のユーザー名、パスワードが設定されていないときに使用するグローバル値。Supplicant ポート固有のユーザー名が設定されているときは、本コマンドで設定した値ではなく、Supplicant ポート固有の設定値が使用される。

パラメーター

PORTAUTH 認証メカニズム。本コマンドでは 8021X（802.1X 認証）のみ有効。省略時は 8021X と見なされるため、特に指定する必要はない。

USERNAME 認証を受けるためのユーザー名。デフォルトは portAuthportAuth

PASSWORD 認証を受けるためのパスワード。METHOD パラメーターに STANDARD を指定した場合は、6〜63 文字の文字列を指定する。METHOD パラメーターに OTP を指定した場合は、10〜63 文字の文字列（認証サーバー上で設定した OTP Initialisation Password と同じ値）を指定する。デフォルトは portAuthportAuth

METHOD パスワード送信時の暗号化方式。STANDARD（EAP-MD5）または OTP（One-Time Password）から選択する。OTP を指定した場合は、ENCRYPTION パラメーターでワンタイムパスワードの生成アルゴリズムも指定する必要がある。デフォルトは STANDARD。

ENCRYPTION ワンタイムパスワードの生成アルゴリズム。MD4、MD5 から選択する。デフォルトは MD5。METHOD パラメーターに OTP を指定した場合の必須パラメーター。

備考・注意事項

パスワードは設定ファイルに平文のまま保存されるため、管理には注意すること。

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE（53 ページ）
ENABLE PORTAUTH（95 ページ）
ENABLE PORTAUTH PORT（96 ページ）

SET PORTAUTH PORT（127 ページ）
SET PORTAUTH PORT SUPPLICANTMAC（131 ページ）
SHOW PORTAUTH（167 ページ）
SHOW PORTAUTH COUNTER（170 ページ）
SHOW PORTAUTH MULTISUPPLICANT PORT（173 ページ）
SHOW PORTAUTH PORT（177 ページ）
SHOW PORTAUTH TIMER（183 ページ）

SET SWITCH LOOPDETECTION

カテゴリー：スイッチング / ポート

SET SWITCH LOOPDETECTION [INTERVAL={*1..600*}] [RXWINDOW={*1..5*}]

解説

LDF 検出機能のパラメーターを設定する

パラメーター

INTERVAL　LDF の送信間隔。単位は秒。デフォルトは 10 秒。スイッチポートが複数の VLAN に所属している場合、該当ポートからは各 VLAN に対して LDF が送信される。大量の LDF が同時に送信される場合は、送信タイミングが調整される。デフォルトより小さな値を指定すると、ループ発生から検出までの平均時間が短くなる。ただし LDF によるトラフィックが増加することに注意する。デフォルトより小さな値を指定する場合は、RXWINDOW の値をデフォルトより大きくすることを推奨。

RXWINDOW　送信した LDF の情報（LDF ID）をいくつまで保持するか。デフォルトは 3。LDF 受信時には、受信した LDF に設定されている LDF ID と、保持している送信済み LDF ID の情報を照合し、受信した LDF ID がいずれかの送信済み LDF ID と一致した場合にループが発生していると見なす。INTERVAL にデフォルトより大きな値（例：60 秒）を指定した場合で、セキュリティーを高めたい場合はデフォルトより小さな値を指定する。INTERVAL と RXWINDOW 両方にデフォルトより小さい値を設定した場合、環境によりループ検出までの時間が長くなったり、検出できなくなったりすることがあるため注意する。

例

■LDF の送信間隔を 60 秒に設定する。

```
SET SWITCH LOOPDETECTION INTERVAL=60
```

関連コマンド

DISABLE SWITCH LOOPDETECTION（81 ページ）
ENABLE SWITCH LOOPDETECTION（101 ページ）
RESET SWITCH LOOPDETECTION COUNTER（117 ページ）
SHOW SWITCH LOOPDETECTION（191 ページ）

SET SWITCH MIRROR

カテゴリー：スイッチング / ポート

SET SWITCH MIRROR={**NONE**|***port-number***}

port-number: スイッチポート番号（1〜）

解説

ミラーポートの設定および解除を行う。
ソースポートと対象トラフィックは、SET SWITCH PORT コマンドの MIRROR パラメーターで指定する。

パラメーター

MIRROR　ミラーポートとして使用するポートを指定する。VLAN default 以外に所属しているポートはミラーポートに設定できない。また、トランクポートも不可。本コマンド実行時に別のポートがミラーポートとして設定されていた場合、先に設定されていたポートはミラーポートでなくなり、VLAN default 所属のタグなしポートとなる。ミラーポートになったポートは、どの VLAN にも所属しない。ミラーポートを削除するには NONE を指定する。

備考・注意事項

ミラーポートとして設定されたポートは通常のスイッチポートとしては機能しない。
ポートトランキングの所属ポートをミラーポートに設定することはできない。
複数のソースポートを指定した場合で、かつ指定ポートにタグ付きとタグなしが混在している場合、送信パケットはすべてタグなしとしてミラーリングされる。
ハードウェアパケットフィルターによってミラーリングされたパケットは、VLAN タグが付いた状態でミラーポートに出力される。

関連コマンド

DISABLE SWITCH MIRROR（82 ページ）
ENABLE SWITCH MIRROR（103 ページ）
SET SWITCH PORT（138 ページ）
SHOW SWITCH（187 ページ）
SHOW SWITCH PORT（194 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**} [POLARITY={MDI|MDIX}] [ACCEPTABLE={ALL|VLAN}] [BCFILTERING={OFF|ON}] [BCLIMIT={NONE|*count*}] [DESCRIPTION=*string*] [DLFLIMIT={NONE|*count*}] [EGRESSLIMIT={NONE|DEFAULT|*0*|*1000..127000*|*8..1016*}] [INFILTERING={OFF|ON}] [INGRESSLIMIT={NONE|DEFAULT|*0*|*1000..127000*|*8..1016*}] [INTRUSIONACTION={DISABLE|DISCARD|TRAP|TRAPCONTINUE|LOG|LOGCONTINUE}] [LEARN={NONE|*0..256*}] [MCLIMIT={NONE|*count*}] [MIRROR={BOTH|NONE|RX|TX}] [MULTICASTMODE={A|B|C}] [RELEARN={OFF|ON}] [MODE=AUTONEGOTIATE] [SPEED={AUTONEGOTIATE|10MHALF|10MFULL|10MHAUTO|10MFAUTO|100MHALF|100MFULL|100MHAUTO|100MFAUTO|1000MFULL}] [THRASHACTION={NONE|LEARNDISABLE|PORTDISABLE|VLANDISABLE|LINKDOWN}] [THRASHTIMEOUT={NONE|*1..86400*}] [LOOPACTION={PORTDISABLE|VLANDISABLE|LINKDOWN|LOGONLY|NONE}] [BLOCKTIMEOUT={NONE|*1..86400*}]

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能)
count: 個数（0〜262143）
string: 文字列（0〜47 文字。使用可能な文字は半角英数字、半角記号（! # $ % & ' ( ) * + - . / : ; < = > @ [\ ] ^ , _ ‘ { | } ~)、半角空白）

解説

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

パラメーター

PORT　ポート番号。複数指定が可能。ALL を指定した場合はすべてのポートが対象となる。パケットストームプロテクションの設定を行うとき（BCLIMIT、DLFLIMIT、MCLIMIT パラメーター）は、1-8、9-16、17-24、25、26 のいずれか（8424XL）、または、1-8、9-16、17-24 のいずれか（8424TX）のポートグループ単位で指定する必要がある。

POLARITY　MDI/MDI-X を指定する。デフォルトは MDI-X。MDI/MDI-X 自動切り替え有効時は設定できない。

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。

BCFILTERING　指定ポートからのブロードキャストパケットの送出を止めるかどうか。ON（送出を止める）か OFF（送出を止めない）を指定する。ON のときは、ブロードキャストパケットは送信されず、

OFF のときは送信される。デフォルトは OFF。

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

DESCRIPTION　ポート名称。SHOW SWITCH PORT コマンド、SHOW INTERFACE コマンドなどで表示されるもので、メモ的に使用する。また、MIB オブジェクト ifName に反映される。

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

EGRESSLIMIT　該当ポートの送信レート上限値（帯域制限機能）。指定可能な値の範囲は、10/100M ポートが 1000～127000Kbps、1000M ポートが 8～1016Mbps。NONE および 0 は制限なし。実際の送信レートは、10/100M ポートでは 1000Kbps の倍数になるよう切り上げられる。また、1000M ポートでは、8Mbps の倍数になるよう切り上げられる。デフォルトは NONE。

INFILTERING　イングレスフィルタリングを行うかどうか。ON（行う）か OFF（行わない）を指定する。ON のときは、受信フレームの VLAN ID が受信ポートの所属 VLAN と一致した場合のみフレームを受け入れ、それ以外は破棄する。OFF の場合はすべてのフレームを受け入れる。デフォルトは OFF。

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

LEARN　該当ポートで学習可能な送信元 MAC アドレス（ダイナミックエントリー）の最大数。0 を指定した場合、ポートはロック状態になり、FDB の自動学習機能が停止する。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 NONE（ポートセキュリティーオフ）

RELEARN　ポートセキュリティー機能で学習した送信元 MAC アドレスのエージング機能を有効にするかどうか。ON（有効）にすることで、Dynamic Limited モードとなる。OFF（無効）にすることで、Limited モードとなる。デフォルトは OFF。

INTRUSIONACTION　未学習の送信元 MAC アドレスを持つフレームを、LEARN パラメーターで指定した制限値を超えて受信した場合のアクション。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）、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。すでにトラップ送信済みのアドレスの場合はトラップを送信しない。）、TRAPCONTINUE（受信パケットを破棄した後、SNMP トラップを送信する。すでにトラップ送信済みのアドレスの場合も再度トラップを送信する。）、LOG（受信パケットを破棄した後、ログに記録する。すでにログに記録済みのアドレスの場合はログの記録を行わない。）、LOGCINTINUE（受信パケットを破棄した後、ログに記録する。すでにログに記録済みのアドレスの場合も再度ログの記録を行う。）から選択する。TRAP/TRAPCONTINUE と LOG/LOGCONTINUE は、カンマで区切って同時に指定することができる。TRAP と TRAPCONTINUE、LOG と LOGCONTINUE は併用できない。デフォルトは DISCARD。

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

MIRROR　ミラーリングするトラフィックの向き。該当ポートをポートミラーリングのソースポートにしたいときに指定する。BOTH（送受信パケット）、RX（受信パケット）、TX（送信パケット）、NONE（ミラーリングしない）から選択する。デフォルトは NONE。

MULTICASTMODE　VLAN 内における IP マルチキャストパケットのフィルタリング方式。A（マルチキャストグループの有無に関わらず VLAN 内で全ポートに Flooding）、B（対応するマルチキャストグループがあれば当該ポートへ、無ければ VLAN 内で全ポートに Flooding）、C（対応するマルチキャストグループがあれば当該ポートへ、無ければ破棄する）から選択。デフォルトは B。

MODE　1000BASE-T ポートのマスター/スレーブ。AUTONEGOTIATE のみ指定可能。

SPEED　ポートの通信速度とデュプレックスモードを設定する。トランクグループ所属ポートに対して本コマンドで SPEED オプションを変更した場合、ポートレベルの設定値は変更されるが、実際の値はトランクグループ全体の設定値のまま変化しない。同ポートをトランクグループから除外した時点で設定値が有効になる。デフォルトは AUTONEGOTIATE（オートネゴシエーション）。AT-A50 の拡張モジュールは AUTONEGOTIATE、1000MFULL、100MFULL、100MHALF のみ、AT-A51、AT-A53 の拡張モジュールは AUTONEGOTIATE、1000MFULL のみサポートする。デフォルトは AUTONEGOTIATE（オートネゴシエーション）。

THRASHACTION　該当スイッチポートで MAC アドレススラッシング（同一 MAC アドレスの登録ポートが頻繁に変更されること）を検出した場合の動作。NONE（なにもしない）、LEARNDISABLE（MAC アドレスの学習を停止する）、PORTDISABLE（ポートをディセーブルにする）、VLANDISABLE（スラッシングが発生した VLAN に対してのみポートをディセーブルにする）、LINKDOWN（ポートを物理的にリンクダウンさせる）から選択する。これらの動作は、THRASHTIMEOUT パラメーターで指定した時間が経過すると終了する（通常のポート動作に戻る）。ただし、PORTDISABLE、LINKDOWN の場合は、ENABLE SWITCH PORT コマンドにより手動で動作を終了させられる。また、VLANDISABLE の場合は、ENABLE SWITCH PORT VLAN コマンドにより手動で動作を終了させられる。LINKDOWN は 10/100Mbps ポートのみリンクダウンさせる。拡張モジュールに対してはポートをディセーブルにするのみ。デフォルトは LEARNDISABLE。

THRASHTIMEOUT　MAC アドレススラッシング検出時の動作の持続時間（秒）。NONE は無期限を示す。THRASHACTION パラメーターに LEARNDISABLE を指定している場合、本パラメーターを NONE に変更することはできない。また、本パラメーターを NONE に設定している状態で、THRASHACTION パラメーターの値を LEARNDISABLE に変更した場合、本パラメーターの値は自動的に 1 に変更される。デフォルトは 1 秒。

LOOPACTION　該当スイッチポートでループを検出した場合の動作。PORTDISABLE（ポートをディセーブルにする）、VLANDISABLE（ループが発生した VLAN に対してのみポートをディセーブルにする）、LINKDOWN（ポートを物理的にリンクダウンさせる）、LOGONLY（ポートの制御は行わず、ログへの記録と SNMP トラップの送信のみを行う）、NONE（動作を行わず、LDF の送受信およびカウンター処理のみを行う）のいずれか。これらの動作は、BLOCKTIMEOUT パラメーターで指定した時間が経過すると終了する（通常のポート動作に戻る）。PORTDISABLE または LINKDOWN の場合は、ENABLE SWITCH PORT コマンドにより手動で動作を終了させられる。また、VLANDISABLE の場合は、ENABLE SWITCH PORT VLAN コマンドにより手動で動作を終了させられる。LINKDOWN は 10/100Mbps ポートのみリンクダウンさせる。拡張モジュールに対してはポートをディセーブルにするのみ。デフォルトは PORTDISABLE。

BLOCKTIMEOUT　対象スイッチポートで LDF 検出機能がループを検出した場合の動作の持続時間（秒）。NONE は無期限を示す。デフォルトは 7。

備考・注意事項

BCLIMIT、DLFLIMIT、MCLIMIT パラメーターに 0/NONE 以外の値を指定する場合は、すべて同じ値を指定しなくてはならない。また、これらのパラメーターを指定する場合は、PORT に 1-8、9-16、17-24、25、26 のいずれか（25、26 は 8424XL のみ）を指定する必要がある。
INGRESSLIMIT を設定すると、該当ポートのハードウェアパケットフィルターのエントリーが 1 つ作成される。
LEARN=0 に設定すると警告文（Warning）が表示される。これは LEARN オプションに 0 を指定してもセキュリティーが解除されていないことを示しており、ポートセキュリティーをオフにするには、LEARN=NONE に設定する必要がある。
SPEED=1000MFULL は、拡張モジュール AT-A50/51/53 でのみ有効。
パケットストームプロテクションの設定（BCLIMIT、DLFLIMIT、MCLIMIT パラメーター）で指定する受信レートの上限値は、1 ポートあたりの上限値として動作する。上限値の設定は、ポートグループ単位でのみ指定可能。
拡張モジュールスロットに、拡張モジュール「AT-A51」または「AT-A53」を装着したときに、本コマンドで SPEED=1000MFULL を指定してケーブルを接続してリンクが確立した後にケーブルを抜くと、下記の場合に、LINK LED の表示が正しくなくなる。
○ TX ポートのケーブルを抜くと、ケーブルを抜いた機器の LINK LED が点灯したままになる
○ RX ポートのケーブルを抜くと、ケーブルを抜いていない機器の LINK LED が点灯したままになる
どちらの場合も、LINK LED が点灯したままのポートのリンクステータスは、Up のままになる。

関連コマンド

DISABLE SWITCH PORT（83 ページ）
ENABLE SWITCH PORT（104 ページ）
SHOW SWITCH PORT（194 ページ）

SET SWITCH THRASHLIMIT

カテゴリー：スイッチング / 一般コマンド

SET SWITCH THRASHLIMIT=*5..255*

解説

MAC アドレススラッシング（同一 MAC アドレスの登録ポートが頻繁に変更されること）の検出しきい値を設定する。

パラメーター

THRASHLIMIT　MAC アドレススラッシングの検出しきい値。同一の MAC アドレスが 1 秒間に本パラメーターで指定した回数ポート間を移動すると、本製品は MAC アドレススラッシングが発生したと見なし、関連するポートにおいて、SET SWITCH PORT コマンド、CREATE SWITCH TRUNK コマンド、SET SWITCH TRUNK コマンド、SET LACP コマンドの THRASHACTION パラメーターで指定された動作を実行する。デフォルトは 10。

関連コマンド

CREATE SWITCH TRUNK（64 ページ）
DISABLE SWITCH PORT VLAN（86 ページ）
ENABLE SWITCH PORT VLAN（107 ページ）
SET LACP（123 ページ）
SET SWITCH PORT（138 ページ）
SET SWITCH TRUNK（143 ページ）
SHOW LACP（160 ページ）
SHOW SWITCH（187 ページ）
SHOW SWITCH PORT（194 ページ）
SHOW SWITCH TRUNK（206 ページ）

SET SWITCH TRUNK

カテゴリー：スイッチング / ポート

SET SWITCH TRUNK=*trunk* [SELECT={MACSRC|MACDEST|MACBOTH|IPSRC|IPDEST|IPBOTH}] [SPEED={10M|100M|1000M}] [THRASHACTION={NONE|LEARNDISABLE|PORTDISABLE|VLANDISABLE|LINKDOWN}] [THRASHTIMEOUT={NONE|*1..86400*}] [LOOPACTION={PORTDISABLE|VLANDISABLE|LINKDOWN|LOGONLY|NONE}] [BLOCKTIMEOUT={NONE|*1..86400*}]

trunk: トランクグループ名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。大文字小文字を区別しない）

解説

トランクグループの設定を変更する。

パラメーター

TRUNK　トランクグループ名

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

SPEED　トランクポートの通信速度。トランクグループに参加したポートは、ここで指定した速度のオートネゴシエーション（AUTONEGOTIATE）となる。デフォルトは 100M。実際の通信速度は 10M に設定した場合は 10MFULL Autonegotiate、100M に設定した場合は 100MFULL Autonegotiate、1000M に設定した場合は 1000MFULL Autonegotiate で動作する。

THRASHACTION　該当トランクグループで MAC アドレススラッシング（同一 MAC アドレスの登録ポートが頻繁に変更されること）を検出した場合の動作。NONE（なにもしない）、LEARNDISABLE（トランクグループ内の全ポートで MAC アドレスの学習を停止する）、PORTDISABLE（トランクグループ内の全ポートをディセーブルにする）、VLANDISABLE（スラッシングが発生した VLAN に対してのみトランクグループ内の全ポートをディセーブルにする）、LINKDOWN（トランクグループ内の全ポートを物理的にリンクダウンさせる）から選択する。これらの動作は、THRASHTIMEOUT パラメーターで指定した時間が経過すると終了する（通常のポート動作に戻る）。ただし、PORTDISABLE、LINKDOWN の場合は、ENABLE SWITCH PORT コマンドにより手動で動作を終了させられる。また、VLANDISABLE の場合は、ENABLE SWITCH PORT VLAN コマンドにより手動で動作を終了させられる。LINKDOWN は 10/100Mbps ポートのみリンクダウンさせる。拡張モジュールに対してはポートをディセーブルにするのみ。デフォルトは LEARNDISABLE。

THRASHTIMEOUT　MAC アドレススラッシング検出時の動作の持続時間（秒）。NONE は無期限を示す。THRASHACTION パラメーターに LEARNDISABLE を指定している場合、本パラメーターを NONE に変更することはできない。また、本パラメーターを NONE に設定している状態で、

THRASHACTION パラメーターの値を LEARNDISABLE に変更した場合、本パラメーターの値は自動的に 1 に変更される。デフォルトは 1 秒。

LOOPACTION　該当トランクグループでループを検出した場合の動作。PORTDISABLE（トランクグループ内の全ポートをディセーブルにする）、VLANDISABLE（ループが発生した VLAN に対してのみトランクグループ内の全ポートをディセーブルにする）、LINKDOWN（トランクグループ内の全ポートを物理的にリンクダウンさせる）、LOGONLY（ポートの制御は行わず、ログへの記録と SNMP トラップの送信のみを行う）、NONE（動作を行わず、LDF の送受信およびカウンター処理のみを行う）のいずれか。これらの動作は、BLOCKTIMEOUT パラメーターで指定した時間が経過すると終了する（通常のポート動作に戻る）。PORTDISABLE または LINKDOWN の場合は、ENABLE SWITCH PORT コマンドにより手動で動作を終了させられる。また、VLANDISABLE の場合は、ENABLE SWITCH PORT VLAN コマンドにより手動で動作を終了させられる。LINKDOWN は 10/100Mbps ポートのみリンクダウンさせる。拡張モジュールに対してはポートをディセーブルにするのみ。デフォルトは PORTDISABLE。

BLOCKTIMEOUT　対象トランクグループで LDF 検出機能がループを検出した場合の動作の持続時間（秒）。NONE は無期限を示す。デフォルトは 7。

備考・注意事項

THRASHACTION/LOOPACTION パラメーターの値を VLANDISABLE に変更すると、トランクグループ内の全ポートで自動的にイングレスフィルタリング（SET SWITCH PORT コマンドの INFILTERING パラメーター）が有効になる。また、VLANDISABLE からそれ以外に変更すると、イングレスフィルタリングが無効になる。

関連コマンド

ADD SWITCH TRUNK（61 ページ）
CREATE SWITCH TRUNK（64 ページ）
DELETE SWITCH TRUNK（69 ページ）
DESTROY SWITCH TRUNK（71 ページ）
SHOW SWITCH TRUNK（206 ページ）

SHOW DHCPSNOOPING

カテゴリー：スイッチング / DHCP Snooping

SHOW DHCPSNOOPING

解説

DHCP Snooping の全般的な設定情報を表示する。

入力・出力・画面例

```
Manager > show dhcpsnooping

DHCP Snooping Information
-------------------------------------------------------------------------------
DHCP Snooping ............... Enabled
  Option 82 status ......... Enabled
  ARP security ............. Enabled
  Debug enabled ............ None

DHCP Snooping Database:
  Full Leases/Max Leases ... 2/26
  Check Interval ........... 60 seconds
  Check Options ............ DHCPRELEASE,LINKDOWN
-------------------------------------------------------------------------------
```

DHCP Snooping	DHCP Snooping の有効・無効
Option 82 status	リレーエージェント情報オプション（オプションコード 82）の付加・検査・削除機能の有効・無効
ARP security	ARP セキュリティー機能の有効・無効
Debug enabled	未サポート
Full Leases/Max Leases	DHCP Snooping テーブル（バインディングデータベース）に現在登録されているクライアントの数 / 登録可能なクライアントの総数
Check Interval	バインディングデータベースのチェック間隔
Check Options	バインディングデータベースからクライアント情報を削除する条件。リース満了以外に指定された条件を表示する。DHCPRELEASE（DHCP RELEASE パケットを受信した場合）、LINKDOWN（クライアントが所属するポートがリンクダウンした場合）、その両方、または None（リース満了以外の条件を指定しない）

表 10:

関連コマンド

ENABLE DHCPSNOOPING（89 ページ）

SHOW DHCPSNOOPING COUNTER

カテゴリー：スイッチング / DHCP Snooping

SHOW DHCPSNOOPING COUNTER

解説

DHCP Snooping の統計情報を表示する。

入力・出力・画面例

```
Manager > show dhcpsnooping counter

DHCP Snooping Counters
------------------------------------------------------------------------------

DHCP Snooping
  InPackets ..................... 16
  InBootpRequests ............... 14
  InBootpReplies ................ 2
  InDiscards .................... 0

ARP Security
  InPackets ..................... 6
  InDiscards .................... 3
    NoLease ..................... 3
    Invalid ..................... 0

------------------------------------------------------------------------------
```

DHCP Snooping セクション	
InPackets	受信した DHCP/BOOTP パケットの総数
InBootpRequests	受信した DHCP/BOOTP 要求パケットの数
InBootpReplies	受信した DHCP/BOOTP 応答パケットの数
InDiscards	受信後破棄した DHCP/BOOTP パケットの数
ARP Security セクション	
InPackets	受信した ARP パケットの総数
InDiscards	受信後破棄した ARP パケットの総数
NoLease	上記「受信後破棄した ARP パケットの総数」のうち、DHCP Snooping テーブル（バインディングデータベース）未登録のため破棄したものの数

Invalid	上記「受信後破棄した ARP パケットの総数」のうち、パケットフォーマット不正のため破棄したものの数

表 11:

関連コマンド

ENABLE DHCPSNOOPING（89 ページ）
ENABLE DHCPSNOOPING ARPSECURITY（90 ページ）

SHOW DHCPSNOOPING DATABASE

カテゴリー：スイッチング / DHCP Snooping

SHOW DHCPSNOOPING DATABASE

解説

DHCP Snooping テーブル（バインディングデータベース）の内容を表示する。

入力・出力・画面例

```
Manager > show dhcpsnooping database

DHCP Snooping Binding Database
--------------------------------------------------------------------------------
Full Leases/Max Leases ... 2/26
Check Interval ........... 60 seconds
Check Options ............ DHCPRELEASE,LINKDOWN
Database Listeners ....... CLASSIFR

Current valid entries
MAC Address        IP Address       Expires(s)  VLAN  Port       ID     Source
--------------------------------------------------------------------------------
00-00-00-00-00-01  192.168.10.5     Static      1     5          4      User
00-0a-79-34-06-12  192.168.10.200   2231        1     11         1      Dynamic
--------------------------------------------------------------------------------

Entries with client lease but no listeners
MAC Address        IP Address       Expires(s)  VLAN  Port       ID     Source
--------------------------------------------------------------------------------
None...
--------------------------------------------------------------------------------

Entries with no client lease and no listeners
MAC Address        IP Address       Expires(s)  VLAN  Port       ID     Source
--------------------------------------------------------------------------------
None...
--------------------------------------------------------------------------------
```

Full Leases/Max Leases	バインディングデータベースに現在登録されているクライアントの数 / 登録可能なクライアントの総数

Check Interval	バインディングデータベースのチェック間隔
Check Options	バインディングデータベースからクライアント情報を削除する条件。リース満了以外に指定された条件を表示する。DHCPRELEASE（DHCP RELEASE パケットを受信した場合)、LINKDOWN（クライアントが所属するポートがリンクダウンした場合)、その両方、または None（リース満了以外の条件を指定しない）
Database Listeners	バインディングデータベースを利用しているソフトウェアモジュール名（DHCP Snooping を有効にする前は none、一度有効にした後はつねに CLASSIFR モジュール）
Current valid entries セクション	現在有効なクライアントの登録情報が MAC アドレスの昇順で表示される
Entries with client lease but no listeners セクション	CLASSIFR モジュールとの連携がうまくいかなかったなどの理由で現在無効となっているクライアントの登録情報が表示される
Entries with no client lease and no listeners セクション	DHCP メッセージに問題があったなどの理由で現在無効となっているクライアントの登録情報が表示される
MAC Address	クライアントの MAC アドレス
IP Address	クライアントの IP アドレス
Expires(s)	該当エントリーの残り有効時間（秒）（IP アドレス使用期限までの残り時間）
VLAN	クライアントが所属している VLAN
Port	クライアントが接続されているスイッチポート
ID	バインディングデータベースにおけるエントリー ID
Source	エントリー（クライアント）の種類。Dynamic（ダイナミックエントリー。DHCP クライアント)、User（スタティックエントリー。IP 固定設定クライアント)、File（DHCP Snooping が有効化されたときに bindings.dsn ファイルからロードしたエントリー）

表 12:

関連コマンド

ENABLE DHCPSNOOPING（89 ページ）

SHOW DHCPSNOOPING FILTER

カテゴリー：スイッチング / DHCP Snooping

SHOW DHCPSNOOPING FILTER

解説

DHCP Snooping によって自動生成されたフィルターエントリーの内容を表示する。

入力・出力・画面例

```
Manager > show dhcpsnooping filter

DHCPSnooping ACL ( 2 entries )
ClassID    FlowID    Port    EntryID    IP Address/Port/Mac
--------------------------------------------------------------------------------
  20001       0      11         1       192.168.10.200/11/00-0a-79-34-06-12
  20004       0      5          4       192.168.10.5/5/00-00-00-00-00-01
```

DHCPSnooping ACL	エントリー数
ClassID	内部的なクラシファイア ID
FlowID	つねに 0
Port	スイッチポート番号
EntryID	DHCP Snooping テーブル（バインディングデータベース）のエントリー ID
IP Address	クライアントの IP アドレス
Port	クライアントが接続されているスイッチポート
Mac	クライアントの MAC アドレス

表 13:

関連コマンド

ADD DHCPSNOOPING BINDING（56 ページ）
ENABLE DHCPSNOOPING（89 ページ）

SHOW DHCPSNOOPING PORT

カテゴリー：スイッチング / DHCP Snooping

SHOW DHCPSNOOPING PORT[={*port-list*|ALL}]

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）

解説

指定したスイッチポートにおける DHCP Snooping の設定情報を表示する。

パラメーター

PORT　スイッチポート。複数指定が可能。

入力・出力・画面例

```
Manager > show dhcpsnooping port=11

DHCP Snooping Port Information:
------------------------------------------------------------------------

Port ..................... 11
  Trusted ................. No
  Full Leases/Max Leases ... 1/1
  Subscriber-ID ............

------------------------------------------------------------------------
```

Port	スイッチポート番号
Trusted	DHCP Snooping におけるポート種別。Yes（Trusted ポート）、No（Untrusted ポート）のいずれか
Full Leases/Max Leases	DHCP Snooping テーブル（バインディングデータベース）に現在登録されている該当ポート上のクライアントの数 / 該当ポート上で登録可能なクライアントの総数
Subscriber-ID	該当ポートの Subscriber-ID

表 14:

関連コマンド

ENABLE DHCPSNOOPING（89 ページ）

SET DHCPSNOOPING PORT（121 ページ）

SHOW EPSR

カテゴリー：スイッチング / EPSR アウェア

SHOW EPSR[={*epsrname*|ALL}]

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

解説

EPSR ドメインの情報を表示する。

パラメーター

EPSR　EPSR ドメイン名。省略時および ALL 指定時はすべての EPSR ドメインの情報が表示される。

入力・出力・画面例

```
Manager > show epsr

 EPSR Information
--------------------------------------------------------------------------------
 Name ....................... domain_one
 Mode ........................ AWARE
 Status ...................... Enabled
 State ....................... Links-Up
 Control Vlan ................ control (2)
 Data VLAN(s) ................ data (100)
 First Port .................. 1
 First Port Status ........... Up
 First Port Direction ........ Downstream
 Second Port ................. 2
 Second Port Status .......... Up
 Second Port Direction ....... Upstream
 Master Node ................. 00-00-cd-24-03-4e
--------------------------------------------------------------------------------
```

Name	EPSR ドメイン名
Mode	EPSR ドメインにおける役割。Aware（アウェア機能を持つトランジットノード）のみ
Status	EPSR ドメインの有効・無効
State	EPSR ドメインの状態。Idle、Links-Up、Links-Down、Pre-Forwarding のいずれか

Control Vlan	コントロール VLAN。カッコ内は VLAN ID（VID）
Data VLAN(s)	データ VLAN の一覧。カッコ内は VLAN ID（VID）
First Port	リングを構成する第 1 ポートの番号
First Port Status	リングを構成する第 1 ポートの状態。Up/Down/Unknown のいずれか。Unknown は EPSR ドメインが無効に設定されていることを示す
First Port Direction	リングを構成する第 1 ポートの向き。Upstream（マスターノードのプライマリーポート方向)、Downstream（マスターノードのセカンダリーポート方向)、Unknown（EPSR ドメインが無効に設定されている）のいずれか
Second Port	リングを構成する第 2 ポートの番号
Second Port Status	リングを構成する第 2 ポートの状態。UP/DOWN/Unknown のいずれか。Unknown は EPSR ドメインが無効に設定されていることを示す
Second Port Direction	リングを構成する第 2 ポートの向き。Upstream（マスターノードのプライマリーポート方向)、Downstream（マスターノードのセカンダリーポート方向)、Unknown（EPSR ドメインが無効に設定されている）のいずれか
Master Node	マスターノードの MAC アドレス。マスターノードからのメッセージをまだ受信していない場合は Unknown と表示される

表 15:

関連コマンド

ADD EPSR DATAVLAN（58 ページ）
CREATE EPSR（62 ページ）
CREATE VLAN（「バーチャル LAN」の 14 ページ）
ENABLE EPSR（92 ページ）
SHOW EPSR COUNTER（157 ページ）

SHOW EPSR COUNTER

カテゴリー：スイッチング / EPSR アウェア

SHOW EPSR[={*epsrname*|ALL}] **COUNTER**

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

解説

EPSR ドメインの統計カウンターを表示する。

パラメーター

EPSR　EPSR ドメイン名。省略時および ALL 指定時はすべての EPSR ドメインの情報が表示される。

入力・出力・画面例

```
Manager > show epsr counter

 EPSR Counters
------------------------------------------------------------------------------
 Name: domain_two
  Receive:                                Transmit:
  Total EPSR Packets             4674     Total EPSR Packets            2
  Health                         4671     Health                        0
  Ring Up                           2     Ring Up                           2
  Ring Down                         0     Ring Down                         0
  Link Down                         1     Link Down                         0
  Invalid EPSR Packets              0

 Name: domain_one
  Receive:                                Transmit:
  Total EPSR Packets             1609     Total EPSR Packets                3
  Health                         1603     Health                            0
  Ring Up                           3     Ring Up                           0
  Ring Down                         3     Ring Down                         0
  Link Down                         0     Link Down                         3
  Invalid EPSR Packets              0
------------------------------------------------------------------------------
```

Name	EPSR ドメイン名
Receive セクション	受信パケット数が表示される

Total EPSR Packets	受信した EPSR 制御パケットの総数
Health	受信した Healthcheck メッセージの数
Ring Up	受信した Ring Up メッセージの数
Ring Down	受信した Ring Down メッセージの数
Link Down	受信した Link Down メッセージの数
Invalid EPSR Packets	無効な EPSR 制御パケットの数
Transmit セクション	送信パケット数が表示される
Total EPSR Packets	送信した EPSR 制御パケットの総数
Health	送信した Healthcheck メッセージの数。常に 0
Ring Up	送信した Ring Up メッセージの数
Ring Down	送信した Ring Down メッセージの数。常に 0
Link Down	送信した Link Down メッセージの数

表 16:

関連コマンド

SHOW EPSR（155 ページ）

SHOW EPSR DEBUG

カテゴリー：スイッチング / EPSR アウェア

SHOW EPSR[={*epsrname*|ALL}] **DEBUG**

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

解説

EPSR ドメインで有効になっているデバッグオプションを表示する。

パラメーター

EPSR　EPSR ドメイン名。省略時および ALL 指定時はすべての EPSR ドメインの情報が表示される。

入力・出力・画面例

```
Manager > show epsr debug

 EPSR Name           Enabled Debug Modes       Output         Timeout
------------------------------------------------------------------------------
 domain_one          None
------------------------------------------------------------------------------
```

EPSR Name	EPSR ドメイン名
Enabled Debug Modes	現在有効になっている EPSR デバッグオプション。INFO（EPSR に関する全般的情報を表示）、MSG（EPSR パケットをデコードして表示）、PKT（EPSR パケットを ASCII 表示）、STATE（EPSR の状態遷移を表示）、ALL（すべてのオプション）、None（なし）がある
Output	デバッグ情報の出力先（仮想端末（TTY）番号）
Timeout	デバッグオプションの残り有効期間（秒）

表 17:

関連コマンド

SHOW EPSR（155 ページ）

SHOW LACP

カテゴリー：スイッチング / LACP（IEEE 802.3ad）

SHOW LACP

解説

LACP の一般情報を表示する。

入力・出力・画面例

```
Manager > show lacp

LACP Information
--------------------------------------------------------------------------------
  Status ......................... Enabled
  Actor System Priority ........... 32768
  Actor System .................... 00-00-cd-24-02-0e
  Address learn thrash action ..... Learn Disable
  Address learn thrash timeout .... 1 second
  Loop detection action ........... Link Down
  Loop detection block timeout .... 1 second
  LACP Ports ...................... 1-24
    Active ........................ 1-24
    Passive ....................... None
```

Status	LACP モジュールの状態。Enabled か Disabled
Actor System Priority	システムプライオリティー
Actor System	システム ID（MAC アドレス）
Address learn thrash action	MAC アドレススラッシング検出時の動作。None（何もしない）、Learn Disable（トランクグループ内の全ポートで MAC アドレスの学習を停止する）、Port Disable（トランクグループ内の全ポートをディセーブルにする）、VLAN Disable（スラッシングが発生した VLAN に対してのみトランクグループ内の全ポートをディセーブルにする）、Link Down（トランクグループ内の全ポートを物理的にリンクダウンさせる）のいずれか

Address learn thrash timeout	MAC アドレススラッシング検出時の動作の持続時間（秒）。None は無期限であることを示す
Loop detection action	ループ検出時の動作。Port Disable（トランクグループ内の全ポートをディセーブルにする）、VLAN Disable（ループが発生した VLAN に対してのみトランクグループ内の全ポートをディセーブルにする）、Link Down（トランクグループ内の全ポートを物理的にリンクダウンさせる）、Log Only（ログの記録のみ）、None（何もしない）のいずれか。
Loop detection block timeout	ループ検出時の動作の持続時間（秒）。None は無期限であることを示す。
LACP Ports	LACP の管理下にあるポートの一覧
Active	LACP の管理下にあるポートのうち、Active モードで動作しているものの一覧
Passive	LACP の管理下にあるポートのうち、Passive モードで動作しているものの一覧

表 18:

関連コマンド

DISABLE LACP（77 ページ）
ENABLE LACP（94 ページ）
SET LACP（123 ページ）
SHOW LACP PORT（162 ページ）

SHOW LACP PORT

カテゴリー：スイッチング / LACP（IEEE 802.3ad）

SHOW LACP PORT[={*port-list*|ALL}]

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）

解説

スイッチポートの LACP 関連情報を表示する。

パラメーター

PORT　ポート番号。

入力・出力・画面例

```
Manager > show lacp port=1,5
LACP Port Information
------------------------------------------------------------------------------

Actor Port ....................... 1
  Trunk Group ................ lacp26     Partner Information:
  Selected .................. Selected      Partner Sys Priority ........ 32768
  Port Priority ............... 32768      Partner System .. 00-00-f4-27-2c-74
  LACP Port Number ................ 1      Port Key ....................... 3
  Port Key ....................... 2      Port Priority ............... 32768
    Admin Key ..................... 1      Port Number ..................... 1
  Mode ...................... Active      Mode ....................... Active
  Periodic ..................... Fast      Periodic ..................... Fast
  Individual ..................... No      Individual ..................... No
  Synchronised .................. Yes      Synchronised .................. Yes
  Collecting .................... Yes      Collecting .................... Yes
  Distributing .................. Yes      Distributing .................. Yes
  Defaulted ...................... No      Defaulted ...................... No
  Expired ........................ No      Expired ........................ No
  Actor Churn .................... No
  Partner Churn .................. No

Actor Port ....................... 5
  Trunk Group ..................... -     Partner Information:
  Selected .................. Selected      Partner Sys Priority ............ 0
  Port Priority ............... 32768      Partner System .. 00-00-00-00-00-00
  LACP Port Number ................ 5      Port Key ....................... 0
  Port Key ....................... 1      Port Priority ................... 0
    Admin Key ..................... 1      Port Number ..................... 0
```

```
  Mode ..................... Active       Mode ..................... Passive
  Periodic ..................... Fast     Periodic ..................... Fast
  Individual ..................... No     Individual ..................... Yes
  Synchronised .................. Yes     Synchronised ................... No
  Collecting ..................... No     Collecting ..................... Yes
  Distributing ................... No     Distributing ................... Yes
  Defaulted ..................... Yes     Defaulted ..................... Yes
  Expired ....................... No      Expired ....................... No
  Actor Churn ................... No
  Partner Churn ................. No

--------------------------------------------------------------------------------
```

Actor Port	ポート番号
Port is LACP Disabled - Port in a Manual Trunk	該当ポートが手動設定されたトランクポートであるため、LACP が自動的に無効化されたことを示す
Port is LACP Disabled - Half Duplex Link	該当ポートが Half Duplex で動作しているため、LACP が自動的に無効化されたことを示す
Trunk Group	所属先のトランクグループ名。LACP によって自動設定されたトランクグループには「lacpXXXX」形式の名前が自動的に割り当てられる（XXXX は SHOW INTERFACE コマンドで表示されるインターフェースインデックス）。トランクグループに所属していない場合は「-」と表示される
Selected	LACP の状態。Selected（LACP の管理下にある）、Standby（LACP の管理下にあり、現在スタンバイ状態である）、Unselected（LACP の管理下にない）がある
Priority	LACP ポートプライオリティー
LACP Port Number	エンコードされたポート番号
Port Key	LACP ポート鍵
Admin Key	LACP ポート鍵のもととなる設定可能値（ADMINKEY）
Mode	LACP 動作モード。Active、Passive のどちらか
Periodic	Active モード時の LACP パケットの送信間隔。Fast（1 秒）、Slow（30 秒）のどちらか
Individual	Aggregation フラグの状態。Yes（Individual = 同一トランクグループを構成可能な他のポートがない）、No（Aggregatable = 同一トランクグループを構成可能な他のポートがある）のどちらか

Synchronised	Sychronization フラグの状態。Yes（IN_SYNC）、No（OUT_OF_SYNC）のどちらか
Collecting	Collecting フラグの状態。Yes（パケットを受信できる）、No（パケットを受信できない）のどちらか
Distributing	Distributing フラグの状態。Yes（パケットを送信できる）、No（パケットを送信できない）のどちらか
Defaulted	Defaulted フラグの状態。Yes（対向機器から LACP パケットを受け取っていないため、対向機器の情報としてデフォルトの値を仮定している）、No（対向機器から受信した LACP パケットの情報を使っている）
Expired	Expired フラグの状態。Yes（Receive Machine が EXPIRED 状態にある）、No（Receive Machine が EXPIRED 状態にない）
Actor Churn	自ポート側で Churn（Synchronized フラグが安定せず、一定時間内に LACP グループに所属できなかった状態）を検出したかどうか。Yes（Churn を検出した）、No（Churn を検出していない）
Partner Churn	対向ポート側で Churn（Synchronized フラグが安定せず、一定時間内に LACP グループに所属できなかった状態）を検出したかどうか。Yes（Churn を検出した）、No（Churn を検出していない）
Partner Information セクション	対向する機器・ポートの情報が表示される。
Partner Sys Priority	対向機器の LACP システムプライオリティー
Partner System	対向機器の LACP システム ID（MAC アドレス）
Port Key	対向機器の LACP ポート鍵
Port Priority	対向機器の LACP ポートプライオリティー
Port Number	対向機器のポート番号
Mode	対向機器の LACP 動作モード。Active、Passive のどちらか
Periodic	対向機器の LACP パケットの送信間隔。Fast（1 秒）、Slow（30 秒）のどちらか
Individual	対向機器の Aggregation フラグの状態

Synchronised	対向機器の Synchronization フラグの状態
Collecting	対向機器の Collecting フラグの状態
Distributing	対向機器の Distributing フラグの状態
Defaulted	対向機器の Defaulted フラグの状態
Expired	対向機器の Expired フラグの状態

表 19:

関連コマンド

ADD LACP PORT（59 ページ）
SET LACP PORT（125 ページ）
SHOW LACP（160 ページ）

SHOW LACP TRUNK

カテゴリー：スイッチング / LACP（IEEE 802.3ad）

SHOW LACP TRUNK

解説

LACP によって自動生成されたトランクグループの情報を表示する。

入力・出力・画面例

```
Manager > show lacp trunk

LACP Dynamic Trunk Group Information
--------------------------------------------------------------------------------

 Trunk group name .......... lacp26:
   Speed ................... 100 Mbps
   Ports in Trunk .......... 1-4
   LAG ID:
   [(8000,00-00-cd-24-02-0e,0002,00,0000),(8000,00-00-f4-27-2c-74,0003,00,0000)]

--------------------------------------------------------------------------------
```

Trunk group name	トランクグループ名。LACPによって自動設定されたトランクグループには「lacp-XXXX」形式の名前が自動的に割り当てられる（XXXX はSHOW INTERFACE コマンドで表示されるインターフェースインデックス）
Speed	トランクポートの通信速度。10Mbps、100Mbps、1000Mbps、-（未設定）のいずれか
Ports in Trunk	所属ポート
LAG ID	LAG ID（Link Aggregation Identifier）。自システム（Actor）と対向システム（Partner）それぞれのシステムプライオリティー、システム ID（MAC アドレス）、ポート鍵、ポートプライオリティー、ポート番号を組み合わせたもの

表 20:

関連コマンド

ADD LACP PORT（59 ページ）
SET LACP PORT（125 ページ）
SHOW LACP（160 ページ）
SHOW LACP PORT（162 ページ）

SHOW PORTAUTH

カテゴリー：スイッチング / ポート認証

SHOW PORTAUTH[={8021X|MACBASED}]

解説

ポート認証機能（802.1X 認証、MAC ベース認証）の全般的な設定と状態を表示する。

パラメーター

PORTAUTH　認証メカニズム。8021X（802.1X 認証）、MACBASED（MAC ベース認証）から選択する。
省略時は 8021X と見なされる。

入力・出力・画面例

```
Manager > show portauth=8021x

802.1X System
-------------------------------------------------------------------------------
  SystemAuthControl............. ENABLED
  Global Username............... portAuthPortAuth
  Global Password............... portAuthPortAuth
  Global Encryption Method..... Standard
  Number of Multi Supplicants.. 0   (limit 480)


  Port                    PAE Capabilities                    Protocol Version
  ---------------------------------------------------------------------------
  port1               Authenticator (Single)                        1
  port2               Authenticator (Single)                        1
  port3               Authenticator (Single)                        1
  port4               Authenticator (Single)                        1
  port5               Authenticator (Single)                        1
  port6               Authenticator (Single)                        1
  port7               Authenticator (Single)                        1
  port8               Authenticator (Multi)                         1
  port9               None                                          1
  port10              None                                          1
  port11              None                                          1
  port12              None                                          1
  port13              None                                          1
  port14              None                                          1
  port15              None                                          1
  port16              None                                          1
```

```
  port17              None                                          1
  port18              None                                          1
  port19              None                                          1
  port20              None                                          1
  port21              None                                          1
  port22              None                                          1
  port23              None                                          1
  port24              None                                          1
  port25              None                                          1
  port26              None                                          1

Manager > show portauth=macbased

MAC Based Authentication System
-------------------------------------------------------------------------------
  SystemAuthControl..... ENABLED
  Number of Supplicants........ 0   (limit 480)


  Port                PAE Status
  ------------------------------
  port1               Disabled
  port2               Disabled
  port3               Disabled
  port4               Disabled
  port5               Disabled
  port6               Disabled
  port7               Disabled
  port8               Disabled
  port9               Enabled
  port10              Enabled
  port11              Enabled
  port12              Enabled
  port13              Enabled
  port14              Enabled
  port15              Enabled
  port16              Enabled
  port17              Disabled
  port18              Disabled
  port19              Disabled
  port20              Disabled
  port21              Disabled
  port22              Disabled
  port23              Disabled
  port24              Disabled
  port25              Disabled
  port26              Disabled
```

SystemAuthControl	802.1X 認証モジュールの有効・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
Number of Multi Supplicants	Supplicant の数（カッコ内はシステムがサポートしている Supplicant の最大数）
Port	スイッチポートのインターフェース名
PAE Capabilities	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 21: PORTAUTH=8021X のとき

SystemAuthControl	MAC ベース認証機能の有効・無効
Number of Supplicants	Supplicant の数（カッコ内はシステムがサポートしている Supplicant の最大数）
Port	スイッチポートのインターフェース名
PAE Capabilities	該当スイッチポートにおける MAC ベース認証の有効・無効

表 22: PORTAUTH=MACBASED のとき

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE（53 ページ）
ENABLE PORTAUTH（95 ページ）
ENABLE PORTAUTH PORT（96 ページ）
SET PORTAUTH PORT（127 ページ）
SET PORTAUTH PORT SUPPLICANTMAC（131 ページ）
SHOW PORTAUTH COUNTER（170 ページ）
SHOW PORTAUTH MULTISUPPLICANT PORT（173 ページ）
SHOW PORTAUTH PORT（177 ページ）
SHOW PORTAUTH TIMER（183 ページ）

SHOW PORTAUTH COUNTER

カテゴリー：スイッチング / ポート認証

SHOW PORTAUTH[=8021X] **COUNTER PORT=**{***port-list***|**ALL**}

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）

解説

指定ポートの 802.1X 統計カウンターを表示する。

パラメーター

PORTAUTH　認証メカニズム。本コマンドでは 8021X（802.1X 認証）のみ有効。省略時は 8021X と見なされるため、特に指定する必要はない。

PORT　スイッチポート。複数指定が可能。

入力・出力・画面例

```
Manager > show portauth counter port=5
802.1X Counters
-------------------------------------------------------------------------------
  port5
  PAE Type..................... Authenticator
    Last EAPOL Frame Version.... 1
    Last EAPOL Frame Source..... 00-00-e2-59-56-48

    Receive                            Transmit
       EAPOL Frames..............    32    EAPOL Frames..............   122
       EAPOL Start Frames........     0    EAP Req/Id Frames.........    70
       EAPOL Logoff Frames.......     0    EAP Request Frames........     3
       EAP Resp/Id Frames........    29
       EAP Response Frames.......     3
       EAP Length Error Frames....    0
       Invalid EAPOL Frames......     0

Manager > show portauth counter port=7
802.1X Counters
-------------------------------------------------------------------------------
  port7
  PAE Type..................... Both

  Authenticator - Attached Supplicant(s)
    Last EAPOL Frame Source..... 00-00-f4-95-30-6a
```

```
  MAC Address.................. 00-00-e2-59-56-48
  Last EAPOL Frame Version..... 1

     Receive                            Transmit
        EAPOL Frames.............     3    EAPOL Frames.............     3
        EAPOL Start Frames.......     0    EAP Req/Id Frames........     1
        EAPOL Logoff Frames......     0    EAP Request Frames........    1
        EAP Resp/Id Frames.......     2
        EAP Response Frames......     1
        EAP Length Error Frames....   0
        Invalid EAPOL Frames.....     0

  MAC Address.................. 00-00-f4-95-30-6a
  Last EAPOL Frame Version..... 1

     Receive                            Transmit
        EAPOL Frames.............     3    EAPOL Frames.............     3
        EAPOL Start Frames.......     0    EAP Req/Id Frames........     1
        EAPOL Logoff Frames......     0    EAP Request Frames........    1
        EAP Resp/Id Frames.......     2
        EAP Response Frames......     1
        EAP Length Error Frames....   0
        Invalid EAPOL Frames.....     0

Supplicant
  Last EAPOL Frame Version.... 0
  Last EAPOL Frame Source..... ff-ff-ff-ff-ff-ff

  Receive                          Transmit
     EAPOL Frames.............     0    EAPOL Frames.............     3
     EAP Req/Id Frames........     0    EAPOL Start Frames.......     3
     EAP Request Frames.......     0    EAPOL Logoff Frames......     0
     Invalid EAPOL Frames.....     0    EAP Resp/Id Frames.......     0
     EAP Length Error Frames....   0    EAP Response Frames......     0
```

Interface	スイッチポートのインターフェース名
PAE Type	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 23:

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE（53 ページ）
ENABLE PORTAUTH（95 ページ）
ENABLE PORTAUTH PORT（96 ページ）
SET PORTAUTH PORT（127 ページ）
SET PORTAUTH PORT SUPPLICANTMAC（131 ページ）
SHOW PORTAUTH（167 ページ）
SHOW PORTAUTH MULTISUPPLICANT PORT（173 ページ）
SHOW PORTAUTH PORT（177 ページ）
SHOW PORTAUTH TIMER（183 ページ）

SHOW PORTAUTH MULTISUPPLICANT PORT

カテゴリー：スイッチング / ポート認証

SHOW PORTAUTH[=8021X|MACBASED] **MULTISUPPLICANT PORT=**{***port-list***|**ALL**}
[SUPPLICANTMAC=*macadd*]

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）
macadd: MAC アドレス（xx-xx-xx-xx-xx-xx の形式）

解説

802.1X Multi-Supplicant モードで動作している Authenticator ポート、または、MAC ベース認証ポートの基本設定、および、接続/設定されている Supplicant の情報を表示する。

パラメーター

PORTAUTH　認証メカニズム。8021X（802.1X 認証）、MACBASED（MAC ベース認証）から選択する。省略時は 8021X と見なされる。
PORT　スイッチポート。複数指定が可能。
SUPPLICANTMAC　Supplicant の MAC アドレス。

入力・出力・画面例

```
Manager > show portauth multisupplicant port=8
802.1X Multi-Supplicant Configuration
--------------------------------------------------------------------------------
Interface: port8
  Multi-Supplicant Authenticator
  Number of Multi Supplicants.......... 1
    Default Settings
          AuthControlPortControl........ Auto
          quietPeriod................... 60
          txPeriod...................... 30
          suppTimeout................... 30
          serverTimeout................. 30
          maxReq........................ 2
          reAuthMax..................... 2
          reAuthPeriod.................. 3600
          reAuthEnabled................. False
          secureVlan.................... On
          trap.......................... None
          mibReset...................... Enabled
          vlanAssignment................ Enabled

    Attached Supplicant(s)
```

```
      MAC Address...................... 00-00-f4-95-30-6a
          Authenticator PAE State....... AUTHENTICATED
          Port Status................... authorised
          Backend Authenticator State... IDLE
          AuthControlPortControl........ Auto
          quietPeriod................... 60
          txPeriod...................... 30
          suppTimeout................... 30
          serverTimeout................. 30
          maxReq........................ 2
          reAuthMax..................... 2
          reAuthPeriod.................. 1800
          reAuthEnabled................. True
          keyTransmissionEnabled........ False (not supported)
          adminControlledDirections..... Both (not supported)
          secureVlan.................... On
          trap.......................... None
          mibReset...................... Enabled
          vlanAssignment................ Enabled

Manager > show portauth=macbased multisupplicant port=9

MAC Based Authentication Configuration
------------------------------------------------------------------------------
Interface: port9
  PAE Status............... Enabled
  Number of Supplicants.... 1
  Default Settings
        AuthControlPortControl........ Auto
        quietPeriod................... 60
        reAuthPeriod.................. 3600
        reAuthEnabled................. False
        secureVlan.................... On
        trap.......................... None
        mibReset...................... Enabled
        vlanAssignment................ Enabled

  Attached Supplicant(s)
    MAC Address..................... 00-00-f4-22-33-44
        Authenticator PAE State....... INITIALISE
        Port Status................... unauthorised
        Backend Authenticator State... IDLE
        AuthControlPortControl........ Auto
        quietPeriod................... 60
        reAuthPeriod.................. 3600
        reAuthEnabled................. False
        secureVlan.................... On
        trap.......................... Both
        mibReset...................... Enabled
        vlanAssignment................ Enabled
```

Interface	スイッチポートのインターフェース名
Number of Multi Supplicants	Multi-Supplicant モードにおける 802.1X Supplicant の数
Default Settings	明示的に設定していない Supplicant に適用される設定値の一覧
Attached Supplicant(s)	明示的に設定した Supplicant に適用される設定値の一覧、および、ポート配下に接続されている Supplicant の情報一覧
Authenticator PAE State	Authenticator としての状態。INITIALISE（初期化）、DISCONNECTED（未接続）、CONNECTING（接続中）、AUTHENTICATING（認証中）、AUTHENTICATED（認証済み）、ABORTING（認証断念中）、HELD（待機中）、FORCEAUTH（「認証済み」に固定設定）、FORCEUNAUTH（「未認証」に固定設定）のいずれか
Port Status	ポートの状態。unauthorised（未認証）か authorised（認証済み）
Backend Authenticator State	認証機構の状態。IDLE（アイドル）、INITIALISE（初期化）、RESPONSE（Supplicant から応答受信）、REQUEST（認証サーバーに要求送信）、SUCCESS（認証成功）、FAIL（認証失敗）、TIMEOUT（タイムアウト）のいずれか
AuthControlPortControl	手動設定によるポート状態。Auto（認証結果に応じて変動。通常の設定）、forceUnauthorised（未認証に固定）、forceAuthorised（認証済みに固定）のいずれか
quietPeriod	認証失敗後、Supplicant との通信を拒否する期間（秒）
txPeriod	Supplicant に EAPOL パケットを再送信する間隔（秒）
suppTimeout	Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間（秒）
serverTimeout	RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間（秒）
maxReq	Supplicant に対する EAPOL-Request パケットの最大再送回数
reAuthMax	再認証時における EAPOL-Request パケットの最大再送回数
reAuthPeriod	Supplicant を再認証する間隔（秒）
reAuthEnabled	再認証の有効・無効
keyTransmissionEnabled	未サポート
adminControlledDirections	未サポート
secureVlan	ダイナミック VLAN 有効時、2 番目以降に接続された Supplicant の所属 VLAN が、最初に認証を通った Supplicant と同じでないと認証を許可しない機能の有効・無効
trap	ポート認証機能に関する SNMP トラップを送信するかどうか。また、どのようなときに送信するか
mibReset	古い Supplicant 情報をエージアウトするかどうか
vlanAssignment	ダイナミック VLAN の有効・無効

表 24: PORTAUTH=8021X のとき

Interface	スイッチポートのインターフェース名

PAE Status	該当スイッチポートにおける MAC ベース認証の有効・無効
Number of Supplicants	MAC ベース Supplicant の数
Default Settings	明示的に設定していない Supplicant に適用される設定値の一覧
Attached Supplicant(s)	明示的に設定した Supplicant に適用される設定値の一覧、および、ポート配下に接続されている Supplicant の情報一覧
Authenticator PAE State	Authenticator としての状態。INITIALISE（初期化）、DISCONNECTED（未接続）、CONNECTING（接続中）、AUTHENTICATING（認証中）、AUTHENTICATED（認証済み）、ABORTING（認証断念中）、HELD（待機中）、FORCEAUTH（「認証済み」に固定設定）、FORCEUNAUTH（「未認証」に固定設定）のいずれか
Port Status	ポートの状態。unauthorised（未認証）か authorised（認証済み）
Backend Authenticator State	認証機構の状態。IDLE（アイドル）、INITIALISE（初期化）、RESPONSE（Supplicant から応答受信）、REQUEST（認証サーバーに要求送信）、SUCCESS（認証成功）、FAIL（認証失敗）、TIMEOUT（タイムアウト）のいずれか
AuthControlPortControl	手動設定によるポート状態。Auto（認証結果に応じて変動。通常の設定）、forceUnauthorised（未認証に固定）、forceAuthorised（認証済みに固定）のいずれか
quietPeriod	認証失敗後、Supplicant との通信を拒否する期間（秒）
reAuthPeriod	Supplicant を再認証する間隔（秒）
reAuthEnabled	再認証の有効・無効
secureVlan	ダイナミック VLAN 有効時、2 番目以降に接続された Supplicant の所属 VLAN が、最初に認証を通った Supplicant と同じでないと認証を許可しない機能の有効・無効
trap	ポート認証機能に関する SNMP トラップを送信するかどうか。また、どのようなときに送信するか
mibReset	古い Supplicant 情報をエージアウトするかどうか
vlanAssignment	ダイナミック VLAN の有効・無効

表 25: PORTAUTH=MACBASED のとき

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE（53 ページ）
ENABLE PORTAUTH（95 ページ）
ENABLE PORTAUTH PORT（96 ページ）
SET PORTAUTH PORT（127 ページ）
SET PORTAUTH PORT SUPPLICANTMAC（131 ページ）
SHOW PORTAUTH（167 ページ）
SHOW PORTAUTH COUNTER（170 ページ）
SHOW PORTAUTH PORT（177 ページ）
SHOW PORTAUTH TIMER（183 ページ）

SHOW PORTAUTH PORT

カテゴリー：スイッチング / ポート認証

SHOW PORTAUTH[={8021X|MACBASED}] **PORT=**{***port-list***|**ALL**}

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）

解説

指定ポートにおけるポート認証機能（802.1X 認証、MAC ベース認証）の設定を表示する。

パラメーター

PORTAUTH　認証メカニズム。8021X（802.1X 認証）、MACBASED（MAC ベース認証）から選択する。省略時は 8021X と見なされる。

PORT　ポート番号。複数指定が可能。

入力・出力・画面例

```
Manager > show portauth=8021x port=1

802.1X Configuration
--------------------------------------------------------------------------------
Interface: port1
  PAE Type.............. Authenticator
          Authenticator PAE State....... AUTHENTICATED
          Port Status................... authorised
          Backend Authenticator State... IDLE
          AuthControlPortControl........ Auto
          quietPeriod................... 60
          txPeriod...................... 30
          suppTimeout................... 30
          serverTimeout................. 30
          maxReq........................ 2
          reAuthMax..................... 2
          reAuthPeriod.................. 3600
          reAuthEnabled................. False
          piggyBack..................... True
          keyTransmissionEnabled........ False (not supported)
          adminControlledDirections..... Both (not supported)
          guestVlan..................... None (VLAN ID=0)
          trap.......................... None
          vlanAssignment................ Enabled

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

```
802.1X Configuration
--------------------------------------------------------------------------------
Interface: port7
  PAE Type.............. Both

  Multi-Supplicant Authenticator
    Default Settings
          AuthControlPortControl........ Auto
          quietPeriod................... 60
          txPeriod...................... 30
          suppTimeout................... 30
          serverTimeout................. 30
          maxReq........................ 2
          reAuthMax..................... 2
          reAuthPeriod.................. 3600
          reAuthEnabled................. False
          secureVlan.................... On
          trap.......................... None
          mibReset...................... Enabled
          vlanAssignment................ Enabled

    Attached Supplicant(s)
      MAC Address..................... 00-00-e2-59-56-48
          Authenticator PAE State....... AUTHENTICATED
          Port Status................... authorised
          Backend Authenticator State... IDLE
          AuthControlPortControl........ Auto
          quietPeriod................... 60
          txPeriod...................... 30
          suppTimeout................... 30
          serverTimeout................. 30
          maxReq........................ 2
          reAuthMax..................... 2
          reAuthPeriod.................. 3600
          reAuthEnabled................. False
          keyTransmissionEnabled........ False (not supported)
          operControlledDirections...... False (not supported)
          secureVlan.................... On
          trap.......................... None
          mibReset...................... Enabled
          vlanAssignment................ Disabled

Manager > show portauth=macbased port=10

MAC Based Authentication Configuration
--------------------------------------------------------------------------------
Interface: port10
  PAE Status.............. Enabled
  Number of Supplicants.... 1
  Default Settings
```

```
       AuthControlPortControl........ Auto
       quietPeriod................... 60
       reAuthPeriod.................. 3600
       reAuthEnabled................. False
       secureVlan.................... On
       trap.......................... None
       mibReset...................... Enabled
       vlanAssignment................ Enabled

 Attached Supplicant(s)
   MAC Address..................... 00-00-f4-42-01-6b
       Authenticator PAE State....... AUTHENTICATED
       Port Status................... authorised
       Backend Authenticator State... IDLE
       AuthControlPortControl........ Auto
       quietPeriod................... 60
       reAuthPeriod.................. 3600
       reAuthEnabled................. False
       secureVlan.................... On
       trap.......................... None
       mibReset...................... Enabled
       vlanAssignment................ Enabled
```

Interface	スイッチポートのインターフェース名
PAE Type	802.1X 認証におけるスイッチポートの役割。Authenticator、Supplicant、Both のいずれか
	Authenticator としての設定
MAC Address	Supplicant の MAC アドレス
Authenticator PAE State	Authenticator としての状態。INITIALISE（初期化）、DISCONNECTED（未接続）、CONNECTING（接続中）、AUTHENTICATING（認証中）、AUTHENTICATED（認証済み）、ABORTING（認証断念中）、HELD（待機中）、FORCEAUTH（「認証済み」に固定設定）、FORCEUNAUTH（「未認証」に固定設定）のいずれか
Port Status	ポートの状態。unauthorised（未認証）か authorised（認証済み）
Backend Authenticator State	認証機構の状態。IDLE（アイドル）、INITIALISE（初期化）、RESPONSE（Supplicant から応答受信）、REQUEST（認証サーバーに要求送信）、SUCCESS（認証成功）、FAIL（認証失敗）、TIMEOUT（タイムアウト）のいずれか
AuthControlPortControl	手動設定によるポート状態。Auto（認証結果に応じて変動。通常の設定）、forceUnauthorised（未認証に固定）、forceAuthorised（認証済みに固定）のいずれか
quietPeriod	認証失敗後、Supplicant との通信を拒否する期間（秒）
txPeriod	Supplicant に EAPOL パケットを再送信する間隔（秒）

suppTimeout	Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間（秒）
serverTimeout	RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間（秒）
maxReq	Supplicant に対する EAPOL-Request パケットの最大再送回数
reAuthMax	再認証時における EAPOL-Request パケットの最大再送回数
reAuthPeriod	Supplicant を再認証する間隔（秒）
reAuthEnabled	再認証の有効・無効
piggyBack	Single-Supplicant モードにおいて、最初に接続された Supplicant の認証に成功した後、他のデバイスからのパケットも許可するかどうか
keyTransmissionEnabled	未サポート
adminControlledDirections	未サポート
secureVlan	ダイナミック VLAN 有効時、2 番目以降に接続された Supplicant の所属 VLAN が、最初に認証を通った Supplicant と同じでないと認証を許可しない機能の有効・無効
trap	ポート認証機能に関する SNMP トラップを送信するかどうか。また、どのようなときに送信するか
mibReset	古い Supplicant 情報をエージアウトするかどうか
vlanAssignment	ダイナミック VLAN の有効・無効
	Supplicant としての設定
heldPeriod	認証失敗後、Authenticator との通信を試みない期間（秒）
authPeriod	Authenticator に EAP-Response パケットを送信した後、Authenticator からの応答を待つ時間（秒）
startPeriod	Authenticator に EAPOL-Start パケットを再送信する間隔（秒）
maxStart	EAPOL-Start パケットの最大送信回数。Supplicant ポートは、EAPOL-Start パケットを MAXSTART 回送信しても応答がない場合、Authenticator が存在しておらずポート認証の必要はないと判断する
Supplicant PAE State	Supplicant としての状態。Authorised と Unauthorised のいずれか

表 26: PORTAUTH=8021X のとき

Interface	スイッチポートのインターフェース名
PAE Status	該当スイッチポートにおける MAC ベース認証の有効・無効
Number of Supplicants	MAC ベース Supplicant の数
MAC Address	Supplicant の MAC アドレス
Authenticator PAE State	Authenticator としての状態。INITIALISE（初期化）、DISCONNECTED（未接続）、CONNECTING（接続中）、AUTHENTICATING（認証中）、AUTHENTICATED（認証済み）、ABORTING（認証断念中）、HELD（待機中）、FORCEAUTH（「認証済み」に固定設定）、FORCEUNAUTH（「未認証」に固定設定）のいずれか

Port Status	ポートの状態。unauthorised（未認証）か authorised（認証済み）
Backend Authenticator State	認証機構の状態。IDLE(アイドル)、INITIALISE(初期化)、RESPONSE(Supplicant から応答受信)、REQUEST（認証サーバーに要求送信)、SUCCESS（認証成功)、FAIL（認証失敗)、TIMEOUT（タイムアウト）のいずれか
AuthControlPortControl	手動設定によるポート状態。Auto（認証結果に応じて変動。通常の設定)、forceUnauthorised（未認証に固定)、forceAuthorised（認証済みに固定）のいずれか
quietPeriod	認証失敗後、Supplicant との通信を拒否する期間（秒）
reAuthPeriod	Supplicant を再認証する間隔（秒）
reAuthEnabled	再認証の有効・無効
secureVlan	ダイナミック VLAN 有効時、2 番目以降に接続された Supplicant の所属 VLAN が、最初に認証を通った Supplicant と同じでないと認証を許可しない機能の有効・無効
trap	ポート認証機能に関する SNMP トラップを送信するかどうか。また、どのようなときに送信するか
mibReset	古い Supplicant 情報をエージアウトするかどうか
vlanAssignment	ダイナミック VLAN の有効・無効

表 27: PORTAUTH=MACBASED のとき

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE（53 ページ）
ENABLE PORTAUTH（95 ページ）
ENABLE PORTAUTH PORT（96 ページ）
SET PORTAUTH PORT（127 ページ）
SET PORTAUTH PORT SUPPLICANTMAC（131 ページ）
SHOW PORTAUTH（167 ページ）
SHOW PORTAUTH COUNTER（170 ページ）
SHOW PORTAUTH MULTISUPPLICANT PORT（173 ページ）
SHOW PORTAUTH TIMER（183 ページ）

SHOW PORTAUTH TIMER

カテゴリー：スイッチング / ポート認証

SHOW PORTAUTH[={8021X|MACBASED}] **TIMER PORT=**{***port-list***|**ALL**}

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）

解説

指定ポートにおけるポート認証機能（802.1X 認証または MAC ベース認証）の各種タイマー（残り時間）を表示する。

パラメーター

PORTAUTH　認証メカニズム。8021X（802.1X 認証）、MACBASED（MAC ベース認証）から選択する。省略時は 8021X と見なされる。

PORT　スイッチポート。複数指定が可能。

入力・出力・画面例

```
Manager > show portauth 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）。TXPERIOD パラメーターの値が初期値となる
	Supplicant 用タイマー
authWhile	Authenticator に EAP-Response パケットを送信した後、Authenticator からの応答を待つ時間（秒）。AUTHPERIOD パラメーターの値が初期値となる
heldWhile	認証失敗後、Authenticator との通信を試みない期間（秒）を示すタイマー。HELDPERIOD パラメーターの値が初期値となる
startWhen	Authenticator に EAPOL-Start パケットを送信するまでの待ち時間（秒）。STARTPERIOD パラメーターの値が初期値となる

表 28: PORTAUTH=8021X のとき

Interface	スイッチポートのインターフェース名
Supplicant	MAC ベース Supplicant の MAC アドレス
quietWhile	認証失敗後、Supplicant との通信を拒否する期間（秒）を示すタイマー。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

表 29: PORTAUTH=MACBASE のとき

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE（53 ページ）
ENABLE PORTAUTH（95 ページ）
ENABLE PORTAUTH PORT（96 ページ）
SET PORTAUTH PORT（127 ページ）
SET PORTAUTH PORT SUPPLICANTMAC（131 ページ）
SHOW PORTAUTH（167 ページ）
SHOW PORTAUTH MULTISUPPLICANT PORT（173 ページ）
SHOW PORTAUTH PORT（177 ページ）

SHOW RRPSNOOPING

カテゴリー：スイッチング / RRP Snooping

SHOW RRPSNOOPING

解説

RRP Snooping の状態、および、マスターポート一覧を表示する。

入力・出力・画面例

```
Manager > show rrpsnooping

RRP Snooping
--------------------------------------------------------------------------------
Status ........................... Enabled

    Vlan         Master     Virtual MAC Address     UpTime
  ----------------------------------------------------------------------------
    vlan1        2          00-00-5e-00-01-05       1 day, 06:03:17
    vlan100      10         00-e0-2b-00-00-85       00:00:39
--------------------------------------------------------------------------------
```

Status	RRP Snooping の状態。Enabled か Disabled のどちらか。
Vlan	Vlan ID
Master	マスターポート
Virtual MAC Address	ルーターの仮想 MAC アドレス
UpTime	マスターポートの切り替わりからの経過時間 (hh:mm:ss)

表 30:

関連コマンド

DISABLE RRPSNOOPING（80 ページ）
ENABLE RRPSNOOPING（100 ページ）

SHOW SWITCH

カテゴリー：スイッチング / 一般コマンド

SHOW SWITCH

解説

スイッチングモジュールの全般的情報を表示する。

入力・出力・画面例

```
Manager > show switch

 Switch Configuration
------------------------------------------------------------------------------
 Switch Address ..... 00-00-f4-12-34-56
 Learning ..... ON
 Learning log ..... DISABLED
 Ageing Timer ..... ON
 Number of Fixed Ports ..... 24
 Number of Uplink Ports ..... 0
 Mirroring ..... DISABLED
 Mirror port ..... None
 Ports mirroring on Rx ..... None
 Ports mirroring on Tx ..... None
 Ports mirroring on Both .... None
 Thrash limit ..... 10
 Number of WAN Interfaces ... -
 Name of Interface(s) ..... -
 Ageingtime ..... 300
 L3 Ageingtime ..... -
 UpTime ..... 01:04:33
 STP Forwarding ..... DISABLED
 Powersaving ..... Disabled

------------------------------------------------------------------------------
```

Switch Address	MAC アドレス
Learning	フォワーディングデータベースの自動学習機能。ON か OFF
Learning log	MAC アドレス学習ログの有効・無効。ENABLED か DISABLED
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	フロントポートの数

Number of Uplink Ports	アップリンクポートの数
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
Thrash limit	MAC アドレススラッシング（同一 MAC アドレスの登録ポートが頻繁に変更されること）の検出しきい値
Ageingtime	フォワーディングデータベースのエージングタイム
Uptime	再起動後の経過時間（時:分:秒の形式）。MIB-II オブジェクト sysUpTime と同じ。
STP Forwarding	BPDU 透過機能の状態。ENABLED か DISABLED
Powersaving	省電力モードの状態。有効（Enabled）または無効（Disabled）

表 31:

関連コマンド

RESET SWITCH（116 ページ）
SET SWITCH THRASHLIMIT（142 ページ）

SHOW SWITCH COUNTER

カテゴリー：スイッチング / 一般コマンド

SHOW SWITCH COUNTER

解説

スイッチングモジュールの統計カウンターを表示する。

入力・出力・画面例

```
Manager > show switch counter

 Switch Counters
-------------------------------------------------------------------------------
Switch instance:        0

Packet DMA counters:

  Receive:                              Transmit:
Packets                      71202      Packets                      71196
Discards                         0      Discards                         2
TooFewBuffers                    0      Aborts                           0
DescriptorsExhausteds            0      DescriptorAreaFilleds            0
QueueLength                      0      QueueLength                     12

  PCI bus counters:
ParityErrors                     0      ErrorChannel                     0
FatalErrors                      0      ErrorResets                      0

  General counters:
Resets                           0
-------------------------------------------------------------------------------
```

Packet DMA counters セクション	DMA に関するカウンターが表示される。
Receive サブセクション	受信パケットに関する統計が表示される。
Packets	スイッチチップから CPU に渡されたパケットの数
Discards	スイッチチップから受け取ったパケットのうち、受信キューが 4096 を超えたか、空きバッファー容量が 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
ErrorResets	未サポート
General counters セクション	一般的なカウンターが表示される。
Resets	エラーによる DMA チャンネルのリセット回数

表 32:

関連コマンド

RESET SWITCH（116 ページ）
SHOW SWITCH（187 ページ）

SHOW SWITCH LOOPDETECTION

カテゴリー：スイッチング / ポート

SHOW SWITCH LOOPDETECTION [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

LDF 検出機能の設定、状態、カウンターの情報を表示する。

パラメーター

COUNTER　LDF 検出機能のカウンター情報を表示する
PORT　ポート番号または ALL を指定する。省略時は ALL

入力・出力・画面例

```
Manager > show switch loopdetection port=1,2

LDF Interval:       10
LDF Rx Window:       3
                                                          Timeout
  Port          Enabled  Action     Status    Timeout    Remain  Tx port
  ------------------------------------------------------------------------
   1            Yes      vlan-dis   Normal    7          -
   2            Yes      vlan-dis   Blocking  7          4       2

Manager > show switch loopdetection counter port=1,2

Switch Loop Detection Counter

  Port          Tx         Rx        Rx Invalid     Last LDF Rx
  ------------------------------------------------------------------------
   1            309        0         0                    -
   2            147        20        0              26-Oct-2009 14:10:04
```

LDF Interval	LDF（Loop Detection Frame）の送信間隔（秒）
LDF Rx Window	送信した LDF の情報（LDF ID）をいくつまで保持するか
Port	ポート番号
Enabled	LDF 検出機能の状態。Yes（有効）か No（無効）
Action	該当スイッチポートでループを検出した場合の動作。port-dis（ポートを無効化する）、vlan-dis（ループを検出した VLAN に対してのみポートを無効化する）、link-dwn（ポートを物理的にリンクダウンさせる）、log-only（ポートの制御は行わず、ログへの記録と SNMP トラップ送信（有効時）のみを行う）、none（何もしない）のいずれか
Status	ループ検出状況。Normal（ループ未検出状態）、Detected（ループ検出状態）、Blocking（アクションによりブロッキングされた状態）のいずれか
Timeout	ループ検出時に行うアクションの実行後、アクション実行前の状態に戻るまでの時間の設定値（秒）
Timeout Remain	実行したアクションが実行前の状態に戻るまでに必要な残り時間。アクションに logonly を指定した場合は検出処理を再開するまでの時間（秒）
Tx port	このポートで受信された LDF が送信されたポートのポート番号

表 33:

Port	ポート番号
Tx	LDF の送信数
Rx	LDF の受信数
Rx Invalid	破棄された不正な LDF の数。受信 LDF フレーム内の LDF ID が、装置で記憶している LDF ID と異なっていた場合を含む
Last LDF Rx	最後に LDF を受信した日時

表 34: COUNTER 指定時

例

■ポート 1、2 の LDF 検出機能の設定、状態を表示する

```
SHOW SWITCH LOOPDETECTION PORT=1,2
```

■ポート 1、2 の LDF 検出機能のカウンター情報を表示する

```
SHOW SWITCH LOOPDETECTION COUNTER PORT=1,2
```

関連コマンド

DISABLE SWITCH LOOPDETECTION（81 ページ）
ENABLE SWITCH LOOPDETECTION（101 ページ）

RESET SWITCH LOOPDETECTION COUNTER（117 ページ）
SET SWITCH LOOPDETECTION（136 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}] [{SUMMARY|SECURITY}]

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。複数指定が可能。
SUMMARY　このオプションを指定したときは、ポート情報表示フォーマットを一覧形式にする。省略時は、各ポートの詳細情報が表示される。
SECURITY　ポートセキュリティー情報を表示する。

入力・出力・画面例

```
Manager > show switch port=1

 Switch Port Information
------------------------------------------------------------------------------
 Port ........................... 1
   Description ................... -
   Status ........................ ENABLED
   Link State .................... Up
   UpTime ........................ 01:14:44
   Port Media Type ............... ETHERNET CSMACD
   Configured speed/duplex ....... Autonegotiate
   Actual speed/duplex ........... 100 Mbps, full duplex
   MDI Configuretion (Polarity)  . Automatic(MDI-X)
   Configured master/slave mode .. Not applicable
   Actual master/slave mode ...... Not applicable
   Acceptable Frame Types ........ Admit All Frames
   Broadcast rate limit .......... -
   Multicast rate limit .......... -
   DLF rate limit ................ -
   Ingress rate limit ............ -
   Egress rate limit ............. -
   Learn limit ................... -
   Intrusion action .............. TrapContinue, LogContinue
   Current learned, lock state ... 0, not locked
   Address learn thrash status ... Not Detected
```

```
   Address learn thrash action ... Learn Disable
   Address learn thrash timeout .. 1 second
   VLAN Status Trap ............... OFF
   Relearn ........................ OFF
   Mirroring ...................... None
   Is this port mirror port ...... No
   VLAN(s) ........................ default (1)
   Enabled flow control(s) ....... Pause
   Send tagged pkts for VLAN(s) .. -
   Port-based VLAN ................ default (1)
   Ingress Filtering .............. OFF
   Trunk Group .................... -
   STP ............................ default
   IGMP Filter .................... None
   Max-groups/Joined .............. Undefined/0
   IGMP Max-groups Action ........ Deny
   Multicast filtering mode ...... (B) Forward all unregister groups
   Broadcast egress filtering .... OFF
   Loop detection status ......... Not Detected
   Loop detection action ......... Port Disable
   Loop detection block timeout .. 5
-------------------------------------------------------------------------------


Manager > show switch port=1-10 summary

 Port                State     Config      IRate   Mirror  Port-based VLAN
                     Link      Actual      ERate   MDI
-------------------------------------------------------------------------------
 1:Room301           Enabled   10MHalf     -       -       default(1)
                     Down      -           -       MDI
 2:Room302           Enabled   10MFull     -       -       default(1)
                     Down      -           -       MDI
 3:Room303           Enabled   100MHalf    -       -       default(1)
                     Down      -           -       MDI
 4:Room304           Enabled   100MFull    -       -       default(1)
                     Down      -           -       MDI
 5:Port5             Enabled   100MFull    -       -       default(1)
                     Down      -           -       MDI
 6:Management        Enabled   Autonego    -       -       default(1)
                     Down      -           -       Auto
 7:                  Enabled   Autonego    -       -       default(1)
                     Down      -           -       Auto
 8:                  Enabled   Autonego    -       -       default(1)
                     Down      -           -       Auto
 9:                  Enabled   Autonego    -       -       default(1)
                     Down      -           -       Auto
10:                  Enabled   Autonego    -       -       default(1)
                     Down      -           -       Auto
-------------------------------------------------------------------------------
```

```
Manager > show switch port=1-10 security

 Port                Learn  Relearn  Learned  Locked  IntrusionAction
-------------------------------------------------------------------------------
 1:                  10     On       0        Off     Disable
 2:                  0      Off      0        On      TrapContinue, LogContinue
 3:                  -      On       -        -       Trap, Log
 4:                  20     Off      0        Off     TrapContinue, Log
 5:                  30     On       0        Off     Trap, LogContinue
 6:                  -      Off      -        -       Discard
 7:                  -      Off      -        -       Discard
 8:                  -      Off      -        -       Discard
 9:                  -      Off      -        -       Discard
10:                  -      Off      -        -       Discard
-------------------------------------------------------------------------------
```

Port	ポート番号。
Description	ポート名称（メモ）
Status	ポートのステータス。ENABLED か DISABLED。MAC アドレススラッシング検出時の動作によりディセーブルとなっている場合、DISABLED (by address thrashing) と表示される。ループ検出時の動作によりディセーブルとなっている場合、DISABLED (by loop detection) と表示される。
Link state	ポートのリンクステータス。Up か Down
UpTime	ポートがリセット（初期化）されてから現在までの経過時間（hh:mm:ss の形式）
Port Media Type	MIB-II オブジェクト ifType で定義される物理層インターフェースタイプ
Configured speed/duplex	通信モードの設定値。Autonegotiate、10Mbps、100Mbps、1000Mbps/half duplex、Full duplex で表示される
Actual speed/duplex	実際の通信モード
MDI Configuration (Polarity)	MDI/MID-X 自動切り替え機能の状態と、実際の MDI/MDI-X。自動切り替えの状態は、有効なら Automatic、無効なら Manual と表示される。また、実際の MDI/MDI-X は、カッコ内に MDI-X、MDI、-（未決定）のいずれかで表示される。
Configured master/slave mode	1000BASE-T ポートのマスター/スレーブ設定値。その他のポートの場合は、Not applicable と表示される。
Actual master/slave mode	1000BASE-T ポートの実際のマスター/スレーブ。その他のポートの場合は、Not applicable と表示される。
Acceptable Frames Type	受信可能なフレームタイプ。Acceptable All Frames か Admit Only Vlan-tagged Frames
Broadcast rate limit	ブロードキャストパケットの 1 秒当たり最大受信数。

Multicast rate limit	マルチキャストパケットの１秒当たり最大受信数。
DLF rate limit	DLF（Destination Lookup Failure）パケットの１秒当たり最大受信数。
Ingress rate limit	受信レート上限値（帯域制限機能）
Egress rate limit	送信レート上限値（帯域制限機能）
Learn limit	MAC アドレス登録数の上限。設定した数まで MAC アドレスを学習すると、それ以上の MAC アドレスの登録を行わない。未設定の場合は-で表示される。
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。Disable、Discard、Trap、Log、TrapContinue、LogContinue のいずれか。
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。
Address learn thrash status	MAC アドレススラッシング検出機能の状態。Not Detected（スラッシング未検出）、Thrashing（スラッシング検出中）、Disabled（検出機能が無効。THRASHACTION=NONE に設定されていることを示す）、Trunk（該当ポートがトランクグループに所属しているため、検出機能の状態がトランクグループ側で管理されていることを示す）のいずれか。
Address learn thrash action	MAC アドレススラッシング検出時の動作。None（何もしない）、Learn Disable（MAC アドレスの学習を停止する）、Port Disable（ポートをディセーブルにする）、VLAN Disable（スラッシングが発生した VLAN に対してのみポートをディセーブルにする）、Link Down（ポートを物理的にリンクダウンさせる）のいずれか。
Address learn thrash timeout	MAC アドレススラッシング検出時の動作の持続時間（秒）。動作の実行中は、カッコ内に残り秒数が表示される。None は無期限であることを示す。
Relearn	Learn limit を設置した場合に、学習した MAC アドレスがエージング対象（ON）か対象でないか（OFF）。
Mirroring	ミラーリング対象パケットの向き。Rx、TX、Both、None（未設定）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。
VLAN(s)	所属 VLAN の名前と VLAN ID
Enabled flow control(s)	有効なフロー制御方式。Pause（IEEE 802.3x PAUSE）のみサポート。

Send tagged pkts for VLAN(s)	ポートが所属するタグ VLAN 名（VID）
Port-based VLAN	ポートが所属するポートベース VLAN 名（VID）
Ingress Filtering	イングレスフィルタリングのオン・オフ
Trunk Group	ポートが所属するトランクグループ名
STP	ポートが所属する STP ドメイン名
IGMP Filter	ポートに適用されている IGMP フィルターの番号。適用されていない場合は None と表示される。未サポート。
Max-groups/Joined	ポート配下から Join 可能なマルチキャストグループの最大数と実際に Join されているグループ数。最大数が設定されていないときは Undefined と表示される。未サポート。
IGMP Max-groups Action	ポート配下から Join されたマルチキャストグループの数が最大数に達した場合の動作。未サポート。
Multicast filtering mode	VLAN 内における IP マルチキャストパケットのフィルタリング方式。「(A) forward all groups」、「(B) forward all unregistered groups」、「(C) filter all unregistered groups」のいずれか。
Broadcast egress filtering	ブロードキャストパケットの送出を抑止するかどうか。
Loop detection status	ループ検出の状態。Not Detected（ループ未検出）、Blocking（ループ検出およびアクションの実行中）、Detected（ループ検出のみ）、Disabled（検出機能が無効）、Trunk（該当ポートがトランクグループに所属しているため、検出機能の状態がトランクグループ側で管理されていることを示す）のいずれか。
Loop detection action	ループ検出時の動作。Port Disable（ポートをディセーブルにする）、VLAN Disable（ループが発生した VLAN に対してのみポートをディセーブルにする）、Link Down（ポートを物理的にリンクダウンさせる）、Log Only（ログの記録のみ。Loop detection status は Detected 表示）のいずれか。
Loop detection timeout	ループ検出時の動作の持続時間（秒）。動作の実行中は、カッコ内に残り秒数が表示される。None は無期限であることを示す。

表 35:

Port	ポート番号とポート名称。ポート名称は最大 16 文字まで表示。
State	ポートのステータス。Enabled か Disabled
Link	ポートのリンクステータス。Up か Down
Config	通信モードの設定値。Autonego、10MHalf、10MFull、10MHAuto、10MFAuto、100MHalf、100MFull、100MHAuto、100MFAuto で表示される
Actual	実際の通信モード。
IRate	受信レート上限値（帯域制限機能）
ERate	送信レート上限値（帯域制限機能）
Mirror	ミラーリング設定。Mirror、Rx、Tx、Both のいずれか。
MDI	MDI/MDI-X 状態。Auto、MDI、MDI-X のいずれか。リンクダウン時はConfig、リンクアップ時は Actual を表示。AT-A51(SX)、A53(LX) モジュールポートは「-」を表示。
Port-based VLAN	ポートが所属するポートベース VLAN 名と VLAN ID。VLAN 名は最大 15 文字まで表示。

表 36: SUMMARY オプション指定時

Port	ポート番号とポート名称。ポート名称は最大 16 文字まで表示。
Learn	学習可能な MAC アドレス最大数（0～256）
Relearn	学習可能な MAC アドレス最大数を設定した場合に、学習した MAC アドレスがエージング対象（On）か対象でないか（Off）。
Learned	学習可能な MAC アドレス最大数（0～256）。セキュリティーオフ時は「-」。
Locked	ポートロック状態。Off、On、-のいずれか。ACTIVATE SWITCH PORT LOCK コマンドによるロック時は「#」が付与される。セキュリティーオフ時は「-」。
IntrusionAction	学習可能な MAC アドレス最大数まで 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。Disable、Discard、Trap、Log、TrapContinue、LogContinue のいずれか。

表 37: SECURITY オプション指定時

関連コマンド

SET SWITCH PORT（138 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**[={DETAIL|SUMMARY}]

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。複数指定が可能。省略時および ALL 指定時は、全ポートの情報が表示される。

COUNTER　カウンター情報を表示する。DETAIL 指定時は詳細なカウンター情報を表示。SUMMARY 指定時は一覧形式で表示する。省略時は DETAIL 指定時と同じ

入力・出力・画面例

```
anager> show switch port=1 counter

 Switch Port Counters
------------------------------------------------------------------------------

Port 1. Fast Ethernet MAC counters:
 Combined receive/transmit packets by size (octets) counters:
  64                                63 512 - 1023                          0
  65 - 127                           7 1024 - MaxPktSz                     0
  128 - 255                          3 1519 - 1522                         0
  256 - 511                          1

 General Counters:
 Receive                            Transmit
  Octets                          5510 Octets                              0
  Pkts                              74 Pkts                                0
  FCSErrors                          0 FCSErrors                           0
  MulticastPkts                      7 MulticastPkts                       0
  BroadcastPkts                     26 BroadcastPkts                       0
  PauseMACCtlFrms                    0 PauseMACCtrlFrm                     0
  OversizePkts                       0 OversizePkts                        0
  Fragments                          0 Fragments                           0
  Jabbers                            0 Jabbers                             0
  MACControlFrms                     0
  UnsupportOpcode                    0
  AlignmentErrors                    0
```

```
  OutOfRngeLenFld                   0
  SymErDurCarrier                   0
  CarrierSenseErr                   0
  UndersizePkts                     0
                                      PauseCtrlFrms                   0
                                      FrameWDeferrdTx                 0
                                      FrmWExcesDefer                  0
                                      SingleCollsnFrm                 0
                                      MultCollsnFrm                   0
                                      LateCollsns                     0
                                      ExcessivCollsns                 0
                                      CollisionFrames                 0

 Layer 3 Counters:
  ifInUcastPkts                   - ifOutUcastPkts                  -
  ifInDiscards                    - ifOutErrors                     -
  ipInHdrErrors                   -

 Miscellaneous Counters:
  DropEvents                        0
  ifOutDiscards                     0
  taggedPktTx                       0
  totalPktTxAbort                   0

 HW Multicasting Counters:
  TTL expired                     -
  Bridged Frames                  -
  Routed Frames                   -
  Receive Drops                   -
  Transmit Drops                  -
--------------------------------------------------------------------------------

Manager > show switch port=1-10 counter=summary

 Port                     InPkts      InUcastPkts    InNUcastPkts         InErrors
                         OutPkts     OutUcastPkts   OutNUcastPkts        OutErrors
--------------------------------------------------------------------------------
 1:Room301                     0                0               0                0
                               0                0               0                0
 2:Room302                     0                0               0                0
                               0                0               0                0
 3:Room303                     0                0               0                0
                               0                0               0                0
 4:Room304                     0                0               0                0
                               0                0               0                0
 5:Port5                       0                0               0                0
                               0                0               0                0
 6:Management                  0                0               0                0
                               0                0               0                0
 7:                            0                0               0                0
                               0                0               0                0
```

```
 8:                    0                    0                    0                    0
                       0                    0                    0                    0
 9:                    0                    0                    0                    0
                       0                    0                    0                    0
10:                    0                    0                    0                    0
                       0                    0                    0                    0
--------------------------------------------------------------------------------
```

Combined receive/transmit packets by size (octets) counters	フレームサイズ別送受信数分布
64	64 オクテット長のフレーム送受信数
65 - 127	65～127 オクテット長のフレーム送受信数
128 - 255	128～255 オクテット長のフレーム送受信数
256 - 511	256～511 オクテット長のフレーム送受信数
512 - 1023	512～1023 オクテット長のフレーム送受信数
1024 - MaxPktSz	1024 オクテット～最大サイズのフレーム送受信数
1519 - 1522	1519～1522 オクテット長のフレーム送受信数
General Counters	一般的な送受信カウンター
Receive	受信トラフィックカウンターが表示される。
Octets	受信オクテット数
Pkts	受信パケット数
FCSErrors	FCS エラーフレーム受信数
MulticastPkts	マルチキャストフレーム受信数
BroadcastPkts	ブロードキャストフレーム受信数
PauseMACCtlFrms	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。
MACControlFrms	MAC 制御フレーム受信数（PAUSE フレームと未サポートのフレームの合計）
UnsupportOpcode	未サポートの MAC 制御フレーム受信数（PAUSE フレーム以外の制御フレーム）
AlignmentErrors	アライメントエラーフレーム受信数。フレーム長がオクテットの整数倍でないフレームの数
OutOfRngeLenFld	長さフィールドの値が範囲外のフレーム受信数
SymErDurCarrier	不正なデータシンボルを持つフレームの受信数

CarrierSenseErr	フレーム間の搬送波にエラーがあった回数
UndersizePkts	アンダーサイズフレーム数。正しい形式であるが、長さが 64 オクテットより短いフレームの総数
Transmit	送信トラフィックカウンターが表示される。
Octets	送信オクテット数
Pkts	送信パケット数
FCSErrors	送信対象フレームのうち FCS エラーがあったものの数
MulticastPkts	マルチキャストフレーム送信数
BroadcastPkts	ブロードキャストフレーム送信数
PauseMACCtlFrms	有効な PAUSE フレーム送信数
OversizePkts	オーバーサイズフレーム送信数。正しい形式であるが、長さが 1518 オクテットより長いパケットの総数
Fragments	フラグメントフレーム送信数。不正な FCS を持ち、なおかつ、長さが 64 オクテットより短いフレームの総数。アライメントエラーを含む。
Jabbers	ジャバーフレーム送信数。1518 オクテットより長いフレームのうち、不正な FCS を持つものの総数。アライメントエラーパケットも含む。
PauseCtrlFrms	PAUSE フレーム数
FrameWDeferrdTx	最初の送信が延期されたあとに送信されたフレーム数
FrmWExcesDefer	遅延過多により送信が中止されたフレーム数
SingleCollsnFrm	1 回だけコリジョンを発生したフレームの数
MultCollsnFrm	2〜15 回コリジョンを発生したフレームの数（レイトコリジョンを含む）
LateCollsns	レイトコリジョンを発生したフレームの数
ExcessivCollsns	16 回コリジョンを発生したため送信が中止されたフレームの数
CollisionFrames	コリジョンフレーム総数
Miscellaneous Counters	その他のカウンター
DropEvents	受信ポートでとりこぼされたパケットの数
ifOutDiscards	エージングのため送信前に破棄されたパケットの数。未サポート
taggedPktTx	VLAN タグ付きパケット送信数
totalPktTxAbort	送信されずに破棄されたレイヤー 2/3 パケット数

表 38:

Port	ポート番号とポート名称。最大 16 文字まで表示
InPkts	受信パケット数
InUcastPkts	受信ユニキャストパケット数
InNUcastPkts	受信ブロードキャストパケット数
InErrors	受信後に破棄したエラーパケット数（FCSErrors、OversizePkts、Fragments、Jabbers、AlignmentErrors、OutOfRngeLenFld、SymErDurCarrier、UndersizePkts のエラーカウンターの合計値を表示する。）

OutPkts	送信パケット数
OutUcastPkts	送信ユニキャストパケット数
OutNUcastPkts	送信ブロードキャストパケット数
OutErrors	送信前に破棄したエラーパケット数（FCSErrors、OversizePkts、Fragments、Jabbers、FrmWExcesDefer、ExcessivCollsns のエラーカウンターの合計値を表示する。Giga Port の Fragments、FrmWExcesDefer、ExcessivCollsns のエラーカウンターは含まない。）

表 39: SUMMARY オプション指定時

備考・注意事項

COUNTER のオプションに DETAIL を指定した場合は 64bit カウンターを使用 (0～18446744073709551615 で表示)、SUMMARY を指定した場合は 32bit カウンターを使用 (0～4294967295 で表示)

関連コマンド

SET SWITCH PORT（138 ページ）
SHOW SWITCH COUNTER（189 ページ）
SHOW SWITCH PORT（194 ページ）

SHOW SWITCH PORT INTRUSION

カテゴリー：スイッチング / ポート

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

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能)

解説

ポートセキュリティー機能がオンのポート（LEARN パラメーターが NONE 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。複数指定が可能。

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（138 ページ）

SHOW SWITCH TRUNK

カテゴリー：スイッチング / ポート

SHOW SWITCH TRUNK[=*trunk*]

trunk: トランクグループ名（1〜15 文字。英数字とアンダースコア（_）、ハイフンを使用可能。大文字小文字を区別しない）

解説

トランクグループの情報を表示する。

パラメーター

TRUNK　トランクグループ名。省略時はすべてのトランクグループの情報が表示される。

入力・出力・画面例

```
Manager > show switch trunk

 Switch Trunk Groups
--------------------------------------------------------------------------------
 Trunk group name ..................... uplink
   Speed ............................... 100 Mbps
   Select .............................. source and destination mac address
   Ports ............................... 1-4
   Address learn thrash status ......... Not Detected
   Address learn thrash action ......... Learn Disable
   Address learn thrash timeout ........ 1 second
   Ports disabled by learn thrashing ... Not Applicable
   Loop detection status ............... Not Detected
   Loop detection action ............... Port Disable
   Loop detection block timeout ........ 5 second
   Ports disabled by loop detection .... Not Applicable
--------------------------------------------------------------------------------
```

Trunk group name	トランクグループ名
Speed	トランクポートの通信速度。10Mbps、100Mbps、1000Mbps、-（未設定）のいずれか。
Selection criterion	送出ポートの選択基準
Ports	所属ポート
Address learn thrash status	MAC アドレススラッシング検出機能の状態。Not Detected（スラッシング未検出）、Thrashing（スラッシング検出中）、Disabled（検出機能が無効。THRASHACTION=NONE に設定されていることを示す）のいずれか
Address learn thrash action	MAC アドレススラッシング検出時の動作。None（何もしない）、Learn Disable（トランクグループ内の全ポートで MAC アドレスの学習を停止する）、Port Disable（トランクグループ内の全ポートをディセーブルにする）、VLAN Disable（スラッシングが発生した VLAN に対してのみトランクグループ内の全ポートをディセーブルにする）、Link Down（トランクグループ内の全ポートを物理的にリンクダウンさせる）のいずれか
Address learn thrash timeout	MAC アドレススラッシング検出時の動作の持続時間（秒）。動作の実行中は、カッコ内に残り秒数が表示される。None は無期限であることを示す
Ports disabled by learn thrashing	MAC アドレススラッシング検出によりディセーブルにされたポート。Address learn thrash action が Port Disable か Link Down のときだけ有効。Address learn thrash action が前記以外に設定されている場合、および、検出機能が無効に設定されている場合は、Not Applicable と表示される
Loop detection status	ループ検出の状態。Not Detected（ループ未検出）、Blocking（ループ検出およびアクション実行中）、Detected（ループ検出のみ）、Disabled（検出機能が無効）のいずれか
Loop detection action	ループ検出時の動作。Port Disable（トランクグループ内の全ポートをディセーブルにする）、VLAN Disable（ループが発生した VLAN に対してのみトランクグループ内の全ポートをディセーブルにする）、Link Down（トランクグループ内の全ポートを物理的にリンクダウンさせる）、Log Only（ログの記録のみ。Loop detection status は Detected 表示）、None（何もしない）のいずれか

Loop detection block timeout	ループ検出時の動作の持続時間（秒）。動作の実行中は、カッコ内に残り秒数が表示される。None は無期限であることを示す
Ports disabled by loop detection	ループ検出によりディセーブルにされたポート。Loop detection action が Port Disable または Link Down のときのみ有効。Loop detection action がそれ以外に設定されている場合、および、検出機能が無効に設定されている場合は、Not Applicable と表示される

表 40:

関連コマンド

ADD SWITCH TRUNK（61 ページ）
CREATE SWITCH TRUNK（64 ページ）
DELETE SWITCH TRUNK（69 ページ）
DESTROY SWITCH TRUNK（71 ページ）
SET SWITCH TRUNK（143 ページ）