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場合、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 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。詳細は各コマンドの説明をご覧ください。

■ ポートを有効にするには、ENABLE SWITCH PORT コマンド（92 ページ）を使います。

```
ENABLE SWITCH PORT=8 ↵
```

■ ポートを無効にするには、DISABLE SWITCH PORT コマンド（73 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（120 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 ↵
```

■ デフォルトでは、すべてのポートで MDI/MDI-X 自動認識が有効になっています。MDI/MDI-X 自動認識を無効にするには、DISABLE SWITCH PORT AUTOMDI コマンド（75 ページ）を実行します。

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

✎ SFP ポートでは、MDI/MDI-X 自動認識有効/無効コマンド（DISABLE SWITCH PORT AUTOMDI コマンド（75 ページ）および ENABLE SWITCH PORT AUTOMDI コマンド（93 ページ））は使用できません。

■ MDI/MDI-X 自動認識を無効にした直後のポートは、現在設定されている MDI/MDI-X の状態にしたがいます（デフォルトは、MDI-X）。MDI/MDI-X を変更するには、SET SWITCH PORT コマンド（120 ページ）の POLARITY パラメーターを使います。

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

✎ SFP ポートでは、MDI/MDI-X の設定を変更することはできません。

■ 強制的にオートネゴシエーションを行わせるには、ACTIVATE SWITCH PORT AUTONEGOTIATE コマンド（43 ページ）を使います。通信モードが AUTONEGOTIATE のポートでのみ有効です。

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

■ ポートをハードウェア的にリセットするには、RESET SWITCH PORT コマンド（105 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（153 ページ）を使います。

```
SHOW SWITCH PORT ↵
```

■ ポートの送受信の統計情報を確認するには、SHOW SWITCH PORT COUNTER コマンド（159 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（105 ページ）に COUNTER オプションを指定して実行します。COUNTER オプションを省略すると、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ます）。

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

ポートトランキング

ポートトランキングは複数の物理ポートを束ねてスイッチ間の帯域幅を拡大する機能です。束ねたポートはトランクグループと呼ばれ、論理的に 1 本のポートとして扱われます。トランクグループは、VLAN 内でも単一ポートとして認識されます。また、トランクグループ内のポートに障害が発生しても残りのポートで通

信が継続できるため、信頼性を向上します。
トランクグループは 16 グループまで作成可能です。それぞれのトランクグループには、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。
ここでは、コマンドラインインターフェースによる設定方法を中心に説明します。なお、Web GUI では「スイッチ設定」-「トランキング」で設定できます。（詳細は「Web GUI」/「スイッチ設定」をご覧ください。）
ポートトランキングの仕様は、次のとおりです。

- 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指定できません。
- トランクポートは同じ VLAN に所属している必要があります。
- ポートセキュリティーが有効なポート、ミラーポート、ポート認証の Authenticator ポートと Supplicant ポートはトランクグループに所属させることができません。
- SFP ポートと SFP ポート以外のポートを、同一のトランクグループに所属させることはできません。
- STP 有効ポートと STP 無効ポートは、同じトランクグループには所属できません。
- LDF 検出が有効なポートと無効なポートは同じトランクグループに所属させることができません。
- 受信レート検出が有効なポートと無効なポートは同じトランクグループに所属させることができません。
- トランクポートに接続される対向機器の通信速度を固定に設定すると通信できません。
- トランクポートを MLD Snooping のルーターポートに設定する場合は、トランクグループのすべてのポートをルーターポートに設定してください。
- ポートトランキングと IGMP Snooping または MLD Snooping の併用時、トランクグループ内で最も番号の小さいポートを DISABLE SWITCH PORT コマンド（73 ページ）で無効に設定すると、トランクグループ内のそれ以外のポートでマルチキャストデータが転送されなくなります。DISABLE SWITCH PORT コマンド（73 ページ）実行時に LINK パラメーターに DISABLE を指定して、該当ポートを物理的にリンクダウンさせると、本現象は発生しません。
- 100M SFP ポートは、トランクグループに所属させることができません。

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。グループ名は任意に指定できます。

   ```
   CREATE SWITCH TRUNK=uplink SPEED=1000M ↵
   ```

2. トランクグループにポートを追加します。束ねるポートはあらかじめ同じ VLAN に所属させておく必要があります。

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

基本設定は以上です。

✎ 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双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、スパニングツリープロトコル、ループガード、これらすべての機能を同時に使用することはできません。

■ トランクグループの情報は SHOW SWITCH TRUNK コマンド（169 ページ）で確認できます。

```
SHOW SWITCH TRUNK=uplink ↵
```

■ トランクグループを通るパケットはすべて、トランキングアルゴリズムによって割り振られます。このアルゴリズムは、送信元/宛先 IP アドレス、TCP/UDP ポート番号（送信元、宛先）と接続ポート数によって計算します。

■ トランクグループに追加されたポートの通信モードは、CREATE SWITCH TRUNK コマンド（54 ページ）、または、SET SWITCH TRUNK コマンド（126 ページ）指定した速度となります。個別ポートの設定はトランクグループに追加した時点で上書きされます。

■ トランクグループからポートを削除するには DELETE SWITCH TRUNK コマンド（59 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（62 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（59 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できます。ここでは、コマンドラインインターフェースによる設定方法を中心に説明します。なお、Web GUI では「スイッチ設定」-「ミラーリング」で設定できます。（詳細は「Web GUI」/「スイッチ設定」をご覧ください。）なお、本製品でのポートミラーリング機能には以下の特徴があります。

- ミラーポートには 1 ポート指定できます。ソースポートは複数指定できます。
- VLAN default 以外に所属しているポート、トランクグループに所属しているポート、およびタグ付きポートはミラーポートに設定できません。
- STP 有効ポート、ポートセキュリティーが有効なポート、ポート認証の Authenticator ポートと Supplicant ポートはミラーポートに設定できません。
- 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。
- SET SWITCH MIRROR コマンド（118 ページ）でミラーポートの設定を行いますが、すで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ります。ミラーポートになったポートは、どの VLAN にも所属しません。
- PAUSE フレームもミラーリングの対象となります。
- 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。

✎ 本製品のポートミラーリング機能では、ソースポートのタグの有無に関係なく、送信パケットはタグ付きでミラーポートに出力されます。受信パケットはソースポートで受信したタグ付き、またはタグなしのままミラーポートに出力されます。

基本設定

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

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（118 ページ）を実行します。

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

   SET SWITCH MIRROR コマンド（118 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. 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 ↵
   ```

3. ポートミラーリング機能を有効にします。あらかじめミラーポートおよびソースポートが設定されていないと本コマンドは失敗します。手順 1、2 にしたがってミラーポートとソースポートを指定してから本コマンドを実行してください。

   ```
   ENABLE SWITCH MIRROR ↵
   ```

   ✎ 複数のポートをミラーしたいときは、SET SWITCH PORT コマンド（120 ページ）を複数回実行してください。ただし、ミラーリング対象ポートを 4 ポート以上に増やすことは、ミラーリング機能のパフォーマンス低下につながりますので、ご注意ください。

設定は以上です。

■ ポートミラーリングの設定を確認するには SHOW SWITCH コマンド（144 ページ）および SHOW

SWITCH MIRROR コマンド（152 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 20 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（153 ページ）の「Mirroring」および「Is this port mirror port」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（72 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（118 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 ↵
```

■ ソースポートのミラーリングを行わないようにするには SET SWITCH PORT コマンド（120 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（118 ページ）を実行した時点で、ミラーポートはいずれの VLAN にも所属していない状態となります。

ポートセキュリティー

ポートセキュリティーは、MAC アドレスに基づき、ポートごとに通信を許可するデバイスを制限する機能です。許可していないデバイスからフレームを受信したときには、パケットを破棄する、SNMP トラップを送信するなどのアクションを実行させることができます。
ここでは、コマンドラインインターフェースによる設定方法を中心に説明します。なお、Web GUI では「セキュリティー設定」-「ポートセキュリティー」で設定できます。（詳細は「Web GUI」/「セキュリティー設定」をご覧ください。）
本機能は、SET SWITCH PORT コマンド（120 ページ）の SECURITYMODE パラメーターでセキュリティーモードを設定することによって有効になります。SET SWITCH PORT コマンド（120 ページ）で設定できるのは、次の 4 種類のモードです。

モード	説明
AUTOMATIC	通常の学習モード（セキュリティーモード無効）。
DYNAMIC	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する。学習された 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る（Dynamic Limited モード）。学習可能な MAC アドレスの最大数は、LEARN パラメーターで設定。

LIMITED	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する。学習された 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ない（Limited モード）。学習可能な MAC アドレスの最大値は、LEARN パラメーターで設定。
SECURED	学習機能を停止し、それまでに学習済みの MAC アドレスをスタティックエントリーとし、セキュリティーモードとなる。（Secure モード）

表 1:

✎ ポートセキュリティーが有効なポートは、トランクグループに所属させることができません。

✎ ポートセキュリティーが有効なポートは、ミラーポート、ポート認証の Authenticator ポートに設定することはできません。

✎ ポートセキュリティーが有効なポートではスパニングツリープロトコルは使用できません。

✎ ポートセキュリティー（Dynamic Limited モード）が有効なポートにはスタティックエントリーは登録できません。

■ Limited モード使用の注意

- ポートをリンクダウンしても、そのポートの FDB はクリアされません。
- MAC アドレスの学習を開始した後にポートの移動を行う場合は、移動元のポートの設定を一度ポートセキュリティー無効（SECURITYMODE=AUTOMATIC）に変更して学習状態 (FDB) をクリアする必要があります。クリアしない場合、他ポートに移動しても移動前のポートのアドレス学習状態が解除されません。
- ループガードを併用している場合、ループを検出しても併用ポートの FDB をクリアしません。
- ポートセキュリティーを Limited モードに設定したポートでは、本体宛通信の受信レートがチェックされるため、FDB 学習に時間がかかります。

また、ポートセキュリティーが Dynamic Limited/Limited モードの場合、学習済みの MAC アドレスが制限値に達した後で受信した、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（120 ページ）の INTRUSION パラメーターで指定）。

DISCARD	不正なフレームを破棄する。
DISABLE	不正なフレームを破棄し、SNMP トラップを送信した後、該当ポートを無効にする。
LOG	不正なフレームを破棄し、ログに記録する。
TRAP	不正なフレームを破棄し、SNMP トラップを送信する。

表 2:

■ ポートに、Secure モードのポートセキュリティーを設定するには、SET SWITCH PORT コマンド（120 ページ）を使います。

```
SET SWITCH PORT=1 SECURITYMODE=SECURED ↵
```

■ ポートに、Dynamic Limited モードのポートセキュリティーを設定するには、SET SWITCH PORT コマンド（120 ページ）の SECURITYMODE パラメーターを使います。たとえば、ポート 2 の MAC アドレス学習数の上限を 20 個に設定するには次のようにします。

```
SET SWITCH PORT=2 SECURITYMODE=DYNAMIC LEARN=20 ↵
```

■ ポートに、Limited モードのポートセキュリティーを設定するには、SET SWITCH PORT コマンド（120 ページ）の SECURITYMODE パラメーターを使います。たとえば、ポート 3 の MAC アドレス学習数の上限を 20 個に設定するには次のようにします。

```
SET SWITCH PORT=3 SECURITYMODE=LIMITED LEARN=20  ↵
```

■ 学習済みのアドレスを確認するには、SHOW SWITCH FDB コマンド（「フォワーディングデータベース」の 14 ページ）を使います。ポートセキュリティーが有効なポートで学習されたアドレスは、「Status」欄に「Static」または「Dynamic」と表示されます。

```
SHOW SWITCH FDB ↵
SHOW SWITCH FDB PORT=3 ↵
```

■ ポートセキュリティーの設定状況は SHOW SWITCH PORT コマンド（153 ページ）、または、SHOW SWITCH PORT コマンド（153 ページ）の SECURITY オプションで確認できます。

```
SHOW SWITCH PORT=3 ↵
SHOW SWITCH PORT=3 SECURITY ↵
```

■ ポートセキュリティーが有効（Secure モード、Limited モード）なポートに対して、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 6 ページ）を使って、スタティック MAC アドレスを登録します。

```
ADD SWITCH FILTER DESTADDRESS=00-00-f4-ab-cd-ef PORT=10 ↵
```

■ 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 8 ページ）で行います。

```
DELETE SWITCH FILTER PORT=1 DESTADDRESS=00-00-f4-ab-cd-ef ↵
```

■ 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（120 ページ）で SECURITYMODE パラメーターに AUTOMATIC を設定します。
Secure モードまたは Limited モード設定して、スタティックエントリーとなった学習済みのアドレスは削除されます。

```
SET SWITCH PORT=11 SECURITYMODE=AUTOMATIC ↵
```

■ ポートセキュリティーの設定（セキュリティーモードに関する設定）は CREATE CONFIG コマンド（「運用・管理」の 61 ページ）によって保存されます。SECURED モードを設定して、スタティックエントリーとなった学習済みのアドレスは保存されます。

パケットストームプロテクション

パケットストームプロテクションは、ブロードキャスト/マルチキャスト/未学習のユニキャスト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。
ここでは、コマンドラインインターフェースによる設定方法を中心に説明します。なお、Web GUI では「スイッチ設定」-「プロテクション」で設定できます。（詳細は「Web GUI」/「スイッチ設定」をご覧ください。）
パケットストームプロテクションで制限できるのは以下のフレームです。

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

■ 受信レートは SET SWITCH LIMITATION コマンド（115 ページ）で設定し、有効/無効の設定は SET SWITCH PORT コマンド（120 ページ）で行います。ここでは、ポート 1〜8 に対して、ブロードキャストフレームの受信レートの設定を有効とし、受信レートを 10240kbps に制限します。

```
SET SWITCH PORT=1-8 BCLIMIT=ON ↵
SET SWITCH LIMITATION=10240 ↵
```

■ 受信レートの制限を解除するには次のようにします。

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

■ 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（153 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
- 受信レート検出

✎ ポートトランキング、スパニングツリープロトコル、ループガード、これらすべての機能を同時に使用することはできません。

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。
他の接続機器を介して機器に LDF が戻って来る場合、LDF の送信元 MAC アドレスと機器自身の MAC アドレスが一致し、かつ LDF 検出機能が有効なスイッチポート番号が LDF に記録された情報と一致すると、ループ状態と判断されます。
すべてのポートで受信した LDF が判断の対象になります。（LDF 検出機能が無効のポートで受信した LDF も対象です。）
ここでは、コマンドラインインターフェースによる設定方法を中心に説明します。なお、Web GUI では「スイッチ設定」-「LDF 検出」で設定できます。（詳細は「Web GUI」/「スイッチ設定」をご覧ください。）
LDF 検出の仕様は、次のとおりです。

- ミラーリングポート、ポートセキュリティーが有効なポートでは、すべてまたは指定以外の受信フレームは破棄されるため、併用できない。
- LDF 検出が有効かつパケットストームプロテクションが有効に設定されたポートが存在する場合、LDF 検出時のアクションに BCDISCARD を指定することはできない。
- SET SWITCH LOOPDETECTION コマンド（116 ページ）の ACTION パラメーターに BCDISCARD が指定されており、かつパケットストームプロテクションを有効にしたポートが存在する場合、エラーメッセージが表示される。
- トランクポートに対して LDF 検出機能を有効にする場合、トランクグループの全ポートを指定する必要がある。
- フローコントロールとは併用できない。

カスケード接続したノンインテリジェントスイッチなどの対向機器でループ接続された環境では、以下の場合に LDF の検出ができない可能性があります。

- 対向機器のループ接続ポート間でフローコントロールが動作するなどして、本製品が送信した LDF を対向機器にて破棄される、または転送されない場合。
- 対向機器のループ接続ポート間で本製品が以前送出した LDF がループすることにより、本製品が受信する LDF に含まれる ID が異なるため破棄される場合。この場合には、SET SWITCH LOOPDETECTION コマンド（116 ページ）で SECURE パラメーターを設定し、セキュアな LDF の受信を OFF に設定変更することで回避可能となる。

```
SET SWITCH LOOPDETECTION PORT=2 ACTION=LINKDOWN SECURE=OFF ↵
```

ループ状態と判断された場合、LDF を送信したポートに対し、以下のアクションのうちいずれかを行います。

- ポートを無効にする（物理的なリンクは保持する）。
- ポートをリンクダウンする。
- ポートのブロードキャストフレームの受信を止める。
- 何もしない（ログのみ）。

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、または下記の条件でアクション実行前の状態に戻ります。

- ENABLE SWITCH PORT コマンド（92 ページ）が設定されたとき
- DISABLE SWITCH PORT コマンド（73 ページ）が設定されたとき
- リンクダウンが発生したとき（ACTION=LINKDOWN は除く）
- PORTOFF モードのエコトリガーが起動されたとき
- PORTOFF モードのエコトリガーが終了したとき
- ポートセキュリティーの DISABLE アクションが実行されたとき
- ポートセキュリティーの DISABLE アクションが解除されたとき

■ 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（89 ページ）を使用します。LDF 検出機能はフローコントロールとは併用できませんが、フローコントロールはデフォルト有効のため、先に DISABLE SWITCH PORT FLOW コマンド（77 ページ）でポート 2 のフローコントロールを無効にします。

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

■ ポート 2 の LDF 送出間隔を 1 秒、LDF 検出時のアクションを BCDISCARD（ブロードキャストパケットを破棄する）、アクションからの復帰時間を 1 時間に設定するには SET SWITCH LOOPDETECTION コマンド（116 ページ）を使用します。

```
SET SWITCH LOOPDETECTION PORT=2 INTERVAL=1 ACTION=BCDISCARD
  BLOCKTIMEOUT=3600 ↵
```

■ ポート 2 の LDF 検出機能の設定情報を表示するには SHOW SWITCH LOOPDETECTION コマンド（147 ページ）を使用します。

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

■ ポート 2 の LDF 検出機能の状態を表示するには SHOW SWITCH LOOPDETECTION コマンド（147 ページ）を使用します。

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

■ 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（147 ページ）を使用します。

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

受信レート検出

受信レート検出機能を有効にしたポートでは、一定時間ごとに受信レートを算出し、指定されたしきい値と比較して、しきい値を超えた場合にループ状態と判断されます。

受信レートは 1 ポートにつき、2 レベル（LOWRATE、HIGHRATE）設定できます。各レベルに対して、受信レートしきい値とアクションを設定できます。
ここでは、コマンドラインインターフェースによる設定方法を中心に説明します。なお、Web GUI では「スイッチ設定」-「受信レート検出」で設定できます。（詳細は「Web GUI」/「スイッチ設定」をご覧ください。）
受信レート検出の仕様は次のとおりです。

- 受信レート検出が有効かつパケットストームプロテクションを有効に設定されたポートが存在する場合、高レート時/低レート時のアクションに BCDISCARD を指定することはできない。
- パケットストームプロテクションと受信レート検出を併用する場合、受信レートカウンターには、パケットストームプロテクションによって破棄されたパケットも計上される。
- SET SWITCH STORMDETECTION コマンド（124 ページ）の HIGHRATEACTION パラメーターまたは LOWRATEACTION パラメーターに BCDISCARD が指定されており、かつパケットストームプロテクションを有効にしたポートが存在する場合、エラーメッセージが表示される。
- トランクポートに対して受信レート検出機能を有効にする場合、トランクグループの全ポートを指定する必要がある。
- エラーパケットを受信した場合も受信レートカウンターに計上される。

受信レートがしきい値を越えたポートに対し、以下のアクションのうちいずれかを行います。

- ポートを無効にする（物理的なリンクは保持する）。
- ポートをリンクダウンする。
- ポートのブロードキャストフレームのみ、受信を止める。
- 何もしない（ログのみ）。

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、または下記の条件でアクション実行前の状態に戻ります。

- ENABLE SWITCH PORT コマンド（92 ページ）が設定されたとき
- DISABLE SWITCH PORT コマンド（73 ページ）が設定されたとき
- リンクダウンが発生したとき（ACTION=LINKDOWN は除く）
- PORTOFF モードのエコトリガーが起動されたとき
- PORTOFF モードのエコトリガーが終了したとき
- ポートセキュリティーの DISABLE アクションが実行されたとき
- ポートセキュリティーの DISABLE アクションが解除されたとき

■ ポート 2 の受信レート検出機能を有効にするには ENABLE SWITCH STORMDETECTION コマンド（96 ページ）を使用します。

```
ENABLE SWITCH STORMDETECTION PORT=2 ↵
```

■ ポート 2 の高レートのしきい値を 1024000Kbps、アクションを BCDISCARD（ブロードキャストパケットを破棄する）に設定するには SET SWITCH STORMDETECTION コマンド（124 ページ）を使用します。

```
SET SWITCH STORMDETECTION PORT=2 HIGHRATETHRESHOLD=1024000
  HIGHRATEACTION=BCDISCARD ↵
```

■ ポート 2 の受信レート検出機能の設定情報を表示するには SHOW SWITCH STORMDETECTION コマンド（163 ページ）を使用します。

```
SHOW SWITCH STORMDETECTION PORT=2 CONFIG ↵
```

■ ポート 2 の受信レート検出機能の状態を表示するには SHOW SWITCH STORMDETECTION コマンド（163 ページ）を使用します。

```
SHOW SWITCH STORMDETECTION PORT=2 STATUS ↵
```

■ ポート 2 の受信レート検出機能のカウンターの情報を表示するには SHOW SWITCH STORMDETECTION コマンド（163 ページ）を使用します。

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

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。
以下の設定は、Web GUI では「スイッチ設定」-「ポート」で設定できます。（詳細は「Web GUI」/「スイッチ設定」をご覧ください。）

■ 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（95 ページ）を使います。

```
ENABLE SWITCH POWERSAVE ↵
```

■ 本製品の省電力モードを無効にするには、DISABLE SWITCH POWERSAVE コマンド（78 ページ）を使います。

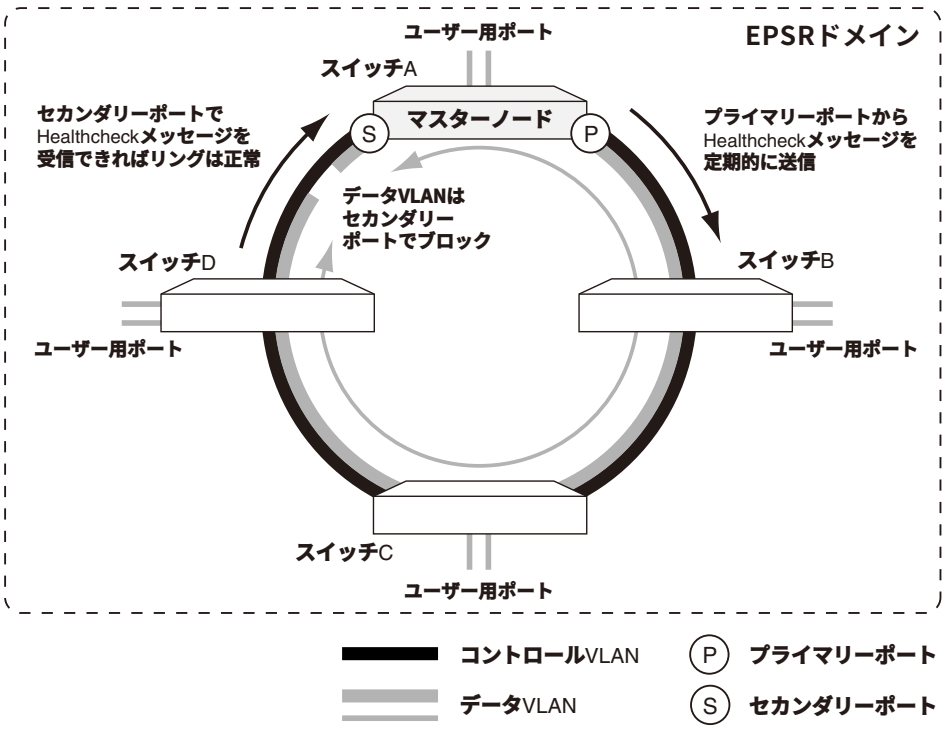
```
DISABLE SWITCH POWERSAVE ↵
```

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、コマンドラインインターフェースによる設定を中心に説明します。なお、Web GUI では「スイッチ設定」-「EPSR」で設定できます。（詳細は「Web GUI」/「スイッチ設定」をご覧ください。）

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。



✎ ポート認証の Authenticator ポートと Supplicant ポートを、EPSR のリングを構成するポートにすることはできません。

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ます。本製品は、このうちトランジットノードの「アウェア機能」に対応しています。また、コマンドにより「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」と「トラップ送信機能」を有効にし、トランジットノードの「フル実装」と同等の動作をすることもできます。
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（本製品の実装）	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 3: トランジットノードの機能

※　CREATE EPSR コマンド（52 ページ）の MODE パラメーターで TRANSIT を指定すると、「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」と「トラップ送信機能」を有効にすることができます。

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

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 4: EPSR 制御メッセージ

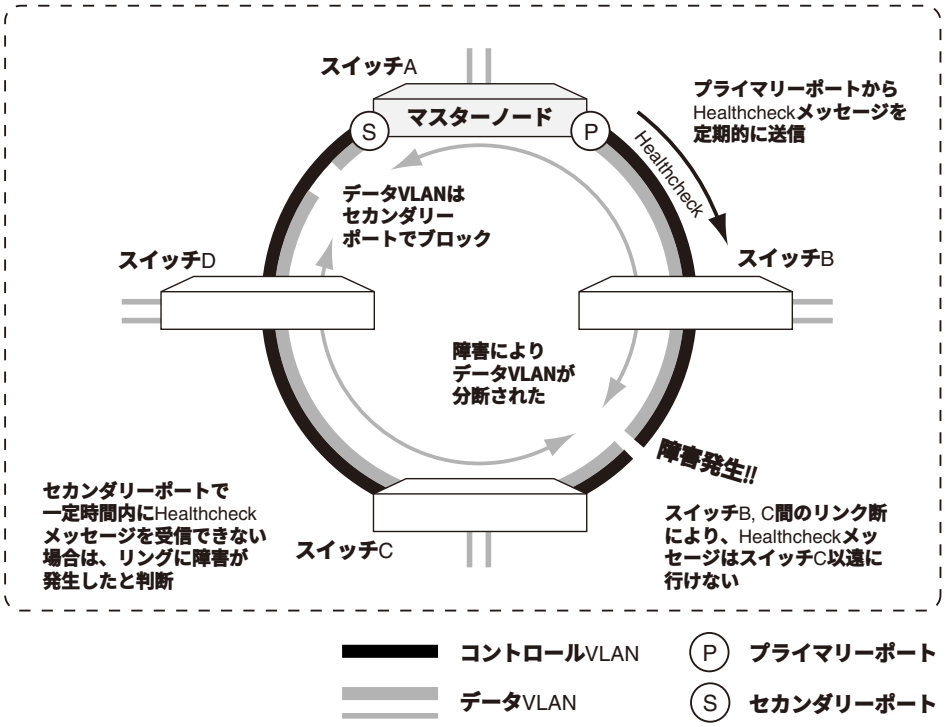
障害検出機能

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）

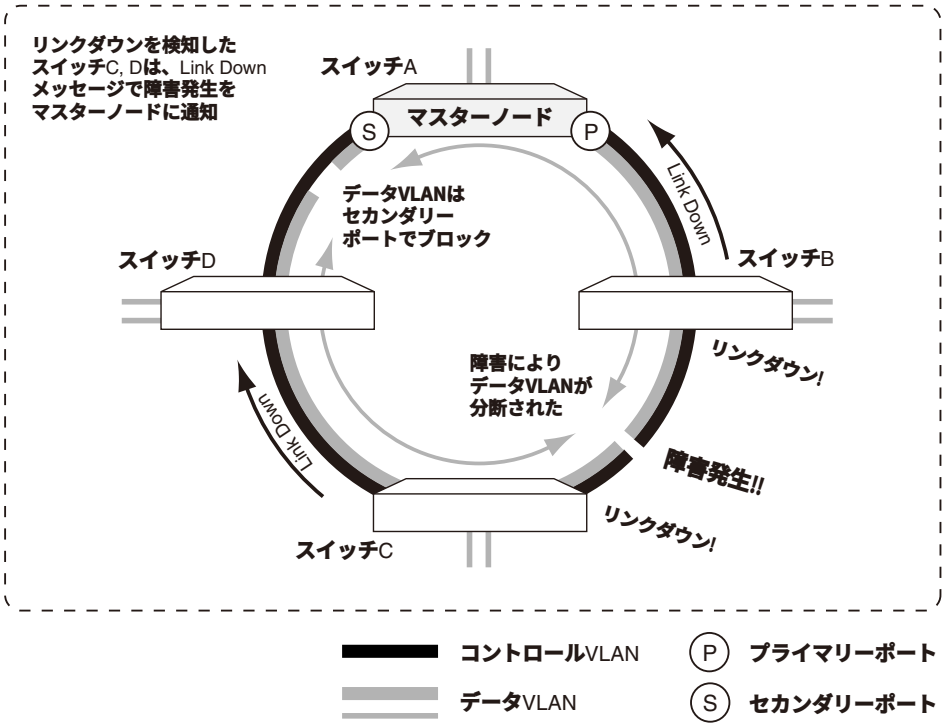
Healthcheck メッセージ

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。



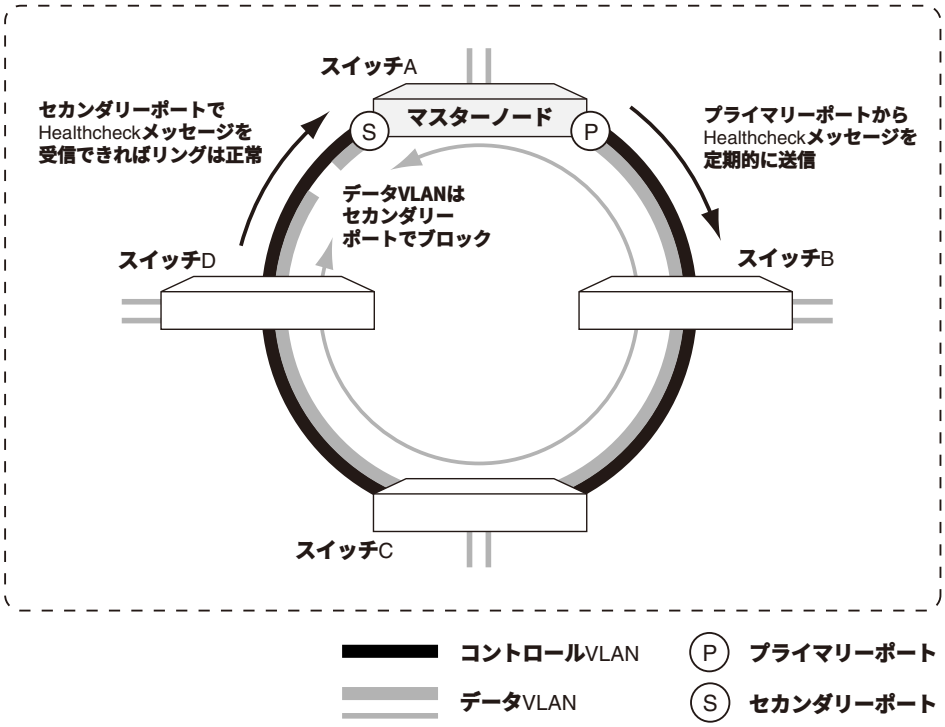
✎ トランジットノードがスヌーピング機能にのみ対応している場合は、Link Down メッセージの送出は行いません。

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」状態にあるとみなし、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。

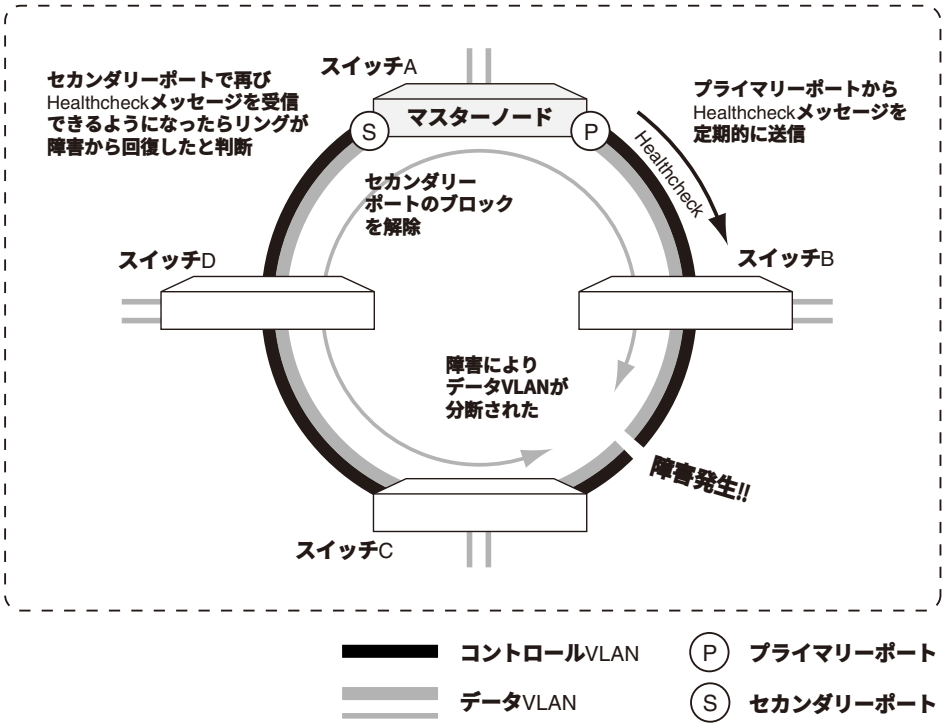


障害発生時

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。

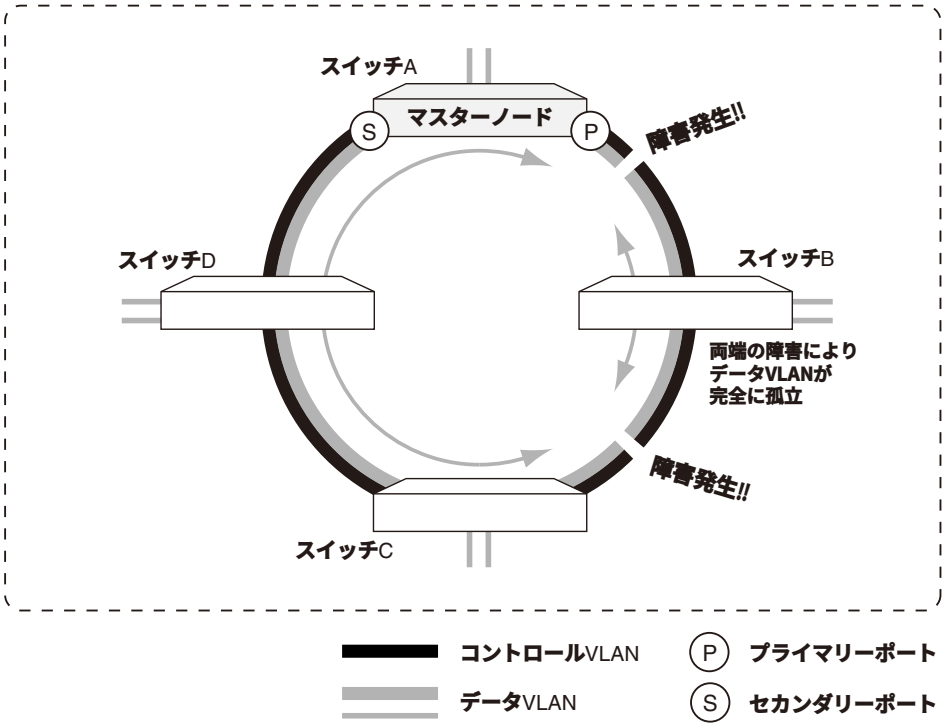
障害回復時

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

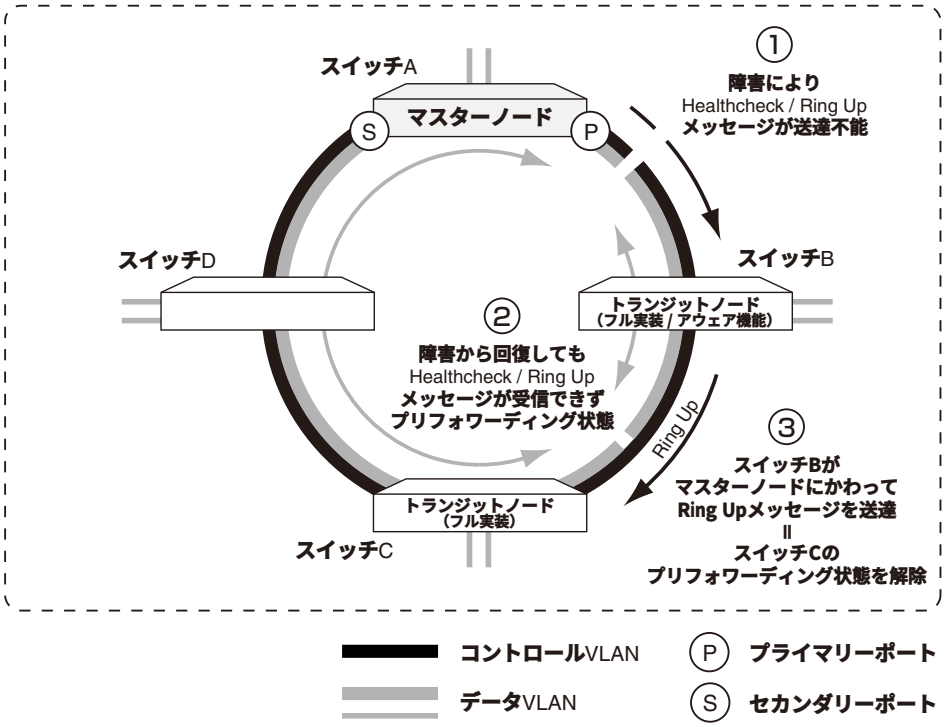
あるノードの両端のリンクに障害が発生している状態を Double Fail と呼びます。
下図のように、Double Fail が発生したノードであるスイッチ B の下流側（マスターノードのセカンダリー

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、もう一方のプライマリー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。



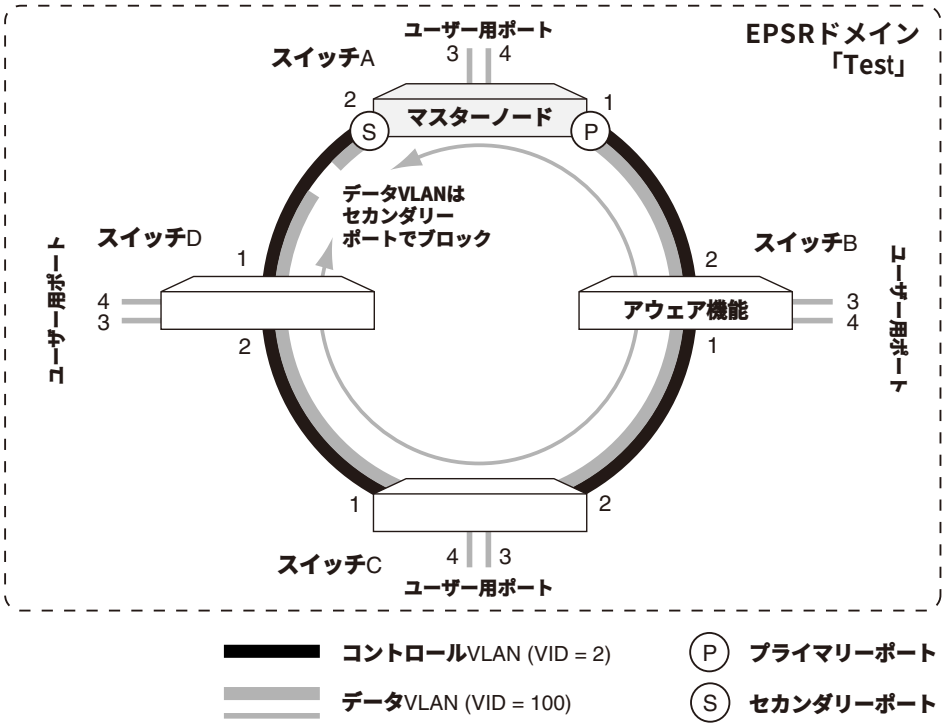
この問題を解決するため、スイッチ B は、片方のポートがリンクアップしてから 4 秒経過してももう一方のポートがリンクアップしない場合、マスターノードの代わりに Ring Up メッセージを送出してスイッチ C をフォワーディング状態に遷移させます。

✎ 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（タグ無しポートとして）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。

UDLD

UDLD（UniDirectional Link Detection）は、UDLD プローブメッセージ (UDLD PDU) というフレームを使って、対向機器との間でフレームの到達性を監視する機能（RFC5171）です。
フレームの送信、もしくは受信が正しく行えない、Unidirectional（単一方向）のリンク状態を検出したとき、ポートを閉塞します。
オプションを設定することで、ポート閉塞後、一定期間を置いて閉塞状態を解除することができます。
本機能はデフォルトでは無効になっています。
ここでは、コマンドラインインターフェースによる設定方法を中心に説明します。なお、Web GUI では「スイッチ設定」-「UDLD」で設定できます。（詳細は「Web GUI」/「スイッチ設定」をご覧ください。）

✎ 本製品では UDLD PDU フレームの送信元 MAC アドレスに固有のアドレス「00-00-F4-27-71-09」を使用しており、対向機器との接続によっては MAC アドレスの移動が発生するため、MAC アドレススラッシングプロテクションによるループガード機能を有効にした機器との接続はできません。

✎ UDLD 動作機器同士の間に、UDLD 非サポートの HUB やスイッチ製品を接続しないでください。

UDLD の構成

UDLD 機能の基本的な用語を解説します。

Bidirectional state

UDLD で検出される稼働状況（Bidirectional state）については、下表をご覧ください。

Unknown	初期状態
Neighbor’s echo is empty	受信した UDLD プローブメッセージの Neighbor キャッシュの内容がない場合
Bidirectional（双方向）	対向機器との間で、イーサネットの TX ポートからフレームを送信し、RX ポートでフレームを受信できる状態
Unidirectional（単一方向）	対向機器との間で、イーサネットの TX ポートからフレームが送信できない、もしくは、RX ポートでフレームを受信できない状態
Transmit-to-receive loop	該当ポートで自身の UDLD プローブメッセージを受信した状態（対向機器からループバックしてしまった）

表 5:

Operational state

UDLD の状態（Operational state）には、以下の種類があり、処理の流れで遷移します。

Inactive (Link down / Disabled port)	UDLD が無効となっているか、ポートがリンクダウンしている状態

Link up	ポートがリンクアップして、UDLD プローブメッセージを受信していない状態
Detection	対向機器から UDLD プローブメッセージを受信して、UDLD の稼働状態が Bidirectional となるまでの状態
Extended detection	Detection フェーズで Neighbor 情報が収集できなかった場合の状態
Advertisement	対向機器から UDLD プローブメッセージを受信しない状態
Advertisement - Single neighbor detected	単一の対向機器との間で、Bidirectional が確立した状態
Advertisement - MULTIPLE NEIGHBORS DETECTED	複数の対向機器との間で、Bidirectional が確立した状態（未サポート）

表 6: Operational state (フェーズ)

UDLD のタイマー

UDLD で使用されるタイマーには、以下の種類があります。

メッセージインターバル	対向機器に UDLD プローブメッセージを送信する間隔。デフォルトは 15 秒
ディテクションウィンドウ	対向機器から最初に UDLD プローブメッセージを受信してから、Bidirectional となるまでに許容される間隔。5 秒で固定

表 7:

✎ メッセージインターバルの設定値が有効となるのは、UDLD の稼働状況が Bidirectional で、状態が Advertisement フェーズとなった場合のみであり、Link up および Detection フェーズでは、設定値ではなく 1 秒間隔で送信します。また、稼働状況が Bidirectional でないときに、Advertisement フェーズとなった場合には、7 秒間隔で送信します。

UDLD の基本動作

UDLD 機能では、次の手順で対向機器との間で到達性を確認し、単一方向のリンクを検出した場合はポートを閉塞します。

Link up フェーズ

UDLD が有効となっているポートがリンクアップすると、1 秒間隔で UDLD プローブメッセージを送信し始めます。
8 回 UDLD プローブメッセージを送信するまでの間に、対向機器からの UDLD プローブメッセージを受信できない場合は、Advertisement フェーズへ移行します。
対向機器から UDLD プローブメッセージを受信すると、Detection フェーズへ移行します。

Detection フェーズ

対向機器に対して、1 秒間隔で 5 回（＝ディテクションウィンドウ）、受信したプローブメッセージから抽出した情報を埋め込んだエコーメッセージを送信します。
ディテクションウィンドウの間に自分の情報が格納されているエコーメッセージを受信すると、ディテクションウィンドウ終了後、稼働状況を Bidirectional とし、Advertisement フェーズに移行します。

Extended detection フェーズ

ディテクションウィンドウの間に自分の情報が格納されているエコーメッセージを受信できない場合、拡張ディテクションウィンドウが開始され、以後は 7 秒間隔でエコーを送信します。
拡張ディテクションウィンドウの間に空のエコーを受信すると Unidirectional と判断し、該当ポートを閉塞します。
拡張ディテクションウィンドウに移行した後、対向機器から通知されるメッセージインターバルの 3 倍の時間が経過すると、Link up フェーズへ移行します。

Advertisement フェーズ

稼働状況が Bidirectional の場合、設定されたメッセージインターバルの間隔で UDLD プローブメッセージを送信し続けます。（ただし、Advertisement フェーズに移行した最初の 5 回分は、7 秒間隔で送信）
稼働状況が Bidirectional でない場合、7 秒間隔でプローブメッセージを送信し続けます。
対向機器から送られてくる UDLD プローブメッセージに、自分の情報が含まれなくなった後、対向機器から通知されるメッセージインターバルの 3 倍の時間が経過すると、Link up フェーズへ移行します。

UDLD の動作モード

UDLD の動作モードにはノーマルモードとアグレッシブモードの 2 種類があり、一旦 Bidirectional が確立した後に、Unidirectional のリンク状態を検出する処理が異なります。
UDLD 機能がノーマルモードで動作しているときは、Extended detection フェーズにおいて、拡張ディテクションウィンドウの間に空のエコーを受信することで Unidirectional と判断し、ポートを閉塞します。
このため、対向機器のポートが送信も受信もできない状態の場合、Unidirectional を検出することができません。
動作モードをアグレッシブモードに設定すると、Link up フェーズに移行後、1 秒間隔で 8 回、UDLD プローブメッセージを送信し、その間に対向機器から UDLD プローブメッセージを受信できなかった場合、リンク状態は Unidirectional と判断され、ポートを閉塞します。
このため、対向機器のポートが送信も受信もできない状態でも、Unidirectional を検出できます。

> ✎ アグレッシブモードが動作する条件として、一度、対向機器とのリンクが Bidirectional で確立した後、Link up フェーズに移行する必要があります。

UDLD 機能の有効/無効

本製品で UDLD 機能を使うには、UDLD 機能を有効にする必要があります。

■ UDLD 機能を有効にするには、ENABLE UDLD コマンド（98 ページ）を使います。例えば、ポート 1

～5 で UDLD 機能を有効にするには、次のように設定します。

```
ENABLE UDLD PORT=1-5 ↵
```

■ UDLD の動作モードをアグレッシブモードに切り替えるには、ENABLE UDLD コマンド（98 ページ）の AGGRESSIVE パラメーターを指定します。本パラメーターを省略した場合は、UDLD はノーマルモードで動作します。

```
ENABLE UDLD PORT=2 AGGRESSIVE ↵
```

■ UDLD 機能を無効にするには、DISABLE UDLD コマンド（80 ページ）を使います。

```
DISABLE UDLD PORT=1-5 ↵
```

UDLD の各種設定

対向機器に UDLD プローブメッセージを送信する間隔や、Unidirectional 検出によるポート閉塞の持続時間を変更する方法と、ポート閉塞状態を解除する方法を説明します。

■ 対向機器に UDLD プローブメッセージを送信する間隔（メッセージインターバル）は、SET UDLD コマンド（127 ページ）の MESSAGETIME パラメーターで設定可能です。単位は秒で、デフォルトは 15 秒です。

```
SET UDLD MESSAGETIME=10 ↵
```

■ Unidirectional 検出によるポート閉塞の持続時間は、SET UDLD コマンド（127 ページ）の DISABLETIME パラメーターで設定可能です。単位は秒で、NONE を指定するとポート閉塞時間は無制限に設定されます。デフォルトは NONE です。

```
SET UDLD DISABLETIME=60 ↵
```

■ Unidirectional 検出によるポート閉塞状態を解除するには、RESET UDLD コマンド（108 ページ）を使います。

```
RESET UDLD ↵
```

その他

■ UDLD 機能の各種情報を確認するには、SHOW UDLD コマンド（171 ページ）、SHOW UDLD NEIGHBORS コマンド（174 ページ）を使います。

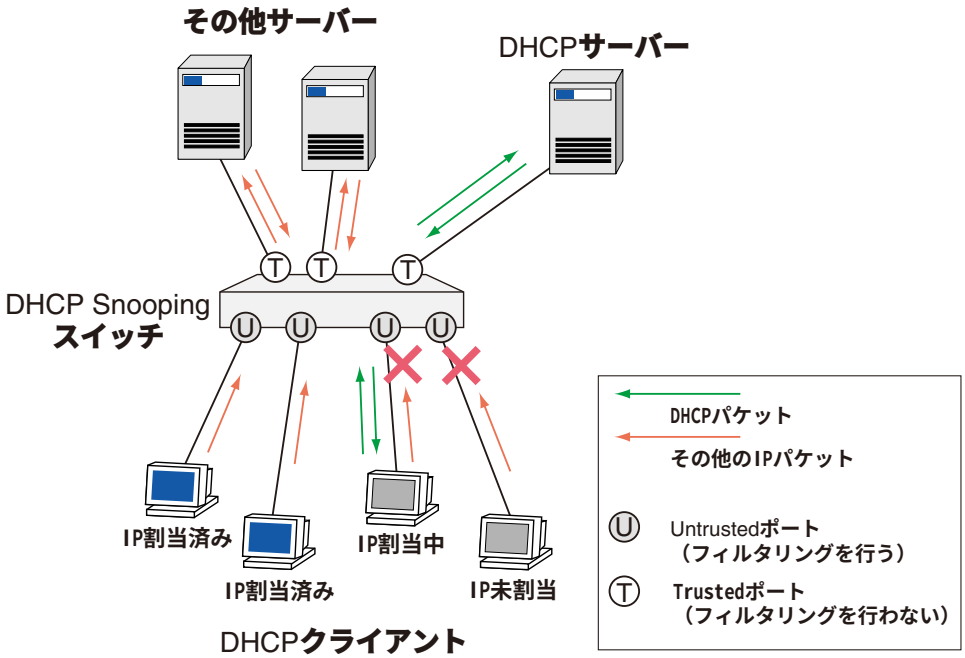
```
SHOW UDLD PORT=1-3 ↵


SHOW UDLD NEIGHBORS ↵
```

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。

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。



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。

✎ DHCP Snooping とスパニングツリープロトコルの併用はできません。

✎ Untrusted ポートと下記のポートは併用できません。

- ポートトランキング
- Web 認証ポート
- EPSR アウェア
- ポートセキュリティー
- RSTP/MSTP

登録できるクライアントの数

ポートごとに、最大 5 クライアントまで登録でき、装置全体では最大 255 クライアントまで登録できます。

基本設定

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

1. DHCP Snooping を有効にします。

```
ENABLE 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 ↵
```

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

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

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

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

ポート種別の設定は、SET DHCPSNOOPING PORT コマンド（113 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（113 ページ）の MAXLEASES パラメーターで接続台数を指定します。

```
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 コマンド（44 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（113 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（82 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、MAC アドレスフィルタリング機能を使用して、IP アドレスを割り当てるクライアントを MAC アドレスで制限することができます。
Untrusted ポートで受信した DHCP パケット（BOOTREQUEST）に対して、条件にマッチした登録エントリーのアクションに従って、許可または破棄を行うことができます。特定の機器に対してのみ DHCP で IP アドレスを配布したい場合などの用途で利用できます。
MAC アドレスフィルタリングエントリーを作成するには、CREATE DHCPSNOOPING MACFILTER コマンド（50 ページ）を使います。

■ 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（84 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（113 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（109 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 CHECKOPTION コマンド（110 ページ）を使います。

```
SET DHCPSNOOPING CHECKOPTION=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 NVS（Non-Volatile Storage）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 NVS からクライアント情報を読み込み、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（128 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（137 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（132 ページ）を使います。

```
SHOW DHCPSNOOPING DATABASE ↵
```

■ MAC アドレスフィルタリングの設定情報を表示するには、SHOW DHCPSNOOPING MACFILTER コマンド（135 ページ）を使います。

```
SHOW DHCPSNOOPING MACFILTER ↵
```

コマンドリファレンス編

機能別コマンド索引

概要・基本設定

ACTIVATE SWITCH PORT AUTONEGOTIATE

カテゴリー：スイッチング

ACTIVATE SWITCH PORT={***port-list***|**ALL**} **AUTONEGOTIATE**

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

解説

指定ポートでオートネゴシエーションプロセスを強制起動し、接続先ポートと通信モード（速度/デュプレックス）のネゴシエーションを行わせる。指定ポートがオートネゴシエーションでない場合は実行されない

パラメーター

PORT　対象となるスイッチポート番号または ALL。ALL を指定した場合はすべてのスイッチポートが対象となる

入力・出力・画面例

```
Manager > activate switch port=1 autonegotiate

 Operation successful.
```

例

■ポート 1 にオートネゴシエーションを行わせる

```
ACTIVATE SWITCH PORT=1 AUTONEGOTIATE
```

関連コマンド

DISABLE SWITCH PORT（73 ページ）
ENABLE SWITCH PORT（92 ページ）
RESET SWITCH PORT（105 ページ）
SET SWITCH PORT（120 ページ）
SHOW SWITCH PORT（153 ページ）

ADD DHCPSNOOPING

カテゴリー：スイッチング

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 から VLANvid の形式。name は VLAN 名、vid は VLAN ID)
ipadd: IP アドレス（xxx.xxx.xxx.xxx の形式）
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

入力・出力・画面例

```
Manager > ADD DHCPSNOOPING BINDING=00-00-00-00-00-01 INTER-
FACE=vlan2 IP=192.168.10.5 PORT=5

Operation successful.
```

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「vlan2」、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=vlan2
  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。
Trusted ポートにスタティックエントリーを登録することはできない。
スタティックエントリーと同じ IP アドレスを DHCP Server から付与することはできない。DHCP レンジ内の IP アドレスをスタティック登録してはならない。

関連コマンド

DELETE DHCPSNOOPING（56 ページ）
DISABLE DHCPSNOOPING（63 ページ）
ENABLE DHCPSNOOPING（81 ページ）
SHOW DHCPSNOOPING DATABASE（132 ページ）

ADD EPSR DATAVLAN

カテゴリー：スイッチング

ADD EPSR=*epsrname* DATAVLAN={***vlan-name***|*1..4094*}

epsrname: EPSR ドメイン名（1〜15 文字。英数字とハイフン [-]、アンダーバー [_]、ピリオド [.]、開始丸かっこ [(]、終了丸かっこ [)] が使用可能。大文字小文字を区別しない）
vlan-name: VLAN 名

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 255 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）
・MSTP の MST インスタンスに関連付けられた VLAN は指定できない

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。

入力・出力・画面例

```
Manager > add epsr=blue datavlan=skyblue

 Operation successful.
```

例

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

```
ADD EPSR=blue DATAVLAN=skyblue
```

関連コマンド

CREATE EPSR（52 ページ）
CREATE VLAN（「バーチャル LAN」の 14 ページ）
DELETE EPSR DATAVLAN（57 ページ）
SHOW EPSR（139 ページ）

ADD SWITCH TRUNK

カテゴリー：スイッチング

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

trunk: トランクグループ名
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　対象となるスイッチポート番号。1 グループに 8 ポートまで追加可能

入力・出力・画面例

```
Manager > add switch trunk=uplink port=1

 Operation successful.
```

例

■トランクグループ「uplink」にポート 1 を追加する

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

備考・注意事項

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指定できない。
ポートセキュリティーが有効なポート、ポート認証の Authenticator ポートと Supplicant ポートはトランクグループに所属させることはできない。
トランクポートは同じ VLAN に所属している必要がある。
STP 有効ポートと STP 無効ポートは同じトランクグループに所属できない。
SFP ポートと SFP ポート以外のポートは同じトランクグループに所属できない。
セキュリティーモードを設定したポートは指定できない。
LDF 検出機能が有効に設定されたポートと無効に設定されたポートを同じトランクグループに指定することはできない。

受信レート検出機能が有効に設定されたポートと無効に設定されたポートを同じトランクグループに指定することはできない。
トランクポートを MDI/MDI-X 自動認識無効に設定できない。ただし、MDI/MDI-X 自動認識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。
SET SWITCH PORT コマンドの FLOWCONTROL パラメーターはトランクポートでは同じ設定する必要がある。
フローコントロールの有効/無効（ENABLE SWITCH PORT FLOW コマンド/DISABLE SWITCH PORT FLOW コマンド）はトランクポートでは同じ設定にする必要がある。
トランクグループに所属するポートからケーブルを抜くと、そのトランクグループに所属する MAC アドレスはすべて消去される。
100M SFP ポートは、トランクグループに所属させることができない。

関連コマンド

CREATE SWITCH TRUNK（54 ページ）
DELETE SWITCH TRUNK（59 ページ）
DESTROY SWITCH TRUNK（62 ページ）
SET SWITCH TRUNK（126 ページ）
SHOW SWITCH TRUNK（169 ページ）

CREATE DHCPSNOOPING MACFILTER

カテゴリー：スイッチング

CREATE DHCPSNOOPING MACFILTER=*1..999* [ADDRESS={*macadd*|ANY}]
[MASK=*macadd*] [VLAN={*vlan-name*|*1..4094*|ANY}] [PORT={*port-list*|ALL|NONE}]
[ACTION={DENY|PERMIT}]

macadd: MAC アドレス（xx:xx:xx:xx:xx:xx の形式）
vlan-name: VLAN 名
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

MAC アドレスフィルタリングエントリーを作成する。

パラメーター

MACFILTER　作成するエントリーの ID。
ADDRESS　フィルタリング対象装置の MAC アドレス。省略時は ANY。
MASK　フィルタリング対象装置の MAC アドレスへのマスクを指定する。省略時は ff-ff-ff-ff-ff-ff
VLAN　入力 VLAN 名または VID。省略時は ANY。
PORT　MAC アドレスフィルタリングを割り当てるポートを指定する。デフォルトは NONE。
ACTION　条件に一致したときのアクション。PERMIT（許可）、DENY（破棄）から選択する。デフォルトは DENY。

入力・出力・画面例

```
Manager > create dhcpsnooping macfilter=1 address=00-09-41-00-00-00 mask=ff-ff-
ff-00-00-00 port=all action=permit

Operation successful.


Manager > create dhcpsnooping macfilter=2 address=00-1a-eb-00-00-00 mask=ff-ff-
ff-00-00-00 port=all action=permit

Operation successful.

Manager >create dhcpsnooping macfilter=3 port=all action=deny

Operation successful.
```

例

■ベンダー ID が 000941 と 001AEB の装置だけスヌーピング対象にする。

```
CREATE DHCPSNOOPING MACFILTER=1 ADDRESS=00-09-41-00-00-00
  MASK=ff-ff-ff-00-00-00 PORT=ALL ACTION=PERMIT
CREATE DHCPSNOOPING MACFILTER=2 ADDRESS=00-1a-eb-00-00-00
  MASK=ff-ff-ff-00-00-00 PORT=ALL ACTION=PERMIT
CREATE DHCPSNOOPING MACFILTER=3 PORT=ALL ACTION=DENY
```

備考・注意事項

エントリーは 128 個まで作成できる。
エントリー ID の番号順に検索し、マッチしたエントリーのアクションを実行する。それ以降のエントリーはチェックされない。
Trusted ポートでは MAC アドレスフィルタリング機能は働かない。
ポート設定が NONE のエントリーは機能しない。無効なエントリーとして扱われる。
MAC アドレスが ANY のエントリーはすべての装置が対象となる。
どのエントリーにもマッチしない場合は、許可（Permit）として扱われる。
エントリー作成時に、既に該当エントリーがバインディングデータベースに登録されていた場合、そのエントリーに対してはなにも処理されない。
作成されたエントリーは、次回の更新などでクライアントから DHCP パケットを受信した際に機能する。
従って、CHECKOPTION で DHCPRELEASE を有効にしていた場合に、作成したエントリーのアクションが破棄（Deny）のときは機能しなくなるので注意が必要。
エントリー作成時には、適宜バインディングデータベースのエントリーを削除すること。

関連コマンド

DESTROY DHCPSNOOPING MACFILTER（60 ページ）
SET DHCPSNOOPING MACFILTER（111 ページ）
SHOW DHCPSNOOPING MACFILTER（135 ページ）

CREATE EPSR

カテゴリー：スイッチング

CREATE EPSR=*epsrname* MODE={AWARE|TRANSIT} CONTROLVLAN={*vlan-name*|*1..4094*} [DELETEMCAST]

epsrname: EPSR ドメイン名（1〜15 文字。英数字とハイフン [-]、アンダーバー [_]、ピリオド [.]、開始丸かっこ [(]、終了丸かっこ [)] が使用可能。大文字小文字を区別しない）
vlan-name: VLAN 名

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 8 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 ポートとみなす）。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。
・スパニングツリープロトコル（STP/RSTP/MSTP）、ポートセキュリティー、ポート認証が有効なポートが所属する VLAN はコントロール VLAN に指定できない。

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）と TRANSIT（通常のアウェア機能に加え ” 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 ” および ” トラップ送信機能 ” を行い「フル実装」と同等の動作を行うトランジットノード）から選択する。
CONTROLVLAN　コントロール VLAN。VLAN 名または VLAN ID（VID）で指定する
DELETEMCAST　リングトポロジーチェンジが発生した場合、IGMP Snooping/MLD Snooping で使用するマルチキャストアドレスを FDB から削除する。このパラメーターを指定しない場合、FDB からマルチキャストエントリーを削除しない。ただし、MLD マルチキャストアドレスが手動で登録されている場合は、このパラメーターを指定した場合でも削除しない。

入力・出力・画面例

```
Manager > create epsr=blue mode=aware controlvlan=blue_control

 Operation successful.
```

例

■EPSR ドメイン「blue」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「blue_control」を指定する。

```
CREATE EPSR=blue MODE=AWARE CONTROLVLAN=blue_control
```

備考・注意事項

コントロール VLAN には 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 リングポートと Authenticator/Supplicant ポートの併用は不可

関連コマンド

ADD EPSR DATAVLAN（46 ページ）
CREATE VLAN（「バーチャル LAN」の 14 ページ）
DESTROY EPSR（61 ページ）
ENABLE EPSR（85 ページ）
SHOW EPSR（139 ページ）

CREATE SWITCH TRUNK

カテゴリー：スイッチング

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

trunk: トランクグループ名（1〜20 文字。半角英数字、およびハイフン [-]、アンダーバー [_]、ピリオド [.]、開始丸かっこ [(]、終了丸かっこ [)] が使用可。大文字・小文字の属性は無視されるが、表示には大文字・小文字の区別が反映される）
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。16 グループまで作成可能。1 グループには 8 ポートまで追加可能。

パラメーター

TRUNK　トランクグループ名
PORT　対象となるスイッチポート番号
SPEED　トランクポートの通信速度（1000M、100M、10M）。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となる。デフォルトは 1000M。SFP ポートは 1000M のみ指定可能。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

入力・出力・画面例

```
Manager > create switch trunk=uplink speed=1000m

 Operation successful.
```

例

■トランクグループ「uplink」を作成する。通信速度は 1000M とする

```
CREATE SWITCH TRUNK=uplink SPEED=1000M
```

備考・注意事項

マスターポートはトランクグループに所属するポートのうちポート番号の一番小さいポートとなる。
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指定できない。
ポートセキュリティーが有効なポート、ポート認証の Authenticator ポートと Supplicant ポートはトラン

クグループに所属させることはできない。
トランクポートは同じ VLAN に所属している必要がある。
STP 有効ポートと STP 無効ポートは同じトランクグループに所属できない。
SFP ポートと SFP ポート以外のポートは同じトランクグループに所属できない。
セキュリティーモードを設定したポートは指定できない。
LDF 検出機能が有効に設定されたポートと無効に設定されたポートを同じトランクグループに指定することはできない。
受信レート検出機能が有効に設定されたポートと無効に設定されたポートを同じトランクグループに指定することはできない。
SET SWITCH PORT コマンドの FLOWCONTROL パラメーターはトランクポートでは同じ設定にする必要がある。
100M SFP ポートは、トランクグループに所属させることができない。

関連コマンド

ADD SWITCH TRUNK（48 ページ）
DELETE SWITCH TRUNK（59 ページ）
DESTROY SWITCH TRUNK（62 ページ）
SET SWITCH TRUNK（126 ページ）
SHOW SWITCH TRUNK（169 ページ）

DELETE DHCPSNOOPING

カテゴリー：スイッチング

DELETE DHCPSNOOPING BINDING[=*macadd*] [IP=*ipadd*]

macadd: MAC アドレス（xx-xx-xx-xx-xx-xx の形式）
ipadd: IP アドレス（xxx.xxx.xxx.xxx の形式）

解説

DHCP Snooping テーブル（バインディングデータベース）からエントリーを削除する。

パラメーター

BINDING　クライアントの MAC アドレス
IP　　クライアントの IP アドレス

入力・出力・画面例

```
Manager >Delete Dhcpsnooping Binding=00-00-00-00-00-01  IP=192.168.10.5

Operation successful.
```

例

■IP アドレス 192.168.10.5、MAC アドレス 00-00-00-00-00-01 のクライアントのバインディングデータベースを削除する

```
DELETE DHCPSNOOPING BINDING=00-00-00-00-00-01 IP=192.168.10.5
```

関連コマンド

ADD DHCPSNOOPING（44 ページ）
DISABLE DHCPSNOOPING（63 ページ）
ENABLE DHCPSNOOPING（81 ページ）
SHOW DHCPSNOOPING DATABASE（132 ページ）

DELETE EPSR DATAVLAN

カテゴリー：スイッチング

DELETE EPSR=*epsrname* DATAVLAN={*vlan-name*|*1..4094*|ALL}

epsrname: EPSR ドメイン名（1〜15 文字。英数字とハイフン [-]、アンダーバー [_]、ピリオド [.]、開始丸かっこ [(]、終了丸かっこ [)] が使用可能。大文字小文字を区別しない）
vlan-name: VLAN 名

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無効にする
・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

入力・出力・画面例

```
Manager > delete epsr=blue datavlan=skyblue

 Operation successful.
```

例

■EPSR ドメイン「blue」からデータ VLAN「skyblue」を削除する

```
DELETE EPSR=blue DATAVLAN=skyblue
```

関連コマンド

ADD EPSR DATAVLAN（46 ページ）
CREATE EPSR（52 ページ）
DELETE VLAN PORT（「バーチャル LAN」の 15 ページ）
DISABLE SWITCH PORT（73 ページ）

SHOW EPSR（139 ページ）

DELETE SWITCH TRUNK

カテゴリー：スイッチング

DELETE SWITCH TRUNK=*trunk* PORT={*port-list*|ALL}

trunk: トランクグループ名
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　対象となるスイッチポート番号。ALL を指定した場合は指定したトランクグループに所属するすべてのポートが対象となる

入力・出力・画面例

```
Manager > delete switch trunk=uplink port=1

 Operation successful.
```

例

■トランクグループ「uplink」からポート 1 を削除する

```
DELETE SWITCH TRUNK=uplink PORT=1
```

関連コマンド

ADD SWITCH TRUNK（48 ページ）
CREATE SWITCH TRUNK（54 ページ）
DESTROY SWITCH TRUNK（62 ページ）
SET SWITCH TRUNK（126 ページ）
SHOW SWITCH TRUNK（169 ページ）

DESTROY DHCPSNOOPING MACFILTER

カテゴリー：スイッチング

DESTROY DHCPSNOOPING MACFILTER={***id-list***|**ALL**}

id-list: フィルター番号（1〜999。ハイフン、カンマを使った複数指定も可能）

解説

MAC アドレスフィルタリングエントリーを削除する。

パラメーター

MACFILTER　削除するエントリーの ID。複数指定が可能。ALL を指定した場合はすべてのエントリーが対象となる。

入力・出力・画面例

```
Manager > destroy dhcpsnooping macfilter=2,3

Operation successful.
```

例

■MAC フィルターエントリー 2 から 3 を削除する

```
DESTROY DHCPSNOOPING MACFILTER=2,3
```

関連コマンド

CREATE DHCPSNOOPING MACFILTER（50 ページ）
SET DHCPSNOOPING MACFILTER（111 ページ）
SHOW DHCPSNOOPING MACFILTER（135 ページ）

DESTROY EPSR

カテゴリー：スイッチング

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

epsrname: EPSR ドメイン名（1〜15 文字。英数字とハイフン [-]、アンダーバー [_]、ピリオド [.]、開始丸かっこ [(]、終了丸かっこ [)] が使用可能。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無効にする
・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

入力・出力・画面例

```
Manager > destroy epsr=blue

 Operation successful.
```

例

■EPSR ドメイン「blue」を削除する

```
DESTROY EPSR=blue
```

関連コマンド

CREATE EPSR（52 ページ）
DELETE EPSR DATAVLAN（57 ページ）
DELETE VLAN PORT（「バーチャル LAN」の 15 ページ）
DISABLE EPSR（67 ページ）
DISABLE SWITCH PORT（73 ページ）
SHOW EPSR（139 ページ）

DESTROY SWITCH TRUNK

カテゴリー：スイッチング

DESTROY SWITCH TRUNK=*trunk*

trunk: トランクグループ名

解説

トランクグループを削除する

パラメーター

TRUNK　トランクグループ名

入力・出力・画面例

```
Manager > destroy switch trunk=uplink

 Operation successful.
```

例

■トランクグループ「uplink」を削除する

```
DESTROY SWITCH TRUNK=uplink
```

備考・注意事項

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。

関連コマンド

ADD SWITCH TRUNK（48 ページ）
CREATE SWITCH TRUNK（54 ページ）
DELETE SWITCH TRUNK（59 ページ）
SET SWITCH TRUNK（126 ページ）
SHOW SWITCH TRUNK（169 ページ）

DISABLE DHCPSNOOPING

カテゴリー：スイッチング

DISABLE DHCP SNOOPING

解説

DHCP Snooping を無効にする。デフォルトは無効。

入力・出力・画面例

```
Manager > disable dhcp snooping

Operation successful.
```

例

■DHCP Snooping を無効にする

```
DISABLE DHCP SNOOPING
```

関連コマンド

ENABLE DHCPSNOOPING（81 ページ）
SHOW DHCPSNOOPING（128 ページ）

DISABLE DHCPSNOOPING ARPSECURITY

カテゴリー：スイッチング

DISABLE DHCP SNOOPING ARPSECURITY

解説

ARP セキュリティーを無効にする。デフォルトは無効。

入力・出力・画面例

```
Manager > disable dhcp snooping arpsecurity

Operation successful.
```

例

■ARP セキュリティーを無効にする

```
DISABLE DHCP SNOOPING ARPSECURITY
```

関連コマンド

ENABLE DHCPSNOOPING（81 ページ）
ENABLE DHCPSNOOPING ARPSECURITY（82 ページ）
SHOW DHCPSNOOPING（128 ページ）

DISABLE DHCPSNOOPING LOG

カテゴリー：スイッチング

DISABLE DHCPSNOOPING LOG={**ARPSECURITY**|**MACFILTER**}

解説

DHCP Snooping のログ機能を無効にする。デフォルトは無効。

パラメーター

LOG ログに記録するイベントの種類。カンマ区切りによる複数指定が可能。ARPSECURITY イベントは、ARP セキュリティー機能によってバインディングデータベース未登録の送信元からの ARP パケットを破棄したときに発生する。MACFILTER イベントは、MAC アドレスフィルタリング機能によって DHCP パケットを破棄したときに発生する。

入力・出力・画面例

```
Manager > disable dhcp snooping log=arpsecurity,macfilter

Operation successfu.
```

例

■ログ機能 (ARPSECURITY と MACFILTER の両方) を無効にする

```
DISABLE DHCP SNOOPING LOG=ARPSECURITY,MACFILTER
```

関連コマンド

ENABLE DHCPSNOOPING（81 ページ）
ENABLE DHCPSNOOPING LOG（83 ページ）
SHOW DHCPSNOOPING（128 ページ）

DISABLE DHCPSNOOPING OPTION82

カテゴリー：スイッチング

DISABLE DHCPSNOOPING OPTION82

解説

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（81 ページ）
ENABLE DHCPSNOOPING OPTION82（84 ページ）
SHOW DHCPSNOOPING（128 ページ）

DISABLE EPSR

カテゴリー：スイッチング

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

epsrname: EPSR ドメイン名（1〜15 文字。英数字とハイフン [-]、アンダーバー [_]、ピリオド [.]、開始丸かっこ [(]、終了丸かっこ [)] が使用可能。大文字小文字を区別しない）

解説

EPSR ドメインを無効にする。
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無効にする
・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

入力・出力・画面例

```
Manager > disable epsr=blue

 Operation successful.
```

例

■EPSR ドメイン「blue」を無効にする

```
DISABLE EPSR=blue
```

関連コマンド

CREATE EPSR（52 ページ）
DELETE VLAN PORT（「バーチャル LAN」の 15 ページ）
DISABLE SWITCH PORT（73 ページ）
ENABLE EPSR（85 ページ）
SHOW EPSR（139 ページ）

DISABLE SWITCH BPDUFORWARDING

カテゴリー：スイッチング

DISABLE SWITCH BPDUFORWARDING

解説

BPDU 透過機能を無効にする。デフォルトは無効

入力・出力・画面例

```
Manager > disable switch bpduforwarding

 Operation successful.
```

例

■BPDU 透過機能を無効にする

```
DISABLE SWITCH BPDUFORWARDING
```

備考・注意事項

STP 有効ポートがある場合、BPDU 透過機能は使用できない。

関連コマンド

ENABLE SWITCH BPDUFORWARDING（86 ページ）

DISABLE SWITCH EAPFORWARDING

カテゴリー：スイッチング

DISABLE SWITCH EAPFORWARDING

解説

EAP 透過機能を無効にする。デフォルトは無効

入力・出力・画面例

```
Manager > disable switch eapforwarding

 Operation successful.
```

例

■EAP 透過機能を無効にする

```
DISABLE SWITCH EAPFORWARDING
```

備考・注意事項

ポート認証有効の場合、EAP 透過機能は使用できない。

関連コマンド

ENABLE SWITCH EAPFORWARDING（87 ページ）

DISABLE SWITCH INFILTERING

カテゴリー：スイッチング

DISABLE SWITCH INFILTERING

解説

イングレスフィルタリングを無効にする。有効のときは、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。無効の場合はすべてのフレームを受け入れる。デフォルトは無効

入力・出力・画面例

```
Manager > disable switch infiltering

 Operation successful.
```

例

■イングレスフィルタリングを無効にする

```
DISABLE SWITCH INFILTERING
```

備考・注意事項

イングレスフィルタリング無効時は、受信パケットの VID が受信ポートの所属 VLAN と一致していない場合でも該当パケットは破棄されないが、ポート認証やポートセキュリティーによってスタティックエントリーとして FDB に登録されている MAC アドレスを送信元 MAC アドレスに持つパケットについては、VID が一致していないと転送されずに破棄される。

関連コマンド

ENABLE SWITCH INFILTERING（88 ページ）

DISABLE SWITCH LOOPDETECTION

カテゴリー：スイッチング

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

入力・出力・画面例

```
Manager > disable switch loopdetection port=2

Operation successful.
```

例

■ポート 2 の LDF 機能を無効にする

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

関連コマンド

ENABLE SWITCH LOOPDETECTION（89 ページ）
RESET SWITCH LOOPDETECTION COUNTER（104 ページ）
SET SWITCH LOOPDETECTION（116 ページ）
SHOW SWITCH LOOPDETECTION（147 ページ）

DISABLE SWITCH MIRROR

カテゴリー：スイッチング

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わらない。デフォルトは無効

入力・出力・画面例

```
Manager > disable switch mirror

 Operation successful.
```

例

■ ポートミラーリング機能を無効にする

```
DISABLE SWITCH MIRROR
```

関連コマンド

ENABLE SWITCH MIRROR（91 ページ）
SET SWITCH MIRROR（118 ページ）
SHOW SWITCH MIRROR（152 ページ）

DISABLE SWITCH PORT

カテゴリー：スイッチング

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

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 対象となるスイッチポート番号または ALL。ALL を指定した場合はすべてのスイッチポートが対象となる

LINK 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）、または ENABLE（物理的にはリンクアップのまま）。省略時は ENABLE

入力・出力・画面例

```
Manager > disable switch port=1

 Operation successful.
```

例

■ポート 1 を無効にする（物理的なリンクは保持する）

```
DISABLE SWITCH PORT=1
DISABLE SWITCH PORT=1 LINK=ENABLE
```

■ポート 1 を無効にし、物理的にリンクダウンさせる

```
DISABLE SWITCH PORT=1 LINK=DISABLE
```

備考・注意事項

LINK パラメーターを明示的に指定しないで、または ENABLE を指定して本コマンドを実行した場合は、LINK パラメーターに DISABLE を指定して本コマンドを再度実行することで物理的にリンクダウンさせることができる。ただし、LINK パラメーターに DISABLE を指定して物理リンクをリンクダウンさせた場合、

LINK パラメーターに ENABLE を設定して本コマンドを再度実行しても物理リンクをリンクアップさせることはできない。物理リンクを再度リンクアップさせる場合は ENABLE SWITCH PORT コマンドを実行する。

関連コマンド

ACTIVATE SWITCH PORT AUTONEGOTIATE（43 ページ）
ENABLE SWITCH PORT（92 ページ）
RESET SWITCH PORT（105 ページ）
SET SWITCH PORT（120 ページ）
SHOW SWITCH PORT（153 ページ）

DISABLE SWITCH PORT AUTOMDI

カテゴリー：スイッチング

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

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

解説

指定したスイッチポートで MDI/MDI-X 自動認識を無効にする。デフォルトは有効。
本コマンド実行後のスイッチポートの MDI/MDI-X の状態は、ポートの MDI/MDI-X の設定状態にしたがう。デフォルトは、MDI-X。

パラメーター

PORT　対象となるスイッチポート番号または ALL。ALL を指定した場合は、SFP ポートを除くすべてのスイッチポートが対象となる

入力・出力・画面例

```
Manager > disable switch port=1 automdi

 Operation successful.
```

例

■ポート 1 の MDI/MDI-X 自動認識を無効にする

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

備考・注意事項

SFP ポートに対しては、本コマンドを実行できない。
トランクポートを MDI/MDI-X 自動認識無効に設定できない。ただし、MDI/MDI-X 自動認識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。
100MFULL/1000MFULL に設定したポート（SET SWITCH PORT コマンドの SPEED パラメーター）では、本コマンドを実行できない。

関連コマンド

ENABLE SWITCH PORT AUTOMDI（93 ページ）
SHOW SWITCH（144 ページ）

DISABLE SWITCH PORT FLOW

カテゴリー：スイッチング

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

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

フローコントロール（Full Duplex 時の IEEE 802.3x PAUSE 受信）を無効にする。デフォルトは有効

パラメーター

PORT　対象となるスイッチポート番号または ALL。ALL を指定した場合はすべてのスイッチポートが対象となる

入力・出力・画面例

```
Manager > disable switch port=1 flow

 Operation successful.
```

例

■ポート 1 のフローコントロールを無効にする

```
DISABLE SWITCH PORT=1 FLOW
```

備考・注意事項

トランクポートをフローコントロール無効にする場合、トランクグループの全ポートを指定する必要がある。

関連コマンド

ENABLE SWITCH PORT FLOW（94 ページ）
SHOW SWITCH（144 ページ）

DISABLE SWITCH POWERSAVE

カテゴリー：スイッチング

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

入力・出力・画面例

```
Manager > disable switch powersave

 Operation successful.
```

例

■省電力モードを無効にする

```
DISABLE SWITCH POWERSAVE
```

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（95 ページ）
SHOW SWITCH（144 ページ）

DISABLE SWITCH STORMDETECTION

カテゴリー：スイッチング

DISABLE SWITCH STORMDETECTION 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

受信レート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

入力・出力・画面例

```
Manager > disable switch stormdetection port=2

Operation successful
```

例

■ポート 2 の受信レート検出機能を無効にする

```
DISABLE SWITCH STORMDETECTION PORT=2
```

関連コマンド

ENABLE SWITCH STORMDETECTION（96 ページ）
RESET SWITCH STORMDETECTION PORT COUNTER（107 ページ）
SET SWITCH STORMDETECTION（124 ページ）
SHOW SWITCH STORMDETECTION（163 ページ）

DISABLE UDLD

カテゴリー：スイッチング

DISABLE UDLD 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

指定したポートの UDLD 機能を無効にする。デフォルトは無効。

パラメーター

PORT　対象となるスイッチポート番号または ALL。ALL を指定した場合はすべてのポートが対象となる。

入力・出力・画面例

```
Manager > disable udld port=1-5

Operation successful.
```

例

■ポート 1〜5 の UDLD 機能を無効にする

```
DISABLE UDLD PORT=1-5
```

関連コマンド

ENABLE UDLD（98 ページ）
SHOW UDLD（171 ページ）

ENABLE DHCPSNOOPING

カテゴリー：スイッチング

ENABLE DHCP SNOOPING

解説

DHCP Snooping を有効にする。デフォルトは無効。

入力・出力・画面例

```
Manager > enable dhcp snooping

Operation successful.
```

例

■DHCP Snooping を有効にする

```
ENABLE DHCP SNOOPING
```

備考・注意事項

Untrusted ポートと併用できない機能（ポートトランキングや Web 認証）がすでに設定されていてもエラーにはならないので注意。

関連コマンド

DISABLE DHCPSNOOPING（63 ページ）
SHOW DHCPSNOOPING（128 ページ）

ENABLE DHCPSNOOPING ARPSECURITY

カテゴリー：スイッチング

ENABLE DHCP SNOOPING ARPSECURITY

解説

ARP セキュリティーを有効にする。デフォルトは無効。
DHCP Snooping が有効になっていないと動作しない。
本機能を有効にした場合、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る。

入力・出力・画面例

```
Manager > enable dhcp snooping arpsecurity

Operation successful.
```

例

■ARP セキュリティーを有効にする

```
ENABLE DHCP SNOOPING ARPSECURITY
```

備考・注意事項

本体宛てにも機能する。

関連コマンド

DISABLE DHCPSNOOPING（63 ページ）
DISABLE DHCPSNOOPING ARPSECURITY（64 ページ）
SHOW DHCPSNOOPING（128 ページ）

ENABLE DHCPSNOOPING LOG

カテゴリー：スイッチング

ENABLE DHCPSNOOPING LOG={**ARPSECURITY**|**MACFILTER**}

解説

DHCP Snooping のログ機能を有効にする。デフォルトは無効。

パラメーター

LOG ログに記録するイベントの種類。カンマ区切りによる複数指定が可能。ARPSECURITY イベントは、ARP セキュリティー機能によってバインディングデータベース未登録の送信元からの ARP パケットを破棄したときに発生する。MACFILTER イベントは、MAC アドレスフィルタリング機能によって DHCP パケットを破棄したときに発生する。

入力・出力・画面例

```
Manager > enable dhcp snooping log=arpsecurity,macfilter

Operation successful.
```

例

■ログ機能 (ARPSECURITY と MACFILTER の両方) を有効にする

```
ENABLE DHCP SNOOPING LOG=ARPSECURITY,MACFILTER
```

関連コマンド

DISABLE DHCPSNOOPING LOG（65 ページ）
ENABLE DHCPSNOOPING（81 ページ）
SHOW DHCPSNOOPING（128 ページ）

ENABLE DHCPSNOOPING OPTION82

カテゴリー：スイッチング

ENABLE DHCPSNOOPING OPTION82

解説

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）の処理機能を有効にする。デフォルトは無効。DHCP Snooping が有効になっていないと動作しない。
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。

関連コマンド

DISABLE DHCPSNOOPING（63 ページ）
DISABLE DHCPSNOOPING OPTION82（66 ページ）
ENABLE DHCPSNOOPING（81 ページ）
SHOW DHCPSNOOPING（128 ページ）

ENABLE EPSR

カテゴリー：スイッチング

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

epsrname: EPSR ドメイン名（1〜15 文字。英数字とハイフン [-]、アンダーバー [_]、ピリオド [.]、開始丸かっこ [(]、終了丸かっこ [)] が使用可能。大文字小文字を区別しない）

解説

EPSR ドメインを有効にする

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

入力・出力・画面例

```
Manager > enable epsr=blue

 Operation successful.
```

例

■EPSR ドメイン「blue」を有効にする

```
ENABLE EPSR=blue
```

関連コマンド

CREATE EPSR（52 ページ）
DISABLE EPSR（67 ページ）
SHOW EPSR（139 ページ）

ENABLE SWITCH BPDUFORWARDING

カテゴリー：スイッチング

ENABLE SWITCH BPDUFORWARDING

解説

BPDU 透過機能を有効にする。デフォルトは無効

入力・出力・画面例

```
Manager > enable switch bpduforwarding

 Operation successful.
```

例

■BPDU 透過機能を有効にする

```
ENABLE SWITCH BPDUFORWARDING
```

備考・注意事項

STP 有効ポートがある場合、BPDU 透過機能は使用できない。

関連コマンド

DISABLE SWITCH BPDUFORWARDING（68 ページ）

ENABLE SWITCH EAPFORWARDING

カテゴリー：スイッチング

ENABLE SWITCH EAPFORWARDING

解説

EAP 透過機能を有効にする。デフォルトは無効

入力・出力・画面例

```
Manager > enable switch eapforwarding

 Operation successful.
```

例

■EAP 透過機能を有効にする

```
ENABLE SWITCH EAPFORWARDING
```

備考・注意事項

ポート認証有効の場合、EAP 透過機能は使用できない。
タグポートでは EAP にタグが付与される

関連コマンド

DISABLE SWITCH EAPFORWARDING（69 ページ）

ENABLE SWITCH INFILTERING

カテゴリー：スイッチング

ENABLE SWITCH INFILTERING

解説

イングレスフィルタリングを有効にする。有効のときは、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。無効の場合はすべてのフレームを受け入れる。デフォルトは無効

入力・出力・画面例

```
Manager > enable switch infiltering

 Operation successful.
```

例

■イングレスフィルタリングを有効にする

```
ENABLE SWITCH INFILTERING
```

関連コマンド

DISABLE SWITCH INFILTERING（70 ページ）

ENABLE SWITCH LOOPDETECTION

カテゴリー：スイッチング

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

入力・出力・画面例

```
Manager > enable switch loopdetection port=2

Operation successful.
```

例

■ポート 2 の LDF 機能を有効にする

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

備考・注意事項

SET SWITCH LOOPDETECTION コマンドの ACTION パラメーターに BCDISCARD が指定されており、かつパケットストームプロテクションを有効にしたポートが存在する場合、エラーメッセージが表示される。
トランクポートに対して LDF 検出機能を有効にする場合、トランクグループの全ポートを指定する必要がある。
LDF 検出機能は、フローコントロールとは併用できない。
タグ付きポートで LDF 検出機能を有効にする場合、該当ポートをタグなしポートとしても VLAN に所属させる必要がある（LDF の送出と検出はタグなしパケットで行われるため）。

関連コマンド

DISABLE SWITCH LOOPDETECTION（71 ページ）
RESET SWITCH LOOPDETECTION COUNTER（104 ページ）
SET SWITCH LOOPDETECTION（116 ページ）
SHOW SWITCH LOOPDETECTION（147 ページ）

ENABLE SWITCH MIRROR

カテゴリー：スイッチング

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

入力・出力・画面例

```
Manager > enable switch mirror

 Operation successful.
```

例

■ポートミラーリング機能を有効にする

```
ENABLE SWITCH MIRROR
```

関連コマンド

DISABLE SWITCH MIRROR（72 ページ）
SET SWITCH MIRROR（118 ページ）
SHOW SWITCH MIRROR（152 ページ）

ENABLE SWITCH PORT

カテゴリー：スイッチング

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　対象となるスイッチポート番号または ALL。ALL を指定した場合はすべてのスイッチポートが対象となる

入力・出力・画面例

```
Manager > enable switch port=1

 Operation successful.
```

例

■ポート 1 を有効にする

```
ENABLE SWITCH PORT=1
```

関連コマンド

ACTIVATE SWITCH PORT AUTONEGOTIATE（43 ページ）
DISABLE SWITCH PORT（73 ページ）
RESET SWITCH PORT（105 ページ）
SET SWITCH PORT（120 ページ）
SHOW SWITCH PORT（153 ページ）

ENABLE SWITCH PORT AUTOMDI

カテゴリー：スイッチング

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

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

解説

指定したスイッチポートで MDI/MDI-X 自動認識を有効にする。デフォルトは有効。
通信モードがオートネゴシエーション（Autonegotiate）のときのみ実行可能。

パラメーター

PORT　対象となるスイッチポート番号または ALL。ALL を指定した場合は、SFP ポートを除くすべてのスイッチポートが対象となる

入力・出力・画面例

```
Manager > enable switch port=1 automdi

 Operation successful.
```

例

■ポート 1 の MDI/MDI-X 自動認識を有効にする

```
ENABLE SWITCH PORT=1 AUTOMDI
```

備考・注意事項

SFP ポートに対しては、本コマンドを実行できない。
100MFULL/1000MFULL に設定したポート（SET SWITCH PORT コマンドの SPEED パラメーター）では、本コマンドを実行できない。

関連コマンド

DISABLE SWITCH PORT AUTOMDI（75 ページ）
SHOW SWITCH（144 ページ）

ENABLE SWITCH PORT FLOW

カテゴリー：スイッチング

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

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

フローコントロール（Full Duplex 時の IEEE 802.3x PAUSE 受信）を有効にする。デフォルトは有効

パラメーター

PORT　対象となるスイッチポート番号または ALL。ALL を指定した場合はすべてのスイッチポートが対象となる

入力・出力・画面例

```
Manager > enable switch port=1 flow

 Operation successful.
```

例

■ポート 1 のフローコントロールを有効にする

```
ENABLE SWITCH PORT=1 FLOW
```

備考・注意事項

本製品の実装では、PAUSE フレームの受信（受信により送信を一時停止）のみをサポート。本製品が PAUSE フレームを送信することはない。
トランクポートをフローコントロール有効にする場合、トランクグループの全ポートを指定する必要がある。

関連コマンド

DISABLE SWITCH PORT FLOW（77 ページ）
SHOW SWITCH（144 ページ）

ENABLE SWITCH POWERSAVE

カテゴリー：スイッチング

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

入力・出力・画面例

```
Manager > enable switch powersave

 Operation successful.
```

例

■省電力モードを有効にする

```
ENABLE SWITCH POWERSAVE
```

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 0〜3 秒程度の遅延が伴う。

関連コマンド

DISABLE SWITCH POWERSAVE（78 ページ）
SHOW SWITCH（144 ページ）

ENABLE SWITCH STORMDETECTION

カテゴリー：スイッチング

ENABLE SWITCH STORMDETECTION 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

受信レート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

入力・出力・画面例

```
Manager > enable switch stormdetection port=2

Operation successful
```

例

■ポート 2 の受信レート検出機能を有効にする

```
ENABLE SWITCH STORMDETECTION PORT=2
```

備考・注意事項

SET SWITCH STORMDETECTION コマンドの HIGHRATEACTION パラメーターまたは LOWRATE-ACTION パラメーターに BCDISCARD が指定されており、かつパケットストームプロテクションを有効にしたポートが存在する場合、エラーメッセージが表示される。
トランクポートに対して受信レート検出機能を有効にする場合、トランクグループの全ポートを指定する必要がある。

関連コマンド

DISABLE SWITCH STORMDETECTION（79 ページ）
RESET SWITCH STORMDETECTION PORT COUNTER（107 ページ）
SET SWITCH STORMDETECTION（124 ページ）

SHOW SWITCH STORMDETECTION（163 ページ）

ENABLE UDLD

カテゴリー：スイッチング

ENABLE UDLD PORT={***port-list***|**ALL**} [AGGRESSIVE]

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

指定したポートの UDLD 機能を有効にする。デフォルトは無効。
ノーマルモードとアグレッシブモードを切り替えるために、本コマンドの同一ポートで複数回の実行が可能。

パラメーター

PORT　対象となるスイッチポート番号または ALL。ALL を指定した場合はすべてのポートが対象となる。
AGGRESSIVE　UDLD をアグレッシブモードで動作する。省略時は、ノーマルモードで動作する。

入力・出力・画面例

```
Manager > enable udld port=1-5

Operation successful.
```

例

■ポート 1〜5 の UDLD 機能を有効にする

```
ENABLE UDLD PORT=1-5
```

関連コマンド

DISABLE UDLD（80 ページ）
SHOW UDLD（171 ページ）

PURGE DHCPSNOOPING

カテゴリー：スイッチング

PURGE DHCPSNOOPING

解説

DHCP Snooping の設定情報、動作情報をすべて削除し、機能を無効にする。

入力・出力・画面例

```
Manager > purge dhcpsnooping

Operation successful.
```

例

■DHCP Snooping の情報を削除し、機能を無効にする

```
PURGE DHCPSNOOPING
```

関連コマンド

DELETE DHCPSNOOPING（56 ページ）
DISABLE DHCPSNOOPING（63 ページ）
ENABLE DHCPSNOOPING（81 ページ）

PURGE EPSR

カテゴリー：スイッチング

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無効にする
・該当 VLAN のリング接続用ポートからケーブルを抜く

入力・出力・画面例

```
Manager > purge epsr

 Operation successful.
```

例

■EPSR の設定をデフォルト状態に戻す

```
PURGE EPSR
```

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（52 ページ）
SHOW EPSR（139 ページ）

RESET DHCPSNOOPING COUNTER

カテゴリー：スイッチング

RESET DHCPSNOOPING COUNTER

解説

DHCP Snooping の統計情報をリセットする。

入力・出力・画面例

```
Manager > reset dhcpsnooping counter

Operation successful.
```

例

■DHCPSnooping のカウンターをリセットする

```
RESET DHCPSNOOPING COUNTER
```

関連コマンド

SHOW DHCPSNOOPING COUNTER（130 ページ）

RESET DHCPSNOOPING DATABASE

カテゴリー：スイッチング

RESET DHCPSNOOPING DATABASE [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のダイナミックエントリーを DHCP Snooping テーブル（バインディングデータベース）から削除する。

パラメーター

PORT　ポート番号。 複数指定が可能。ALL を指定した場合はすべてのポートが対象となる

入力・出力・画面例

```
Manager > reset dhcpsnooping database port=1-2

Operation successful.
```

例

■Port1,2 のダイナミックエントリー (dhcpsnooping) をバイディングデータベースから削除する

```
RESET DHCPSNOOPING DATABASE PORT=1-2
```

関連コマンド

DISABLE DHCPSNOOPING（63 ページ）
ENABLE DHCPSNOOPING（81 ページ）

RESET SWITCH

カテゴリー：スイッチング

RESET SWITCH [COUNTER]

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

パラメーター

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

入力・出力・画面例

```
Manager > reset switch

 Operation successful.
```

例

■スイッチングモジュールをリセットする

```
RESET SWITCH
```

関連コマンド

SHOW SWITCH（144 ページ）

RESET SWITCH LOOPDETECTION COUNTER

カテゴリー：スイッチング

RESET SWITCH LOOPDETECTION [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

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

入力・出力・画面例

```
Manager > reset switch loopdetection port=2 counter

Operation successful.
```

例

■ポート 2 の LDF 検出機能のカウンターをリセットする

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

関連コマンド

DISABLE SWITCH LOOPDETECTION（71 ページ）
ENABLE SWITCH LOOPDETECTION（89 ページ）
SET SWITCH LOOPDETECTION（116 ページ）
SHOW SWITCH LOOPDETECTION（147 ページ）

RESET SWITCH PORT

カテゴリー：スイッチング

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

スイッチポートをリセットする。リセットを実行すると、オートネゴシエーションプロセスを開始し、ポートの統計カウンターをクリアする

パラメーター

PORT　対象となるスイッチポート番号または ALL。ALL を指定した場合はすべてのスイッチポートが対象となる

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

入力・出力・画面例

```
Manager > reset switch port=1 counter

 Operation successful.
```

例

■ポート 1 のカウンターをリセットする

```
RESET SWITCH PORT=1 COUNTER
```

備考・注意事項

COUNTER オプションを指定せず実行すると、ポートがハードウェア的にリセットされてしまうため注意が必要。

関連コマンド

ACTIVATE SWITCH PORT AUTONEGOTIATE（43 ページ）
DISABLE SWITCH PORT（73 ページ）
ENABLE SWITCH PORT（92 ページ）

SET SWITCH PORT（120 ページ）
SHOW SWITCH PORT（153 ページ）

RESET SWITCH STORMDETECTION PORT COUNTER

カテゴリー：スイッチング

RESET SWITCH STORMDETECTION [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

受信レート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

入力・出力・画面例

```
Manager > reset switch stormdetection port=2 counter

Operation successful.
```

例

■ポート 2 の受信レート検出機能のカウンター情報をリセットする

```
RESET SWITCH STORMDETECTION PORT=2 COUNTER
```

関連コマンド

DISABLE SWITCH STORMDETECTION（79 ページ）
ENABLE SWITCH STORMDETECTION（96 ページ）
SET SWITCH STORMDETECTION（124 ページ）
SHOW SWITCH STORMDETECTION（163 ページ）

RESET UDLD

カテゴリー：スイッチング

RESET UDLD

解説

Unidirectional 検出によるポート閉塞状態を解除する。

入力・出力・画面例

```
Manager> reset udld

2 ports disabled by UDLD were reset
 Operation successful.
```

関連コマンド

DISABLE UDLD（80 ページ）
ENABLE UDLD（98 ページ）
SET UDLD（127 ページ）
SHOW UDLD（171 ページ）

SET DHCPSNOOPING CHECKINTERVAL

カテゴリー：スイッチング

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。デフォルトは 60 秒。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）。
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 NVS（Non-Volatile Storage）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 NVS からクライアント情報を読み込み、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。

パラメーター

CHECKINTERVAL　チェック間隔（秒）。デフォルトは 60 秒。

入力・出力・画面例

```
Manager > set dhcpsnooping checkinterval=40

Operation successful.
```

例

■チェック間隔を 40 秒に変更する

```
SET DHCPSNOOPING CHECKINTERVAL=40
```

備考・注意事項

スタティックエントリーは NVS（Non-Volatile Storage）に書き込まない。

関連コマンド

DISABLE DHCPSNOOPING（63 ページ）
ENABLE DHCPSNOOPING（81 ページ）
SHOW DHCPSNOOPING（128 ページ）

SET DHCPSNOOPING CHECKOPTION

カテゴリー：スイッチング

SET DHCPSNOOPING CHECKOPTION={**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設定する。

パラメーター

CHECKOPTION　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。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。

入力・出力・画面例

```
Manager > set dhcpsnooping checkoption=linkdown

Operation successful.
```

例

■Linkdown を検出したらリース満了以外のダイナミックエントリーを削除する

```
SET DHCPSNOOPING CHECKOPTION=LINKDOWN
```

備考・注意事項

リース満了以外のダイナミックエントリーの削除条件によって削除されたとき、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（SET DHCPSNOOPING CHECKINTERVAL コマンドで設定）でのチェックを待たずに、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 NVS（Non-Volatile Storage）に書き込む。

SET DHCPSNOOPING MACFILTER

カテゴリー：スイッチング

SET DHCPSNOOPING MACFILTER=*1..999* [ADDRESS={*macadd*|ANY}] [MASK=*macadd*] [VLAN={*vlan-name*|*1..4094*|ANY}] [PORT={*port-list*|ALL|NONE}] [ACTION={DENY|PERMIT}]

macadd: MAC アドレス（xx:xx:xx:xx:xx:xx の形式）
vlan-name: VLAN 名
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

MAC アドレスフィルタリングエントリーの設定を変更する。

パラメーター

MACFILTER　設定変更するエントリーの ID。
ADDRESS　フィルタリング対象装置の MAC アドレス
MASK　フィルタリング対象装置の MAC アドレスへのマスクを指定する
VLAN　入力 VLAN 名または VID
PORT　MAC アドレスフィルタリングを割り当てるポートを指定する
ACTION　条件に一致したときのアクション。PERMIT（許可）、DENY（破棄）から選択する。

入力・出力・画面例

```
Manager > set dhcpsnooping macfilter=2 address=00-44-56-77-88-00 mask=ff-ff-ff-
ff-ff-ff

Operation successful.
```

例

■MAC フィルターエントリー 2 の設定を変更する

```
SET DHCPSNOOPING MACFILTER=2 ADDRESS=00-44-56-77-88-00
  mask=ff-ff-ff-ff-ff-ff
```

関連コマンド

CREATE DHCPSNOOPING MACFILTER（50 ページ）

DESTROY DHCPSNOOPING MACFILTER（60 ページ）
SHOW DHCPSNOOPING MACFILTER（135 ページ）

SET DHCPSNOOPING PORT

カテゴリー：スイッチング

SET DHCPSNOOPING PORT={***port-list***|**ALL**} [MAXLEASES=*0..5*]
[SUBSCRIBERID={*string*|NONE}] [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 (1〜50 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　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。

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。最大は 5。

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。本パラメーターに NONE 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 NONE（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)。

入力・出力・画面例

```
Manager > set dhcpsnooping port=4 trusted=true

Operation successful.
```

例

■ポート 4 を TrustedPort にする

```
SET DHCPSNOOPING PORT=4 TRUSTED=TRUE
```

備考・注意事項

Trusted ポートに指定されるポートには、スタティックおよびダイナミックエントリーが登録されていてはならない。登録されたポートを Trusted ポートに設定しようとするとコマンドエラーになる。
DHCP サーバーが繋がるポートは Trusted ポートに指定しなければならない。Untrusted ポートに繋がれた DHCP サーバーから IP アドレスを取得することはできない。
トランクグループに所属しているポートは、Untrusted ポートにはできない。

SET SWITCH LIMITATION

カテゴリー：スイッチング

SET SWITCH LIMITATION={**NONE**|***0..1024000***}

解説

パケットストームプロテクションで使用する受信上限値を Kbps（Kilobits per second）で指定する。デフォルトは 0 で、パケットストームプロテクション無効

パラメーター

LIMITATION　パケットストームプロテクションで使用する受信上限値を Kbps で指定。デフォルトは 0。
設定値はファームウェア内部で 64Kbps の倍数値に切り上げられ設定される。0 は NONE と同じ

入力・出力・画面例

```
Manager > set switch limitation=10240

 Operation successful.
```

例

■パケットストームプロテクションの受信上限値を 10240Kbps にする

```
SET SWITCH LIMITATION=10240
```

備考・注意事項

LDF 検出機能、または受信レート検出機能を有効にし、ポートのアクションが BCDISCARD に設定されたポートがある場合、本機能は有効にできない。
パケットストームプロテクションと受信レート検出を併用する場合、受信レートカウンターには、パケットストームプロテクションによって破棄されたパケットも計上される。

SET SWITCH LOOPDETECTION

カテゴリー：スイッチング

SET SWITCH LOOPDETECTION PORT={***port-list***|**ALL**} [ACTION={PORTDISABLE|LINKDOWN|BCDISCARD|NONE}] [INTERVAL={*1..1000000*}] [SECURE={ON|OFF}] [BLOCKTIMEOUT={*1..86400*|NONE}]

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

解説

LDF 検出機能のパラメーターを設定する

パラメーター

PORT　ポート番号または ALL を指定する

ACTION　LDF を検出した場合のアクション。NONE（何もしない（ログのみ））、PORTDISABLE（ポートを無効にする（物理的なリンクは保持する））、LINKDOWN（ポートを物理的にリンクダウンさせる）、BCDISCARD(ポートのブロードキャストフレームの受信を止める) から選択する。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アクション実行前の状態に戻る。デフォルトは PORTDISABLE

INTERVAL　LDF の送信間隔。単位は秒。デフォルト 120 秒

SECURE　セキュアな LDF の受信をするかどうか。ON の場合、LDF に含まれる ID コードのチェックを行い ID が異なる場合は LDF を破棄する。 ID コードは LDF の送信ごとに変更されるため、送出した LDF の有効時間は LDF の送出間隔 (INTERVAL) の時間となる。デフォルト ON

BLOCKTIMEOUT　ACTION パラメーターで指定した動作が実行された後、自動的に実行前の状態に戻るまでの時間。単位は秒。NONE を指定した場合、自動的に実行前の状態には戻らない。デフォルト 300 秒

入力・出力・画面例

```
Manager > set switch loopdetection port=2 action=linkdown inter-
val=60 blocktimeout=3600

 Operation successful.
```

例

■ポート 2 で LDF を受信した場合のアクションをリンクダウン、LDF の送信間隔を 60 秒、実行前の状態に戻るまでの時間を 3600 秒に設定する。

```
SET SWITCH LOOPDETECTION PORT=2 ACTION=LINKDOWN INTERVAL=60
  BLOCKTIMEOUT=3600
```

備考・注意事項

トランクポートに対して LDF 検出機能を有効に設定する場合は、アクションには LINKDOWN を指定することを推奨。
LDF 検出が有効かつパケットストームプロテクションが有効に設定されたポートが存在する場合、LDF 検出時のアクションに BCDISCARD を指定することはできない。
LDF 検出時のアクションを LINKDOWN に指定する場合は、INTERVAL オプションは 1 以上、BLOCKTIMEOUT オプションは 60 以上の値を推奨
次の条件によりアクション実行前の状態に戻すことができる。
・ENABLE SWITCH PORT コマンド/DISABLE SWITCH PORT コマンド実行時
・リンクダウン発生時
・PORTOFF モードのパワーセーブトリガー起動/終了時
・ポートセキュリティーの DISABLE アクション実行/解除時

関連コマンド

DISABLE SWITCH LOOPDETECTION（71 ページ）
ENABLE SWITCH LOOPDETECTION（89 ページ）
RESET SWITCH LOOPDETECTION COUNTER（104 ページ）
SHOW SWITCH LOOPDETECTION（147 ページ）

SET SWITCH MIRROR

カテゴリー：スイッチング

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

port-number: スイッチポート番号（1〜。単一ポートのみ指定可）

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の指定は、SET SWITCH PORT コマンドの MIRROR パラメーターで行う

パラメーター

MIRROR　ミラーポートとして使用するポート。NONE を指定するとミラーポートの設定は削除され、ポートミラーリング機能は無効となる。タグ付きポートは指定できない

入力・出力・画面例

```
Manager > set switch mirror=1

 Operation successful.
```

例

■ポート 1 をミラーポートに設定する

```
SET SWITCH MIRROR=1
```

備考・注意事項

VLAN default 以外に所属しているポート、タグ付きポート、ポートセキュリティーが有効なポート、ポート認証の Authenticator ポートと Supplicant 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。
ミラーポートに設定したポートでは、ポートミラーリング機能が無効でも他のポートとの通信ができない（スイッチポートとして機能しない）。
ソースポートの受信パケットをミラーする場合（SET SWITCH PORT コマンドの MIRROR パラメーターに RX または、BOTH を指定）に、ソースポートがタグなしパケットを受信した場合のみ、タグなしでミ

ラーされる。それ以外はタグ付きパケットとしてミラーされる。
ミラーポートではスパニングツリープロトコルを有効にすることはできない。

関連コマンド

DISABLE SWITCH MIRROR（72 ページ）
ENABLE SWITCH MIRROR（91 ページ）
SHOW SWITCH MIRROR（152 ページ）

SET SWITCH PORT

カテゴリー：スイッチング

SET SWITCH PORT={***port-list***|**ALL**} [ACCEPTABLE={ALL|VLAN}]
[DESCRIPTION=*string*] [MIRROR={BOTH|NONE|RX|TX}] [PRIORITY=*priority*]
[SPEED={AUTONEGOTIATE|10MHALF|10MFULL|100MHALF|100MFULL|10MHAUTO|
10MFAUTO|100MHAUTO|100MFAUTO|*10*-100MAUTO|1000MFULL}]
[SECURITYMODE={AUTOMATIC|DYNAMIC|LIMITED|SECURED}] [LEARN=*0..256*]
[INTRUSIONACTION={DISCARD|DISABLE|LOG|TRAP}] [POLARITY={MDI|MDIX}]
[BCLIMIT={ON|OFF}] [DLFLIMIT={ON|OFF}] [MCLIMIT={ON|OFF}]

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）
string: ポート名称。SHOW SWITCH PORT コマンドなどで表示されるもので、メモ的に使用する。20 文字までの半角英数字、およびシャープ [#]、パーセント [%]、クエスチョン [?]、円マーク [\] を除く半角記号で入力する。空白を含む場合はダブルクォート ["] で囲み指定する。消去する場合は 2 つのダブルクォートを指定するか何も指定しない
priority: ユーザープライオリティー値（0〜7）

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、通信モード、受信フレームタイプ（VLAN タグあり・なし）、セキュリティーモードの設定を行う

パラメーター

PORT　対象となるスイッチポート番号または ALL。ALL を指定した場合はすべてのスイッチポートが対象となる

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）または、ALL（すべて）を選択する。タグなし VLAN 所属ポートのデフォルトは ALL。タグ VLAN にしか所属していないポートでは、自動的に本パラメーターが VLAN に設定され変更できない

DESCRIPTION　ポート名称。SHOW SWITCH PORT コマンドなどで表示されるもので、メモ的に使用する

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。複数ポートに指定可能。ただし、トラフィックの向きをポート単位で設定することはできない。

PRIORITY　ユーザープライオリティー値 (0〜7) を指定する。デフォルトは 0

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。AUTONEGOTIATE を指定した場合、自動

的に MDI/MDI-X 自動認識が有効になる。固定 SPEED 設定時は MDI/MDI-X 自動認識が無効となる。1000MFULL 設定時、1000BASE-T ポートでは AUTONEGOTIATE 有効で Speed を 1000M、Duplex を Full Duplex 固定にする。1000MFULL 設定時、SFP ポートでは AUTONEGOTIATE 無効で 1000MFULL 固定とする。1000BASE-T モジュールを使用している SFP ポートでは、1000MFULL 設定は未サポート。100M SFP は、100MFULL 固定のみをサポートし、Autonego はサポートしない

SECURITYMODE　指定ポートのセキュリティーモードを設定。SECURED（Secure モード）、DYNAMIC（Dynamic Limited モード）、AUTOMATIC（セキュリティーモード解除）、LIMITED（Limited モード）から選択する。デフォルトは AUTOMATIC。Secured モードでは、FDB の学習機能を停止し、選択した時点での学習済 MAC アドレスをスタティック登録する。それ以降に受信した未登録の MAC アドレスを持つパケットは不正パケットとして破棄する。不正パケット検出時のアクションは、INTRUSIONACTION パラメーターにて指定。CREATE CONFIG コマンドでポートセキュリティーの設定（セキュリティーモードに関する設定）を保存後は、スタティック登録された MAC アドレスは、エージング機能や設定保存後のシステムのリセットによって削除されない。これを MAC アドレステーブルから削除する場合は、一度、Secured モード以外を選択するか、DELETE SWITCH FILTER コマンドを実行する。本モード選択前に、既にスタティックエントリーが登録されていてる場合は、エントリーは削除されずに引き継がれる。Dynamic Limited モードでは、学習済み MAC アドレス数が LEARN パラメーターで指定した学習可能な送信元 MAC アドレス（ダイナミックエントリー）の最大数の制限値に達している状態で未学習の送信元 MAC アドレスを持つパケットを受信すると破棄される。不正パケット検出時のアクションは、INTRUSIONACTION パラメーターにて DISCARD のみ指定可能。SECURITYMODE=DYNAMIC 指定時は LEARN パラメーターの指定が必須。本モード選択前にスタティックエントリーが登録されているポートは本モードに選択できない。DELETE SWITCH FILTER コマンドを実施して削除する必要がある。Limited モードでは、学習済み MAC アドレス数が LEARN パラメーターで指定した学習可能な送信元 MAC アドレス（スタティックエントリー）の最大数の制限値に達している状態で未学習の送信元 MAC アドレスを持つパケットを受信すると破棄される。不正パケット検出時のアクションは、INTRUSIONACTION パラメーターにて指定。SECURITYMODE=LIMITED 指定時は LEARN パラメーターの指定が必須。本モード選択前に、既にスタティックエントリーが登録されていてる場合は、エントリーは削除されずに引き継がれる。スタティックエントリーは、最大数の制限値には含まれない。Automatic モードでは、ポートセキュリティーは解除される。本モード以外から、Automatic モードに変更した場合は該当ポートのダイナミック、スタティックエントリーすべてが削除される。

LEARN　該当ポートで学習可能な送信元 MAC アドレスの最大数。設定可能な最大数は、1 ポートでは 256 まで、システム全体では 5120 まで。セキュリティーモードが、Dynamic Limited モード、Limited モードの時のみ制御対象となる。SECURITYMODE パラメーターを指定しないで、本パラメーターに 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し、自動的に Secure モードに変更される。0 以外の値を指定した場合は、SECURITYMODE パラメーターは省略可能（省略した場合は、Dynamic Limited モードを設定したことになる）

INTRUSIONACTION　SECURITYMODE パラメーターで、LIMITED または SECURED 指定時に、不正パケット受信時の動作を設定する。デフォルトは DISCARD。DISCARD（不正パケットを破棄）、DISABLE（不正パケットを破棄し、SNMP トラップを送信して、ポートを DISABLE にする。DISABLE の解除は、SECURITYMODE パラメーターで AUTOMATIC を指定し、ポートセキュリティーを解除することで可能）、LOG（不正パケットを破棄し、不正パケット送信元の MAC アドレス、VID、ポート番号を LOG LEVEL=4(NOTICE) としてログに保存する。SYSLOG 設定がある場

合は、SYSLOG に送信する。2回目以降、送信元が同一な場合はログに記録しない)、TRAP（不正パケットを破棄し、不正パケット送信元の MAC アドレス、VID、ポート番号を SNMP トラップとして送信する。別途、送信設定が必要）のいずれか

POLARITY　MDI/MDI-X 自動認識を無効にしたときの MDI/MDI-X を指定する。デフォルトは MDI-X。SFP ポートでは、MDI/MDI-X の設定を変更することはできない

BCLIMIT　ブロードキャスト MAC アドレスに対するパケットストームプロテクションの有効/無効を設定する。デフォルトは無効。

DLFLIMIT　未学習のユニキャスト MAC アドレスに対するパケットストームプロテクションの有効/無効を設定する。デフォルトは無効。

MCLIMIT　マルチキャスト MAC アドレスに対するパケットストームプロテクションの有効/無効を設定する。デフォルトは無効。

入力・出力・画面例

```
Manager > set switch port=1 speed=100mhalf

 Operation successful.
```

例

■ポート 1 の通信モードを 100MHALF に固定する

```
SET SWITCH PORT=1 SPEED=100MHALF
```

備考・注意事項

ポートセキュリティーが有効なポートはミラーポート、ポート認証の Authenticator ポートに設定することはできない。また、トランクグループに所属させることもできない。
ポートセキュリティーが有効なポートではスパニングツリープロトコルは併用できない。
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。
本コマンドの SPEED パラメーターで、10M または 100M 固定スピード（10MHALF、10MFULL、100MHALF、100MFULL）を設定した場合、MDI/MDI-X 自動認識は無効になる（有効には変更できない)。また、オートネゴシエーション（AUTONEGOTIATE、10MHAUTO、10MFAUTO、100MHAUTO、100MFAUTO）または、1000MFULL を設定した場合は、MDI/MDI-X 自動認識は有効になる（無効にも変更できる)。
ポートの MDI/MDI-X の設定は、MDI/MDI-X 自動認識が無効のときに有効になる。
LDF 検出機能、または受信レート検出機能を有効にし、ポートのアクションが BCDISCARD に設定されたポートがある場合、BCLIMIT、DLFLIMIT、MCLIMIT を ON に設定することはできない。
ADD SWITCH FILTER コマンドで指定していないマルチキャスト MAC アドレスは、未学習のユニキャスト MAC アドレスに対するパケットストームプロテクションの対象となる。

予約済みのマルチキャスト MAC アドレス（01-80-c2-00-00-00～01-80-c2-00-00-2f）は、パケットストームプロテクションの対象にならない。
INTRUSIONACTION パラメーターで DISABLE 指定時、ポートが DISABLE になった状態で、設定を保存すると、再起動時もポートの DISABLE 状態は引き継がれる。ただし、再起動後の DISABLE 状態は、DISABLE SWITCH PORT コマンド実行時と同一で、ENABLE SWITCH PORT コマンドで有効化が可能。
INTRUSIONACTION パラメーターで LOG 指定時、ログに記録できる件数は、1 ポートあたり 150 件まで。150 件を超えた場合は INTRUSIONACTION=DISCARD と同様の動作でパケットが破棄されるのみ。
INTRUSIONACTION パラメーターで TRAP 指定時、2 回目以降、送信元が同一な場合はトラップを送信しない。トラップを発行する回数は、1 ポートあたり 150 件まで。150 件を超えた場合 INTRUSIONACTION=DISCARD と同様の動作でパケットが破棄されるのみ。
アクションに TRAP 指定時、10 ポート以上のポートで同時に大量の不正パケットの検出した場合、不正検出処理の輻輳状態が発生する。このとき、450 件以上の検出をロスする場合がある。検出処理の輻輳状態が回復すると、通常通り 1 ポートあたり 150 件の最大数まで検出と通知ができる。
150 件までの不正検出アドレスは、装置起動中保持される。ただし、再起動、または、次の設定変更（ポート単位）によって不正検出アドレスはリセットされる。
・LIMITED モード時は、LEARN 数の変更
・INTRUSIONACTION パラメーターの設定変更
・SECURITYMODE パラメーターの設定変更
・所属 VLAN の変更
ミラーリングできるトラフィックの向きは 1 つの機器につき 1 つのパラメーターしか設定できない。
PAUSE フレームもミラーリングの対象になる。
セキュリティーモードを Limited に設定したポートでは、本体宛通信の受信レートがチェックされるため、FDB 学習に時間がかかる。
100M SFP ポートは、トランクグループに所属させることができない。

関連コマンド

ACTIVATE SWITCH PORT AUTONEGOTIATE（43 ページ）
DISABLE SWITCH PORT（73 ページ）
ENABLE SWITCH PORT（92 ページ）
RESET SWITCH PORT（105 ページ）
SHOW SWITCH PORT（153 ページ）

SET SWITCH STORMDETECTION

カテゴリー：スイッチング

SET SWITCH STORMDETECTION PORT={***port-list***|**ALL**}
[LOWRATEACTION={PORTDISABLE|LINKDOWN|BCDISCARD|NONE}]
[HIGHRATEACTION={PORTDISABLE|LINKDOWN|BCDISCARD|NONE}]
[LOWRATETHRESHOLD={*1..1023999*}] [HIGHRATETHRESHOLD={*2..1024000*}]
[BLOCKTIMEOUT={*1..86400*|NONE}] [FRAMETYPE={BROADCAST|MULTICAST|ALL}]
[FRAMESIZE={*64....1522*|AUTO]

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

解説

受信レート検出機能のパラメーターを設定する

パラメーター

PORT　ポート番号または ALL を指定する

HIGHRATEACTION　該当スイッチポートで受信レートが高レートのしきい値 (HIGHRATETHRESHOLD の値) を超えた場合のアクション。NONE（何もしない（ログのみ））、PORTDISABLE（ポートを無効にする（物理的なリンクは保持する））、LINKDOWN（ポートを物理的にリンクダウンさせる）、BCDISCARD(ポートのブロードキャストフレームの受信を止める) から選択する。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アクション実行前の状態に戻る。デフォルトは PORTDISABLE。また、該当ポートの受信レート検出機能が有効かつパケットストームプロテクションを有効にしたポートが存在する場合は BCDISCARD は設定できない。LOWRATEACTION の指定した値以下の値は設定できない

LOWRATEACTION　該当スイッチポートで受信レートが低レートのしきい値 (LOWTRATETHRESHOLD の値) を超えた場合のアクション。NONE（何もしない（ログのみ））、PORTDISABLE（ポートを無効にする（物理的なリンクは保持する））、LINKDOWN（ポートを物理的にリンクダウンさせる）、BCDISCARD(ポートのブロードキャストフレームの受信を止める) から選択する。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アクション実行前の状態に戻る。 ただし、HIGHRATEACTION と同様の条件でもアクション実行前の状態に戻る。デフォルトは NONE。また、該当ポートの受信レート検出機能が有効かつパケットストームプロテクションを有効にしたポートが存在する場合は BCDISCARD は設定できない。HIGHRATEACTION で指定した値以上の値は設定できない

HIGHRATETHRESHOLD　受信レートが高レート時のしきい値を Kbps (Kilobits per second) で指定する。LOWRATETHRESHOLD 以下の値はエラーとなる。デフォルトは 819200(800Mbps)

LOWRATETHRESHOLD　受信レートが低レート時のしきい値を Kbps (Kilobits per second) で指定する。HIGHRATETHRESHOLD より大きい値はエラーとなる。デフォルトは 512000(500Mbps)

BLOCKTIMEOUT　HIGHRATEACTION または LOWRATEACTION パラメーターで指定した動作が

実行された後、自動的に実行前の状態に戻るまでの時間。単位は秒。NONE を指定した場合、自動的に実行前の状態には戻らない。デフォルト 300 秒

FRAMETYPE　受信レートの対象となるフレームの種類。 BROADCAST を指定した場合ブロードキャストフレームが、MULTICAST を指定した場合マルチキャストフレームが、ALL を指定した場合全ての受信フレームがそれぞれ受信レートの対象となる。デフォルトは ALL

FRAMESIZE　受信対象フレームの平均フレームサイズを指定する。本パラメーターで指定したフレームサイズと受信レートの対象フレームの pps(Packet per seconds) から受信レートを算出する。FRAMETYPE に BROADCAST もしくは MULTICAST を指定した場合のみ、本パラメーターが有効となる。AUTO を指定した場合、全ての受信フレームのフレームサイズから自動的に決定される。デフォルトは AUTO

入力・出力・画面例

```
Manager > set switch stormdetection port=2 highratethresh-
old=1024000 highrateaction=bcdiscard

 Operation successful.
```

備考・注意事項

トランクポートに対して受信レート検出機能を有効に設定する場合は、高レート時/低レート時のアクションには LINKDOWN を指定することを推奨。
ポート認証を併用する場合、アクションには PORTDISABLE または LINKDOWN を指定することを推奨。
受信レート検出が有効かつパケットストームプロテクションを有効に設定されたポートが存在する場合、高レート時/低レート時のアクションに BCDISCARD を指定することはできない。
パケットストームプロテクションと受信レート検出を併用する場合、受信レートカウンターには、パケットストームプロテクションによって破棄されたパケットも計上される。
次の条件によりアクション実行前の状態に戻すことができる。
・ENABLE SWITCH PORT コマンド/DISABLE SWITCH PORT コマンド実行時
・リンクダウン発生時
・PORTOFF モードのパワーセーブトリガー起動/終了時
・ポートセキュリティーの DISABLE アクション実行/解除時

関連コマンド

DISABLE SWITCH STORMDETECTION（79 ページ）
ENABLE SWITCH STORMDETECTION（96 ページ）
RESET SWITCH STORMDETECTION PORT COUNTER（107 ページ）
SHOW SWITCH STORMDETECTION（163 ページ）

SET SWITCH TRUNK

カテゴリー：スイッチング

SET SWITCH TRUNK=*trunk* SPEED={**1000M**|**100M**|**10M**}

trunk: トランクグループ名

解説

トランクグループの設定を変更する

パラメーター

TRUNK　トランクグループ名

SPEED　トランクポートの通信速度。トランクグループに参加したポートは、ここで指定した速度となる。デフォルトは 1000M。SFP ポートは 1000M のみ指定可能。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

入力・出力・画面例

```
Manager > set switch trunk=uplink speed=1000m

 Operation successful.
```

例

■トランクグループ「uplink」の通信速度を 1000M へ変更する

```
SET SWITCH TRUNK=uplink SPEED=1000M
```

関連コマンド

ADD SWITCH TRUNK（48 ページ）
CREATE SWITCH TRUNK（54 ページ）
DELETE SWITCH TRUNK（59 ページ）
DESTROY SWITCH TRUNK（62 ページ）
SHOW SWITCH TRUNK（169 ページ）

SET UDLD

カテゴリー：スイッチング

SET UDLD [MESSAGETIME=*7..90*] [DISABLETIME={*30..86400*|NONE}]

解説

UDLD の各種タイマーの設定を変更する。

パラメーター

MESSAGETIME　UDLD プローブメッセージの送信間隔（秒）。デフォルトは 15 秒。

DISABLETIME　Unidirectional 検出によるポート閉塞の持続時間 (秒)。NONE は無制限を示す。デフォルトは NONE。

入力・出力・画面例

```
Manager > set udld disabletime=60

Operation successful.
```

例

■Unidirectional 検出によるポート閉塞の持続時間を変更する。

```
SET UDLD DISABLETIME=60
```

関連コマンド

DISABLE UDLD（80 ページ）
ENABLE UDLD（98 ページ）
RESET UDLD（108 ページ）
SHOW UDLD（171 ページ）

SHOW DHCPSNOOPING

カテゴリー：スイッチング

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
  Logging enabled .......... None

DHCP Snooping Database:
  Full Leases/Max Leases ... 2/260
  Check Interval ........... 60 seconds
  Check Options ............ None
------------------------------------------------------------------------------
```

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 セキュリティーの有効・無効
Logging enabled	ログ機能の有効・無効。無効時は None、有効時はログへの記録対象イベント（現時点では ARP セキュリティー のみ）が表示される
Full Leases/Max	LeasesDHCP 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 8:

例

■設定情報を表示する

```
SHOW DHCPSNOOPING
```

関連コマンド

ADD DHCPSNOOPING（44 ページ）
DELETE DHCPSNOOPING（56 ページ）
DISABLE DHCPSNOOPING（63 ページ）
ENABLE DHCPSNOOPING（81 ページ）

SHOW DHCPSNOOPING COUNTER

カテゴリー：スイッチング

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 9:

例

■DHCP Snooping の統計情報を表示する

```
SHOW DHCPSNOOPING COUNTER
```

関連コマンド

ENABLE DHCPSNOOPING（81 ページ）
ENABLE DHCPSNOOPING ARPSECURITY（82 ページ）

SHOW DHCPSNOOPING DATABASE

カテゴリー：スイッチング

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 ... 2/24
Check Interval ........... 60 seconds
Check Options ............ None

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）
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 IP 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	ハードウェアフィルターテーブルに登録でき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)。スタティックエントリーは Static。
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	未サポート
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)、Nvs（DHCP Snooping が有効化されたときに NVS からロードしたエントリー)

表 10:

例

■DHCP Snooping テーブルの内容を表示する

```
SHOW DHCPSNOOPING DATABASE
```

関連コマンド

DISABLE DHCPSNOOPING（63 ページ）
ENABLE DHCPSNOOPING（81 ページ）

SHOW DHCPSNOOPING MACFILTER

カテゴリー：スイッチング

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

id-list: フィルター番号（1〜999。ハイフン、カンマを使った複数指定も可能）
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

MAC アドレスフィルタリングの設定情報を表示する。

パラメーター

MACFILTER　エントリーの ID。複数指定が可能。省略時および ALL を指定した場合はすべてのエントリーが対象となる。
PORT　ポート番号。複数指定が可能。ALL を指定した場合はすべてのポートが対象となる。

入力・出力・画面例

```
Manager > show dhcpsnooping macfilter

DHCP Snooping MAC Filter ( 3 entries )
--------------------------------------------------------------------------------

Filter ID ................ 1
MAC Address .............. 00-09-41-00-00-00
MAC Address Mask ......... ff-ff-ff-00-00-00
Port ..................... ALL
Action ................... Permit
Is Active ................ Yes

Filter ID ................ 2
MAC Address .............. 00-1a-eb-00-00-00
MAC Address Mask ......... ff-ff-ff-00-00-00
Port ..................... ALL
Action ................... Permit
Is Active ................ Yes

Filter ID ................ 3
Port ..................... ALL
Action ................... Deny
Is Active ................ Yes

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

Filter ID	エントリーの ID
MAC Address DHCP Snooping	対象装置の MAC アドレス。ADDRESS が設定されている場合に表示される
MAC Address Mask DHCP Snooping	対象装置の MAC アドレスへのマスク。MASK が設定されている場合に表示される
VLAN ID	入力 VLAN の ID。VLAN が設定されている場合に表示される
Port	エントリーが割り当てられているポート
Action	条件に一致したときのアクション。Permit または Deny
Is Active	エントリーがポートに割り当てられている（Yes）、またはいない（No）

表 11:

例

■MAC アドレスフィルタリングの設定情報を表示する

```
SHOW DHCPSNOOPING MACFILTER
```

備考・注意事項

エントリーの ID とポート番号を同時に指定することはできない。いずれか片方だけを指定すること。

関連コマンド

CREATE DHCPSNOOPING MACFILTER（50 ページ）
DESTROY DHCPSNOOPING MACFILTER（60 ページ）
SET DHCPSNOOPING MACFILTER（111 ページ）

SHOW DHCPSNOOPING PORT

カテゴリー：スイッチング

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　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。

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 ............ None

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

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。設定されていない場合は None と表示される

表 12:

例

■設定情報を表示する

```
SHOW DHCPSNOOPING PORT=11
```

関連コマンド

DISABLE DHCPSNOOPING（63 ページ）
ENABLE DHCPSNOOPING（81 ページ）
SET DHCPSNOOPING PORT（113 ページ）

SHOW EPSR

カテゴリー：スイッチング

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

epsrname: EPSR ドメイン名（1〜15 文字。英数字とハイフン [-]、アンダーバー [_]、ピリオド [.]、開始丸かっこ [(]、終了丸かっこ [)] が使用可能。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 ........................ blue
 Mode ........................ AWARE
 Status ...................... Enabled
 State ....................... Links-Up
 Delete Multicast Entry ........ Disabled
 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）または Transit（トランジットノード）
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
Delete Multicast Entry	トポロジーチェンジ発生時に FDB からのマルチキャストアドレスエントリーを削除する機能の有効・無効
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。トランクポートの場合はトランクグループ名
First Port Status	リングを構成する第 1 ポートの状態。Aware の場合は Up/Down/Unknown のいずれか。Transit の場合は、Unknown/Forwarding/Down/Blocking のいずれか。Unknown は EPSR ドメインが無効に設定されていることを示す
First Port Direction	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。トランクポートの場合はトランクグループ名
Second Port Status	リングを構成する第 2 ポートの状態。Aware の場合は Up/Down/Unknown のいずれか。Transit の場合は、Unknown/Forwarding/Down/Blocking のいずれか。Unknown は EPSR ドメインが無効に設定されていることを示す
Second Port Direction	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 13:

例

■EPSR ドメインの情報を表示する

```
SHOW EPSR
```

関連コマンド

ADD EPSR DATAVLAN（46 ページ）
CREATE EPSR（52 ページ）
CREATE VLAN（「バーチャル LAN」の 14 ページ）
ENABLE EPSR（85 ページ）

SHOW EPSR COUNTER（142 ページ）

SHOW EPSR COUNTER

カテゴリー：スイッチング

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

epsrname: EPSR ドメイン名（1〜15 文字。英数字とハイフン [-]、アンダーバー [_]、ピリオド [.]、開始丸かっこ [(]、終了丸かっこ [)] が使用可能。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 14:

例

■すべての EPSR ドメインの統計カウンターを表示する

```
SHOW EPSR COUNTER
```

関連コマンド

SHOW EPSR（139 ページ）

SHOW SWITCH

カテゴリー：スイッチング

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。Ctrl+C でスクロールを中止できる

入力・出力・画面例

```
Manager > show switch

Switch Configuration
-----------------------------------------------
 Switch Address ............ 00-00-F4-27-14-65
 Ageingtimer ............... On
 Number of Fixed Ports ..... 52
 Mirroring ................. Disabled
 Mirror port ............... None
 Ports mirroring on Rx ..... None
 Ports mirroring on Tx ..... None
 Ports mirroring on Both ... None
 BPDU Forwarding ........... Disabled
 EAP Forwarding ............ Disabled
 Powersaving ............... Disabled
 Ageingtime ................ 300
 UpTime .................... 04:59:27
-----------------------------------------------
```

Switch Address	本製品の MAC アドレス
Ageingtimer	フォワーディングデータベースのエージングタイマーの状態。機能している（On）または機能していない（Off）
Number of Fixed Ports	固定イーサネットポートの数
Mirroring	ポートミラーリング機能の状態。有効（Enabled）または無効（Disabled）
Mirror port	ミラーポート
Ports mirroring on Rx	受信パケットだけをミラーリングしているソースポート
Ports mirroring on Tx	送信パケットだけをミラーリングしているソースポート
Ports mirroring on Both	送受信両方のパケットをミラーリングしているソースポート
BPDU Forwarding	BPDU 透過機能の状態。有効（Enabled）または無効（Disabled）
EAP Forwarding	EAP 透過機能の状態。有効（Enabled）または無効（Disabled）
Powersaving	省電力モードの状態。有効（Enabled）または無効（Disabled）

Ageingtime	フォワーディングデータベースのエージングタイム（秒）
UpTime	再起動後の経過時間 (時:分:秒の形式)。 MIB-II オブジェクトの sysUpTime と同じ

表 15:

例

■スイッチングモジュールの全般的情報を表示する

```
SHOW SWITCH
```

関連コマンド

RESET SWITCH（103 ページ）

SHOW SWITCH COUNTER

カテゴリー：スイッチング

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
-----------------------------------------------
Receive                  Transmit
 packets   :          0    packets :          0
 errors    :          0    errors  :          0
-----------------------------------------------
```

Receive	受信パケットに関する統計
packets	スイッチチップから CPU に渡されたパケットの数
errors	スイッチチップで正常に受信されたが、エラーのため CPU で処理できなかったパケットの数
Transmit	送信パケットに関する統計
packets	CPU からスイッチチップに渡されたパケットの数
errors	エラーのために CPU で破棄されて送出できなかったパケットの数

表 16:

例

■スイッチングモジュールの統計カウンターを表示する

```
SHOW SWITCH COUNTER
```

関連コマンド

SHOW SWITCH PORT COUNTER（159 ページ）

SHOW SWITCH LOOPDETECTION

カテゴリー：スイッチング

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

LDF 検出機能の設定、状態、カウンターの情報を表示する。CONFIG、STATUS、COUNTER のいずれのパラメーターも指定しない場合、設定情報、状態、カウンター情報の順に、指定ポートのすべての情報が表示される

パラメーター

PORT　ポート番号または ALL を指定する。省略時は ALL
CONFIG　LDF 検出機能の設定情報を表示する
STATUS　LDF 検出機能の状態情報を表示する
COUNTER　LDF 検出機能のカウンター情報を表示する

入力・出力・画面例

```
Manager > show switch loopdetection port=1,2 config

Switch Loop Detection configuration
------------------------------------------------------------------------------
 Port ........................... 1
 Status ......................... Disabled
 Frame Action ................... PortDisable
 Frame Interval ................. 120 sec
 Secure Frame ................... On
 Blocking Timeout ............... 300 sec

 Port ........................... 2
 Status ......................... Enabled
 Frame Action ................... Linkdown
 Frame Interval ................. 1      (sec)
 Secure Frame ................... Off
 Blocking Timeout ............... 3600   (sec)

Manager > show switch loopdetection status

Switch Loop Detection Status
```

```
-------------------------------------------------------------------------------
Port Loop     Expiry Port Status    Link Status  B/C Status
-------------------------------------------------------------------------------
 1    Blocking 115    Disabled(Act)  Up          Discard
 2    Normal   --     Disabled(User) Up          Forward
 3    Detected 32     Enabled        Up          Forward
 4    Blocking 192    Disabled(Act)  Down(Act)   Forward
 5    --       --     Enabled        Down        Forward
 6    --       --     Enabled        Down        Forward
 7    --       --     Disabled(User) Down(User)  Forward
 8    --       --     Enabled        Down        Forward
 9    --       --     Enabled        Down        Forward
 10   --       --     Enabled        Down        Forward
 11   --       --     Enabled        Down        Forward
 12   --       --     Enabled        Down        Forward
 13   --       --     Enabled        Down        Forward
 14   --       --     Enabled        Down        Forward
 15   --       --     Enabled        Down        Forward
 16   --       --     Enabled        Down        Forward
 17   --       --     Enabled        Down        Forward
 18   --       --     Enabled        Down        Forward
 19   --       --     Enabled        Down        Forward
 20   --       --     Enabled        Down        Forward
 21   --       --     Enabled        Down        Forward
 22   --       --     Enabled        Down        Forward
 23   --       --     Enabled        Down        Forward
 24   --       --     Enabled        Down        Forward
 25   --       --     Enabled        Down        Forward
 26   --       --     Enabled        Down        Forward
 27   --       --     Enabled        Down        Forward
 28   --       --     Enabled        Down        Forward
 29   --       --     Enabled        Down        Forward
 30   --       --     Enabled        Down        Forward
 31   --       --     Enabled        Down        Forward
 32   --       --     Enabled        Down        Forward
 33   --       --     Enabled        Down        Forward
 34   --       --     Enabled        Down        Forward
 35   --       --     Enabled        Down        Forward
 36   --       --     Enabled        Down        Forward
 37   --       --     Enabled        Down        Forward
 38   --       --     Enabled        Down        Forward
 39   --       --     Enabled        Down        Forward
 40   --       --     Enabled        Down        Forward
 41   --       --     Enabled        Down        Forward
 42   --       --     Enabled        Down        Forward
 43   --       --     Enabled        Down        Forward
 44   --       --     Enabled        Down        Forward
 45   --       --     Enabled        Down        Forward
 46   --       --     Enabled        Down        Forward
 47   --       --     Enabled        Down        Forward
 48   --       --     Enabled        Down        Forward
```

```
 49   --       --     Enabled        Down        Forward
 50   --       --     Enabled        Down        Forward
 51   --       --     Enabled        Down        Forward
 52   --       --     Enabled        Down        Forward

Manager > show switch loopdetection counter

Switch Loop Detection Counter
-------------------------------------------------------------------------------
 Port Frame Tx       Frame Rx       Action          Frame Rx Discards
-------------------------------------------------------------------------------
 1    0              0              0               0
 2    67295          1              1               0
 3    0              0              0               0
 4    0              0              0               0
 5    0              0              0               0
 6    0              0              0               0
 7    0              0              0               0
 8    0              0              0               0
 9    0              0              0               0
 10   0              0              0               0
 11   0              0              0               0
 12   0              0              0               0
 13   0              0              0               0
 14   0              0              0               0
 15   0              0              0               0
 16   0              0              0               0
 17   0              0              0               0
 18   0              0              0               0
 19   0              0              0               0
 20   0              0              0               0
 21   0              0              0               0
 22   0              0              0               0
 23   0              0              0               0
 24   0              0              0               0
 25   0              0              0               0
 26   0              0              0               0
 27   0              0              0               0
 28   0              0              0               0
 29   0              0              0               0
 30   0              0              0               0
 31   0              0              0               0
 32   0              0              0               0
 33   0              0              0               0
 34   0              0              0               0
 35   0              0              0               0
 36   0              0              0               0
 37   0              0              0               0
 38   0              0              0               0
 39   0              0              0               0
 40   0              0              0               0
```

```
41    0                0                0                0
42    0                0                0                0
43    0                0                0                0
44    0                0                0                0
45    0                0                0                0
46    0                0                0                0
47    0                0                0                0
48    0                0                0                0
49    0                0                0                0
50    0                0                0                0
51    0                0                0                0
52    0                0                0                0
```

Port	ポート番号
Status	機能の状態。Enabled または Disabled
Frame Action	試験フレームの受信によるループ検出時に行うアクション。None（何もしない）、PortDisable（ポートを無効にする（物理的なリンクは保持する））、Linkdown（ポートを物理的にリンクダウンさせる）、BCDiscard（該当スイッチポートのブロードキャストフレームの受信を止める）
Frame Interval	試験フレームの送信間隔
Secure Frame	セキュアな試験フレームの受信をするかどうか。On または Off
Blocking Timeout	ループ検出時に行うアクションの実行後、アクション実行前状態に戻るまでの時間の設定値

表 17: CONFIG 指定時

Port	ポート番号
Loop	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）
Expiry	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 NONE を指定した場合は次のループパケット検出処理を再開するまでの時間。単位は秒
Port Status	該当ポートの状態。Enabled または Disabled。アクションによって Disabled になった場合は（Act）、コマンドによって Disabled になった場合は（User）がそれぞれ表示される
Link Status	該当ポートのリンクの状態。Up または Down。アクションによって Down になった場合は（Act）、コマンドによって Down になった場合は（User）がそれぞれ表示される
B/C Status	該当ポートのブロードキャストフレームの通信状態。Forward（正常通信）、Discard（ブロードキャストフレームの受信ができない状態）

表 18: STATUS 指定時

Port	ポート番号
Frame Tx	試験フレームの送信数
Frame Rx	試験フレームの受信数
Action	試験フレームの受信によるアクションが実行された回数
Frame Rx Discards	破棄された試験フレームの数

表 19: COUNTER 指定時

例

■ポート 1、2 の LDF 検出機能の設定を表示する

```
SHOW SWITCH LOOPDETECTION PORT=1,2 CONFIG
```

■LDF 検出機能の状態を表示する

```
SHOW SWITCH LOOPDETECTION STATUS
```

■LDF 検出機能のカウンター情報を表示する

```
SHOW SWITCH LOOPDETECTION COUNTER
```

関連コマンド

DISABLE SWITCH LOOPDETECTION（71 ページ）
ENABLE SWITCH LOOPDETECTION（89 ページ）
RESET SWITCH LOOPDETECTION COUNTER（104 ページ）
SET SWITCH LOOPDETECTION（116 ページ）

SHOW SWITCH MIRROR

カテゴリー：スイッチング

SHOW SWITCH MIRROR

解説

ミラーポートの設定情報を表示する

入力・出力・画面例

```
Manager > show switch mirror

Port Mirroring Information
--------------------------------------------------
 Mirror Port ............... 1
 Status .................... Disabled
 Port Mirroring on Rx ...... None
 Port Mirroring on Tx ...... None
 Port Mirroring on Both .... None
--------------------------------------------------
```

Mirror Port	ミラーポート番号
Status	ポートミラーリング機能の状態。有効（Enabled）または無効（Disabled）
Port Mirroring on Rx	受信パケットだけをミラーリングしているソースポート
Port Mirroring on Tx	送信パケットだけをミラーリングしているソースポート
Port Mirroring on Both	送受信両方のパケットをミラーリングしているソースポート

表 20:

例

■ミラーポートの設定情報を表示

```
SHOW SWITCH MIRROR
```

関連コマンド

DISABLE SWITCH MIRROR（72 ページ）
ENABLE SWITCH MIRROR（91 ページ）
SET SWITCH MIRROR（118 ページ）

SHOW SWITCH PORT

カテゴリー：スイッチング

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　対象となるスイッチポート番号または ALL。ALL を指定した場合はすべてのスイッチポートが対象となる。

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、詳細情報が表示される

SECURITY　ポートセキュリティーの全般的な情報を表示

入力・出力・画面例

```
Manager > show switch port=1

Switch Port Information
------------------------------------------------------------------------------
 Port ........................... 1
   Description ..................... -
   Status ......................... Enabled
   Link State ..................... Down
   UpTime ......................... -
   Port Media Type ................ Ethernet CSMA/CD
   Port Type ...................... 10/100/1000Base-T
   Configured speed/duplex ....... Autonegotiate
   Actual speed/duplex ........... -
   MDI Configuration (Polarity) .. Automatic (-)
   Acceptable Frame Types ........ Acceptable All Frames
   Broadcast rate limit .......... -
   Multicast rate limit .......... -
   DLF rate limit ................ -
   Security Mode .................. Automatic
   Learn Limit .................... -
   Intrusion Action ............... Discard
   Mirroring ...................... None
   Is this port mirror port ...... No
   Enabled flow control(s) ....... -
```

```
   Send tagged pkts for VLAN(s)... -
   Port-based VLAN ............... vlan2(2)
   Ingress Filtering ............. Off
   Trunk Group ................... -
   Port Priority ................. 0
   STP ........................... default
-------------------------------------------------------------------------------

Manager > show switch port=1 summary

 Port                State     Config      Mirror  Port-based VLAN
                     Link      Actual      MDI     Trunk
-------------------------------------------------------------------------------
 1:-                 Enabled   Autonego    None    default(1)
                     Up        100MFull    Auto(-)     -
-------------------------------------------------------------------------------

Manager > show switch port=1 summary

 Port                State     Config      Mirror  Multiple VLAN
                     Link      Actual      MDI     Trunk
-------------------------------------------------------------------------------
 1:-                 Enabled   Autonego    None    UV1
                     Up        100MFull    Auto(-)     -
-------------------------------------------------------------------------------

Manager > show switch port=1-10 security

 Port                    Security Mode   Learn Learned Locked IntrusionAction
-------------------------------------------------------------------------------
 1:                      Secured          -     -      ON     Log
 2:                      Secured          -     -      ON     Discard
 3:                      Secured          -     -      ON     Disable
 4:                      Dynamic Limited  10    0      OFF    Discard
 5:                      Limited          2     2      ON     Trap
 6:                      Secured          -     -      ON     Discard
 7:                      Automatic        -     -      OFF    Discard
 8:                      Automatic        -     -      OFF    Discard
 9:                      Automatic        -     -      OFF    Discard
10:                      Automatic       -     -       OFF    Discard
-------------------------------------------------------------------------------
```

Port	ポート番号
Description	ポートの説明（メモ）。
Status	ポートのステータス。有効（Enabled）または無効（Disabled）。LDF 検出機能または受信レート検出機能によって無効にされている場合は、"Disabled by Loop/Storm Detection"、エコトリガーにより無効になった場合、"DISABLED by Powersave trigger"、ポートトランキングによりリンクダウンポートが無効になった場合、"DISABLED by Trunk"、ポートセキュリティーの設定により一時的に無効になった場合、"DISABLED by Port Security"、UDLD 機能によりポートが閉塞された場合は"Disabled by UDLD"と表示される
Link State	ポートのリンクステータス。リンクが確立（Up）または確立していない（Down）。DISABLE SWITCH PORT コマンドの LINK パラメーター指定によりリンクダウンさせた場合は"Down by User"、LDF 検出機能または受信レート検出機能によってダウンさせた場合は、"Down by Loop/Storm Detection"、エコトリガーによりリンクダウンした場合は"Down by Powersave trigger"、UDLD 機能によりポートが閉塞された場合は"Down by UDLD" と表示される
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（xxx days, 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
Port Type (Fibre Actual)	ポートの種類。SFP ポートの場合はリンクしているメディア
Configured speed/duplex	通信モードの設定値。Autonegotiate、10/100 Mbps Half/Full duplex、Autonegotiate (10/100 Mbps Half/Full duplex、10-100 Mbps、1000 Mbps Full duplex)、1000Mbps, full duplex で表示される。1000Mbps, full duplex は SFP ポートが 1000MFull に設定されているときに表示。Autonegotiate (1000 Mbps Full duplex) は固定ポートが 1000MFull に設定されているときに表示
Actual speed/duplex	実際の通信モード。1000Mbps, full duplex は SFP ポートが 1000MFull に設定され、1000BASE-T でリンクしているときに表示。Autonegotiate (1000 Mbps Full duplex) は固定ポートまたは SFP ポートが 1000MFull に設定され、1000BASE-T でリンクしているときに表示

MDI Configuration (Polarity)	MDI/MDI-X 自動認識の設定と実際の極性。MDI/MDI-X 自動認識の設定は、Automatic（自動認識有効）、または Manual（自動認識無効）が表示される。実際の極性はカッコ内に MDI、MDI-X(AUTOMDI の場合でリンクダウン時) が表示される。また SFP ポートは Not applicable と表示される
Acceptable Frame Types	受信可能なフレームタイプ。すべてのフレーム（Acceptable All Frames）またはタグ付き VLAN フレームのみ（Admit Only Vlan-tagged Frames）
Broadcast rate limit	パケットストームプロテクションのブロードキャストフレームの受信レート（pps）
Multicast rate limit	パケットストームプロテクションのマルチキャストフレームの受信レート（pps）
DLF rate limit	パケットストームプロテクションの未学習のユニキャストフレームの受信レート（pps）
Security Mode	ポートのセキュリティーモード。Automatic/Dynamic/Limited/Secured のいずれか
Learn Limit	DynamicLimite モード、Limited モードの登録可能な MAC アドレススタティックエントリーアドレス数
Intrusion Action	ポートセキュリティー機能で不正パケットを検出した場合の動作設定。Discard/Disable/Log/Trap のいずれか。
Mirroring	ミラーリング対象パケットの向き。ミラーリングしない（None）、受信（Rx）、送信（Tx）、送受信（Both）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。設定されている（Yes）またはされていない（No）
Enabled flow control(s)	有効なフロー制御方式。Full Duplex 時（Pause）
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)。コンフィグの情報を表示する。
Ingress Filtering	イングレスフィルタリングの有効（On）または無効（Off）
Trunk Group	ポートが所属するトランクグループ名
Port Priority	ユーザープライオリティー値 (0〜7)
STP	ポートが所属する STP ドメイン名

表 21:

Port	ポート番号およびポートの説明
State	ポートの状態。有効（Enabled）または無効（Disabled）
Link	ポートのリンクステータス。リンクが確立（Up）または確立していない（Down）
Config	通信モードの設定値。Autonego、10/100MHalf/Full、10/100MH/FAuto、10-100M Auto、1000MFull のいずれか

Actual	実際の通信モード。1000MFULL 設定時は 1000BASE-T ポート、SFP ポートどちらも 1000MFULL と表示される
Mirroring	ミラーリング対象ポートのパケットの向きまたはミラーポート。ミラーリングしない（None）、受信（Rx）、送信（Tx）、送受信（Both）、ミラーポート（Mirror）のいずれか
MDI	MDI の設定（Auto、MDI、MDI-X のいずれか）と（）内に実際の極性を表示。SFP ポートの場合は N/A
Port-based VLAN	ポートが所属するポートベース VLAN 名（VID）
Trunk	ポートが所属するトランクグループ名

表 22: SUMMARY オプション指定時

Port	ポート番号およびポートの説明
Security Mode	該当ポートのセキュリティーモード。
Learn	登録可能 MAC アドレス数が表示される。
Learned	実際に学習している MAC アドレス数が表示される。スタティックエントリーの数は含まれない。
Locked	Dynamic Limited/Limited モード時は、学習済み MAC アドレス数が LEARN パラメーターで指定した学習可能な送信元 MAC アドレス（スタティックエントリー）の最大数に達しているときに ON、それ以外は OFF となる。Secured モード時は、常に ON
IntrusionAction	設定している IntrusionAction が表示される。

表 23: SECURITY オプション指定時

例

■スイッチポート 1 の情報を表示する

```
SHOW SWITCH PORT=1
```

■全ポートの一覧を簡易表示する

```
SHOW SWITCH PORT
```

備考・注意事項

GUI では Security Mode には Atomatic と表示される。Learn Limit、IntrusionAction は表示されない。表示される VLAN 情報はコンフィグの情報を表示している。現在所属している VLAN 情報は SHOW VLAN コマンドで確認する。

関連コマンド

ACTIVATE SWITCH PORT AUTONEGOTIATE（43 ページ）
DISABLE SWITCH PORT（73 ページ）
ENABLE SWITCH PORT（92 ページ）
RESET SWITCH PORT（105 ページ）
SET SWITCH PORT（120 ページ）

SHOW SWITCH PORT COUNTER

カテゴリー：スイッチング

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

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

解説

スイッチポートの統計カウンターを表示する。Ctrl+C でスクロールを中止できる

パラメーター

PORT　スイッチポート番号または ALL を指定する。省略時は ALL

入力・出力・画面例

```
Manager > show switch port=1 counter

Switch Port Counters
------------------------------------------------------------------------------
Port 1. Counters:
Combined receive/transmit packets counters:
 64           :                1757    1024-1518    :                    0
 65-127       :                 314    1519-1522(T) :                    0
 128-255      :                 485    1519-2047    :                    0
 256-511      :                 113    2048-4095    :                    0
 512-1023     :                   0    4096-9216    :              2503749

General Counters:
Receive                              Transmit
 Octets       :         21341360956    Octets       :                    0
 UnicastPkts  :                   1    UnicastPkts  :                    0
 MulticastPkts:                  12    MulticastPkts:                    0
 BroadcastPkts:                2656    BroadcastPkts:                    0
 Discards     :             2506241    Discards     :                    0
 Errors       :            13839360    Errors       :                    0
 PauseFrames  :                   0    PauseFrames  :                    0

 AlignmentErrors        :         0
 FCSErrors              :         0
 LateCollisions         :         0
 ExcessiveCollisions    :         0
 CarrierSenseErrors     :         0
 FrameTooLongs          :         0
 SymbolErrors           :         0
```

```
 UndersizePkts           :  13839360
 Fragments               :         0
 Jabbers                 :         0
 SingleCollisionFrames   :         0
 MultipleCollisionFrames:          0
 DeferredTransmissions   :         0
-------------------------------------------------------------------------------
```

Combined receive/transmit packets 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
1024-1518	1024～1518 オクテット長のフレーム送受信数
1519-1522(T)	1519～1522 オクテット長のタグ付きフレーム送受信数
1519-2047	1519～2047 オクテット長のフレーム送受信数
2048-4095	2048～4095 オクテット長のフレーム送受信数
4096-9216	4095～9216 オクテット長のフレーム送受信数
General Counters	
Receive	受信カウンター
Octets	受信オクテット数
UnicastPkts	上位のレイヤーに配送されたユニキャストパケット数
MulticastPkts	上位のレイヤーに配送されたマルチキャストパケット数
BroadcastPkts	上位のレイヤーに配送されたブロードキャストパケット数
Discards	バッファーのオーバーフローなどで破棄された受信パケット数
Errors	エラーを含んでいるために破棄された受信パケット数
PauseFrames	受信 pause フレーム数
Transmit	送信カウンター
Octets	送信オクテット数
UnicastPkts	上位のレイヤーからの送信を要求されたユニキャストパケット数（破棄されたパケットも含む）
MulticastPkts	上位のレイヤーからの送信を要求されたマルチキャストパケット数（破棄されたパケットも含む）

BroadcastPckts	上位のレイヤーからの送信を要求されたブロードキャストパケット数（破棄されたパケットも含む）
Discards	バッファーのオーバーフローなどで破棄された送信パケット数。未サポート
Errors	エラーを含んでいるために破棄された送信パケット数
PauseFrames	送信 pause フレーム数。未サポート
AlignmentErrors	フレーム長がオクテットの整数倍でないフレームの受信数 (10M/100M のみ)。未サポート
FCSErrors	FCS エラーフレーム数
LateCollisions	512 ビット時間経過後、送信コリジョンを検出した回数
ExcessiveCollisions	16 回コリジョンが発生したため送信が中止されたフレームの数。未サポート
CarrierSenseErrors	受信フレーム間の搬送波にエラーが発生した回数
FrameTooLongs	9216Byte を超える正しいフォーマットの受信フレーム数
SymbolErrors	シンボル（符号）エラーフレーム数
UndersizePkts	64Byte 未満の受信フレーム数（10〜63Byte で、正しいフォーマットのフレーム）
Fragments	64Byte 未満の受信エラーフレーム数（10〜63Byte で、FCS が正しくないか、アライメントエラーのフレーム）
Jabbers	9216Byte を超える送信エラーフレーム数（FCS が正しくないか、アライメントエラーのフレーム)。未サポート
SingleCollisionFrames	1 回のみコリジョンが発生した送信フレームの数 (10M/100M のみ)
MultipleCollisionFrames	2〜15 回コリジョンが発生した送信フレーム数（レイトコリジョンを含む）(10M/100M のみ)
DeferredTransmissions	最初の送信が延期された後に送信されたフレーム数 (10M/100M のみ)

表 24:

例

■ポート 1 の統計情報を参照する

```
SHOW SWITCH PORT=1 COUNTER
```

備考・注意事項

Pause フレーム受信時に受信カウンターの Discards がカウントアップする。

関連コマンド

SHOW SWITCH PORT（153 ページ）

SHOW SWITCH STORMDETECTION

カテゴリー：スイッチング

SHOW SWITCH STORMDETECTION [PORT={*port-list*|ALL}] [{CONFIG|STATUS|
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

受信レート検出機能の設定、状態、カウンターの情報を表示する。CONFIG、STATUS、COUNTER のいずれのパラメーターも指定しない場合、設定情報、状態、カウンター情報の順に、指定ポートのすべての情報が表示される

パラメーター

PORT　ポート番号または ALL を指定する。省略時は ALL
CONFIG　受信レート検出機能の設定情報を表示する
STATUS　受信レート検出機能の状態情報を表示する
COUNTER　受信レート検出機能のカウンター情報を表示する

入力・出力・画面例

```
Manager > show switch stormdetection port=1,2 config

Switch Storm Detection configuration
--------------------------------------------------------------------------------
 Port ........................... 1
 Status ......................... Disabled
 High Rate Action ............... PortDisable
 Low Rate Action ................ None
 High Rate Threshold ............ 81940 Kbps
 Low Rate Threshold ............. 51200 Kbps
 Blocking Timeout ............... 300 sec
 Frame Type ..................... ALL
 Frame Size ..................... AUTO

 Port ........................... 2
 Status ......................... Enabled
 High Rate Action ............... PortDisable
 Low Rate Action ................ None
 High Rate Threshold ............ 81940 Kbps
 Low Rate Threshold ............. 40960 Kbps
 Blocking Timeout ............... 3600   (sec)
```

```
 Frame Type ................... Broadcast
 Frame Size ................... 64

Manager > show switch stormdetection status

Switch Storm Detection Status
--------------------------------------------------------------------------------
 Port Threshold Storm    Expiry Port Status    Link Status B/C Status
--------------------------------------------------------------------------------
 1    High      Blocking 115    Disabled(Act)  Up          Discard
      Low       Blocking 115
 2    High      Normal   --     Disabled(User) Up          Forward
      Low       Blocking 115
 3    High      Detected 32     Enabled        Up          Forward
      Low       Detected 32
 4    --        --       --     Disabled(Act)  Down(Act)   Forward
 5    --        --       --     Enabled        Down        Forward
 6    --        --       --     Enabled        Down        Forward
 7    --        --       --     Disabled(User) Down(User)  Forward
 8    --        --       --     Enabled        Down        Forward
 9    --        --       --     Enabled        Down        Forward
 10   --        --       --     Enabled        Down        Forward
 11   --        --       --     Enabled        Down        Forward
 12   --        --       --     Enabled        Down        Forward
 13   --        --       --     Enabled        Down        Forward
 14   --        --       --     Enabled        Down        Forward
 15   --        --       --     Enabled        Down        Forward
 16   --        --       --     Enabled        Down        Forward
 17   --        --       --     Enabled        Down        Forward
 18   --        --       --     Enabled        Down        Forward
 19   --        --       --     Enabled        Down        Forward
 20   --        --       --     Enabled        Down        Forward
 21   --        --       --     Enabled        Down        Forward
 22   --        --       --     Enabled        Down        Forward
 23   --        --       --     Enabled        Down        Forward
 24   --        --       --     Enabled        Down        Forward
 25   --        --       --     Enabled        Down        Forward
 26   --        --       --     Enabled        Down        Forward
 27   --        --       --     Enabled        Down        Forward
 28   --        --       --     Enabled        Down        Forward
 29   --        --       --     Enabled        Down        Forward
 30   --        --       --     Enabled        Down        Forward
 31   --        --       --     Enabled        Down        Forward
 32   --        --       --     Enabled        Down        Forward
 33   --        --       --     Enabled        Down        Forward
 34   --        --       --     Enabled        Down        Forward
 35   --        --       --     Enabled        Down        Forward
 36   --        --       --     Enabled        Down        Forward
 37   --        --       --     Enabled        Down        Forward
 38   --        --       --     Enabled        Down        Forward
 39   --        --       --     Enabled        Down        Forward
```

```
 40   --         --         --      Enabled         Down         Forward
 41   --         --         --      Enabled         Down         Forward
 42   --         --         --      Enabled         Down         Forward
 43   --         --         --      Enabled         Down         Forward
 44   --         --         --      Enabled         Down         Forward
 45   --         --         --      Enabled         Down         Forward
 46   --         --         --      Enabled         Down         Forward
 47   --         --         --      Enabled         Down         Forward
 48   --         --         --      Enabled         Down         Forward
 49   --         --         --      Enabled         Down         Forward
 50   --         --         --      Enabled         Down         Forward
 51   --         --         --      Enabled         Down         Forward
 52   --         --         --      Enabled         Down         Forward

Manager > show switch stormdetection counter

Switch Storm Detection Counter
--------------------------------------------------------------------------------
Port Detected(High) Action(High)   Detected(Low)  Action(Low)    RxRate(Kbps)
--------------------------------------------------------------------------------
 1    1              1              1              0              1000230
 2    0              0              1              1              0
 3    0              0              0              0              0
 4    0              0              0              0              0
 5    0              0              0              0              0
 6    0              0              0              0              0
 7    0              0              0              0              0
 8    0              0              0              0              0
 9    0              0              0              0              0
 10   0              0              0              0              0
 11   0              0              0              0              0
 12   0              0              0              0              0
 13   0              0              0              0              0
 14   0              0              0              0              0
 15   0              0              0              0              0
 16   0              0              0              0              0
 17   0              0              0              0              0
 18   0              0              0              0              0
 19   0              0              0              0              0
 20   0              0              0              0              0
 21   0              0              0              0              0
 22   0              0              0              0              0
 23   0              0              0              0              0
 24   0              0              0              0              0
 25   0              0              0              0              0
 26   0              0              0              0              0
 27   0              0              0              0              0
 28   0              0              0              0              0
 29   0              0              0              0              0
 30   0              0              0              0              0
 31   0              0              0              0              0
```

```
32    0                0                0                0                0
33    0                0                0                0                0
34    0                0                0                0                0
35    0                0                0                0                0
36    0                0                0                0                0
37    0                0                0                0                0
38    0                0                0                0                0
39    0                0                0                0                0
40    0                0                0                0                0
41    0                0                0                0                0
42    0                0                0                0                0
43    0                0                0                0                0
44    0                0                0                0                0
45    0                0                0                0                0
46    0                0                0                0                0
47    0                0                0                0                0
48    0                0                0                0                0
49    0                0                0                0                0
50    0                0                0                0                0
51    0                0                0                0                0
52    0                0                0                0                0
```

Port	ポート番号
Status	機能の状態。Enabled または Disabled
High Rate Action	受信レートが高レートのしきい値を超えた場合に行うアクション。None（何もしない）、PortDisable（ポートを無効にする（物理的なリンクは保持する））、Linkdown（ポートを物理的にリンクダウンさせる）、BCDiscard（該当スイッチポートのブロードキャストフレームの送受信を止める）
Low Rate Action	受信レートが低レートのしきい値を超えた場合に行うアクション。None（何もしない）、PortDisable（ポートを無効にする（物理的なリンクは保持する））、Linkdown（ポートを物理的にリンクダウンさせる）、BCDiscard（該当スイッチポートのブロードキャストフレームの送受信を止める）
High Rate Threshold	受信レートの高レート時のしきい値。値は Kbps (Kilobits per second)
Low Rate Threshold	受信レートの低レート時のしきい値。値は Kbps (Kilobits per second)
Blocking Timeout	ループ検出時に行うアクションの実行後、アクション実行前状態に戻るまでの時間の設定値
Frame Type	受信レートの対象となるフレームの種類の設定値
Frame Size	受信対象フレームの平均フレームサイズの設定値

表 25: CONFIG 指定時

Port	ポート番号
Threshold	High（高レート時）、Low（低レート時）
Storm	パケットストーム検出状況。Normal（パケットストーム未検出状態）、Detected（パケットストーム検出状態）、Blocking（アクションによりブロッキングされた状態）
Expiry	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 NONE を指定した場合は次のループ検出処理を再開するまでの時間。単位は秒
Port Status	該当ポートの状態。Enabled または Disabled。アクションによって Disabled になった場合は（Act）、コマンドによって Disabled になった場合は（User）がそれぞれ表示される
Link Status	該当ポートのリンクの状態。Up または Down。アクションによって Down になった場合は（Act）、コマンドによって Down になった場合は（User）がそれぞれ表示される
B/C Status	該当ポートのブロードキャストフレームの通信状態。Forward（正常通信）、Discard（ブロードキャストフレームの受信ができない状態）

表 26: STATUS 指定時

Port	ポート番号
Detected(High)	受信レートが高レートのしきい値を超えストームと判断された回数
Action(High)	受信レートが高レートのしきい値を超えストームと判断された場合にアクションが実行された回数
Detected(Low)	受信レートが低レートのしきい値を超えストームと判断された回数
Action(Low)	受信レートが低レートのしきい値を超えストームと判断された場合にアクションが実行された回数
RxRate(Kbps)	該当ポートの現在の受信レート。単位は Kbps(Kilobits per second)。受信対象フレームに BROADCAST もしくは MULTICAST を指定した場合、対象フレームの受信レートが表示される

表 27: COUNTER 指定時

例

■ポート 1、2 の受信レート検出機能の設定を表示する

```
SHOW SWITCH STORMDETECTION PORT=1,2 CONFIG
```

■受信レート検出機能の状態を表示する

```
SHOW SWITCH STORMDETECTION STATUS
```

■受信レート検出機能のカウンター情報を表示する

```
SHOW SWITCH STORMDETECTION COUNTER
```

関連コマンド

DISABLE SWITCH STORMDETECTION（79 ページ）
ENABLE SWITCH STORMDETECTION（96 ページ）
RESET SWITCH STORMDETECTION PORT COUNTER（107 ページ）
SET SWITCH STORMDETECTION（124 ページ）

SHOW SWITCH TRUNK

カテゴリー：スイッチング

SHOW SWITCH TRUNK[=*trunk*]

trunk: トランクグループ名

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を表示

入力・出力・画面例

```
Manager > show switch trunk

Switch Trunk Group
-------------------------------------------------------------
 Trunk group name ... uplink
   Speed ............... 1000 Mbps
   Ports ............... 1-8
-------------------------------------------------------------
```

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。1000M bps、100M bps、10M bps のいずれか
Ports	所属ポートの番号

表 28:

例

■トランクグループの情報を表示する

```
SHOW SWITCH TRUNK
```

関連コマンド

ADD SWITCH TRUNK（48 ページ）

CREATE SWITCH TRUNK（54 ページ）
DELETE SWITCH TRUNK（59 ページ）
DESTROY SWITCH TRUNK（62 ページ）
SET SWITCH TRUNK（126 ページ）

SHOW UDLD

カテゴリー：スイッチング

SHOW UDLD [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

UDLD の状態を表示する。

パラメーター

PORT　対象となるスイッチポート番号または ALL。ALL を指定した場合はすべてのポートが対象となる。

入力・出力・画面例

```
Manager> show udld port=1-3


UDLD Information:
--------------------------------------------------------------------------------

Port ..................... 1
  Status ................... Enabled
  Bidirectional state ...... Bidirectional
  Operational state ........ Advertisement - Single neighbor detected
  Message interval ......... 15
  Time out interval ........ 5

  Entry 1
    Expiration time .......... 35
    Current neighbor state ... Bidirectional
    Device ID ................ 0000F4272DA2
    Port ID .................. Port_01
    Neighbor echo 1 device ... 0000F427750F
    Neighbor echo 1 port ..... Port_01
    Message interval ......... 15
    Time out interval ........ 5
    Device name .............. GS908MV2

Port ..................... 2
  Status ................... Enabled
  Bidirectional state ...... Unknown
  Operational state ........ Link down
  Message interval ......... 7
```

```
  Time out interval ........ 5

  No neighbor cache information stored

Port ..................... 3
  Status ................... Disabled
  Bidirectional state ...... Unknown

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

Port	ポート番号
Status	UDLD の有効・無効。（Enabled、Enabled in aggressive mode、Disabled のいずれか）
Bidirectional state	UDLD の稼働状況。（Unknown、Neighbor's echo is empty、Bidirectional、Unidirectional、Transmit-to-receive loop のいずれか）
Operational state	UDLD の状態。（Link down、Link up、Detection、Extended detection、Advertisement、Advertisement - Single neighbor detected、Advertisement - MULTIPLE NEIGHBORS DETECTED、Disabled port のいずれか）
Message interval	UDLD PDU を送信する間隔 (秒)
Time out interval	ディテクションウィンドウの長さ (秒)
Entry n	対向機器のキャッシュエントリー
Expiration time	エントリーの有効期間
Current neighbor state	対向機器の状態。（Bidirectional、Unknown、Mismatch with neighbor state reported のいずれか）
Device ID	対向機器の Device-ID
Port ID	対向機器の Port-ID
Neighbor echo n device	対向機器から受け取った Echo TLV 情報（Device-ID）
Neighbor echo n port	対向機器から受け取った Echo TLV 情報（Port-ID）
Message interval	対向機器の UDLD PDU を送信する間隔 (秒)
Time out interval	対向機器のディテクションウィンドウの長さ (秒)
Device name	対向機器の装置名

表 29:

例

■ポート 1〜3 の UDLD の状態を表示する。

```
SHOW UDLD PORT=1-3
```

関連コマンド

DISABLE UDLD（80 ページ）
ENABLE UDLD（98 ページ）
RESET UDLD（108 ページ）
SET UDLD（127 ページ）
SHOW UDLD NEIGHBORS（174 ページ）

SHOW UDLD NEIGHBORS

カテゴリー：スイッチング

SHOW UDLD NEIGHBORS

解説

UDLD の対向機器を一覧形式で表示する。

入力・出力・画面例

```
Manager > show udld neighbors


UDLD Neighbor Information:
--------------------------------------------------------------------------
Port    Device-ID                       Port-ID       OperState
--------------------------------------------------------------------------
1       0000F4272DA2                    Port_01       Bidirectional
10      0000F4277514                    Port_09       Bidirectional
--------------------------------------------------------------------------
```

Port	ポート番号
Device-ID	対向機器の Device-ID
Port-ID	対向機器の Port-ID
OperState	対向機器の状態。（Bidirectional、Unknown、Mismatch with neighbor state reported のいずれか）

表 30:

関連コマンド

DISABLE UDLD（80 ページ）
ENABLE UDLD（98 ページ）
RESET UDLD（108 ページ）
SET UDLD（127 ページ）
SHOW UDLD（171 ページ）