スイッチング

概要・基本設定

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

ポートの指定方法

スイッチポートに対する設定コマンドには、複数のポートを一度に指定できるものがあります。

■ 1 つのポートを指定

```
ENABLE SWITCH PORT=2 ↵
```

■ 連続するポート番号をハイフン区切りで指定

```
ADD VLAN=black PORT=3-7 ↵
```

■ 連続していないポート番号をカンマ区切りで指定

```
SHOW SWITCH PORT=2,4,8 ↵
```

■ カンマとハイフンの組み合わせ指定

```
SHOW SWITCH PORT=2,4-7 ↵
```

■ すべてのポートを意味する特殊なキーワード ALL を指定

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

基本コマンド

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

■ ポートをイネーブルにするには ENABLE SWITCH PORT コマンド（71 ページ）を使います。

```
ENABLE SWITCH PORT=8 ↵
```

■ ポートをディセーブルにするには DISABLE SWITCH PORT コマンド（63 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（96 ページ）の SPEED パラメーターを使います。デフォルトは AUTONEGOTIATE です。

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

■ ポートをハードウェア的にリセットするには RESET SWITCH PORT コマンド（77 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（144 ページ）を使います。

```
SHOW SWITCH PORT ↵
```

■ ポートの送受信統計を見るには SHOW SWITCH PORT COUNTER コマンド（147 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（77 ページ）に COUNTER オプションをつけて実行します。COUNTER オプションをつけないと、ポートがハードウェア的にリセットされてしまうので注意してください（カウンターもクリアされる）。

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

ポートトランキング

ポートトランキングは複数の物理ポートを束ねてスイッチ間の帯域幅を拡大する機能です。束ねたポートはトランクグループと呼ばれ、論理的に 1 本のポートとして扱われます。トランクグループは、VLAN 内でも単一ポートとして認識されます。また、トランクグループ内のポートに障害が発生しても残りのポートで通信が継続できるため、信頼性の向上にも貢献します。
ポートトランキング機能の仕様は、以下のようになっています。

- トランクグループを 6 つまで作成可能
- それぞれのトランクグループには、最大 8 ポートまで所属させることが可能
- 同一グループ内に、異なるタイプのポートを混在させることはできない
- SFP ポートにポートトランキングを設定する場合は、2 ポートともリンクダウンした状態で設定を行う
- 隣接していないポートでも、同一グループに所属させることができる
- 同一グループに所属するポートの、通信速度とデュプレックスモードの設定およびフローコントロールの設定は、同じ設定でなければならない（設定が異なっている場合は、グループの中でポート番号が一番小さいポートの設定で上書きされます）
- 同一グループに所属するポートは、同一 VLAN に所属し、同一のタグ設定（TAGGED または UNTAGGED）でなければならない

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。

■ トランクグループを作成するには、CREATE SWITCH TRUNK コマンド（55 ページ）を使用します。ここでは、トランクグループ「uplink」を作成します。グループ名は自由につけられます。

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

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

✎ 2 つのグループ内の接続は、それぞれのグループ内で、ポート番号が最も小さいポートからポート番号順に接続してください。

✎ ポートトランキングと IGMP Snooping、MLD Snooping、ポートセキュリティー、マルチプルスパニングツリープロトコルは併用できません。

✎ ポートのデュプレックスモードが「Half Duplex」のポートを、トランキンググループに追加しないでください。

■ トランクグループの情報は SHOW SWITCH TRUNK コマンド（157 ページ）で確認できます。

```
SHOW SWITCH TRUNK ↵
```

■ 送信時のポート選択基準は CREATE SWITCH TRUNK コマンド（55 ページ）、SET SWITCH TRUNK コマンド（104 ページ）の SELECT パラメーターで指定できます。次の例ではトランクグループ「uplink」のポート選択基準を、送信元 MAC アドレスに変更しています。デフォルトでは、送信元 MAC アドレスと宛先 MAC アドレスの両方（MACBOTH）を使って、トランク内のどのポートを使用するかが決定されます。

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

■ フラッディングパケットは、トランクグループ内でポート番号が一番小さいポートから送出されます。

■ トランクグループにポートを追加するには ADD SWITCH TRUNK コマンド（54 ページ）を使います。

```
ADD SWITCH TRUNK=uplink PORT=5-7 ↵
```

✎ トランクグループに追加されたポートの通信モードは、グループの中でポート番号が一番小さいポートの設定で上書きされます。ポートを追加する場合は、設定に注意してください。

■ 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（57 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（58 ページ）を使います。

```
DESTROY SWITCH TRUNK=uplink ↵
```

ポートミラーリング

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

- ソースポートは複数指定可能
- ソースポートを複数設定している状態で、あるソースポートから入力されたパケットが、L2 スイッチングされて別のソースポートから出力された場合、ミラーポートにはパケットが 1 個だけ出力されます。

基本設定

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

1. ミラーポートを指定します。SET SWITCH MIRROR コマンド（94 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ます。

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

   ✎ 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 ↵
   ```

   ✎ 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。

   ✎ 複数のポートをミラーしたいときは、SET SWITCH PORT コマンド（96 ページ）を複数回実行してください。ただし、ミラーリング対象ポートを増やすことはパフォーマンス低下につながりますのでご注意ください（複数のソースポートを指定すると、ミラーポートですべてのパケットを処理できないことがあります）。また、複数のソースポートを指定した場合で、かつ指定ポートにタグ付きとタグなしが混在している場合、送信パケットはすべてタグなしとしてミラーリングされます。

設定は以上です。

■ ポートミラーリングの設定を確認するには SHOW SWITCH MIRROR コマンド（143 ページ）を実行します。ポートミラーリングの状態とミラーポートは、SHOW SWITCH PORT コマンド（144 ページ）の「Mirroring State」欄および「Is this port mirror port」でも確認できます。

■ ミラーポートの設定を解除し、ポートミラーリング機能を無効にするには SET SWITCH MIRROR コマンド（94 ページ）で、0 または NONE を指定します。

```
SET SWITCH MIRROR=0 ↵
```

```
SET SWITCH MIRROR=NONE ↵
```

■ ソースポートでのミラーリングをやめるには SET SWITCH PORT コマンド（96 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 ↵
```

■ ソースポートから入力したパケットと、ミラーポートから出力されるパケットの関係は、次のようになります。

- 入力したパケットがタグなし、かつソースポートと同一の VLAN にミラーポートがタグなしポートとして所属している場合、タグなしとして出力される
- 入力したパケットがタグなし、かつソースポートと異なる VLAN にミラーポートがタグなしポートとして所属している場合、タグ付きとして出力される
- 入力したパケットがタグ付き、かつタグの VID と同一の VLAN にミラーポートがタグなしポートとして所属している場合、タグなしとして出力される
- 入力したパケットがタグ付き、かつタグの VID と異なる VLAN にミラーポートがタグなしポートとして所属している場合、タグ付きとして出力される

表にすると、下記のようになります。
条件欄のソースポートの VID、ミラーポートの VID、タグの VID は、下記を意味します。
ソースポートの VID：ソースポートがタグなしポートとして所属している VLAN の VID
ミラーポートの VID：ミラーポートがタグなしポートとして所属している VLAN の VID
タグの VID：ミラー対象パケットに付いているタグの VID

ミラー対象パケット	条件	ミラーリングされたパケット
タグなし	ソースポートの VID とミラーポートの VID が同じ	タグなし
タグなし	ソースポートの VID とミラーポートの VID が同じでない	タグ付き
タグ付き	タグの VID とミラーポートの VID が同じ	タグなし
タグ付き	タグの VID とミラーポートの VID が同じでない	タグ付き

表 1:

✎ 本製品宛の ICMP Echo Request パケットをミラーリングすると、送信元 MAC アドレスが本製品自身の MAC アドレスに書き換えられて出力されます。さらに、9424T / SP-E については、タグが付与されて出力されます。

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 トラップを上げるなどのアクションを実行させることができます。
本機能は、SET SWITCH PORT SECURITYMODE コマンド（100 ページ）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 SECURITYMODE コマンド（100 ページ）で設定できるのは、次の 3 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）。
LIMITED	学習可能な MAC アドレス数の最大数を設定したセキュリティーモード。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る。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。
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。

表 2:

✎ ポートセキュリティーが有効なポートでは、ポート認証、ポートトランキングを使用できません。また、ポートセキュリティーとスパニングツリープロトコルは併用できません。

■ 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 SECURITYMODE コマンド（100 ページ）を使います。たとえば、ポート 11 の MAC アドレス学習数の上限を 20 個、アクションを DISABLE に設定するには次のようにします。

```
SET SWITCH PORT=11 SECURITYMODE=LIMITED LEARN=20 INTRUSIONACTION=DISABLE
  PARTICIPATE=ON ↵
```

セキュリティーモードに LIMITED モードを設定すると、すでに同ポートで学習していたアドレスエントリー（ダイナミックエントリー）がフォワーディングデータベースから削除され、エントリーなしの状態からアドレス学習が開始されます。
また、ポートセキュリティーが 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 SECURITYMODE コマンド（100 ページ）の INTRUSIONACTION パラメーターで指定）。

アクション名	**動作**
DISCARD	不正なフレームを破棄する。
TRAP	不正なフレームを破棄し、SNMP トラップを送信する。
DISABLE	不正なフレームを破棄し、SNMP トラップを送信した後、該当ポートをディセーブルにする。

表 3:

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

```
#

Port 11: Link DOWN
```

✎ INTRUSIONACTION パラメーターで不正なフレームを受信したときのアクションを指定する場合は、PARTICIPATE パラメーターに ON を指定しないと、アクションは実行されません。

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

■ ポートに、SECURED モードのポートセキュリティーを設定するには、SET SWITCH PORT SECURITYMODE コマンド（100 ページ）を使います。

```
SET SWITCH PORT=12 SECURITYMODE=SECURED ↵
```

■ 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 15 ページ）を使います。ポートセキュリティーがオンのポートで学習されたアドレスは、Source 欄に「Static」と表示されます。

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

■ ポートセキュリティーの設定状況は SHOW SWITCH PORT SECURITYMODE コマンド（152 ページ）で確認できます。「Security Mode」欄には現在のセキュリティーモード、「Intrusion action」欄には不正フレーム受信時のアクション、「Participating」欄には不正フレーム受信時のアクションの有効・無効、「MAC Limit」欄には現在設定されている学習可能な MAC アドレスの上限が表示されます

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

■ 不正なフレームを受信したかどうかは、SHOW SWITCH PORT INTRUSION コマンド（150 ページ）で確認できます。

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

■ ポートセキュリティーが有効なポートに対して、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 7 ページ）または ADD SWITCH FDB 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 MACADDRESS=00-00-f4-ab-cd-ef PORT=10 VLAN=1 ↵

ADD SWITCH FDB MACADDRESS=00-00-f4-ab-cd-ef PORT=10 VLAN=Default_VLAN ↵
```

■ 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 10 ページ）または DELETE SWITCH FDB 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 MACADDRESS=00-00-f4-ab-cd-ef VLAN=1 ↵

DELETE SWITCH FDB MACADDRESS=00-00-f4-ab-cd-ef VLAN=1 ↵
```

■ ポートセキュリティー機能をオフにするには、SET SWITCH PORT SECURITYMODE コマンド（100 ページ）で SECURITY モードに AUTOMATIC を設定します。
LIMITED モードが設定され、学習可能な MAC アドレスの最大数まで学習されたスタティックエントリーはデータベースから削除されますが、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削除されません。

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

■ ポートセキュリティー機能のアクションによってディセーブルにされたポートは ENABLE SWITCH PORT コマンド（71 ページ）でイネーブルに戻します。

```
# enable switch port=1
#

Port 11: Link UP (100Mbps Full-Duplex, 10/100/1000Base-T)
```

■ 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やポートの状態）は CREATE CONFIG コマンド（「運用・管理」の 83 ページ）または SAVE CONFIGURATION コマンド（「運用・管理」の 169 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が、LIMITED 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せん。

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。

- パケットストームプロテクション
- 受信レート検出

パケットストームプロテクション

パケットストームプロテクションは、ポートごとにブロードキャスト / マルチキャスト / 未学習のユニキャストフレームの受信レートに上限を設定し、パケットストームを防止するための機能です。設定値を上回るレートでこれらのフレームを受信した場合、フレームは破棄されます。本機能はデフォルトではオフになっています。
制限できるのは以下のフレームです。かっこ内は設定パラメーターの名前です。

- ブロードキャストフレーム（BCASTRATELIMITING、BCASTRATE）
- マルチキャストフレーム（MCASTRATELIMITING、MCASTRATE）
- 未学習のユニキャストフレーム（UNKUCASTRATELIMITING、UNKUCASTRATE）

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

■ 受信レートの設定は SET SWITCH PORT コマンド（96 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 1 秒あたり 1000 個に制限します。

```
SET SWITCH PORT=1-8 BCASTRATELIMITING=YES BCASTRATE=1000 ↵
```

■ 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 BCASTRATELIMITING=NO ↵
```

■ 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（144 ページ）で確認できます。「Broadcast Rate Limiting Status」、「Broadcast Rate」、「Multicast Rate Limiting Status」、「Multicast Rate」、「Unknown Unicast Rate Limiting Status」、「Unknown Unicast Rate」をご覧ください。

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。
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。

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

■ ポート 2 の受信レート検出機能を有効にするには ENABLE SWITCH PORT STORMDETECTION コマンド（73 ページ）を使用します。

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

■ ポート 2 の高レートのしきい値を 1048576Kbps、アクションを BCASTDISCARD（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 PORT STORMDETECTION コマンド（102 ページ）を使用します。

```
SET SWITCH PORT=2 STORMDETECTION HIGHRATETHRESHOLD=1048576
  HIGHRATEACTION=BCASTDISCARD ↵
```

■ 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 PORT STORMDETECTION コマンド（154 ページ）を使用します。

```
SHOW SWITCH PORT=2 STORMDETECTION 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 PORT STORMDETECTION コマンド（154 ページ）を使用します。

```
SHOW SWITCH PORT=2 STORMDETECTION 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 PORT STORMDETECTION コマンド（154 ページ）を使用します。

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

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フィルタリ

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フィルタリング機能は、ポートごとに、ブロードキャスト / マルチキャスト / 未学習のユニキャストフレームを受信しないようにし、ネットワークのパフォーマンスの低下を防ぐ機能です。
それぞれのフィルタリング機能を有効にすると、受信した該当パケットはすべて破棄されます。本機能は、デフォルトではオフになっています。
フィルタリングの設定は、SET SWITCH PORT コマンド（96 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フィルタリング機能を有効とします。

```
SET SWITCH PORT=1-8 BCASTFILTERING=YES ↵
```

■ フィルタリング機能を無効にするには次のようにします。

```
SET SWITCH PORT=1-8 BCASTFILTERING=NO ↵
```

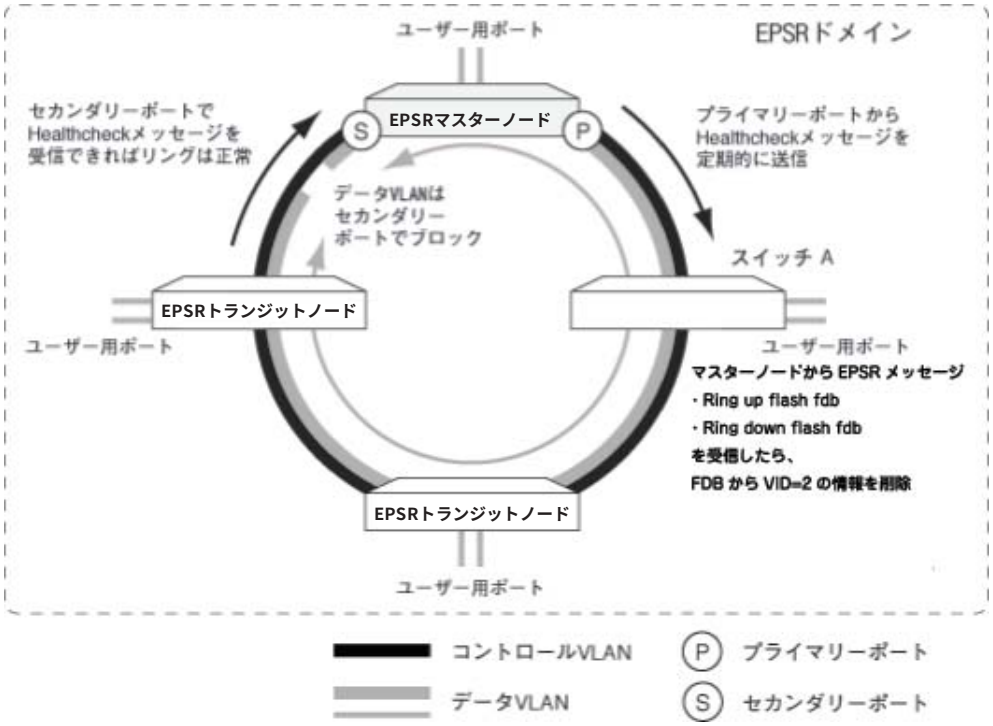
■ ブロードキャスト / マルチキャスト / 未学習のユニキャストフレームのフィルタリングの設定状況は SHOW SWITCH PORT コマンド（144 ページ）で確認できます。「Broadcast Filter」、「Unknown Multicast Filter」、「Unknown Unicast Filter」をご覧ください。

EPSR Snooping

EPSR スヌーピングは EPSR 機能を持たないスイッチをリング内に設置して利用する場合に、高速な冗長性を実現するための機能です。

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・冗長機能です。

EPSR スヌーピングを有効にすると、EPSR のコントロール VLAN でやりとりさせる動作制御メッセージのうちの Ring Up、Ring Down メッセージを監視し、FDB および ARP エントリーを削除します。



■ 指定したコントロール VLAN 上の制御メッセージ監視を有効にするには、ENABLE EPSRSNOOPING コマンド（67 ページ）を実行します。

```
ENABLE EPSRSNOOPING CONTROLVLAN=red ↵
```

■ 指定したコントロール VLAN 上の制御メッセージ監視を無効にするには、DISABLE EPSRSNOOPING コマンド（59 ページ）を実行します。

```
DISABLE EPSRSNOOPING CONTROLVLAN=red ↵
```

■ すべてのコントロール VLAN 上の制御メッセージ監視の情報を表示するには、SHOW EPSRSNOOPING コマンド（108 ページ）を実行します。

```
SHOW EPSRSNOOPING CONTROLVLAN=ALL ↵
```

基本設定

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

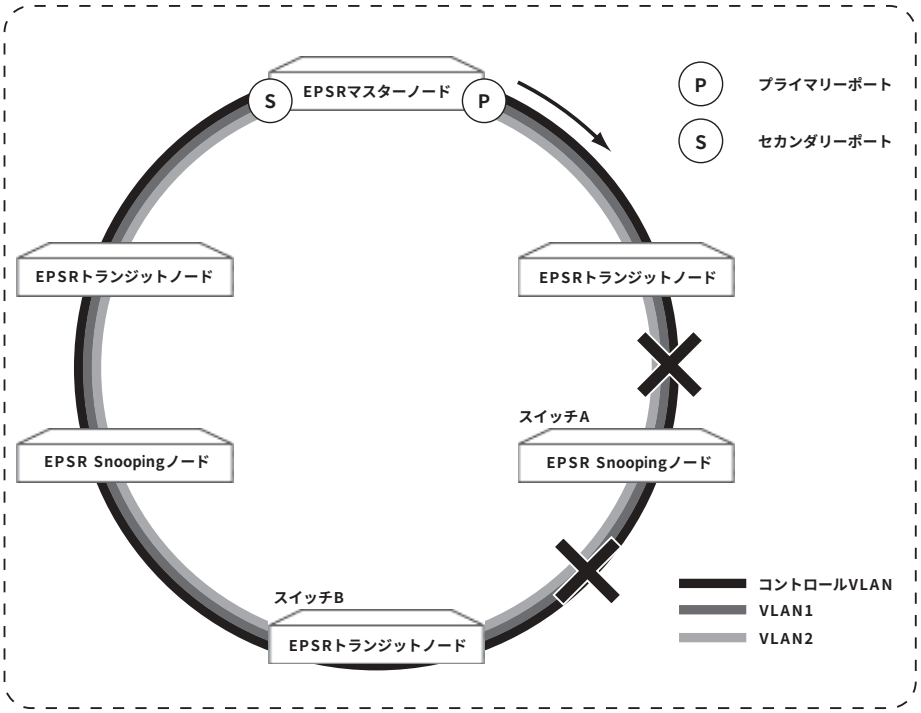
   ```
   CREATE VLAN=ctrl VID=2 ↵
   ADD VLAN=ctrl PORT=1,2 FRAME=TAGGED ↵
   ```

2. スイッチ A の EPSR スヌーピングを有効にします。

   ```
   ENABLE EPSRSNOOPING CONTROLVLAN=ctrl ↵
   ```

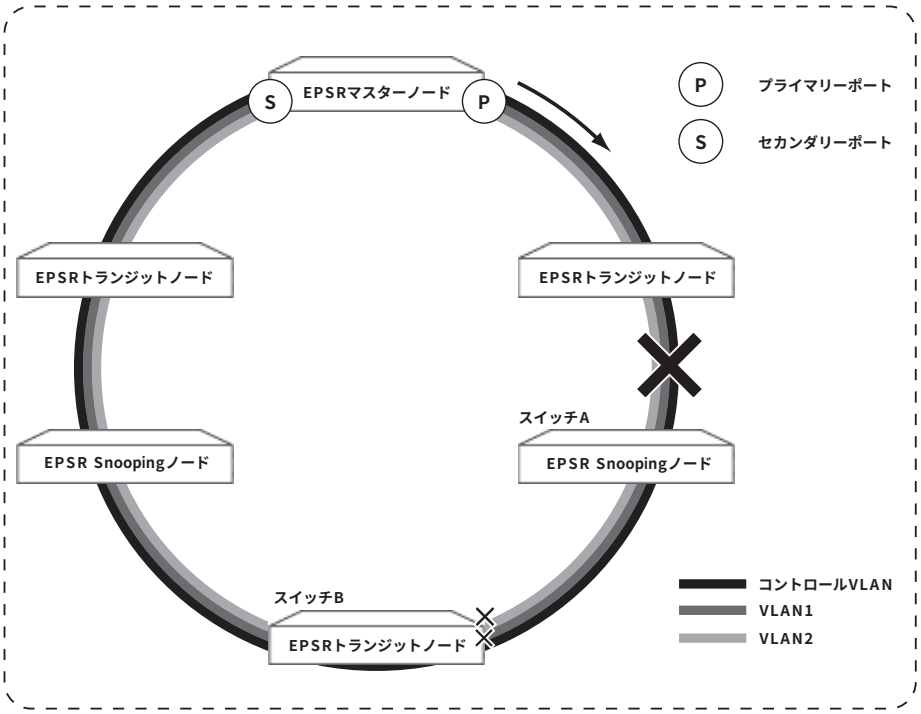
構成上の注意事項

本製品をリング内に設置して利用する場合には、下記の点にご注意ください。
下記の図のようにスイッチ A の両端がリンクダウンしている状態を、Double Fail と呼びます。



この状態から片方のリンクダウンが復旧した場合、EPSR スヌーピングノードのスイッチ A は、片方のみリンクアップ状態になります。
EPSR トランジットノードのスイッチ B は、両方向リンクアップ状態になりますが、コントロール VLAN 以外の VLAN をブロックし、通信を遮断している状態のままになっています。ブロック状態を解除する

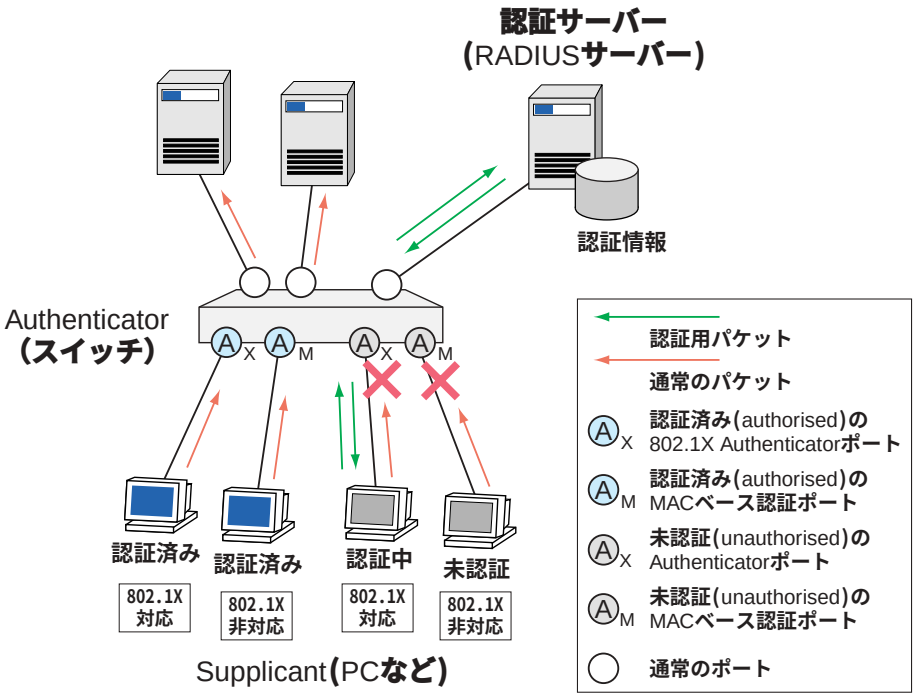
には、EPSR マスターノードからの Healthcheck メッセージを受信する必要がありますが、スイッチ B は Healthcheck メッセージを受信できません。このように EPSR トランジットノードは通信できる状態であるにも関わらず、EPSR ドメイン内で孤立するノードが発生してしまう場合がありますので、ご注意ください。



ポート認証

概要

ポート認証のシステムは、通常下記の 3 要素から成り立っています。



- Authenticator（認証者）：ポートに接続してきた Supplicant（クライアント）を認証する機器またはソフトウェア。
  - IEEE 802.1X 認証方式（以下、802.1X 認証）
    EAP メッセージの交換によって Supplicant を認証する（ユーザー認証）。802.1X の認証を受けるためには、802.1X Supplicant の機能を備えている必要がある。802.1X Supplicant 機能は、一部の OS に標準装備されているほか、単体のクライアントソフトウェアとして用意されていることもある。
  - MAC アドレスベース認証方式（以下、MAC ベース認証）
    Supplicant の MAC アドレスによって認証を行う（機器認証）。MAC ベース認証を受けるために特殊な機能は必要ない。
  - Web 認証方式
    Supplicant 上の Web ブラウザーからのユーザー名とパスワードを入力することによって認証を行う（ユーザー認証）。Web 認証を受けるには、Supplicant 上に対応 Web ブラウザーが必要。

  認証に成功した場合はポート経由の通信を許可、失敗した場合はポート経由の通信を拒否する。
  認証処理そのものは、認証サーバー（RADIUS サーバー）に依頼する（Supplicant の情報を認証サーバーに中継して、認証結果（成功・失敗）を受け取る）。

- 認証サーバー（RADIUS サーバー）：Authenticator の要求に応じて、Supplicant を認証する機器またはソフトウェア。ユーザー名、パスワード、MAC アドレス、所属 VLAN などの認証情報を一元管理している。Authenticator との間の認証情報の受け渡しには RADIUS プロトコルを用いる。
- Supplicant（クライアント）：ポートへの接続時に Authenticator から認証を受ける機器またはソフトウェア。後述の「Supplicant として使用する際の設定例」をご覧ください。

本製品の各スイッチポートは、上記のうち、Authenticator と Supplicant になることができます。認証サーバー（RADIUS サーバー）は別途用意する必要があります。

✎ Protected Ports VLAN と併用する場合は、先に VLAN の設定を行ってから、ポート認証に関する設定を行ってください。

✎ ポート認証と MLD Snooping、IGMP Snooping、ポートセキュリティーは併用できません。

認証方式

本製品は、スイッチポート単位で LAN 上のユーザーや機器を認証するポート認証機能を実装しています。ポートに接続された機器（および機器を使用するユーザー。以下同様）の認証方法としては、大きく分けて次の 3 種類をサポートしています。

- 802.1X 認証
- MAC ベース認証
- Web 認証

ポート認証機能を使用すれば、スイッチポートに接続された機器を認証し、認証に成功したときだけ同機器からの通信、および、同機器への通信を許可するよう設定できます。また、認証に成功した機器を特定の VLAN にアサインすることも可能です（ダイナミック VLAN）。さらに、本製品は Supplicant 機能にも対応しているため、他の機器から認証を受けるよう設定することもできます。

機能・用語の説明

ダイナミック VLAN

ダイナミック VLAN（Dynamic VLAN Assignment）は、RADIUS サーバーから受け取った認証情報に基づいてポートの所属 VLAN を動的に変更する機能です。
Supplicant が認証された後、Supplicant の所属 VLAN および、ポートをどの VLAN に移動させるかは、SET PORTAUTH PORT コマンド（87 ページ）の、VLANASSIGNMENT パラメーター、VLANASSIGNMENTTYPE パラメーターで設定します。
各設定を組み合わせた場合の、動作は以下のようになります。

VLANASSIGNMENT	VLANASSIGNMENTTYPE	認証後の Supplicant の所属 VLAN
DISABLED	-	ポートの VLAN
ENABLED	PORT	ポートの VLAN または最初の Supplicant に指定された VLAN。ポートの所属する VLAN と通信については下記の「■ VLANASSIGNMENT=ENABLE、VLANASSIGNMENTTYPE=PORT のとき」をご覧ください。
ENABLED	USER(Multi-Supplicant モード時のみ)	認証サーバーから指定された VLAN。Supplicant の所属する VLAN と通信については下記の「■ VLANASSIGNMENT=ENABLE、VLANASSIGNMENTTYPE=USER のとき」をご覧ください。

表 4:

■ VLANASSIGNMENT=ENABLE、VLANASSIGNMENTTYPE=PORT のとき

- Supplicant の認証に失敗した場合、ポートは本来の VLAN（ADD VLAN コマンド（「バーチャル LAN」の 12 ページ）で指定した VLAN）の所属となります。ポート越えの通信は不可能です。
- RADIUS サーバーから有効な VLAN の情報が返ってきた場合、ポートはその VLAN の所属となります。認証に成功すれば、ポート越えの通信も可能です。
- RADIUS サーバーから無効な VLAN の情報が返ってきた場合、ポートは本来の VLAN 所属となります。また、認証も失敗となるため、ポート越えの通信は不可能です。
- RADIUS サーバーから VLAN の情報が返ってこなかった場合、ポートは本来の VLAN 所属となります。認証に成功すれば、ポート越えの通信も可能です。
- 該当ポートまたはシステム全体でポート認証が無効に設定された場合、ポートは本来の VLAN 所属となります。ポート認証が無効なので、ポート越えの通信に関する制限はありません。
- 未認証のポート、および、CONTROL=UNAUTHORISED（未認証固定）または CONTROL=AUTHORISED（認証済み固定）に設定されたポートは、本来の VLAN 所属となります。
- ポートがダイナミック VLAN にアサインされているとき、ポートがダイナミック VLAN から本来の VLAN に戻るのは、次のときです。
  - 認証済みの Supplicant がいなくなったとき。
  - リンクがダウンしたとき。
  - システム上でポート認証が無効にされたとき（DISABLE PORTAUTH コマンド（61 ページ））。

■ VLANASSIGNMENT=ENABLE、VLANASSIGNMENTTYPE=USER のとき

- Supplicant の認証に失敗した場合、Supplicant は本来の VLAN（ADD VLAN コマンド（「バーチャル LAN」の 12 ページ）で指定した VLAN）の所属となります。ポート越えの通信は不可能です。
- RADIUS サーバーから有効な VLAN の情報が返ってきた場合、Supplicant はその VLAN の所属となります。認証に成功すれば、ポート越えの通信も可能です。
- RADIUS サーバーから無効な VLAN の情報が返ってきた場合、Supplicant は本来の VLAN 所属となります。また、認証も失敗となるため、ポート越えの通信は不可能です。
- RADIUS サーバーから VLAN の情報が返ってこなかった場合、Supplicant 本来の VLAN 所属となります。認証に成功すれば、ポート越えの通信も可能です。
- 該当ポートまたはシステム全体でポート認証が無効に設定された場合、Supplicant は本来の VLAN

所属となります。ポート認証が無効なので、ポート越えの通信に関する制限はありません。

- 未認証のポート、および、CONTROL=UNAUTHORISED（未認証固定）またはCONTROL=AUTHORISED（認証済み固定）に設定されたポート上の Supplicant は、本来の VLAN 所属となります。

✎ 「ダイナミック VLAN の設定例」を参照してください。

ゲスト VLAN

ゲスト VLAN を使用すると、認証前および、認証に失敗した Supplicant が所属する VLAN を指定できます。
未認証の Supplicant の所属する VLAN を SET PORTAUTH PORT コマンド（87 ページ）の GUESTVLAN パラメーターで指定することができます。ゲスト VLAN 内では、通信が可能です。

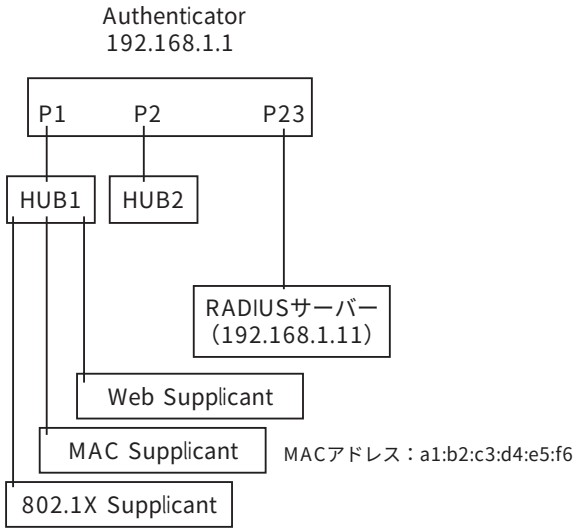
✎ ゲスト VLAN に指定する VLAN は、CREATE VLAN コマンド（「バーチャル LAN」の 15 ページ）に、L2ONLY パラメーターを指定して作成します。

✎ 「ゲスト VLAN の設定例」を参照してください。

ポートの移動について

ポートをリンクダウンさせずに、同一スイッチ内の他のポートに Supplicant が移動した場合、再認証せずに、通信を続けることができます。

■ 構成例



上記構成で、Supplicant が、P1 に接続されている HUB1 から、P2 に接続されている HUB2 に移動した場合、認証情報が引き継がれ、再認証せずに、通信を継続可能です。ポート移動は、802.1X 認証、MAC ベース認証、Web 認証のすべての認証方式で可能です。

■ ポート移動を可能にするには、以下の条件があります。

- 移動元と移動先ポートの認証方式が同じであること。
- 移動元と移動先ポートで、SET PORTAUTH PORT コマンド（87 ページ）の VLANASSIGNMENT-TYPE パラメーターが同じであること。
- 移動元と移動先ポートで、SET PORTAUTH PORT コマンド（87 ページ）の PORTMOVEREAUTH パラメーターが ENABLED になっていること。
- SET PORTAUTH PORT コマンド（87 ページ）に「VLANASSIGNMENTTYPE=PORT」が指定されている場合、移動元と移動先ポートのゲスト VLAN やダイナミック VLAN が設定されていないこと。

Ping ポーリング機能

Web 認証では、認証済み Supplicant の Ping 監視ができます。SET WEBAUTHSERVER コマンド（105 ページ）の PINGPOLL パラメーターで機能の有効・無効を設定します。その他の設定は、下記のパラメーターで設定します。

項目	説明
NORMALINTERVAL	認証が成功している状態での Ping 監視間隔を設定できる。デフォルトは 30 秒である。
TIMEOUT	Ping を送信して返信を待つ時間を設定できる。デフォルトは 1 秒である。
FAILCOUNT	タイムアウトが連続して発生した回数の最大値を設定できる。デフォルトは 5 回である。この回数を超えた Supplicant は未認証状態へ強制的に移動する。
REAUTHREFLESH	Ping の返信を受信した時に再認証タイマーを初期値に戻すかを設定できる。デフォルトは「更新しない」である。

表 5:

✎ 通常の Ping コマンドとの併用が可能です。

✎ ダイナミック VLAN と併用する場合、DHCP サーバーと併用しなければなりません。

✎ 「テンポラリー IP アドレスを使用する場合の設定例」を参照してください。

認証サーバーの設定

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

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

- 802.1X 認証方式を使用する場合、ユーザーごとに下記の属性を定義してください。

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

表 6:

認証方式は、EAP-MD5、PEAP(EAP-MSCHAPv2)、TLS、TTLS を指定します。

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

- MAC ベース認証方式を使用する場合、機器ごとに下記の属性を定義してください。

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

表 7:

認証方式は、PAP を指定します。

- Web 認証方式を使用する場合、ユーザーごとに下記の属性を定義してください。

属性名	属性値	備考
User-Name	ユーザー名	ユーザー名を指定します。
User-Password	パスワード	ユーザー名に対応するパスワードを指定します。

表 8:

認証方式は、PAP を指定します。

- ダイナミック VLAN を使用するときは、前述の諸属性に加え、下記の 3 属性を追加設定してください。

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

表 9:

✎ 後述の「ダイナミック VLAN の設定例」を参照してください。

802.1X 認証方式

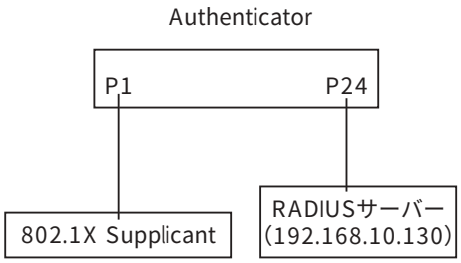
802.1X 認証は、EAP（Extensible Authentication Protocol）というプロトコルを使って、ユーザー単位で認証を行うしくみです。802.1X 認証を利用するには、認証する側と認証される側の両方が 802.1X に対応している必要があります。
802.1X 認証では、EAP-MD5、EAP-TLS、EAP-TTLS、EAP-PEAP など様々な認証方式が使用されています。このうち、本製品の 802.1X 認証モジュールが現在サポートしている EAP 認証方式は以下のとおりです。

- Authenticator 時：EAP-MD5、EAP-TLS、EAP-TTLS、EAP-PEAP
- Supplicant 時：EAP-MD5

基本設定

本製品を Authenticator として使用し、802.1X Supplicant を受け付ける場合の基本設定を示します。
Authenticator としての動作には、IP の設定と RADIUS サーバーの指定が必須です。
以下の設定では、802.1X Supplicant には、802.1X Supplicant を搭載した PC 等が接続されているものとします。
802.1X Supplicant から認証情報として、「ユーザー名:userA」 /「パスワード:passwordA」 が入力され、認証に成功すると、802.1X Supplicant は、VLAN-1(VID=1) で通信が可能になります。

■ 構成



■ 認証サーバー (RADIUS サーバー) には、以下のように設定されているものとします。

User-Name	User-Password	備考
userA	passwordA	802.1X Supplicant 用のユーザー名 / パスワード

表 10:

■ 設定

1. RADIUS サーバーを使って認証を行うため、最初に RADIUS サーバーと通信するための設定をします。最初に、IP アドレスを設定します。

   ```
   ADD IP INT=VLAN1 IP=192.168.10.5 MASK=255.255.255.0 ↵
   ```

2. RADIUS サーバーを登録します。IP アドレスと UDP ポート、共有パスワードを指定します。

   ```
   ADD RADIUSSERVER SERVER=192.168.10.130 ORDER=1 PORT=1812 ACCPORT=1813
     SECRET=himitsu ↵
   ```

3. ポート認証機能を有効にします。

   ```
   ENABLE PORTAUTH ↵
   ```

4. ポート 1〜16 で 802.1X 認証を行うよう設定します。SET PORTAUTH PORT コマンド（87 ページ）の PORTAUTH=8021X TYPE=AUTHENTICATOR を指定することにより、ポート 1〜16 は 802.1X 認証の Authenticator ポートとなります。

   ```
   SET PORTAUTH=8021X PORT=1-16 TYPE=AUTHENTICATOR ↵
   ```

   ✎ Authenticator ポートをタグ付きに設定することはできません。

   ✎ RADIUS サーバーを接続するポートは、Authenticator ポートにしないでください。SET PORTAUTH PORT コマンド（87 ページ）の TYPE/ROLE パラメーターを NONE に設定してください。

Supplicant として使用する際の設定例

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

■ 設定

1. ポート認証機能を有効にします。

   ```
   ENABLE PORTAUTH ↵
   ```

2. ポート 1 で認証を受けるよう設定します。認証を受けるためのユーザー名とパスワードを指定してください。SET PORTAUTH PORT コマンド（87 ページ）の「TYPE=SUPPLICANT」の指定により、ポート 1 は Supplicant ポートとなります。

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

   ✎ Supplicant ポートをタグ付きに設定することはできません。

MAC ベース認証方式

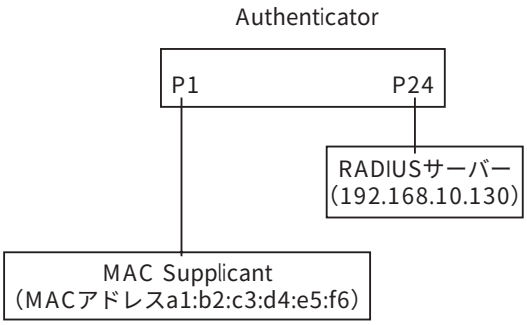
MAC ベース認証は、機器の MAC アドレスに基づいて機器単位で認証を行うしくみです。認証される側に

特殊な機能を必要としないため、802.1X 認証の環境に 802.1X 非対応の機器（例：ネットワークプリンター）を接続したい場合などに利用できます。おもに、802.1X 認証を補完するものとして利用されます。

基本設定

本製品を Authenticator とし、MAC ベース認証を行う場合の基本設定を示します。
Authenticator としての動作には、IP の設定と RADIUS サーバーの指定が必須です。
MAC Supplicant から通信が行われた時点で、Authenticator は、自動的に認証サーバー (RADIUS サーバー) に認証情報を問い合わせ、認証の可否を決定します。
認証が成功すると、MAC Supplicant は、VLAN-1(VID=1) で通信が可能になります。

■ 構成



■ 認証サーバー (RADIUS サーバー) には、以下のように設定されているものとします。

User-Name	User-Password	備考
a1-b2-c3-d4-e5-f6	a1-b2-c3-d4-e5-f6	MAC Supplicant 用のユーザー名 / パスワード

表 11:

認証方式は、PAP を指定します。

■ 設定

1. RADIUS サーバーを使って認証を行うため、最初に RADIUS サーバーと通信するための設定をします。最初に、IP アドレスを設定します。

   ```
   ADD IP INT=VLAN1 IP=192.168.10.5 MASK=255.255.255.0 ↵
   ```

2. RADIUS サーバーを登録します。IP アドレスと UDP ポート、共有パスワードを指定します。

   ```
   ADD RADIUSSERVER SERVER=192.168.10.130 ORDER=1 PORT=1812 ACCPORT=1813
     SECRET=himitsu ↵
   ```

3. ポート認証機能を有効にします。

   ```
   ENABLE PORTAUTH ↵
   ```

4. ポート 1 で MAC ベース認証を行うよう設定します。SET PORTAUTH PORT コマンド（87 ペー

ジ）の「PORTAUTH=MACBASED TYPE=AUTHENTICATOR」の指定により、ポート 1 は MAC ベース認証の Authenticator ポートとなります。

```
SET PORTAUTH=MACBASED PORT=1 TYPE=AUTHENTICATOR MODE=MULTI ↵
```

✎ MAC ベース認証を指定したポートでは、自動的に 「MODE=MULTI」が設定されます。

Web 認証方式

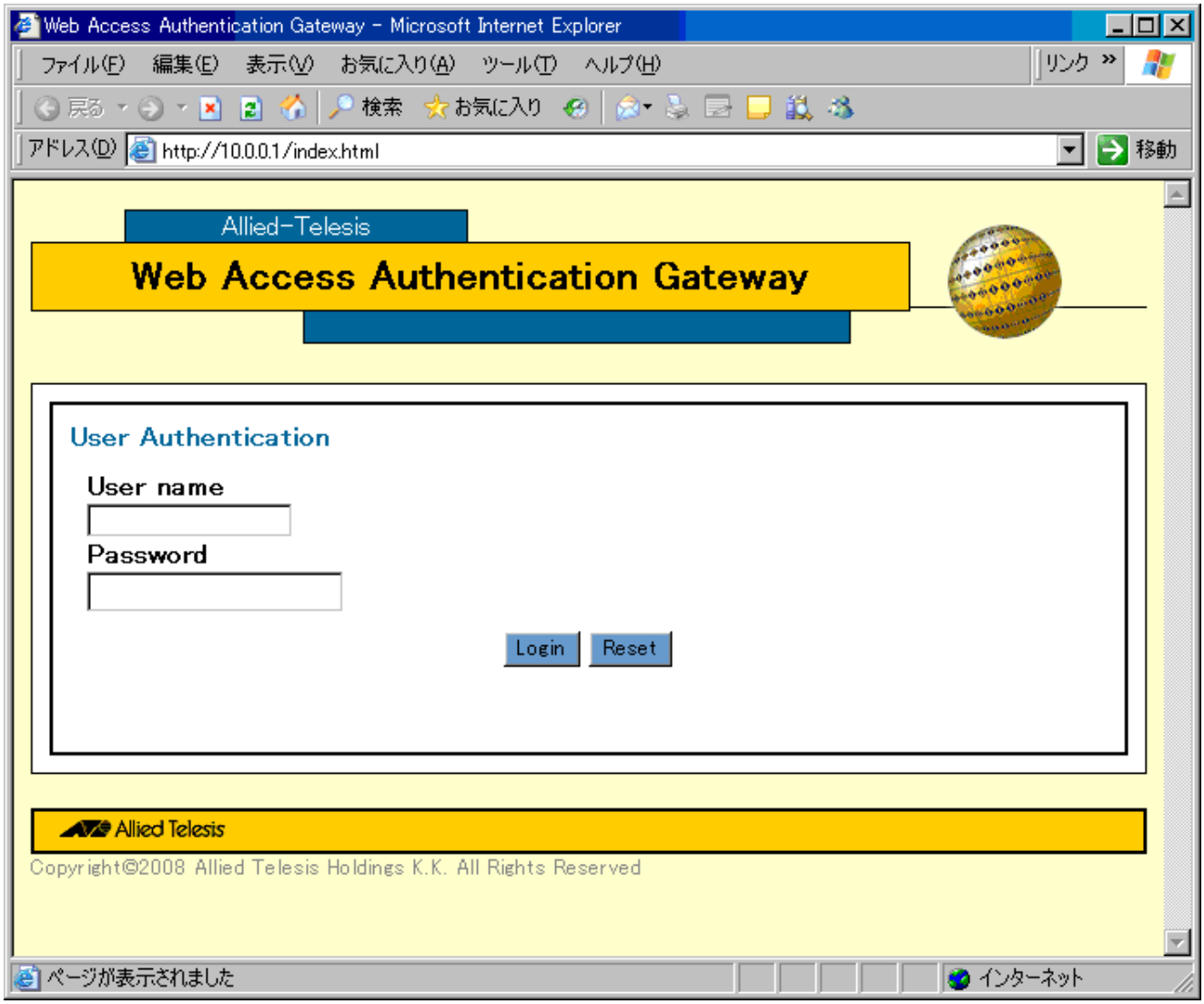
Web 認証は、Web ブラウザーを利用して認証を行うしくみです。ユーザーは Authenticator の Web 認証サーバーに接続し、ユーザー名とパスワードを入力することで認証が行われます。
HTTP 接続を行う場合は、「http:/ / IP アドレス」でアクセス可能です。
通信を暗号化する場合は、「https:/ /IP アドレス」にアクセスすることにより、HTTPS 接続を使用できます。
対応ブラウザー、プロトコルは以下のとおりです。

対応ブラウザー	IE 6.0/7.0、Firefox 2.0（Windows/Mac/Linux/Unix）、Safari 2.0、Opera 9.0（Windows/Mac/Linux/Unix）
対応プロトコル	HTTP 1.0/1.1、SSL 2.0/3.0、TLS 1.0

表 12:

Supplicant から、Web 認証を行う場合は、以下の様に操作します。

1. Web ブラウザーを起動します。
2. 「アドレス」に、Web 認証サーバーの IP アドレスを入力し、「Enter」キーを押します。
3. 次の画面が表示されますので、「ユーザー名」と「パスワード」を入力し、「Login」をクリックします。



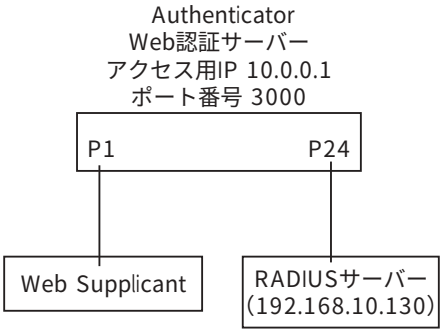
✎ Web 認証で、同時に Web 認証サーバーにアクセスできる Supplicant 数（認証用画面が同時に開ける数）は最大 48 です。認証に成功すれば、他の Supplicant がアクセス可能になります。

その他表示される画面については、後述の「画面遷移」を参照してください。

HTTP サーバーの設定例

本製品を Authenticator とし、Web 認証を行う場合の基本設定を示します。
Authenticator としての動作には、IP の設定と RADIUS サーバーの指定が必須です。
以下の設定では、Web Supplicant には、対応 Web ブラウザーが搭載されており、「http://10.0.0.1:3000」にアクセスするものとします。 Web Supplicant には、IP アドレスの設定が必要です。
Web Supplicant から認証情報として、「ユーザー名:WebUserA」/「パスワード:WebPasswordA」が入力され、認証に成功すると、Web Supplicant は、VLAN-1(VID=1) で通信が可能になります。

■ 構成



■ 認証サーバー (RADIUS サーバー) には、以下のように設定されているものとします。

User-Name	User-Password	**備考**
WebUserA	WebPasswordA	Web Supplicant 用のユーザー名 / パスワード

表 13:

認証方式は、PAP を指定します。

■ 設定

1. RADIUS サーバーを使って認証を行うため、最初に RADIUS サーバーと通信するための設定をします。最初に、IP アドレスを設定します。

   ```
   ADD IP INT=VLAN1 IP=192.168.10.5 MASK=255.255.255.0 ↵
   ```

2. RADIUS サーバーを登録します。IP アドレスと UDP ポート、共有パスワードを指定します。

   ```
   ADD RADIUSSERVER SERVER=192.168.10.130 ORDER=1 PORT=1812 ACCPORT=1813
     SECRET=himitsu ↵
   ```

3. ポート認証機能を有効にします。

   ```
   ENABLE PORTAUTH ↵
   ```

4. ポート 1 で Web 認証を行うよう設定します。SET PORTAUTH PORT コマンド（87 ページ）の「PORTAUTH=WEBBASED TYPE=AUTHENTICATOR」の指定により、ポート 1 は Web 認証の Authenticator ポートとなります。

   ```
   SET PORTAUTH=WEBBASED PORT=1 TYPE=AUTHENTICATOR MODE=MULTI ↵
   ```

5. Web サーバーを設定します。「IPADDRESS=10.0.0.1 PORT=3000」の指定により、「http: / / 10.0.0.1:3000」でアクセス可能にします。

   ```
   SET WEBAUTHSERVER IPADDRESS=10.0.0.1 PORT=3000 ↵
   ```

6. Web 認証サーバーを有効にします。

   ```
   ENABLE WEBAUTHSERVER ↵
   ```

✎ Web 認証を指定したポートでは、自動的に 「MODE=MULTI」が設定されます。

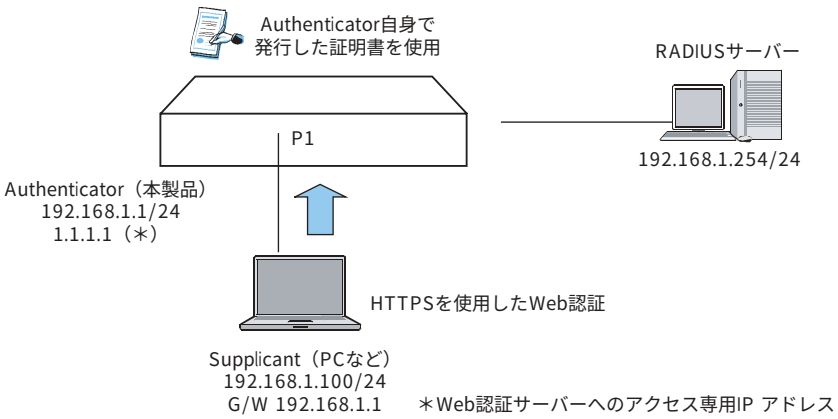
HTTPS サーバーの設定例

HTTPS サーバー機能を使用することにより、Web 認証時の本製品との通信を暗号化する事ができます。

自己認証による設定例

ここでは本製品自身によって発行された公開鍵証明書を使用した HTTPS サーバーの設定を示します。

■ 構成



■ 設定

1. RSA 公開鍵を鍵番号 0 として生成します。推奨鍵長は 1024 ビットです。

```
CREATE ENCO KEY=0 TYPE=rsa LENGTH=1024 DESCRIPTION=my-rsa-key ↵
```

✎ RSA 公開鍵の作成には時間がかかります。「Key Generation completed with [Success]」と表示されるまで待ってから、次の手順に進んでください。また、RSA 公開鍵の作成を行うと、CPU に処理に負荷がかかるため、スイッチの動作に影響を与えます。RSA 公開鍵の作成は、本製品をネットワークに接続していない状態かネットワークの負荷が低いときに行うことをお勧めします。

✎ CREATE ENCO KEY コマンド（「運用・管理」の 84 ページ）はコンソールから入力したときだけ有効なコマンドです。設定ファイルにこのコマンドを記述しておいても無効ですのでご注意ください。また、本コマンドで作成された鍵設定はユーザーがアップロード・ダウンロード可能な設定ファイルには保存されませんので、設定のバックアップを行う場合には、本製品からアップロードした設定ファイルとは別に設定コマンド自体をテキストファイルなどで保管してください。

✎ 鍵番号は 0～65535 の範囲で自由に選択できます。以後、鍵は番号だけで識別することになるため、鍵を作成するときは、CREATE ENCO KEY コマンド（「運用・管理」の 84 ページ）の DESCRIPTION パラ

メーターを使って、鍵の用途などコメントを付けておくとよいでしょう。このコメントはSHOW ENCO KEY コマンド（「運用・管理」の 236 ページ）で表示されます。

2. 公開鍵証明書の発行を行うために、本製品の X.500 識別名（DN = Distinguished Name）を設定します。これは、SET SYSTEM DISTINGUISHEDNAME コマンド（「運用・管理」の 209 ページ）で行います。

```
SET SYSTEM DISTINGUISHEDNAME="cn=1.1.1.1,o=toy-organization,ou=toy-
  organization-unit,l=toy-city,st=toy-pref,c=jp" ↵
```

ここでは、下記の各属性値を設定しています。

属性名	名称	設定値
CN	Common Name	1.1.1.1
O	Organization	toy-organization
OU	Organization Unit	toy-organization-unit
L	Locality	toy-city
ST	State or Province	toy-pref
C	Country	jp

表 14:

✎ CN（Common Name）には Web 認証サーバーへのアクセス専用 IP アドレスの指定を推奨します。

3. 生成した RSA 公開鍵を使用して、公開鍵証明書を発行します。ここでは発行した証明書の名前を my-cert、シリアル番号を 0 とします。

```
CREATE PKI CERTIFICATE=my-cert KEYPAIR=0 SERIALNUMBER=0 ↵
```

本コマンド実行により、本製品のファイルシステム上に公開鍵証明書 my-cert.cer が発行されます。

✎ このコマンドはコンソールから入力したときだけ有効なコマンドです。設定ファイルにこのコマンドを記述しておいても無効ですのでご注意ください。また、本コマンドで作成された公開鍵証明書は設定ファイルには含まれませんのでご注意ください。

4. 発行した公開鍵証明書を証明書データベースへ登録します。ここでは証明書データベースへの登録名を for https server とします。

```
ADD PKI CERTIFICATE="for https server" LOCATION=my-cert.cer TYPE=SELF
  TRUSTED=yes ↵
```

5. IP インターフェースを作成します。

```
ADD IP INTERFACE=vlan1 IPADDRESS=192.168.1.1 MASK=255.255.255.0 ↵
```

6. RADIUS サーバーの設定を行います。ここではシークレットの値を secret とします。

```
ADD RADIUSSERVER SERVER=192.168.1.254 ORDER=1 SECRET=secret ↵
```

7. ポート 1 にポート認証機能として、Web 認証を設定します。

```
SET PORTAUTH=webbased PORT=1 TYPE=authenticator ↵
```

8. Web 認証サーバーへのアクセス専用 IP アドレスを設定します。さらに Web 認証で HTTPS を使用するための設定を行います。

```
SET WEBAUTHSERVER IPADDRESS=1.1.1.1 SECURITY=enabled SSLKEYID=0  ↵
```

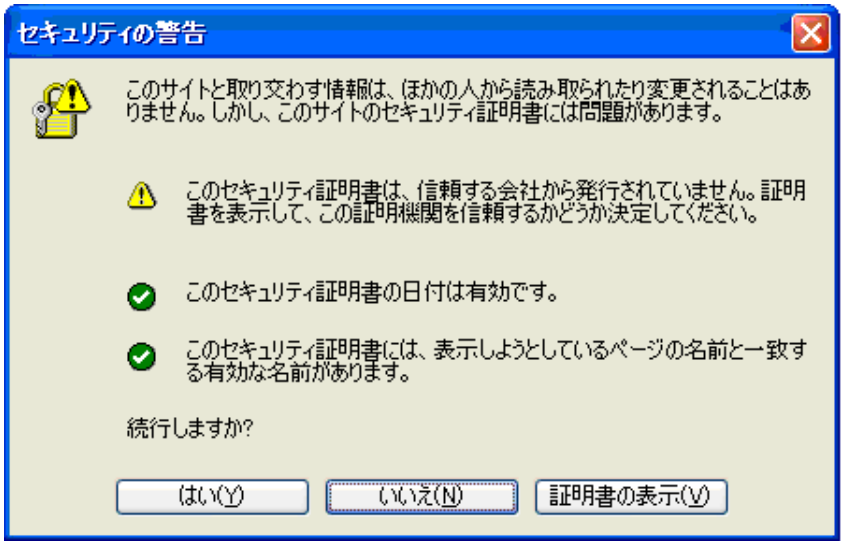
9. Web 認証サーバーを有効にします。

```
ENABLE WEBAUTHSERVER ↵
```

10. ポート認証機能を有効にします。

```
ENABLE PORTAUTH ↵
```

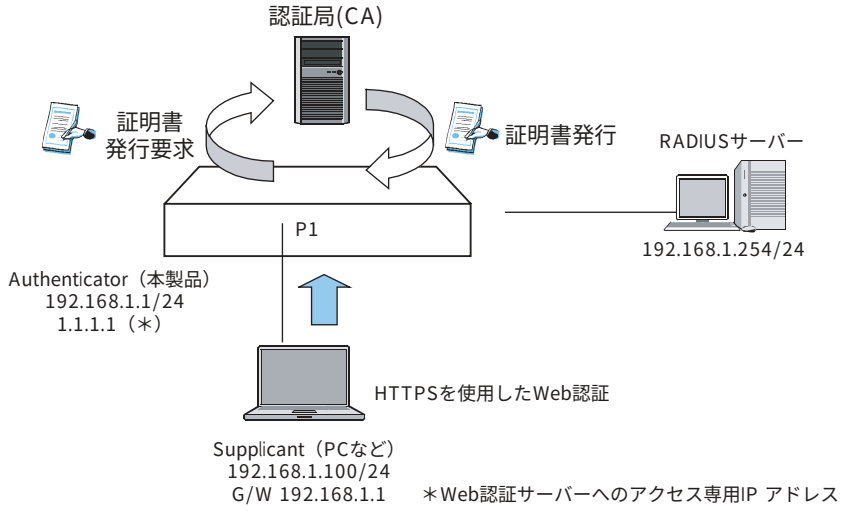
✎ 上記設定で HTTPS 接続を開始すると、お使いのブラウザーによっては、下図のような「警告ウィンドウ」が表示される場合があります。はい（Y）をクリックすることで、認証ページへ移動することができます。



外部認証による設定例

ここでは第三者機関によって発行された公開鍵証明書を使用した HTTPS サーバーの設定を示します。

■ 構成



■ 設定

1. RSA 公開鍵を鍵番号 0 として生成します。推奨鍵長は 1024 ビットです。

```
CREATE ENCO KEY=0 TYPE=rsa LENGTH=1024 DESCRIPTION=my-rsa-key ↵
```

✎ RSA 公開鍵の作成には時間がかかります。「Key Generation completed with [Success]」と表示されるまで待ってから、次の手順に進んでください。また、RSA 公開鍵の作成を行うと、CPU に処理に負荷がかかるため、スイッチの動作に影響を与えます。RSA 公開鍵の作成は、本製品をネットワークに接続していない状態かネットワークの負荷が低いときに行うことをお勧めします。

✎ CREATE ENCO KEY コマンド（「運用・管理」の 84 ページ）はコンソールから入力したときだけ有効なコマンドです。設定ファイルにこのコマンドを記述しておいても無効ですのでご注意ください。また、本コマンドで作成された鍵設定はユーザーがアップロード・ダウンロード可能な設定ファイルには保存されませんので、設定のバックアップを行う場合には、本製品からアップロードした設定ファイルとは別に設定コマンド自体をテキストファイルなどで保管してください。

✎ 鍵番号は 0～65535 の範囲で自由に選択できます。以後、鍵は番号だけで識別することになるため、鍵を作成するときは、CREATE ENCO KEY コマンド（「運用・管理」の 84 ページ）の DESCRIPTION パラメーターを使って、鍵の用途などコメントを付けておくとよいでしょう。このコメントは SHOW ENCO KEY コマンド（「運用・管理」の 236 ページ）で表示されます。

2. 公開鍵証明書の発行要求を行うために、本製品の X.500 識別名（DN = Distinguished Name）を設定します。これは、SET SYSTEM DISTINGUISHEDNAME コマンド（「運用・管理」の 209 ページ）で行います。

```
SET SYSTEM DISTINGUISHEDNAME="cn=1.1.1.1,o=toy-organization,ou=toy-
  organization-unit,l=toy-city,st=toy-pref,c=jp" ↵
```

ここでは各属性値を下記に設定しています。

属性値	設定値
CN（Common Name）	1.1.1.1
O（Organization）	toy-organization
OU（Organization Unit）	toy-organization-unit
L（Locality）	toy-city
ST（State or Province）	toy-pref
C（Country）	jp

表 15:

✎ CN（Common Name）には Web 認証サーバーへのアクセス専用 IP アドレスの指定を推奨します。

3. 生成した RSA 公開鍵を使用して公開鍵証明書の発行要求ファイルを生成します。ここでは証明書発行要求ファイルの名前を enroll_pem、エンコード形式を PEM（Privacy Enhanced Mail）形式とします。

```
CREATE PKI ENROLLMENTREQUEST="enroll_pem" KEYPAIR=0 FORMAT=pem ↵
```

本コマンド実行により、本製品のファイルシステム上に証明書発行要求ファイル ”enroll_pem.csr ” が生成されます。

✎ このコマンドはコンソールから入力したときだけ有効なコマンドです。設定ファイルにこのコマンドを記述しておいても無効ですのでご注意ください。また、本コマンドで作成された証明書要求ファイルは設定ファイルには含まれませんのでご注意ください。

4. 生成した証明書発行要求ファイルを UPLOAD コマンド（「運用・管理」の 283 ページ）で TFTP サーバーなどにアップロードし、それを CA に渡します。CA から証明書が発行され、証明書ファイルが作成されます。ここでは発行された証明書を cert.cer とします。また、CA 自体の証明書を ca_cert.cer とします。
5. 発行された公開鍵証明書および CA 自体の証明書を TFTP サーバーなどへ置き、LOAD コマンド（「運用・管理」の 154 ページ）でロードします。ロードした各ファイルを証明書データベースへ登録します。ここでは証明書データベース上の名前をそれぞれ、for https server、ca とします。

```
ADD PKI CERTIFICATE="ca" LOCATION=ca_cert.cer TRUSTED=yes TYPE=CA ↵


ADD PKI CERTIFICATE="for https server" LOCATION=cert.cer TRUSTED=yes
  TYPE=EE ↵
```

6. IP インターフェースを作成します。

```
ADD IP INTERFACE=vlan1 IPADDRESS=192.168.1.1 MASK=255.255.255.0 ↵
```

7. RADIUS サーバーの設定を行います。ここではシークレットの値を secret とします。

```
ADD RADIUSSERVER SERVER=192.168.1.254 ORDER=1 SECRET=secret ↵
```

8. ポート 1 にポート認証機能として、Web 認証を設定します。

```
SET PORTAUTH=webbased PORT=1 TYPE=authenticator ↵
```

9. Web 認証サーバーへのアクセス専用 IP アドレスを設定します。さらに Web 認証で HTTPS を使用するための設定を行います。

```
SET WEBAUTHSERVER IPADDRESS=1.1.1.1 SECURITY=enabled SSLKEYID=0  ↵
```

10. Web 認証サーバーを有効にします。

```
ENABLE WEBAUTHSERVER ↵
```

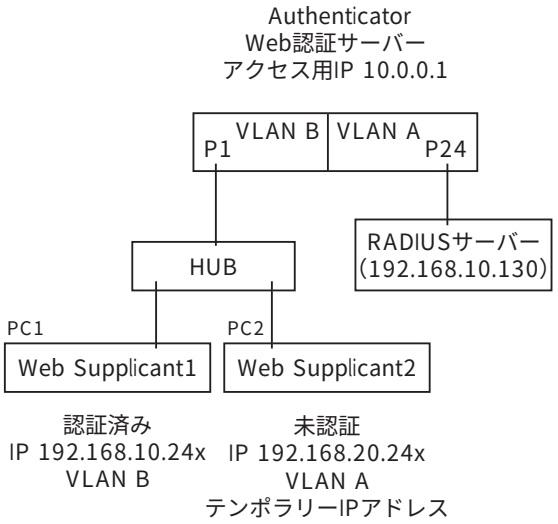
11. ポート認証機能を有効にします。

```
ENABLE PORTAUTH ↵
```

テンポラリー IP アドレスを利用する場合の設定例

テンポラリー IP アドレスは、Web 認証サーバーへアクセスできるように、スイッチの DHCP サーバーを使用し、未認証の Web Supplicant に IP アドレスを一時的 (LeaseTime 20 秒) に付与する機能です。
本製品を Authenticator とし、テンポラリー IP アドレスを利用した、Web 認証を行う場合の基本設定を示します。
テンポラリー IP アドレス機能を使用するには、DHCP サーバーの設定が必要です。
Web Supplicant には、IP アドレスを設定せず、DHCP クライアント機能を有効にします。
以下の設定では、Web Supplicant には、DHCP サーバーより テンポラリー IP として VLAN-B のサブネットの IP アドレス (192.168.20.24x) が割り当てられ、搭載されている対応 Web ブラウザーより「http: / / 10.0.0.1」にアクセスするものとします。
Web Supplicant1 から認証情報として、「ユーザー名:WebUserA」 /「パスワード:WebPasswordA」 が入力され、認証に成功すると、Web Supplicant1 は、VLAN-A(VID=10) で通信が可能になります。
Web Supplicant1 には、認証成功後、本製品の DHCP サーバーから、VLAN-A のサブネットの IP アドレス (192.168.10.24x) が再度割り当てられます。

■ 構成



■ 認証サーバー (RADIUS サーバー) には、以下のように設定されているものとします。

User-Name	User-Password	Tunnel-Type	Tunnel-Medium-Type	Tunnel-Private-Group-ID	**備考**
WebUserA	Web-Password-A	VLAN (13)	IEEE-802 (6)	10	PC1 Web Supplicant1 用のユーザー名/パスワードおよび、認証後に所属させる VLAN
WebUserB	Web-Password-B	VLAN (13)	IEEE-802 (6)	10	PC2 Web Supplicant2 用のユーザー名/パスワードおよび、認証後に所属させる VLAN

表 16:

認証方式は、PAP を指定します。

■ 設定

1. VLAN を作成します。

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

2. VLAN にポートを割り当てます。

```
ADD VLAN=A PORT=24 ↵
ADD VLAN=B PORT=1-23 ↵
```

3. VLAN に IP アドレスを割り当てます。

```
ADD IP INT=VLAN-A IP=192.168.10.5 MASK=255.255.255.0 ↵
ADD IP INT=VLAN-B IP=192.168.20.5 MASK=255.255.255.0 ↵
```

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

```
ADD RADIUSSERVER SERVER=192.168.10.130 ORDER=1 PORT=1812 ACCPORT=1813
  SECRET=himitsu ↵
```

5. ポート認証機能を有効にします。

```
ENABLE PORTAUTH ↵
```

6. ポート 1 で Web 認証を行うよう設定します。SET PORTAUTH PORT コマンド（87 ページ）の「PORTAUTH=WEBBASED TYPE=AUTHENTICATOR」の指定により、ポート 1 は Web 認証の Authenticator ポートとなります。

```
SET PORTAUTH=WEBBASED PORT=1 TYPE=AUTHENTICATOR MODE=MULTI
  VLANASSIGNMENTTYPE=USER ↵
```

7. Web 認証サーバーを設定します。「IPADDRESS=10.0.0.1」の指定により、「http://10.0.0.1」でアクセス可能にします。「PINGPOLL=ENABLED REAUTHREFRESH=ENABLED」の設定により、Ping ポーリング機能が有効になり、Supplicant が Authenticator からの Ping に応答している間、再認証までの時間が延長されます。「TEMPORARYIP=ENABLED」の指定により、テンポラリー IP アドレス機能が有効になります。

```
SET WEBAUTHSERVER IPADDRESS=10.0.0.1 PINGPOLL=ENABLED
  REAUTHREFRESH=ENABLED TEMPORARYIP=ENABLED ↵
```

8. Web 認証サーバーを有効にします。

```
ENABLE WEBAUTHSERVER ↵
```

9. DHCP サーバーを有効にします。

```
ENABLE DHCP ↵
```

10. DHCP サーバーを設定します。認証成功後、所属する VLAN-A の IP インターフェース用設定です。

```
CREATE DHCP POLICY=mypolicy1 LEASE=7200 ↵

ADD DHCP POLICY=mypolicy1 SUBNET=255.255.255.0 ROUTER=192.168.10.5 ↵

CREATE DHCP RANGE=myip1 POLICY=mypolicy1 IP=192.168.10.240
  NUMBER=10 ↵
```

11. DHCP サーバーを設定します。VLAN-B の IP インターフェース用設定です。この設定が、テンポラリー IP アドレスとして、使用されます。

```
CREATE DHCP POLICY=mypolicy2 LEASE=7200 ↵

ADD DHCP POLICY=mypolicy2 SUBNET=255.255.255.0 ROUTER=192.168.20.5 ↵

CREATE DHCP RANGE=myip2 POLICY=mypolicy2 IP=192.168.20.240
  NUMBER=10 ↵
```

✎ Ping ポーリング機能と Web 認証のダイナミック VLAN を併用する場合、スイッチに DHCP サーバーを設定する必要があります。

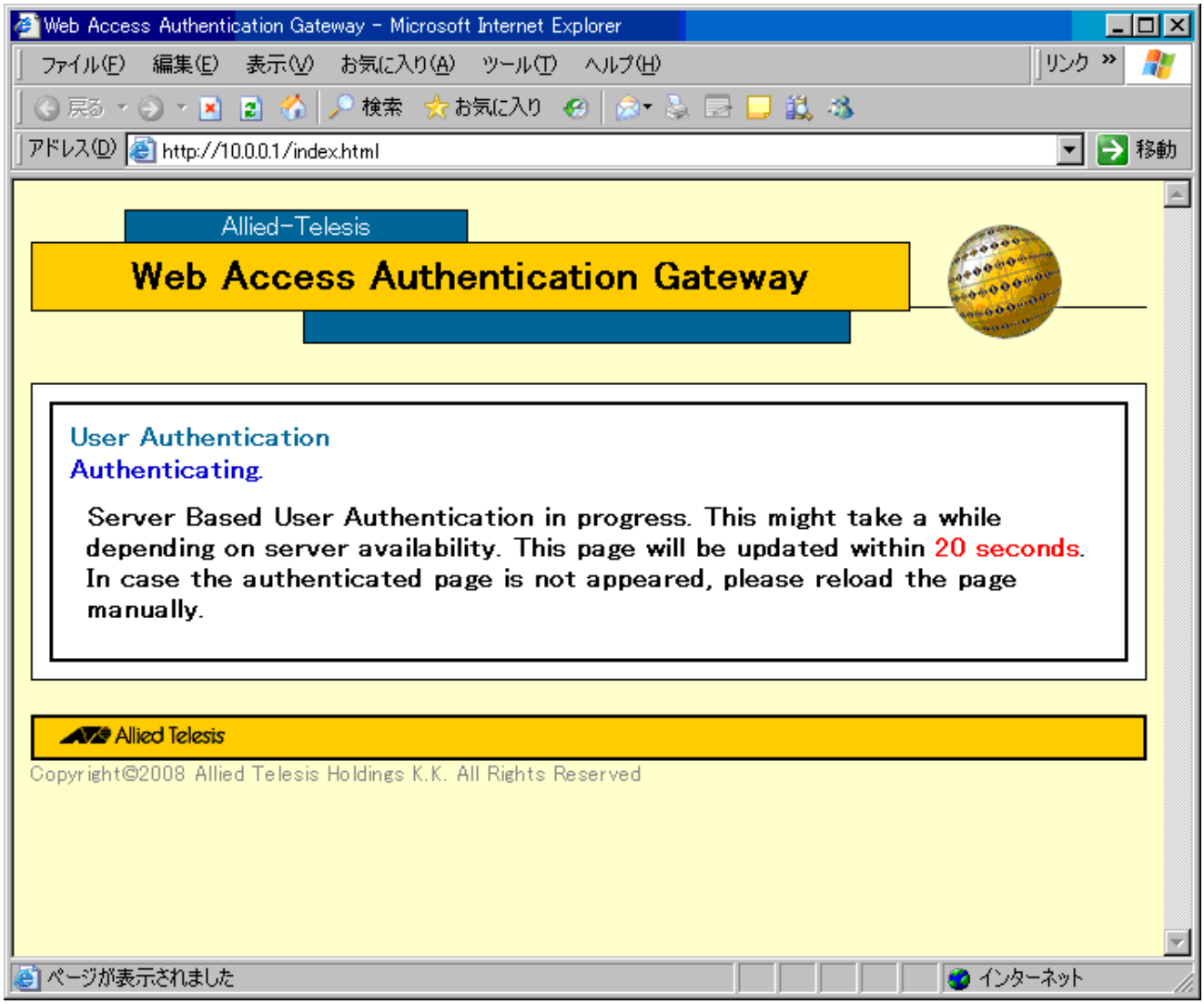
画面遷移

以下が、Web 認証において、Supplicant 上の Web ブラウザーに表示される画面 / メッセージとなります。
画面に表示される一部の文字列は、SET WEBAUTHSERVER コマンド（105 ページ）の HEADER / SUBHEADERTOP / SUBHEA
パラメーターで変更可能です。
認証成功後、リダイレクトする URL を指定するには、SET WEBAUTHSERVER コマンド（105 ページ）の
REDIRECTURL パラメーターを設定します。

認証中

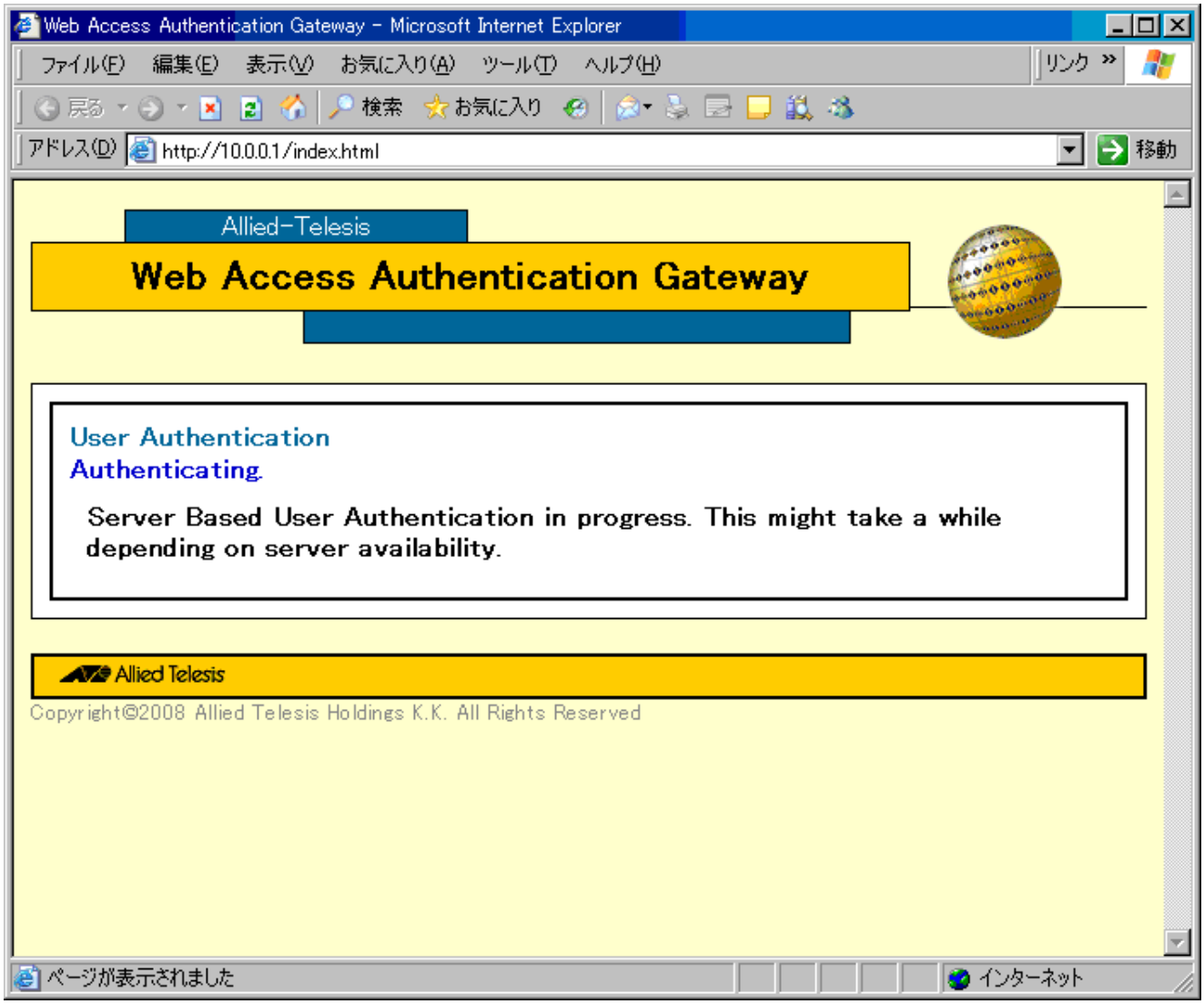
以下の条件の場合、認証中は 以下の画面を表示します。

- ダイナミック VLAN が有効（SET PORTAUTH PORT コマンド（87 ページ）の VLANASSIGNMENT パラメーターが ENABLED）の場合
- PVID とは異なる VLAN が ゲスト VLAN に設定されている場合



ユーザー認証を実行中です。サーバーからの応答により、しばらく時間がかかる場合があります。このページは、20 秒以内に更新されます。認証済みページが表示されない場合は、手動でページを更新してください。以下の条件の場合、認証中は以下の画面を表示します。

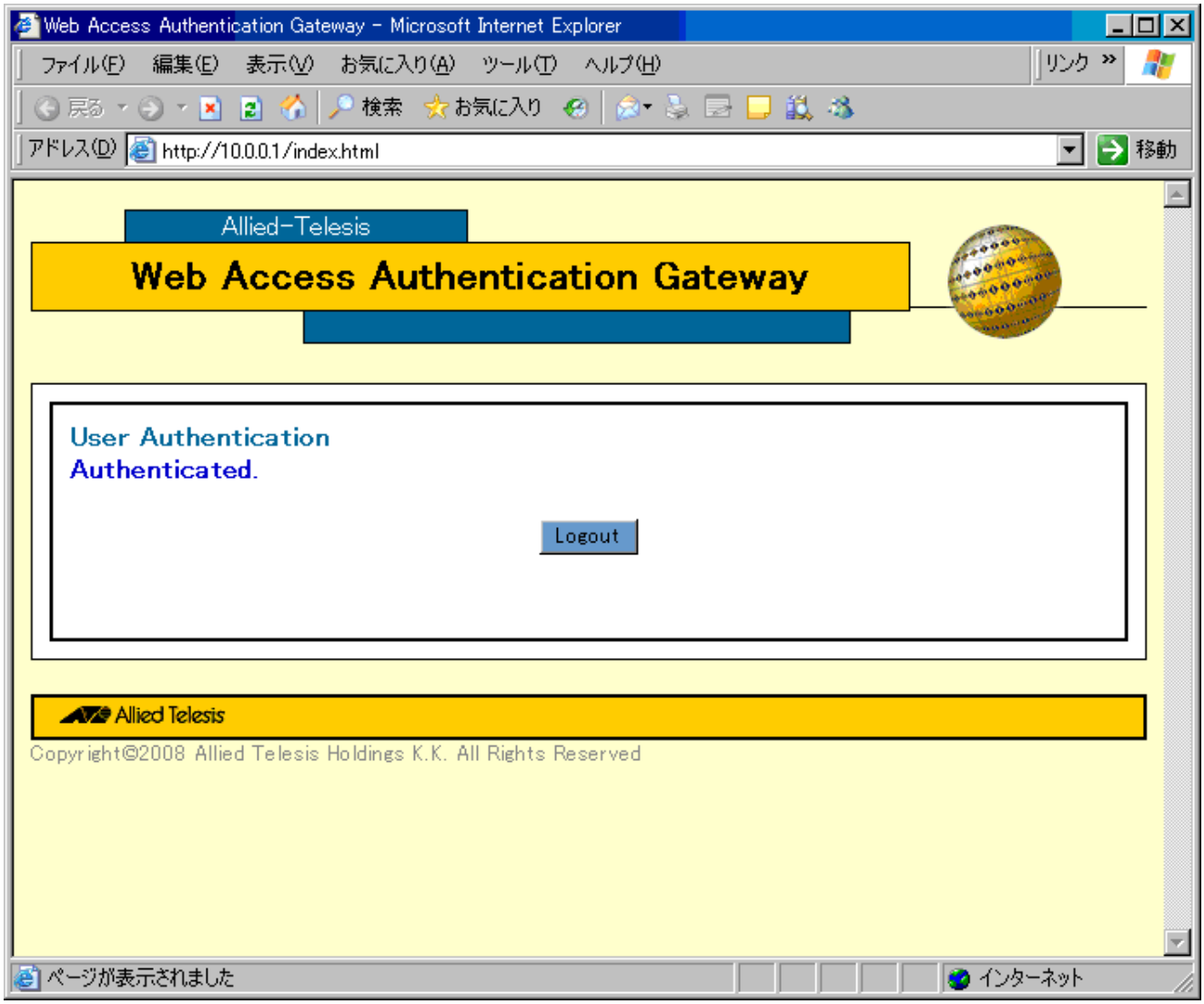
- ダイナミック VLAN が無効（SET PORTAUTH PORT コマンド（87 ページ）の VLANASSIGNMENT パラメーターが DISABLED）かつ ゲスト VLAN を使用しない（SET PORTAUTH PORT コマンド（87 ページ）の GUESTVLAN パラメーターが NONE）場合
- ダイナミック VLAN が無効（SET PORTAUTH PORT コマンド（87 ページ）の VLANASSIGNMENT パラメーターが DISABLED）かつ PVID がゲスト VLAN と同じ設定の場合



ユーザー認証が実行中です。サーバーからの応答により、しばらく時間がかかる場合があります。

認証成功

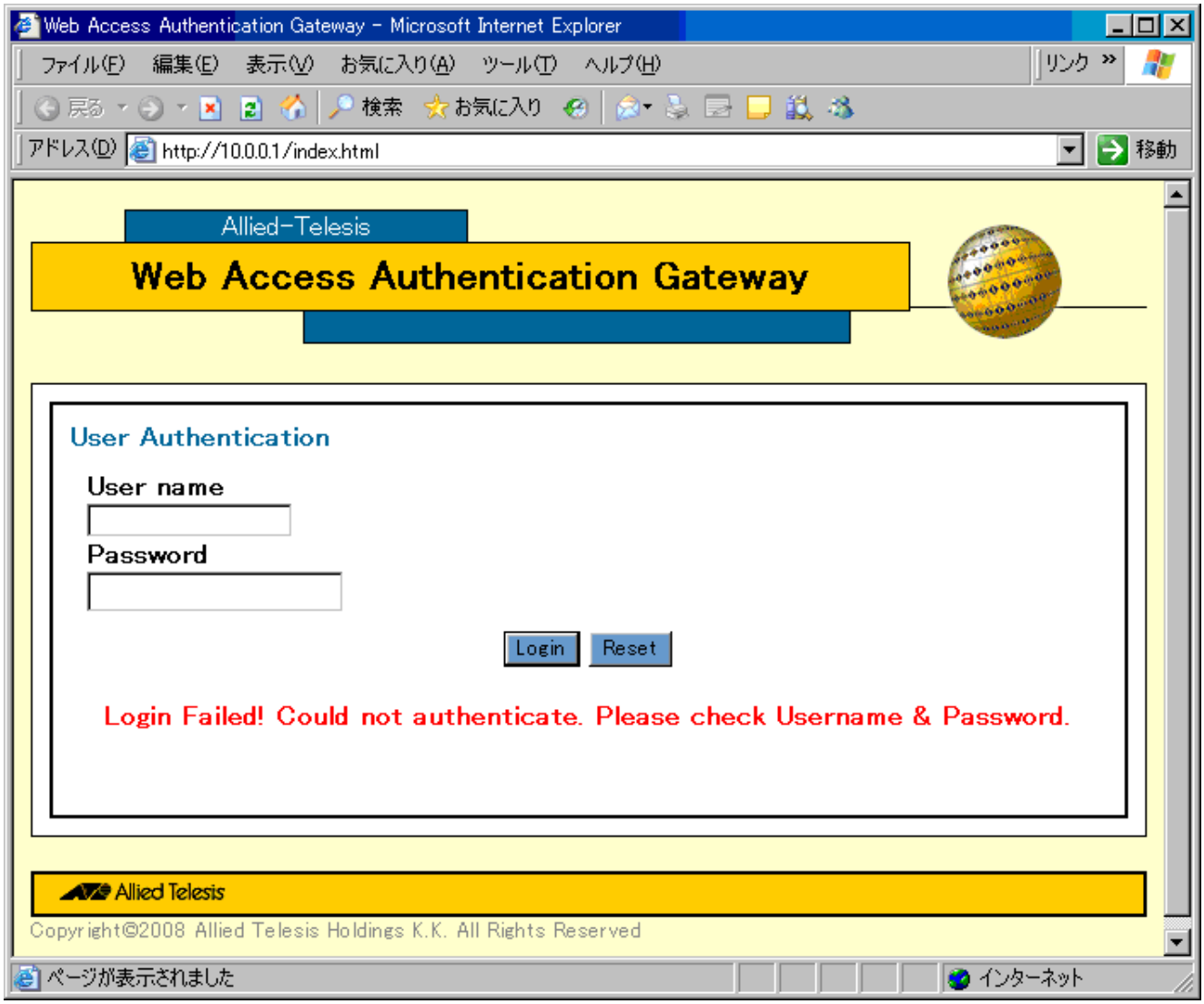
認証に成功するとこの画面を表示します。



認証されました。

認証失敗

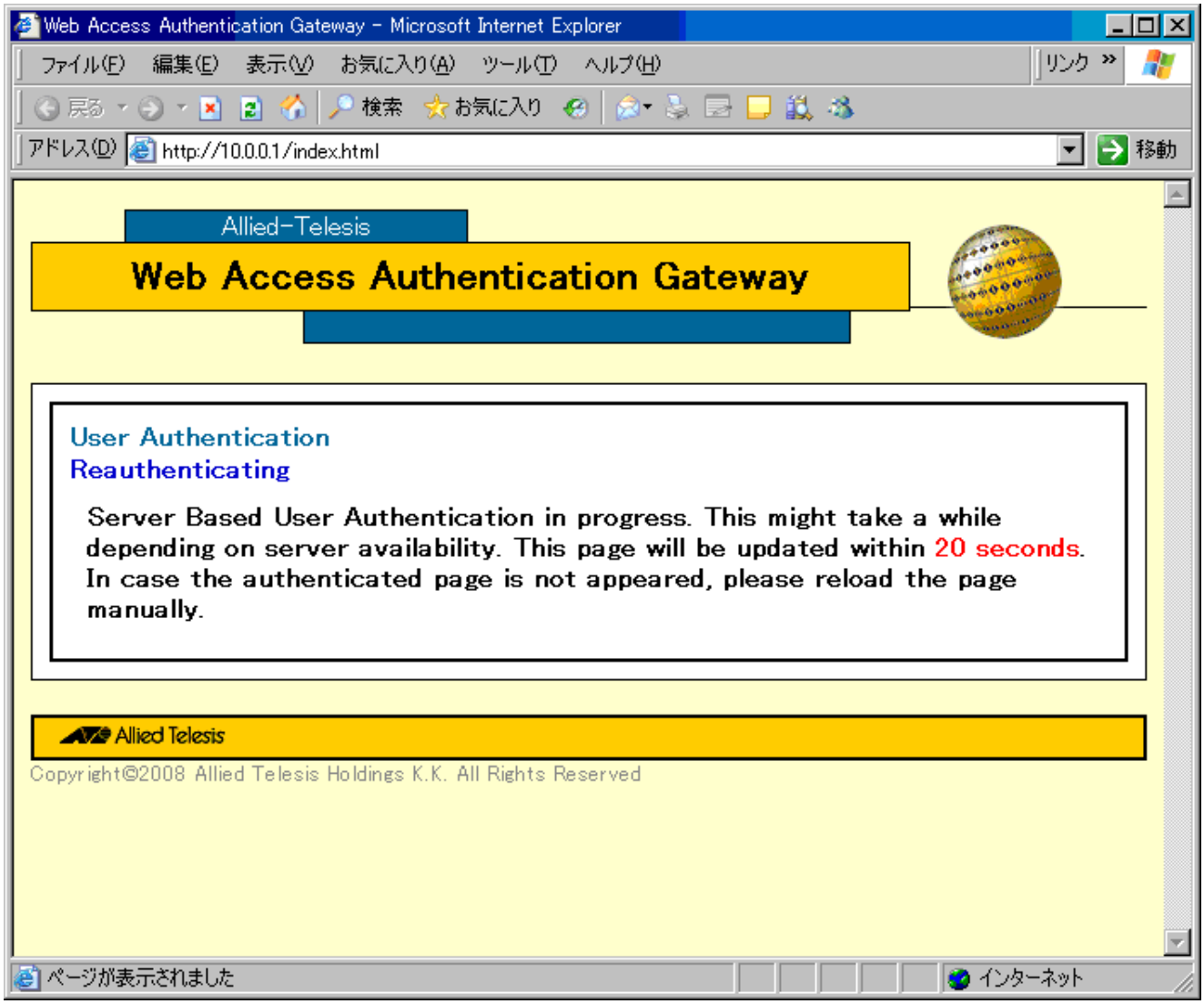
認証に失敗するとこの画面を表示します。



ログインに失敗しました。サーバー認証が失敗しました。

再認証中

再認証中はこの画面を表示します。



ユーザー認証を実行中です。サーバーからの応答により、しばらく時間がかかる場合があります。このページは２０秒以内に更新されます。認証済みのページが表示されない場合は、手動でページを更新してください。

- 本製品の配下のルーターからなど、本製品と異なるセグメントの Supplicant から、Web 認証画面へのアクセスは受け付けられません。

- 本製品をレイヤー 3 スイッチとして使用する構成の場合、ダイナミック VLAN と DHCP サーバー使用時に、Web 認証で元の VLAN 以外にアサインされた後、ログアウトすると、Web 認証画面にアクセスできません。アクセスする場合には、Supplicant で IP アドレスを再取得する必要があります。また、レイヤー 2 スイッチとして使用する構成の場合、Web 認証でゲスト VLAN 以外にアサインされた後、Web 認証画面へアクセスできません。

- 本製品をレイヤー 3 スイッチとして使用する構成の場合、ゲスト VLAN と DHCP サーバー使用時に、Web 認証でゲスト VLAN 以外にアサインされた後、REAUTHPERIOD（Supplicant の再認証間隔）の時間経過後に、Web 認証画面にアクセスできません。また、本製品をレイヤー 2 スイッチとして使用する構成の場合の場合、Web 認証で元の VLAN 以外にアサインされた後、Web 認証画面へアクセスできません。

エラーメッセージについて

認証失敗時に初期画面に表示されるメッセージは次のとおりです。

表示されるメッセージ	エラーの原因
Login Failed! Please check the supplied User Name & Password.	空白のみの入力または、MAC アドレス形式。
Login Failed! Maximum sessions active. Please try later.	同時接続数が最大数に達した。
Login Failed! Could not authenticate with server.	内部的な制限 (メモリー上限等) に達し、要求が受け付けられなかった。認証処理がタイムアウトし、RADIUS サーバーとの通信が失敗した。
Login Failed! Could not authenticate. Please check Username & Password.	RADIUS サーバーで認証に失敗した。
Login Failed! Could not start authentication. Please try later.	Held / Lockout 状態になった。
Login Failed! Could not authenticate.	別の Supplicant が認証中。ポートの設定が未認証固定に手動設定されている。

表 17:

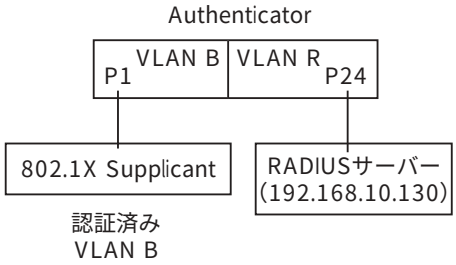
ダイナミック VLAN の設定例

ダイナミック VLAN（Dynamic VLAN Assignment）は、RADIUS サーバーから受け取った認証情報に基づいてポートの所属 VLAN を動的に変更する機能です。
以下、本製品を Authenticator として使用し、さらにダイナミック VLAN 機能を利用する場合の基本設定を示します。Authenticator としての動作には、IP の設定と RADIUS サーバーの指定が必須です。
利用者機器のために 3 つの VLAN「A」、「B」、「C」を用意します。また、RADIUS サーバーを接続するための VLAN「R」も作成します。各ポートに接続された機器は、認証成功後、RADIUS サーバー側から返された VLAN-B に自動的にアサインされます。
ここでは、ポート 1〜16 で 802.1X 認証を行うものとします。また、RADIUS サーバーは、VLAN「R」所属のポート 24（通常のポート）に接続されているものとします。

✎ 以下の例は、802.1X Supplicant を使用していますが、MAC ベース認証、Web 認証でも同様に動作します。

✎ Web 認証では、Web 認証サーバーの設定も必要です。「テンポラリー IP アドレスを利用する場合の設定例」を参照してください。

■ 構成



■ 認証サーバー (RADIUS サーバー) には、以下のように設定されているものとします。

User-Name	User-Password	Tunnel-Type	Tunnel-Medium-Type	Tunnel-Private-Group-ID	**備考**
user1	password1	VLAN (13)	IEEE-802 (6)	20	802.1X Supplicant 用のユーザー名/パスワードおよび、認証後に所属させるVLAN

表 18:

■ 設定

1. VLAN を作成します。

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

2. RADIUS サーバーを接続するポート 24 を VLAN「R」に割り当てます。

```
ADD VLAN=R PORT=24 ↵
```

3. RADIUS サーバーを使って認証を行うため、最初に RADIUS サーバーと通信するための設定をします。最初に、IP アドレスを設定します。

```
ADD IP INT=VLAN-R IP=192.168.10.5 MASK=255.255.255.0 ↵
```

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

```
ADD RADIUSSERVER SERVER=192.168.10.130 ORDER=1 PORT=1812 ACCPORT=1813
  SECRET=himitsu ↵
```

5. ポート認証機能を有効にします。

```
ENABLE PORTAUTH ↵
```

6. ポート 1〜16 で 802.1X 認証を行うよう設定します。SET PORTAUTH PORT コマンド（87 ページ）の「PORTAUTH=8021X TYPE=AUTHENTICATOR」の指定により、ポート 1 は 802.1X 認証の Authenticator ポートとなります。 また、「VLANASSIGNMENT=ENABLED」の指定により、ダイナミック VLAN を有効にします。

```
SET PORTAUTH=8021X PORT=1-16 TYPE=AUTHENTICATOR
  VLANASSIGNMENT=ENABLED ↵
```

✎ Authenticator ポートをタグ付きに設定することはできません。

✎ RADIUS サーバーを接続するポートは、Authenticator ポートにしないでください。SET PORTAUTH PORT コマンド（87 ページ）の TYPE/ROLE パラメーターを NONE に設定してください。

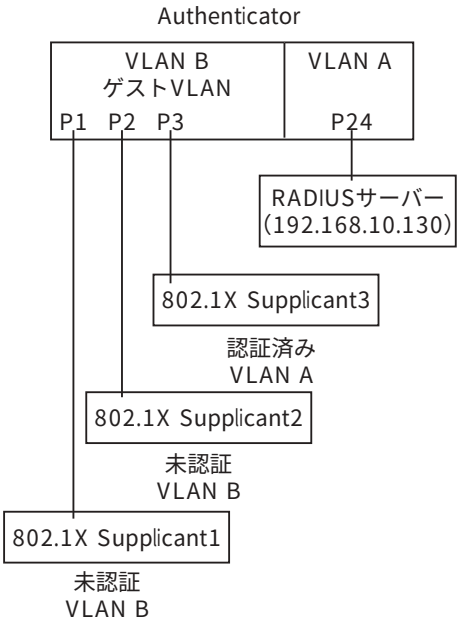
✎ Web 認証では、Web 認証サーバーの設定も必要です。「テンポラリー IP アドレスを利用する場合の設定例」を参照してください。

ゲスト VLAN の設定例

ゲスト VLAN を使用すると、認証前および、認証失敗した Supplicant が所属する VLAN を指定できます。以下の設定では、認証前および、認証失敗した 802.1X Supplicant は、VLAN-B に所属しています。
認証が成功すると、VLAN-A で通信が可能です。

✎ 以下の例は、802.1X Supplicant を使用していますが、MAC ベース認証、Web 認証でも同様に動作します。

■ 構成



■ 認証サーバー (RADIUS サーバー) には、以下のように設定されているものとします。

User-Name	User-Password	**備考**
user1	password1	802.1X Supplicant1 用のユーザー名/パスワード
user2	password2	802.1X Supplicant2 用のユーザー名/パスワード
user3	password3	802.1X Supplicant3 用のユーザー名/パスワード

表 19:

■ 設定

1. VLAN を作成します。

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

2. ゲスト VLAN を作成します。ルーティングさせないように、L2ONLY パラメーターを指定します。

   ```
   CREATE VLAN=B VID=20 L2ONLY ↵
   ```

3. RADIUS サーバーを接続するポート 24 を VLAN「A」に割り当てます。

   ```
   ADD VLAN=A PORT=24 ↵
   ```

4. RADIUS サーバーを使って認証を行うため、最初に RADIUS サーバーと通信するための設定をします。最初に、IP アドレスを設定します。

   ```
   ADD IP INT=VLAN-A IP=192.168.10.5 MASK=255.255.255.0 ↵
   ```

5. RADIUS サーバーを登録します。IP アドレスと UDP ポート、共有パスワードを指定します。

```
ADD RADIUSSERVER SERVER=192.168.10.130 ORDER=1 PORT=1812 ACCPORT=1813
  SECRET=himitsu ↵
```

6. ポート認証機能を有効にします。

```
ENABLE PORTAUTH ↵
```

7. ポート 1〜16 で 802.1X を行うよう設定します。SET PORTAUTH PORT コマンド（87 ページ）の「PORTAUTH=8021X TYPE=AUTHENTICATOR」の指定により、ポート 1 は 802.1X 認証の Authenticator ポートとなります。
「GUESTVLAN=20」の指定により、ゲスト VLAN は、VLAN-B となります。また、「VLANASSIGNMENTTYPE=USER」の指定により、接続している Supplicant ごとに、VLAN が割り当てられます。

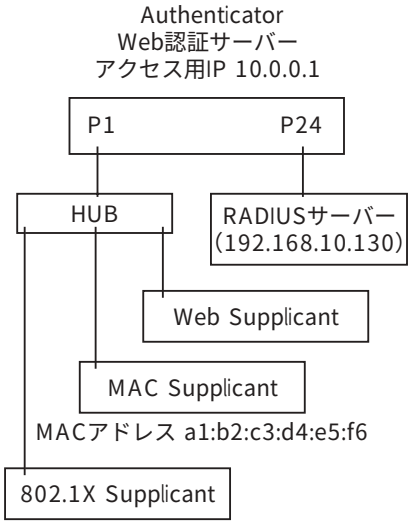
```
SET PORTAUTH=8021X PORT=1-16 TYPE=AUTHENTICATOR MODE=MULTI
  VLANASSIGNMENTTYPE=USER GUESTVLAN=20 ↵
```

✎ Multi-supplicant モードで ゲスト VLAN を使用する場合、「VLANASSIGNMENTTYPE=USER」に指定する必要があります。

認証方式の併用

同一ポート上に、複数の認証方式を設定することができます。

■ 構成



■ 認証サーバー (RADIUS サーバー) には、以下のように設定されているものとします。

User-Name	User-Password	備考

user1	password1	PC1 802.1X Supplicant 用のユーザー名 / パスワード
a1:b2:c3:d4:e5:f6	a1:b2:c3:d4:e5:f6	PC2 MAC Supplicant 用のユーザー名 / パスワード
user3	password3	PC3 WEB Supplicant 用のユーザー名 / パスワード

表 20:

■ 設定

1. RADIUS サーバーを使って認証を行うため、最初に RADIUS サーバーと通信するための設定をします。最初に、IP アドレスを設定します。

   ```
   ADD IP INT=VLAN1 IP=192.168.10.5 MASK=255.255.255.0 ↵
   ```

2. RADIUS サーバーを登録します。IP アドレスと UDP ポート、共有パスワードを指定します。

   ```
   ADD RADIUSSERVER SERVER=192.168.10.130 ORDER=1 PORT=1812 ACCPORT=1813
     SECRET=himitsu ↵
   ```

3. ポート認証機能を有効にします。

   ```
   ENABLE PORTAUTH ↵
   ```

4. ポート 1 で 802.1X 認証を行うよう設定します。SET PORTAUTH PORT コマンド（87 ページ）の「PORTAUTH=8021X TYPE=AUTHENTICATOR」の指定により、ポート 1 は 802.1X 認証の Authenticator ポートとなります。

   ```
   SET PORTAUTH=8021X PORT=1 TYPE=AUTHENTICATOR MODE=MULTI
     VLANASSIGNMENTTYPE=USER ↵
   ```

5. ポート 1 で MAC ベース認証を行うよう設定します。SET PORTAUTH PORT コマンド（87 ページ）の「PORTAUTH=MACBASED TYPE=AUTHENTICATOR」の指定により、ポート 1 は MAC ベース認証の Authenticator ポートとなります。同一ポートでの ポート認証のパラメーターの設定は 全認証方式で共通であるため、以下の設定で、MAC ベース認証でも「MODE=MULTI VLANASSIGNMENTTYPE=USER」で機能します。

   ```
   SET PORTAUTH=MACBASED PORT=1 TYPE=AUTHENTICATOR ↵
   ```

6. ポート 1 で Web 認証を行うよう設定します。SET PORTAUTH PORT コマンド（87 ページ）の「PORTAUTH=WEBBASED TYPE=AUTHENTICATOR」の指定により、ポート 1 は Web 認証の Authenticator ポートとなります。

   ```
   SET PORTAUTH=WEBBASED PORT=1 TYPE=AUTHENTICATOR ↵
   ```

7. Web 認証サーバーを設定します。IPADDRESS=10.0.0.1 の指定により、「http://10.0.0.1」でアクセス可能にします。

   ```
   SET WEBAUTHSERVER IPADDRESS=10.0.0.1 ↵
   ```

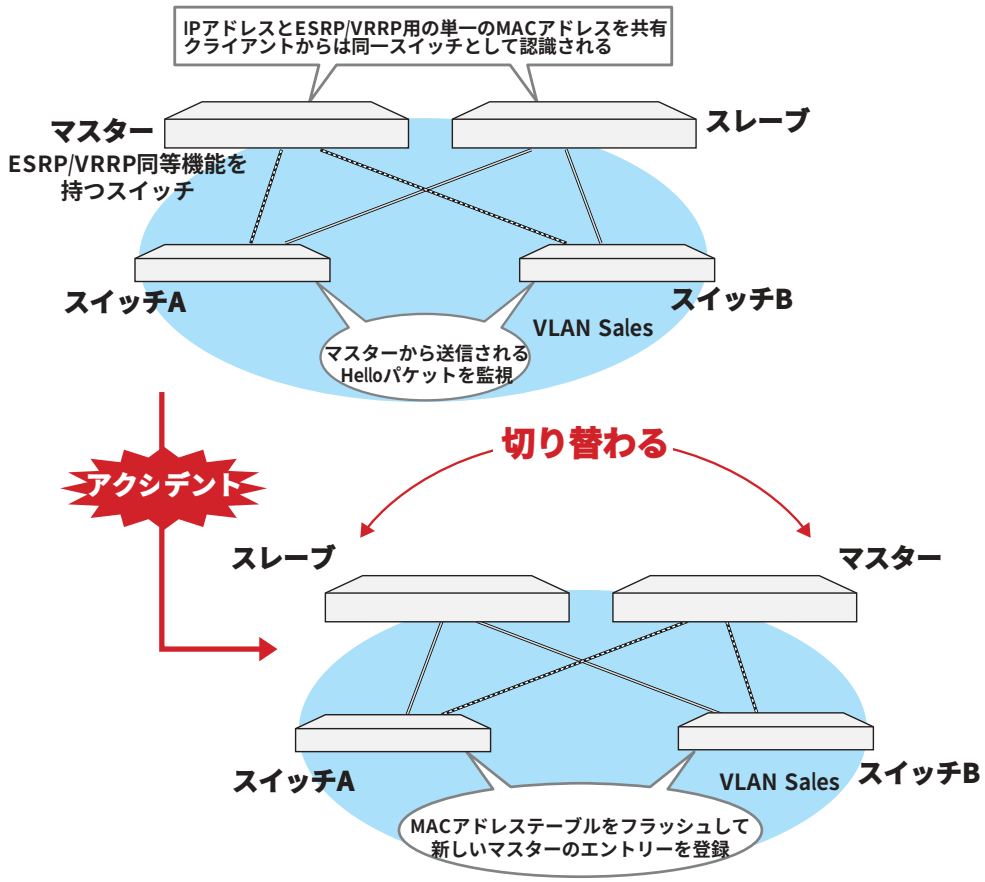
8. Web 認証サーバーを有効にします。

   ```
   ENABLE WEBAUTHSERVER ↵
   ```

RRP Snooping

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

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



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

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

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

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

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

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

■ RRP Snooping を有効にするには、ENABLE RRPSNOOPING コマンド（70 ページ）を使います。

```
ENABLE RRPSNOOPING ↵
```

■ RRP Snooping を無効にするには、DISABLE RRPSNOOPING コマンド（62 ページ）を使います。

```
DISABLE RRPSNOOPING ↵
```

■ RRP Snooping に関する設定を表示するには、SHOW RRPSNOOPING コマンド（138 ページ）を使います。

```
SHOW RRPSNOOPING ↵
```

RRP Snooping を有効にすると、学習機能により登録されたダイナミックエントリーが、フォワーディングデータベースから削除されます。

✎ RRP Snooping とマルチプルスパニングツリープロトコル、スパニングツリープロトコルは併用できません。

コマンドリファレンス編

機能別コマンド索引

一般コマンド

ポート

EPSR スヌーピング

ポート認証

RRP Snooping

ACTIVATE SWITCH PORT AUTONEGOTIATE

カテゴリー：スイッチング / ポート

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

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

解説

指定ポートでオートネゴシエーションプロセスを強制起動し、接続先ポートと通信モード（速度/デュプレックス）のネゴシエーションを行わせる。SET SWITCH PORT コマンドの RENEGOTIATION パラメーターに AUTO を指定したのと同義。

パラメーター

PORT　スイッチポート。複数指定が可能。通信モード（SET SWITCH PORT コマンドの SPEED パラメーター）が AUTONEGOTIATE に設定されているポートでのみ有効。

例

■ポート 6 にオートネゴシエーションを行わせる。

```
ACTIVATE SWITCH PORT=6 AUTONEGOTIATE
```

備考・注意事項

・本コマンドは、通信モードがオートネゴシエーション（AUTONEGOTIATE）に設定されているポートでのみ有効。

関連コマンド

SET SWITCH PORT（96 ページ）
SHOW SWITCH PORT（144 ページ）

ADD SWITCH TRUNK

カテゴリー：スイッチング / ポート

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

trunk: トランクグループ名（1〜16 文字。英数字が使用可能。大文字小文字を区別しない）
port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能)

解説

既存のトランクグループにポートを追加する。

パラメーター

TRUNK　トランクグループ名。

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

例

■トランクグループ「uplink」にポート 1〜4 を追加する。

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

関連コマンド

CREATE SWITCH TRUNK（55 ページ）
DELETE SWITCH TRUNK（57 ページ）
DESTROY SWITCH TRUNK（58 ページ）
SET SWITCH TRUNK（104 ページ）
SHOW SWITCH TRUNK（157 ページ）

CREATE SWITCH TRUNK

カテゴリー：スイッチング / ポート

CREATE SWITCH TRUNK=*trunk* PORT=*port-list* [SELECT={MACSRC|MACDEST|MACBOTH|IPSRC|IPDEST|IPBOTH}]

trunk: トランクグループ名（1〜16 文字。英数字が使用可能。大文字小文字を区別しない）
port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能)

解説

トランクグループを作成する。6 グループまで作成可能。

パラメーター

TRUNK トランクグループ名。

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

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

例

■ポート 1-5 にトランクグループ「uplink」を作成する。

```
CREATE SWITCH TRUNK=uplink port=1-5
```

備考・注意事項

・フラッディングパケットは、トランクグループ内で一番小さいポート番号のポートから送出される。
・トランクグループ ID は、自動的に 1 から順番に割り当てられる

関連コマンド

ADD SWITCH TRUNK（54 ページ）
DELETE SWITCH TRUNK（57 ページ）
DESTROY SWITCH TRUNK（58 ページ）

SET SWITCH TRUNK（104 ページ）
SHOW SWITCH TRUNK（157 ページ）

DELETE SWITCH TRUNK

カテゴリー：スイッチング / ポート

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

trunk: トランクグループ名（1〜16 文字。英数字が使用可能。大文字小文字を区別しない）
port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能)

解説

トランクグループからポートを削除する。

パラメーター

TRUNK　トランクグループ名。
PORT　削除するポートの一覧。

例

■トランクグループ「uplink」からポート 1、2 を削除する。

```
DELETE SWITCH TRUNK=uplink PORT=1,2
```

関連コマンド

ADD SWITCH TRUNK（54 ページ）
CREATE SWITCH TRUNK（55 ページ）
DESTROY SWITCH TRUNK（58 ページ）
SET SWITCH TRUNK（104 ページ）
SHOW SWITCH TRUNK（157 ページ）

DESTROY SWITCH TRUNK

カテゴリー：スイッチング / ポート

DESTROY SWITCH TRUNK=*trunk*

trunk: トランクグループ名（1〜16 文字。英数字が使用可能。大文字小文字を区別しない）

解説

トランクグループを削除する。

パラメーター

TRUNK　トランクグループ名。

例

■トランクグループ「uplink」を削除する。

```
DESTROY SWITCH TRUNK=uplink
```

関連コマンド

ADD SWITCH TRUNK（54 ページ）
CREATE SWITCH TRUNK（55 ページ）
DELETE SWITCH TRUNK（57 ページ）
SET SWITCH TRUNK（104 ページ）
SHOW SWITCH TRUNK（157 ページ）

DISABLE EPSRSNOOPING

カテゴリー：スイッチング / EPSR スヌーピング

DISABLE EPSRSNOOPING [CONTROLVLAN={*1..4094*|*vlanname*|ALL}]

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

解説

指定したコントロール VLAN 上の制御メッセージ監視を無効にする。デフォルトは無効。

関連コマンド

ENABLE EPSRSNOOPING（67 ページ）
SHOW EPSRSNOOPING（108 ページ）

DISABLE PORTACCESS

カテゴリー：スイッチング / ポート認証

DISABLE PORTACCESS

解説

ポート認証機能（802.1X 認証、MAC ベース認証、Web 認証）を無効にする。デフォルトは無効。DISABLE PORTAUTH コマンドは同義。

関連コマンド

ENABLE PORTACCESS（68 ページ）
SHOW PORTACCESS（109 ページ）
SHOW PORTACCESS PORT（117 ページ）

DISABLE PORTAUTH

カテゴリー：スイッチング / ポート認証

DISABLE PORTAUTH

解説

ポート認証機能（802.1X 認証、MAC ベース認証、Web 認証）を無効にする。デフォルトは無効。DISABLE PORTACCESS コマンドは同義。

関連コマンド

ENABLE PORTAUTH（69 ページ）
SHOW PORTAUTH（123 ページ）
SHOW PORTAUTH PORT（131 ページ）

DISABLE RRPSNOOPING

カテゴリー：スイッチング / RRP Snooping

DISABLE RRPSNOOPING

解説

RRP Snooping を無効にする。デフォルトは無効。

関連コマンド

ENABLE RRPSNOOPING（70 ページ）
SHOW RRPSNOOPING（138 ページ）

DISABLE SWITCH PORT

カテゴリー：スイッチング / ポート

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

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

解説

スイッチポートをディセーブルにする。SET SWITCH PORT コマンドの STATUS パラメーターに DISABLE を指定したのと同義。

パラメーター

PORT　ポート番号。

関連コマンド

ENABLE SWITCH PORT（71 ページ）
SHOW SWITCH PORT（144 ページ）

DISABLE SWITCH PORT FLOW

カテゴリー：スイッチング / ポート

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

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

解説

指定したスイッチポートでフローコントロール（802.3x PAUSE）を無効にする。デフォルトは無効。SET SWITCH PORT コマンドの FLOWCONTROL パラメーターに DISABLE を指定したのと同義。

パラメーター

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

備考・注意事項

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

関連コマンド

ENABLE SWITCH PORT FLOW（72 ページ）
SHOW SWITCH PORT（144 ページ）

DISABLE SWITCH PORT STORMDETECTION

カテゴリー：スイッチング / ポート

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

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。指定したポートが存在しない場合はエラーとなる。

例

■ポート 2 の受信レート検出機能を無効にする

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

関連コマンド

ENABLE SWITCH PORT STORMDETECTION（73 ページ）
RESET SWITCH PORT STORMDETECTION COUNTER（78 ページ）
SET SWITCH PORT STORMDETECTION（102 ページ）
SHOW SWITCH PORT STORMDETECTION（154 ページ）

DISABLE WEBAUTHSERVER

カテゴリー：スイッチング / ポート認証

DISABLE WEBAUTHSERVER

解説

Web 認証サーバーを無効にする。デフォルトは無効。

関連コマンド

ENABLE WEBAUTHSERVER（74 ページ）
SHOW PORTAUTH（123 ページ）
SHOW PORTAUTH PORT（131 ページ）

ENABLE EPSRSNOOPING

カテゴリー：スイッチング / EPSR スヌーピング

ENABLE EPSRSNOOPING CONTROLVLAN={***1..4094***|***vlanname***}

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

解説

指定したコントロール VLAN 上の制御メッセージ監視を有効にする。デフォルトは無効。

関連コマンド

DISABLE EPSRSNOOPING（59 ページ）
SHOW EPSRSNOOPING（108 ページ）

ENABLE PORTACCESS

カテゴリー：スイッチング / ポート認証

ENABLE PORTACCESS

解説

ポート認証機能（802.1X 認証、MAC ベース認証、Web 認証）を有効にする。デフォルトは無効。ENABLE PORTAUTH コマンドは同義。

関連コマンド

DISABLE PORTACCESS（60 ページ）
SHOW PORTACCESS（109 ページ）
SHOW PORTACCESS PORT（117 ページ）

ENABLE PORTAUTH

カテゴリー：スイッチング / ポート認証

ENABLE PORTAUTH

解説

ポート認証機能（802.1X 認証、MAC ベース認証、Web 認証）を有効にする。デフォルトは無効。ENABLE PORTACCESS コマンドは同義。

関連コマンド

DISABLE PORTAUTH（61 ページ）
SHOW PORTAUTH（123 ページ）
SHOW PORTAUTH PORT（131 ページ）

ENABLE RRPSNOOPING

カテゴリー：スイッチング / RRP Snooping

ENABLE RRPSNOOPING

解説

RRP Snooping を無効にする。デフォルトは無効。

関連コマンド

DISABLE RRPSNOOPING（62 ページ）
SHOW RRPSNOOPING（138 ページ）

ENABLE SWITCH PORT

カテゴリー：スイッチング / ポート

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

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

解説

スイッチポートをイネーブルにする。デフォルトはイネーブル。SET SWITCH PORT コマンドの STATUS パラメーターに ENABLE を指定したのと同義。

パラメーター

PORT　ポート番号。

関連コマンド

DISABLE SWITCH PORT（63 ページ）
SHOW SWITCH PORT（144 ページ）

ENABLE SWITCH PORT FLOW

カテゴリー：スイッチング / ポート

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

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

解説

指定したスイッチポートでフローコントロール（802.3x PAUSE）を有効にする。デフォルトは無効。SET SWITCH PORT コマンドの FLOWCONTROL パラメーターに ENABLE を指定したのと同義。

パラメーター

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

備考・注意事項

・本製品の実装では、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。

関連コマンド

DISABLE SWITCH PORT FLOW（64 ページ）
SHOW SWITCH PORT（144 ページ）

ENABLE SWITCH PORT STORMDETECTION

カテゴリー：スイッチング / ポート

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

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。指定したポートが存在しない場合はエラーとなる

例

■ポート 2 の受信レート検出機能を有効にする

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

関連コマンド

DISABLE SWITCH PORT STORMDETECTION（65 ページ）
RESET SWITCH PORT STORMDETECTION COUNTER（78 ページ）
SET SWITCH PORT STORMDETECTION（102 ページ）
SHOW SWITCH PORT STORMDETECTION（154 ページ）

ENABLE WEBAUTHSERVER

カテゴリー：スイッチング / ポート認証

ENABLE WEBAUTHSERVER

解説

Web 認証サーバーを有効にする。デフォルトは無効。

関連コマンド

DISABLE WEBAUTHSERVER（66 ページ）
SHOW PORTAUTH（123 ページ）
SHOW PORTAUTH PORT（131 ページ）

PURGE SWITCH

カテゴリー：スイッチング / 一般コマンド

PURGE 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

ポートの設定情報をすべて消去する。

例

■すべてのポートの設定情報を消去する

```
PURGE SWITCH   PORT=ALL
```

関連コマンド

SHOW SWITCH（139 ページ）
SHOW SWITCH FDB（「フォワーディングデータベース」の 15 ページ）

RESET SWITCH

カテゴリー：スイッチング / 一般コマンド

RESET SWITCH

解説

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

関連コマンド

SHOW SWITCH（139 ページ）
SHOW SWITCH FDB（「フォワーディングデータベース」の 15 ページ）

RESET SWITCH PORT

カテゴリー：スイッチング / ポート

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

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

解説

スイッチポートをハードウェア的にリセットする。
リセットを実行すると、(1) 送受信キュー内のパケットを破棄し、(2) オートネゴシエーションプロセスを開始し、(3) ポートの統計カウンターをクリアする。

パラメーター

PORT　ポート番号。
COUNTER　統計カウンターだけをリセットしたいときに指定する。

関連コマンド

DISABLE SWITCH PORT（63 ページ）
ENABLE SWITCH PORT（71 ページ）
SHOW SWITCH PORT（144 ページ）

RESET SWITCH PORT STORMDETECTION COUNTER

カテゴリー：スイッチング / ポート

RESET SWITCH PORT={***port-list***|**ALL**} **STORMDETECTION 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。省略時は ALL。指定したポートが存在しない場合はエラーとする。

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 PORT=2 STORMDETECTION COUNTER
```

関連コマンド

DISABLE SWITCH PORT STORMDETECTION（65 ページ）
ENABLE SWITCH PORT STORMDETECTION（73 ページ）
SET SWITCH PORT STORMDETECTION（102 ページ）
SHOW SWITCH PORT STORMDETECTION（154 ページ）

SET PORTACCESS AUTHMETHOD

カテゴリー：スイッチング / ポート認証

SET PORTACCESS AUTHMETHOD[=RadiusEAP]

解説

802.1X 認証モジュールの認証プロトコルを設定する。SET PORTAUTH AUTHMETHOD コマンドは同義。

パラメーター

AUTHMETHOD　認証プロトコル。RadiusEAP を指定。

関連コマンド

SHOW PORTACCESS（109 ページ）
SHOW PORTACCESS PORT（117 ページ）

SET PORTACCESS PORT

カテゴリー：スイッチング / ポート認証

SET PORTAUTH[={ALL|8021X|MACBASED|WEBBASED}]

PORT={***port-list***|**ALL**} {**TYPE**|**ROLE**}**=AUTHENTICATOR** [CONTROL={AUTHORISED|
UNAUTHORISED|AUTO|FORCEAUTHENTICATE|FORCEUNAUTHENTICATE}]
[QUIETPERIOD=*0..65535*] [TXPERIOD=*1..65535*] [REAUTHPERIOD=*1..65535*]
[SUPPTIMEOUT=*1..600*] [{SERVERTIMEOUT|SERVTIMEOUT}=*1..600*]
[CTRLDIRBOTH={INGRESS|BOTH}] [REAUTHENABLED={ENABLED|DISABLED}]
[PIGGYBACK={ENABLED|DISABLED}] [MODE={SINGLE|MULTI}] [SUPPLIMIT=*1..320*]
[VLANASSIGNMENT={ENABLED|DISABLED}] [SECUREVLAN={ON|OFF}] [MAXREQ=*1..10*]
[GUESTVLAN={*vlanname*|*1..4094*|NONE}] [VLANASSIGNMENTTYPE={PORT|USER}]
[MAXREAUTHREQ=*1..10*] [ARPFORWARDING={ENABLED|DISABLED}]
[TCPPORTFORWARDING={*1..65535*|ALL|NONE}] [UDPPORTFORWARDING={*1..65535*|ALL|
NONE}] [PORTMOVEREAUTH={ENABLED|DISABLED}] [LOCKCOUNT=*0..10*]

[802.1X 認証 Authenticator 有効時]

SET PORTAUTH[=*8021 *] **PORT=**{***port-list***|**ALL**} {**TYPE**|**ROLE**}**=AUTHENTICATOR**

[802.1X 認証 Supplicant 時]

SET PORTAUTH[=8021X] **PORT=**{***port-list***|**ALL**} {**TYPE**|**RULR**}**=SUPPLICANT**
[AUTHPERIOD=*1..300*] [HELDPERIOD=*0..65535*] [MAXSTART=*1..10*]
[STARTPERIOD=*1..60*] [USERNAME=*login-name*] [PASSWORD=*password*]

[MAC ベース認証 有効時]

SET PORTAUTH=MACBASED PORT={***port-list***|**ALL**} {**TYPE**|**ROLE**}**=AUTHENTICATOR**

[WEB ベース認証 有効時]

SET PORTAUTH=WEBBASED PORT={***port-list***|**ALL**} {**TYPE**|**ROLE**}**=AUTHENTICATOR**

[認証ポートの解除]

SET PORTAUTH=ALL PORT={***port-list***|**ALL**} {**TYPE**|**ROLE**}**=NONE**

SET PORTAUTH=8021X PORT={***port-list***|**ALL**} {**TYPE**|**ROLE**}**=NONE**

SET PORTAUTH=MACBASED PORT={*port-list*|ALL} {TYPE|ROLE}=NONE

SET PORTAUTH=WEBBASED PORT={*port-list*|ALL} {TYPE|ROLE}=NONE

port-list: スイッチポート番号（1〜。ハイフン、カンマを使った複数指定も可能）
login-name: ログイン名（1〜63 文字。英数字のみ使用可能）
password: パスワード（1〜63 文字。英数字のみ使用可能）

解説

指定ポートにおけるポート認証機能（802.1X 認証、MAC ベース認証、Web 認証）の設定を変更する。SET PORTAUTH PORT コマンドは同義。TYPE の設定は認証メカニズムごとに設定できる。それ以外のパラメーターは全認証メカニズムで共通の値となる。

パラメーター

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

PORT スイッチポート。複数指定が可能。

TYPE/ROLE スイッチポートの役割。AUTHENTICATOR（802.1X 認証、MAC ベース認証の Authenticator ポート、Web 認証の Authenticator ポート）、SUPPLICANT（802.1X 認証の Supplicant ポート）、NONE（802.1X 認証機能無効）のいずれかを指定する。

MODE （802.1X Authenticator ポート、MAC ベース認証ポート、Web 認証ポート）Supplicant が 1 台だけ接続されていることを想定した Single-Supplicant モード（MODE=SINGLE）と、Supplicant が複数台接続されていることを想定した Multi-Supplicant モード（MODE=MULTI）がある。Single-Supplicant モードでは、該当ポート配下に最初に接続された Supplicant だけが認証対象となる（その他の Supplicant からの通信を許可するかどうかは、PIGGYBACK パラメーターで制御可能）。Multi-Supplicant モードでは、該当ポート配下に接続された個々の Supplicant を識別し、個別に認証を行う。802.1X Authenticator ポートのデフォルトは SINGLE。MAC ベース認証ポートと Web 認証ポートでは、Multi-Supplicant モード (MODE=MULTI) のみ有効で、MODE を省略した場合は自動的に Multi-Supplicant モードとなる。Ver2.3.1 以前の Single-Supplicant モード (MODE=SINGLE) と同様の動作をさせるには、MODE=MULTI SUPPLIMIT=1 を指定する。また Ver2.3.1 以前のファームの設定スクリプトファイルの対応で MAC ベース認証で Single-Supplicant モード (MODE=SINGLE) を指定した場合、Ver2.4.1 では自動的に Multi-Supplicant モードの 1 ユーザーのみ認証可能な設定 (MODE=MULTI SUPPLIMIT=1) に変更される

GUESTVLAN （802.1X Authenticator ポート、MAC ベース認証ポート、Web 認証ポート）ゲスト VLAN を指定する。ゲスト VLAN に指定する VLAN は、認証前にルーティングさせないようにするため、L2ONLY VLAN（CREATE VLAN コマンドで、L2ONLY パラメーターを指定して作成）でなければならない。VLAN 名または VLAN ID を指定する。NONE はゲスト VLAN を使用しないことを意味する。NONE 以外を指定すると直ちにゲスト VLAN の所属となる。認証が成功するとゲスト VLAN から他の VLAN の所属となる。認証に失敗すると、またゲスト VLAN の所属となる。また、

ゲスト VLAN が指定されていた場合、Web 認証でログインしてから、認証結果画面が表示されるまでに 待機時間が発生する。待機時間 (SET WEBAUTHSERVER コマンドの RENEWALTIME × 3 + 5) 秒。Multi-Supplicant モード (MODE=MULTI) では NONE 以外に指定できない。デフォルトは NONE

VLANASSIGNMENTTYPE （802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート、Web 認証ポート）ダイナミック VLAN をポート単位で設定するか、ユーザー (MAC アドレス) 単位で設定するかを指定する。 デフォルトは PORT。MODE=MULTI、VLANASSIGNMENT=ENABLED のときに有効になる。

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

ARPFORWARDING （Web 認証ポートで有効）未認証状態で、ARP パケットを受信したときに 透過するか破棄するかを指定する。 ENABLED は透過する、DISABLED は破棄する。デフォルトは DISABLED。

TCPPORTFORWARDING （Web 認証ポートで有効）未認証状態で、透過する TCP ポートのパケットを指定する。複数指定や ALL 指定が可能。デフォルトは NONE。入力は文字列 (1〜100 文字。使用可能な文字は半角英数字、半角記号（- ,）)

UDPPORTFORWARDING （Web 認証ポートで有効）未認証状態で、透過する UDP ポートのパケットを指定する。複数指定や ALL 指定が可能。デフォルトは NONE。入力は文字列（1〜100 文字。使用可能な文字は半角英数字、半角記号（- ,））

PORTMOVEREAUTH （802.1X Authenticator ポート、MAC ベース認証ポート、Web 認証ポートで有効）認証済みの Supplicant がポートを移動したときに、再度、認証を行うかを指定する。ENABLED のときは認証を行わずに認証済みとなり、DISABLED のときは認証を行う。デフォルトは DISABLED。

LOCKCOUNT （Web 認証ポートで有効） Web 認証において、Held の状態になるまでの 認証の連続失敗回数を指定する。 3 を指定した場合、Web 認証で、3 回 ログインに失敗すると Held の状態になる。デフォルトは 3。

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

CONTROL （802.1X Authenticator ポート、MAC ベース認証ポート、Web 認証ポート）手動設定による Authenticator ポートの状態。AUTO（認証結果に応じて変動）、UNAUTHORISED（未認証固定。FORCEUNAUTHENTICATE 同じ）、AUTHORISED（認証済み固定。FORCEAUTHENTICATE 同じ）から選択する。デフォルトは AUTO。通常は AUTO のままでよい。

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

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

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

REAUTHPERIOD （802.1X Authenticator ポート、MAC ベース認証ポート、Web 認証ポート）Supplicant の再認証間隔（秒）。デフォルトは 3600 秒。

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

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

CTRLDIRBOTH （802.1X Single-Supplicant Authenticator ポート）未認証状態で、送受信したブロードキャストまたはマルチキャストパケットをどう扱うか。INGRESS（未認証のクライアントから受信したパケットは廃棄するが、クライアントへの送信は行う）、または、BOTH（受信パケットも送信パケットも廃棄する）のいずれかを指定する。MODE=SINGLE の場合、または、ゲスト VLAN を設定している場合は INGRESS 固定に設定される。

REAUTHENABLED （802.1X Authenticator ポート、MAC ベース認証ポート、Web 認証ポート）802.1X Authenticator ポートと MAC ベース認証ポートでは、Supplicant ポートの再認証を行うかどうかを選択する。ENABLED（再認証を行う）または DISABLED（再認証を行わない）から選択する。Web 認証ポートでは、REAUTHPERIOD の時間経過後に 未認証にするか、しないかを選択する。ENABLED の場合は未認証にし、DISABLED の場合は未認証にせず、認証を継続する。デフォルトは ENABLED。

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

SUPPLIMIT （802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート、Web 認証ポート）Multi-Supplicant モード（MODE=MULTI）のとき、認証可能な Supplicant の最大数を指定する。デフォルトは 320。

VLANASSIGNMENT （802.1X Authenticator ポート、MAC ベース認証ポート、Web 認証ポート）ダイナミック VLAN の有効・無効。有効時は、RADIUS サーバーが返してきた Tunnel-Private-Group-ID の値をもとに、指定ポートの所属 VLAN を動的に変更する。また、有効時、Web 認証でログインしてから、認証結果画面が表示されるまでに待機時間が発生する。 待機時間 (SET WEBAUTHSERVER コマンドの RENEWALTIME × 3 + 5) 秒。デフォルトは ENABLED。

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

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

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

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

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

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

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

備考・注意事項

・TYPE / ROLE パラメーターに NONE を指定すると、指定ポートの設定をデフォルトに戻すことができるが、このとき、PORTAUTH / PORTACCESS パラメーターに認証メカニズム（802.1X / MACBASED / WEBBASED）を指定する必要はない。

・サポートサプリカント数はすべての認証メカニズムを合わせて、320 / PORT、480 / SWITCH である。

・認証メカニズムは同時に実行（RADIUS サーバーと通信）することはできない。1 つの認証メカニズムが実行中の場合、他は待ち状態となる。

・MAC 認証 / Web 認証と併用した場合は 802.1X も必ず Multi-Supplicant モードとなる。

・1 つの認証メカニズムで認証が成功すれば、認証許可状態となる。

・MAC 認証を有効にしている場合は必ず MAC 認証が最初に実行される。

・802.1X / MAC 認証を併用した場合、MAC 認証で HELD になると同時に EAP-request を Supplicant に送信する。

・802.1X / MAC 認証は 1 回目の HELD で HELD 状態となる。Web 認証は 3 回連続で HELD となった場合に HELD 状態となる。HELD 期間は QUIETPERIOD パラメーターに依存する。HELD 状態は 1 つの認証メカニズムで認証が成功すれば、解除される。

・802.1X / Web 認証では Connecting 時に「ユーザー名」と「パスワード」を入力させるタイミングが存在する。入力されてボタンが押されるまでは他の認証アルゴリズムを実行することができる。

・802.1X / MAC 認証は REAUTHPERIOD パラメーターで設定した再認証間隔を過ぎると再認証を実行し、HELD になった場合、未認証状態となる。Web 認証は再認証間隔を過ぎると強制的に未認証状態となる。

・802.1X / MAC 認証において再認証は認証に成功した認証メカニズムに対して HELD となった場合にのみ未認証状態となる。

・802.1X はスタティック MAC アドレスとして登録される。MAC 認証 / Web 認証はダイナミック MAC アドレスとして登録されるため、通信がなかった場合、FDB Ageout で認証が解除される。

・1 つの認証メカニズムが HELD → CONNECTING になった時、他の認証メカニズムが CONNECTING であれば、Supplicant 情報は削除される。

・認証アルゴリズムを併用し、ひとつの認証アルゴリズムで認証許可状態となった場合、その認証が解除されるまで、他の認証アルゴリズムは動作しない。

・Web 認証設定時、Connecting 状態で Supptimeout SuppAgeout(300s 固定) 期間中にアクセスがない場合、Supplicant は削除される。

・MAC 認証は mode=single を設定した場合、 Multi-Supplicant Mode / supplicant limit=1 として実行される。その時、WARNING メッセージが表示される。

・Web 認証でダイナミック VLAN 有効時 か PVID 以外の ゲスト VLAN 設定時、Login ボタンが押されてから、実際に RADIUS に Access-Request を送信するまでに 3 秒 待機 (※ 1) する。Authenticating の画面 (<認証中 1 >画面) 表示し、(RenewalTime × 3 + 5) 秒 待機 (※ 2) 後に認証結果の画面を表示する。

※ 1 Authenticating 画面を確実に表示させるため。

※ 2 VLAN が変更された場合に、DHCP サーバーから新たに IP アドレスを取得するため。

・Web 認証で Supplicant が DHCP Server から IP アドレスを取得していて、ダイナミック VLAN 有効設定 もしくはゲスト VLAN 設定がされている場合は、Supplicant の認証を解除後、IP アドレスを再取得する必要がある。
・TYPE 以外のパラメーターは ポートごとに 全メカニズム共通で設定される。
・MAC 認証が HELD 以外の状態で、Web 認証の Login を行うと、認証失敗画面が表示されずに Login が表示される。この認証の失敗は、失敗回数 (lockcount) にカウントされない。
・MAC 認証 / Web 認証は認証成功後、FDB 上の MAC アドレスが Age Out などでクリアされると、認証登録もクリアされる。
・Authenticator ポートにて、Supplicant の登録がない場合、show portauth status で Attached Supplicant(s) 情報は表示しない。

関連コマンド

SHOW PORTACCESS（109 ページ）
SHOW PORTACCESS PORT（117 ページ）

SET PORTAUTH AUTHMETHOD

カテゴリー：スイッチング / ポート認証

SET PORTAUTH AUTHMETHOD[=RadiusEAP]

解説

802.1X 認証モジュールの認証プロトコルを設定する。SET PORTACCESS AUTHMETHOD コマンドは同義。

パラメーター

AUTHMETHOD　認証プロトコル。RadiusEAP を指定。

関連コマンド

SHOW PORTAUTH（123 ページ）
SHOW PORTAUTH PORT（131 ページ）

SET PORTAUTH PORT

カテゴリー：スイッチング / ポート認証

SET PORTAUTH[={ALL|8021X|MACBASED|WEBBASED}]

PORT={***port-list***|**ALL**} {**TYPE**|**ROLE**}**=AUTHENTICATOR** [CONTROL={AUTHORISED|
UNAUTHORISED|AUTO|FORCEAUTHENTICATE|FORCEUNAUTHENTICATE}]
[QUIETPERIOD=*0..65535*] [TXPERIOD=*1..65535*] [REAUTHPERIOD=*1..65535*]
[SUPPTIMEOUT=*1..600*] [{SERVERTIMEOUT|SERVTIMEOUT}=*1..600*]
[CTRLDIRBOTH={INGRESS|BOTH}] [REAUTHENABLED={ENABLED|DISABLED}]
[PIGGYBACK={ENABLED|DISABLED}] [MODE={SINGLE|MULTI}] [SUPPLIMIT=*1..320*]
[VLANASSIGNMENT={ENABLED|DISABLED}] [SECUREVLAN={ON|OFF}] [MAXREQ=*1..10*]
[GUESTVLAN={*vlanname*|*1..4094*|NONE}] [VLANASSIGNMENTTYPE={PORT|USER}]
[MAXREAUTHREQ=*1..10*] [ARPFORWARDING={ENABLED|DISABLED}]
[TCPPORTFORWARDING={*1..65535*|ALL|NONE}] [UDPPORTFORWARDING={*1..65535*|ALL|
NONE}] [PORTMOVEREAUTH={ENABLED|DISABLED}] [LOCKCOUNT=*0..10*]

[802.1X 認証 Authenticator 有効時]

SET PORTAUTH[=*8021*] **PORT=**{***port-list***|**ALL**} {**TYPE**|**ROLE**}**=AUTHENTICATOR**

[802.1X 認証 Supplicant 時]

SET PORTAUTH[=8021X] **PORT=**{***port-list***|**ALL**} {**TYPE**|**RULR**}**=SUPPLICANT**
[AUTHPERIOD=*1..300*] [HELDPERIOD=*0..65535*] [MAXSTART=*1..10*]
[STARTPERIOD=*1..60*] [USERNAME=*login-name*] [PASSWORD=*password*]

[MAC ベース認証 有効時]

SET PORTAUTH=MACBASED PORT={***port-list***|**ALL**} {**TYPE**|**ROLE**}**=AUTHENTICATOR**

[WEB ベース認証 有効時]

SET PORTAUTH=WEBBASED PORT={***port-list***|**ALL**} {**TYPE**|**ROLE**}**=AUTHENTICATOR**

[認証ポートの解除]

SET PORTAUTH[={8021X|MACBASED|WEBBASED|ALL}] **PORT=**{***port-list***|**ALL**} {**TYPE**|
ROLE}**=NONE**

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

login-name: ログイン名（1〜63 文字。英数字のみ使用可能）
password: パスワード（1〜63 文字。英数字のみ使用可能）

解説

指定ポートにおけるポート認証機能（802.1X 認証、MAC ベース認証、Web 認証）の設定を変更する。SET PORTACCESS PORT コマンドは同義。TYPE の設定は認証メカニズムごとに設定できる。それ以外のパラメーターは全認証メカニズムで共通の値となる。

パラメーター

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

PORT スイッチポート。複数指定が可能。

TYPE/ROLE スイッチポートの役割。AUTHENTICATOR（802.1X 認証、MAC ベース認証の Authenticator ポート、Web 認証の Authenticator ポート）、SUPPLICANT（802.1X 認証の Supplicant ポート）、NONE（802.1X 認証機能無効）のいずれかを指定する。

MODE （802.1X Authenticator ポート、MAC ベース認証ポート、Web 認証ポート）Supplicant が 1 台だけ接続されていることを想定した Single-Supplicant モード（MODE=SINGLE）と、Supplicant が複数台接続されていることを想定した Multi-Supplicant モード（MODE=MULTI）がある。Single-Supplicant モードでは、該当ポート配下に最初に接続された Supplicant だけが認証対象となる（その他の Supplicant からの通信を許可するかどうかは、PIGGYBACK パラメーターで制御可能）。Multi-Supplicant モードでは、該当ポート配下に接続された個々の Supplicant を識別し、個別に認証を行う。802.1X Authenticator ポートのデフォルトは SINGLE。MAC ベース認証ポートと Web 認証ポートでは、Multi-Supplicant モード (MODE=MULTI) のみ有効で、MODE を省略した場合は自動的に Multi-Supplicant モードとなる。Ver2.3.1 以前の Single-Supplicant モード (MODE=SINGLE) と同様の動作をさせるには、MODE=MULTI SUPPLIMIT=1 を指定する。また Ver2.3.1 以前のファームの設定スクリプトファイルの対応で MAC ベース認証で Single-Supplicant モード (MODE=SINGLE) を指定した場合、Ver2.4.1 では自動的に Multi-Supplicant モードの 1 ユーザーのみ認証可能な設定 (MODE=MULTI SUPPLIMIT=1) に変更される

GUESTVLAN （802.1X Authenticator ポート、MAC ベース認証ポート、Web 認証ポート）ゲスト VLAN を指定する。ゲスト VLAN に指定する VLAN は、認証前にルーティングさせないようにするため、L2ONLY VLAN（CREATE VLAN コマンドで、L2ONLY パラメーターを指定して作成）でなければならない。VLAN 名または VLAN ID を指定する。NONE はゲスト VLAN を使用しないことを意味する。NONE 以外を指定すると直ちにゲスト VLAN の所属となる。認証が成功するとゲスト VLAN から他の VLAN の所属となる。認証に失敗すると、またゲスト VLAN の所属となる。また、ゲスト VLAN が指定されていた場合、Web 認証でログインしてから、認証結果画面が表示されるまでに 待機時間が発生する。待機時間 (SET WEBAUTHSERVER コマンドの RENEWALTIME × 3 + 5) 秒。Multi-Supplicant モード (MODE=MULTI) では NONE 以外に指定できない。デフォルトは NONE

VLANASSIGNMENTTYPE （802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポー

ト、Web 認証ポート）ダイナミック VLAN をポート単位で設定するか、ユーザー (MAC アドレス) 単位で設定するかを指定する。 デフォルトは PORT。MODE=MULTI、VLANASSIGNMENT=ENABLED のときに有効になる。

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

ARPFORWARDING （Web 認証ポートで有効）未認証状態で、ARP パケットを受信したときに 透過するか破棄するかを指定する。 ENABLED は透過する、DISABLED は破棄する。デフォルトは DISABLED。

TCPPORTFORWARDING （Web 認証ポートで有効）未認証状態で、透過する TCP ポートのパケットを指定する。複数指定や ALL 指定が可能。デフォルトは NONE。入力は文字列 (1〜100 文字。使用可能な文字は半角英数字、半角記号（- ,）)

UDPPORTFORWARDING （Web 認証ポートで有効）未認証状態で、透過する UDP ポートのパケットを指定する。複数指定や ALL 指定が可能。デフォルトは NONE。入力は文字列（1〜100 文字。使用可能な文字は半角英数字、半角記号（- ,））

PORTMOVEREAUTH （802.1X Authenticator ポート、MAC ベース認証ポート、Web 認証ポートで有効）認証済みの Supplicant がポートを移動したときに、再度、認証を行うかを指定する。ENABLED のときは認証を行わずに認証済みとなり、DISABLED のときは認証を行う。デフォルトは DISABLED。

LOCKCOUNT （Web 認証ポートで有効） Web 認証において、Held の状態になるまでの 認証の連続失敗回数を指定する。 3 を指定した場合、Web 認証で、3 回 ログインに失敗すると Held の状態になる。デフォルトは 3。

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

CONTROL （802.1X Authenticator ポート、MAC ベース認証ポート、Web 認証ポート）手動設定による Authenticator ポートの状態。AUTO（認証結果に応じて変動）、UNAUTHORISED（未認証固定。FORCEUNAUTHENTICATE 同じ）、AUTHORISED（認証済み固定。FORCEAUTHENTICATE 同じ）から選択する。デフォルトは AUTO。通常は AUTO のままでよい。

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

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

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

REAUTHPERIOD （802.1X Authenticator ポート、MAC ベース認証ポート、Web 認証ポート）Supplicant の再認証間隔（秒）。デフォルトは 3600 秒。

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

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

CTRLDIRBOTH （802.1X Single-Supplicant Authenticator ポート）未認証状態で、送受信したブロードキャストまたはマルチキャストパケットをどう扱うか。INGRESS（未認証のクライアントから受信したパケットは廃棄するが、クライアントへの送信は行う）、または、BOTH（受信パケットも送信パケットも廃棄する）のいずれかを指定する。MODE=MULTI の場合、または、ゲスト VLAN を設定している場合は INGRESS 固定に設定される。MODE=SINGLE の場合、または、ゲスト VLAN を設定していない場合に設定が有効。

REAUTHENABLED （802.1X Authenticator ポート、MAC ベース認証ポート、Web 認証ポート）802.1X Authenticator ポートと MAC ベース認証ポートでは、Supplicant ポートの再認証を行うかどうかを選択する。ENABLED（再認証を行う）または DISABLED（再認証を行わない）から選択する。Web 認証ポートでは、REAUTHPERIOD の時間経過後に 未認証にするか、しないかを選択する。ENABLED の場合は未認証にし、DISABLED の場合は未認証にせず、認証を継続する。デフォルトは ENABLED。

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

SUPPLIMIT （802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート、Web 認証ポート）Multi-Supplicant モード（MODE=MULTI）のとき、認証可能な Supplicant の最大数を指定する。デフォルトは 320。

VLANASSIGNMENT （802.1X Authenticator ポート、MAC ベース認証ポート、Web 認証ポート）ダイナミック VLAN の有効・無効。有効時は、RADIUS サーバーが返してきた Tunnel-Private-Group-ID の値をもとに、指定ポートの所属 VLAN を動的に変更する。また、有効時、Web 認証でログインしてから、認証結果画面が表示されるまでに待機時間が発生する。 待機時間 (SET WEBAUTHSERVER コマンドの RENEWALTIME × 3 + 5) 秒。デフォルトは ENABLED。

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

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

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

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

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

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

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

備考・注意事項

・TYPE / ROLE パラメーターに NONE を指定すると、指定ポートの設定をデフォルトに戻すことができるが、このとき、PORTAUTH / PORTACCESS パラメーターに認証メカニズム（802.1X / MACBASED / WEBBASED）を指定する必要はない。
・サポートサプリカント数はすべての認証メカニズムを合わせて、320 / PORT、480 / SWITCH である。
・認証メカニズムは同時に実行（RADIUS サーバーと通信）することはできない。1 つの認証メカニズムが実行中の場合、他は待ち状態となる。
・MAC 認証 / Web 認証と併用した場合は 802.1X も必ず Multi-Supplicant モードとなる。
・1 つの認証メカニズムで認証が成功すれば、認証許可状態となる。
・MAC 認証を有効にしている場合は必ず MAC 認証が最初に実行される。
・802.1X / MAC 認証を併用した場合、MAC 認証で HELD になると同時に EAP-request を Supplicant に送信する。
・802.1X / MAC 認証は 1 回目の HELD で HELD 状態となる。Web 認証は 3 回連続で HELD となった場合に HELD 状態となる。HELD 期間は QUIETPERIOD パラメーターに依存する。HELD 状態は 1 つの認証メカニズムで認証が成功すれば、解除される。
・802.1X / Web 認証では Connecting 時に「ユーザー名」と「パスワード」を入力させるタイミングが存在する。入力されてボタンが押されるまでは他の認証アルゴリズムを実行することができる。
・802.1X / MAC 認証は REAUTHPERIOD パラメーターで設定した再認証間隔を過ぎると再認証を実行し、HELD になった場合、未認証状態となる。Web 認証は再認証間隔を過ぎると強制的に未認証状態となる。
・802.1X / MAC 認証において再認証は認証に成功した認証メカニズムに対して HELD となった場合にのみ未認証状態となる。
・802.1X はスタティック MAC アドレスとして登録される。MAC 認証 / Web 認証はダイナミック MAC アドレスとして登録されるため、通信がなかった場合、FDB Ageout で認証が解除される。
・1 つの認証メカニズムが HELD → CONNECTING になった時、他の認証メカニズムが CONNECTING であれば、Supplicant 情報は削除される。
・認証アルゴリズムを併用し、ひとつの認証アルゴリズムで認証許可状態となった場合、その認証が解除されるまで、他の認証アルゴリズムは動作しない。
・Web 認証設定時、Connecting 状態で Supptimeout SuppAgeout(300s 固定) 期間中にアクセスがない場合、Supplicant は削除される。
・MAC 認証は mode=single を設定した場合、 Multi-Supplicant Mode / supplicant limit=1 として実行される。その時、WARNING メッセージが表示される。
・Web 認証でダイナミック VLAN 有効時 か PVID 以外の ゲスト VLAN 設定時、Login ボタンが押されてから、実際に RADIUS に Access-Request を送信するまでに 3 秒 待機 (※ 1) する。Authenticating の画面 (<認証中 1 >画面) 表示し、(RenewalTime × 3 + 5) 秒 待機 (※ 2) 後に認証結果の画面を表示する。
※ 1 Authenticating 画面を確実に表示させるため。
※ 2 VLAN が変更された場合に、DHCP サーバーから新たに IP アドレスを取得するため。
・Web 認証で Supplicant が DHCP Server から IP アドレスを取得していて、ダイナミック VLAN 有効設定 もしくはゲスト VLAN 設定がされている場合は、Supplicant の認証を解除後、IP アドレスを再取得する必要がある。
・TYPE 以外のパラメーターは ポートごとに 全メカニズム共通で設定される。
・MAC 認証が HELD 以外の状態で、Web 認証の Login を行うと、認証失敗画面が表示されずに Login が

表示される。この認証の失敗は、失敗回数 (lockcount) にカウントされない。
・MAC 認証 / Web 認証は認証成功後、FDB 上の MAC アドレスが Age Out などでクリアされると、認証登録もクリアされる。
・Authenticator ポートにて、Supplicant の登録がない場合、show portauth status で Attached Supplicant(s) 情報は表示しない。

関連コマンド

SHOW PORTAUTH（123 ページ）
SHOW PORTAUTH PORT（131 ページ）

SET SWITCH INFILTERING

カテゴリー：スイッチング / 一般コマンド

SET SWITCH INFILTERING={**YES**|**NO**|**ON**|**OFF**|**TRUE**|**FALSE**}

解説

イングレスフィルタリングを行うかどうかを設定する。デフォルトは、イングレスフィルタリングは行わない。

パラメーター

INFILTERING　ON（行う）または OFF（行わない）を指定する。ON のときは、受信フレームの VLAN ID が受信ポートの所属 VLAN と一致した場合のみフレームを受け入れ、それ以外は破棄する。OFF の場合は、すべてのフレームを受け入れる。

関連コマンド

SHOW SWITCH（139 ページ）

SET SWITCH MIRROR

カテゴリー：スイッチング / ポート

SET SWITCH MIRROR={***0***|**NONE**|***port-number***}

port-number: スイッチポート番号（1〜）

解説

ミラーポートの設定および解除を行う。ミラーポートを設定すると、ポートミラーリング機能は有効になる。
デフォルトは、ポートミラーリング機能は無効。
ソースポートと対象トラフィックは、SET SWITCH PORT MIRROR コマンドで指定する。

パラメーター

MIRROR　ミラーポートとして使用するポートを指定する。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る。ミラーポートを削除（ミラーポートの機能を無効に）するには NONE（または 0）を指定する。

備考・注意事項

・ポートトランキングの所属ポートをミラーポートに設定することはできない。

関連コマンド

SET SWITCH PORT（96 ページ）
SHOW SWITCH（139 ページ）
SHOW SWITCH MIRROR（143 ページ）
SHOW SWITCH PORT（144 ページ）

SET SWITCH MULTICASTMODE

カテゴリー：スイッチング / 一般コマンド

SET SWITCH MULTICASTMODE={**A**|**B**|**C**|**D**}

解説

マルチキャストフレームのフラッディング仕様を設定する。

パラメーター

MULTICASTMODE　フラッディング仕様を選択する。A（BPDU/EAP パケットをすべて破棄する）、B（BPDU/EAP パケットを、VLAN を超えて、すべてのポートに転送する）、C（BPDU/EAP パケットを、VLAN 内に転送する。タグ付きポートを除く）、または D（BPDU/EAP パケットを、VLAN 内に転送する。タグ付きポートを含む。ただし、BPDU/EAP パケットにタグが付けられることはない）から選択する。デフォルトは、A。

例

■マルチキャストフレームのフラッディング仕様を C に設定する。

```
SET SWITCH MULTICASTMODE=C
```

関連コマンド

SHOW SWITCH（139 ページ）

SET SWITCH PORT

カテゴリー：スイッチング / ポート

SET SWITCH PORT={***port-list***|**ALL**} [DESCRIPTION=*string*] [STATUS={ENABLE|DISABLE}] [FLOWCONTROL={ENABLE|DISABLE}] [BCASTRATELIMITING={YES|NO|ON|OFF|TRUE|FALSE|ENABLED|DISABLED}] [MCASTRATELIMITING={YES|NO|ON|OFF|TRUE|FALSE|ENABLED|DISABLED}] [UNKUCASTRATELIMITING={YES|NO|ON|OFF|TRUE|FALSE|ENABLED|DISABLED}] [BCASTRATE=*0..262143*] [MCASTRATE=*0..262143*] [UNKUCASTRATE=*0..262143*] [BCASTFILTERING={YES|NO|ON|OFF|TRUE|FALSE|ENABLED|DISABLED}] [UNKMCASTFILTERING={YES|NO|ON|OFF|TRUE|FALSE|ENABLED|DISABLED}] [UNKUCASTFILTERING={YES|NO|ON|OFF|TRUE|FALSE|ENABLED|DISABLED}] [BCASTEGRESSFILTERING={YES|NO|ON|OFF|TRUE|FALSE|ENABLED|DISABLED}] [UNKMCASTEGRESSFILTERING={YES|NO|ON|OFF|TRUE|FALSE|ENABLED|DISABLED}] [UNKUCASTEGRESSFILTERING={YES|NO|ON|OFF|TRUE|FALSE|ENABLED|DISABLED}] [SPEED={AUTONEGOTIATE|10MHALF|10MFULL|100MHALF|100MFULL|1000MFULL}] [MDIMODE={MDI|MDIX}] [SOFTRESET] [PRIORITY=*0..7*] [OVERRIDEPRIORITY={YES|NO|ON|OFF|TRUE|FALSE}] [RENEGOTIATION=Auto] [COMBO=(FIBERAUTO|FIBER|COPPER)]

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（1〜16 文字）

解説

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

パラメーター

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

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。

STATUS　ポートのイネーブル、ディセーブルの設定。デフォルトはイネーブル。ENABLE SWITCH PORT コマンド、DISABLE SWITCH PORT コマンドと同義。

FLOWCONTROL　フローコントロール（802.3x PAUSE）の有効・無効。デフォルトは無効。ENABLE SWITCH PORT FLOW コマンド、DISABLE SWITCH PORT FLOW コマンドと同義。

BCASTRATELIMITING　ブロードキャストパケットの受信上限値を設定するかしないか。YES を指定した場合は、BCASTRATE パラメーターで、1 秒間の最大受信パケット数を指定する。上限を超えたパケットは破棄される。NO を指定した場合は、制限なしとなる。デフォルトは NO。

MCASTRATELIMITING　マルチキャストパケットの受信上限値を設定するかしないか。YES を指定し

た場合は、MCASTRATE パラメーターで、1 秒間の最大受信パケット数を指定する。上限を超えたパケットは破棄される。NO を指定した場合は、制限なしとなる。デフォルトは NO。

UNKUCASTRATELIMITING　未学習のユニキャストパケットの受信上限値を設定するかしないか。YES を指定した場合は、UNKUCASTRATE パラメーターで、1 秒間の最大受信パケット数を指定する。上限を超えたパケットは破棄される。NO を指定した場合は、制限なしとなる。デフォルトは NO。

BCASTRATE　ブロードキャストパケットの受信上限値を、0〜262143 で指定する。デフォルトは、262143。

MCASTRATE　マルチキャストパケットの受信上限値を、0〜262143 で指定する。デフォルトは、262143。

UNKUCASTRATE　未学習のユニキャストパケットの受信上限値を、0〜262143 で指定する。デフォルトは、262143。

BCASTFILTERING　ブロードキャストパケットのフィルタリング機能の有効・無効。ON（有効）か OFF（無効）を指定する。ON のときは、ブロードキャストパケットは受信されず、OFF のときは受信される。デフォルトは OFF。

UNKMCASTFILTERING　未学習のマルチキャストパケットのフィルタリング機能の有効・無効。ON（有効）か OFF（無効）を指定する。ON のときは、未学習のマルチキャストパケットは受信されず、OFF のときは受信される。デフォルトは OFF。

UNKUCASTFILTERING　未学習のユニキャストパケットのフィルタリング機能の有効・無効。ON（有効）か OFF（無効）を指定する。ON のときは、未学習のユニキャストパケットは受信されず、OFF のときは受信される。デフォルトは OFF。

BCASTEGRESSFILTERING　ブロードキャストパケットのフィルタリング機能の有効・無効。ON（有効）か OFF（無効）を指定する。ON のときは、ブロードキャストパケットは送信されず、OFF のときは送信される。デフォルトは OFF。

UNKMCASTEGRESSFILTERING　未学習のマルチキャストパケットのフィルタリング機能の有効・無効。ON（有効）か OFF（無効）を指定する。ON のときは、未学習のマルチキャストパケットは送信されず、OFF のときは送信される。デフォルトは OFF。

UNKUCASTEGRESSFILTERING　未学習のユニキャストパケットのフィルタリング機能の有効・無効。ON（有効）か OFF（無効）を指定する。ON のときは、未学習のユニキャストパケットは送信されず、OFF のときは送信される。デフォルトは OFF。

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。トランクグループ作成時は、トランクグループ内でポート番号が一番小さいポートのスピードに変更される。デフォルトは AUTONEGOTIATE。

MDIMODE　ポートの MDI/MDI-X を設定する。SPEED が AUTONEGOTIATE 以外のときに指定可能。SPEED が AUTONEGOTIATE 以外のとき、デフォルトは MDIX。

SOFTRESET　ポートをリセットする。

PRIORITY　ポート単位で、QoS の優先順位を設定する。デフォルトは 0。

OVERRIDEPRIORITY　ポートプライオリティーとタグプライオリティーのどちらを優先するかを設定する。YES の場合は、ポートプライオリティーを優先する。NO の場合は、タグプライオリティーを優先する。デフォルトは NO

RENEGOTIATION　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。ACTIVATE SWITCH PORT AUTONEGOTIATE コマンドを実行したのと同義。AUTONEGOTIATE に設定されたポートにのみ有効。

COMBO　コンボポートのメディア選択モードの設定を行う。1000BASE-T ポートと SFP ポートのどちらも使用可能とする場合は、FIBERAUTO を指定する（両方リンク可能な状態にある場合は、SFP ポー

トが優先される）。SFP ポートのみ使用可能とする場合は、FIBER を指定する。1000BASE-T ポートのみ使用可能とする場合は、COPPER を指定する。デフォルトは FIBERAUTO。

備考・注意事項

・タグ VLAN にしか所属していないポートでは PRIORITY パラメーターと OVERRIDEPRIORITY パラメーターを設定できない

9424Ts / XP-E では COMBO パラメーターに FIBER を指定する場合、コンボポートの 1000BASE-T ポートを接続してはならない。

9424Ts / XP-E では COMBO パラメーターに COPPER を指定する場合、コンボポートの SFP ポートを接続してはならない。

関連コマンド

DISABLE SWITCH PORT（63 ページ）
ENABLE SWITCH PORT（71 ページ）
SHOW SWITCH PORT（144 ページ）

SET SWITCH PORT MIRROR

カテゴリー：スイッチング / ポート

SET SWITCH PORT={***port-list***|**ALL**} **MIRROR=**{**NONE**|**RX**|**TX**|**BOTH**}

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

ミラーリング機能のソースポートと対象トラフィックを指定する。

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。

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。

関連コマンド

SET SWITCH MIRROR（94 ページ）
SHOW SWITCH（139 ページ）
SHOW SWITCH MIRROR（143 ページ）
SHOW SWITCH PORT（144 ページ）

SET SWITCH PORT SECURITYMODE

カテゴリー：スイッチング / ポート

SET SWITCH PORT={***port-list***|**ALL**} **SECURITYMODE=**{**AUTOMATIC**|**LIMITED**|**SECURED**}
[LEARN=*1..255*] [INTRUSIONACTION={DISCARD|TRAP|DISABLE}] [PARTICIPATE={ON|OFF|YES|NO|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)

解説

セキュリティーモードに関する設定を行う。MAC アドレステーブルは、デフォルトでは通常の学習モード。

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。

SECURITYMODE　セキュリティーモードを指定する。AUTOMATIC は、通常の学習モード。LIMITED は、学習可能な MAC アドレス数の最大数を設定したセキュリティーモード。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。学習可能な MAC アドレスの最大数は、LEARN パラメーターで設定。SECURED は、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。デフォルトは、AUTOMATIC。

LEARN　該当ポートで学習可能な送信元 MAC アドレス（ダイナミックエントリー）の最大数。デフォルトは 100。SECURITYMODE に LIMITED を指定したときのみ有効。

INTRUSIONACTION　学習済み MAC アドレスが制限値に達した後、未知の送信元 MAC アドレスを持つパケットを受信したときに実行するアクションを指定する。DISCARD は、不正なフレームを破棄する。TARP は、不正なフレームを破棄し、SNMP トラップを送信する。DISABLED は、不正なフレームを破棄し、SNMP トラップを送信した後、該当ポートをディセーブルにする。SECURITYMODE に LIMITED を指定したときのみ有効。

PARTICIPATE　INTRUSIONACTION に TRAP または DISABLE が設定されている場合、指定したアクションを実行するかしないかを選択する。ON はアクションを実行する。OFF はアクションを実行しない。デフォルトは OFF。SECURITYMODE に LIMITED を指定したときのみ有効。

備考・注意事項

・INTRUSIONACTION パラメーターで不正なパケットを受信したときのアクションを TRAP または DISABLE に設定しても、PARTICIPATE パラメーターを ON にしないとアクションは実行されない。
・SECURITYMODE を LIMITED から SECURED に変更する場合は、一度、AUTOMATIC に変更してから、SECURED に変更する

関連コマンド

SHOW SWITCH PORT INTRUSION（150 ページ）
SHOW SWITCH PORT SECURITYMODE（152 ページ）

SET SWITCH PORT STORMDETECTION

カテゴリー：スイッチング / ポート

SET SWITCH PORT={***port-list***|**ALL**} **STORMDETECTION** [LOWRATEACTION={LINKDOWN|BCASTDISCARD|NONE}] [HIGHRATEACTION={LINKDOWN|BCASTDISCARD|NONE}] [LOWRATETHRESHOLD={*1..1048575*|*10485759*}] [HIGHRATETHRESHOLD={*1..1048576*|*10485760*}] [BLOCKTIMEOUT={*60..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

受信レート検出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。指定したポートが存在しない場合はエラーとなる。

LOWRATEACTION 該当ポートで受信レートが低レートのしきい値（LOWRATETHRESHOLD パラメーターの設定値）を超えた場合のアクション。NONE（何もしない)、BCASTDISCARD（ブロードキャストパケットを破棄する)、LINKDOWN（ポートを物理的にリンクダウンする）から選択する。デフォルトは NONE。LOWRATE アクション実行中に、このパラメーターによって別のアクションを設定した場合は、次回のアクション実行時から適用する。

HIGHRATEACTION 該当ポートで受信レートが高レートのしきい値（HIGHRATETHRESHOLD パラメーターの設定値）を超えた場合のアクション。NONE（何もしない)、BCASTDISCARD（ブロードキャストパケットを破棄する)、LINKDOWN（ポートを物理的にリンクダウンする）から選択する。デフォルトは LINKDOWN。HIGHRATE アクション実行中に、このパラメーターによって別のアクションを設定した場合は、次回のアクション実行時から適用する。

HIGHRATETHRESHOLD 受信レートが高レート時のしきい値を Kbps（Kilo bit per second）で指定する。10 / 100 / 1000BASE-T ポートのデフォルトは 819200、10G ポートのデフォルトは 8388608。10 / 100 / 1000BASE-T ポートに 1048576 より大きい値を設定した場合はエラーとなる。10G ポートに 10485760 より大きい値を設定した場合はエラーとなる。

LOWRATETHRESHOLD 受信レートが低レート時のしきい値を Kbps（Kilo bit per second）で指定する。HIGHRATETHRESHOLD より大きい値はエラーとなる。10 / 100 / 1000BASE-T ポートのデフォルトは 512000、10G ポートのデフォルトは 5242880。10 / 100 / 1000BASE-T ポートに 1048576 以上の値を設定した場合はエラーとなる。10G ポートに 10485760 以上の値を設定した場合はエラーとなる。

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。

例

■ポート 2 の受信レートが 819200Kbps を超えたら、リンクダウンするように設定する

```
SET SWITCH PORT=2 STORMDETECTION HIGHRATEACTION=LINKDOWN
  HIGHRATETHRESHOLD=819200
```

備考・注意事項

・LINKDOWN、BCASTDISCARD アクションが実行中のとき、BLOCKTIMEOUT が経過する以外に、次のコマンドを実行するとアクションから復旧する（アクションの実行を中断する）。ENABLE SWITCH PORT コマンド、DISABLE SWITCH PORT コマンド、DISABLE SWITCH PORT STORMDETECTION コマンド、PURGE SWITCH コマンド
・BCASTDISCARD アクションが実行中のとき、BLOCKTIMEOUT が経過する以外に次のコマンドを実行、または動作を行うとアクションから復旧する（アクションの実行を中断する）。SET SWITCH PORT コマンドの BCASTRATELIMITING パラメーター / BCASTFILTERING パラメーター、ポートを物理的にリンクダウンする（ポートからケーブルを抜く）
・高レートのしきい値と低レートのしきい値を同時にこえた場合、高レートのアクションのみ実行する。

関連コマンド

DISABLE SWITCH PORT STORMDETECTION（65 ページ）
ENABLE SWITCH PORT STORMDETECTION（73 ページ）
RESET SWITCH PORT STORMDETECTION COUNTER（78 ページ）
SHOW SWITCH PORT STORMDETECTION（154 ページ）

SET SWITCH TRUNK

カテゴリー：スイッチング / ポート

SET SWITCH TRUNK=*trunk* [SELECT={MACSRC|MACDEST|MACBOTH|IPSRC|IPDEST|IPBOTH}]

trunk: トランクグループ名（1〜16 文字。英数字が使用可能。大文字小文字を区別しない）

解説

トランクグループの設定を変更する。

パラメーター

TRUNK トランクグループ名。

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

例

■トランクグループ「uplink」の設定を変更する。

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

備考・注意事項

・フラッディングパケットは、トランクグループ内で一番番号の小さいポートから送出される。

関連コマンド

ADD SWITCH TRUNK（54 ページ）
CREATE SWITCH TRUNK（55 ページ）
DELETE SWITCH TRUNK（57 ページ）
DESTROY SWITCH TRUNK（58 ページ）
SHOW SWITCH TRUNK（157 ページ）

SET WEBAUTHSERVER

カテゴリー：スイッチング / ポート認証

```
SET WEBAUTHSERVER [IPADDRESS={ipadd|NONE}] [PORT=port]
    [REDIRECTURL={string|NONE}] [SECURITY={ENABLED|DISABLED}] [SSLKEYID={id|
    NONE}] [SSLPORT=port] [HEADER={string|NONE}] [SUBHEADERTOP={string|
    NONE}] [SUBHEADERBOTTOM={string|NONE}] [FOOTER={string|NONE}]
    [PINGPOLL={ENABLED|DISABLED}] [NORMALINTERVAL=1..65535] [TIMEOUT=1..30]
    [FAILCOUNT=1..100] [REAUTHREFRESH={ENABLED|DISABLED}]
    [TEMPORARYIP={ENABLED|DISABLED}] [RENEWALTIME=5..10]
```

ipadd: IP アドレス
port: ポート番号
string: 文字列（1〜64 文字。英数字のみ使用可能。空白を含む場合はダブルクォートで囲む。”（ダブルクォーテーション）は使用できない）

解説

Web 認証サーバーの設定を変更する。設定を変更する場合は、Web 認証サーバー機能を無効にする。

パラメーター

IPADDRESS Web 認証サーバーへのアクセス専用の IP アドレス。デフォルトは 0.0.0.0(設定なし)。ネットワーク上に存在しない IP アドレスを設定しなければならない。設定しない場合は各 VLAN インターフェースに割り当てられている IP アドレスで接続できる。設定した場合は設定した IP アドレスでのみ認証サーバーに接続できる。通常の VLAN インターフェースの IP アドレスでは接続できない

PORT Web 認証サーバーの TCP ポート番号。HTTP のデフォルトは 80、HTTPS のデフォルトは 443。IPADDRESS パラメーターと併用しない場合は Authenticator 内で動作していない TCP ポート番号を指定しなければならない。IPADDRESS パラメーターと併用した場合はすべての TCP ポート番号を指定できる。（重複した TCP ポート番号を指定できる）

REDIRECTURL Web 認証の成功後に 自動的にジャンプするページの URL。デフォルトは NONE。最大入力文字数は 100 文字。

SECURITY Web 認証サーバーの HTTPS の有効・無効設定。 有効設定時、SSLKEYID の同時設定が必須。無効設定時、SSLKEYID の設定が削除される。デフォルトは DISABLED。

SSLKEYID Web 認証サーバーの HTTPS にて使用する SSL 鍵の鍵番号。SECURITY が有効の場合に設定可能となる。デフォルトは NONE。

SSLPORT Web 認証サーバーの HTTPS の TCP ポート番号。デフォルトは 443 番。

HEADER Web 認証ログインページのヘッダー部の表示内容。デフォルトは NONE で”Web Access Authentication Gateway”と表示される。最大入力文字数は 64 文字。

SUBHEADERTOP Web 認証ログインページのサブヘッダーの上部の表示内容。デフォルトは NONE で”Allied-Telesis”と表示される。最大入力文字数は 64 文字。

SUBHEADERBOTTOM　Web 認証ログインページのサブヘッダーの下部の表示内容。デフォルトは NONE で表示はなし。最大入力文字数は 64 文字。

FOOTER　Web 認証ログインページのフッター部の表示内容。デフォルトは NONE で”Allied Telesis”と表示される。最大入力文字数は 64 文字。

PINGPOLL　Ping ポーリング機能の有効・無効。 有効時は、認証されているユーザー宛に定期的に Ping パケットを送信し、通信可能か監視する。デフォルトは DISABLED。

NORMALINTERVAL　認証機器が通信可能のときのポーリング間隔（秒）。デフォルトは 30 秒。

TIMEOUT　Ping パケットの応答待ち時間（秒）。Ping（Echo request）パケット送信後、この時間内に応答パケットを受信しなかった場合は 無応答 と見なす。Ping 無応答時は TIMEOUT の間隔で Ping パケットが送信される。デフォルトは 1 秒。

FAILCOUNT　到達性が失われたと判断するために必要な Ping 無応答の回数。連続で FAILCOUNT 回無応答であった場合、認証機器が到達不可能になったと判断し、認証をログアウトする。デフォルトは 5 回。

REAUTHREFLESH　認証機器より Ping 応答がある間、再認証タイマー (REAUTHPERIOD) を更新するかの設定。 有効時は認証機器より Ping 応答があると、再認証タイマーをリセットする。 無効時は Ping 応答があっても、再認証タイマー経過後にログアウトされる。デフォルトは DISABLED。

TEMPORARYIP　Web 認証サーバーへ一時的にアクセスできるように、未認証の Supplicant に IP アドレスを付与するかの設定（テンポラリー IP アドレス機能の有効 / 無効の設定）。Web 認証サーバーが有効時に、この設定が有効になっている場合は DHCP サーバー機能より LEASETIME 20 秒で IP アドレスを付与する。無効時は付与しない。デフォルトは DISABLED。

RENEWALTIME　TEMPORARYIP の有効により 一時的に付与された IP アドレスの再 REQUEST 時間。 未認証 Supplicant は OPTION58（T1）としてこの値が利用され、OPTION59（T2）は +3 となる。デフォルトは 5 秒。また Web 認証でダイナミック VLAN を有効にしている場合（VLANASSIGNMENT=ENABLE）やゲスト VLAN を設定していた場合、ログインしてから、認証成功画面が表示されるまでの待機時間にも この値が使用される。 待機時間は (RENEWALTIME × 3 + 5) 秒。

例

■Web 認証サーバーの IP アドレスを 192.168.1.200 に設定する

```
SET WEBAUTHSERVER IPADDRESS=192.168.1.200
```

備考・注意事項

・IPADDRESS パラメーターの値には、すでに VLAN インターフェースに割り当てられている IP アドレスと同じセグメントの IP アドレスは指定できない。

関連コマンド

DISABLE WEBAUTHSERVER（66 ページ）

ENABLE WEBAUTHSERVER（74 ページ）
SET PORTACCESS PORT（80 ページ）
SET PORTAUTH PORT（87 ページ）
SHOW PORTACCESS（109 ページ）
SHOW PORTACCESS PORT（117 ページ）
SHOW PORTAUTH（123 ページ）
SHOW PORTAUTH PORT（131 ページ）
SHOW WEBAUTHSERVER（159 ページ）

SHOW EPSRSNOOPING

カテゴリー：スイッチング / EPSR スヌーピング

SHOW EPSRSNOOPING [CONTROLVLAN={*1..4094*|*vlanname*|ALL}]

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

解説

EPSR スヌーピングの情報を表示する

入力・出力・画面例

```
# show epsrsnooping controlvlan=10

EPSR Snooping Information:
  Control VLAN:
    VLAN Name ......................... vlan10
    VLAN ID ........................... 10
```

VLAN Name	管理対象のコントロール VLAN 名
VLAN ID	VLAN ID

表 21:

例

■コントロール VLAN（VID=10）の EPSR Snooping の情報を表示する

```
SHOW EPSRSNOOPING CONTROLVLAN=10
```

関連コマンド

DISABLE EPSRSNOOPING（59 ページ）
ENABLE EPSRSNOOPING（67 ページ）

SHOW PORTACCESS

カテゴリー：スイッチング / ポート認証

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

SHOW PORTACCESS={**8021X**|**MACBASED**|**WEBBASED**|**ALL**} {**CONFIG**|**STATUS**}

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

解説

ポート認証機能（802.1X 認証、MAC ベース認証、Web 認証）の全般的な設定と状態を表示する。SHOW PORTAUTH コマンドは同義。

パラメーター

PORTACCESS　認証方式。8021X（IEEE 802.1X 認証について表示)、MACBASED（MAC アドレスベース認証について表示)、WEBBASED（Web 認証について表示)、ALL のいずれかを指定する。デフォルトは、8021X。

CONFIG　認証モジュールの設定を表示する。

STATUS　認証モジュールの状態を表示する。

PORT　スイッチポート。複数指定が可能。

入力・出力・画面例

```
# show portaccess=all

Port Authentication Information
-------------------------------------------------------------------------------
SystemAuthControl.................. Enabled
Number of 802.1x Supplicants....... 1
Number of MAC Based Supplicants.... 0
Number of WEB Based Supplicants.... 0
Total Supplicants.................. 1

Port AuthMode PortRole VLAN PortStatus   Status         Additional Info
-------------------------------------------------------------------------------
   1 802.1X   Auth     1    Authorized   Authenticated  00:0A:E6:6A:CC:7F
   1 MACBASE  Auth     1    Authorized   Connecting     00:0A:E6:6A:CC:7F
   1 WEBBASE  Auth     1    Authorized   Connecting     00:0A:E6:6A:CC:7F


# show portaccess=8021x port=1
```

```
802.1x Authentication Information
--------------------------------------------------------------------------------
SystemAuthControl.................. Enabled
Number of 802.1x Supplicants....... 1
Total Supplicants.................. 1

Port AuthMode PortRole VLAN PortStatus   Status         Additional Info
--------------------------------------------------------------------------------
   1 802.1X   Auth     1    Authorized   Authenticated  00:0A:E6:6A:CC:7F


# show portaccess=all config

Port 1

802.1x Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Authenticator

MAC BASE Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Authenticator

WEB BASE Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Authenticator

Supplicant Mode........... Multiple
Supplicant Limit.......... 320
AuthControlPortControl.... Auto
quietPeriod............... 60
txPeriod.................. 30
suppTimeout............... 30
serverTimeout............. 30
maxReq.................... 2
reAuthPeriod.............. 3600
reAuthEnabled............. Enabled
reAuthMAX................. 2
vlanAssignment............ Enabled
vlanAssignmentType........ USER
secureVlan................ On
lockCount................. 3
portMoveReauth............ Disabled
ForceRenewing............. Disabled
guestVlan................. None
adminControlDirection..... Ingress
piggyBack................. -
ARP Forwarding............ Disabled
TCP Forwarding............ -
UDP Forwarding............ -
```

```
Port 2

802.1x Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Supplicant
heldPeriod..................... 60
authPeriod..................... 30
startPeriod.................... 30
maxStart....................... 3
username....................... test
password....................... test



# show portaccess=all status

Port 1

802.1x Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Authenticator
Supplicant Mode........... Multiple
Number of Supplicants..... 1

Attached Supplicant(s)
    MAC Address..................... 00:0A:E6:6A:CC:7F
    Authenticator PAE State......... Authenticated
    Port Status..................... Authorized
    Backend Authenticator State..... Idle
    VLAN ID......................... 1

MAC BASE Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Authenticator
Supplicant Mode........... Multiple
Number of Supplicants..... 1

Attached Supplicant(s)
    MAC Address..................... 00:0A:E6:6A:CC:7F
    Authenticator PAE State......... Connecting
    Port Status..................... Authorized
    Backend Authenticator State..... Idle
    VLAN ID......................... 1

WEB BASE Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Authenticator
Supplicant Mode........... Multiple
Number of Supplicants..... 1

Attached Supplicant(s)
```

```
    MAC Address..................... 00:0A:E6:6A:CC:7F
    Authenticator PAE State......... Connecting
    Port Status..................... Authorized
    Backend Authenticator State..... Idle
    VLAN ID......................... 1

Port 2

802.1x Authentication Information
--------------------------------------------------------------------------------
PAE Type................. Supplicant
Supplicant PAE State............ Connecting
```

SystemAuthControl	ポート認証機能の有効・無効。Enabled か Disabled
Number of 802.1x Supplicants	802.1X 認証のサプリカントの数
Number of MAC Based Supplicants	MAC ベース認証のサプリカントの数
Number of WEB Based Supplicants	Web 認証のサプリカントの数
Total Supplicants	サプリカントの数
Port	ポート番号
AuthMode	認証メカニズム。802.1X、MACBASE、WEBBASE のいずれか
PortRole	スイッチポートのタイプ（802.1X における役割）。Authenticator、Supplicant、None のいずれか
VLAN	SUPPLICANT の接続している VLAN
PortStatus	ポートの状態。unauthorised（未認証）か authorised（認証済み）
Status	認証の状態。（ポートのタイプが設定され、認証モジュールが有効の場合に、次のステータスを表示する。）AUTHENTICATOR ポートの場合は、Initialize（初期化）、Connecting（接続中）、Authenticating（認証中）、Authenticated（認証済み）、Aborting（認証断念中）、Held（待機中）、Force_Auth（「認証済み」に固定設定）、Force_Unauth（「未認証」に固定設定）のいずれか。SUPPLICANT ポートの場合は、Acquired（要求中）、Connecting（接続中）、Authenticating（認証中）、Authenticated（認証済み）、Held（待機中）、Logoff（ログオフ）のいずれか。SET PORTAUTH PORT コマンド / SET PORTACCESS PORT コマンドの CONTROL パラメーターに AUTHORISED を指定した場合、Authenticated（認証済み）を表示、CONTROL パラメーターに UNAUTHORISED を指定した場合、Connecting（接続中）を表示する

Additional Info	AUTHENTICATOR ポートで、AUTHENTICATED 状態のときに、SUPPLICANT の MAC アドレスを表示する

表 22: CONFIG、STATUS を指定しない場合

Port	ポート番号
PAE Type	スイッチポートのタイプ。Authenticator、Supplicant のいずれか
Supplicant Mode	（Authenticator ポート）Authenticator ポートのモード。Single か Multiple
Supplicant Limit	（Authenticator ポート）SUPPLICANT の最大接続数
AuthControlPortControl	（Authenticator ポート）手動設定による Authenticator ポートの状態。Auto、ForceUnauth か ForceAuth
quietPeriod	（Authenticator ポート）認証失敗後、Supplicant との通信を拒否する期間（秒）
txPeriod	（Authenticator ポート）Supplicant に EAPOL パケットを再送信する間隔（秒）
suppTimeout	（Authenticator ポート）Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間（秒）
serverTimeout	（Authenticator ポート）RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間（秒）
maxReq	（Authenticator ポート）Supplicant に対する EAPOL-Request パケットの最大再送回数
reAuthPeriod	（Authenticator ポート）Supplicant を再認証する間隔（秒）
reAuthEnabled	（Authenticator ポート）Supplicant ポートの再認証を行うかどうか。Enabled または Disabled
reAuthMax	（Authenticator ポート）Supplicant を再認証する回数
vlanAssignment	（Authenticator ポート）ダイナミック VLAN の有効・無効。Enabled または Disabled
vlanAssignmentType	（Authenticator ポート）ダイナミック VLAN のタイプ。PORT または、USER
secureVlan	（Authenticator ポート）Multi-Supplicant モード（MODE=MULTI）のとき、2 番目以降の Supplicant の認証方法。On（最初の Supplicant と同じ VLAN でなければ認証しない）か Off（有効 VLAN であれば認証する）
lockCount	（Authenticator ポート）Web 認証において、Held の状態になるまでの認証の連続失敗回数
portMoveReauth	（Authenticator ポート）認証済みの Supplicant がポートを移動したときに、再度、認証を行うかどうか。Enabled または Disabled
ForceRenewing	未サポート
guestvlan	（Authenticator ポート）ゲスト VLAN に指定した VLAN 名と VLAN ID

adminControlDirection	（Authenticator ポート）未認証状態で、送受信したブロードキャストまたはマルチキャストパケットをどう扱うか。Ingress か Both
piggyBack	（Authenticator ポート）Piggy back モードの有効/無効。Enabled または Disabled
ARP Forwarding	（Authenticator ポート）Web 認証の場合、未認証状態で、ARP パケットを受信したときに 透過するか破棄するか。Enabled または Disabled
TCP Forwarding	（Authenticator ポート）Web 認証の場合、未認証状態で、透過する TCP ポートのパケット
UDP Forwarding	（Authenticator ポート）Web 認証の場合、未認証状態で、透過する UDP ポートのパケット
Port	ポート番号
PAE Type	スイッチポートのタイプ。Authenticator、Supplicant のいずれか
heldPeriod	（Supplicant ポート）認証失敗後、Authenticator との通信を試みない期間（秒）
authPeriod	（Supplicant ポート）EAPOL-Start パケットの最大送信回数。Supplicant ポートは、EAPOL-Start パケットを MAXSTART 回送信しても応答がない場合、ポート認証の必要はないと判断する
startPeriod	（Supplicant ポート）認証失敗後、Supplicant との通信を拒否する期間（秒）
maxStart	（Supplicant ポート）Authenticator に EAPOL-Start パケットを再送信する間隔（秒）
username	ユーザー名
password	パスワード

表 23: CONFIG を指定した場合

Port	ポート番号
PAE Type	スイッチポートのタイプ。Authenticator、Supplicant のいずれか
Supplicant Mode	Authenticator ポートのモード。Single か Multiple
Number of Supplicant	サプリカント数
Attached Supplicant(s)	ポートに接続しているサプリカントの情報を表示
MAC Address	MAC アドレスを表示
Authenticator/Supplicant PAE State	ポートの状態。（ポートのタイプが設定され、802.1X 認証モジュールが有効の場合に、次のステータスを表示する。）AUTHENTICATOR ポートの場合は、Initialize（初期化）、Connecting（接続中）、Authenticating（認証中）、Authenticated（認証済み）、Aborting（認証断念中）、Held（待機中）、Force_Auth（「認証済み」に固定設定）、Force_Unauth（「未認証」に固定設定）のいずれか。SUPPLICANT ポートの場合は、Acquired（要求中）、Connecting（接続中）、Authenticating（認証中）、Authenticated（認証済み）、Held（待機中）、Logoff（ログオフ）のいずれか。SET PORTAUTH PORT コマンド/SET PORTACCESS PORT コマンドの CONTROL パラメーターに AUTHORISED を指定した場合、Authenticated（認証済み）を表示、CONTROL パラメーターに UNAUTHORISED を指定した場合、Connecting（接続中）を表示する
Port Status	ポートの状態。unauthorised（未認証）か authorised（認証済み）
Backend Authenticator State	認証機構の状態。IDLE（アイドル）、INITIALISE（初期化）、RESPONSE（Supplicant から応答受信）、REQUEST（認証サーバーに要求送信）、SUCCESS（認証成功）、FAIL（認証失敗）、TIMEOUT（タイムアウト）のいずれか
VLAN ID	サプリカントが接続している VLAN の VID

表 24: STATUS を指定した場合

例

■802.1X 認証の全般的な設定と状態を表示する

```
SHOW PORTACCESS=8021 x
```

■802.1X 認証モジュールの設定を表示する

```
SHOW PORTACCESS=8021x CONFIG
```

■802.1X 認証モジュールの状態を表示する

```
SHOW PORTACCESS=8021x STATUS
```

■MAC ベース認証の全体的な設定と状態を表示する

```
SHOW PORTACCESS=MACBASED
```

備考・注意事項

・パラメーターに CONFIG を指定した場合、指定した認証方式でサポートしていないパラメーターも含めすべてのパラメーターの一覧が表示される。
・パラメーターはポートごとに管理され、認証方式ごとには設定できない。1 つのポートで複数の認証メカニズムを設定した場合、いずれかの認証方式でパラメーターを設定すると、SHOW CONFIG コマンドの DYNAMIC パラメーターを指定すると、各認証方式に同じ設定値が表示されるが、そのパラメーターは該当する認証方式以外では動作しない。

関連コマンド

DISABLE PORTACCESS（60 ページ）
ENABLE PORTACCESS（68 ページ）
SET PORTACCESS AUTHMETHOD（79 ページ）
SET PORTACCESS PORT（80 ページ）
SHOW PORTACCESS PORT（117 ページ）

SHOW PORTACCESS PORT

カテゴリー：スイッチング / ポート認証

SHOW PORTACCESS={**8021X**|**MACBASED**|**WEBBASED**} **PORT=**{***port-list***|**ALL**}
[{AUTHENTICATOR|SUPPLICANT}] [{CONFIG|STATUS}]

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

解説

指定ポートのポート認証設定を表示する。SHOW PORTAUTH PORT コマンドは同義。

パラメーター

PORTACCESS　認証方式。8021X（IEEE 802.1X 認証について表示）、MACBASED（MAC アドレスベース認証について表示）、WEBBASED（Web 認証について表示）、ALL のいずれかを指定する。デフォルトは、8021X。

PORT　スイッチポート。複数指定が可能。

AUTHENTICATOR/SUPPLICANT　802.1X 認証モジュールの設定を表示する。

CONFIG　認証モジュールの設定を表示する。

STATUS　認証モジュールの状態を表示する。

入力・出力・画面例

```
# show portaccess=all port=1 authenticator config

Port 1

802.1x Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Authenticator

MAC BASE Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Authenticator

WEB BASE Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Authenticator

Supplicant Mode........... Multiple
Supplicant Limit.......... 320
AuthControlPortControl.... Auto
quietPeriod............... 60
```

```
txPeriod.................. 30
suppTimeout............... 30
serverTimeout............. 30
maxReq.................... 2
reAuthPeriod.............. 3600
reAuthEnabled............. Enabled
reAuthMAX................. 2
vlanAssignment............ Enabled
vlanAssignmentType........ USER
secureVlan................ On
lockCount................. 3
portMoveReauth............ Disabled
ForceRenewing............. Disabled
guestVlan................. None
adminControlDirection..... Ingress
piggyBack................. -
ARP Forwarding............ Disabled
TCP Forwarding............ -
UDP Forwarding............ -




# show portaccess=all port=1 authenticator status

Port 1

802.1x Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Authenticator
Supplicant Mode........... Multiple
Number of Supplicants..... 1

Attached Supplicant(s)
    MAC Address..................... 00:0A:E6:6A:CC:7F
    Authenticator PAE State......... Authenticated
    Port Status..................... Authorized
    Backend Authenticator State..... Idle
    VLAN ID......................... 1

MAC BASE Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Authenticator
Supplicant Mode........... Multiple
Number of Supplicants..... 1

Attached Supplicant(s)
    MAC Address..................... 00:0A:E6:6A:CC:7F
    Authenticator PAE State......... Connecting
    Port Status..................... Authorized
    Backend Authenticator State..... Idle
```

```
    VLAN ID..................... 1

WEB BASE Authentication Information
------------------------------------------------------------------------------
PAE Type................. Authenticator
Supplicant Mode.......... Multiple
Number of Supplicants..... 1

Attached Supplicant(s)
    MAC Address..................... 00:0A:E6:6A:CC:7F
    Authenticator PAE State......... Connecting
    Port Status..................... Authorized
    Backend Authenticator State..... Idle
    VLAN ID..................... 1



# show portaccess all port=2 supplicant config

Port 2

802.1x Authentication Information
------------------------------------------------------------------------------
PAE Type................. Supplicant
heldPeriod..................... 60
authPeriod..................... 30
startPeriod.................... 30
maxStart....................... 3
username....................... test
password....................... test



# show portaccess all port=2 supplicant status

Port 2

802.1x Authentication Information
------------------------------------------------------------------------------
PAE Type................. Supplicant
Supplicant PAE State............ Connecting
```

Port	ポート番号
PAE Type（802.1x Authentication Information）	スイッチポートのタイプ（802.1X における役割）。Authenticator、Supplicant のいずれか

PAE Type（MAC BASED Authentication Information）	スイッチポートのタイプ（MAC ベース認証における役割）。Authenticator、Supplicant のいずれか
PAE Type（WEB BASED Authentication Information）	スイッチポートのタイプ（Web 認証における役割）。Authenticator、Supplicant のいずれか
Supplicant Mode	（Authenticator ポート）Authenticator ポートのモード。Single か Multiple
Supplicant Limit	（Authenticator ポート）SUPPLICANT の最大接続数
AuthControl-PortControl	（Authenticator ポート）手動設定による Authenticator ポートの状態。Auto、ForceUnauth か ForceAuth
quietPeriod	（Authenticator ポート）認証失敗後、Supplicant との通信を拒否する期間（秒）
txPeriod	（Authenticator ポート）Supplicant に EAPOL パケットを再送信する間隔（秒）
suppTimeout	（Authenticator ポート）Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間（秒）
serverTimeout	（Authenticator ポート）RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間（秒）
maxReq	（Authenticator ポート）Supplicant に対する EAPOL-Request パケットの最大再送回数
reAuthPeriod	（Authenticator ポート）Supplicant を再認証する間隔（秒）
reAuthEnabled	（Authenticator ポート）Supplicant ポートの再認証を行うかどうか。Enabled または Disabled
reAuthMax	（Authenticator ポート）Supplicant を再認証する回数
vlanAssignment	（Authenticator ポート）ダイナミック VLAN の有効・無効。Enabled または Disabled
vlan-Assignment-Type	（Authenticator ポート）ダイナミック VLAN のタイプ。PORT または、USER
secureVlan	（Authenticator ポート）Multi-Supplicant モード（MODE=MULTI）のとき、2 番目以降の Supplicant の認証方法。On（最初の Supplicant と同じ VLAN でなければ認証しない）か Off（有効 VLAN であれば認証する）
lockCount	（Authenticator ポート）Web 認証において、Held の状態になるまでの 認証の連続失敗回数
portMove-Reauth	（Authenticator ポート）認証済みの Supplicant がポートを移動したときに、再度、認証を行うかどうか。Enabled または Disabled

ForceRenewing	未サポート
guestvlan	（Authenticator ポート）ゲスト VLAN に指定した VLAN 名と VLAN ID
adminControl-Direction	（Authenticator ポート）未認証状態で、送受信したブロードキャストまたはマルチキャストパケットをどう扱うか。Ingress か Both
piggyBack	（Authenticator ポート）Piggy back モードの有効 / 無効。Enabled または Disabled
ARP Forward-ing	（Authenticator ポート）未認証状態で、ARP パケットを受信したときに 透過するか破棄するか。Enabled または Disabled
TCP Forward-ing	（Authenticator ポート）未認証状態で、透過する TCP ポートのパケット
UDP Forward-ing	（Authenticator ポート）未認証状態で、透過する UDP ポートのパケット

表 25: AUTHENTICATOR、CONFIG を指定した場合

Port	ポート番号
PAE Type	スイッチポートのタイプ。Authenticator、Supplicant のいずれか
Supplicant Mode	Authenticator ポートのモード。Single か Multiple
Number of Supplicant	サプリカント数
Attached Supplicant(s)	ポートに接続しているサプリカントの情報を表示
MAC Address	MAC アドレスを表示
Authenticator / Supplicant PAE State	ポートの状態。（ポートのタイプが設定され、802.1X 認証モジュールが有効の場合に、次のステータスを表示する。）AUTHENTICATOR ポートの場合は、Initialize（初期化）、Connecting（接続中）、Authenticating（認証中）、Authenticated（認証済み）、Aborting（認証断念中）、Held（待機中）、Force_Auth（「認証済み」に固定設定）、Force_Unauth（「未認証」に固定設定）のいずれか。SUPPLICANT ポートの場合は、Acquired（要求中）、Connecting（接続中）、Authenticating（認証中）、Authenticated（認証済み）、Held（待機中）、Logoff（ログオフ）のいずれか
Port Status	ポートの状態。unauthorised（未認証）か authorised（認証済み）
Backend Authenticator State	認証機構の状態。IDLE（アイドル）、INITIALISE（初期化）、RESPONSE（Supplicant から応答受信）、REQUEST（認証サーバーに要求送信）、SUCCESS（認証成功）、FAIL（認証失敗）、TIMEOUT（タイムアウト）のいずれか

VLAN ID	サプリカントが接続している VLAN の VID

表 26: AUTHENTICATOR、STATUS を指定した場合

Port	ポート番号
PAE Type	スイッチポートのタイプ（802.1X における役割）。Authenticator、Supplicant のいずれか
heldPeriod	（Supplicant ポート）認証失敗後、Authenticator との通信を試みない期間（秒）
authPeriod	（Supplicant ポート）EAPOL-Start パケットの最大送信回数。Supplicant ポートは、EAPOL-Start パケットを MAXSTART 回送信しても応答がない場合、ポート認証の必要はないと判断する
startPeriod	（Supplicant ポート）認証失敗後、Supplicant との通信を拒否する期間（秒）
maxStart	（Supplicant ポート）Authenticator に EAPOL-Start パケットを再送信する間隔（秒）
username	ユーザー名
password	パスワード

表 27: SUPPLICANT、CONFIG を指定した場合

Port	ポート番号
PAE Type	スイッチポートのタイプ（802.1X における役割）。Authenticator、Supplicant のいずれか
Supplicant PAE State	ポートの状態。（ポートのタイプが設定され、802.1X 認証モジュールが有効の場合に、次のステータスを表示する。）AUTHENTICATOR ポートの場合は、Initialize（初期化）、Connecting（接続中）、Authenticating（認証中）、Authenticated（認証済み）、Aborting（認証断念中）、Held（待機中）、Force_Auth（「認証済み」に固定設定）、Force_Unauth（「未認証」に固定設定）のいずれか。SUPPLICANT ポートの場合は、Acquired（要求中）、Connecting（接続中）、Authenticating（認証中）、Authenticated（認証済み）、Held（待機中）、Logoff（ログオフ）のいずれか
Port Status	ポートの状態。unauthorised（未認証）か authorised（認証済み）

表 28: SUPPLICANT、STATUS を指定した場合

関連コマンド

DISABLE PORTACCESS（60 ページ）
ENABLE PORTACCESS（68 ページ）
SET PORTACCESS AUTHMETHOD（79 ページ）
SET PORTACCESS PORT（80 ページ）
SHOW PORTACCESS（109 ページ）

SHOW PORTAUTH

カテゴリー：スイッチング / ポート認証

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

SHOW PORTAUTH={**8021X**|**MACBASED**|**WEBBASED**|**ALL**} {**CONFIG**|**STATUS**}

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

解説

ポート認証機能（802.1X 認証、MAC ベース認証、Web 認証）の全般的な設定と状態を表示する。SHOW PORTACCESS コマンドは同義。

パラメーター

PORTAUTH　認証方式。8021X（IEEE 802.1X 認証について表示)、MACBASED（MAC アドレスベース認証について表示)、WEBBASED（Web 認証について表示)、ALL のいずれかを指定する。デフォルトは、8021X。

CONFIG　認証モジュールの設定を表示する。

STATUS　認証モジュールの状態を表示する。

PORT　スイッチポート。複数指定が可能。

入力・出力・画面例

```
# show portauth=all

Port Authentication Information
--------------------------------------------------------------------------------
SystemAuthControl.................. Enabled
Number of 802.1x Supplicants....... 1
Number of MAC Based Supplicants.... 0
Number of WEB Based Supplicants.... 0
Total Supplicants.................. 1

Port AuthMode PortRole VLAN PortStatus   Status         Additional Info
--------------------------------------------------------------------------------
   1 802.1X   Auth     1    Authorized   Authenticated  00:0A:E6:6A:CC:7F
   1 MACBASE  Auth     1    Authorized   Connecting     00:0A:E6:6A:CC:7F
   1 WEBBASE  Auth     1    Authorized   Connecting     00:0A:E6:6A:CC:7F


# show portauth=8021x port=1
```

```
802.1x Authentication Information
--------------------------------------------------------------------------------
SystemAuthControl.................. Enabled
Number of 802.1x Supplicants....... 1
Total Supplicants.................. 1

Port AuthMode PortRole VLAN PortStatus   Status         Additional Info
--------------------------------------------------------------------------------
   1 802.1X   Auth     1    Authorized   Authenticated  00:0A:E6:6A:CC:7F


# show portauth=all config

Port 1

802.1x Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Authenticator

MAC BASE Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Authenticator

WEB BASE Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Authenticator

Supplicant Mode........... Multiple
Supplicant Limit.......... 320
AuthControlPortControl.... Auto
quietPeriod............... 60
txPeriod.................. 30
suppTimeout............... 30
serverTimeout............. 30
maxReq.................... 2
reAuthPeriod.............. 3600
reAuthEnabled............. Enabled
reAuthMAX................. 2
vlanAssignment............ Enabled
vlanAssignmentType........ USER
secureVlan................ On
lockCount................. 3
portMoveReauth............ Disabled
ForceRenewing............. Disabled
guestVlan................. None
adminControlDirection..... Ingress
piggyBack................. -
ARP Forwarding............ Disabled
TCP Forwarding............ -
UDP Forwarding............ -
```

```
Port 2

802.1x Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Supplicant
heldPeriod..................... 60
authPeriod..................... 30
startPeriod.................... 30
maxStart....................... 3
username....................... test
password....................... test



# show portauth=all status

Port 1

802.1x Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Authenticator
Supplicant Mode........... Multiple
Number of Supplicants..... 1

Attached Supplicant(s)
    MAC Address..................... 00:0A:E6:6A:CC:7F
    Authenticator PAE State......... Authenticated
    Port Status..................... Authorized
    Backend Authenticator State..... Idle
    VLAN ID......................... 1

MAC BASE Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Authenticator
Supplicant Mode........... Multiple
Number of Supplicants..... 1

Attached Supplicant(s)
    MAC Address..................... 00:0A:E6:6A:CC:7F
    Authenticator PAE State......... Connecting
    Port Status..................... Authorized
    Backend Authenticator State..... Idle
    VLAN ID......................... 1

WEB BASE Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Authenticator
Supplicant Mode........... Multiple
Number of Supplicants..... 1

Attached Supplicant(s)
```

```
    MAC Address..................... 00:0A:E6:6A:CC:7F
    Authenticator PAE State......... Connecting
    Port Status..................... Authorized
    Backend Authenticator State..... Idle
    VLAN ID......................... 1

Port 2

802.1x Authentication Information
--------------------------------------------------------------------------------
PAE Type................. Supplicant
Supplicant PAE State............ Connecting
```

SystemAuthControl	ポート認証機能の有効・無効。Enabled か Disabled
Number of 802.1x Supplicants	802.1X 認証のサプリカントの数
Number of MAC Based Supplicants	MAC ベース認証のサプリカントの数
Number of WEB Based Supplicants	Web 認証のサプリカントの数
Total Supplicants	サプリカントの数
Port	ポート番号
AuthMode	認証メカニズム。802.1X、MACBASE、WEBBASE のいずれか
PortRole	スイッチポートのタイプ（802.1X における役割）。Authenticator、Supplicant、None のいずれか
VLAN	SUPPLICANT の接続している VLAN
PortStatus	ポートの状態。unauthorised（未認証）か authorised（認証済み）
Status	認証の状態。（ポートのタイプが設定され、認証モジュールが有効の場合に、次のステータスを表示する。）AUTHENTICATOR ポートの場合は、Initialize（初期化）、Connecting（接続中）、Authenticating（認証中）、Authenticated（認証済み）、Aborting（認証断念中）、Held（待機中）、Force_Auth（「認証済み」に固定設定）、Force_Unauth（「未認証」に固定設定）のいずれか。SUPPLICANT ポートの場合は、Acquired（要求中）、Connecting（接続中）、Authenticating（認証中）、Authenticated（認証済み）、Held（待機中）、Logoff（ログオフ）のいずれか。SET PORTAUTH PORT コマンド / SET PORTACCESS PORT コマンドの CONTROL パラメーターに AUTHORISED を指定した場合、Authenticated（認証済み）を表示、CONTROL パラメーターに UNAUTHORISED を指定した場合、Connecting（接続中）を表示する

Additional Info	AUTHENTICATOR ポートで、AUTHENTICATED 状態のときに、SUPPLICANT の MAC アドレスを表示する

表 29: CONFIG または STATUS を指定しない場合

Port	ポート番号
PAE Type	スイッチポートのタイプ。Authenticator、Supplicant のいずれか
Supplicant Mode	（Authenticator ポート）Authenticator ポートのモード。Single か Multiple
Supplicant Limit	（Authenticator ポート）SUPPLICANT の最大接続数
AuthControlPortControl	（Authenticator ポート）手動設定による Authenticator ポートの状態。Auto、ForceUnauth か ForceAuth
quietPeriod	（Authenticator ポート）認証失敗後、Supplicant との通信を拒否する期間（秒）
txPeriod	（Authenticator ポート）Supplicant に EAPOL パケットを再送信する間隔（秒）
suppTimeout	（Authenticator ポート）Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間（秒）
serverTimeout	（Authenticator ポート）RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間（秒）
maxReq	（Authenticator ポート）Supplicant に対する EAPOL-Request パケットの最大再送回数
reAuthPeriod	（Authenticator ポート）Supplicant を再認証する間隔（秒）
reAuthEnabled	（Authenticator ポート）Supplicant ポートの再認証を行うかどうか。Enabled または Disabled
reAuthMax	（Authenticator ポート）Supplicant を再認証する回数
vlanAssignment	（Authenticator ポート）ダイナミック VLAN の有効・無効。Enabled または Disabled
vlanAssignmentType	（Authenticator ポート）ダイナミック VLAN のタイプ。PORT または、USER
secureVlan	（Authenticator ポート）Multi-Supplicant モード（MODE=MULTI）のとき、2 番目以降の Supplicant の認証方法。On（最初の Supplicant と同じ VLAN でなければ認証しない）か Off（有効 VLAN であれば認証する）
lockCount	（Authenticator ポート）Web 認証において、Held の状態になるまでの認証の連続失敗回数
portMoveReauth	（Authenticator ポート）認証済みの Supplicant がポートを移動したときに、再度、認証を行うかどうか。Enabled または Disabled
ForceRenewing	未サポート
guestvlan	（Authenticator ポート）ゲスト VLAN に指定した VLAN 名と VLAN ID

adminControlDirection	（Authenticator ポート）未認証状態で、送受信したブロードキャストまたはマルチキャストパケットをどう扱うか。Ingress か Both
piggyBack	（Authenticator ポート）Piggy back モードの有効/無効。Enabled または Disabled
ARP Forwarding	（Authenticator ポート）Web 認証の場合、未認証状態で、ARP パケットを受信したときに 透過するか破棄するか。Enabled または Disabled
TCP Forwarding	（Authenticator ポート）Web 認証の場合、未認証状態で、透過する TCP ポートのパケット
UDP Forwarding	（Authenticator ポート）Web 認証の場合、未認証状態で、透過する UDP ポートのパケット
Port	ポート番号
PAE Type	スイッチポートのタイプ。Authenticator、Supplicant のいずれか
heldPeriod	（Supplicant ポート）認証失敗後、Authenticator との通信を試みない期間（秒）
authPeriod	（Supplicant ポート）EAPOL-Start パケットの最大送信回数。Supplicant ポートは、EAPOL-Start パケットを MAXSTART 回送信しても応答がない場合、ポート認証の必要はないと判断する
startPeriod	（Supplicant ポート）認証失敗後、Supplicant との通信を拒否する期間（秒）
maxStart	（Supplicant ポート）Authenticator に EAPOL-Start パケットを再送信する間隔（秒）
username	ユーザー名
password	パスワード

表 30: CONFIG を指定した場合

Port	ポート番号
PAE Type	スイッチポートのタイプ。Authenticator、Supplicant のいずれか
Supplicant Mode	Authenticator ポートのモード。Single か Multiple
Number of Supplicant	サプリカント数
Attached Supplicant(s)	ポートに接続しているサプリカントの情報を表示
MAC Address	MAC アドレスを表示
Authenticator/Supplicant PAE State	ポートの状態。（ポートのタイプが設定され、802.1X 認証モジュールが有効の場合に、次のステータスを表示する。）AUTHENTICATOR ポートの場合は、Initialize（初期化）、Connecting（接続中）、Authenticating（認証中）、Authenticated（認証済み）、Aborting（認証断念中）、Held（待機中）、Force_Auth（「認証済み」に固定設定）、Force_Unauth（「未認証」に固定設定）のいずれか。SUPPLICANT ポートの場合は、Acquired（要求中）、Connecting（接続中）、Authenticating（認証中）、Authenticated（認証済み）、Held（待機中）、Logoff（ログオフ）のいずれか。SET PORTAUTH PORT コマンド/SET PORTACCESS PORT コマンドの CONTROL パラメーターに AUTHORISED を指定した場合、Authenticated（認証済み）を表示、CONTROL パラメーター UNAUTHORISED を指定した場合、Connecting（接続中）を表示する
Port Status	ポートの状態。unauthorised（未認証）か authorised（認証済み）
Backend Authenticator State	認証機構の状態。IDLE（アイドル）、INITIALISE（初期化）、RESPONSE（Supplicant から応答受信）、REQUEST（認証サーバーに要求送信）、SUCCESS（認証成功）、FAIL（認証失敗）、TIMEOUT（タイムアウト）のいずれか
VLAN ID	サプリカントが接続している VLAN の VID

表 31: STATUS を指定した場合

例

■802.1X 認証の全般的な設定と状態を表示する

```
SHOW PORTAUTH=8021 x
```

■802.1X 認証モジュールの設定を表示する

```
SHOW PORTAUTH=8021x CONFIG
```

■802.1X 認証モジュールの状態を表示する

```
SHOW PORTAUTH=8021x STATUS
```

備考・注意事項

・パラメーターに CONFIG を指定した場合、指定した認証方式でサポートしていないパラメーターも含めすべてのパラメーターの一覧が表示される。
・パラメーターはポートごとに管理され、認証方式ごとには設定できない。1 つのポートで複数の認証メカニズムを設定した場合、いずれかの認証方式でパラメーターを設定すると、SHOW CONFIG コマンドの DYNAMIC パラメーターを指定すると、各認証方式に同じ設定値が表示されるが、そのパラメーターは該当する認証方式以外では動作しない。

関連コマンド

DISABLE PORTAUTH（61 ページ）
ENABLE PORTAUTH（69 ページ）
SET PORTAUTH AUTHMETHOD（86 ページ）
SET PORTAUTH PORT（87 ページ）
SHOW PORTAUTH PORT（131 ページ）

SHOW PORTAUTH PORT

カテゴリー：スイッチング / ポート認証

SHOW PORTAUTH={**8021X**|**MACBASED**|**WEBBASED**|**ALL**} **PORT=**{***port-list***|**ALL**}
[{AUTHENTICATOR|SUPPLICANT}] [{CONFIG|STATUS}]

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

解説

指定ポートのポート認証設定を表示する。SHOW PORTACCESS PORT コマンドは同義。

パラメーター

PORTAUTH　認証方式。8021X（IEEE 802.1X 認証について表示）、MACBASED（MAC アドレスベース認証について表示）、WEBBASED（Web 認証について表示）、ALL のいずれかを指定する。デフォルトは、8021X。

PORT　スイッチポート。複数指定が可能。

AUTHENTICATOR/SUPPLICANT　802.1X 認証モジュールの設定を表示する。

CONFIG　認証モジュールの設定を表示する。

STATUS　認証モジュールの状態を表示する。

入力・出力・画面例

```
# show portauth=all port=1 authenticator config

Port 1

802.1x Authentication Information
------------------------------------------------------------------------------
PAE Type.................. Authenticator

MAC BASE Authentication Information
------------------------------------------------------------------------------
PAE Type.................. Authenticator

WEB BASE Authentication Information
------------------------------------------------------------------------------
PAE Type.................. Authenticator

Supplicant Mode........... Multiple
Supplicant Limit.......... 320
AuthControlPortControl.... Auto
quietPeriod............... 60
```

```
txPeriod.................. 30
suppTimeout............... 30
serverTimeout............. 30
maxReq.................... 2
reAuthPeriod.............. 3600
reAuthEnabled............. Enabled
reAuthMAX................. 2
vlanAssignment............ Enabled
vlanAssignmentType........ USER
secureVlan................ On
lockCount................. 3
portMoveReauth............ Disabled
ForceRenewing............. Disabled
guestVlan................. None
adminControlDirection..... Ingress
piggyBack................. -
ARP Forwarding............ Disabled
TCP Forwarding............ -
UDP Forwarding............ -



# show portauth=all port=1 authenticator status

Port 1

802.1x Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Authenticator
Supplicant Mode........... Multiple
Number of Supplicants..... 1

Attached Supplicant(s)
    MAC Address..................... 00:0A:E6:6A:CC:7F
    Authenticator PAE State......... Authenticated
    Port Status..................... Authorized
    Backend Authenticator State..... Idle
    VLAN ID......................... 1

MAC BASE Authentication Information
--------------------------------------------------------------------------------
PAE Type.................. Authenticator
Supplicant Mode........... Multiple
Number of Supplicants..... 1

Attached Supplicant(s)
    MAC Address..................... 00:0A:E6:6A:CC:7F
    Authenticator PAE State......... Connecting
    Port Status..................... Authorized
    Backend Authenticator State..... Idle
    VLAN ID......................... 1
```

```
WEB BASE Authentication Information
--------------------------------------------------------------------------------
PAE Type................. Authenticator
Supplicant Mode.......... Multiple
Number of Supplicants..... 1

Attached Supplicant(s)
    MAC Address..................... 00:0A:E6:6A:CC:7F
    Authenticator PAE State......... Connecting
    Port Status..................... Authorized
    Backend Authenticator State..... Idle
    VLAN ID......................... 1



# show portauth all port=2 supplicant config

Port 2

802.1x Authentication Information
--------------------------------------------------------------------------------
PAE Type................. Supplicant
heldPeriod..................... 60
authPeriod..................... 30
startPeriod.................... 30
maxStart....................... 3
username....................... test
password....................... test



# show portauth all port=2 supplicant status

Port 2

802.1x Authentication Information
--------------------------------------------------------------------------------
PAE Type................. Supplicant
Supplicant PAE State............ Connecting
```

Port	ポート番号
PAE Type（802.1x Authentication Information）	スイッチポートのタイプ（802.1X における役割）。Authenticator、Supplicant のいずれか

PAE Type（MAC BASED Authentication Information）	スイッチポートのタイプ（MAC ベース認証における役割）。Authenticator、Supplicant のいずれか
PAE Type（WEB BASED Authentication Information）	スイッチポートのタイプ（Web 認証における役割）。Authenticator、Supplicant のいずれか
Supplicant Mode	（Authenticator ポート）Authenticator ポートのモード。Single か Multiple
Supplicant Limit	（Authenticator ポート）SUPPLICANT の最大接続数
AuthControl-PortControl	（Authenticator ポート）手動設定による Authenticator ポートの状態。Auto、ForceUnauth か ForceAuth
quietPeriod	（Authenticator ポート）認証失敗後、Supplicant との通信を拒否する期間（秒）
txPeriod	（Authenticator ポート）Supplicant に EAPOL パケットを再送信する間隔（秒）
suppTimeout	（Authenticator ポート）Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間（秒）
serverTimeout	（Authenticator ポート）RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間（秒）
maxReq	（Authenticator ポート）Supplicant に対する EAPOL-Request パケットの最大再送回数
reAuthPeriod	（Authenticator ポート）Supplicant を再認証する間隔（秒）
reAuthEnabled	（Authenticator ポート）Supplicant ポートの再認証を行うかどうか。Enabled または Disabled
reAuthMax	（Authenticator ポート）Supplicant を再認証する回数
vlanAssignment	（Authenticator ポート）ダイナミック VLAN の有効・無効。Enabled または Disabled
vlan-Assignment-Type	（Authenticator ポート）ダイナミック VLAN のタイプ。PORT または、USER
secureVlan	（Authenticator ポート）Multi-Supplicant モード（MODE=MULTI）のとき、2 番目以降の Supplicant の認証方法。On（最初の Supplicant と同じ VLAN でなければ認証しない）か Off（有効 VLAN であれば認証する）
lockCount	（Authenticator ポート）Web 認証において、Held の状態になるまでの 認証の連続失敗回数
portMove-Reauth	（Authenticator ポート）認証済みの Supplicant がポートを移動したときに、再度、認証を行うかどうか。Enabled または Disabled

ForceRenewing	未サポート
guestvlan	（Authenticator ポート）ゲスト VLAN に指定した VLAN 名と VLAN ID
adminControl-Direction	（Authenticator ポート）未認証状態で、送受信したブロードキャストまたはマルチキャストパケットをどう扱うか。Ingress か Both
piggyBack	（Authenticator ポート）Piggy back モードの有効 / 無効。Enabled または Disabled
ARP Forward-ing	（Authenticator ポート）未認証状態で、ARP パケットを受信したときに 透過するか破棄するか。Enabled または Disabled
TCP Forward-ing	（Authenticator ポート）未認証状態で、透過する TCP ポートのパケット
UDP Forward-ing	（Authenticator ポート）未認証状態で、透過する UDP ポートのパケット

表 32: AUTHENTICATOR、CONFIG を指定した場合

Port	ポート番号
PAE Type	スイッチポートのタイプ。Authenticator、Supplicant のいずれか
Supplicant Mode	Authenticator ポートのモード。Single か Multiple
Number of Supplicant	サプリカント数
Attached Supplicant(s)	ポートに接続しているサプリカントの情報を表示
MAC Address	MAC アドレスを表示
Authenticator / Supplicant PAE State	ポートの状態。（ポートのタイプが設定され、802.1X 認証モジュールが有効の場合に、次のステータスを表示する。）AUTHENTICATOR ポートの場合は、Initialize（初期化）、Connecting（接続中）、Authenticating（認証中）、Authenticated（認証済み）、Aborting（認証断念中）、Held（待機中）、Force_Auth（「認証済み」に固定設定）、Force_Unauth（「未認証」に固定設定）のいずれか。SUPPLICANT ポートの場合は、Acquired（要求中）、Connecting（接続中）、Authenticating（認証中）、Authenticated（認証済み）、Held（待機中）、Logoff（ログオフ）のいずれか
Port Status	ポートの状態。unauthorised（未認証）か authorised（認証済み）
Backend Authenticator State	認証機構の状態。IDLE（アイドル）、INITIALISE（初期化）、RESPONSE（Supplicant から応答受信）、REQUEST（認証サーバーに要求送信）、SUCCESS（認証成功）、FAIL（認証失敗）、TIMEOUT（タイムアウト）のいずれか

VLAN ID	サプリカントが接続している VLAN の VID

表 33: AUTHENTICATOR、STATUS を指定した場合

Port	ポート番号
PAE Type	スイッチポートのタイプ（802.1X における役割）。Authenticator、Supplicant のいずれか
heldPeriod	（Supplicant ポート）認証失敗後、Authenticator との通信を試みない期間（秒）
authPeriod	（Supplicant ポート）EAPOL-Start パケットの最大送信回数。Supplicant ポートは、EAPOL-Start パケットを MAXSTART 回送信しても応答がない場合、ポート認証の必要はないと判断する
startPeriod	（Supplicant ポート）認証失敗後、Supplicant との通信を拒否する期間（秒）
maxStart	（Supplicant ポート）Authenticator に EAPOL-Start パケットを再送信する間隔（秒）
username	ユーザー名
password	パスワード

表 34: SUPPLICANT、CONFIG を指定した場合

Port	ポート番号
PAE Type	スイッチポートのタイプ（802.1X における役割）。Authenticator、Supplicant のいずれか
Supplicant PAE State	ポートの状態。（ポートのタイプが設定され、802.1X 認証モジュールが有効の場合に、次のステータスを表示する。）AUTHENTICATOR ポートの場合は、Initialize（初期化）、Connecting（接続中）、Authenticating（認証中）、Authenticated（認証済み）、Aborting（認証断念中）、Held（待機中）、Force_Auth（「認証済み」に固定設定）、Force_Unauth（「未認証」に固定設定）のいずれか。SUPPLICANT ポートの場合は、Acquired（要求中）、Connecting（接続中）、Authenticating（認証中）、Authenticated（認証済み）、Held（待機中）、Logoff（ログオフ）のいずれか
Port Status	ポートの状態。unauthorised（未認証）か authorised（認証済み）

表 35: SUPPLICANT、STATUS を指定した場合

例

■ポート 1 の 802.1X 認証の Authenticator の設定を表示する

```
SHOW PORTAUTH=8021x PORT=1 AUTHENTICATOR
```

関連コマンド

DISABLE PORTAUTH（61 ページ）
ENABLE PORTAUTH（69 ページ）
SET PORTAUTH AUTHMETHOD（86 ページ）
SET PORTAUTH PORT（87 ページ）
SHOW PORTAUTH（123 ページ）

SHOW RRPSNOOPING

カテゴリー：スイッチング / RRP Snooping

SHOW RRPSNOOPING

解説

RRP Snooping の状態を表示する。

入力・出力・画面例

```
# show rrpsnooping

RRP Snooping Status:
 Status ..............................Disabled
```

Status	RRP Snooping の状態。Enabled か Disabled

表 36:

例

■RRP Snooping の状態を表示する

```
SHOW RRPSNOOPING
```

関連コマンド

DISABLE RRPSNOOPING（62 ページ）
ENABLE RRPSNOOPING（70 ページ）
SHOW RRPSNOOPING（138 ページ）

SHOW SWITCH

カテゴリー：スイッチング / 一般コマンド

SHOW SWITCH

解説

スイッチングモジュールの全般的情報を表示する。

入力・出力・画面例

```
# show switch

Switch Information:

 Application Software Version ......... ATS63 v2.4.1J
 Application Software Build Date ...... Jan 25 2008 10:45:48
 Bootloader Version ................... ATS63_LOADER v2.0.1
 Bootloader Build Date ................ Jan 19 2007 13:42:08
 MAC Address .......................... 00:09:41:FC:59:47
 VLAN Mode ............................ User Configured
 Ingress Filtering .................... OFF
 Active Spanning Tree version ......... RSTP
 Mirroring State ...................... Disabled
 Enhanced Stacking mode ............... Slave
 Console Disconnect Timer Interval .... 10 minute(s)

 Web Server Status .................... Disabled
 Telnet Server status ................. Enabled
 Telnet insert NULL ................... OFF
 MAC address aging time ............... 300 second(s)
 Console Startup Mode ................. CLI
 Multicast Mode ....................... Do Not Forward
```

Application Software Version	ファームウェアの名称、バージョン
Application Software Build Date	ファームウェアのビルト
Bootloader Version	ブートイメージの名称、バージョン
Bootloader Build Date	ブートイメージのビルト
MAC Address	MAC アドレス
VLAN Mode	VLAN モード。User Configured のみ
Ingress Filtering	イングレスフィルタリングの有効・無効。ON か OFF
Active Spanning Tree version	現在のスパニングツリーのバージョン
Mirroring State	ポートミラーリング機能の状態。Enabled か Disabled

Enhanced Stacking mode	エンハンストスタッキンググループ内での役割。Master、Slave または Unavailable
Console Disconnect Timer Interval	コンソールのタイムアウト時間
Web Server Status	HTTP サーバーの状態。Enabled か Disabled
Telnet Server Status	Telnet サーバーの状態。Enabled か Disabled
Telnet insert NULL	CR のあとにヌル文字を挿入するかどうか。ON か OFF
MAC address aging time	フォワーディングデータベースのエージングタイム
Console Startup Mode	CLI のみ
Multicast Mode	マルチキャストフレームのフラッディング仕様。Do Not Forward、Forward Across VLANs、Forward within VLAN (untagged ports)、または、Forward within VLAN (all ports)

表 37:

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（76 ページ）

SHOW SWITCH COUNTER

カテゴリー：スイッチング / 一般コマンド

SHOW SWITCH COUNTER

解説

スイッチングモジュールの統計カウンターを表示する。

入力・出力・画面例

```
# show switch counter

Switch Statistics:

Port: All

Bytes Rx ......... 2120                Bytes Tx ......... 2488
Frames Rx ........ 12                  Frames Tx ........ 38
Bcast Frames Rx .. 8                   Bcast Frames Tx .. 2
Mcast Frames Rx .. 0                   Mcast Frames Tx .. 31
Frames 64 ........ 35                  Frames 65-127 .... 8
Frames 128-255 ... 7                   Frames 256-511 ... 0
Frames 512-1023 .. 0                   Frames 1024-1518 . 0
CRC Error ........ 0                   Jabber ........... 0

No. of Rx Errors . 0                   No. of Tx Errors . 0
UnderSize Frames . 0                   OverSize Frames .. 0
Fragments ........ 0                   Collision ........ 0
Frames 1519-1522 . 0                   Dropped Frames ... 1
```

受信フレーム情報	
Bytes Rx	受信バイト数
Frames Rx	受信フレーム数
Bcast Frames Rx	ブロードキャストフレーム受信数
Mcast Frames Rx	マルチキャストキャストフレーム受信数
CRC Error	CRC エラーのあるフレーム数。
Jabbers	ジャバーフレーム受信数。1518 オクテットより長いフレームのうち、不正な FCS を持つものの総数。アライメントエラーパケットも含む。
No. of Rx Errors	受信エラーの数
UnderSize Frames	アンダーサイズフレーム数。正しい形式であるが、長さが 64 オクテットより短いフレームの総数

OverSize Frames	オーバーサイズフレーム送信数。正しい形式であるが、長さが 1518 オクテットより長いパケットの総数
Fragments	フラグメントフレーム送信数。不正な FCS を持ち、なおかつ、長さが 64 オクテットより短いフレームの総数。アライメントエラーを含む。
送信フレーム情報	
Bytes Tx	送信バイト数
Frames Tx	送信フレーム数
Bcast Frames Tx	ブロードキャストフレーム送信数
Mcast Frames Tx	マルチキャストキャストフレーム送信数
No. of Tx Errors	送信エラーの数
Collision	コリジョンフレーム総数
Dropped Frames	受信ポートでとりこぼされたフレームの数
RMON フレーム情報	
Frames 64 Bytes	64 バイト長のフレーム送受信数
Frames 65-127 Bytes	65〜127 バイト長のフレーム送受信数
Frames 128-255 Bytes	128〜255 バイト長のフレーム送受信数
Frames 256-511 Bytes	256〜511 バイト長のフレーム送受信数
Frames 512-1023 Bytes	512〜1023 バイト長のフレーム送受信数
Frames 1024-1518 Bytes	1024〜1518 バイト長のフレーム送受信数
Frames 1519-1522 Bytes	1519〜1522 バイト長のフレーム送受信数（タグフレーム）

表 38:

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

RESET SWITCH（76 ページ）
SHOW SWITCH（139 ページ）

SHOW SWITCH MIRROR

カテゴリー：スイッチング / ポート

SHOW SWITCH MIRROR

解説

ポートミラーリング機能の設定を表示する。

入力・出力・画面例

```
# show switch mirror

Port Mirroring:
Mirroring State..................... Enabled
Mirror-To (Destination) Port........ 10
Ingress(Rx) Mirror(Source) Ports..... 1-5
Egress(Tx) Mirror(Source) Ports...... 1-5
```

Mirroring State	ポートミラーリング機能の有効・無効。Enabled か Disabled
Mirror-To (Destination) Port	ミラーポート
Ingress(Rx) Mirror(Source) Ports	受信パケットをミラーリングするソースポート
Egress(Tx) Mirror(Source) Ports	送信パケットをミラーリングするソースポート

表 39:

関連コマンド

SET SWITCH MIRROR（94 ページ）
SET SWITCH PORT MIRROR（99 ページ）
SHOW SWITCH（139 ページ）
SHOW SWITCH PORT（144 ページ）

SHOW SWITCH PORT

カテゴリー：スイッチング / ポート

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

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

解説

スイッチポートの情報を表示する。

パラメーター

PORT　ポート番号。指定しない場合はすべてのポートが対象となる。

入力・出力・画面例

```
# show switch port=1

Port #1 Information:

 Port Description (ifName) ............ Port_01
 Port Type ............................ 10/100/1000Base-T
 Status ............................... Enabled
 Link State ........................... Down
 Configured Speed/Duplex .............. Auto
 Configured MDI Crossover ............. N/A
 Actual Speed/Duplex .................. -
 Actual MDI Crossover ................. -
 Flow Control Status .................. Disabled
 Flow Control Threshold ............... 7935 cells
 Backpressure Status .................. Disabled

 Backpressure Threshold ............... 7935 cells
 Broadcast Ingress Filtering .......... Disabled
 Broadcast Egress Filtering ........... Disabled
 Unknown Multicast Ingress Filtering .. Disabled
 Unknown Multicast Egress Filtering ... Disabled
 Unknown Unicast Ingress Filtering .... Disabled
 Unknown Unicast Egress Filtering ..... Disabled
 Broadcast Rate Limiting Status ....... Disabled
 Broadcast Rate ....................... 262143 packet/second
 Multicast Rate Limiting Status ....... Disabled
 Multicast Rate ....................... 262143 packet/second
 Unknown Unicast Rate Limiting Status . Disabled
 Unknown Unicast Rate ................. 262143 packet/second
```

```
PVID ..............................1
Port Priority (0-7) 0=Low 7=High..... 0

Override Priority ..................No
Mirroring State.....................Disabled
```

Port Description	ポート名称（メモ）
Port Type	ポートの種類
Status	ポートのステータス。Enabled か Disabled。受信レート検出により Disabled になった場合、”Disabled by Detection Functions”となる。
Link state	ポートのリンクステータス。Up か Down。受信レート検出によりリンクダウンした場合は” Down by Storm Detection”。
Configured Speed / Duplex	通信モードの設定値。Auto、10Mbps、100Mbps / Half Duplex、Full Duplex で表示される
Configured MDI Crossover	MDI / MDI-X の設定値。N / A、MDI、MDI-X で表示される。
Actual speed / duplex	実際の通信モード
Actual MDI Crossover	実際の MDI / MDI-X
Flow Control Status	フローコントロール（802.1x　PAUSE）の状態
Flow Control Threshold	フローコントロール（802.1x　PAUSE）が実行される受信パケット数
Backpressure Status	バックプレッシャーの状態（未サポート）
Backpressure Threshold	バックプレッシャーが実行される受信パケット数（未サポート）
Broadcast Ingress Filtering	ブロードキャストパケットのフィルタリング機能の有効・無効。Enabled か Disabled。受信レート検出により Disabled になった場合、”Disabled by Detection Functions”となる。
Broadcast Egress Filtering	ブロードキャストパケットのフィルタリング機能の有効・無効。Enabled か Disabled。Enabled のときは、ブロードキャストパケットは送信されず、Disabled のときは送信される。受信レート検出により Enabled になった場合、”Enabled by Loop / Storm Detection”となる。
Unknown Multicast Ingress Filtering	未学習のマルチキャストパケットのフィルタリング機能の有効・無効。Enabled か Disabled
Unknown Multicast Egress Filtering	未学習のマルチキャストパケットのフィルタリング機能の有効・無効。Enabled か Disabled。Enabled のときは、未学習のマルチキャストパケットは送信されず、Disabled のときは送信される。

Unknown Unicast Ingress Filtering	未学習のユニキャストパケットのフィルタリング機能の有効・無効。Enabled か Disabled
Unknown Unicast Egress Filtering	未学習のユニキャストパケットのフィルタリング機能の有効・無効。Enabled か Disabled。Enabled のときは、未学習のユニキャストパケットは送信されず、Disables のときは送信される。
Broadcast Rate Limiting Status	ブロードキャストパケットの受信上限値の設定を行うかどうか。Enabled か Disabled
Broadcast Rate	ブロードキャストパケットの 1 秒当たり最大受信数。
Multicast Rate Limiting Status	マルチキャストパケットの受信上限値の設定を行うかどうか。Enabled か Disabled
Multicast Rate	マルチキャストパケットの 1 秒当たり最大受信数。
Unknown Unicast Rate Limiting Status	未学習のユニキャストパケットの受信上限値の設定を行うかどうか。Enabled か Disabled
Unknown Unicast Rate	未学習のユニキャストパケットの 1 秒当たり最大受信数。
PVID	ポートが所属するポートベース VLAN 名（VID）
Port Priority (0-7) 0=Low 7=High	QoS の優先順位。
Override Priority	ポートプライオリティーとタグプライオリティーのどちらを優先するか。YES の場合は、ポートプライオリティーを優先する。NO の場合は、タグプライオリティーを優先する。
Mirroring State	ポートモニター機能の有効・無効

表 40:

例

■ポート 1 の情報を表示する

```
SHOW SWITCH PORT=1
```

関連コマンド

SET SWITCH PORT（96 ページ）

SHOW SWITCH PORT COUNTER

カテゴリー：スイッチング / ポート

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

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

解説

スイッチポートの統計カウンターを表示する。

パラメーター

PORT　ポート番号。指定しない場合はすべてのポートの統計カウンターを表示する。

入力・出力・画面例

```
# show switch port=1 counter

Port Statistics:

Port: 1

Bytes Rx ......... 0                    Bytes Tx ......... 1472
Frames Rx ........ 0                    Frames Tx ........ 23
Bcast Frames Rx .. 0                    Bcast Frames Tx .. 0
Mcast Frames Rx .. 0                    Mcast Frames Tx .. 23
Frames 64 ........ 23                   Frames 65-127 .... 0
Frames 128-255 ... 0                    Frames 256-511 ... 0
Frames 512-1023 .. 0                    Frames 1024-1518 . 0
CRC Error ........ 0                    Jabber ........... 0

No. of Rx Errors . 0                    No. of Tx Errors . 0
UnderSize Frames . 0                    OverSize Frames .. 0
Fragments ........ 0                    Collision ........ 0
Frames 1519-1522 . 0                    Dropped Frames ... 0
```

受信フレーム情報	
Bytes Rx	受信バイト数
Frames Rx	受信フレーム数
Bcast Frames Rx	ブロードキャストフレーム受信数
Mcast Frames Rx	マルチキャストキャストフレーム受信数

CRC Error	CRC エラーのあるフレーム数。
Jabbers	ジャバーフレーム受信数。1518 オクテットより長いフレームのうち、不正な FCS を持つものの総数。アライメントエラーパケットも含む。
No. of Rx Errors	受信エラーの数
UnderSize Frames	アンダーサイズフレーム数。正しい形式であるが、長さが 64 オクテットより短いフレームの総数
OverSize Frames	オーバーサイズフレーム受信数。正しい形式であるが、長さが 1518 オクテットより長いパケットの総数
Fragments	フラグメントフレーム受信数。不正な FCS を持ち、なおかつ、長さが 64 オクテットより短いフレームの総数。アライメントエラーを含む。
送信フレーム情報	
Bytes Tx	送信バイト数
Frames Tx	送信フレーム数
Bcast Frames Tx	ブロードキャストフレーム送信数
Mcast Frames Tx	マルチキャストキャストフレーム送信数
No. of Tx Errors	送信エラーの数
Collision	コリジョンフレーム総数
Dropped Frames	受信ポートでとりこぼされたフレームの数
RMON フレーム情報	
Frames 64 Bytes	64 バイト長のフレーム送受信数
Frames 65-127 Bytes	65〜127 バイト長のフレーム送受信数
Frames 128-255 Bytes	128〜255 バイト長のフレーム送受信数
Frames 256-511 Bytes	256〜511 バイト長のフレーム送受信数
Frames 512-1023 Bytes	512〜1023 バイト長のフレーム送受信数
Frames 1024-1518 Bytes	1024〜1518 バイト長のフレーム送受信数
Frames 1519-1522 Bytes	1519〜1522 バイト長のフレーム送受信数（タグフレーム）

表 41:

例

■ポート 1 の統計カウンターを表示する

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

関連コマンド

SET SWITCH PORT（96 ページ）
SHOW SWITCH COUNTER（141 ページ）

SHOW SWITCH PORT（144 ページ）

SHOW SWITCH PORT INTRUSION

カテゴリー：スイッチング / ポート

SHOW SWITCH PORT={*port-list*|ALL} INTRUSION

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

解説

ポートセキュリティー機能が有効のとき（SECURITYMODE が LIMITED で、すでに学習済み MAC アドレスが制限値に達している場合、または SECURITYMODE が SECURED の場合)、未知の送信元 MAC アドレスを持つパケットを受信したかどうかを表示する。

パラメーター

PORT　ポート番号。指定しない場合はすべてのポートが対象となる。

入力・出力・画面例

```
# show switch port intrusion
Port   Intrusion Status
-------------------------------
1       Intrusion Detected
2       No Intrusion
3       No Intrusion
4       No Intrusion
5       No Intrusion
6       No Intrusion
7       No Intrusion
8       No Intrusion
9       No Intrusion
10      No Intrusion
11      No Intrusion
12      No Intrusion
13      No Intrusion
14      No Intrusion
15      No Intrusion
16      No Intrusion
17      No Intrusion
18      No Intrusion
19      No Intrusion
20      No Intrusion
21      No Intrusion
22      No Intrusion
23      No Intrusion
```

```
24      No Intrusion
```

Port	ポート番号
Intrusion Status	不正なパケットを受信したかどうか。Intrusion Detected（受信有り）か No Intrusion（受信なし）

表 42:

備考・注意事項

関連コマンド

SET SWITCH PORT SECURITYMODE（100 ページ）

SHOW SWITCH PORT SECURITYMODE

カテゴリー：スイッチング / ポート

SHOW SWITCH PORT={***port-list***|**ALL**} **SECURITYMODE**

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

セキュリティーモードに関する情報を表示する。

パラメーター

PORT　ポート番号。指定しない場合はすべてのポートが対象となる。

入力・出力・画面例

```
# show switch port securitymode
Port   Security Mode      Intrusion Action    Participating    MAC Limit
-------------------------------------------------------------------------
1      Limited            Discard             No               0/20
2      Automatic          ----                ----             ----
3      Automatic          ----                ----             ----
4      Automatic          ----                ----             ----
5      Automatic          ----                ----             ----
6      Automatic          ----                ----             ----
7      Automatic          ----                ----             ----
8      Automatic          ----                ----             ----
9      Automatic          ----                ----             ----
10     Automatic          ----                ----             ----
11     Automatic          ----                ----             ----
12     Automatic          ----                ----             ----
13     Automatic          ----                ----             ----
14     Automatic          ----                ----             ----
15     Automatic          ----                ----             ----
16     Automatic          ----                ----             ----
17     Automatic          ----                ----             ----
18     Automatic          ----                ----             ----
19     Automatic          ----                ----             ----
20     Automatic          ----                ----             ----
21     Automatic          ----                ----             ----
22     Automatic          ----                ----             ----
23     Automatic          ----                ----             ----
24     Automatic          ----                ----             ----
```

Port	ポート番号
Security Mode	セキュリティーモードの設定。Automatic、Secured または Limited
Intrusion Action	セキュリティーモードが LIMITED モードの場合に、未知の送信元 MAC アドレスを持つパケットを受信したときに実行するアクションの設定。Discard / Trap / Disable
Participating	セキュリティーモードが LIMITED モードで、INTRUSIONACTION に TRAP または DISABLE が設定されている場合、指定したアクションを実行するかしないか。On か Off
MAC Limit	セキュリティーモードが LIMITED モードの場合に、該当ポートで学習済みの MAC アドレス数と学習可能な送信元 MAC アドレス（ダイナミックエントリー）の最大数

表 43:

備考・注意事項

関連コマンド

SET SWITCH PORT SECURITYMODE（100 ページ）

SHOW SWITCH PORT STORMDETECTION

カテゴリー：スイッチング / ポート

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

受信レート検出の設定、状態、カウンターの情報を表示する

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。指定したポートが存在しない場合はエラーとする。

CONFIG　受信レート検出の設定情報を表示する。

STATUS　受信レート検出の状態情報を表示する。

COUNTER　受信レート検出のカウンター情報を表示する。C

入力・出力・画面例

```
# show switch po=1,2 stormdetection config

Switch Storm Detection Configuration
---------------------------------------------------------------
Port ........................ 1
 Status ..................... Enabled
 High Rate Action ........... LinkDown
 Low Rate Action ............ None
 High Rate Threshold ......... 819200 Kbps
 Low Rate Threshold .......... 512000 Kbps
 Blocking Timeout ............ 300 sec

Port ........................ 2
 Status ..................... Enabled
 High Rate Action ........... LinkDown

 Low Rate Action ............ None
 High Rate Threshold ......... 819200 Kbps
 Low Rate Threshold .......... 512000 Kbps
 Blocking Timeout ............ 300 sec

# show switch po=1,2 stormdetection status
```

```
Switch Storm Detection Status
----------------------------------------------------------------
 Port  Threshold  Storm     Expiry  Port Status      Bcast Status
----------------------------------------------------------------
 1     High       Normal    --      Enabled          Forward
       Low        Normal    --
 2     High       Normal    --      Enabled          Forward
       Low        Normal    --

# show switch po=1,2 stormdetection counter

Switch Storm Detection Counter
-------------------------------------------------------------------------------
 Port  Detected(High)  Action(High)  Detected(Low)  Action(Low)  Rx Rate(Kbps)
-------------------------------------------------------------------------------
 1                  0             0              0            0             0
 2                  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（なにもしない）、BcastDiscard(ブロードキャストパケットを破棄する)、Linkdown（ポートを物理的にリンクダウンさせる）。
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（なにもしない）、BcastDiscard(ブロードキャストパケットを破棄する)、Linkdown（ポートを物理的にリンクダウンさせる）。
High Rate Threshold	受信レートの高レート時のしきい値。値は Kbps (Kilo bit per second)。
Low Rate Threshold	受信レートの低レート時のしきい値。値は Kbps (Kilo bit 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。

表 44: 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。単位は秒。
Port Status	該当ポートの状態。ポートが Disable のときは、”Disabled(Act)” または ”Disabled(User)” と表示される。アクション実行によってポートが Disable にされた場合 Disabled(Act)、ユーザーがコマンドによってポートを Disable にした場合 Disabled(User) と表示される。

Bcast Status	該当ポートのブロードキャストフレームの通信状態。ブロードキャストフレームを破棄しているときは、”Discard(Act)” または ”Discard(User)” と表示される。アクション実行によってブロードキャストフレームが破棄される場合 Discard(Act)、ユーザーがコマンドによってブロードキャストフレームを破棄する設定をした場合 Discard(User) と表示。

表 45: STATUS 指定時

Port	ポート番号。
Detected(High)	高レート検出回数。
Action(High)	High Rate Action 実行回数。
Detected(Low)	低レート検出回数。
Action(Low)	Low Rate Action 実行回数。
Rx Rate(bps)	コマンド実行時の受信レート。

表 46: COUNTER 指定時

関連コマンド

DISABLE SWITCH PORT STORMDETECTION（65 ページ）
ENABLE SWITCH PORT STORMDETECTION（73 ページ）
RESET SWITCH PORT STORMDETECTION COUNTER（78 ページ）
SET SWITCH PORT STORMDETECTION（102 ページ）

SHOW SWITCH TRUNK

カテゴリー：スイッチング / ポート

SHOW SWITCH TRUNK[=*trunk*]

trunk: トランクグループ名（1〜16 文字。英数字が使用可能。大文字小文字を区別しない）

解説

トランクグループの情報を表示する。

パラメーター

TRUNK　トランクグループ名。省略時はすべてのトランクグループの情報が表示される。

入力・出力・画面例

```
# show switch trunk
Switch trunk group(s)
--------------------------------------------------------------------------

Trunk group ID ..................... 1
   Trunk Status   .................. DOWN
   Trunk group name ................ trunk1
   Trunk method .................... SRC/DST IP
   Ports ........................... 2-5
--------------------------------------------------------------------------
```

Trunk group ID	トランクグループの ID
Trunk group name	トランクグループ名
Trunk method	送出ポートの選択基準
Ports	所属ポート

表 47:

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（54 ページ）
CREATE SWITCH TRUNK（55 ページ）
DELETE SWITCH TRUNK（57 ページ）
DESTROY SWITCH TRUNK（58 ページ）
SET SWITCH TRUNK（104 ページ）

SHOW WEBAUTHSERVER

カテゴリー：スイッチング / ポート認証

SHOW WEBAUTHSERVER

解説

Web 認証サーバーの情報を表示する。

入力・出力・画面例

```
# show webauthserver
Web Authentication Server Information:
 Status ............................. Enabled
 IP Address ......................... 0.0.0.0
 Port ............................... 80(80), 443(443)
 Listen Port ........................ Open
 SSL Security ....................... Disabled
 SSL Key ID ......................... none
 Redirect URL .......................
 Header .............................
 Sub Header Top .....................
 Sub Header Bottom...................
 Footer .............................
 Ping Poll .......................... Disabled
 Normal Interval .................... 30

 Timeout ............................ 1
 Fail Count ......................... 5
 Reauth Refresh ..................... Disabled
 Temporary IP ....................... Disabled
 Temporary IP Renewal Time .......... 5
 Temporary IP Rebinding Time ........ 8
 Temporary IP Server Lease Time ..... 20
```

Status	Web 認証サーバーの状態。Enabled または Disabled
IP Address	Web 認証サーバーの IP アドレス
Port	Web 認証サーバーの TCP ポート番号,Web 認証サーバーの HTTPS の TCP ポート番号
Listen Port	ポートの状態。
SSL Security	Web 認証サーバーの HTTPS の有効・無効。Enabled または Disabled

SSL Key ID	Web 認証サーバーの HTTP にて使用する SSL 鍵の鍵番号
Redirect URL	Web 認証の成功後に 自動的にジャンプするページの URL
Header	Web 認証ログインページのヘッダー部の表示内容
Sub Header Top	Web 認証ログインページのサブヘッダーの上部の表示内容
Sub Header Bottom	Web 認証ログインページのサブヘッダーの下部の表示内容
Footer	Web 認証ログインページのフッター部の表示内容
Ping Poll	Ping ポーリング機能の有効・無効。Enabled または Disabled
Normal Interval	認証機器が通信可能のときのポーリング間隔（秒）
Timeout	Ping パケットの応答待ち時間（秒）
Fail Count	到達性が失われたと判断するために必要な Ping 無応答の回数
Reauth Refresh	認証機器より Ping 応答がある間、再認証タイマー (REAUTH-PERIOD) を更新するかの設定。Enabled または Disabled
Temporary IP	Web 認証サーバーへ一時的にアクセスできるように、未認証の Supplicant に IP アドレスを付与するかの設定。Enabled または Disabled
Temporary IP Renewal Time	IP アドレスの更新間隔
Temporary IP Rebinding Time	IP アドレスの再割り当て間隔
Temporary IP Server Lease Time	IP アドレスのリース時間

表 48:

関連コマンド

DISABLE WEBAUTHSERVER（66 ページ）
ENABLE WEBAUTHSERVER（74 ページ）
SET WEBAUTHSERVER（105 ページ）
SHOW PORTAUTH（123 ページ）
SHOW PORTAUTH PORT（131 ページ）