

スイッチング

概要・基本設定	5
ポートの指定方法	5
基本コマンド	5
ポートランキング	6
ポートミラーリング	7
基本設定	8
ポートセキュリティー	9
パケットストームプロテクション	12
ループガード	12
LDF 検出	13
受信レート検出	14
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	15
EPSP Snooping	16
基本設定	16
構成上の注意事項	17
ポート認証	19
概要	19
802.1X 認証方式	21
基本設定	21
Supplicant として使用する際の設定例	22
MAC ベース認証方式	22
基本設定	22
Web 認証方式	24
Ping ポーリング機能	25
HTTP リダイレクト	26
HTTP サーバーの基本設定	27
HTTPS サーバーの基本設定	28
機能・用語の説明	33
ダイナミック VLAN	33
ゲスト VLAN	35
ポートの移動について	35
認証アルゴリズムの併用	36
設定例	41
ダイナミック VLAN の設定例	41

ゲスト VLAN の設定例	43
テンポラリー IP アドレスを利用する場合の設定例	44
プロキシサーバーを使用した場合の設定例	47
マルチプル VLAN (Protected Ports VLAN) を用いた設定例	52
資料編	56
Web 認証の画面遷移	56
認証ログ	62
認証サーバーの設定	68
DHCP Snooping	70
概要	70
登録できるクライアントの数	71
基本設定	71
RRP Snooping	75
コマンドリファレンス編	77
機能別コマンド索引	77
ACTIVATE SWITCH PORT AUTONEGOTIATE	80
ADD DHCP Snooping	81
ADD SWITCH TRUNK	83
CREATE DHCP Snooping MACFILTER	84
CREATE SWITCH TRUNK	86
DELETE DHCP Snooping	88
DELETE SWITCH TRUNK	89
DESTROY DHCP Snooping MACFILTER	90
DESTROY SWITCH TRUNK	91
DISABLE DHCP Snooping	92
DISABLE DHCP Snooping ARPSECURITY	93
DISABLE DHCP Snooping LOG	94
DISABLE DHCP Snooping OPTION82	95
DISABLE ESR Snooping	96
DISABLE PORTAUTH	97
DISABLE PORTAUTH PORT LOGTYPE	98
DISABLE RRP Snooping	99
DISABLE SWITCH PORT	100
DISABLE SWITCH PORT FLOW	101
DISABLE SWITCH PORT LOOPDETECTION	102
DISABLE SWITCH PORT STORMDETECTION	103
DISABLE WEBAUTHSERVER	104
ENABLE DHCP Snooping	105
ENABLE DHCP Snooping ARPSECURITY	106
ENABLE DHCP Snooping LOG	107
ENABLE DHCP Snooping OPTION82	108
ENABLE ESR Snooping	109

ENABLE PORTAUTH	110
ENABLE PORTAUTH PORT LOGTYPE	111
ENABLE RRPSNOOPING	112
ENABLE SWITCH PORT	113
ENABLE SWITCH PORT FLOW	114
ENABLE SWITCH PORT LOOPDETECTION	115
ENABLE SWITCH PORT STORMDETECTION	116
ENABLE WEBAUTHSERVER	117
PURGE DHCP Snooping	118
PURGE SWITCH PORT	119
PURGE WEBAUTHSERVER	120
RESET DHCP Snooping Counter	121
RESET DHCP Snooping Database	122
RESET PORTAUTH PORT	123
RESET SWITCH	124
RESET SWITCH PORT	125
RESET SWITCH PORT LOOPDETECTION Counter	126
RESET SWITCH PORT STORMDETECTION Counter	127
SET DHCP Snooping CheckInterval	128
SET DHCP Snooping CheckOptions	129
SET DHCP Snooping MacFilter	130
SET DHCP Snooping Port	131
SET PORTAUTH AuthMethod	133
SET PORTAUTH CSIDFormat	134
SET PORTAUTH PORT	136
SET PORTAUTH UserIDFormat	141
SET SWITCH InFiltering	143
SET SWITCH Mirror	144
SET SWITCH MulticastMode	145
SET SWITCH PORT	146
SET SWITCH PORT LOOPDETECTION	149
SET SWITCH PORT Mirror	151
SET SWITCH PORT SecurityMode	152
SET SWITCH PORT STORMDETECTION	154
SET SWITCH Trunk	156
SET WEBAUTHSERVER	157
SHOW DHCP Snooping	160
SHOW DHCP Snooping Counter	162
SHOW DHCP Snooping Database	164
SHOW DHCP Snooping MacFilter	167
SHOW DHCP Snooping Port	169
SHOW RRPSNOOPING	171

SHOW PORTAUTH	172
SHOW PORTAUTH PORT	178
SHOW RRPSNOOPING	185
SHOW SWITCH	186
SHOW SWITCH COUNTER	188
SHOW SWITCH MIRROR	190
SHOW SWITCH PORT	191
SHOW SWITCH PORT COUNTER	195
SHOW SWITCH PORT INTRUSION	198
SHOW SWITCH PORT LOOPDETECTION	200
SHOW SWITCH PORT SECURITYMODE	204
SHOW SWITCH PORT STORMDETECTION	206
SHOW SWITCH PORT SUMMARY	209
SHOW SWITCH TRUNK	211
SHOW WEBAUTHSERVER	213

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。

ポートをイネーブルにするには ENABLE SWITCH PORT コマンド (113 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 (100 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 (146 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 (125 ページ) を使

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 (191 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 (195 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 (125 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、所属させる SFP ポートはすべて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
- トランクグループ作成時に、同一グループに所属するポートは通信速度とデュプレックスモードおよびフローコントロールの設定を同じ設定にしなければならない (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る)
- トランクグループに所属するポートの設定変更は、グループ内のすべてのポートに反映される
- 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 (86 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。
- ✎ ポートトランキングと IGMP Snooping、MLD Snooping、ポートセキュリティー、マルチブ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、トランクグループに追加しないでください。
- ✎ トランクグループの最若番ポートを抜き差しすると、接続の組み合わせによって、ポートのリンクアップトラップが生成されない場合があります。

トランクグループの情報は SHOW SWITCH TRUNK コマンド (211 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 (86 ページ)、SET SWITCH TRUNK コマンド (156 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、トランクグループ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 ↓
```

- ✎ SELECT パラメーターに MAC アドレスの選択基準 (MACSRC、MACDEST、MACBOTH) が指定されていると、ルーティング後のパケットが負荷分散されずに送出されます。
- ✎ フラッドパケットは、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 (83 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 (89 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 (91 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 個だけ出力される。
- L3 スイッチングされるパケットは、ルーティング処理後にミラーポートに出力される。
- ソースポートを複数設定している状態で、あるソースポートから入力されたパケットが、L3 スイッチングされて別のソースポートから出力された場合、ミラーポートにはルーティング処理後のパケットが1 個だけ出力される。

- ✎ ポートミラーリング機能が有効の場合、「01:80:C2:00:00:00」などの予約マルチキャストアドレスをソースポートで受信すると、ミラーポートからパケットが重複して送信されます。

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 (144 ページ) を実行すると、指定ポートはミラーポートとして設定されます。

```
SET SWITCH MIRROR=1 ↵
```

- ✎ 本製品はミラーポートでもスイッチング動作を行います。ミラーポートと通常ポートの間でのスイッチングはサポート対象外です。

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。

- ✎ 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)。

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 (190 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 (191 ページ) の「Mirroring State」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 (144 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 (146 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、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	タグなし
タグ付き	タグの VID とミラーポートの VID が同じ	タグ付き
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。

ポートセキュリティ

ポートセキュリティは、MAC アドレスに基づき、ポートごとに通信を許可するデバイスを制限する機能です。許可していないデバイスから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 (152 ページ) でセキュリティ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 (152 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 SECURITY-MODE コマンド（152 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（152 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、PAR-

TICIPATE 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 (152 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 11 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 (204 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 (198 ページ) で確認できます。

```
SHOW SWITCH PORT INTRUSION ↓
SHOW 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 6 ページ) を使って、スタティック MAC アドレスを登録します。

```
ADD SWITCH FILTER DESTADDRESS=00-00-f4-ab-cd-ef PORT=10 VLAN=1 ↓
```

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 7 ページ) で行います。

```
DELETE SWITCH FILTER DESTADDRESS=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 (152 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 (113 ページ) でイネーブルに戻します。

```
# enable switch port=11
#

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

ポートセキュリティの設定 (セキュリティ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 91 ページ) または SAVE CONFIGURATION コマンド (「運用・管理」の 184 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。

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。カッコ内は設定パラメーターの名前です。

- ブロードキャストフレーム (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)

受信レートの設定は SET SWITCH PORT コマンド (146 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 (191 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。

ループガード

本製品ではループガードとして以下の2つをサポートしています。

ループ検出したポート番号をログ、トラップで管理者に通知することにより、ループの原因特定、対策が容易になります。設定方法については、「運用・管理」/「ログ」、「運用・管理」/「SNMP」をご覧ください。

- LDF 検出
- 受信レート検出

LDF 検出

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

LDF は、特殊な宛先 MAC アドレス (00-00-F4-27-71-01) を持った試験フレームです。

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

他の接続機器を介して機器に LDF が戻って来る場合、LDF の送信元 MAC アドレスと機器自身の MAC アドレスが一致し、かつ LDF 検出機能が有効なスイッチポート番号が LDF に記録された情報と一致すると、ループ状態と判断します。

すべてのポートで受信した LDF が判断の対象になります (LDF 検出機能が無効のポートで受信した LDF も対象です)。

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

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

- ポートをリンクダウンする。
- ポートのブロードキャストフレームのみ、受信を止める。
- 何もしない。

アクション実行後は、タイマーが起動し、指定した時間が経過する、または下記の条件でアクション実行前の状態に戻ります。

- ENABLE SWITCH PORT コマンド (113 ページ) が設定されたとき
- DISABLE SWITCH PORT コマンド (100 ページ) が設定されたとき
- リンクダウンが発生したとき (ACTION=LINKDOWN は除く)
- SET SWITCH PORT コマンド (146 ページ) で BCASTFILTERING=OFF が設定されたとき (ACTION=LINKDOWN は除く)
- LDF 検出を無効にしたとき

ポート 2 の LDF 検出機能を有効にするには ENABLE SWITCH PORT LOOPDETECTION コマンド (115 ページ) を使用します。

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

ポート 2 の LDF 送出間隔を 1 秒、LDF 検出時のアクションを BCASTDISCARD (ブロードキャストパケットを破棄する) アクションからの復帰時間を 1 時間に設定するには SET SWITCH PORT LOOPDETECTION

コマンド (149 ページ) を使用します。

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

ポート 2 の LDF 検出機能の設定情報を表示するには SHOW SWITCH PORT LOOPDETECTION コマンド (200 ページ) を使用します。

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

ポート 2 の LDF 検出機能の状態を表示するには SHOW SWITCH PORT LOOPDETECTION コマンド (200 ページ) を使用します。

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

ポート 2 の LDF 検出機能のカウンターの情報を表示するには SHOW SWITCH PORT LOOPDETECTION コマンド (200 ページ) を使用します。

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

受信レート検出

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

受信レートは 1 ポートにつき、2 レベル (LOWRATE、HIGHRATE) 設定できます。各レベルに対して、受信レートしきい値とアクションを設定できます。

受信レートがしきい値を超えたポートに対し、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。
- 何もしない。

アクション実行後は、タイマーが起動し、指定した時間が経過する、または下記の条件でアクション実行前の状態に戻ります。

- ENABLE SWITCH PORT コマンド (113 ページ) が設定されたとき
- DISABLE SWITCH PORT コマンド (100 ページ) が設定されたとき
- リンクダウンが発生したとき (ACTION=LINKDOWN は除く)
- SET SWITCH PORT コマンド (146 ページ) で BCASTFILTERING=OFF が設定されたとき (ACTION=LINKDOWN は除く)
- 受信レート検出を無効にしたとき

ポート 2 の受信レート検出機能を有効にするには ENABLE SWITCH PORT STORMDETECTION コマンド (116 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（154 ページ）を使用します。

```
SET SWITCH PORT=2 STORMDETECTION HIGHRATE THRESHOLD=1048576
HIGHRATE ACTION=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（206 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（206 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（206 ページ）を使用します。

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

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

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または、送信しないようにし、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、または、該当パケットの送信が抑止されます。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（146 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（191 ページ）で確認できます。「Broadcast Ingress Filtering」、「Broadcast Egress Filtering」、「Unknown Multicast Ingress Filtering」、「Unknown Multicast Egress Filtering」、「Unknown Unicast Ingress Filtering」、「Unknown Unicast Egress Filtering」をご覧ください。

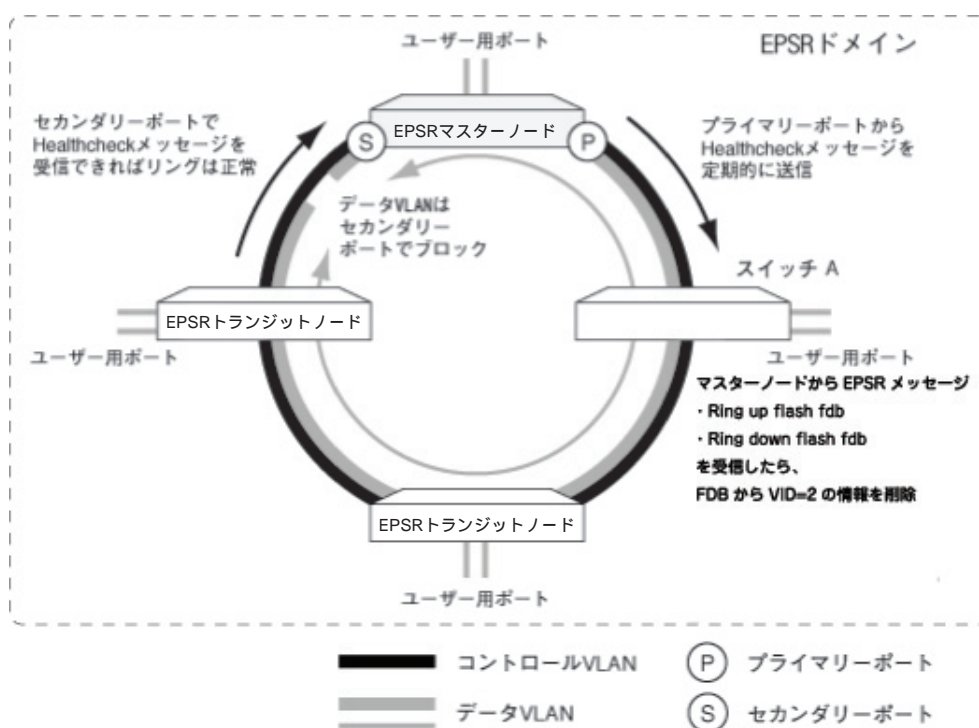
- ☞ 認証ポートに設定したポートの BCASTEGRESSFILTERING、UNKMCASTEGRESSFILTERING、UNKUCASTEGRESSFILTERING の設定は変更しないでください。

EPSR Snooping

EPSR Snooping 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 Snooping 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 (109 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 (96 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 (171 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 ↵
```

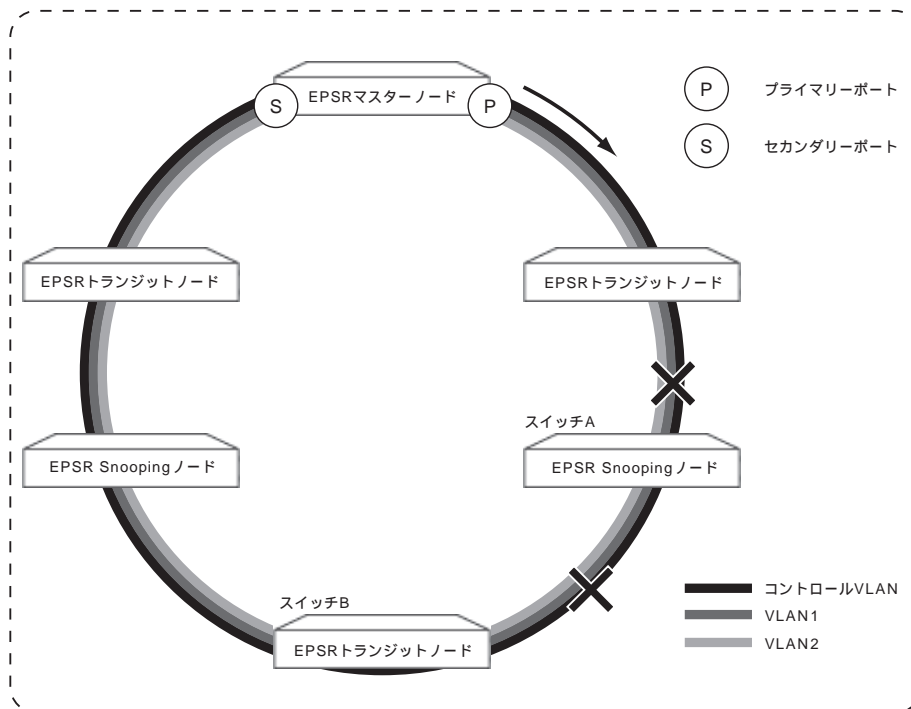
2. スイッチ A の EPSR Snooping を有効にします。

```
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。

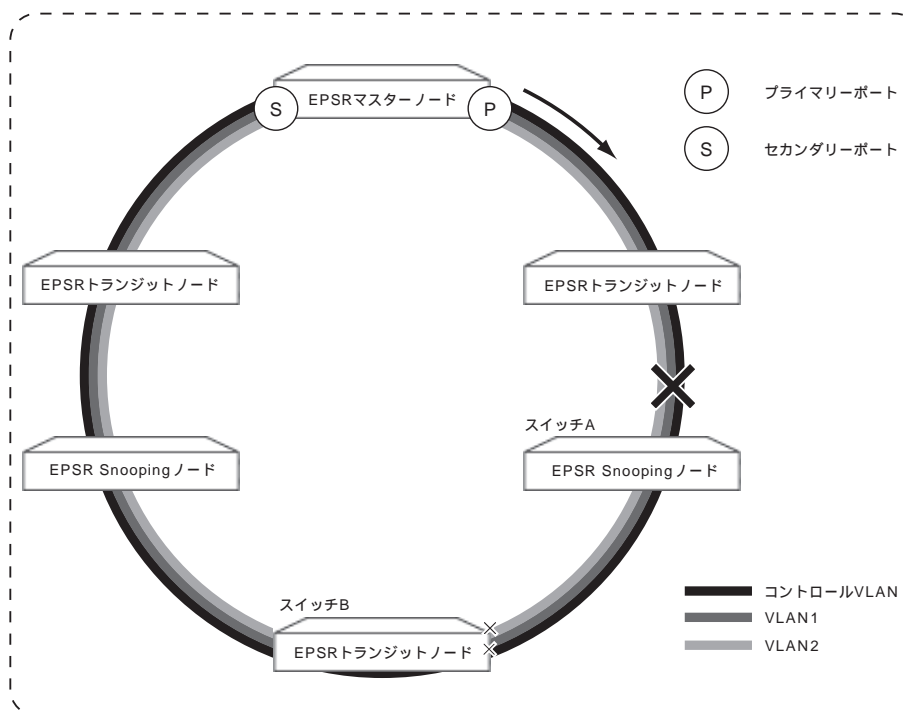
下記の図のようにスイッチ A の両端がリンクダウンしている状態を、Double Fail と呼びます。



この状態から片方のリンクダウンが復旧した場合、EPSR Snooping 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かかわらず、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

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。

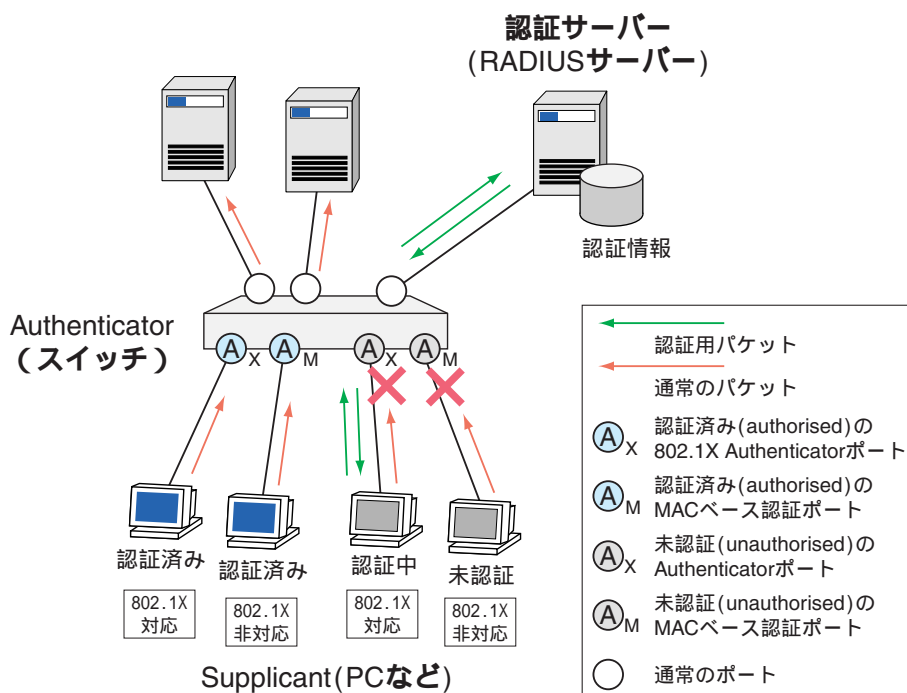
1 つのポートに複数の認証アルゴリズム（802.1X 認証/MAC ベース認証/Web 認証）を設定することもできます。後述の「認証アルゴリズムの併用」を参照してください。

- 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。

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。

- ✎ Supplicant ポートはタグ付きにはできません。
- ✎ Authenticator ポートとタグ付きポートを併用する場合は、ダイナミック VLAN、ゲスト VLAN は使用できません。
- ✎ 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。
- ✎ 認証ポートに設定されたポートは VLAN の設定を変更できません。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。
- ✎ MAC ベース認証と Web 認証では、Supplicant の MAC アドレスがエージングにより FDB から削除されると、認証許可状態が解除されます。
- ✎ 複数の VLAN インターフェースに IP を割り当てている場合、認証時に Authenticator から Radius サーバーへ送信される Radius Request Packet の NAS-IP-Address の値が 0.0.0.0 になります。
- ✎ 認証ポートでタグ付きの EAPOL-Start を受信しているにもかかわらず、認証ポートが所属するすべての VLAN タグを付与した EAP-Request と EAP-Failure を送信します。
- ✎ 認証ポートに設定するとブロードキャスト/未学習のマルチキャスト/未学習のユニキャストフレームのフィルタリング機能（BCASTEGRESSFILTERING、UNKMCASTEGRESSFILTERING、UNKUCASTEGRESSFILTERING）が自動で設定されますが、本設定は変更しないでください。

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

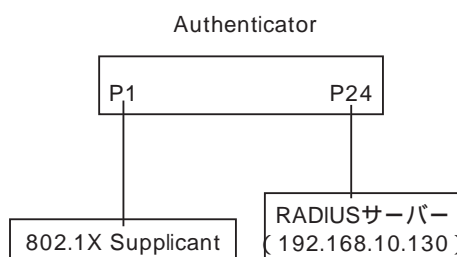
本製品を Authenticator として使用し、802.1X Supplicant を受け付ける場合の基本設定を示します。

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 4:

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 (136 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 ↵
```

✎ 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 (136 ページ) の TYPE 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 (136 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

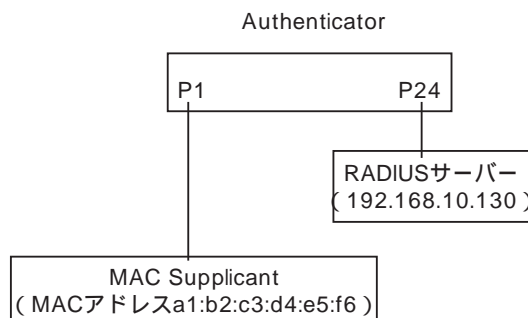
本製品を Authenticator とし、MAC ベース認証を行う場合の基本設定を示します。

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 5:

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 (136 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。

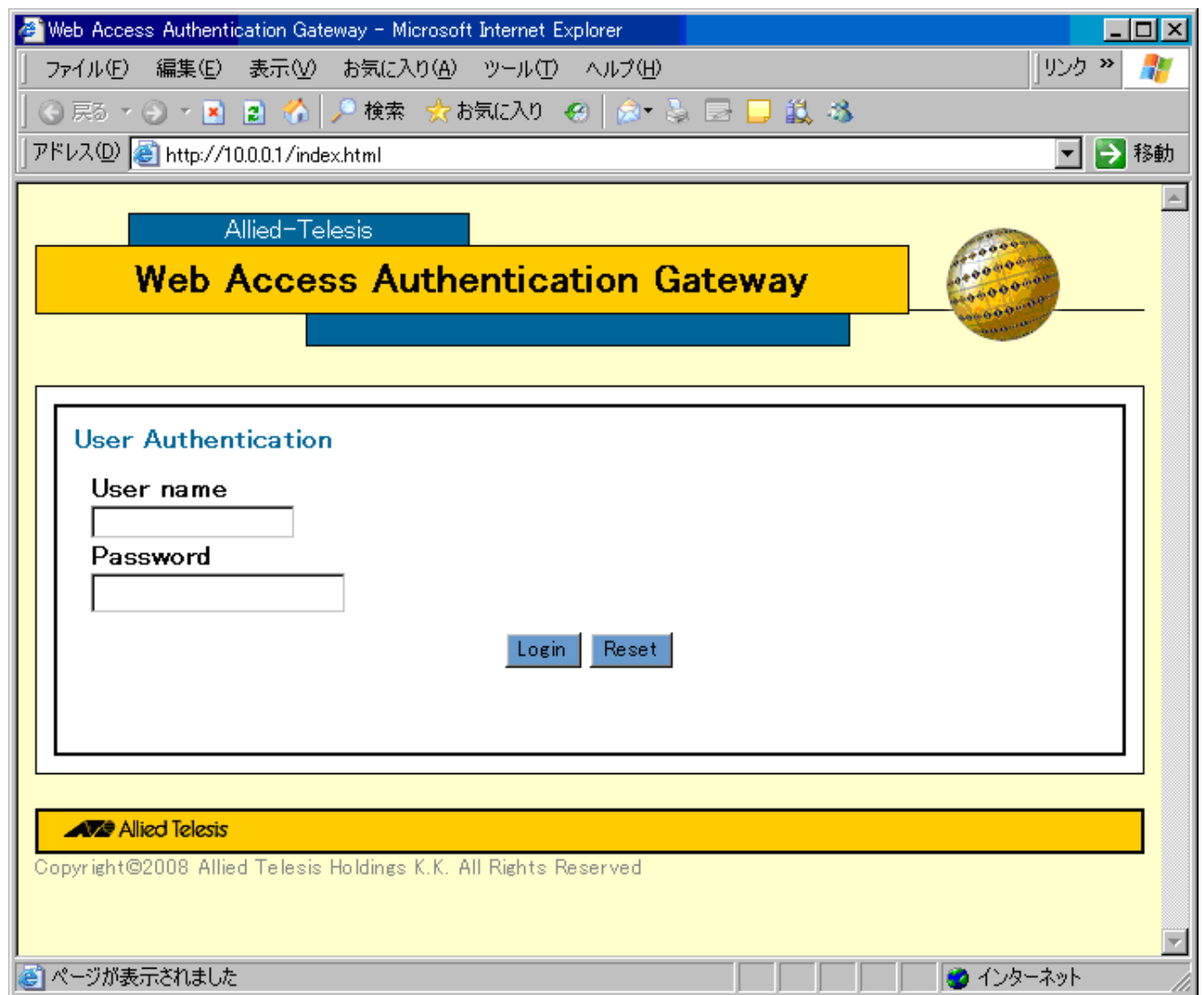
通信を暗号化する場合は、「https://IP アドレス」にアクセスすることにより、HTTPS 接続を使用できます。対応ブラウザ、プロトコルは以下のとおりです。

対応ブラウザ	IE 6.0/7.0、Firefox 3.0 (Windows/Mac)、Firefox 2.0 (Linux/Unix)、Safari 2.0、Opera 9.5 (Windows/Mac)、Opera 9.0 (Linux/Unix)
対応プロトコル	HTTP 1.0/1.1、SSL 2.0/3.0、TLS 1.0

表 6:

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「Web 認証の画面遷移」を参照してください。

- L3 構成にてゲスト VLAN と DHCP サーバーを使用時に、Web 認証でゲスト VLAN 以外にアサインされた後、ログアウトをすると Web 認証画面へアクセスできません。アクセスできるようにするためには Supplicant で IP アドレスを再取得する必要があります。また L2 構成の場合には、Web 認証で認証が成功し、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。
- 本製品と異なるセグメントの Supplicant から Web 認証画面へはアクセスできません。

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（157

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。Ping ポーリング機能で使用するパラメーターは以下の通りです。

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。
REAUTHREFRESH	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 7:

- ✎ 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。

HTTP リダイレクト

ユーザーは Authenticator を意識することなく、任意の Web ページアクセス(たとえば <http://www.allied-teleasis.co.jp/>)により、Web 認証のログイン画面が表示され、認証できます。Web ページへのアクセスは、Supplicant と同じサブネット内ではなく、スイッチを経由したルーティング先にしなければなりません。この場合、Supplicant のデフォルトゲートウェイを Authenticator の IP アドレスにします。

HTTP リダイレクトを有効にします。

```
SET WEBAUTHSERVER HTTPREDIRECT=ENABLED ↵
```

- ✎ URL がホスト名(たとえば <http://www.allied-teleasis.co.jp/>)の場合、認証前に名前解決をする必要があります。
- ✎ HTTP リダイレクト機能が有効 (SET WEBAUTHSERVER HTTPREDIRECT=ENABLED) かつ、Web 認証サーバーの HTTPS が有効 (SET WEBAUTHSERVER SECURITY=ENABLED) な場合、HTTPS による接続を行います。

セッションキープ

ユーザーが HTTP リダイレクト機能を利用して任意の Web ページにアクセスし認証を行い、認証許可となった場合に、接続しようとした Web ページを自動的に表示します。

- ✎ セッションキープは HTTP リダイレクトが有効の場合のみ動作します。

- 802.1X 認証や MAC ベース認証と併用している場合、802.1X 認証や MAC ベース認証の HELD が解除されると、セッションキーも解除されます。

- 認証成功時、HTTP リダイレクトよりもセッションキーの方が優先されます。

HTTP サーバーの基本設定

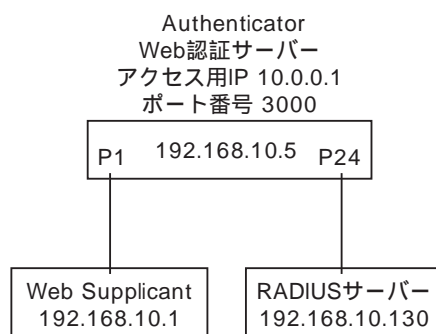
本製品を Authenticator とし、Web 認証を行う場合の基本設定を示します。

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 アドレスとデフォルトゲートウェイの設定が必要です。

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 8:

認証方式は、PAP を指定します。

設定

- 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 ↵
```

- 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 (136 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。

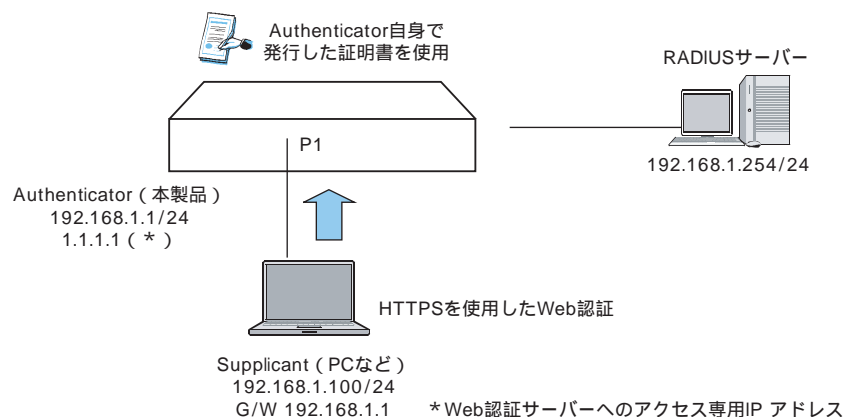
HTTPS サーバーの基本設定

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ことができます。

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 92 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 92 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 255 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 222 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 9:

✎ 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 ↵
```

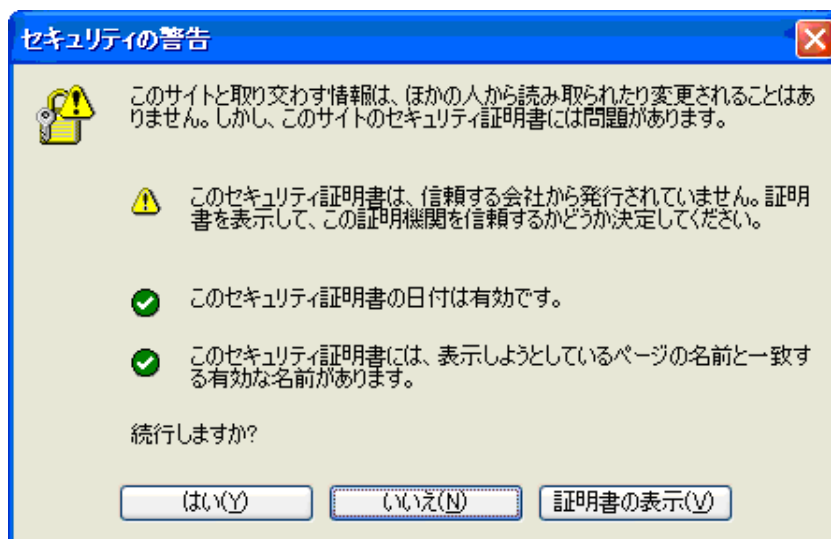
9. Web 認証サーバーを有効にします。

```
ENABLE WEBAUTHSERVER ↵
```

10. ポート認証機能を有効にします。

ENABLE PORTAUTH ↩

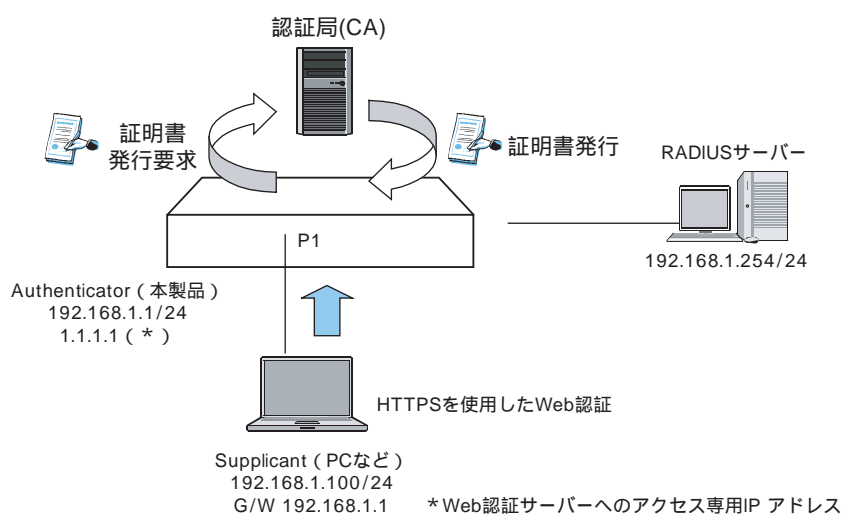
- 上記設定で HTTPS 接続を開始すると、お使いのブラウザによっては、下図のような「警告ウィンドウ」が表示される場合があります。はい (Y) をクリックすることで、認証ページへ移動することができます。



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が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 92 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 92 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いよいでしょう。このコメントは SHOW ENCO KEY コマンド（「運用・管理」の 255 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 222 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 10:

- ✎ 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。

- 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 309 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。
- 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 166 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 ↵
```

- 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 ↵
```

- 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 ↵
```

- 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 ↵
```

- 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 ↵
```

- Web 認証サーバーを有効にします。

```
ENABLE WEBAUTHSERVER ↵
```

- ポート認証機能を有効にします。

```
ENABLE PORTAUTH ↵
```

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 (136 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=ENABLED、VLANASSIGNMENTTYPE=PORT のとき」をご覧ください。
ENABLED	USER(Multi-認証サーバーから指定された VLAN。Supplicant 単位 Supplicant で VLAN が割り当てられる (マルチプルダイナミックモード時のみ)	Supplicant の所属する VLAN と通信については下記の「 VLANASSIGNMENT=ENABLED、VLANASSIGNMENTTYPE=USER のとき」をご覧ください。

表 11:

VLANASSIGNMENT=ENABLED、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 13 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 (97 ページ))。

VLANASSIGNMENT=ENABLED、VLANASSIGNMENTTYPE=USER のとき (マルチプルダイナミック VLAN)

- 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 13 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」も参照してください。

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 (136 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。

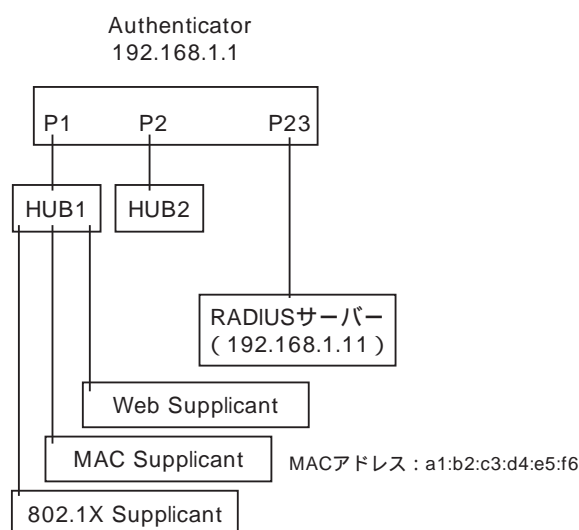
ゲスト VLAN に指定する VLAN は、認証前にルーティングさせないようにするため、L2ONLY VLAN (CREATE VLAN コマンド (「バーチャル LAN」の 16 ページ) の L2ONLY パラメーターで作成) を指定するか、ハードウェアパケットフィルターでルーティングを制限する必要があります。「ゲスト VLAN の設定例」を参照してください。

🔗 認証ポートとタグ付きポートを併用する場合は、ゲスト VLAN は使用できません。

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 (136 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 (136 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 (136 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にゲスト VLAN やダイナミック VLAN が設定されていないこと。

🔗 リンクダウン・リンクアップ時に EAPOL-Start を送出する Supplicant (Windows XP SP3、Windows Vista など) は、再認証を行わずにポート移動させることはできません。

認証アルゴリズムの併用

1 つのポートに複数の認証アルゴリズム (802.1X 認証/MAC ベース認証/Web 認証) を設定できます。認証アルゴリズムを併用した場合は、下記の動作となります。

- 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 ベース認証/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。
- 802.1X/MAC ベース認証を併用した場合、MAC ベース認証が先に実行されるが、EAPOL-Start を受信したときはただちに 802.1X 認証が実行される。

- 802.1X/MAC ベース認証を併用した場合、MAC ベース認証で HELD になると同時に EAP-Request を Supplicant に送信する。
- 802.1X/MAC ベース認証は 1 回目の認証の失敗で HELD 状態となる。Web 認証は 3 回連続で認証に失敗した場合に 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 ベース認証は 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 ベース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。
- 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、1 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。ただし MAC ベース認証で認証許可状態で、EAPOL-Start を受信したときは、MAC ベース認証が解除され、802.1X 認証が実行される。

Supplicant の状態と遷移

- Initialize
初期化状態。処理終了後、Disconnected に移行する。
現状設定変更があるといったリセットしているのでこの状態になることはない。
- Disconnected
未認証（リセット）状態。サブリカントがどの状態であったとしても以下のイベントが発生した場合にこの状態になる。
 - EAPOL-Logoff 受信時
 - WEB 画面でログアウトボタンを押した時
 - Ageout した時
 処理終了後、Connecting に移行する。
- Connecting
認証開始待ち状態。HELD 期間中はその認証アルゴリズムは実行できない。HELD 期間でない場合に以下のイベントが発生することで Authenticating に移行する。
 - MAC ベース認証：フレームを受信
 - 802.1X 認証：EAP-Response を受信
 - Web 認証：「ユーザー名」と「パスワード」を入力してログインボタンを押す
 Connecting の状態でアクセスがない場合 SuppAgeout Timer (300 秒固定) 経過後に、Supplicant 情報は削除される。
- Authenticating
RADIUS SERVER と通信中の状態。通信結果を受けて以下のどれかに移行する。
(Authenticated)
 - RADIUS SERVER から Access-Accept を受信し、正常に VLAN 移動が終了した（認証アルゴ

リズムの内、どれか1つでも成功すればよい)

(Aborting)

- 再認証が発生
- EAPOL-Start 受信
- EAPOL-Logoff 受信
- RADIUS SERVER から応答がなかった

(HELD)

- RADIUS SERVER から Access-Reject を受信
- RADIUS SERVER から Access-Accept を受信したが、VLAN 移動で異常が発生した場合 (不正な Access-Accept/指定された VLAN が存在しない/指定された VLAN の Type が Port Based 以外/ Secure 設定されていて1台目と違う VLAN が指定された/ VLAN の移動に失敗した)

- Authenticated

認証許可状態。再認証期間を過ぎることで 802.1X 認証/MAC ベース認証は Connecting に移行する。Web 認証は Disconnected に移行する。

- Aborting

RADIUS との通信状態を初期化している状態。処理終了後、Disconnected に移行する。

- Held

一定期間認証をブロックする状態。認証アルゴリズムごとに存在するため、HELD 以外の認証アルゴリズムは実行することができる。(他の認証アルゴリズムは Connecting となる) 認証が成功するとすべて HELD がリセットされる。

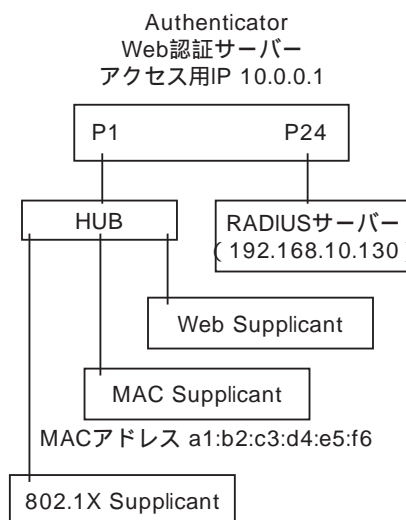
- ForceAuth

強制的にすべてのサブリカントを認証成功にする状態。

- ForceUnauth

強制的にすべてのサブリカントを未認証にする状態。

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 12:

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 (136 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 (136 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 (136 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 ↵

設定例

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。

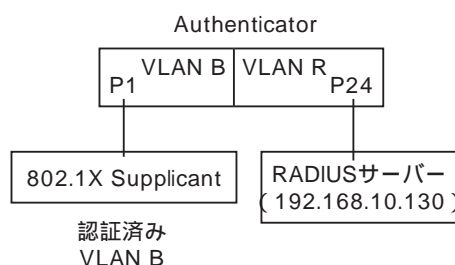
以下、本製品を Authenticator として使用し、さらにダイナミック VLAN 機能を利用する場合の基本設定を示します。Authenticator としての動作には、IP の設定と RADIUS サーバーの指定が必須です。

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。
- 📎 認証ポートとタグ付きポートを併用する場合は、ダイナミック VLAN は使用できません。
- 📎 L3 構成にてダイナミック VLAN と DHCP サーバーを使用時に、Web 認証で元の VLAN 以外にアサインされた後、REAUTHPERIOD の時間が経過すると Web 認証画面へアクセスできなくなります。アクセスできるようにするためには Supplicant で IP アドレスを再取得する必要があります。また、L2 構成の場合には 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。

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 13:

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 (136 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 ↓
```

☞ 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 (136 ページ) の TYPE パラメーターを NONE に設定してください。

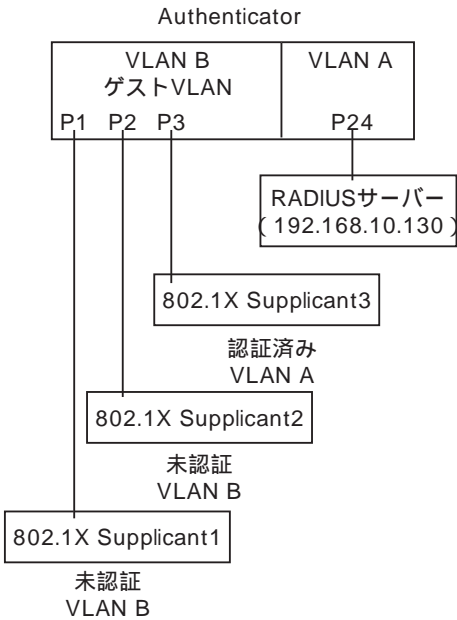
🔑 Web 認証では、Web 認証サーバーの設定も必要です。「テンポラリー IP アドレスを利用する場合の設定例」を参照してください。

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。

🔑 認証ポートとタグ付きポートを併用する場合は、ゲスト VLAN は使用できません。

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)	10	802.1X Supplicant1 用のユーザー名/パスワード
user2	password2	VLAN (13)	IEEE-802 (6)	10	802.1X Supplicant2 用のユーザー名/パスワード
user3	password3	VLAN (13)	IEEE-802 (6)	10	802.1X Supplicant3 用のユーザー名/パスワード

表 14:

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 (136 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。(マルチプルダイナミック VLAN)

```
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。

テンポラリー IP アドレスを利用する場合の設定例

Web Supplicant が DHCP で IP アドレスを取得する場合、未認証の Web Supplicant は IP アドレス取得前であるため、Web 認証サーバーへアクセスできません。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。

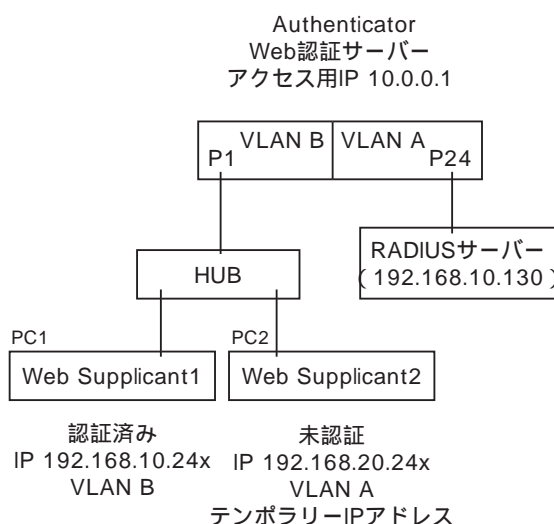
Web Supplicant には、IP アドレスを設定せず、DHCP クライアント機能を有効にします。

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 15:

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 (136 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。また、マルチプルダイナミック VLAN (ユーザー単位のダイナミック VLAN) を設定します。

```
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 ↵
```

📎 ここでは IP アドレスのリース時間を 7200 秒に指定していますが、テンポラリー IP アドレスのリース時間は 20 秒固定なので、リース時間 7200 秒の設定は有効にはなりません。

📎 Ping ボーリング機能と 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。

プロキシサーバーを使用した場合の設定例

本製品は Supplicant にプロキシサーバーが設定されていても、HTTP リダイレクト機能を利用して、Web 認証を実行できます。また、Supplicant の認証成功後、本製品の DHCP サーバーを使用することで、Supplicant のプロキシサーバーを設定することもできます。

📎 プロキシサーバーは Supplicant と同じサブネット内ではなく、スイッチを経由したルーティング先にします。Supplicant のデフォルトゲートウェイは Authenticator の IP アドレスに設定します。

📎 Supplicant のプロキシサーバーに対応するためには HTTP リダイレクトを有効にする必要があります。

Supplicant のプロキシサーバーを構成するには、以下の 3 通りの方法があります。

1. WPAD (Web Proxy Auto Discovery) を使用する。

プロキシサーバーの IP アドレス/ポート番号を意識することなく、認証後、プロキシサーバーを通して外部にアクセスすることが可能になります。

ブラウザはDHCP INFORM パケットにより、PAC(Proxy Auto Configuration) ファイルの位置を取得し、プロキシサーバーの設定を自動的に構成します。

本製品の設定

- SET WEBAUTHSERVER HTTPREDIRECT=ENABLED
- SET WEBAUTHSERVER SESSIONKEEP=ENABLED
- SET WEBAUTHSERVER PROXYSERVER={ プロキシサーバーの IP アドレス }
- SET WEBAUTHSERVER PROXYPORT = { プロキシサーバーのポート番号 }
- DHCP サーバーを有効にします

Supplicant の設定

Microsoft Internet Explorer では、[設定を自動的に検出する] オプションが相当します。

- ☞ Internet Explorer で未認証の Supplicant が PAC ファイルを取得できなかった場合、プロキシ設定はされず、HTTP リダイレクトが機能します。

- ☞ 認証成功後に Web ブラウザーの再起動で PAC ファイルの再取得が行われます。

2. PAC (Proxy Auto Configuration) ファイルを手動で設定する

プロキシサーバーの設定を記述した、PAC ファイルを用意し、ネットワーク上の位置をブラウザに設定します。

本製品の設定

- SET WEBAUTHSERVER HTTPREDIRECT=ENABLED
- SET WEBAUTHSERVER SESSIONKEEP=ENABLED
- SET WEBAUTHSERVER PROXYSERVER={ プロキシサーバーの IP アドレス }
- SET WEBAUTHSERVER PROXYPORT = { プロキシサーバーのポート番号 }
- DHCP サーバーを有効にします

Supplicant の設定

http://{PAC ファイルを配置した、サーバーの URL}/{PAC ファイル名} を設定します。

(例) http://192.168.2.2/proxy.pac

Microsoft Internet Explorer では、[自動構成スクリプトを使用する] に、PAC ファイルの位置を設定します。

- ☞ Internet Explorer で [自動構成スクリプトを使用する] のオプションに スイッチ以外の PAC ファイルを指定した場合、未認証の Supplicant は PAC ファイルを取得できないため、プロキシ設定はされず、HTTP リダイレクトが機能します。

- ☞ 認証成功後に Web ブラウザーの再起動で PAC ファイルの再取得が行われます。

3. プロキシサーバーを直接指定する。

プロキシサーバーの IP アドレス、ポート番号を手動で、設定します。

本製品の設定

- SET WEBAUTHSERVER HTTPREDIRECT=ENABLED
- SET WEBAUTHSERVER SESSIONKEEP=ENABLED
- SET WEBAUTHSERVER PROXYPORT = { プロキシサーバーのポート番号 }

Supplicant の設定

Microsoft Internet Explorer では、[LAN にプロキシサーバーを使用する] に、プロキシサーバーのアドレス、ポート番号を設定します。

- ☞ Internet Explorer ではプロキシサーバーの設定の [例外] に Web 認証サーバーの IP アドレスを設定しなければ、認証成功後、Web 認証サーバーへアクセスできません。

PAC(Proxy Auto Configuration) ファイルについて

PAC ファイルには、本製品の Web 認証サーバーへの IP アドレスが、DIRECT となるように記述してください。

以下の、PAC ファイルの例では、

- 10.0.0.1、192.168.1.1、192.168.3.1、192.168.4.1 へのアクセスは、プロキシサーバーを経由せず直接アクセスします。
- それ以外の宛先へのアクセスは、192.168.1.11 のプロキシサーバー経由でアクセスするように指定しています。

```
function FindProxyForURL(url,host) ↵
{ ↵
if(isPlainHostName(host) ↵
||shExpMatch(host,"10.0.0.1") ↵
||shExpMatch(host,"192.168.1.1") ↵
||shExpMatch(host,"192.168.2.1") ↵
||shExpMatch(host,"192.168.3.1") ↵
||shExpMatch(host,"192.168.4.1") ↵
) ↵
{ ↵
return "DIRECT"; ↵
} ↵
return "PROXY 192.168.1.11:8080;DIRECT"; ↵
} ↵
```

設定例について

- Supplicant は WPAD を使用します。
- 任意の Web ページアクセス (たとえば <http://www.allied-teleasis.co.jp/>) を行い、Web 認証を行います。
- 認証成功後、任意の Web ページへ自動的にアクセスします。
- Supplicant は 認証前はスイッチの DHCP サーバーから、認証成功後は外部の DHCP サーバーから IP アドレスを取得するものとします。

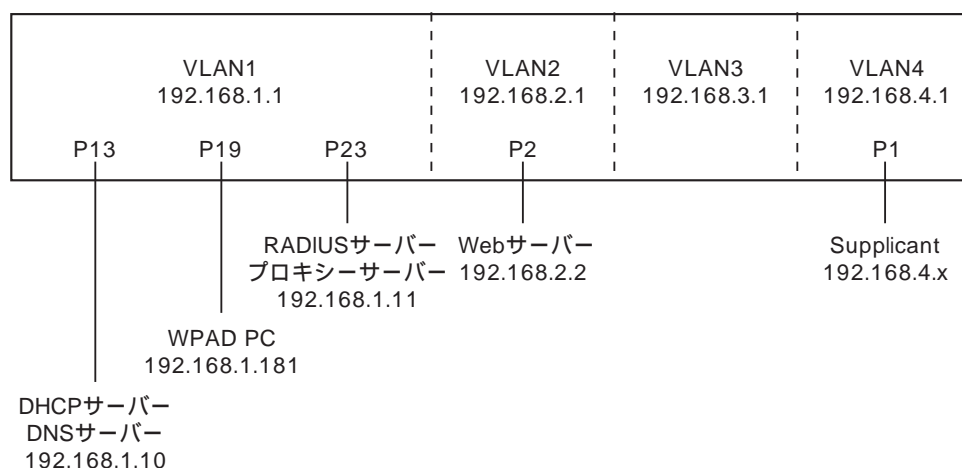
Supplicant の設定

- Supplicant の Web ブラウザーで、WPAD を有効にします。
- 認証後は、<http://10.0.0.1> にアクセスすると、本製品の認証ページにアクセスできます。

外部サーバーの設定

- WPAD PC 上には、PAC ファイルが proxy.pac というファイル名でアクセス可能とします。この proxy.pac ファイルが認証後 Supplicant に使用されます。
- DHCP サーバーは、Option 252 として、WPAD PC 上の proxy.pac ファイルへの URL を答えるように構成されています。
- プロキシサーバーは、ポート番号 8080 で待ち受けているものとします。

構成



設定例

1. 認証サーバーリストに RADIUS サーバーを追加します。

```
ADD RADIUS SERVER=192.168.1.11 ORDER=1 SECRET=test ↵
```

2. VLAN を作成します。

認証前の VLAN v4 と認証成功後のダイナミック VLAN 用の VLAN v3 を作成します。

```
CREATE VLAN=v2 VID=2 UNTAGGEDPORT=2 ↵
```

```
CREATE VLAN=v3 VID=3 UNTAGGEDPORT=3 ↵
```

```
CREATE VLAN=v4 VID=4 UNTAGGEDPORT=1 ↵
```

3. ポート 1 に Web 認証の設定をします。

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

4. ポート認証を有効にします。

```
ENABLE PORTAUTH ↵
```

5. Web 認証サーバーを設定します。

- 「TEMPORARYIP=ENABLED」の指定により、認証前の Supplicant は、スイッチの DHCP サーバーよりテンポラリー IP アドレスを取得できます。
- 「PROXYSERVER="192.168.1.11" PROXYPORT=8080」の指定により、認証前の Supplicant のプロキシサーバーのアクセス先を、「http://192.168.1.11:8080」とする PAC ファイルを作成します。
- 「HTTPREDIRECT=enabled」の指定により、任意の Web サーバーへのアクセスで、Web 認証のログイン画面を表示します。
- 「SESSIONKEEP=enabled」の指定により、認証成功後、自動的に Web サーバーへアクセスします。
- 「RENEWALTIME=8」の指定により、認証成功後、Web サーバーへアクセスする時間を調整します。

```
SET WEBAUTHSERVER IPADDRESS=10.0.0.1 PROXYSERVER="192.168.1.11"
    PROXYPORT=8080 HTTPREDIRECT=enabled SESSIONKEEP=enabled
    TEMPORARYIP=enabled RENEWALTIME=8 ↵
```

6. Web 認証サーバーを有効にします。

```
ENABLE WEBAUTHSERVER ↵
```

7. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INTERFACE=vlan1 IPADDRESS=192.168.1.1 MASK=255.255.255.0 ↵
ADD IP INTERFACE=vlan2 IPADDRESS=192.168.2.1 MASK=255.255.255.0 ↵
ADD IP INTERFACE=vlan3 IPADDRESS=192.168.3.1 MASK=255.255.255.0 ↵
ADD IP INTERFACE=vlan4 IPADDRESS=192.168.4.1 MASK=255.255.255.0 ↵
```

8. DHCP/BOOTP リレー機能を有効にします。

DHCP/BOOTP リレーの設定で認証成功後、Supplicant がダイナミック VLAN で VLAN v3 へ移動したときに 外部の DHCP サーバーより IP アドレスを取得するように設定します。

```
ENABLE BOOTP RELAY INTERFACE=vlan3 ↵
```

9. DHCP/BOOTP リクエストの転送先 IP アドレスを設定します。

```
ADD BOOTP RELAY=192.168.1.10 INTERFACE=vlan3 ↵
```

10. DHCP ポリシーを作成し、IP 設定情報を追加します。

認証前に VLAN v4 で Supplicant が IP アドレスを取得できるようにします。

```
CREATE DHCP POLICY="poli4" LEASE=60 ↵
ADD DHCP POLICY="poli4" SUBNETMASK=255.255.255.0 ↵
ADD DHCP POLICY="poli4" ROUTER=192.168.4.1 ↵
ADD DHCP POLICY="poli4" DNSSERVER=192.168.4.1 ↵
ADD DHCP POLICY="poli4" DOMAINNAME=test.com ↵
```

11. Supplicant に貸し出す IP アドレスの範囲 (DHCP レンジ) を定義します。

```
CREATE DHCP RANGE="ran3" POLICY="poli4" IP=192.168.4.201 NUMBER=10 ↵
```

12. DHCP サーバーを有効にします。

```
ENABLE DHCP ↵
```

13. DNS サーバーリストに DNS サーバーの IP アドレスを追加します。

認証前および認証後、Supplicant での Web ページアクセスを、DNS 解決できるようにします。

```
ADD IP DNS PRIMARY=192.168.1.10 ↵
```

14. DNS リレー機能を有効にします。

```
ENABLE IP DNSRELAY ↵
```

- ✎ 認証成功後、ダイナミック VLAN で VLAN を変更し、Supplicant が外部の DHCP サーバー (DHCP リレーを含む) を使用する場合、RenewalTime を 8 以上に設定します。RenewalTime を 8 以下に設定していると、認証後のページが表示されなかったり、セッションキープが機能しない場合があります。

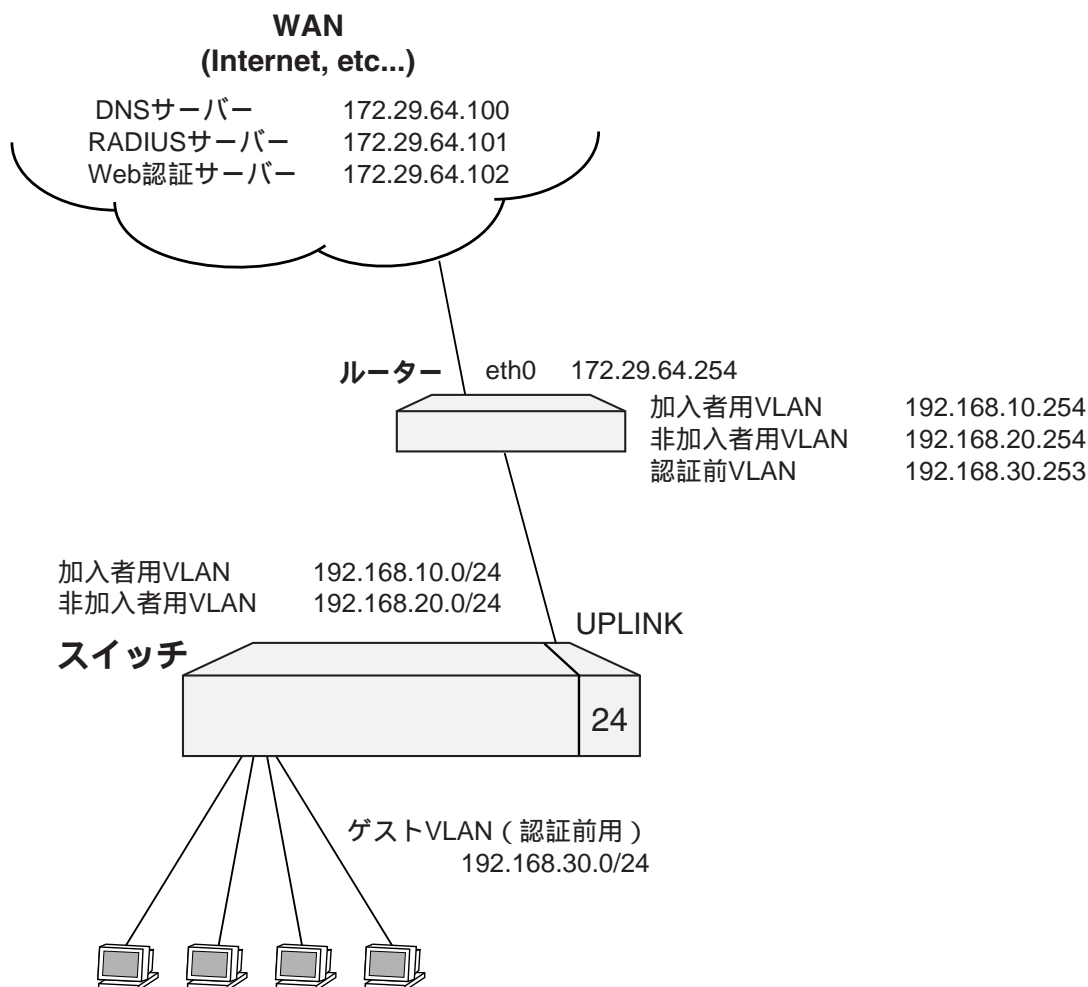
マルチプル VLAN (Protected Ports VLAN) を用いた設定例

ゲスト VLAN にマルチプル VLAN (Protected Ports VLAN) を利用することで、インターネットマンションなどで、各居住者間の通信を遮断しつつ、Web 認証を利用した契約管理システムを構築することができます。

- ルーター配下のスイッチに本製品を使用し、Web 認証 + ゲスト VLAN を使用する。
- 各住居の端末は契約の有無にかかわらず、ゲスト VLAN にて IP を取得できる。
- 各住居からインターネットへのアクセスを試みると、本製品の認証画面にリダイレクトされる。
- ゲスト用のアカウント (事前にお客様へ周知) にてログインすると、インターネット上の Web 認証サーバーのみアクセスが可能となり、申し込みを行うと正規アカウントが取得できる。
- ゲストアカウントからログアウト後、正規アカウントにてログインすると、制限なくインターネットへのアクセスが可能となる。

ルーターは次のように設定されているものと仮定します。

- 加入者 VLAN は制限なくインターネットへアクセスできる。
- 非加入者 VLAN はインターネット上の DNS サーバーおよび契約用 Web 認証サーバーのみにアクセスできる。
- 認証前 VLAN はインターネットへはアクセスできない。
- 非契約者用 VLAN と契約者用 VLAN の DHCP サーバーが有効。



新規加入者がインターネットにアクセスするまでの流れは以下のようになります。

1. 利用者が端末を接続すると、本製品のゲスト VLAN からテンポラリー IP アドレスが付与されます。
2. 利用者が Web ブラウザーを開くと、HTTP リダイレクト機能によって認証ページにリダイレクトされます。
3. 利用者はあらかじめ通知を受けているゲストアカウントでログインします。
4. 本製品は管理センターの RADIUS サーバーに問い合わせを行います。問い合わせたゲストアカウントに対して非加入者用 VLAN ID が返ってきます。
5. 本製品は利用者端末を非加入者用 VLAN に登録します。

6. 認証後、リース期間経過により利用者端末は テンポラリー IP アドレスを解放し、新たにルーターの非加入者用 VLAN から IP アドレスが付与されます。
7. 利用者端末では、リダイレクト URL 機能により管理センターの Web 認証サーバーの登録ページにリダイレクトされます。
8. 利用者は 登録ページから登録し、契約します。
9. 契約後、一度ログアウトし、利用者は再度接続します。
10. 認証ページにて、登録した利用者アカウントでログインします。
11. 本製品は管理センターの RADIUS サーバーに問い合わせを行います。問い合わせた利用者アカウントに対して加入者用 VLAN ID が返ってきます。
12. 本製品は利用者端末を加入者用 VLAN に登録します。
13. 認証後、リース期間経過により利用者端末は テンポラリー IP アドレスを解放し、新たにルーターの加入者用 VLAN から IP アドレスが付与されます。
14. 利用者は自由にインターネットアクセスが可能となります。

✎ 非加入者 VLAN および、加入者 VLAN は通常のポートベース VLAN ですが、ゲスト VLAN のマルチプル VLAN 設定が効いているため、契約の有無に関わらず住居間の通信はできません。

設定例

1. 加入者用 VLAN を作成します。

```
CREATE VLAN=accept VID=10 TAGGEDPORT=24 ↵
```

2. 非加入者用 VLAN を作成します。

```
CREATE VLAN=limited VID=20 TAGGEDPORT=24 ↵
```

3. 認証前 VLAN (ゲスト VLAN) を作成します。マルチプル VLAN (Protected Ports VLAN) をゲスト VLAN として登録するため L2ONLY オプションを指定します。ポート 24 をアップリンク、ポート 1~23 をクライアントに設定します。

```
CREATE VLAN=guest VID=30 PORTPROTECTED L2ONLY ↵
```

```
ADD VLAN=guest TAGGEDPORT=24 GROUP=UPLINK ↵
```

```
ADD VLAN=guest UNTAGGEDPORT=1-23 GROUP=AUTO ↵
```

4. デフォルト VLAN からポート 24 を削除します。

```
DELETE VLAN=Default_VLAN VID=1 UNTAGGEDPORT=24 ↵
```

5. 各 VLAN インターフェースに IP アドレスを付与します。

```
ADD IP INTERFACE=vlan10 IP=192.168.10.253 MASK=255.255.255.0 ↵
ADD IP INTERFACE=vlan20 IP=192.168.20.253 MASK=255.255.255.0 ↵
ADD IP INTERFACE=vlan30 IP=192.168.30.253 MASK=255.255.255.0 ↵
SET IP LOCAL INTERFACE=vlan10 ↵
```

6. デフォルトゲートウェイをルーターの加入者用 VLAN (vlan10) インターフェースに設定します。

```
ADD IP ROUTE=0.0.0.0 INTERFACE=vlan10 NEXTHOP=192.168.10.254 ↵
```

7. RADIUS サーバーを登録します。

```
ADD RADIUS SERVER=172.29.64.101 ORDER=1 SECRET=testing123 ↵
```

8. Web 認証サーバーを設定します。Web 認証サーバーへのアクセス専用の IP アドレスを 1.1.1.1 に設定します。リダイレクト URL 機能を使って、認証後は Web 認証サーバーへリダイレクトさせます。未認証の Supplicant に IP アドレスを付与します。

```
SET WEBAUTHSERVER IPADDRESS=1.1.1.1 REDIRECTURL=http://172.29.64.102/
HTTPREDIRECT=ENABLED TEMPORARYIP=ENABLED ↵
ENABLE WEBAUTHSERVER ↵
```

9. Web 認証設定を行います。ポート 1~23 (クライアントポート) の Web 認証を有効にします。マルチプルダイナミック VLAN (ユーザー単位のダイナミック VLAN) を設定し、ゲスト VLAN は vlan30 (認証前 VLAN/マルチプル VLAN) を設定します。

```
SET PORTAUTH=WEB PORT=1-23 TYPE=AUTHENTICATOR MODE=MULTI
VLANASSIGNMENTTYPE=USER GUESTVLAN=30 ↵
ENABLE PORTAUTH ↵
```

10. ゲスト VLAN 用 DHCP サーバーを設定します。IP アドレスのリース時間は、Web 認証サーバーの設定でテンポラリー IP 機能が有効なため、実際には 20 秒で扱われます。デフォルトゲートウェイは認証前 VLAN (vlan30) のインターフェースを指定、DNS サーバーはルーターのインターフェースを指定し、ルーターで DNS リレーします。

```

CREATE DHCP POLICY="guest" LEASE=3600 ↵
ADD DHCP POLICY="guest" SUBNETMASK=255.255.255.0 ↵
ADD DHCP POLICY="guest" ROUTER=192.168.30.253 ↵
ADD DHCP POLICY="guest" DNSSERVER=192.168.30.254 ↵
CREATE DHCP RANGE="guestip" POLICY="guest" IP=192.168.30.100
    NUMBER=100 ↵
ENABLE DHCP ↵

```

資料編

Web 認証の画面遷移

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。

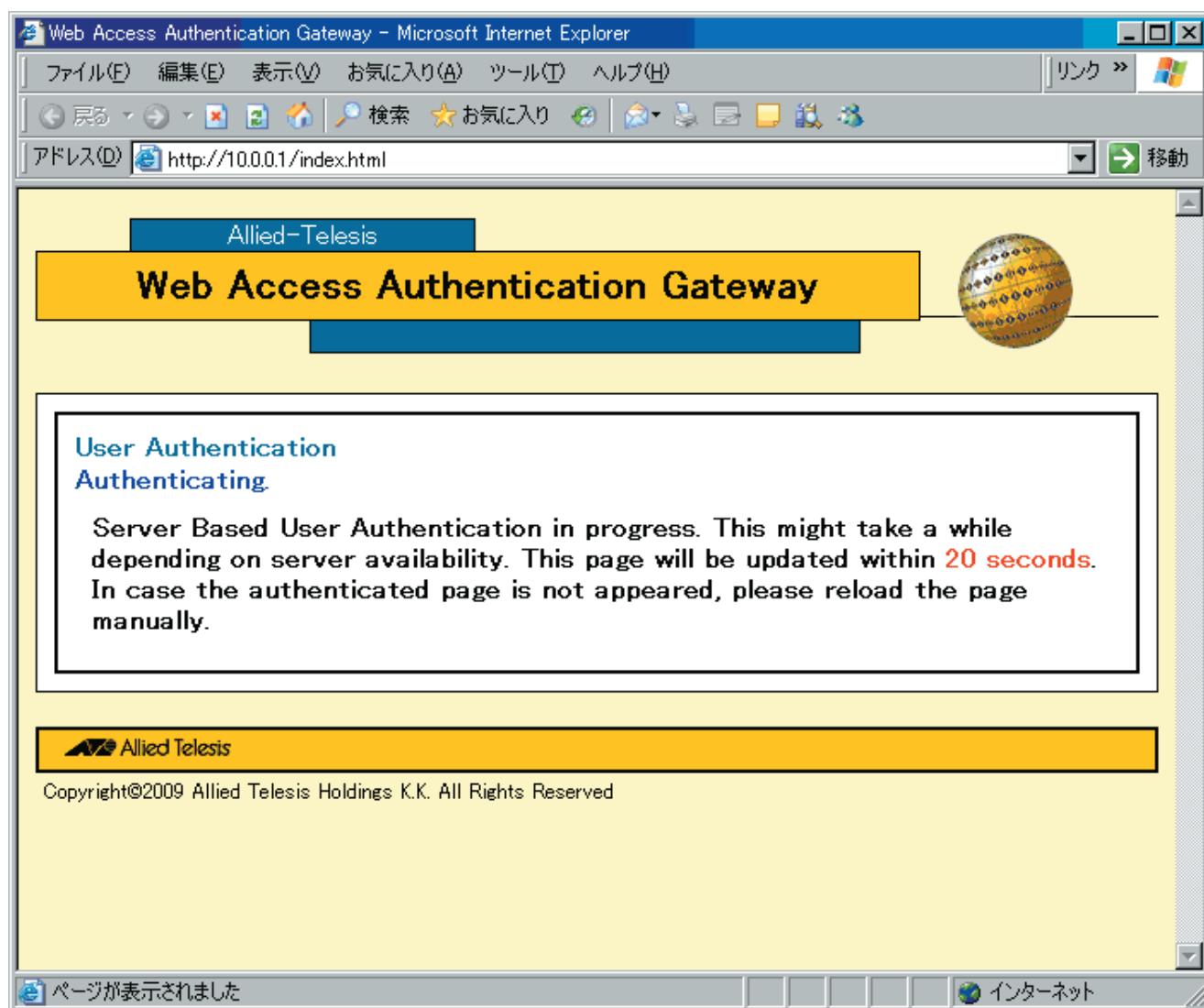
画面に表示される一部の文字列は、SET WEBAUTHSERVER コマンド(157 ページ)の HEADER/SUBHEADERTOP/SUBHEADERTAIL パラメーターで変更可能です。

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(157 ページ)の REDIRECTURL パラメーターを設定します。

認証中

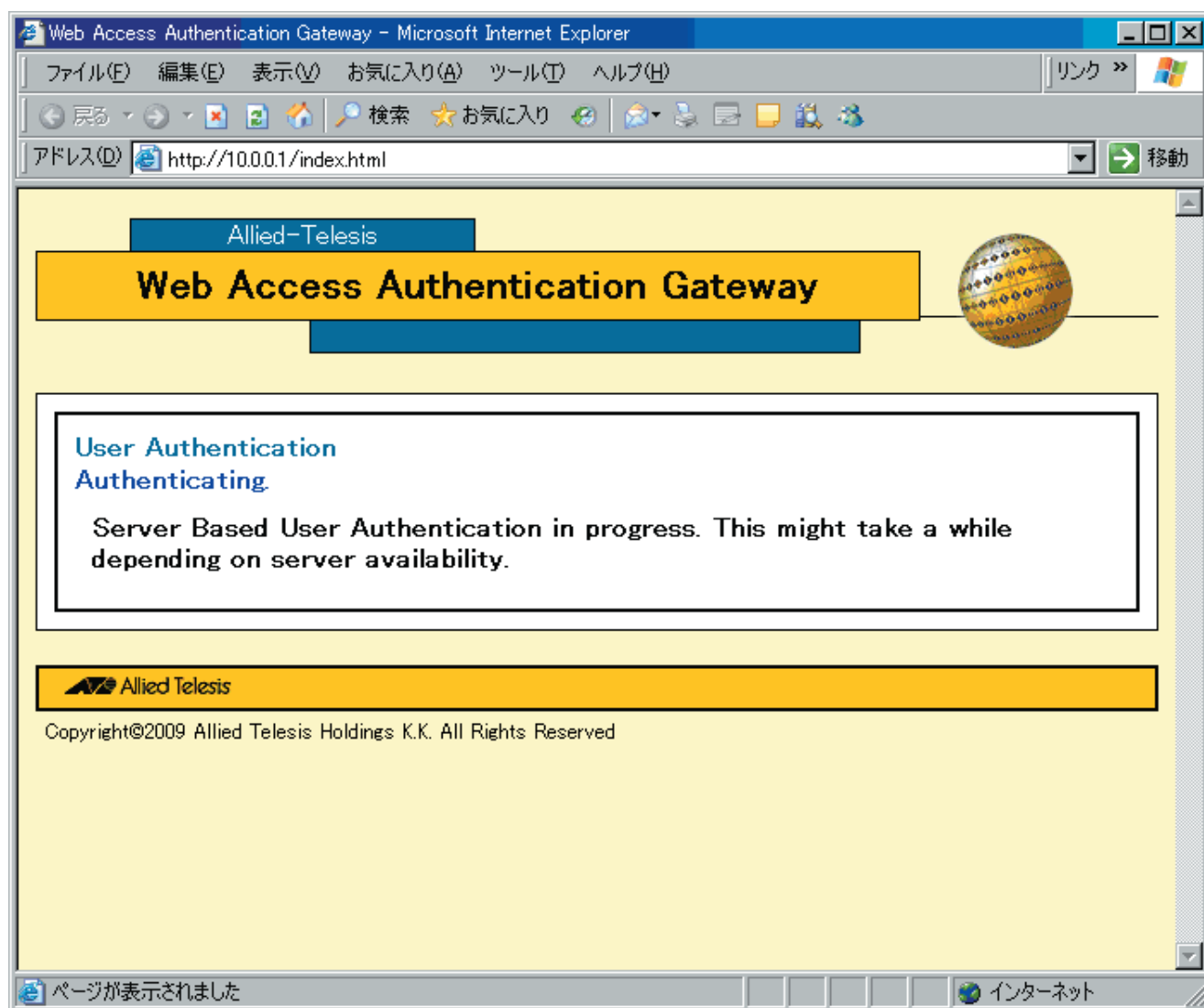
以下の条件の場合、認証中は以下の画面を表示します。

- ダイナミック VLAN が有効 (SET PORTAUTH PORT コマンド(136 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。

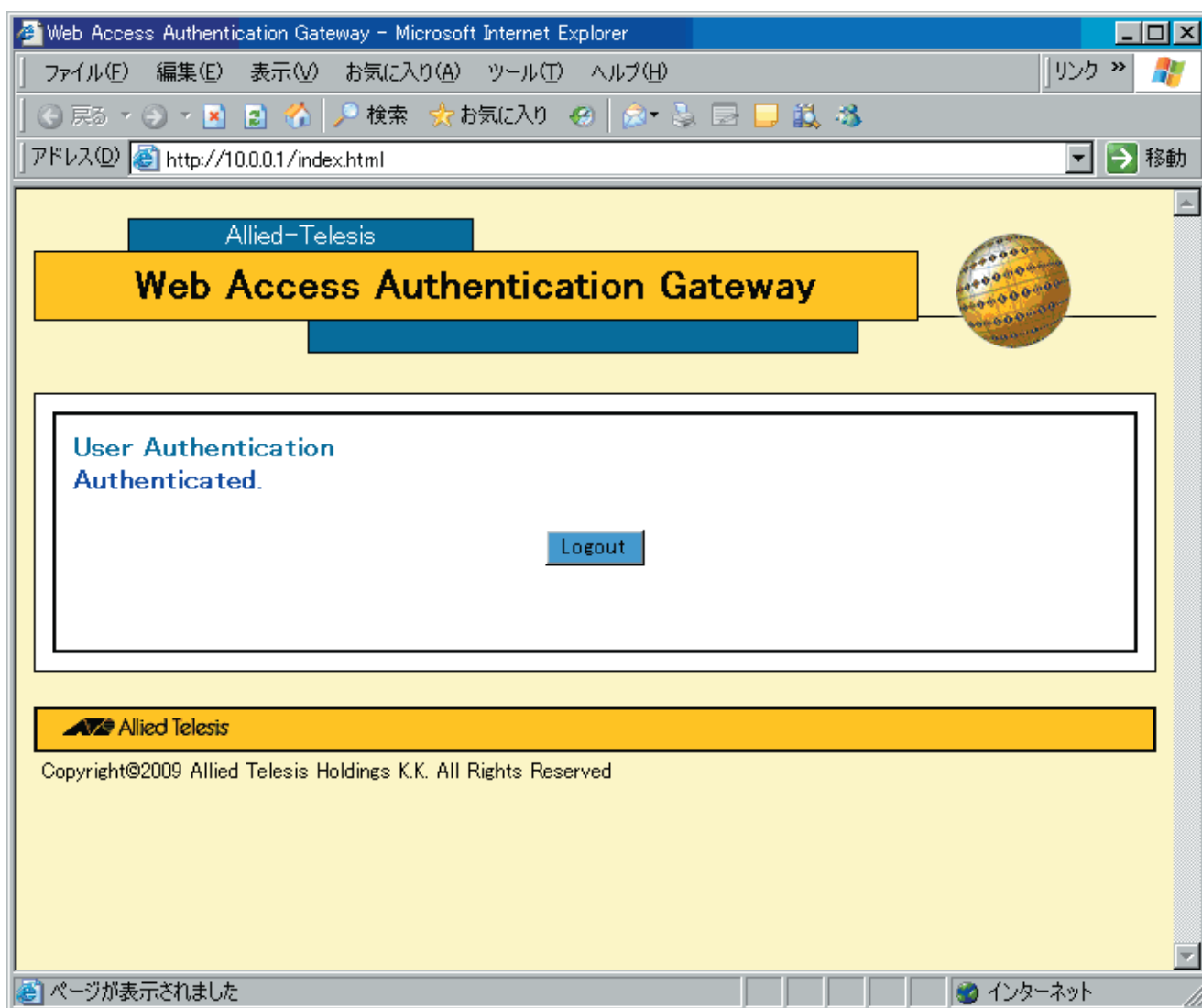
- ダイナミック VLAN が無効 (SET PORTAUTH PORT コマンド (136 ページ) の VLANASSIGNMENT パラメーターが DISABLED) かつ ゲスト VLAN を使用しない (SET PORTAUTH PORT コマンド (136 ページ) の GUESTVLAN パラメーターが NONE) 場合
- ダイナミック VLAN が無効 (SET PORTAUTH PORT コマンド (136 ページ) の VLANASSIGNMENT パラメーターが DISABLED) かつ PVID がゲスト VLAN と同じ設定の場合



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

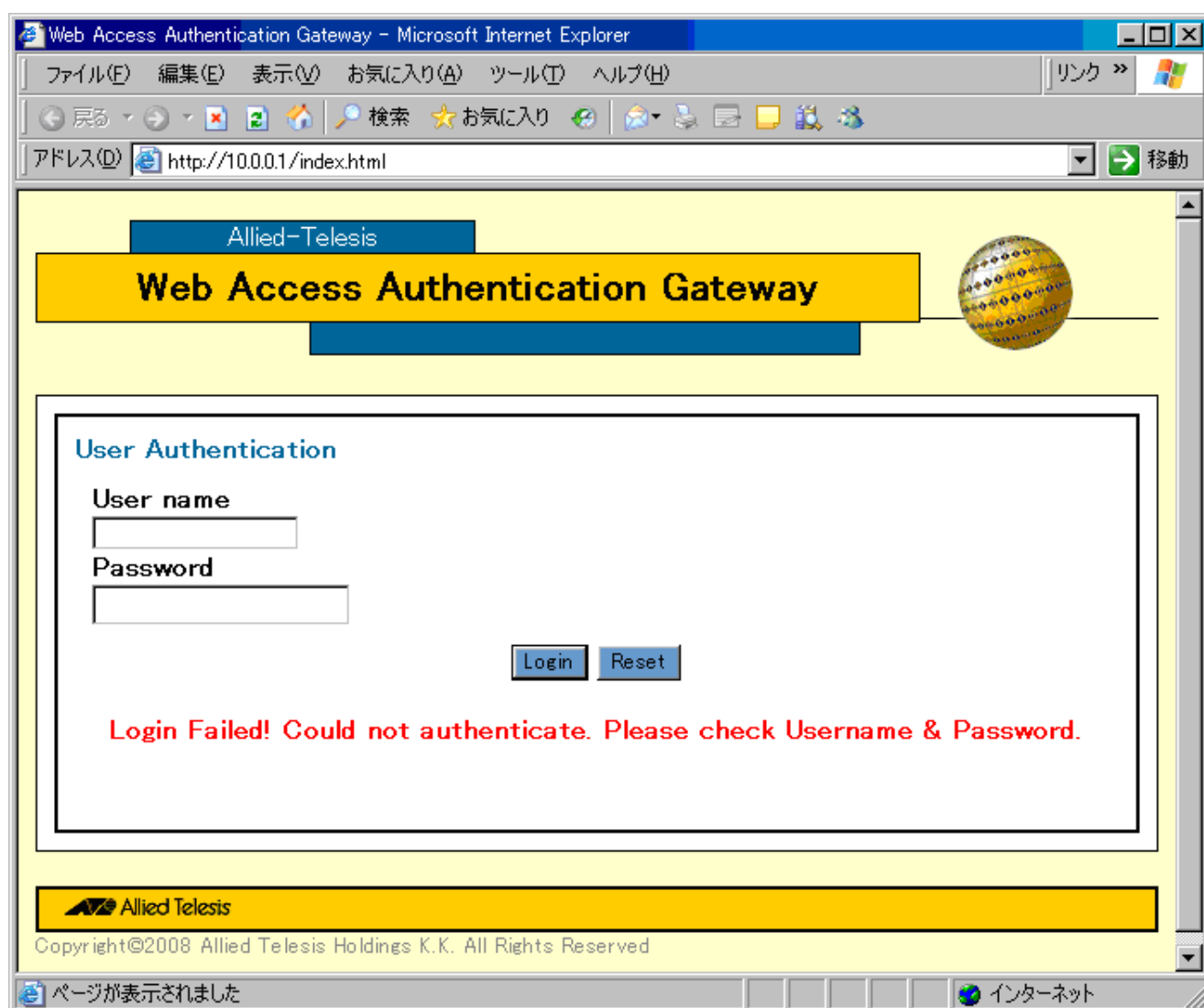
認証に成功するとこの画面を表示します。



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。

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。

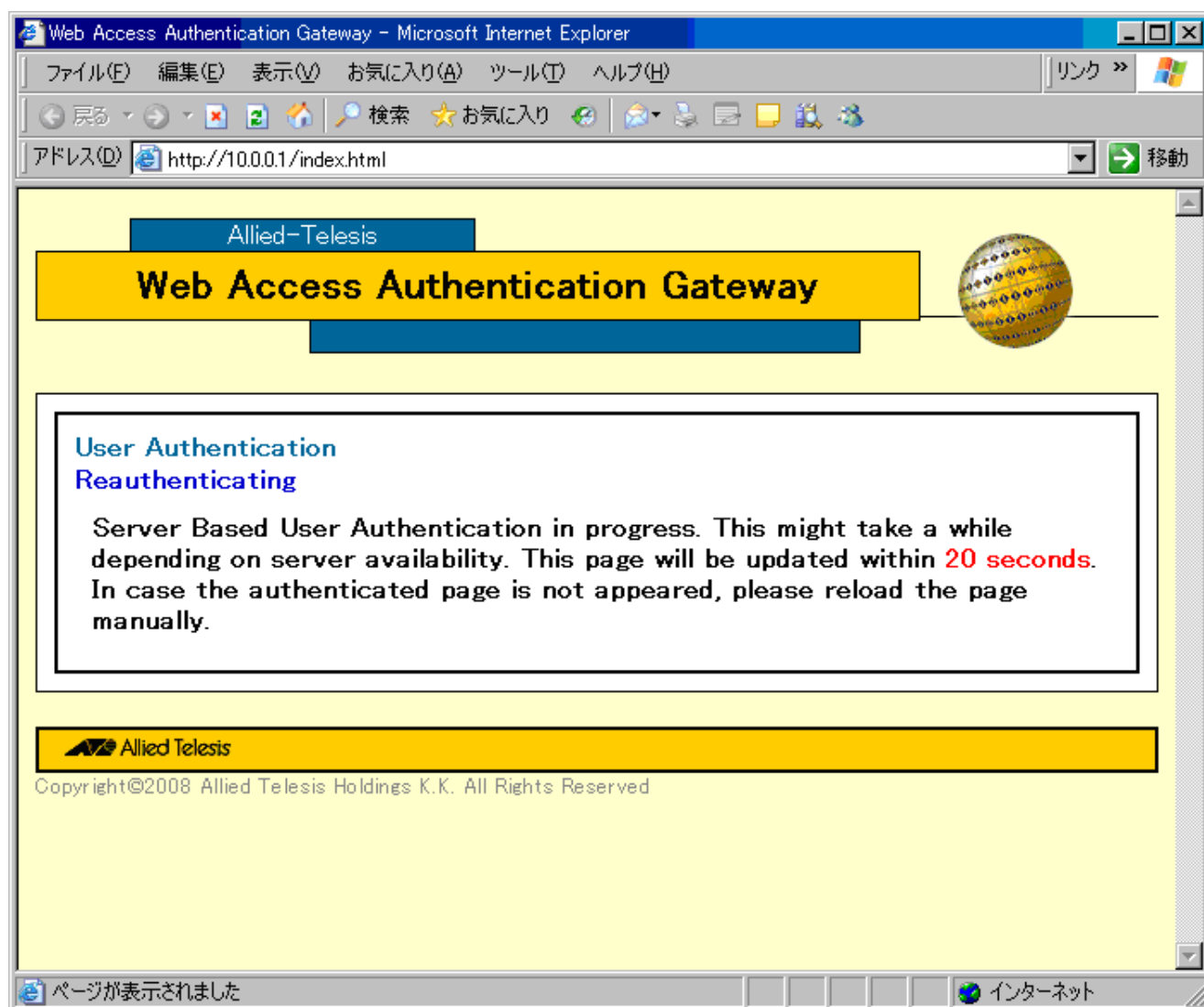
表示されるメッセージ	エラーの原因
Login Failed! Please check the supplied User Name & Password.	空白のみの入力または、MAC アドレス形式。
Login Failed! Maximum sessions active. Please try later.	同時接続数が最大数に達した。
Login Failed! Could not authenticate with server.	内部的な制限 (メモリー上限等) に達し、要求が受け付けられなかった。認証処理がタイムアウトし、RADIUS サーバーとの通信が失敗した。

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 16:

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、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。

認証ログ

認証ログ機能は指定した認証メカニズムの指定したログタイプを残すことができる機能です。

Web 認証の認証成功ログを残すには、ENABLE PORTAUTH PORT LOGTYPE コマンド (111 ページ) を使用します。

```
ENABLE PORTAUTH=WEBBASED PORT=ALL LOGTYPE=SUCCESS ↵
```

認証ログ一覧

Sev	ログレベル。ERR、WRN、INF、DBG のいずれか。
Module	モジュール名。
Message	ログメッセージのフォーマット。
Trigger	ログメッセージが出力される条件。
PORTAUTH	ENABLE/DISABLE PORTAUTH PORT LOGTYPE コマンドの設定条件。
LOGTYPE	ENABLE/DISABLE PORTAUTH PORT LOGTYPE コマンドの設定条件。

表 17:

Sev	Module	Message	Trigger	PORTAUTH	LOGTYPE
INF	WEBAUTH	User(USERNAME) tried to login from IP-ADDRESS on PORT-ID	Web認証ページでログインボタンを押したとき	ALL、WEBBASED	ALL、SUCCESS
INF	WEBAUTH	User(USERNAME) tried to logout from IP-ADDRESS on PORT-ID	Web認証ページでログイン後ログアウトボタンを押したとき	ALL、WEBBASED	ALL、LOGOFF

表 18: Web 認証ログ

Sev	Module	Message	Trigger	PORTAUTH	LOGTYPE
INF	PACCESS	MAC Authentication successful for MAC-ADDRESS on PORT-ID	MAC ベース認証が成功 (PAE state が AUTHENTICATED に 遷移) したとき	ALL、MACBASED	ALL、SUCCESS
INF	PACCESS	802.1X Authentication successful for USER-NAME from MAC-ADDRESS on PORT-ID	802.1X 認証が成功 (PAE state が AUTHENTICATED に 遷移) したとき	ALL、8021X	ALL、SUCCESS

INF	PACCESS	Web Au- thentication successful for USER-NAME from IP- ADDRESS(MAC- ADDRESS) on PORT-ID	Web 認証が成 功 (PAE state が AUTHEN- TICATED に 遷 移) したとき	ALL、WEBBASED	ALL、SUCCESS
-----	---------	--	---	--------------	-------------

表 19: 認証成功ログ

Sev	Module	Message	Trigger	PORTAUTH	LOGTYPE
INF	PACCESS	MAC Au- then- ti- ca- tion failed for MAC- ADDRESS on PORT- ID	MAC ベース認証が失敗 (PAE state が HELD に遷移) したとき	ALL、MACBASED	ALL、FAILURE
INF	PACCESS	802.1X Au- then- ti- ca- tion failed for USER- NAME from MAC- ADDRESS on PORT- ID	802.1X 認証が失敗 (PAE state が HELD に遷移) したとき	ALL、8021X	ALL、FAILURE
INF	PACCESS	Web Au- then- ti- ca- tion failed for USER- NAME from IP- ADDRESS(MAC- ADDRESS) on PORT- ID	Web 認証が失敗 (PAE state が HELD に遷移) したとき	ALL、WEBBASED	ALL、FAILURE

表 20: 認証失敗ログ

Sev	Module	Message	Trigger	PORTAUTH	LOGTYPE
INF	RADIUS	RADIUS server(IP- ADDRESS) timed out. RADIUS session or this server entering DEAD-TIME state for DEAD- TIME-VALUE min.	RADIUS サーバーの応 答待ちタイマーがタイ ムアウトしたとき	ANY	ALL、FAILURE

表 21: RADIUS サーバーログ

Sev	Module	Message	Trigger	PORTAUTH	LOGTYPE
INF	PACCESS	Supplicant USER- NAME logoff from MAC- ADDRESS on PORT-ID	802.1X 認証によ ってログイン していたサブ リカントがロ グオフ (EAPOL- Logoff を受信)し たとき	ALL、8021X	ALL、LOGOFF
INF	PACCESS	Supplicant lo- goff from MAC- ADDRESS on PORT-ID	MAC ベース認証 によってログイン していたサブリカ ントがログオフ (MAC アドレス のエイジアウト) したとき	ALL、MACBASED	ALL、LOGOFF
INF	PACCESS	Supplicant USER-NAME logoff from IP- ADDRESS(MAC- ADDRESS) on PORT-ID	Web 認証によっ てログインして いたサブリカン トがログオフ (認 証ページからの ログアウトボタン 押下、MAC アド レスのエイジアウ ト、Ping ポーリン グによる無応答検 知) したとき	ALL、WEBBASED	ALL、LOGOFF
INF	PACCESS	Supplicant USER-NAME unauthorized from MAC- ADDRESS on PORT-ID	802.1X 認証 サ ブリカントが Authorized から Unauthorized に遷移したとき	ALL、8021X	ALL、LOGOFF
INF	PACCESS	Supplicant unauthorized from MAC- ADDRESS on PORT-ID	MAC ベース認証 サブリカントが Authorized から Unauthorized に遷移したとき	ALL、MACBASED	ALL、LOGOFF

INF	PACCESS	Supplicant USER-NAME unautho- rized from IP- ADDRESS(MAC- ADDRESS) on PORT-ID	Web 認証 サブ リカントが Au- thorized か ら Unauthorized に遷移したとき	ALL、WEBBASED	ALL、LOGOFF
-----	---------	---	---	--------------	------------

表 22: ログオフログ

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 23:

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 24:

認証方式は、PAP を指定します。

- ☞ SET PORTAUTH USERIDFORMAT コマンド (141 ページ) で、User-Name および User-Password で使用する MAC アドレスのフォーマットを任意に変更できます。

- 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 25:

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 26:

- ☞ 「ダイナミック VLAN の設定例」を参照してください。

DHCP Snooping

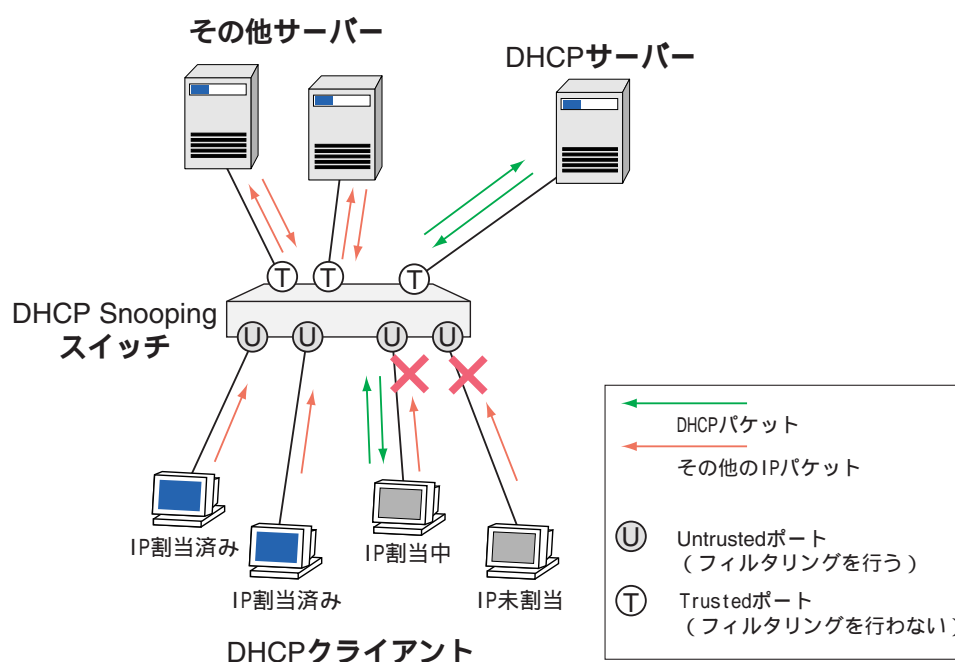
DHCP Snooping は、DHCP サーバー・クライアント間でやりとりされる DHCP メッセージを監視して動的な IP ソースフィルタリングを行う機能です。本機能を利用すれば、DHCP サーバーを用いたネットワーク環境において、正当な DHCP クライアントにだけ IP 通信を許可することができます。

✎ 本機能はレイヤー 2 の機能であるため、IP の設定などをしていなくても使用できます。

概要

DHCP Snooping では、DHCP メッセージのやりとりを監視して DHCP クライアントがどのポート配下に存在するかを追跡し、その情報に基づいて IP パケットのフィルタリングを行います。

DHCP Snooping を利用する場合は、次の図のように本製品を DHCP サーバーと DHCP クライアントの間に配置します。このとき、本製品が DHCP/BOOTP リレーエージェントとして動作していてもかまいません。



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

- Trusted ポート：DHCP Snooping によるフィルタリングが無効なポート。Trusted ポートでは、パケットに対して特別な処理を行わず、すべてのパケットを通過させます。ネットワーク機器やサーバーのように常時接続で信頼のおける装置を接続するポートは通常 Trusted ポートに設定します。DHCP サーバーを接続するポートも Trusted ポートに設定してください。

- Untrusted ポート：DHCP Snooping によるフィルタリングが有効なポート。Untrusted ポートでは、DHCP サーバーから IP アドレスの割り当てを受けたクライアントからの IP パケットだけを通させ、その他の IP パケットは破棄します（DHCP のクライアントパケットを除く）。クライアント PC のように不特定多数の必ずしも信頼のおけない装置を接続するポートは Untrusted ポートに設定します（デフォルトではすべてのポートが Untrusted になります）。

DHCP Snooping を有効にすると、本製品は DHCP サーバー・クライアント間で交換される DHCP メッセージを監視するようになります。

Untrusted ポートに接続されているクライアントが DHCP サーバーから IP アドレスの割り当てを受けると、本製品はクライアントの IP アドレスや MAC アドレス、ポート番号などを DHCP Snooping テーブル（バインディングデータベース）に登録します。

Untrusted ポートでは、バインディングデータベースに登録されているクライアントからの IP パケットだけを許可し、その他の IP パケットは破棄します。これにより、不正に接続されたクライアントがポートを越えてネットワークにアクセスすることを防ぐことができます。

- ☞ デフォルト設定では、Untrusted ポートには DHCP クライアントを 1 台しか接続できません。クライアントを複数接続した場合、最初に IP アドレスを割り当てられたクライアントだけが通信できます。
- ☞ Untrusted ポートに接続された DHCP リレーエージェント経由で IP アドレスの取得を試みたとき、バインディングデータベースには登録されませんが、IP アドレスが取得できます。

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

登録できるクライアントの数

ポート 1～8、9～16、ポート 17～24、トランクグループの 4 つのブロックごとに、それぞれ最大 96 クライアントまで登録できます。（トランクグループに属するポートは、トランクグループのブロックでカウントされ、ポート用ブロックのカウントには含まれません。）

装置全体では、最大 288 クライアントまで登録できます。ただし、ポートトランキングを併用した場合、最大 384 まで設定できます。

基本設定

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

1. DHCP Snooping を有効にします。

```
ENABLE DHCP Snooping ↵
```

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

```
SET DHCP Snooping PORT=1 TRUSTED=YES ↵
```

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

基本設定は以上です。

デフォルトではすべてのポートが Untrusted ポートに設定されているため、手順 2 で Trusted ポートに設定した DHCP サーバーの接続ポートを除き、他のすべてのポートで IP パケット（DHCP のクライアントパケットを除く）が破棄されます。

Untrusted ポートにおいて、DHCP クライアントが DHCP サーバーから IP アドレスを割り当てられたことを検知すると（DHCPACK をクライアントに転送すると）、そのポートでは該当クライアントからの IP パケットを通過させるようになります。

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

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

ポート種別の設定は、SET DHCP Snooping PORT コマンド（131 ページ）の TRUSTED パラメーターで行います。たとえば、DHCP サーバーがポート 1 に接続されている場合は、次のようにして該当ポートを Trusted ポートに設定します。

```
SET DHCP Snooping PORT=1 TRUSTED=YES ↵
```

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

複数のクライアントを接続したい場合は、SET DHCP Snooping PORT コマンド（131 ページ）の MAXLEASES パラメーターで接続台数を指定します。

```
SET DHCP Snooping PORT=1 MAXLEASES=5 ↵
```

IP アドレスを固定設定している装置（DHCP クライアント機能を無効化している装置や DHCP クライアント機能を持たない装置など）を Untrusted ポートで利用したい場合は、バインディングデータベースにクライアント情報をスタティック登録します。

クライアントの登録は ADD DHCP Snooping コマンド（81 ページ）で行います。登録には、IP アドレス、MAC アドレス、所属 VLAN、接続ポートの情報がが必要です。

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

☞ デフォルト設定では、ポートあたり 1 つしかスタティックエントリを登録できません。1 つのポートに複

数のスタティックエントリを登録したいときは、SET DHCP Snooping PORT コマンド (131 ページ) の MAXLEASES パラメーターの値を増やす必要があります。

DHCP Snooping では、IP パケットだけでなく、ARP パケットに対してもフィルタリングを行うことができます。

ENABLE DHCP Snooping ARPSECURITY コマンド (106 ページ) で ARP セキュリティーを有効にすると、Untrusted ポートにおいて、登録済み DHCP クライアントからの ARP パケットだけを他ポートに転送し、その他の ARP パケットは転送せずに破棄するようになります。

```
ENABLE DHCP Snooping ARPSECURITY ↓
```

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

DHCP Snooping では、MAC アドレスフィルタリング機能を使用して、IP アドレスを割り当てるクライアントを MAC アドレスで制限することができます。

Untrusted ポートで受信した DHCP パケット (BOOTREQUEST) に対して、条件にマッチした登録エントリのアクションに従って、許可または破棄を行うことができます。特定の機器に対してのみ DHCP で IP アドレスを配布したい場合などの用途で利用できます。

MAC アドレスフィルタリングエントリを作成するには、CREATE DHCP Snooping MACFILTER コマンド (84 ページ) を使います。

DHCP Snooping では、監視している DHCP メッセージに対して、リレーエージェント情報オプション (オプションコード 82) の付加と削除を行うことも可能です。

ENABLE DHCP Snooping OPTION82 コマンド (108 ページ) でリレーエージェント情報オプションの付加・検査・削除を有効にすると、Untrusted ポートに接続されたクライアントからの DHCP/BOOTP パケットを転送するときに、リレーエージェント情報オプションを挿入するようになります。また、サーバーからの戻りパケットを Untrusted ポートに直接接続されたクライアントに転送するときは同オプションを削除するようになります。

```
ENABLE DHCP Snooping OPTION82 ↓
```

SET DHCP Snooping PORT コマンド (131 ページ) の SUBSCRIBERID パラメーターを利用すれば、リレーエージェント情報オプションに Subscriber-ID サブオプションを含めるかどうか (含めるならばその内容も) をスイッチポートごとに設定することができます。

```
SET DHCP Snooping PORT=5 SUBSCRIBERID="ud-mahahiha" ↓
```

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

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

✎ スタティック登録したクライアントの情報は削除されません。

チェック間隔は、SET DHCP Snooping CHECKINTERVAL コマンド (128 ページ) で変更できます。有効範囲は 1 ~ 3600 秒です。

```
SET DHCP Snooping CHECKINTERVAL=120 ↓
```

また、チェックの際、IP アドレスの使用期限が切れている場合に加えて、クライアントが条件を満たした場合にクライアントの情報をデータベースから削除するよう設定できます。設定には、SET DHCP Snooping CHECKOPTIONS コマンド (129 ページ) を使います。

```
SET DHCP Snooping CHECKOPTIONS=DHCPRELEASE, LINKDOWN ↓
```

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

DHCP Snooping の全般的な情報を確認するには、SHOW DHCP Snooping コマンド (160 ページ) を使います。

```
SHOW DHCP Snooping ↓
```

ポートごとの DHCP Snooping 設定を確認するには、SHOW DHCP Snooping PORT コマンド (169 ページ) を使います。

```
SHOW DHCP Snooping PORT ↓  
SHOW DHCP Snooping PORT=1 ↓
```

バインディングデータベースの内容を確認するには、SHOW DHCP Snooping DATABASE コマンド (164 ページ) を使います。

```
SHOW DHCP Snooping DATABASE ↓
```

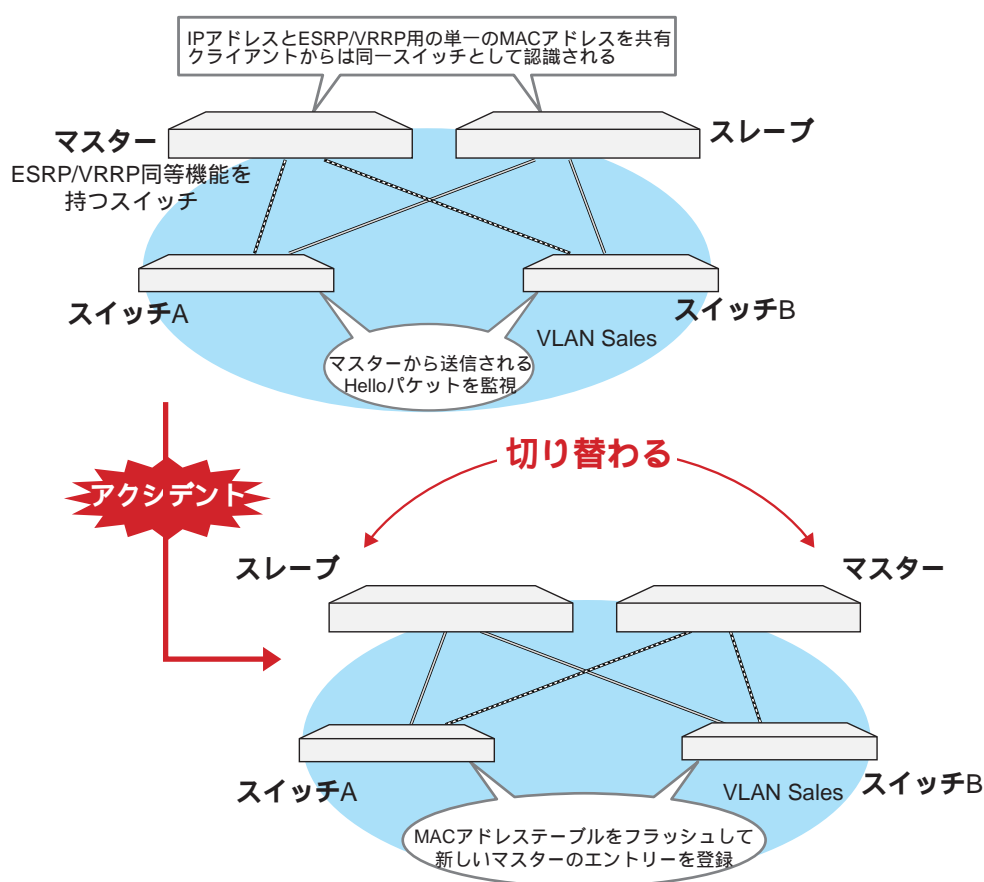
MAC アドレスフィルタリングの設定情報を表示するには、SHOW DHCP Snooping MACFILTER コマンド (167 ページ) を使います。

```
SHOW DHCP Snooping MACFILTER ↓
```

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 (112 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 (99 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 (185 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

RESET SWITCH	124
SET SWITCH INFILTERING	143
SET SWITCH MULTICASTMODE	145
SHOW SWITCH	186
SHOW SWITCH COUNTER	188

ポート

ACTIVATE SWITCH PORT AUTONEGOTIATE	80
ADD SWITCH TRUNK	83
CREATE SWITCH TRUNK	86
DELETE SWITCH TRUNK	89
DESTROY SWITCH TRUNK	91
DISABLE SWITCH PORT	100
DISABLE SWITCH PORT FLOW	101
DISABLE SWITCH PORT LOOPDETECTION	102
DISABLE SWITCH PORT STORMDETECTION	103
ENABLE SWITCH PORT	113
ENABLE SWITCH PORT FLOW	114
ENABLE SWITCH PORT LOOPDETECTION	115
ENABLE SWITCH PORT STORMDETECTION	116
PURGE SWITCH PORT	119
RESET SWITCH PORT	125
RESET SWITCH PORT LOOPDETECTION COUNTER	126
RESET SWITCH PORT STORMDETECTION COUNTER	127
SET SWITCH MIRROR	144
SET SWITCH PORT	146
SET SWITCH PORT LOOPDETECTION	149
SET SWITCH PORT MIRROR	151
SET SWITCH PORT SECURITYMODE	152
SET SWITCH PORT STORMDETECTION	154
SET SWITCH TRUNK	156
SHOW SWITCH MIRROR	190
SHOW SWITCH PORT	191
SHOW SWITCH PORT COUNTER	195
SHOW SWITCH PORT INTRUSION	198
SHOW SWITCH PORT LOOPDETECTION	200

SHOW SWITCH PORT SECURITYMODE	204
SHOW SWITCH PORT STORMDETECTION	206
SHOW SWITCH PORT SUMMARY	209
SHOW SWITCH TRUNK	211

EPSR Snooping

DISABLE EPSRSNOOPING	96
ENABLE EPSRSNOOPING	109
SHOW EPSRSNOOPING	171

ポート認証

DISABLE PORTAUTH	97
DISABLE PORTAUTH PORT LOGTYPE	98
DISABLE WEBAUTHSERVER	104
ENABLE PORTAUTH	110
ENABLE PORTAUTH PORT LOGTYPE	111
ENABLE WEBAUTHSERVER	117
PURGE WEBAUTHSERVER	120
RESET PORTAUTH PORT	123
SET PORTAUTH AUTHMETHOD	133
SET PORTAUTH CSIDFORMAT	134
SET PORTAUTH PORT	136
SET PORTAUTH USERIDFORMAT	141
SET WEBAUTHSERVER	157
SHOW PORTAUTH	172
SHOW PORTAUTH PORT	178
SHOW WEBAUTHSERVER	213

DHCP Snooping

ADD DHCP Snooping	81
CREATE DHCP Snooping MACFILTER	84
DELETE DHCP Snooping	88
DESTROY DHCP Snooping MACFILTER	90
DISABLE DHCP Snooping	92
DISABLE DHCP Snooping ARPSECURITY	93
DISABLE DHCP Snooping LOG	94
DISABLE DHCP Snooping OPTION82	95
ENABLE DHCP Snooping	105
ENABLE DHCP Snooping ARPSECURITY	106
ENABLE DHCP Snooping LOG	107
ENABLE DHCP Snooping OPTION82	108
PURGE DHCP Snooping	118
RESET DHCP Snooping COUNTER	121
RESET DHCP Snooping DATABASE	122

SET DHCP Snooping CHECKINTERVAL	128
SET DHCP Snooping CHECKOPTIONS	129
SET DHCP Snooping MACFILTER	130
SET DHCP Snooping PORT	131
SHOW DHCP Snooping	160
SHOW DHCP Snooping COUNTER	162
SHOW DHCP Snooping DATABASE	164
SHOW DHCP Snooping MACFILTER	167
SHOW DHCP Snooping PORT	169

RRP Snooping

DISABLE RRP Snooping	99
ENABLE RRP Snooping	112
SHOW RRP Snooping	185

ACTIVATE SWITCH PORT AUTONEGOTIATE

カテゴリー：スイッチング / ポート

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

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

解説

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

パラメーター

PORT 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。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 (146 ページ)

SHOW SWITCH PORT (191 ページ)

ADD DHCP Snooping

カテゴリー：スイッチング / DHCP Snooping

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

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

vlan-if: VLAN インターフェース (VLAN-name か VLANvid の形式。name は VLAN 名、vid は VLAN ID)

ipadd: IP アドレス

port-number: スイッチポート番号 (1 ~)

解説

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

パラメーター

BINDING クライアントの MAC アドレス

INTERFACE クライアントの所属 VLAN

IP クライアントの IP アドレス

PORT クライアントが接続されているスイッチポート

例

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

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

備考・注意事項

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

Trusted ポートにスタティックエントリを登録することはできない。

スタティックエントリと同じ IP アドレスを DHCP Server から付与することはできない。DHCP レンジ内の IP アドレスをスタティック登録してはならない。

関連コマンド

DELETE DHCP Snooping (88 ページ)

SET DHCP Snooping Port (131 ページ)

SHOW DHCP Snooping Database (164 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 (86 ページ)

DELETE SWITCH TRUNK (89 ページ)

DESTROY SWITCH TRUNK (91 ページ)

SET SWITCH TRUNK (156 ページ)

SHOW SWITCH TRUNK (211 ページ)

CREATE DHCP Snooping MACFILTER

カテゴリー：スイッチング / DHCP Snooping

```
CREATE DHCP SNOOPING MACFILTER=1..999 [ADDRESS={macadd|ANY}]
      [MASK=macadd] [VLAN={vlanname|1..4094|ANY}] [PORT={port-list|ALL|NONE}]
      [ACTION={DENY|PERMIT}]
```

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

vlanname: VLAN 名 (1~20 文字。英数字とアンダースコア (_)、ハイフンを使用可能。大文字・小文字を区別しない)

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

解説

MAC アドレスフィルタリングエントリーを作成する。

パラメーター

MACFILTER 作成するエントリーの ID。連番でなくてもかまわない。

ADDRESS フィルタリング対象装置の MAC アドレス。省略時は ANY。

MASK フィルタリング対象装置の MAC アドレスへのマスクを指定する。省略時は FF:FF:FF:FF:FF:FF。

VLAN 入力 VLAN 名または VID。省略時は ANY。

PORT MAC アドレスフィルタリングを割り当てるポートを指定する。デフォルトは NONE。

ACTION 条件に一致したときのアクション。PERMIT (許可)、DENY (破棄) から選択する。デフォルトは DENY。

例

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

```
CREATE DHCP SNOOPING MACFILTER=1 ADDRESS=00:09:41:00:00:00
      MASK=FF:FF:FF:00:00:00 PORT=ALL ACTION=PERMIT
CREATE DHCP SNOOPING MACFILTER=2 ADDRESS=00:1A:EB:00:00:00
      MASK=FF:FF:FF:00:00:00 PORT=ALL ACTION=PERMIT
CREATE DHCP SNOOPING MACFILTER=3 PORT=ALL ACTION=DENY
```

備考・注意事項

エントリーは 128 個まで作成できる。

エントリー ID の番号順に検索し、マッチしたエントリーのアクションを実行する。それ以降のエントリーはチェックされない。

Trusted ポートでは MAC アドレスフィルタリング機能は働かない。

ポート設定が NONE のエントリは機能しない。無効なエントリとして扱われる。

MAC アドレスが ANY のエントリはすべての装置が対象となる。

どのエントリにもマッチしない場合は、許可 (Permit) として扱われる。

エントリ作成時に、既に該当エントリがバインディングデータベースに登録されていた場合、そのエントリに対してはなにも処理されない。

作成されたエントリは、次回の更新などでクライアントから DHCP パケットを受信した際に機能する。

したがって、CHECKOPTION で DHCPRELEASE を有効にしていた場合に、作成したエントリのアクションが破棄 (Deny) のときは機能しなくなるので注意が必要。

エントリ作成時には、適宜バインディングデータベースのエントリを削除すること。

関連コマンド

DESTROY DHCP Snooping MAC Filter (90 ページ)

SET DHCP Snooping MAC Filter (130 ページ)

SHOW DHCP Snooping MAC Filter (167 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

フラッドパケットは、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。

スタティック ARP エントリーを登録した後、登録したポートを含んだトランクグループを作成した場合、スタティック ARP エントリーを削除し、登録し直す必要がある。

トランクポートにスタティック ARP エントリーを登録した後、トランクグループを削除した場合、表示はトランクグループのままとなる。

トランクグループにスタティック ARP エントリーを登録し、設定を保存すると、トランクグループの一番小さいポート番号のポートに登録され保存される。

SELECT パラメーターに MAC アドレスの選択基準 (MACSRC、MACDEST、MACBOTH) が指定されていると、ルーティング後のパケットが負荷分散されずに送出される。

関連コマンド

ADD SWITCH TRUNK (83 ページ)

DELETE SWITCH TRUNK (89 ページ)

DESTROY SWITCH TRUNK (91 ページ)

SET SWITCH TRUNK (156 ページ)

SHOW SWITCH TRUNK (211 ページ)

DELETE DHCP Snooping

カテゴリー：スイッチング / DHCP Snooping

DELETE DHCP Snooping BINDING [= *macadd*] [IP= *ipadd*]

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

ipadd: IP アドレス

解説

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

パラメーター

BINDING クライアントの MAC アドレス

IP クライアントの IP アドレス

関連コマンド

ADD DHCP Snooping (81 ページ)

SHOW DHCP Snooping DATABASE (164 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 (83 ページ)

CREATE SWITCH TRUNK (86 ページ)

DESTROY SWITCH TRUNK (91 ページ)

SET SWITCH TRUNK (156 ページ)

SHOW SWITCH TRUNK (211 ページ)

DESTROY DHCP Snooping MACFILTER

カテゴリー：スイッチング / DHCP Snooping

DESTROY DHCP Snooping MACFILTER={*id-list*|ALL}

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

解説

MAC アドレスフィルタリングエントリーを削除する。

パラメーター

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

関連コマンド

CREATE DHCP Snooping MACFILTER (84 ページ)

SET DHCP Snooping MACFILTER (130 ページ)

SHOW DHCP Snooping MACFILTER (167 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 (83 ページ)
CREATE SWITCH TRUNK (86 ページ)
DELETE SWITCH TRUNK (89 ページ)
SET SWITCH TRUNK (156 ページ)
SHOW SWITCH TRUNK (211 ページ)

DISABLE DHCP Snooping

カテゴリー：スイッチング / DHCP Snooping

DISABLE DHCP Snooping

解説

DHCP Snooping を無効にする。デフォルトは無効。

関連コマンド

ENABLE DHCP Snooping (105 ページ)

SHOW DHCP Snooping (160 ページ)

DISABLE DHCP Snooping ARPSECURITY

カテゴリー：スイッチング / DHCP Snooping

DISABLE DHCP Snooping ARPSECURITY

解説

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

関連コマンド

ENABLE DHCP Snooping (105 ページ)

ENABLE DHCP Snooping ARPSECURITY (106 ページ)

SHOW DHCP Snooping (160 ページ)

DISABLE DHCP Snooping LOG

カテゴリー：スイッチング / DHCP Snooping

DISABLE DHCP Snooping LOG={ARPSECURITY|MACFILTER}

解説

DHCP Snooping のログ機能を無効にする。デフォルトは無効。

パラメーター

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

関連コマンド

CREATE DHCP Snooping MACFILTER (84 ページ)

ENABLE DHCP Snooping (105 ページ)

ENABLE DHCP Snooping ARPSECURITY (106 ページ)

ENABLE DHCP Snooping LOG (107 ページ)

SHOW DHCP Snooping (160 ページ)

SHOW LOG (「運用・管理」の 264 ページ)

DISABLE DHCP Snooping OPTION82

カテゴリー：スイッチング / DHCP Snooping

DISABLE DHCP Snooping OPTION82

解説

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

関連コマンド

ENABLE DHCP Snooping（105 ページ）

ENABLE DHCP Snooping OPTION82（108 ページ）

SHOW DHCP Snooping（160 ページ）

DISABLE EPSRSNOOPING

カテゴリー：スイッチング / EPSR Snooping

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

vlanname: VLAN 名 (1~20 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。

パラメーター

CONTROLVLAN コントロール VLAN。VLAN 名または VLAN ID (VID) で指定する。省略時および ALL を指定した場合は、すべてのコントロール VLAN が無効になる。

関連コマンド

ENABLE EPSRSNOOPING (109 ページ)

SHOW EPSRSNOOPING (171 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。

関連コマンド

ENABLE PORTAUTH (110 ページ)

SHOW PORTAUTH (172 ページ)

SHOW PORTAUTH PORT (178 ページ)

DISABLE PORTAUTH PORT LOGTYPE

カテゴリー：スイッチング / ポート認証

```
DISABLE PORTAUTH [= {ALL|8021X|MACBASED|WEBBASED}] PORT={port-list|ALL}
LOGTYPE={SUCCESS|FAILURE|LOGOFF|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

認証ログ機能を無効にする。指定した認証メカニズムで指定したログタイプを残さない。
デフォルトは有効。全認証メカニズムの全ログタイプを残す。

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)、ALL のいずれかを指定する。デフォルトは ALL。

PORT スイッチポート番号。複数指定が可能。

LOGTYPE ログタイプ。SUCCESS (成功のみ)、FAILURE (失敗のみ)、LOGOFF (ログオフ)、ALL (すべて) のいずれかを指定する。カンマ区切りによる複数指定が可能。デフォルトは ALL。SUCCESS 指定時は、「Web 認証ログ」・「認証成功ログ」が対象となる。FAILURE 指定時は、「認証失敗ログ」・「RADIUS サーバーログ」が対象となる。LOGOFF 指定時は、「Web 認証ログ」・「ログオフログ」が対象となる。

関連コマンド

ENABLE PORTAUTH PORT LOGTYPE (111 ページ)

SHOW PORTAUTH (172 ページ)

SHOW PORTAUTH PORT (178 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 (112 ページ)

SHOW RRPSNOOPING (185 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。デフォルトはイネーブル。

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。

備考・注意事項

トランクグループに所属するポートのうち1つをディセーブルに設定すると、トランクグループすべてのポートがディセーブルになる。

関連コマンド

ENABLE SWITCH PORT（113 ページ）

SHOW SWITCH PORT（191 ページ）

DISABLE SWITCH PORT FLOW

カテゴリー：スイッチング / ポート

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

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

解説

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

パラメーター

PORT ポート番号。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。

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 (114 ページ)

SHOW SWITCH PORT (191 ページ)

DISABLE SWITCH PORT LOOPDETECTION

カテゴリー：スイッチング / ポート

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

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

解説

指定したポートの LDF 検出を無効にする。デフォルトは無効

パラメーター

PORT ポート番号。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

例

ポート 2 の LDF 機能を無効にする

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

備考・注意事項

LDF 検出有効時は、各ポートの LDF 検出の有効/無効にかかわらず、すべてのポートで受信した LDF が LDF 検出の対象になる。

関連コマンド

ENABLE SWITCH PORT LOOPDETECTION (115 ページ)

RESET SWITCH PORT LOOPDETECTION COUNTER (126 ページ)

SET SWITCH PORT LOOPDETECTION (149 ページ)

SHOW SWITCH PORT LOOPDETECTION (200 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。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。

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 (116 ページ)

RESET SWITCH PORT STORMDETECTION COUNTER (127 ページ)

SET SWITCH PORT STORMDETECTION (154 ページ)

SHOW SWITCH PORT STORMDETECTION (206 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 (117 ページ)

PURGE WEBAUTHSERVER (120 ページ)

SET WEBAUTHSERVER (157 ページ)

SHOW PORTAUTH (172 ページ)

SHOW PORTAUTH PORT (178 ページ)

SHOW WEBAUTHSERVER (213 ページ)

ENABLE DHCP Snooping

カテゴリー：スイッチング / DHCP Snooping

ENABLE DHCP Snooping

解説

DHCP Snooping を有効にする。デフォルトは無効。

備考・注意事項

攻撃検出機能と DHCP Snooping は同時に有効にできない。

関連コマンド

DISABLE DHCP Snooping (92 ページ)

SHOW DHCP Snooping (160 ページ)

ENABLE DHCP Snooping ARPSECURITY

カテゴリー：スイッチング / DHCP Snooping

ENABLE DHCP Snooping ARPSECURITY

解説

DHCP Snooping のオプション機能である ARP セキュリティーを有効にする。デフォルトは無効。本機能は、DHCP Snooping が有効になっていないと動作しない。

本機能を有効にした場合、Untrusted ポートにおいて、登録済み DHCP クライアントからの ARP パケットだけを他ポートに転送し、その他の ARP パケットは転送せずに破棄するようになる。

備考・注意事項

ARP セキュリティーは、本体宛にも機能する。

関連コマンド

ADD DHCP Snooping (81 ページ)

DISABLE DHCP Snooping (92 ページ)

DISABLE DHCP Snooping ARPSECURITY (93 ページ)

ENABLE DHCP Snooping LOG (107 ページ)

SHOW DHCP Snooping (160 ページ)

ENABLE DHCP Snooping LOG

カテゴリー：スイッチング / DHCP Snooping

ENABLE DHCP Snooping LOG={ARPSECURITY|MACFILTER}

解説

DHCP Snooping のログ機能を有効にする。デフォルトは無効。

パラメーター

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

関連コマンド

CREATE DHCP Snooping MACFILTER (84 ページ)

DISABLE DHCP Snooping LOG (94 ページ)

ENABLE DHCP Snooping (105 ページ)

ENABLE DHCP Snooping ARPSECURITY (106 ページ)

SHOW DHCP Snooping (160 ページ)

SHOW LOG (「運用・管理」の 264 ページ)

ENABLE DHCP Snooping OPTION82

カテゴリー：スイッチング / DHCP Snooping

ENABLE DHCP Snooping OPTION82

解説

DHCP Snooping のオプション機能であるリレーエージェント情報オプション（オプションコード 82）の付加・検査・削除を有効にする。デフォルトは無効。本機能は、DHCP Snooping が有効になっていないと動作しない。

本機能を有効にした場合、Untrusted ポートで受信したクライアントからの DHCP/BOOTP パケットを転送するときに、リレーエージェント情報オプションを挿入する。同オプションには次の情報が含まれる。

- ・ Remote-ID: 本製品の MAC アドレス
- ・ Circuit-ID: クライアントパケットを受信したスイッチポートと VLAN ID
- ・ Subscriber-ID: (オプション) 任意の文字列 (SET DHCP Snooping PORT コマンドの SUBSCRIBERID パラメーターで設定した場合のみ含める)

受信した DHCP/BOOTP パケットにリレーエージェント情報オプションがすでに付加されていた場合の動作は、受信ポートの DHCP Snooping ポート種別によって異なる。なお、このときの動作は、本機能の有効・無効とは関係なくつねに同じとなる。

- ・ Untrusted ポートでは破棄
- ・ Trusted ポートでは変更せずにそのまま転送

本機能が有効のとき、サーバーからの戻りパケットを Untrusted ポート配下のクライアントに転送するときは、クライアントが Untrusted ポートに直接接続されている場合にかぎって同オプションを削除する。

関連コマンド

DISABLE DHCP Snooping (92 ページ)

DISABLE DHCP Snooping OPTION82 (95 ページ)

SHOW DHCP Snooping (160 ページ)

ENABLE EPSRSNOOPING

カテゴリー：スイッチング / EPSR Snooping

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

vlanname: VLAN 名 (1~20 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。

パラメーター

CONTROLVLAN コントロール VLAN。VLAN 名または VLAN ID (VID) で指定する。

関連コマンド

DISABLE EPSRSNOOPING (96 ページ)

SHOW EPSRSNOOPING (171 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。

関連コマンド

DISABLE PORTAUTH（97 ページ）

SHOW PORTAUTH（172 ページ）

SHOW PORTAUTH PORT（178 ページ）

ENABLE PORTAUTH PORT LOGTYPE

カテゴリー：スイッチング / ポート認証

ENABLE PORTAUTH [= {ALL|8021X|MACBASED|WEBBASED}] **PORT**={*port-list*|ALL}
LOGTYPE={SUCCESS|FAILURE|LOGOFF|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

認証ログ機能を有効にする。指定した認証メカニズムで指定したログタイプを残す。デフォルトは有効。全認証メカニズムの全ログタイプを残す。

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)、ALL のいずれかを指定する。デフォルトは ALL。

PORT スイッチポート番号。複数指定が可能。

LOGTYPE ログタイプ。SUCCESS (成功のみ)、FAILURE (失敗のみ)、LOGOFF (ログオフ)、ALL (すべて) のいずれかを指定する。カンマ区切りによる複数指定が可能。デフォルトは ALL。SUCCESS 指定時は、「Web 認証ログ」・「認証成功ログ」が対象となる。FAILURE 指定時は、「認証失敗ログ」・「RADIUS サーバーログ」が対象となる。LOGOFF 指定時は、「Web 認証ログ」・「ログオフログ」が対象となる。

関連コマンド

DISABLE PORTAUTH PORT LOGTYPE (98 ページ)

SHOW PORTAUTH (172 ページ)

SHOW PORTAUTH PORT (178 ページ)

ENABLE RRPSNOOPING

カテゴリー：スイッチング / RRP Snooping

ENABLE RRPSNOOPING

解説

RRP Snooping を有効にする。デフォルトは無効。

関連コマンド

DISABLE RRPSNOOPING (99 ページ)

SHOW RRPSNOOPING (185 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。

パラメーター

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

関連コマンド

DISABLE SWITCH PORT (100 ページ)

SHOW SWITCH PORT (191 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。

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。

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

DISABLE SWITCH PORT FLOW (101 ページ)

SHOW SWITCH PORT (191 ページ)

ENABLE SWITCH PORT LOOPDETECTION

カテゴリー：スイッチング / ポート

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

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

解説

指定したポートの LDF 検出を有効にする。デフォルトは無効。
有効にした直後から、LDF の送信が開始される。

パラメーター

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

例

ポート 2 の LDF 機能を有効にする

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

備考・注意事項

LDF 検出有効時は、各ポートの LDF 検出の有効/無効にかかわらず、すべてのポートで受信した LDF が LDF 検出の対象になる。

関連コマンド

DISABLE SWITCH PORT LOOPDETECTION (102 ページ)

RESET SWITCH PORT LOOPDETECTION COUNTER (126 ページ)

SET SWITCH PORT LOOPDETECTION (149 ページ)

SHOW SWITCH PORT LOOPDETECTION (200 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。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。

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 (103 ページ)

RESET SWITCH PORT STORMDETECTION COUNTER (127 ページ)

SET SWITCH PORT STORMDETECTION (154 ページ)

SHOW SWITCH PORT STORMDETECTION (206 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 (104 ページ)

PURGE WEBAUTHSERVER (120 ページ)

SET WEBAUTHSERVER (157 ページ)

SHOW PORTAUTH (172 ページ)

SHOW PORTAUTH PORT (178 ページ)

SHOW WEBAUTHSERVER (213 ページ)

PURGE DHCP Snooping

カテゴリー：スイッチング / DHCP Snooping

PURGE DHCP Snooping

解説

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

備考・注意事項

NVS に書き込まれているクライアント情報もすべて消去される。

PURGE SWITCH PORT

カテゴリー：スイッチング / ポート

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。

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。

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 (186 ページ)

SHOW SWITCH FDB (「フォワーディングデータベース」の11 ページ)

PURGE WEBAUTHSERVER

カテゴリー：スイッチング / ポート認証

PURGE WEBAUTHSERVER

解説

Web 認証サーバーの設定情報をすべて削除し、機能を無効にする。

関連コマンド

DISABLE WEBAUTHSERVER (104 ページ)

ENABLE WEBAUTHSERVER (117 ページ)

SET WEBAUTHSERVER (157 ページ)

SHOW PORTAUTH (172 ページ)

SHOW PORTAUTH PORT (178 ページ)

SHOW WEBAUTHSERVER (213 ページ)

RESET DHCP Snooping COUNTER

カテゴリー：スイッチング / DHCP Snooping

RESET DHCP Snooping COUNTER

解説

DHCP Snooping の統計情報をリセットする。

関連コマンド

SHOW DHCP Snooping COUNTER (162 ページ)

RESET DHCP Snooping DATABASE

カテゴリー：スイッチング / DHCP Snooping

RESET DHCP Snooping DATABASE [PORT={*port-list*|ALL}]

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

解説

指定したスイッチポートのダイナミックエントリーを DHCP Snooping テーブル (バインディングデータベース) から削除する。

パラメーター

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

備考・注意事項

NVS に書き込まれている該当のクライアント情報も削除される。

RESET PORTAUTH PORT

カテゴリー：スイッチング / 802.1X 認証

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

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

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

解説

指定ポートにおいて、ポート認証機能の状態をリセットする。

パラメーター

PORTAUTH 認証メカニズム。ALL (すべての認証方式)、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。指定した認証方式が設定されているポートの認証状態をリセットする。

PORT スイッチポート。複数指定が可能。

SUPPLICANTMAC ポート配下に複数のクライアントが存在する構成において、対象のクライアントの MAC アドレスを指定する。

関連コマンド

DISABLE PORTAUTH (97 ページ)

ENABLE PORTAUTH (110 ページ)

SHOW PORTAUTH PORT (178 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 (186 ページ)

SHOW SWITCH FDB (「フォワーディングデータベース」の 11 ページ)

RESET SWITCH PORT

カテゴリー：スイッチング / ポート

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

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

解説

スイッチポートをハードウェア的にリセットする。

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

パラメーター

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

COUNTER 統計カウンターだけをリセットしたいときに指定する。

関連コマンド

DISABLE SWITCH PORT (100 ページ)

ENABLE SWITCH PORT (113 ページ)

SHOW SWITCH PORT (191 ページ)

RESET SWITCH PORT LOOPDETECTION COUNTER

カテゴリー：スイッチング / ポート

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

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

解説

LDF 検出機能のカウンター情報をリセット (クリア) する

パラメーター

PORT ポート番号。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

例

ポート 2 の LDF 検出機能のカウンターをリセットする

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

関連コマンド

DISABLE SWITCH PORT LOOPDETECTION (102 ページ)

ENABLE SWITCH PORT LOOPDETECTION (115 ページ)

SET SWITCH PORT LOOPDETECTION (149 ページ)

SHOW SWITCH PORT LOOPDETECTION (200 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。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。

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 (103 ページ)

ENABLE SWITCH PORT STORMDETECTION (116 ページ)

SET SWITCH PORT STORMDETECTION (154 ページ)

SHOW SWITCH PORT STORMDETECTION (206 ページ)

SET DHCP Snooping CHECKINTERVAL

カテゴリー：スイッチング / DHCP Snooping

SET DHCP Snooping CHECKINTERVAL=1..3600

解説

DHCP Snooping テーブル（バインディングデータベース）のチェック間隔を変更する。

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

パラメーター

CHECKINTERVAL チェック間隔（秒）。デフォルトは 60 秒。

備考・注意事項

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

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

Web 認証サーバーのテンポラリー IP アドレスを使用（SET WEBAUTHSERVER コマンドの TEMPORARYIP パラメーターで設定）して登録されたダイナミックエントリーは NVS（Non-Volatile Storage）に書き込まない。

関連コマンド

ENABLE DHCP Snooping（105 ページ）

SHOW DHCP Snooping（160 ページ）

SET DHCP Snooping CHECKOPTIONS

カテゴリー：スイッチング / DHCP Snooping

SET DHCP Snooping CHECKOPTIONS={NONE|DHCPRELEASE|LINKDOWN}

解説

DHCP Snooping テーブル（バインディングデータベース）から DHCP クライアント情報を削除する条件を設定する。

パラメーター

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

備考・注意事項

リース満了以外のダイナミックエントリーの削除条件によって削除されたとき、DHCP Snooping テーブル（バインディングデータベース）のチェック間隔（SET DHCP Snooping CHECKINTERVAL コマンドで設定）でのチェックを待たずに、その時点で有効な（ダイナミック登録された）クライアントの情報を NVS（Non-Volatile Storage）に書き込む。

SET DHCP Snooping MACFILTER

カテゴリー：スイッチング / DHCP Snooping

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

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

vlanname: VLAN 名 (1~20 文字。英数字とアンダースコア (_)、ハイフンを使用可能。大文字・小文字を区別しない)

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

解説

MAC アドレスフィルタリングエントリーの設定を変更する。

パラメーター

MACFILTER 設定変更するエントリーの ID。

ADDRESS フィルタリング対象装置の MAC アドレス。

MASK フィルタリング対象装置の MAC アドレスへのマスクを指定する。

VLAN 入力 VLAN 名または VID。

PORT MAC アドレスフィルタリングを割り当てるポートを指定する。

ACTION 条件に一致したときのアクション。PERMIT (許可)、DENY (破棄) から選択する。

関連コマンド

CREATE DHCP Snooping MACFILTER (84 ページ)

DESTROY DHCP Snooping MACFILTER (90 ページ)

SHOW DHCP Snooping MACFILTER (167 ページ)

SET DHCP Snooping PORT

カテゴリー：スイッチング / DHCP Snooping

SET DHCP Snooping PORT={*port-list*|ALL} [MAXLEASES=0..96]
[SUBSCRIBERID={*string*|NONE}] [TRUSTED={YES|NO|ON|OFF|TRUE|FALSE}]

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

string: 文字列（0～50文字。英数字と空白のみ使用可能。空白を含む場合はダブルクォートで囲む）

解説

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

パラメーター

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

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

SUBSCRIBERID 指定ポートの Subscriber-ID を指定する。DHCP Snooping のオプション機能であるリレーエージェント情報オプション（オプションコード 82）の付加・検査・削除機能が有効化されている場合、本パラメーターに文字列が指定されているときは、リレーエージェント情報オプションに Subscriber-ID サブオプションを含める。本パラメーターに NONE が指定されている場合は、Subscriber-ID サブオプションを含めない。デフォルトは NONE（Subscriber-ID サブオプションを含めない）。

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

備考・注意事項

Trusted ポートに指定されるポートには、スタティックおよびダイナミックエントリが登録されていない。登録されたポートを Trusted ポートに設定しようとするとコマンドエラーになる。

DHCP サーバーが繋がるポートは Trusted ポートに指定しなければならない。Untrusted ポートに繋がれた DHCP サーバーから IP アドレスを取得することはできない。

DHCP リレーエージェントが繋がるポートは Trusted ポートに指定しなければならない。Untrusted ポートに接続された DHCP リレーエージェント経由で IP を取得しても正常に通信できない。

MAXLEASES パラメーターには、既に登録されているスタティックおよびダイナミックエントリ数を下回る数は設定できない。

ポートランキングとの併用時は、以下のように動作する。

指定したスイッチポートがトランクグループに所属するポートだった場合、トランクグループ単位で設定が反映される。

ただし、設定ファイルにはトランクグループの最若番ポートにのみ設定が残る。

新たにトランクグループを作成した場合、所属ポートへの設定はすべてデフォルト値に戻る。

ただし、MAXLEASES パラメーターは、デフォルト値 (1) に戻すことによってブロックごとの合計値が 96 を超える場合は、0 になることがある。

所属ポート上に登録されていたバインディングデータベースのスタティックおよびダイナミックエントリはすべて削除される。

既存のトランクグループにポートを追加した場合、追加ポートの設定は引き継がれない。

追加ポート上に登録されていたバインディングデータベースのスタティックおよびダイナミックエントリはすべて削除される。

既存のトランクグループからポートを削除した場合、削除ポートの設定はデフォルト値に戻る。

ただし、MAXLEASES パラメーターは、デフォルト値 (1) に戻すことによってブロックごとの合計値が 96 を超える場合は、0 になることがある。

削除ポートが最若番ポートだった場合、削除後の新たな最若番ポートに設定ファイルは引き継がれる。

トランクグループを削除した場合、所属ポートへの設定はすべてデフォルト値に戻る。

ただし、MAXLEASES パラメーターは、デフォルト値 (1) に戻すことによってブロックごとの合計値が 96 を超える場合は、0 になることがある。

トランクグループ上に登録されていたバインディングデータベースのスタティックおよびダイナミックエントリはすべて削除される。

関連コマンド

ADD DHCP Snooping (81 ページ)

ENABLE DHCP Snooping (105 ページ)

ENABLE DHCP Snooping OPTION82 (108 ページ)

SHOW DHCP Snooping (160 ページ)

SHOW DHCP Snooping PORT (169 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。

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 (172 ページ)

SHOW PORTAUTH PORT (178 ページ)

SET PORTAUTH CSIDFORMAT

カテゴリー：スイッチング / ポート認証

SET PORTAUTH CSIDFORMAT [SEPARATOR={HYPHEN|COLON|PERIOD|NONE}] [DIGIT={2|4}] [UPPERCASE={TRUE|FALSE}]

解説

RADIUS パケット内の Calling-Station-ID 及び Called-Station-ID アトリビュートの MAC アドレスのフォーマットを指定する。

ポート認証で RADIUS サーバーに問い合わせる際の、RADIUS、RADIUS アカウンティングパケットに載る。

パラメーター

SEPARATOR 区切り文字のタイプを指定。デフォルトは HYPHEN。

DIGIT 区切り文字を挿入する間隔。SEPARATOR=NONE 指定時は無効。デフォルトは 2。

UPPERCASE 大文字・小文字を指定。TRUE 指定時は大文字。デフォルトは TRUE。

フォーマット	区切り文字のタイプ	区切り文字を挿入する間隔	大文字・小文字を指定
XX-XX-XX-XX-XX-XX	hyphen	2	TRUE
xx-xx-xx-xx-xx-xx	hyphen	2	FALSE
XX:XX:XX:XX:XX:XX	colon	2	TRUE
xx:xx:xx:xx:xx:xx	colon	2	FALSE
XXXX.XXXX.XXXX	period	4	TRUE
xxxx.xxxx.xxxx	period	4	FALSE
XXXXXXXXXXXXXX	none	-	TRUE
xxxxxxxxxxxxxx	none	-	FALSE

表 27: 各パラメーター設定時のフォーマット

例

ポート認証で RADIUS サーバーに問い合わせる際のパケットに載る MAC アドレスのフォーマットの区切りをピリオドに設定する

```
SET PORTAUTH CSIDFORMAT SEPARATOR=PERIOD
```

関連コマンド

SHOW PORTAUTH (172 ページ)

SHOW PORTAUTH PORT (178 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=AUTHENTICATOR [EAPOLVERSION={1|2}] [CONTROL={AUTHORISED|
UNAUTHORISED|AUTO}] [QUIETPERIOD=0..65535] [TXPERIOD=1..65535]
[REAUTHPERIOD=1..65535] [SUPPTIMEOUT=1..600] [SERVERTIMEOUT=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}]
[REAUTHMAX=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 [=8021X] PORT={port-list|ALL} TYPE=AUTHENTICATOR
```

[802.1X 認証 Supplicant 時]

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

[Web 認証 有効時]

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

[認証ポートの解除]

```
SET PORTAUTH= {8021X|MACBASED|WEBBASED|ALL} PORT={port-list|ALL}
TYPE=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)

vlanname: VLAN 名 (1～20 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。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)、ALL 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 スイッチポートの役割。AUTHENTICATOR (802.1X 認証の Authenticator ポート、MAC ベース認証ポート、Web 認証ポート)、SUPPLICANT (802.1X 認証の Supplicant ポート)、NONE (ポート認証機能無効) のいずれかを指定する。

EAPOLVERSION (802.1X Authenticator ポート) EAPOL パケットのバージョンを指定する。1 は IEEE 802.1X-2001 準拠モード、2 は IEEE 802.1X-2004 互換モード。デフォルトは 1。2 を設定した場合、TXPERIOD と MAXREQ パラメーターの設定は無効になる。

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。

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 コマンドの L2ONLY パラメーターで作成) を指定するか、L2ONLY VLAN を指定しない場合はハードウェアパケットフィルターでルーティングを制限する必要がある。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 以外を指定するとただちにゲスト 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) かつ、VLANASSIGNMENTTYPE=PORT 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 (マルチプルダイナミック VLAN) 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 EAP-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) 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) 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) 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) 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) 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)、AUTHORISED (認証済み固定) から選択する。デフォルトは AUTO。通常は AUTO のままでよい。

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 パケットを送信した後、Supplicant からの応答を待つ時間 (秒)。デフォルトは 30 秒。

SERVERTIMEOUT (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 パケットを送信した後、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-Suppliant Authenticator ポート、MAC ベース認証ポート、Web 認証ポート) Multi-Suppliant モード (MODE=MULTI) かつ、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 Suppliant 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 Suppliant は、最初に認証を通った Suppliant 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 Suppliant は、実際には最初に認証をパスした Suppliant と同じ VLAN の所属となる。デフォルトは ON。

SUPLIMIT (802.1X Multi-Suppliant Authenticator ポート、MAC ベース認証ポート、Web 認証ポート) Multi-Suppliant モード (MODE=MULTI) のとき、認証可能な Suppliant 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) Suppliant に対する EAP-Request パケットの最大再送回数。デフォルトは 2 回。

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

HELDPERIOD (802.1X Suppliant 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 Suppliant ポート) EAPOL-Start パケットの最大送信回数。Suppliant 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 Suppliant 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 Suppliant ポート) 指定スイッチポートが Suppliant 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 Suppliant ポート) 指定スイッチポートが Suppliant 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

ポート認証に設定されたポートは VLAN の設定を変更できない。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う必要がある。

サポート Suppliant 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。マルチプルダイナミック VLAN 使用時のサポート Suppliant 数は 100 である。

802.1X はスタティック MAC アドレスとして登録される。MAC ベース認証/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。

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、Suppliant は削除される。

MAC ベース認証は mode=single を設定した場合、Multi-Suppliant Mode/suppliant 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 ベース認証が HELD 以外の状態で、Web 認証の Login を行くと、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。

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。

ポートを Authenticator ポートに設定すると、同ポートで自動的にイーグレスフィルタリングが有効になり、その設定が設定ファイルに書き込まれる。Authenticator ポートではイーグレスフィルタリングが有効になっている必要があるので、イーグレスフィルタリングの設定は変更しない。

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。

VLANASSIGNMENTTYPE パラメーターを USER に設定した場合、マルチプル VLAN (Protected Ports VLAN) は併用できない。

PORTAUTH=ALL 指定時、Web 認証を 3 回失敗しても、HELD 状態にならない。

SERVERTIMEOUT パラメーターの設定値が、[SET RADIUSSERVER コマンドの TIMEOUT パラメーター] × [RETRANSMITCOUNT パラメーター] を下回るとき、DEADTIME パラメーターが機能しない。

関連コマンド

SHOW PORTAUTH (172 ページ)

SHOW PORTAUTH PORT (178 ページ)

SET PORTAUTH USERIDFORMAT

カテゴリー：スイッチング / ポート認証

SET PORTAUTH USERIDFORMAT [SEPARATOR={HYPHEN|COLON|PERIOD|NONE}]
[DIGIT={2|4}] [UPPERCASE={TRUE|FALSE}]

解説

MAC ベース認証のときの RADIUS パケット内の User-Name 及び User-Password アトリビュートの MAC アドレスのフォーマットを指定する。
MAC ベース認証で RADIUS サーバーに問い合わせる際の、ユーザー名の MAC アドレスフォーマットに適用され、そのユーザー名からパスワードが生成される。

パラメーター

SEPARATOR 区切り文字のタイプを指定。デフォルトは HYPHEN。
DIGIT 区切り文字を挿入する間隔。SEPARATOR=NONE 指定時は無効。デフォルトは 2。
UPPERCASE 大文字・小文字を指定。TRUE 指定時は大文字。デフォルトは FALSE。

フォーマット	区切り文字のタイプ	区切り文字を挿入する間隔	大文字・小文字を指定
XX-XX-XX-XX-XX-XX	hyphen	2	TRUE
xx-xx-xx-xx-xx-xx	hyphen	2	FALSE
XX:XX:XX:XX:XX:XX	colon	2	TRUE
xx:xx:xx:xx:xx:xx	colon	2	FALSE
XXXX.XXXX.XXXX	period	4	TRUE
xxxx.xxxx.xxxx	period	4	FALSE
XXXXXXXXXXXXXX	none	-	TRUE
xxxxxxxxxxxxxx	none	-	FALSE

表 28: 各パラメーター設定時のフォーマット

例

MAC ベース認証で RADIUS サーバーに問い合わせる際の MAC アドレスのフォーマットの区切りを無しに設定する

SET PORTAUTH USERIDFORMAT SEPARATOR=NONE

関連コマンド

SHOW PORTAUTH (172 ページ)

SHOW PORTAUTH PORT (178 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gress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gress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 (186 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 (146 ページ)

SHOW SWITCH (186 ページ)

SHOW SWITCH MIRROR (190 ページ)

SHOW SWITCH PORT (191 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|E}

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、B、C、D、E のいずれか。デフォルトは、A。

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
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
E	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、EAP パケットにはタグが付けられ、BPDU パケットにはタグが付けられることはない

表 29:

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

備考・注意事項

MULTICASTMODE パラメーターに 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) が設定されていると、マルチプル VLAN (Protected Ports VLAN) のグループを超えて BPDU/EAP パケットが同一 VLAN 内にフラッディングされる。

関連コマンド

SHOW SWITCH (186 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]
[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|10MHAUTO|10MFAUTO|100MHALF|
100MFULL|100MHAUTO|100MFAUTO|1000MFULL}] [MDIMODE={MDI|MDIX}]
[SOFTRESET] [PRIORITY=0..7] [OVERRIDEPRIORITY={YES|NO|ON|OFF|TRUE|
FALSE}] [COMBO=(FIBER|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。

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。デフォルトでは Port_xx (xx はポート番号) のように定義されている。デフォルトに戻す場合は 1 番ポートの場合は、Port_01 と設定する。

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どうか。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どうか。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どうか。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。

UNMKCASTFILTERING 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。

UNMKCASTEGRESSFILTERING 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。10MHAUTO は 10M Half、10MFAUTO は 10M Full/10M Half、100MHAUTO は 10M Full/10M Half/100M Half、100MFAUTO は 10M Full/10M Half/100M Full/100M Half でネゴシエーションする。デフォルトは AUTONEGOTIATE。

MDIMODE ポートの MDI/MDI-X を設定する。SPEED が 10MHALF、10MFULL、100MHALF、100MFULL のときに指定可能。SPEED が 10MHALF、10MFULL、100MHALF、100MFULL 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。

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

Admit Only Tagged Frame のポートでは PRIORITY パラメーターと OVERRIDEPRIORITY パラメーターを設定できない。

認証ポートに設定した場合、ブロードキャスト/未学習のマルチキャスト/未学習のユニキャストフレームのフィルタリング機能 (BCASTEGRESSFILTERING、UNKMCASTEGRESSFILTERING、UNKUCASTEGRESSFILTERING) が自動で設定されるが、本設定を変更してはならない。

関連コマンド

DISABLE SWITCH PORT (100 ページ)

ENABLE SWITCH PORT (113 ページ)

SHOW SWITCH PORT (191 ページ)

SET SWITCH PORT LOOPDETECTION

カテゴリー：スイッチング / ポート

```
SET SWITCH PORT={port-list|ALL} LOOPDETECTION [ACTION={LINKDOWN|
BCASTDISCARD|NONE}] [INTERVAL=1..1000000] [SECURE={ON|OFF}]
[BLOCKTIMEOUT={10..86400|NONE}]
```

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

解説

LDF 検出機能のパラメータを設定する。

パラメーター

PORT ポート番号または ALL を指定する

ACTION LDF を検出した場合のアクション。NONE (何もしない)、LINKDOWN (ポートを物理的にリンクダウンさせる)、BCASTDISCARD (ポートのブロードキャストフレームの受信を止める) から選択する。デフォルトは LINKDOWN。アクション実行中に、このパラメータによって別のアクションを設定した場合は、次回アクション実行時から適用する

INTERVAL LDF の送信間隔。単位は秒。デフォルト 120 秒。INTERVAL を変更した直後に、LDF が送信される

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

BLOCKTIMEOUT ACTION パラメータ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、LDF を検出した場合のアクションをリンクダウン、LDF の送信間隔を 60 秒、実行前の状態に戻るまでの時間を 3600 秒に設定する。

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

備考・注意事項

LDF 検出有効時は、各ポートの LDF 検出の有効/無効にかかわらず、すべてのポートで受信した LDF が

LDF 検出の対象になる。

STP、Rapid STP、Multiple STP、EPSR Snooping を併用する場合、アクションには LINKDOWN を指定することを推奨。

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 LOOPDETECTION 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 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）。

関連コマンド

DISABLE SWITCH PORT LOOPDETECTION (102 ページ)

ENABLE SWITCH PORT LOOPDETECTION (115 ページ)

RESET SWITCH PORT LOOPDETECTION COUNTER (126 ページ)

SHOW SWITCH PORT LOOPDETECTION (200 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 (144 ページ)

SHOW SWITCH (186 ページ)

SHOW SWITCH MIRROR (190 ページ)

SHOW SWITCH PORT (191 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 アドレスをステックエントリとし、セキュリティモードとなる。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) 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。TRAP 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。デフォルトは DISCARD。

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 (198 ページ)

SHOW SWITCH PORT SECURITYMODE (204 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] [HIGHRATETHRESHOLD=1..1048576]
[BLOCKTIMEOUT={10..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。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。

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。デフォルトは 819200。

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。デフォルトは 512000。

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。

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 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超えた場合、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 (103 ページ)

ENABLE SWITCH PORT STORMDETECTION (116 ページ)

RESET SWITCH PORT STORMDETECTION COUNTER (127 ページ)

SHOW SWITCH PORT STORMDETECTION (206 ページ)

SET SWITCH TRUNK

カテゴリー：スイッチング / ポート

```
SET SWITCH TRUNK=trunk SELECT={MACSRC|MACDEST|MACBOTH|IPSRC|IPDEST|
IPBOTH}
```

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

フラッドパケットは、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。

SELECT パラメーターに MAC アドレスの選択基準 (MACSRC、MACDEST、MACBOTH) が指定されていると、ルーティング後のパケットが負荷分散されずに送出される。

関連コマンド

ADD SWITCH TRUNK (83 ページ)
 CREATE SWITCH TRUNK (86 ページ)
 DELETE SWITCH TRUNK (89 ページ)
 DESTROY SWITCH TRUNK (91 ページ)
 SHOW SWITCH TRUNK (211 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] [PORT=port] [REDIRECTURL={url-string|
NONE}] [SECURITY={ENABLED|DISABLED}] [SSLKEYID={key-id|NONE}]
[SSLPORT=port] [HEADER={string|NONE}] [SUBHEADERTOP={string|NONE}]
[SUBHEADERBOTTOM={string|NONE}] [FOOTER={string|NONE}]
[HTTPREDIRECT={ENABLED|DISABLED}] [SESSIONKEEP={ENABLED|DISABLED}]
[PROXYSERVER={long-string|NONE}] [PROXYPORT={port|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: TCP ポート番号 (1~65535)

url-string: 文字列 (1~100 文字。使用可能な文字は半角英数字、半角記号 (- : / . _))

key-id: 鍵番号 (0~65535)

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。" (ダブルクォート) は使用できない)

long-string: 文字列 (1~255 文字。使用可能な文字は半角英数字、半角記号 (# \$ % & ' () ~ | - ^ \ @ ' { + * } [; :] , . / -) 文字列に半角空白、! = ? < > を含む場合は、前後をダブルクォート (") で囲む必要がある。)

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。デフォルトは 80。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。セッションキープが有効な場合、認証成功後はセッションキープが優先される。

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。

HTTPREDIRECT HTTP リダイレクト機能の有効・無効。有効時は、任意の URL へのアクセスの応答として、Web 認証ログインページを表示する。デフォルトは DISABLED。

SESSIONKEEP URL 保持機能の有効無効。有効時は認証後、認証開始時に アクセスしようとしていた URL へ自動的にジャンプする。HTTP リダイレクトが有効の場合に機能する。URL 情報は、認証動作が無い場合、5 分間保持され、削除される。ただし 認証が Held 状態になり、それが解除されると URL 情報は削除される。デフォルトは DISABLED。認証成功後はリダイレクト URL が設定されていても、セッションキープが優先される。

PROXYSERVER スイッチが生成する PAC ファイルに記述されるプロキシサーバーの IP アドレスもしくはホスト名を指定する。デフォルトは NONE。

PROXYPORT プロキシサーバーのポート番号を設定する。設定されたポート番号に、HTTP でのアクセスが可能になる。デフォルトは NONE。

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。

REAUTHREFRESH 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 DHCP サーバーの Policy に設定された LEASETIME で IP アドレスを付与する。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=ENABLED) 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 (104 ページ)

ENABLE WEBAUTHSERVER (117 ページ)

PURGE WEBAUTHSERVER (120 ページ)

SET PORTAUTH PORT (136 ページ)

SHOW PORTAUTH (172 ページ)

SHOW PORTAUTH PORT (178 ページ)

SHOW WEBAUTHSERVER (213 ページ)

SHOW DHCP Snooping

カテゴリー：スイッチング / DHCP Snooping

SHOW DHCP Snooping

解説

DHCP Snooping の全般的な設定情報を表示する。

入力・出力・画面例

```
# show dhcp snooping

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

DHCP Snooping Database:
Full Leases/Max Leases ... 2/24
Block 1 (Port1-8) ..... 1/8
Block 2 (Port9-16) ..... 1/8
Block 3 (Port17-24) .... 0/8
Block 4 (Trunk Group) .. 0/0
Check Interval ..... 60 seconds
Check Options ..... None
-----
```

DHCP Snooping	DHCP Snooping の有効・無効
Option 82 status	リレーエージェント情報オプション（オプションコード 82）の付加・検査・削除機能の有効・無効
ARP security	ARP セキュリティー機能の有効・無効
Logging enabled	ログ機能の有効・無効。無効時は None、有効時はログへの記録対象イベント（現時点では ArpSecurity のみ）が表示される
Full Leases/Max Leases	DHCP Snooping テーブル（バインディングデータベース）に現在登録されているクライアントの数 / 登録可能なクライアントの総数
Block 1 (Port1-8)	DHCP Snooping テーブル（バインディングデータベース）に現在登録されている該当ブロック（Port 1～8）上のクライアントの数 / 該当ブロック（Port 1～8）上で登録可能なクライアントの総数

Block 2 (Port9-16)	DHCP Snooping テーブル (バインディングデータベース) に現在登録されている該当ブロック (Port 9 ~ 16) 上のクライアントの数 / 該当ブロック (Port 9 ~ 16) 上で登録可能なクライアントの総数
Block 3 (Port17-24)	DHCP Snooping テーブル (バインディングデータベース) に現在登録されている該当ブロック (Port 17 ~ 24) 上のクライアントの数 / 該当ブロック (Port 17 ~ 24) 上で登録可能なクライアントの総数
Block 4 (Trunk Group)	DHCP Snooping テーブル (バインディングデータベース) に現在登録されている該当ブロック (Trunk Group) 上のクライアントの数 / 該当ブロック (Trunk Group) 上で登録可能なクライアントの総数
Check Interval	バインディングデータベースのチェック間隔
Check Options	バインディングデータベースからクライアント情報を削除する条件。リース満了以外に指定された条件を表示する。DHCPRELEASE (DHCP RELEASE パケットを受信した場合)、LINKDOWN (クライアントが所属するポートがリンクダウンした場合)、その両方、または None (リース満了以外の条件を指定しない)

表 30:

関連コマンド

ENABLE DHCP Snooping (105 ページ)
 ENABLE DHCP Snooping ARPSECURITY (106 ページ)
 ENABLE DHCP Snooping LOG (107 ページ)
 ENABLE DHCP Snooping OPTION82 (108 ページ)
 SET DHCP Snooping CHECKINTERVAL (128 ページ)
 SET DHCP Snooping PORT (131 ページ)

SHOW DHCP Snooping COUNTER

カテゴリー：スイッチング / DHCP Snooping

SHOW DHCP Snooping COUNTER

解説

DHCP Snooping の統計情報を表示する。

入力・出力・画面例

```
# show dhcp Snooping counter

DHCP Snooping Counters
-----

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

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

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

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

表 31:

関連コマンド

ENABLE DHCP Snooping (105 ページ)

ENABLE DHCP Snooping ARP Security (106 ページ)

RESET DHCP Snooping Counter (121 ページ)

SHOW DHCP Snooping DATABASE

カテゴリー：スイッチング / DHCP Snooping

SHOW DHCP Snooping DATABASE

解説

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

入力・出力・画面例

```
# show dhcp Snooping database

DHCP Snooping Binding Database
-----
Full Leases/Max Leases ... 2/24
  Block 1 (Port1-8) ..... 1/8
  Block 2 (Port9-16) ..... 1/8
  Block 3 (Port17-24) .... 0/8
  Block 4 (Trunk Group) .. 0/0
Check Interval ..... 60 seconds
Check Options ..... None

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

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

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

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

Block 1 (Port1-8)	DHCP Snooping テーブル (バインディングデータベース) に現在登録されている該当ブロック (Port 1 ~ 8) 上のクライアントの数 / 該当ブロック (Port 1 ~ 8) 上で登録可能なクライアントの総数
Block 2 (Port9-16)	DHCP Snooping テーブル (バインディングデータベース) に現在登録されている該当ブロック (Port 9 ~ 16) 上のクライアントの数 / 該当ブロック (Port 9 ~ 16) 上で登録可能なクライアントの総数
Block 3 (Port17-24)	DHCP Snooping テーブル (バインディングデータベース) に現在登録されている該当ブロック (Port 17 ~ 24) 上のクライアントの数 / 該当ブロック (Port 17 ~ 24) 上で登録可能なクライアントの総数
Block 4 (Trunk Group)	DHCP Snooping テーブル (バインディングデータベース) に現在登録されている該当ブロック (Trunk Group) 上のクライアントの数 / 該当ブロック (Trunk Group) 上で登録可能なクライアントの総数
Check Interval	バインディングデータベースのチェック間隔
Check Options	バインディングデータベースからクライアント情報を削除する条件。リース満了以外に指定された条件を表示する。DHCPRELEASE (DHCP RELEASE パケットを受信した場合)、LINKDOWN (クライアントが所属するポートがリンクダウンした場合)、その両方、または None (リース満了以外の条件を指定しない)

Current valid entries セクション	現在有効なクライアントの登録情報が IP アドレスの昇順で表示される
Entries with client lease but no listeners セクション	ハードウェアフィルタテーブルに登録できなかったなどの理由で現在無効となっているクライアントの登録情報が表示される
Entries with no client lease and no listeners セクション	DHCP メッセージに問題があったなどの理由で現在無効となっているクライアントの登録情報が表示される
MAC Address	クライアントの MAC アドレス
IP Address	クライアントの IP アドレス
Expires(s)	該当エントリーの残り有効時間 (秒) (IP アドレス使用期限までの残り時間)。スタティックエントリーは Static、Web 認証サーバーのテンポラリー IP アドレスは Temporary と表示される
VLAN	クライアントが所属している VLAN
Port	クライアントが接続されているスイッチポート
ID	未サポート
Source	エントリー (クライアント) の種類。Dynamic (ダイナミックエントリー。DHCP クライアント)、User (スタティックエントリー。IP 固定設定クライアント)、Nvs (DHCP Snooping が有効化されたときに NVS からロードしたエントリー)

表 32:

関連コマンド

ENABLE DHCP Snooping (105 ページ)

SHOW DHCP Snooping MACFILTER

カテゴリー：スイッチング / DHCP Snooping

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

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

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

解説

MAC アドレスフィルタリングの設定を変更する。

パラメーター

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

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

入力・出力・画面例

```
# show dhcp snooping macfilter

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

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

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

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

-----
```

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

表 33:

備考・注意事項

エントリーの ID とポート番号を同時に指定することはできない。

関連コマンド

CREATE DHCP Snooping MACFILTER (84 ページ)
 DESTROY DHCP Snooping MACFILTER (90 ページ)
 SET DHCP Snooping MACFILTER (130 ページ)

SHOW DHCP Snooping PORT

カテゴリー：スイッチング / DHCP Snooping

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

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

解説

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

パラメーター

PORT スイッチポート。複数指定が可能。省略時および ALL を指定した場合はすべてのポートが対象となる。

入力・出力・画面例

```
# show dhcp snooping port=11

DHCP Snooping Port Information:
-----

Port ..... 11
Trusted ..... No
Full Leases/Max Leases ... 1/1
Subscriber-ID ..... None
-----

# show dhcp snooping port=21

DHCP Snooping Port Information:
-----

Trunk group ID ..... 1
Trunk group name ..... t1
Trunk group ports ..... 21-24
Trusted ..... No
Full Leases/Max Leases ... 0/1
Subscriber-ID ..... None
-----
```

Port	スイッチポート番号
Trunk group ID	トランクグループの ID。指定したスイッチポートがトランクグループに所属していた場合に表示される。
Trunk group name	トランクグループ名。指定したスイッチポートがトランクグループに所属していた場合に表示される。
Trunk group ports	所属ポート。指定したスイッチポートがトランクグループに所属していた場合に表示される。
Trusted	DHCP Snooping における ポート 種別。Yes (Trusted ポート)、No (Untrusted ポート) のいずれか
Full Leases/Max Leases	DHCP Snooping テーブル (バインディングデータベース) に現在登録されている該当ポート上のクライアントの数 / 該当ポート上で登録可能なクライアントの総数
Subscriber-ID	該当ポートの Subscriber-ID。設定されていない場合は None と表示される。

表 34:

関連コマンド

ENABLE DHCP Snooping (105 ページ)

SET DHCP Snooping PORT (131 ページ)

SHOW EPSRSNOOPING

カテゴリー：スイッチング / EPSR Snooping

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

vlanname: VLAN 名 (1~20 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 Snooping の情報を表示する

パラメーター

CONTROLVLAN コントロール VLAN。VLAN 名または VLAN ID (VID) で指定する。省略時および ALL を指定した場合は、すべてのコントロール VLAN の EPSR Snooping 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 35:

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 (96 ページ)

ENABLE EPSRSNOOPING (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。

パラメーター

PORTAUTH 認証メカニズム。8021X (802.1X 認証について表示) MACBASED (MAC 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.... 1
Number of WEB Based Supplicants.... 0
Total Supplicants..... 2

Port AuthMode Role  VID  PortStatus      Status          ReAuth Timer  Tag
              MAC Address      IP Address      User Name
-----
  1 802.1X   Auth  1    Authorized    Connecting      -----      n
                        00:40:CA:1B:6F:1C  192.168.1.10
  1 802.1X   Auth  1    Authorized    Authenticated   3365          n
                        00:0A:E6:6A:CC:7F  192.168.1.12  vlanno
  1 MACBASE  Auth  1    Authorized    Authenticated   3429          n
                        00:40:CA:1B:6F:1C  192.168.1.10  00-40-ca-1b-6f-1c
  1 MACBASE  Auth  1    Authorized    Connecting      -----      n
```

```

00:0A:E6:6A:CC:7F 192.168.1.12 -----
1 WEBBASE Auth 1 Authorized Connecting ----- n
00:40:CA:1B:6F:1C 192.168.1.10 -----
1 WEBBASE Auth 1 Authorized Connecting ----- n
00:0A:E6:6A:CC:7F 192.168.1.12 -----

# show portauth=8021X port=1

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

Port AuthMode Role VID PortStatus Status ReAuth Timer Tag
MAC Address IP Address User Name
-----
1 802.1X Auth 2 Authorized Authenticated 3589 n
00:0A:E6:6A:CC:7F 192.168.2.157 test

# show portauth=all config

Port Authentication Information
-----
SystemAuthControl..... Enabled
MAC Based Auth User-ID Format..... xx-xx-xx-xx-xx-xx
Calling/Called-Station-ID Format... XX-XX-XX-XX-XX-XX

Port 1

802.1x Authentication Information
-----
PAE Type..... None
Log Type..... Full

MAC BASE Authentication Information
-----
PAE Type..... None
Log Type..... Full

WEB BASE Authentication Information
-----
PAE Type..... None
Log Type..... Full

# 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 認証で認証に成功した Supplicant の数

Number of MAC Based Supplicants	MAC ベース認証で認証に成功した Supplicant の数
Number of WEB Based Supplicants	Web 認証で認証に成功した Supplicant の数
Total Supplicants	Supplicant の数（未認証の Supplicant も含む）
Port	ポート番号
AuthMode	認証メカニズム。802.1X、MACBASE、WEBBASE のいずれか
Role	タイプ。Auth、Supp、None のいずれか
VID	VLAN ID。1～4094 の範囲で表示
PortStatus	ポートの状態。Unauthorized（未認証）か Authorized（認証済み）
Status	認証の状態。Initialize、Disconnected、Connecting、Authenticating、Authenticated、Aborting、Held、ForceAuth、ForceUnauth のいずれか。
ReAuth Timer	再認証タイマー。再認証までの残り時間（秒）。
Tag	タグ付きポートで認証したか否か。
MAC Address	サブリカントの MAC アドレス。
IP Address	サブリカントの IP アドレス。ARP テーブルに学習済みの場合のみ表示。
User Name	認証時のユーザー名。最大 20 文字まで。

表 36: CONFIG または STATUS を指定しない場合

SystemAuthControl	ポート認証機能の有効・無効。Enabled か Disabled。
MAC Based Auth User-ID Format	MAC ベース認証時のユーザー名・パスワードのフォーマット
Calling/Called-Station-ID Format	Calling/Called-Station-ID のフォーマット
Port	ポート番号
PAE Type	スイッチポートのタイプ。Authenticator、Supplicant、None のいずれか
Log Type	認証ログの状態。All（認証ログは全て残す）、Success（認証成功ログを残す）、Failure（認証失敗ログを残す）、Logoff（認証解除ログを残す）、None（認証ログは残さない）のいずれか

表 37: 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、None のいずれか
Supplicant Mode	Authenticator ポートのモード。Single か Multiple
Number of Supplicant	Supplicant 数
Attached Supplicant(s)	ポートに接続している Supplicant 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、ポート認証機能が有効の場合に、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) ForceAuth (「認証済み」に固定設定) ForceUnauth (「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。Unauthorized (未認証) か Authorized (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	Supplicant が接続している VLAN の VID

表 38: 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=8021X
```

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ず

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 (97 ページ)

ENABLE PORTAUTH (110 ページ)

SET PORTAUTH AUTHMETHOD (133 ページ)

SET PORTAUTH PORT (136 ページ)

SHOW PORTAUTH PORT (178 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 [{CONFIG|STATUS}]

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

パラメーター

PORTAUTH 認証メカニズム。8021X (802.1X 認証について表示) MACBASED (MAC 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 802.1X Authenticator、MAC ベース認証、Web 認証の情報を表示する。

SUPPLICANT 802.1X Supplicant の情報を表示する。

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
```

```
Log Type..... All
```

```
MAC BASE Authentication Information
```

```
-----
```

```
PAE Type..... Authenticator
```

```
Log Type..... All
```

```
WEB BASE Authentication Information
```

```

-----
PAE Type..... Authenticator
Log Type..... All

Supplicant Mode..... Multiple
Supplicant Limit..... 320
eapolVersion..... 1
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=15 authenticator status

```

```

Port 15

```

```

802.1x Authentication Information
-----

```

```

PAE Type..... None

```

```

MAC BASE Authentication Information
-----

```

```

PAE Type..... Authenticator
Supplicant Mode..... Multiple
Number of Supplicants..... 2

```

```

Attached Supplicant(s)

```

```

Attached Supplicant(s)

```

```

    MAC Address..... 00:40:CA:1B:6F:1C
    User Name..... 00-40-CA-1B-6F-1C
    IP Address..... 192.168.1.10
    Port Status..... Authorized

```

```

    Authenticator PAE State..... Authenticated
    Backend Authenticator State..... Idle
    VLAN ID..... 2
    Re-Auth Timer..... 3600
MAC Address..... 00:0A:E6:6A:CC:7F
    User Name..... 00-0A-E6-6A-CC-7F
    IP Address..... 192.168.1.12
    Port Status..... Authorized
    Authenticator PAE State..... Authenticated
    Backend Authenticator State..... Idle
    VLAN ID..... 2
    Re-Auth Timer..... 3600

# 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 Au- thentication Information)	スイッチポートのタイプ (802.1X における役割)、Authenticator、None 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、None 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、None のいずれ か
Log Type	認証ログの状態。All (認証ログは全て残す)、Success (認証成功ログを残す)、Failure (認証失敗ログを残す)、Logoff (認証解除ログを残す)、None (認証ログは残さない) 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
eapolVersion	(Authenticator ポート) 802.1X 認証のプロトコルバージョン。1 または 2
AuthControl- PortControl	(Authenticator ポート) 手動設定による Authenticator ポートの状態。Auto、Force- Unauth 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、RA- DIUS 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
vlan- Assignment	(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
Force-Renewing	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 Forwarding	(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 Forwarding	(Authenticator ポート) 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) 未認証状態で、透過する UDP ポートのパケット

表 39: 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、None のいずれか
Supplicant Mode	Authenticator ポートのモード。Single か Multiple
Number of Supplicant	Supplicant 数
Attached Supplicant(s)	ポートに接続している Supplicant の情報を表示
MAC Address	サブリカント MAC アドレス。タグ付きポートで認証したときは [TAG] 表示あり。
User Name	ユーザー名。最大 35 文字まで。
IP Address	サブリカント IP アドレス。ARP テーブルに学習済みの場合のみ表示。
Port Status	ポートの状態。Unauthorised (未認証) か Authorised (認証済み)
Authenticator 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。) 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) ForceAuth (「 認証済み 」 に固定設定) ForceUnauth (「 未認証 」 に固定設定) のいずれか。

Backend Authenticator State	認証機構の状態。Request、Response、Success、Fail、Timeout、Idle、Initialize のいずれか。
VLAN ID	VLAN ID。1～4094 の範囲で表示。
Re-Auth Timer	再認証タイマー。再認証までの残り時間（秒）。

表 40: 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）。Supplicant、None 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 41: 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）。Supplicant、None 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。）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 42: 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（97 ページ）

ENABLE PORTAUTH（110 ページ）

SET PORTAUTH AUTHMETHOD (133 ページ)

SET PORTAUTH PORT (136 ページ)

SHOW PORTAUTH (172 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 43:

例

RRP Snooping の状態を表示する

SHOW RRPSNOOPING

関連コマンド

DISABLE RRPSNOOPING (99 ページ)

ENABLE RRPSNOOPING (112 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 v2.11.1J
Application Software Build Date ..... Apr  5 2010 11:41:38
Bootloader Version ..... ATS63_LOADER v3.2.1
Bootloader Build Date ..... Jul  1 2009 11:31:24
MAC Address ..... 00:15:77:9C:D3:EF
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
Powersaving ..... Disabled
```

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。Disabled のみ
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)、Forward within VLAN (tagged/untagged ports)、または、Forward within VLAN (all ports)
Powersaving	省電力モードの状態。有効 (Enabled) または無効 (Disabled)

表 44:

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 (124 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	ジャバースフレーム受信数。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 45:

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 (124 ページ)

SHOW SWITCH (186 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 46:

関連コマンド

- SET SWITCH MIRROR (144 ページ)
- SET SWITCH PORT MIRROR (151 ページ)
- SHOW SWITCH (186 ページ)
- SHOW SWITCH PORT (191 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。複数指定が可能。省略時および ALL を指定した場合はすべてのポートが対象となる。

入力・出力・画面例

```
# show switch port=23

Port #23 Information:

Port Description (ifName) ..... Port_23
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 ..... -
Combo port ..... FiberAuto
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
```

```

GBIC/SFP #1 ..... Not Present
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 Storm Detection)”となる。LDF 検出により Disabled になった場合、“Disabled (by Loop Detection)”となる。
Link state	ポートのリンクステータス。Up か Down
Configured Speed/Duplex	通信モードの設定値。Autonegotiate、10/100 Mbps Half/Full duplex、Autonegotiate (10/100 Mbps Half/Full duplex、1000 Mbps Full duplex)、1000Mbps, full duplex で表示される。1000Mbps, full duplex は SFP ポートが 1000MFull に設定されているときに表示。Autonegotiate (1000 Mbps Full duplex) は 1000BASE-T ポートが 1000MFull に設定されているときに表示
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
Combo port	コンボポートのメディア選択モードの設定を表示。ポート 21/22/23/24 で表示。FiberAuto (SFP ポート優先)、Fiber (SFP ポート固定)、Copper (1000BASE-T ポート固定) のいずれか
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、“Enabled (by Storm Detection)”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
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、Disabled 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とタグプライオリティ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を優先する。NO の場合は、タグプライオリティを優先する
Mirroring State	ポートミラーリング機能の有効・無効
Is this port mirror port	ミラーポートに設定されているかどうか。ポートミラーリング機能が有効のとき、表示される。

表 47:

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 (146 ページ)

SHOW SWITCH PORT COUNTER

カテゴリー：スイッチング / ポート

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

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

解説

スイッチポートの統計カウンターを表示する。

パラメーター

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

COUNTER 省略した場合または、DETAIL を指定した場合はカウンターの詳細情報を表示、SUMMARY を指定した場合は一覧を表示する。

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

# show switch port=1-3 counter=summary

Port                InPkts    InUcastPkts    InNUcastPkts    InErrors
                   OutPkts    OutUcastPkts    OutNUcastPkts    OutErrors
-----
1:Port_01                0              0                0                0
```

	0	0	0	0
2:Port_02	0	0	0	0
	0	0	0	0
3:Port_03	0	0	0	0
	0	0	0	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（破棄されたパケットも含む）

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 48: DETAIL 指定時

Port	ポート番号とポート名称。ポート名称は最大 16 文字まで表示。
InPkts	受信パケット数
InUcastPkts	受信ユニキャストパケット数
InNUcastPkts	受信ブロードキャストマルチキャストパケット数
InErrors	受信後に破棄したエラーパケット数
OutPkts	送信パケット数
OutUcastPkts	送信ユニキャストパケット数
OutNUcastPkts	送信ブロードキャストマルチキャストパケット数
OutErrors	送信前に破棄したエラーパケット数

表 49: SUMMARY 指定時

例

ポート 1 の統計カウンターを表示する

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

備考・注意事項

エラーパケット受信時は InPkts、InUcastPkts、InErrors の 3 カウンターがカウントされる。

関連コマンド

SET SWITCH PORT (146 ページ)

SHOW SWITCH COUNTER (188 ページ)

SHOW SWITCH PORT (191 ページ)

SHOW SWITCH PORT INTRUSION

カテゴリー：スイッチング / ポート

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

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

解説

ポートセキュリティ機能が有効のとき (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。複数指定が可能。省略時および ALL を指定した場合はすべての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 50:

備考・注意事項

関連コマンド

SET SWITCH PORT SECURITYMODE (152 ページ)

SHOW SWITCH PORT LOOPDETECTION

カテゴリー：スイッチング / ポート

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

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

解説

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

パラメーター

PORT ポート番号または ALL を指定する。省略時は ALL

CONFIG LDF 検出機能の設定情報を表示する

STATUS LDF 検出機能の状態情報を表示する

COUNTER LDF 検出機能のカウンター情報を表示する

入力・出力・画面例

```
# show switch port=16,17 loopdetection config

Switch Loop Detection Configuration
-----
Port ..... 16
Status ..... Disabled
Frame Action ..... LinkDown
Frame Interval ..... 120
Secure Frame ..... On
Blocking Timeout ..... 300 sec

Port ..... 17
Status ..... Enabled
Frame Action ..... LinkDown
Frame Interval ..... 60
Secure Frame ..... On
Blocking Timeout ..... 300 sec

#
# show switch port=16,17 loopdetection status
```


Switch Loop Detection Status				
Port	Loop	Expiry	Port Status	Bcast Status
16	--	--	Enabled	Forward
17	Blocking	4	Disabled(Act)	Forward
#				
# show switch port=16,17 loopdetection counter				
Switch Loop Detection Counter				
Port	Frame Tx	Frame Rx	Action	Frame Rx Discards
16	0	0	0	0
17	709	709	607	0
#				

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

表 51: CONFIG 指定時

Port	ポート番号
Loop	ループ検出状況。Normal (ループ未検出状態)、Detected (ループ検出状態)、Blocking (アクションによりブロッキングされた状態)
Expiry	実行したアクションが実行前の状態に戻るまでに必要な残り時間。アクションにNONEを指定した場合は次のループパケット検出処理を再開するまでの時間。単位は秒
Port Status	該当ポートの状態。Enabled または Disabled。アクションによって Disabled になった場合は (Act)、コマンドによって Disabled になった場合は (User) がそれぞれ表示される。受信レート検出のアクションによって Disabled になった場合も (Act) 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 52: STATUS 指定時

Port	ポート番号
Frame Tx	LDF の送信数
Frame Rx	LDF の受信数
Action	LDF の受信によるアクション (LinkDown または BcastDiscard) が実行された回数
Frame Rx Discards	破棄された LDF の数

表 53: COUNTER 指定時

関連コマンド

DISABLE SWITCH PORT LOOPDETECTION (102 ページ)

ENABLE SWITCH PORT LOOPDETECTION (115 ページ)

RESET SWITCH PORT LOOPDETECTION COUNTER (126 ページ)

SET SWITCH PORT LOOPDETECTION (149 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。複数指定が可能。省略時および ALL を指定した場合はすべての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 54:

備考・注意事項関連コマンド

SET SWITCH PORT SECURITYMODE (152 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。複数指定が可能。省略時および ALL を指定した場合はすべてのポートが対象となる。

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。

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
2		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 55: 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 56: 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 57: COUNTER 指定時

関連コマンド

DISABLE SWITCH PORT STORMDETECTION (103 ページ)

ENABLE SWITCH PORT STORMDETECTION (116 ページ)

RESET SWITCH PORT STORMDETECTION COUNTER (127 ページ)

SET SWITCH PORT STORMDETECTION (154 ページ)

SHOW SWITCH PORT SUMMARY

カテゴリー：スイッチング / ポート

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

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

解説

ポートのステータスを一覧形式で表示する。

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 summary						
Port	Status	Link	Actual	Config	MDI	PVID

1:Port_01	Enabled	Up	100MFull	Autonego	MDI	1
2:Port_02	Enabled	Down	-	Autonego	Auto	1
3:Port_03	Enabled	Up	100MFull	Autonego	MDIX	1
4:Port_04	Enabled	Down	-	Autonego	Auto	1
5:Port_05	Enabled	Up	100MFull	Autonego	MDI	1
6:Port_06	Enabled	Down	-	Autonego	Auto	1
7:Port_07	Enabled	Down	-	Autonego	Auto	1
8:Port_08	Enabled	Down	-	Autonego	Auto	1
9:Port_09	Enabled	Down	-	Autonego	Auto	1
10:Port_10	Enabled	Down	-	Autonego	Auto	1
11:Port_11	Enabled	Down	-	Autonego	Auto	1
12:Port_12	Enabled	Down	-	Autonego	Auto	1
13:Port_13	Enabled	Down	-	Autonego	Auto	1
14:Port_14	Enabled	Down	-	Autonego	Auto	1
15:Port_15	Enabled	Down	-	Autonego	Auto	1
16:Port_16	Enabled	Down	-	Autonego	Auto	1
17:Port_17	Enabled	Down	-	Autonego	Auto	1
18:Port_18	Enabled	Down	-	Autonego	Auto	1
19:Port_19	Enabled	Down	-	Autonego	Auto	1
20:Port_20	Enabled	Down	-	Autonego	Auto	1
21:Port_21	Enabled	Down	-	Autonego	Auto	1
22:Port_22	Enabled	Down	-	Autonego	Auto	1
23:Port_23	Enabled	Up	100MFull	Autonego	MDIX	1
24:Port_24	Enabled	Down	-	Autonego	Auto	1

Port	ポート番号とポート名称。ポート名称は最大 16 文字まで表示
Status	ポートのステータス。「Enabled」、「Disabled」のいずれか
Link	ポートのリンクステータス。「Up」、「Down」のいずれか
Actual	実際の通信モード
Config	通信モードの設定値。「Autonego」、「10MHalf」、「10MFull」、「10MHAUTO」、「10MFAuto」、「100MHalf」、「100MFull」、「100MHAUTO」、「100MFAuto」、「1000MFull」のいずれか
MDI	MDI/MDI-X 状態。「Auto」、「MDI」、「MDI-X」のいずれか。リンクダウン時は Config、リンクアップ時は Actual を表示
PVID	ポートが所属するポートベース VLAN ID

表 58:

関連コマンド

SET SWITCH PORT (146 ページ)

SHOW SWITCH COUNTER (188 ページ)

SHOW SWITCH PORT (191 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 Status	トランクグループの状態。トランクグループの所属ポートが全てリンクダウンしているときは DOWN、1 ポートでもリンクアップして通信可能なときは UP が表示される
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 59:

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 (83 ページ)

CREATE SWITCH TRUNK (86 ページ)

DELETE SWITCH TRUNK (89 ページ)

DESTROY SWITCH TRUNK (91 ページ)

SET SWITCH TRUNK (156 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 ..... 10.0.0.1
Port ..... 80 (2715), 443 (3297)
Proxy Port ..... 8080 (3880)
Listen Port ..... Open
SSL Security ..... Disabled
SSL Key ID ..... none
Proxy Server .....
Redirect URL .....
Header .....
Sub Header Top .....
Sub Header Bottom.....
Footer .....
HTTP Redirect ..... Disabled
Session Keep ..... Disabled
Ping Poll ..... Disabled
Normal Interval ..... 30
Timeout ..... 1
Fail Count ..... 5
Reauth Refresh ..... Disabled
Temporary IP ..... Enabled
Temporary IP Renewal Time ..... 8
Temporary IP Rebinding Time ..... 11
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
Proxy Port	プロキシサーバーの 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
Proxy Server	プロキシサーバーの IP アドレスもしくはホスト名
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
HTTP Redirect	HTTP リダイレクト機能の有効・無効。Enabled または Disabled
Session Keep	セッションキープ機能の有効・無効。Enabled または Disabled
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 60:

関連コマンド

DISABLE WEBAUTHSERVER (104 ページ)

ENABLE WEBAUTHSERVER (117 ページ)

PURGE WEBAUTHSERVER (120 ページ)

SET WEBAUTHSERVER (157 ページ)

SHOW PORTAUTH (172 ページ)

SHOW PORTAUTH PORT (178 ページ)