

ポート認証

| | |
|------------------------------------|----|
| 概要・基本設定 | 3 |
| 概要 | 3 |
| 認証方式 | 4 |
| 認証サーバーの設定 | 5 |
| 802.1X 認証方式 | 6 |
| 基本設定 | 6 |
| Supplicant として使用する際の設定例 | 7 |
| MAC ベース認証方式 | 8 |
| 基本設定 | 8 |
| Web 認証方式 | 9 |
| 基本設定 | 10 |
| Web 認証画面 | 12 |
| エラーメッセージについて | 15 |
| 認証用 DHCP サーバー機能を Web 認証で使用する場合 | 15 |
| ダイナミック VLAN | 18 |
| ゲスト VLAN | 21 |
| Supplicant MAC 透過機能 | 22 |
| コマンドリファレンス編 | 24 |
| 機能別コマンド索引 | 24 |
| ADD PORTAUTH PORT SUPPLICANTMAC | 25 |
| DELETE PORTAUTH PORT SUPPLICANTMAC | 27 |
| DISABLE PORTAUTH | 28 |
| DISABLE PORTAUTH PORT LOGTYPE | 29 |
| DISABLE WEBAUTHSERVER | 30 |
| ENABLE PORTAUTH | 31 |
| ENABLE PORTAUTH PORT LOGTYPE | 32 |
| ENABLE WEBAUTHSERVER | 33 |
| SET PORTAUTH AUTHMETHOD | 34 |
| SET PORTAUTH CSIDFORMAT | 35 |
| SET PORTAUTH DHCPSEVER | 37 |
| SET PORTAUTH PORT | 38 |
| SET PORTAUTH PORT SUPPLICANTMAC | 43 |
| SET PORTAUTH USERIDFORMAT | 45 |
| SET WEBAUTHSERVER | 47 |

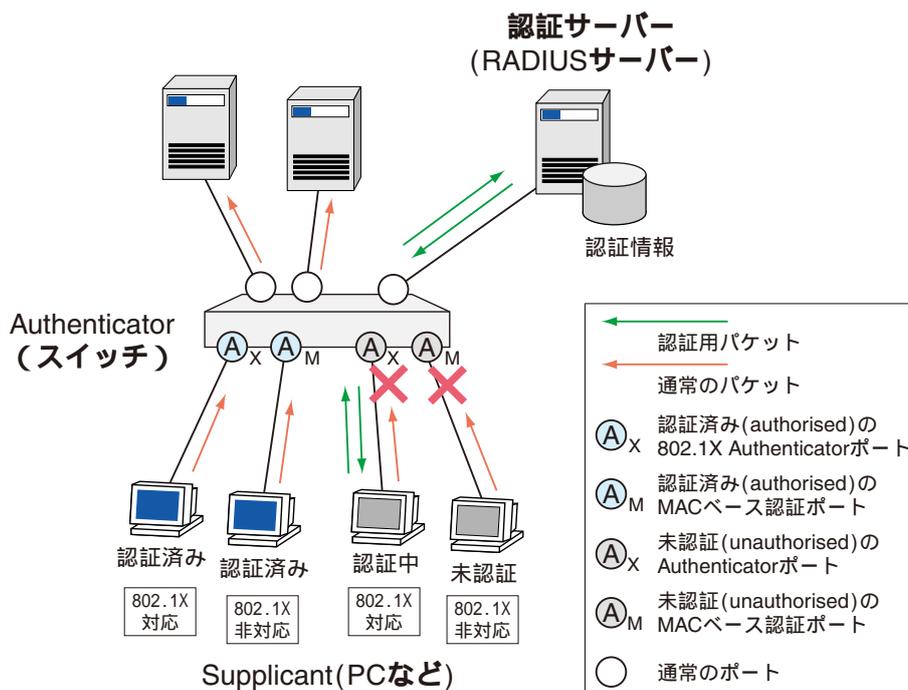
| | |
|--|----|
| SHOW PORTAUTH | 49 |
| SHOW PORTAUTH PORT AUTHENTICATOR | 54 |
| SHOW PORTAUTH PORT SUPPLICANT | 60 |
| SHOW WEBAUTHSERVER | 63 |

概要・基本設定

ここでは、ポート認証機能について、コマンドラインインターフェースによる設定方法を中心に説明します。なお、ここでの設定の一部は、Web GUIでは「セキュリティ設定」の「RADIUS サーバー」、「認証用 WEB サーバー」、「ポート認証」で設定できます。（詳細は「Web GUI」/「セキュリティ設定」をご覧ください。）

概要

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。ポート認証のシステムは、下記の 3 要素から成り立っています。



- Authenticator (認証者): ポートに接続してきた Supplicant (クライアント) を認証する機器またはソフトウェア。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。

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。

- ✧ ポート認証有効の場合、EAP 透過機能は使用できません。
- ✧ Authenticator ポートと Supplicant ポートは、ミラーポートに設定することはできません。
- ✧ Authenticator ポートと Supplicant ポートではスパニングツリープロトコルは使用できません。
- ✧ Authenticator ポートと Supplicant ポートは、トランクグループに所属させることはできません。
- ✧ コンポポート、ポートセキュリティ有効ポートは、Authenticator ポートに設定することはできません。
- ✧ Authenticator ポートにはスタティックエントリは追加できません。
- ✧ Supplicant ポートをタグ付きに設定することはできません。
- ✧ Authenticator ポートをタグ付きに設定する場合は、Multi-Supplicant モード (MODE=MULTI) で、かつダイナミック VLAN 無効 (VLANASSIGNMENT=DISABLED) である必要があります。
- ✧ Supplicant MAC 透過機能とタグ付きポートとの併用はサポート対象外です。
- ✧ 802.1X 認証でゲスト VLAN を設定した場合、認証に失敗した場合にも EAP-Success パケットを送信します

認証方式

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。

- 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 認証を受けるためには、Supplicant 上に対応 Web ブラウザーが必要。

本製品では、同一ポート上に複数の認証方式を設定することもできます (同一ポート上に 802.1X 認証、MAC ベース認証、Web 認証を設定可能)。認証方式を併用した場合は、最初に MAC ベース認証を実施し、次に 802.1X 認証と Web 認証で先に開始された方式を実施します。再認証を行う際は認証に成功した方式で実施します。

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 1:

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留意し、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留意し、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 2:

認証方式は、PAP を指定します。

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

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

表 3:

認証方式は、PAP を指定します。

- ダイナミック VLAN (後述) を使用するとき、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 4:

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

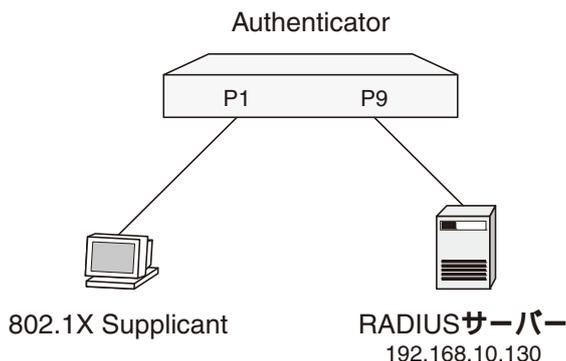
本製品を使ってポート認証のシステムを運用するための基本的な設定例を示します。

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 などが接続されているものとして扱います。

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 default (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 5:

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 IPADDRESS=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（38 ページ）で「PORTAUTH=8021X TYPE=AUTHENTICATOR」を指定することにより、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 ↵
```

- ※ 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（38 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 としての動作には IP の設定が必須です。

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 (38 ページ) で「TYPE=SUPPLICANT」を指定することにより、ポート 1 は Supplicant ポートとなります。

```
SET PORTAUTH PORT=1 TYPE=SUPPLICANT USERNAME=user1 PASSWORD=himitsu ↓
```

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

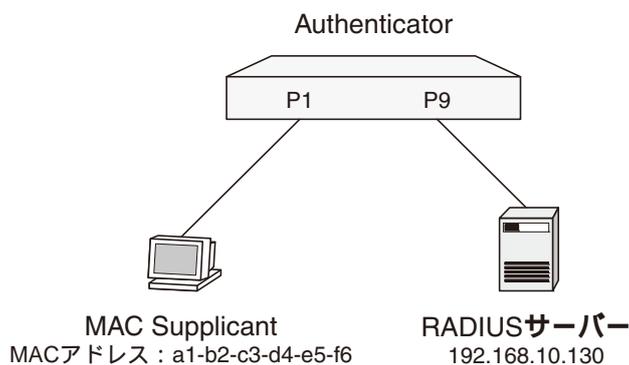
本製品を Authenticator とし、MAC ベース認証を行う場合の基本設定を示します。

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 default (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 6:

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 IPADDRESS=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 (38 ページ) で「PORTAUTH=MACBASED TYPE=AUTHENTICATOR」を指定することにより、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 ↓
```

- ※ 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 (38 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。

OS ごとの対応ブラウザ、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 (Windows/Mac) Firefox 3.0.6 (Windows) Firefox 3.0.1 (Mac) Firefox 2.0 (Linux/Unix) Safari 2.0.4 (Mac) Opera 9.6.3 (Windows/Linux) Opera 9.60 Beta (Mac) Opera 9.0 (Unix) Netscape 9.0.0.6 (Linux) |
| 対応プロトコル | HTTP 1.0/1.1 |

表 7:

Supplicant から Web 認証を行う場合は、以下のように操作します。

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 (本製品の IP アドレス) と TCP ポート番号 (デ

- フォルトは 8080 番) を入力し (入力例: http://192.168.1.1:8080/) 「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、「ログイン」をクリックします。

The screenshot shows a web browser window displaying the login page of a Web Access Authentication Gateway. The page has a yellow header with the Allied-Telesis logo and the title 'Web Access Authentication Gateway'. A central white box contains the login form with the following elements:

- Title: ユーザー認証 (User Authentication)
- Field: ユーザー名 (Username)
- Field: パスワード (Password)
- Buttons: ログイン (Login) and リセット (Reset)

The footer of the page includes the Allied Telesis logo and the text: Copyright©2009 Allied Telesis Holdings K.K. All Rights Reserved.

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。

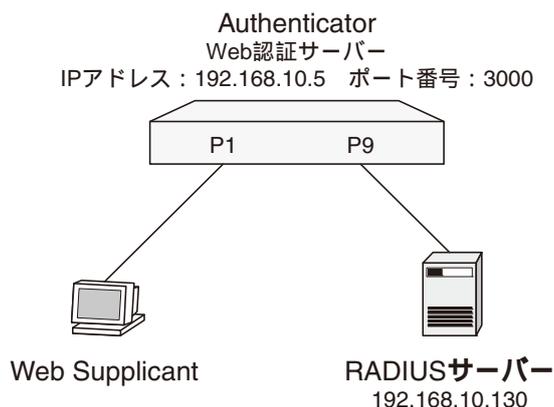
Authenticator としての動作には、IP の設定と RADIUS サーバーの指定が必須です。

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://192.168.10.5:3000」にアクセスするものとします。

Web Supplicant には、IP アドレスの設定が必要です。

Web Supplicant から認証情報として、「ユーザー名:webuserA」/「パスワード:webpasswordA」が入力され、認証に成功すると、Web Supplicant は、VLAN default (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

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。
IP アドレスの設定により、Web Supplicant は本製品の Web 認証サーバーにアクセスできるようになります。

```
ADD IP IPADDRESS=192.168.10.5 MASK=255.255.255.0 ↵
```

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

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

3. ポート認証機能を有効にします。

```
ENABLE PORTAUTH ↵
```

4. ポート 1 で Web 認証を行うよう設定します。SET PORTAUTH PORT コマンド（38 ページ）で「PORTAUTH=WEBBASED TYPE=AUTHENTICATOR」を指定することにより、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 ↵
```

5. Web 認証サーバーの TCP ポート番号を変更します。

```
SET WEBAUTHSERVER PORT=3000 ↵
```

- Web 認証サーバー用の TCP ポート番号は、Web GUI で使用する HTTP サーバー用の TCP ポート番号 (SET HTTP LISTENPORT コマンド (「運用・管理」の 130 ページ) で設定) とは別に設定します。デフォルトは 8080 番です。

6. Web 認証サーバーを有効にします。

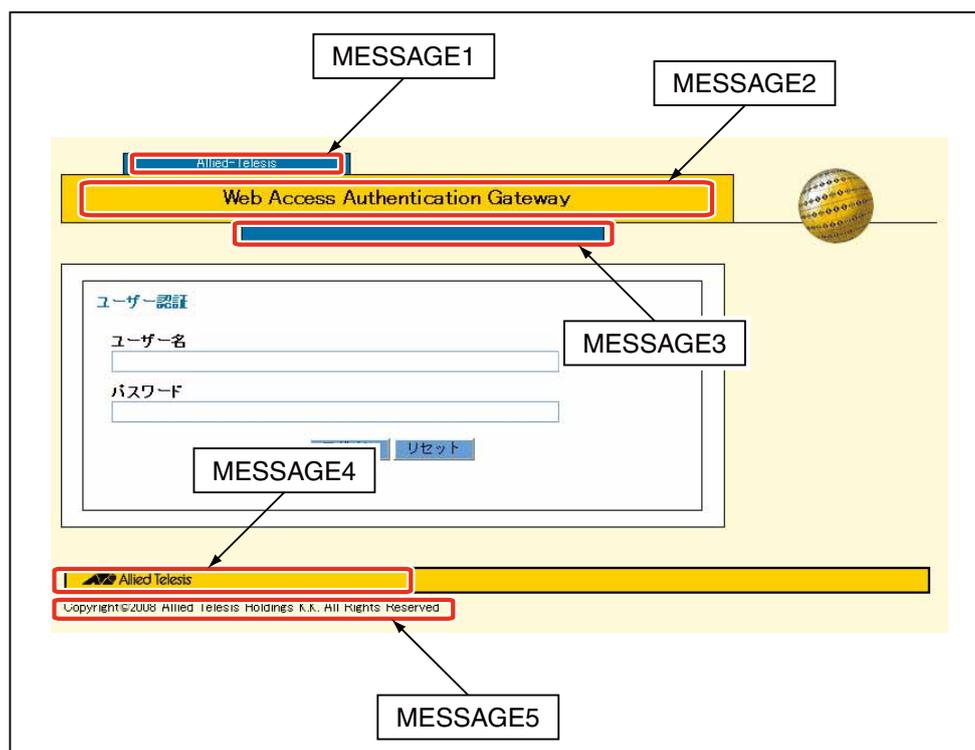
```
ENABLE WEBAUTHSERVER ↓
```

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

Web 認証画面

Supplicant 上の Web ブラウザーに表示される画面・メッセージを紹介します。

- 画面に表示される一部の文字列は、SET WEBAUTHSERVER コマンド (47 ページ) の MESSAGE1 ~ MESSAGE5 のパラメーターで変更可能です。

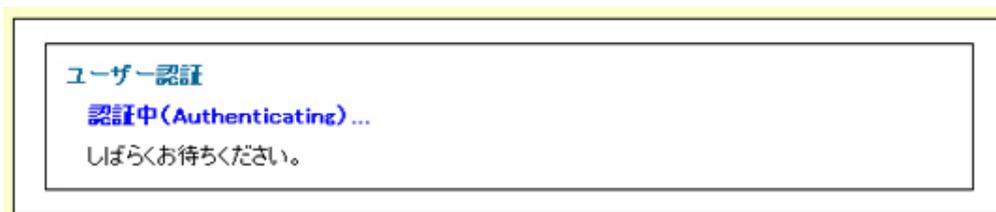


- Web GUI から設定すると、文字列に全角文字 (日本語) を使用することができます (CLI からは半角英数字のみ。使用可能文字についての詳細は、SET WEBAUTHSERVER コマンド (47 ページ) をご覧ください)。

- 認証成功後、指定したページに自動的にジャンプさせるには、SET WEBAUTHSERVER コマンド (47 ページ) の REDIRECTURL パラメーターでリダイレクト URL を指定します。

認証中

認証中は、次の画面が表示されます。



メッセージ内容：

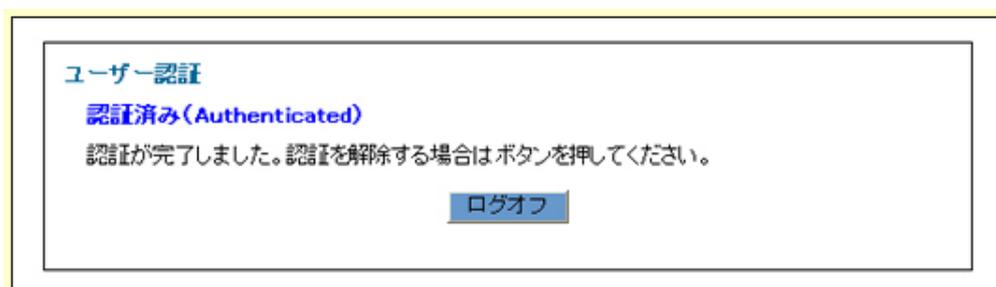
認証中 (Authenticating) ...
しばらくお待ちください。

認証成功

認証に成功すると、次の画面が表示されます。すでに認証済みの Supplicant からアクセスを受けた場合も、次の画面が表示されます。

この画面で「ログオフ」をクリックすると、認証が解除されます。

- 「Enter」キーを押しただけではログオフできません。認証を解除する場合は「ログオフ」ボタンをクリックしてください。



メッセージ内容：

認証済み (Authenticated)
認証が完了しました。
認証を解除する場合はボタンを押してください。

認証失敗

認証に失敗すると、次の画面が表示されます。

The screenshot shows a web form titled "ユーザー認証" (User Authentication). It contains two input fields: "ユーザー名" (Username) and "パスワード" (Password). Below the fields are two buttons: "ログイン" (Login) and "リセット" (Reset). A red error message at the bottom reads: "ログインできません。しばらく経ってから再度ログインしてください。" (Cannot login. Please try logging in again after a short wait).

メッセージ内容：

ログインできません。しばらく経ってから再度ログインしてください。

認証失敗 (Held)

規定回数のログイン失敗により Held の状態 (待機中) になると、次の画面が表示されます。

The screenshot shows the same web form as above, but with the title "ユーザー認証" followed by "待機中(Held)" (Waiting (Held)). The input fields and buttons remain the same. The red error message at the bottom is identical: "ログインできません。しばらく経ってから再度ログインしてください。"

メッセージ内容：

待機中 (Held)

ログインできません。しばらく経ってから再度ログインしてください。

Web 認証画面が表示されない例

以下のような場合には、Web 認証画面は表示されません。

- Web 認証サーバーが無効のとき (DISABLE WEBAUTHSERVER コマンド (30 ページ))
- ポート認証が無効のとき (DISABLE PORTAUTH コマンド (28 ページ))
- 認証方式に Web 認証 (PORTAUTH=WEBBASED、PORTAUTH=AUTO) が指定されていないとき
- Authenticator ポートが CONTROL=AUTHORISED (認証済み固定) に設定されているとき

- Authenticator ポートが CONTROL=UNAUTHORISED (未認証固定) に設定されているとき
- Supplicant MAC 透過アドレスとして登録されている MAC アドレスを持つ Supplicant からアクセスされたとき、Supplicant の接続ポートが登録されているポートと同じ場合には、認証済み Supplicant として強制的に通信可能にし、異なる場合には未認証 Supplicant として認証要求を強制的に拒否する。

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 |
|---|---|
| ログインできません。ユーザー名、パスワードに誤りがあります。 | ユーザー名、パスワードに空白しか入力されていない |
| ログインできません。同時接続数の最大を超えているか、本端末は認証できない可能性があります。 | 同時接続数が最大数(1ポートあたり 320、システムあたり 480) に達している。 Supplicant の MAC アドレスが FDB にスタティックエントリーとして登録されている |
| ログインできません。サーバーが見つかりません。 | 認証処理がタイムアウトしている RADIUS サーバーとの通信に失敗した |
| ログインできません。ユーザー名、パスワードを確認してください。 | RADIUS サーバーで認証に失敗した |
| ログインできません。しばらく経ってから再度ログインしてください。 | Held の状態 (待機中) になっている 別の Supplicant が認証中 |

表 9:

認証用 DHCP サーバー機能を Web 認証で使用する場合

本製品は認証用 DHCP サーバー機能を搭載しているため、Web 認証利用時に認証前の Supplicant に IP アドレスを割り振ることができます。

ここでは、Supplicant に動的に IP アドレスが割り当てられる環境で Web 認証を使用するための設定方法を説明します。

- ◁ ゲスト VLAN とダイナミック VLAN についての詳細は、後述の「ゲスト VLAN」、「ダイナミック VLAN」をご覧ください。

Supplicant が通信可能になるまでの動作

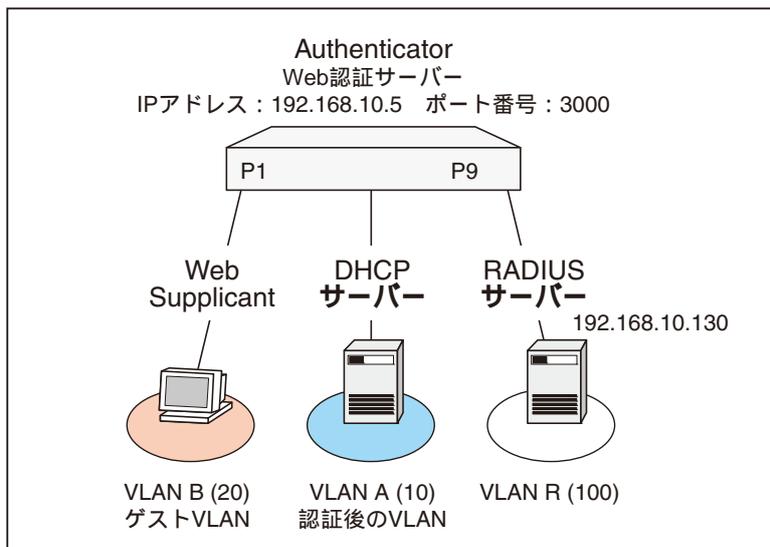
1. DHCP クライアント機能が有効になっている Supplicant が Authenticator に接続。
2. Web 認証が有効なポートでは、Supplicant が未認証の場合、ゲスト VLAN の所属になる。本製品の DHCP サーバー機能によって、Supplicant に IP アドレスが割り当てられる。

3. Supplicant は Web ブラウザーから Authenticator (Web 認証サーバー) にアクセス。ユーザー ID とパスワードの入力により、RADIUS サーバーとの認証処理が開始される。
4. Supplicant の認証が成功すると、認証後の VLAN の所属になる。
5. ゲスト VLAN 内の DHCP サーバーから割り当てられた IP アドレスが解放され、認証後の VLAN 内に存在する DHCP サーバーによって、新たに IP アドレスが割り当てられる。
6. Supplicant は、認証後の VLAN で通信が可能になる。

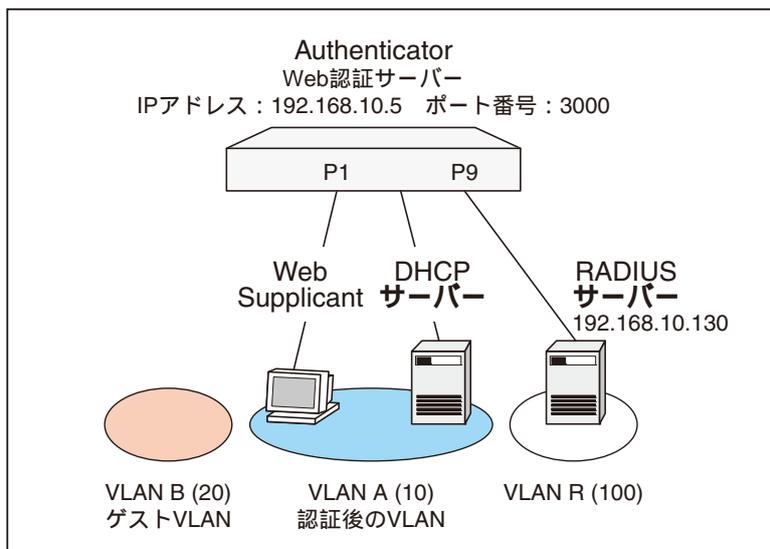
REAUTHENABLED=ENABLED (認証切断を行う) が設定されている場合は、REAUTHPERIOD パラメーターで指定された時間が経過すると認証が切断されます。この場合、上記 2 に戻り、Supplicant は再びゲスト VLAN の所属になります。

構成

認証前の所属VLAN (VLAN B)



認証後の所属VLAN (VLAN A)



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 10:

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 ↓
CREATE VLAN=R VID=100 ↓
```

2. RADIUS サーバーを接続するポート9を VLAN「R」に割り当てます。

```
ADD VLAN=R PORT=9 ↓
```

3. RADIUS サーバーを使って認証を行うため、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=R IPADDRESS=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の認証設定を以下のようにします。SET PORTAUTH PORT コマンド(38 ページ)で「PORTAUTH=AUTO」を指定することにより、ポート1でいったん MAC 認証を実施させ、失敗させることでゲスト VLAN の所属になるようにします。「GUESTVLAN=20」の指定により、VLAN「B」がゲスト VLAN になります。

```
SET PORTAUTH=AUTO PORT=1 TYPE=AUTHENTICATOR MODE=MULTI GUESTVLAN=20
VLANASSIGNMENT=ENABLED VLANASSIGNMENTTYPE=USER ↓
```

7. Web 認証サーバーの TCP ポート番号を変更します。

```
SET WEBAUTHSERVER PORT=3000 ↓
```

※ Web 認証サーバー用の TCP ポート番号は、Web GUI で使用する HTTP サーバー用の TCP ポート番号 (SET HTTP LISTENPORT コマンド(「運用・管理」の130 ページ)で設定)とは別に設定します。デフォルトは8080番です。

8. Web 認証サーバーを有効にします。

```
ENABLE WEBAUTHSERVER ↓
```

9. 認証用 DHCP サーバー機能を有効にします。

```
SET PORTAUTH DHCPSEVER=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(38 ページ)の TYPE パラメーターを NONE に設定してください。

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、またはユーザーの所属 VLAN を動的に変更する機能です。

SET PORTAUTH PORT コマンド (38 ページ) の VLANASSIGNMENT パラメーターに ENABLED を指定することにより、有効にします。ダイナミック VLAN をポート単位で設定するか、ユーザー (MAC アドレス) 単位で設定するかを SET PORTAUTH PORT コマンド (38 ページ) の VLANASSIGNMENTTYPE パラメーターで設定します。

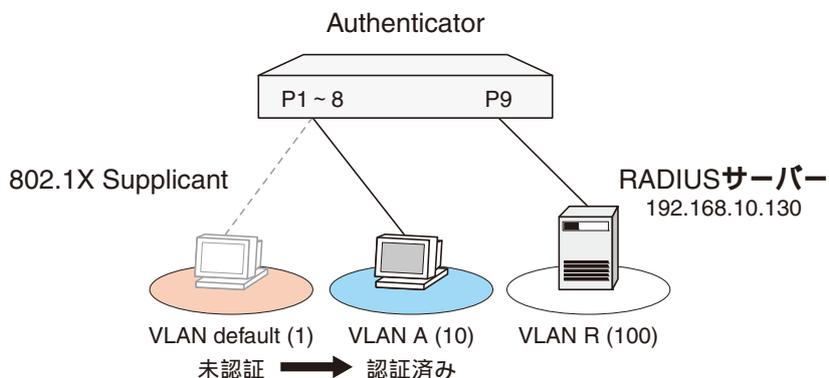
以下、本製品を Authenticator として使用し、さらにダイナミック VLAN 機能を利用する場合の基本設定を示します。Authenticator としての動作には、IP の設定と RADIUS サーバーの指定が必須です。

利用者機器のために VLAN 「A」を用意します。また、RADIUS サーバーを接続するための VLAN 「R」も作成します。各ポートに接続された機器は、認証成功後、RADIUS サーバー側から返された VLAN 「A」に自動的にアサインされます。

ここでは、ポート 1~8 で 802.1X 認証を行うものとします (ポート 1~8 の認証前の所属 VLAN は VLAN default と仮定します)。また、RADIUS サーバーは、VLAN 「R」所属のポート 9 (通常のポート) に接続されているものとします。

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

構成



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

| User-Name | User-Password | 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 11:

設定

1. VLAN を作成します。

```
CREATE VLAN=A VID=10 ↓
CREATE VLAN=R VID=100 ↓
```

2. RADIUS サーバーを接続するポート 9 を VLAN 「R」 に割り当てます。

```
ADD VLAN=R PORT=9 ↓
```

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

```
ADD IP INT=R IPADDRESS=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 1～8 で 802.1X 認証を行うよう設定します。SET PORTAUTH PORT コマンド (38 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=1-8 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 (38 ページ) の TYPE パラメーターを NONE に設定してください。

ダイナミック VLAN の動作仕様は次のとおりです。

- Supplicant の認証に失敗した場合、ポートは本来の VLAN (ADD VLAN PORT コマンド (「バッチャル LAN」の 12 ページ) で指定した VLAN) の所属となります。ポート越えの通信は不可能です。
- RADIUS サーバーから有効な VLAN の情報が返ってきた場合、ポートはその VLAN の所属となります。認証に成功すれば、ポート越えの通信も可能です。
- RADIUS サーバーから無効な VLAN の情報が返ってきた場合、ポートは本来の VLAN 所属となります。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 VLAN の情報が返ってこなかった場合、ポートは本来の VLAN 所属となり

ます。認証に成功すれば、ポート越えの通信も可能です。

- 該当ポートまたはシステム全体でポート認証が無効に設定された場合、ポートは本来の VLAN 所属となります。ポート認証が無効なので、ポート越えの通信に関する制限はありません。
- 未認証のポート、および、CONTROL=UNAUTHORISED(未認証固定)またはCONTROL=AUTHORISED(認証済み固定)に設定されたポートは、本来の VLAN 所属となります。

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

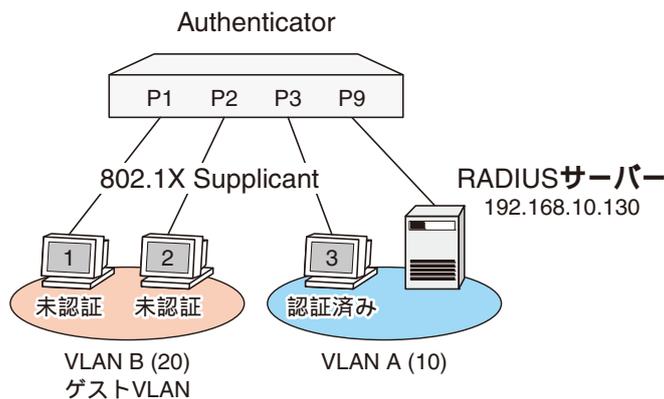
- 認証済みの Supplicant がなくなったとき。
- リンクがダウンしたとき。
- ポート認証が無効にされたとき (DISABLE PORTAUTH コマンド (28 ページ))。

ゲスト VLAN

ゲスト VLAN は、未認証時にのみ割り当てられる、同一 VLAN 内での通信が可能な VLAN です。ゲスト VLAN を設定していない場合、未認証の状態ではたとえ同一 VLAN 所属のポート間であっても通信できませんが、これらのポートに対して同じゲスト VLAN を設定しておけば、未認証状態でもゲスト VLAN 内にかぎって通信が可能になります。なお、認証にパスした後は、ゲスト VLAN ではなくポート本来の VLAN、あるいは、ダイナミック VLAN によって割り当てられた VLAN の所属となります。以下の設定では、認証前および、認証失敗した 802.1X Supplicant は、VLAN「B」に所属しています。認証が成功すると、VLAN「A」で通信が可能です。

- ◇ 以下の例では、802.1X 認証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。ただし、802.1X 認証以外は、VLANASSIGNMENTTYPE=USER のみ使用可能です。

構成



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

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

表 12:

設定

1. VLAN を作成します。

```
CREATE VLAN=A VID=10 ↓
```

```
CREATE VLAN=B VID=20 ↓
```

2. RADIUS サーバーを接続するポート 9 を VLAN 「A」に割り当てます。

```
ADD VLAN=A PORT=9 ↓
```

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

```
ADD IP INT=A IPADDRESS=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 1~3 で 802.1X 認証を行うよう設定します。SET PORTAUTH PORT コマンド (38 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、「GUESTVLAN=20」の指定により、VLAN 「B」がゲスト VLAN になります。

```
SET PORTAUTH=8021X PORT=1-3 TYPE=AUTHENTICATOR MODE=SINGLE  
GUESTVLAN=20 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 (38 ページ) の TYPE パラメーターを NONE に設定してください。

Supplicant MAC 透過機能

本製品は、特定の MAC アドレスを送信元アドレスに持つフレームのみを常に認証済みの Supplicant として通信可能にする Supplicant MAC 透過機能にも対応しています。

Supplicant MAC 透過アドレスを登録する場合は、SET PORTAUTH PORT SUPPLICANTMAC コマ

ンド (43 ページ) を使います。

```
SET PORTAUTH PORT=5 SUPPLICANTMAC=00-00-F4-11-11-11 CONTROL=AUTHORISED ↵
```

登録済みの Supplicant MAC 透過アドレスを削除する場合は、DELETE PORTAUTH PORT SUPPLICANTMAC コマンド (27 ページ) を使います。

```
DELETE PORTAUTH PORT=5 SUPPLICANTMAC=00-00-F4-11-11-11 ↵
```

コマンドリファレンス編

機能別コマンド索引

概要・基本設定

| | |
|--|----|
| ADD PORTAUTH PORT SUPPLICANTMAC | 25 |
| DELETE PORTAUTH PORT SUPPLICANTMAC | 27 |
| DISABLE PORTAUTH | 28 |
| DISABLE PORTAUTH PORT LOGTYPE | 29 |
| DISABLE WEBAUTHSERVER | 30 |
| ENABLE PORTAUTH | 31 |
| ENABLE PORTAUTH PORT LOGTYPE | 32 |
| ENABLE WEBAUTHSERVER | 33 |
| SET PORTAUTH AUTHMETHOD | 34 |
| SET PORTAUTH CSIDFORMAT | 35 |
| SET PORTAUTH DHCPSEVER | 37 |
| SET PORTAUTH PORT | 38 |
| SET PORTAUTH PORT SUPPLICANTMAC | 43 |
| SET PORTAUTH USERIDFORMAT | 45 |
| SET WEBAUTHSERVER | 47 |
| SHOW PORTAUTH | 49 |
| SHOW PORTAUTH PORT AUTHENTICATOR | 54 |
| SHOW PORTAUTH PORT SUPPLICANT | 60 |
| SHOW WEBAUTHSERVER | 63 |

ADD PORTAUTH PORT SUPPLICANTMAC

カテゴリ：ポート認証

ADD PORTAUTH PORT=port-number SUPPLICANTMAC=macadd [CONTROL=AUTHORISED]

port-number: スイッチポート番号 (1~。単一ポートのみ指定可)

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

解説

Supplicant MAC 透過アドレスを登録する。Supplicant MAC 透過アドレスは、Single-Supplicant モード、Multi-Supplicant モードのどちらの場合も 1 ポートに対して 10 個まで登録できる。

SET PORTAUTH PORT SUPPLICANTMAC コマンドは同義

パラメーター

PORT 対象となるポート番号。複数ポートを指定することはできない

SUPPLICANTMAC Supplicant MAC 透過アドレスとして登録する MAC アドレス。ブロードキャスト、マルチキャストアドレスは設定できない

CONTROL 手動設定による Authenticator ポートの状態。AUTHORISED (認証済み固定) のみを指定可能

入力・出力・画面例

```
Manager > add portauth port=1 supplicantmac=00-00-f4-11-11-11 control=authorised
Operation successful.
```

例

Supplicant MAC 透過アドレスを追加する

```
ADD PORTAUTH PORT=1 SUPPLICANTMAC=00-00-f4-11-11-11 CONTROL=AUTHORISED
```

備考・注意事項

ポート認証設定において、TYPE が AUTHENTICATOR、かつ、CONTROL が AUTO に指定されているポートに対して、Supplicant MAC 透過アドレスを登録できる。

ポート認証が有効に設定されていないポートに対して実行した場合、指定された MAC アドレスは本製品の設定にのみ登録され、FDB には登録されない。

すでに FDB にスタティックエントリとして登録されているアドレス、他ポートで認証済みの Supplicant の MAC アドレスは、Supplicant MAC 透過アドレスに登録できない。

ポート認証設定において TYPE を AUTHENTICATOR 以外に変更した場合、または、CONTROL を AUTO 以外に変更した場合、すでに登録されている MAC アドレスは設定および FDB から削除される。

本コマンドで登録した MAC アドレスを違う VLAN でダイナミックエントリとして登録すると設定したエージングタイムと関係なく、約 30 秒で削除される。

関連コマンド

DELETE PORTAUTH PORT SUPPLICANTMAC (27 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (43 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR (54 ページ)

DELETE PORTAUTH PORT SUPPLICANTMAC

カテゴリー：ポート認証

DELETE PORTAUTH PORT=*port-number* [SUPPLICANTMAC=*macadd*]

port-number: スイッチポート番号 (1~。単一ポートのみ指定可)

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

解説

Supplicant MAC 透過アドレスを削除する

パラメーター

PORT スイッチポート番号。複数ポートを指定することはできない

SUPPLICANTMAC 削除する Supplicant MAC 透過アドレス。省略した場合は指定ポートに登録されている全 Supplicant MAC 透過アドレスを削除する

入力・出力・画面例

```
Manager > delete portauth port=1 supplicantmac=00-00-f4-11-11-11
Operation successful
```

例

登録されている Supplicant MAC 透過アドレスを削除する

```
DELETE PORTAUTH PORT=1 SUPPLICANTMAC=00-00-f4-11-11-11
```

関連コマンド

ADD PORTAUTH PORT SUPPLICANTMAC (25 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (43 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR (54 ページ)

DISABLE PORTAUTH

カテゴリ：ポート認証

DISABLE PORTAUTH

解説

ポート認証モジュールを無効にする。デフォルトは無効

入力・出力・画面例

```
Manager > disable portauth  
  
Operation successful
```

例

ポート認証機能を無効にする

DISABLE PORTAUTH

関連コマンド

ENABLE PORTAUTH (31 ページ)

SET PORTAUTH AUTHMETHOD (34 ページ)

SET PORTAUTH PORT (38 ページ)

SHOW PORTAUTH (49 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR (54 ページ)

SHOW PORTAUTH PORT SUPPLICANT (60 ページ)

DISABLE PORTAUTH PORT LOGTYPE

カテゴリー：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。指定した認証方式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 認証方法。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 対象となるスイッチポート番号または ALL。ALL を指定した場合はすべてのスイッチポートが対象となる

LOGTYPE ログタイプ。SUCCESS (認証成功)、FAILURE (認証失敗)、LOGOFF (ログオフ)、ALL (全て) のいずれかを指定する。デフォルトは ALL。カンマ [,] を使った複数指定も可能

入力・出力・画面例

```
Manager > disable portauth=all port=1-5 logtype=all
Operation successful.
```

例

認証ログ機能を無効にする

```
DISABLE PORTAUTH=ALL PORT=1-5 LOGTYPE=ALL
```

関連コマンド

ENABLE PORTAUTH PORT LOGTYPE (32 ページ)

SHOW PORTAUTH (49 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR (54 ページ)

DISABLE WEBAUTHSERVER

カテゴリ：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

入力・出力・画面例

```
Manager > disable webauthserver  
  
Operation successful.
```

例

Web 認証サーバーを無効にする。

DISABLE WEBAUTHSERVER

関連コマンド

ENABLE WEBAUTHSERVER (33 ページ)

SET PORTAUTH AUTHMETHOD (34 ページ)

SET PORTAUTH PORT (38 ページ)

SET WEBAUTHSERVER (47 ページ)

SHOW PORTAUTH (49 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR (54 ページ)

SHOW PORTAUTH PORT SUPPLICANT (60 ページ)

SHOW WEBAUTHSERVER (63 ページ)

ENABLE PORTAUTH

カテゴリー：ポート認証

ENABLE PORTAUTH

解説

ポート認証モジュールを有効にする。デフォルトは無効

入力・出力・画面例

```
Manager > enable portauth  
  
Operation successful.
```

例

ポート認証機能を有効にする

ENABLE PORTAUTH

備考・注意事項

Authenticator ポートと Supplicant ポートではスパニングツリープロトコル、ポートセキュリティは使用できない。

Authenticator ポートと Supplicant ポートはトランクグループに所属することはできない。

Authenticator ポートと Supplicant ポートはミラーポートに設定できない。

ポート認証有効の場合、EAP 透過機能は使用できない。

Combo ポートはポート認証の Authenticator ポートに設定することはできない。

Authenticator ポートにはスタティックエントリは追加できない。

関連コマンド

DISABLE PORTAUTH (28 ページ)

SET PORTAUTH AUTHMETHOD (34 ページ)

SET PORTAUTH PORT (38 ページ)

SHOW PORTAUTH (49 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR (54 ページ)

SHOW PORTAUTH PORT SUPPLICANT (60 ページ)

ENABLE PORTAUTH PORT LOGTYPE

カテゴリ：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。指定した認証方式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 認証方法。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 対象となるスイッチポート番号または ALL。ALL を指定した場合はすべてのスイッチポートが対象となる

LOGTYPE ログタイプ。SUCCESS (認証成功)、FAILURE (認証失敗)、LOGOFF (ログオフ)、ALL (全て) のいずれかを指定する。デフォルトは ALL。カンマ [,] を使った複数指定も可能

入力・出力・画面例

```
Manager > enable portauth=all port=1-5 logtype=all
Operation successful.
```

例

認証ログ機能を有効にする

```
ENABLE PORTAUTH=ALL PORT=1-5 LOGTYPE=ALL
```

関連コマンド

DISABLE PORTAUTH PORT LOGTYPE (29 ページ)

SHOW PORTAUTH (49 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR (54 ページ)

ENABLE WEBAUTHSERVER

カテゴリ：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

入力・出力・画面例

```
Manager > enable webauthserver  
  
Operation successful.
```

例

Web 認証サーバーを有効にする。

ENABLE WEBAUTHSERVER

関連コマンド

DISABLE WEBAUTHSERVER (30 ページ)
SET PORTAUTH AUTHMETHOD (34 ページ)
SET PORTAUTH PORT (38 ページ)
SET WEBAUTHSERVER (47 ページ)
SHOW PORTAUTH (49 ページ)
SHOW PORTAUTH PORT AUTHENTICATOR (54 ページ)
SHOW PORTAUTH PORT SUPPLICANT (60 ページ)
SHOW WEBAUTHSERVER (63 ページ)

SET PORTAUTH AUTHMETHOD

カテゴリ：ポート認証

SET PORTAUTH AUTHMETHOD=RADIUSEAP

解説

ポート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 RadiusEAP のみ

入力・出力・画面例

```
Manager > set portauth authmethod=radiusseap

Operation successful.
```

例

認証プロトコルを RadiusEAP に設定する

SET PORTAUTH AUTHMETHOD=RADIUSEAP

関連コマンド

DISABLE PORTAUTH (28 ページ)

ENABLE PORTAUTH (31 ページ)

SET PORTAUTH PORT (38 ページ)

SHOW PORTAUTH (49 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR (54 ページ)

SHOW PORTAUTH PORT SUPPLICANT (60 ページ)

SET PORTAUTH CSIDFORMAT

カテゴリ：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 および 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。

入力・出力・画面例

```
Manager > set portauth csidformat separator=period

Operation successful.
```

| 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 |
| XX.XX.XX.XX.XX.XX | Period | 2 | TRUE |
| xx.xx.xx.xx.xx.xx | Period | 2 | FALSE |
| XXXX-XXXX-XXXX | Hyphen | 4 | TRUE |
| xxxx-xxxx-xxxx | Hyphen | 4 | FALSE |
| XXXX:XXXX:XXXX | Colon | 4 | TRUE |
| xxxx:xxxx:xxxx | Colon | 4 | FALSE |
| XXXX.XXXX.XXXX | Period | 4 | TRUE |
| xxxx.xxxx.xxxx | Period | 4 | FALSE |

| | | | |
|--------------|------|---|-------|
| XXXXXXXXXXXX | None | - | TRUE |
| xxxxxxxxxxxx | None | - | FALSE |

表 13: 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 (49 ページ)

SET PORTAUTH DHCPSEVER

カテゴリー：ポート認証

SET PORTAUTH DHCPSEVER=[{ENABLED|DISABLED}] [LEASETIME=10..86400]

解説

認証用 DHCP サーバーの有効/無効、およびオプション設定をする。

本機能が有効な場合、未認証 Supplicant からの DHCP パケットのみを DHCP サーバーで受信する。

パラメーター

DHCPSEVER 認証用 DHCP サーバー機能の有効/無効を設定する。デフォルトは無効。省略時は、現在の設定を引き継ぐ。

LEASETIME IP アドレスのリース時間を指定する (秒)。デフォルトは 20 秒。

入力・出力・画面例

```
Manager > set portauth dhcpserver=enabled  
  
Operation successful.
```

例

認証用 DHCP サーバー機能を有効にする。

SET PORTAUTH DHCPSEVER=ENABLED

備考・注意事項

認証用 DHCP サーバーが有効であっても、Web 認証が有効なポートでしか DHCP パケットは受信しない。

SET PORTAUTH PORT

カテゴリ：ポート認証

802.1X 認証、MAC ベース認証、Web 認証併用時

```
SET PORTAUTH=AUTO PORT={port-list|ALL} TYPE=AUTHENTICATOR [MODE={SINGLE|
MULTI}] [CONTROL={AUTHORISED|UNAUTHORISED|AUTO}] [EAPOLVERSION={1|2}]
[SERVERTIMEOUT=1..600] [QUIETPERIOD=0..65535] [TXPERIOD=1..65535]
[REAUTHPERIOD=1..86400] [SUPPTIMEOUT=1..600] [MAXREQ=1..10]
[REAUTHENABLED={ENABLED|DISABLED}] [PIGGYBACK=DISABLED]
[GUESTVLAN={vlan-name|1..4094|NONE}] [SECUREVLAN={ON|OFF}]
[VLANASSIGNMENT={ENABLED|DISABLED}] [VLANASSIGNMENTTYPE={USER|PORT}]
```

802.1X 認証 Authenticator 時

```
SET PORTAUTH[=8021X] PORT={port-list|ALL} TYPE=AUTHENTICATOR
[MODE={SINGLE|MULTI}] [CONTROL={AUTHORISED|UNAUTHORISED|AUTO}]
[EAPOLVERSION={1|2}] [SERVERTIMEOUT=1..600] [QUIETPERIOD=0..65535]
[TXPERIOD=1..65535] [REAUTHPERIOD=1..86400] [SUPPTIMEOUT=1..600]
[MAXREQ=1..10] [REAUTHENABLED={ENABLED|DISABLED}] [PIGGYBACK={ENABLED|
DISABLED}] [GUESTVLAN={vlan-name|1..4094|NONE}] [SECUREVLAN={ON|OFF}]
[VLANASSIGNMENT={ENABLED|DISABLED}] [VLANASSIGNMENTTYPE={USER|PORT}]
```

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 ベース認証時、Web 認証時

```
SET PORTAUTH={MACBASED|WEBBASED} PORT={port-list|ALL} TYPE=AUTHENTICATOR
[MODE={SINGLE|MULTI}] [CONTROL={AUTHORISED|UNAUTHORISED|AUTO}]
[QUIETPERIOD=0..65535] [REAUTHPERIOD=1..86400] [REAUTHENABLED={ENABLED|
DISABLED}] [GUESTVLAN={vlan-name|1..4094|NONE}] [SECUREVLAN={ON|OFF}]
[VLANASSIGNMENT={ENABLED|DISABLED}] [VLANASSIGNMENTTYPE={USER|PORT}]
```

認証ポートの解除

```
SET PORTAUTH 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)
vlan-name: VLAN 名

解説

指定ポートのポート認証設定を変更する

パラメーター

PORTAUTH 8021X(802.1X 認証)、MACBASED(MAC ベース認証)、WEBBASED(Web 認証)、AUTO から選択。AUTO を選択した場合、TYPE=AUTHENTICATOR 以降のパラメーターは、MAC ベース認証、Web 認証のパラメーター制限は PIGGYBACK 無効のみで、その他のパラメーターは 802.1X 認証時と同様。省略時は 8021X とみなされる。ポートセキュリティー (securitymode=automatic 以外) に指定したポートは MAC ベース認証、Web 認証ポートに設定できない

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

TYPE スイッチポートのタイプ (ポート認証における役割)。AUTHENTICATOR (Authenticator ポート)、SUPPLICANT (Supplicant ポート)、NONE (ポート認証機能無効) のいずれかを指定する。ポートセキュリティー (securitymode=automatic 以外) に指定したポートは AUTHENTICATOR に設定できない。ミラーポート、トランクポート、STP ポートに指定したポートは AUTHENTICATOR および SUPPLICANT に設定できない

MODE (802.1X Authenticator ポート、MAC ベース認証ポート、Web 認証ポート) Authenticator ポートのモード。Supplicant が 1 台だけ接続されていることを想定した Single-Supplicant モード (MODE=SINGLE) と、Supplicant が複数台接続されていることを想定した Multi-Supplicant モード (MODE=MULTI) がある。Single-Supplicant モードでは、該当ポート配下に最初に接続された Supplicant だけが認証対象となる。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

EAPOLVERSION (802.1X Authenticator ポート) EAPOL のバージョン。1 は IEEE 802.1X-2001 準拠モード、2 は IEEE 802.1X-2004 準拠モード。デフォルトは 1

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

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

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 EAPOL パケットをすべて破棄する。デフォルトは 60 秒。0 指定時はすぐに通信を許可する

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。Web 認証の場合、自動で再認証は行わないため認証有効時間の意味となる。この時間が経過した場合、認証は切断される。デフォルトは 3600 秒
- SUPPTIMEOUT** (802.1X Authenticator ポート) Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間 (秒)、デフォルトは 30 秒
- MAXREQ** (802.1X Authenticator ポート、Web 認証ポート) Supplicant に対する EAPOL-Request パケットの最大再送回数。デフォルトは 2 回
- REAUTHENABLED** (802.1X Authenticator ポート、MAC ベース認証ポート、Web 認証ポート) 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。デフォルトは、ENABLED。Web 認証の場合、認証切断を行うかどうかの選択の意味となる。ENABLE は認証切断を行い、DISABLE は認証切断を行わない。
- 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。ENABLED (有効) または DISABLED (無効) から選択する。デフォルトは、DISABLED。Multi-Supplicant モードにおいて、設定を行ってもエラーとはならず無視される
- AUTHPERIOD** (802.1X Supplicant ポート) Authenticator に EAP-Response パケットを送信した後、Authenticator からの応答を待つ時間 (秒)、デフォルトは 30 秒
- 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。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。Multi-Supplicant モード (MODE=MULTI) かつ、VLANASSIGNMENTTYPE=PORT では NONE 以外に指定できない。Single-Supplicant モードでゲスト VLAN 指定時、VLANASSIGNMENT=ENABLED VLANASSIGNMENTTYPE=PORT は 802.1X 認証以外は未サポート。デフォルトは NONE
- SECUREVLAN** (802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証 Multi-Supplicant Authenticator ポート、Web 認証 Multi-Supplicant Authenticator ポート) Multi-Supplicant モード (MODE=MULTI) でダイナミック VLAN を使用しているとき、2 番目以降の Supplicant の認証方法を指定する。本パラメータに ON を指定した場合は、2 番目以降の Supplicant は、最初に認証を通った Supplicant と同じ VLAN でないと認証されない。一方、OFF を指定した場合は、認証をパスする。ただし、2 番目以降の Supplicant は、実際には最初に認証をパスした Supplicant と同じ VLAN の所属となる。本パラメータは、VLANASSIGNMENTTYPE=PORT のとき、Multi-Supplicant モード (MODE=MULTI) のポートでのみ有効。デフォルトは ON
- 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/無効を選択する。有効時は、指定ポートの所属 VLAN を動的に変更する。Protected Port VLAN に所属するポートは ENABLED に設定できない。
- VLANASSIGNMENTTYPE** ダイナミック VLAN をポート単位で設定するか、ユーザー (MAC アドレス) 単位で設定するかを指定する。デフォルトは PORT。MODE=MULTI、VLANASSIGNMENT=ENABLED のときに有効になる。
- HELDPERIOD** (802.1X Supplicant ポート) 認証失敗後、Authenticator との通信を試みない期間 (秒)、デフォルトは 60 秒
- MAXSTART** (802.1X Supplicant ポート) EAPOL-Start パケットの最大送信回数。Supplicant ポートは、EAPOL-Start パケットを MAXSTART 回送信しても応答がない場合、ポート認証の必要はないと判断する。デフォルトは 3 回

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

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

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

入力・出力・画面例

```
Manager > set portauth port=1-8 type=authenticator

Operation successful.
```

例

ポート番号 1~8 を Authenticator ポートに設定する

```
SET PORTAUTH PORT=1-8 TYPE=AUTHENTICATOR
```

備考・注意事項

ポートセキュリティーを有効に設定したポートは TYPE=AUTHENTICATOR に設定できない。

トランクポート、ミラーポート、STP ポートに指定したポートは TYPE=AUTHENTICATOR、TYPE=SUPPLICANT に設定できない。

ゲスト VLAN を使用する場合、実際にポートに適用されている VLAN を確認するときは、SHOW VLAN コマンドを使用する。SHOW SWITCH PORT コマンドでは、コンソールなどから設定した VLAN 情報が表示される。

認証ポートの解除後、再設定をすると、解除前の設定が残る場合がある。

PORTAUTH=AUTO で認証を行った場合、通常 MAC ベース認証で問い合わせを行い、失敗した場合 802.1X 認証で再度認証を行うが、Multi-Supplicant モードで Supplicant から EAP-start を受信すると 802.1X 認証で問い合わせを行う。

認証ポートで Supplicant MAC 透過機能、ポートセキュリティーを使ってスタティックエントリーを登録した場合、その MAC アドレスを送信元としたパケットの VID が一致しないと認証ポートで破棄されるため、イングレスフィルタリング無効でもパケットは転送されない。

サポート Supplicant 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 Supplicant 数は 8 である。

802.1X 以外の認証設定時、PORTAUTH=[802.1X 以外] Mode=Single GUESTVLAN=[NONE 以外] VLANASSIGNMENT=ENABLED VLANASSIGNMENTTYPE=PORT は未サポート。

関連コマンド

DISABLE PORTAUTH (28 ページ)

ENABLE PORTAUTH (31 ページ)

SET PORTAUTH AUTHMETHOD (34 ページ)

SHOW PORTAUTH (49 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR (54 ページ)

SHOW PORTAUTH PORT SUPPLICANT (60 ページ)

SET PORTAUTH PORT SUPPLICANTMAC

カテゴリ：ポート認証

SET PORTAUTH PORT=port-number SUPPLICANTMAC=macadd [CONTROL=AUTHORISED]

port-number: スイッチポート番号 (1~。単一ポートのみ指定可)

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

解説

Supplicant MAC 透過アドレスを登録する。Supplicant MAC 透過アドレスは、Single-Supplicant モード、Multi-Supplicant モードのどちらの場合も 1 ポートに対して 10 個まで登録できる。

ADD PORTAUTH PORT SUPPLICANTMAC コマンドは同義

パラメーター

PORT 対象となるポート番号。複数ポートを指定することはできない

SUPPLICANTMAC Supplicant MAC 透過アドレスとして登録する MAC アドレス。ブロードキャスト、マルチキャストアドレスは設定できない

CONTROL 手動設定による Authenticator ポートの状態。AUTHORISED (認証済み固定) のみを指定可能

入力・出力・画面例

```
Manager > set portauth port=1 supplicantmac=00-00-f4-11-11-11 control=authorised
Operation successful.
```

例

Supplicant MAC 透過アドレスを登録する

```
SET PORTAUTH PORT=1 SUPPLICANTMAC=00-00-f4-11-11-11 CONTROL=AUTHORISED
```

備考・注意事項

ポート認証設定において、TYPE が AUTHENTICATOR、かつ、CONTROL が AUTO に指定されているポートに対して、Supplicant MAC 透過アドレスを登録できる。

ポート認証が有効に設定されていないポートに対して実行した場合、指定された MAC アドレスは本製品の設定にのみ登録され、FDB には登録されない。

すでに FDB にスタティックエントリーとして登録されているアドレス、他ポートで認証済みの Supplicant の MAC アドレスは、Supplicant MAC 透過アドレスに登録できない。

ポート認証設定において TYPE を AUTHENTICATOR 以外に変更した場合、または、CONTROL を AUTO 以外に変更した場合、すでに登録されている MAC アドレスは設定および FDB から削除される。

本コマンドで登録した MAC アドレスを違う VLAN でダイナミックエントリーとして登録すると設定した エージングタイムと関係なく、約 30 秒で削除される。

関連コマンド

ADD PORTAUTH PORT SUPPLICANTMAC (25 ページ)

DELETE PORTAUTH PORT SUPPLICANTMAC (27 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR (54 ページ)

SET PORTAUTH USERIDFORMAT

カテゴリ：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 および 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 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

入力・出力・画面例

```
Manager > set portauth useridformat separator=none

Operation successful.
```

| 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 |
| XX.XX.XX.XX.XX.XX | Period | 2 | TRUE |
| xx.xx.xx.xx.xx.xx | Period | 2 | FALSE |
| XXXX-XXXX-XXXX | Hyphen | 4 | TRUE |
| xxxx-xxxx-xxxx | Hyphen | 4 | FALSE |
| XXXX:XXXX:XXXX | Colon | 4 | TRUE |
| xxxx:xxxx:xxxx | Colon | 4 | FALSE |
| XXXX.XXXX.XXXX | Period | 4 | TRUE |
| xxxx.xxxx.xxxx | Period | 4 | FALSE |

| | | | |
|--------------|------|---|-------|
| XXXXXXXXXXXX | None | - | TRUE |
| xxxxxxxxxxxx | None | - | FALSE |

表 14: 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 (49 ページ)

SET WEBAUTHSERVER

カテゴリー：ポート認証

SET WEBAUTHSERVER [PORT=*port*] [REDIRECTURL=*string*] [MESSAGE1=*string*]
[MESSAGE2=*string*] [MESSAGE3=*string*] [MESSAGE4=*string*] [MESSAGE5=*string*]

port: TCP ポート番号

string: リダイレクト URL または、Web 認証ログイン画面の表示内容（半角英数字および記号。ただし記号はシャープ [#]、パーセント [%]、クエスチョン [?]、円マーク [\]、ダブルクォート ["] を除く。半角スペースを含む場合は、ダブルクォート ["] で囲む）

解説

Web 認証サーバーの設定を変更する

CLI から日本語の入力はできない。Web GUI からのみ MESSAGE1 ~ 5 に日本語入力が可能

パラメーター

PORT Web 認証サーバーの TCP ポート番号。デフォルトは 8080。

REDIRECTURL Web 認証の成功後に自動的にジャンプするページの URL。最大長 128Byte。デフォルトは Null。

MESSAGE1 Web 認証ログイン画面の表示内容。最大長 128Byte。デフォルトは Null

MESSAGE2 Web 認証ログイン画面の表示内容変更。最大長 128Byte。デフォルトは Null

MESSAGE3 Web 認証ログイン画面の表示内容変更。最大長 128Byte。デフォルトは Null

MESSAGE4 Web 認証ログイン画面の表示内容変更。最大長 128Byte。デフォルトは Null

MESSAGE5 Web 認証ログイン画面の表示内容変更。最大長 128Byte。デフォルトは Null

入力・出力・画面例

```
Manager > set webauthserver port=8081

Operation successful.
```

例

Web 認証サーバーの設定を変更する。

```
SET WEBAUTHSERVER PORT=8081
```

備考・注意事項

MESSAGE1～5には、HTML タグも入力可能であるが、それによって表示が崩れる可能性がある。

MESSAGE1～5には、128Byte まで入力可能であるが、入力文字列の長さによって表示が崩れる可能性がある。

REDIRECTURL、MESSAGE1～5にシャープ [#] を含む文字列を指定した場合、シャープおよびそれ以降の文字列、パラメーターは無視される。

関連コマンド

DISABLE PORTAUTH (28 ページ)

DISABLE WEBAUTHSERVER (30 ページ)

ENABLE WEBAUTHSERVER (33 ページ)

SET PORTAUTH AUTHMETHOD (34 ページ)

SET PORTAUTH PORT (38 ページ)

SHOW PORTAUTH (49 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR (54 ページ)

SHOW PORTAUTH PORT SUPPLICANT (60 ページ)

SHOW WEBAUTHSERVER (63 ページ)

SHOW PORTAUTH

```

9      ----- None      -----
10     ----- None      -----
11     ----- None      -----
12     ----- None      -----
13     ----- None      -----
14     ----- None      -----
15     ----- None      -----
16     ----- None      -----

```

Manager > show portauth config

```

Port Access Configuration Information:
Port Access Control..... Disabled
Authentication Method ..... RADIUS EAP
DHCP Server ..... Enabled
DHCP Server Lease Time ..... 20
MAC Based Auth User-ID Format..... xx-xx-xx-xx-xx-xx
Calling/Called-Station-ID Foramt.. XX-XX-XX-XX-XX-XX

```

Manager > show portauth status

```

-----
Port AuthMode PortRole  VLAN  PortStatus  Status  Additional Info
-----
1      ----- None      -----
2      ----- None      -----
3      ----- None      -----
4      MACBASE Auth      10    Unauthorized Held      00:00:F4:97:66:1A
4      MACBASE Auth      1000  Authorized  Authenticated 00:90:99:18:29:36
4      MACBASE Auth      1000  Authorized  Authenticated 00:E0:4C:C7:7D:99
5      MACBASE Auth      1000  Authorized  Authenticated 00:00:F4:27:2C:70
5      MACBASE Auth      1000  Authorized  Authenticated 00:09:41:86:FA:45
5      MACBASE Auth      1000  Authorized  Authenticated 00:09:41:A4:15:E1
5      MACBASE Auth      1000  Authorized  Authenticated 00:09:41:A4:59:43
6      8021x  Auth      1000  Authorized  Authenticated 00:03:47:B5:79:89
7      8021x  Auth      1000  Authorized  Authenticated 00:09:41:A4:18:11
8      ----- None      -----
9      ----- None      -----
10     ----- None      -----
11     ----- None      -----
12     ----- None      -----
13     ----- None      -----
14     ----- None      -----
15     ----- None      -----
16     ----- None      -----

```

| | |
|-----------------------|---|
| Port Access Control | ポート認証モジュールの有効/無効。Enabled か Disabled |
| Authentication Method | 認証方式 |
| DHCP Server | 認証用 DHCP サーバ機能が Enabled(有効) か Disabled(無効) を表示。 |

| | |
|----------------------------------|-----------------------------------|
| DHCP Server Lease Time | 認証用 DHCP サーバーのリースタイムを表示 |
| Number of Total Supplicants | Supplicant 数を表示 |
| Number of DynamicVlan per USER | ダイナミック VLAN にアサインされているユーザー数を表示 |
| 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 |

表 15: CONFIG 指定時

| | |
|-----------------|--|
| Port | ポート番号 |
| AuthMode | 使用認証モード。802.1x (802.1X 認証)、MACBASED(MAC ベース認証)、または WEBBASED (Web 認証) |
| Port Role | スイッチポートのタイプ(ポート認証における役割)、Authenticator、Supplicant、None のいずれか |
| VLAN | 現在割り当てられている VLAN ID |
| PortStatus | ポートの状態 Unauthorized (未認証) または、Authorized(認証済み)。Multi-Supplicant 有効時は、各 Supplicant の状態を表示 |
| Status | 認証状態。(ポートのタイプが設定され、ポート認証モジュールが有効の場合に、次のステータスを表示する。) Authenticator ポートの場合は、Initialize (初期化)、Connecting (接続中)、Authenticating (認証中)、Authenticated (認証済み)、Aborting (認証断念中)、Held (待機中)、Force_Auth (「認証済み」に固定設定)、Force_Unauth (「未認証」に固定設定) のいずれか。Supplicant ポートの場合は、Acquired (要求中)、Connecting (接続中)、Authenticating (認証中)、Authenticated (認証済み)、Held (待機中)、Logoff (ログオフ) のいずれか |
| Additional Info | Authenticator ポートで、Authenticated 状態のときに、Supplicant の MAC アドレスを表示する |

表 16: STATUS 指定時

例

ポート認証モジュールの設定を表示する

```
SHOW PORTAUTH CONFIG
```

ポート認証モジュールの状態を表示する

```
SHOW PORTAUTH STATUS
```

関連コマンド

DISABLE PORTAUTH (28 ページ)

ENABLE PORTAUTH (31 ページ)

SET PORTAUTH AUTHMETHOD (34 ページ)

SET PORTAUTH PORT (38 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR (54 ページ)

SHOW PORTAUTH PORT SUPPLICANT (60 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR

カテゴリ：ポート認証

```
SHOW PORTAUTH [= {8021X|MACBASED|WEBBASED}] PORT={port-list|ALL}
  [AUTHENTICATOR] [{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モジュールの設定と情報を表示する

パラメーター

PORTAUTH 8021X(802.1X 認証)、MACBASED(MAC ベース認証)、WEBBASED(Web 認証) から選択。省略時は全認証指定とみなされる。

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

AUTHENTICATOR 802.1X 認証、MAC ベース認証、Web 認証の情報を表示する。

CONFIG ポート認証モジュールの設定を表示する

STATUS ポート認証モジュールの状態を表示する

入力・出力・画面例

```
Manager > show portauth port=5-7

-----All Authenticator Configuration -----
-----
Port Number          5
Auth Mode            MACBASED
Log Type              [8021x] None
Log Type              [Mac] All
Log Type              [Web] None
Port Control          Auto
Supplicant Mode      Multi
eapolVersion         [8021x] 1
Quiet Period          60
Tx Period             [8021x] 30
Reauth Enabled        Enabled
Reauth Period         3600
Supplicant Timeout   [8021x] 30
Server Timeout       [Web][8021x] 30
Max Requests         [8021x] 2
Piggyback Mode       [8021x] Disabled
```

```

vlanAssignment          Enabled
secureVlan              On
guestVlan               None

Port Number             6
Auth Mode               MACBASED
Log Type                [8021x] Success, Logoff
Log Type                [Mac]  Success, Logoff
Log Type                [Web]  Success, Logoff
Port Control            Auto
Supplicant Mode        Multi
eapolVersion            [8021x] 1
Quiet Period           60
Tx Period               [8021x] 30
Reauth Enabled          Enabled
Reauth Period           3600
Supplicant Timeout     [8021x] 30
Server Timeout         [Web][8021x] 30
Max Requests           [8021x] 2
Piggyback Mode         [8021x] Disabled
vlanAssignment          Enabled
secureVlan              On
guestVlan               None

Port Number             7
Auth Mode               WEBBASED
Log Type                [8021x] All
Log Type                [Mac]  All
Log Type                [Web]  All
Port Control            Auto
Supplicant Mode        Multi
eapolVersion            [8021x] 1
Quiet Period           60
Tx Period               [Web][8021x] 30
Reauth Enabled          Enabled
Attached Supplicant(s) 00-00-11-11-11-11
                       00-00-22-22-22-22

```

```

-----
Port AuthMode Role  VID  PortStatus  Status  ReAuth Timer  Tag
                MAC Address  IP Address  User Name
-----
4      MACBASE Auth  10   Unauthorized Held      65535         n
                00:00:F4:97:66:1A 255.255.255.255 00-00-F4-97-66-1A
4      MACBASE Auth  1000 Authorized  Authenticated 3600         n
                00:90:99:18:29:36 255.255.255.255 00-90-99-18-29-36
4      MACBASE Auth  1000 Authorized  Authenticated 3600         n
                00:E0:4C:C7:7D:99 255.255.255.255 00-E0-4C-C7-7D-99
5      MACBASE Auth  1000 Authorized  Authenticated 100          n
                00:00:F4:27:2C:70 255.255.255.255 00-00-F4-27-2C-70
5      MACBASE Auth  1000 Authorized  Authenticated 3600         n

```

SHOW PORTAUTH PORT AUTHENTICATOR

```

5      MACBASE Auth 1000 Authorized 255.255.255.255 00-09-41-86-FA-45
00:09:41:A4:15:E1 255.255.255.255 00-09-41-A4-15-E1
5      MACBASE Auth 1000 Authorized 255.255.255.255 00-09-41-A4-59-43
00:09:41:A4:59:43 255.255.255.255 00-09-41-A4-59-43
6      8021x Auth 1000 Authorized 255.255.255.255 test1
00:03:47:B5:79:89 255.255.255.255 test1
7      WEBBASE Auth 1 Authorized 255.255.255.255 webauth1
00:09:41:A4:18:11 255.255.255.255 webauth1

Manager > show portauth port=4-7 authenticator status

-----
Port AuthMode Role VID PortStatus Status ReAuth Timer Tag
MAC Address IP Address User Name
-----
4      MACBASE Auth 10 Unauthorized Held 65535 n
00:00:F4:97:66:1A 255.255.255.255 00-00-F4-97-66-1A
4      MACBASE Auth 1000 Authorized Authenticated 3600 n
00:90:99:18:29:36 255.255.255.255 00-90-99-18-29-36
4      MACBASE Auth 1000 Authorized Authenticated 3600 n
00:E0:4C:C7:7D:99 255.255.255.255 00-E0-4C-C7-7D-99
5      MACBASE Auth 1000 Authorized Authenticated 100 n
00:00:F4:27:2C:70 255.255.255.255 00-00-F4-27-2C-70
5      MACBASE Auth 1000 Authorized Authenticated 3600 n
00:09:41:86:FA:45 255.255.255.255 00-09-41-86-FA-45
5      MACBASE Auth 1000 Authorized Authenticated 10 n
00:09:41:A4:15:E1 255.255.255.255 00-09-41-A4-15-E1
5      MACBASE Auth 1000 Authorized Authenticated 8 n
00:09:41:A4:59:43 255.255.255.255 00-09-41-A4-59-43
6      8021x Auth 1000 Authorized Authenticated 60000 n
00:03:47:B5:79:89 255.255.255.255 test1
7      WEBBASE Auth 1 Authorized 255.255.255.255 webauth1
00:09:41:A4:18:11 255.255.255.255 webauth1

```

| | |
|-----------------|---|
| Auth Mode | 認証モード。802.1x (802.1X 認証) MACBASED(MAC ベース認証)、または WEBBASED (Web 認証) のいずれか |
| Log Type | 認証ログの状態。All (認証ログをすべて残す) Success (認証成功のログを残す) Failure (認証失敗のログを残す) Logoff (ログオフのログを残す) None (認証ログは残さない) のいずれか |
| Port Control | (Authenticator ポート) 手動設定による Authenticator ポートの状態。AUTO (認証結果に応じて変動) UNAUTHORISED (未認証固定) AUTHORIZED (認証済み固定) のいずれか |
| Supplicant Mode | Single(Single-Supplicant モード)、Multi(Multi-Supplicant モード) のいずれか |

| | |
|------------------------|--|
| eapolVersion | EAPOL のバージョン。1、2 のいずれか。1 は IEEE 802.1X-2001 準拠モード、2 は IEEE 802.1X-2004 準拠モード |
| Quiet Period | (Authenticator ポート) Supplicant の認証に失敗した後、Supplicant との通信を拒否する期間 (秒) |
| Tx Period | (Authenticator ポート) Supplicant に EAPOL パケットを再送信する間隔 (秒) |
| Reauth Enabled | (Authenticator ポート) Supplicant ポートの再認証を行うかどうか。Enabled (再認証を行う) または Disabled (再認証を行わない) のいずれか |
| Reauth Period | (Authenticator ポート) Supplicant の再認証間隔 (秒) |
| Supplicant Timeout | (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) |
| Server Timeout | (Authenticator ポート) RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間 (秒) |
| Max Requests | (Authenticator ポート) Supplicant に対する EAPOL-Request パケットの最大再送回数 |
| Piggyback Mode | (Authenticator ポート) Piggy back モードの有効/無効。 |
| vlanAssignment | ダイナミック VLAN の有効・無効。デフォルトは 802.1Q タグ VLAN モードの場合 enabled、マルチプル VLAN モードの場合 disabled |
| vlanAssignmenttype | ダイナミック VLAN がポート単位かユーザー単位か表示する。PORT、USER のいずれか |
| secureVlan | ダイナミック VLAN 有効時、2 番目以降に接続された Supplicant の所属 VLAN が、最初に認証を通った Supplicant と同じでないとは認証を許可しない機能の有効・無効 |
| guestVlan | ゲスト VLAN に指定した VLAN 名と VLAN ID |
| Attached Supplicant(s) | Supplicant MAC 透過アドレス |

表 17: CONFIG 指定時

| | |
|--------------|--|
| Port | ポート番号 |
| AuthMode | 使用認証モード。802.1x (802.1X 認証) MACBASED(MAC ベース認証)、または WEBBASED (Web 認証) のいずれか |
| Role | スイッチポートのタイプ。Auth、Supp、NONE (ポート認証機能無効) のいずれか |
| VID | 現在割り当てられている VLAN ID |
| PortStatus | ポートの状態 Unauthorized (未認証) または、Authorized (認証済み)。Multi-Supplicant 有効時は、各 Supplicant の状態を、上記のいずれかで表示する。 |
| Status | 認証状態。(ポートのタイプが設定され、ポート認証モジュールが有効の場合に、次のステータスを表示する。) Authenticator ポートの場合は、Initialize (初期化) Connecting (接続中) Authenticating (認証中) Authenticated (認証済み) Aborting (認証断念中) Held (待機中) Force_Auth (「認証済み」に固定設定) Force_Unauth (「未認証」に固定設定) のいずれか。Supplicant ポートの場合は、Acquired (要求中) Connecting (接続中) Authenticating (認証中) Authenticated (認証済み) Held (待機中) Logoff (ログオフ) のいずれか |
| ReAuth Timer | 再認証タイマー。再認証までの残り時間 (秒)。Status が Authenticated 以外の場合、または、ReauthEnabled が無効の場合は "-" (ハイフン) を表示 |
| Tag | タグポートで認証したか否か |
| MAC Address | Authenticator ポートで、Authenticated 状態のときに、Supplicant の Mac アドレスを表示 |
| IP Address | Supplicant の IP アドレス。認証時に Authenticator と Supplicant 間でやりとりするパケットに IP アドレスが含まれている場合のみ表示される。802.1X 認証は表示されない場合あり |
| User Name | 認証時のユーザー名。最大 20 文字 |

表 18: STATUS 指定時

例

ポート 1 のポート認証モジュールの設定を表示する

```
SHOW PORTAUTH PORT=1 AUTHENTICATOR CONFIG
```

ポート 1 のポート認証モジュールの状態を表示する

```
SHOW PORTAUTH PORT=1 AUTHENTICATOR STATUS
```

備考・注意事項

GUI では表示されない。

関連コマンド

DISABLE PORTAUTH (28 ページ)

ENABLE PORTAUTH (31 ページ)

SET PORTAUTH AUTHMETHOD (34 ページ)

SET PORTAUTH PORT (38 ページ)

SHOW PORTAUTH (49 ページ)

SHOW PORTAUTH PORT SUPPLICANT (60 ページ)

SHOW PORTAUTH PORT SUPPLICANT

カテゴリー：ポート認証

SHOW PORTAUTH [=8021X] **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モジュールの設定と情報を表示する

パラメーター

PORTAUTH 8021X(802.1X 認証)

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

CONFIG ポート認証モジュールの設定を表示する

STATUS ポート認証モジュールの状態を表示する

入力・出力・画面例

```
Manager > show portauth port=1 supplicant config
```

```
-----Supplicant Configuration -----
```

```
-----
Port Number      1
Auth Period      30
Held Period      60
Max Start        3
Start Period     30
User Name
User Password
```

```
Manager > show portauth port=5 supplicant status
```

```
-----
Port  PortRole  VLAN  PortStatus  Status  Additional Info
-----
5     Supp      ----  -----    -----  -----
```

| Port Number | ポート番号 |
|-------------|-------|
|-------------|-------|

| | |
|-------------|--|
| Auth Period | 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) |
|-------------|--|

| | |
|---------------|---|
| Held Period | 認証失敗後、Authenticator との通信を試みない期間 (秒) |
| Max Start | 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 |
| Start Period | Authenticator に EAPOL-Start パケットを再送信する間隔 (秒) |
| User Name | ユーザー名 |
| User Password | パスワード |

表 19: CONFIG 指定時

| | |
|-----------------|--|
| Port | ポート番号 |
| PortRole | スイッチポートのタイプ (ポート認証における役割) |
| VLAN | Supplicant 指定時は表示されない |
| PortStatus | Supplicant 指定時は表示されない |
| Status | ポートの状態。(ポートのタイプが設定され、ポート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 |
| Additional Info | Authenticator ポートで、Authenticated 状態のときに、Supplicant の MAC アドレスを表示する。Multi-Supplicant が有効な場合は、各 Supplicant の MAC アドレスを表示 |

表 20: STATUS 指定時

例

ポート 1 のポート認証モジュールの設定を表示する

```
SHOW PORTAUTH PORT=1 SUPPLICANT CONFIG
```

ポート 2 のポート認証モジュールの状態を表示する

```
SHOW PORTAUTH PORT=2 SUPPLICANT STATUS
```

備考・注意事項

GUI では表示されない。

関連コマンド

ADD PORTAUTH PORT SUPPLICANTMAC (25 ページ)

DELETE PORTAUTH PORT SUPPLICANTMAC (27 ページ)

DISABLE PORTAUTH (28 ページ)

ENABLE PORTAUTH (31 ページ)

SET PORTAUTH AUTHMETHOD (34 ページ)

SET PORTAUTH PORT (38 ページ)

SHOW PORTAUTH (49 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR (54 ページ)

SHOW WEBAUTHSERVER

カテゴリ：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

```

Manager > show webauthserver

Web Authentication Server Module Configuration:
-----
Status      : Enabled
TCP port    : 8080
RedirectURL  :
Message1    : Allied-Telesis
Message2    : User Login
Message3    :
Message4    :
Message5    : Copyright (C) Allied Telesis K.K.

```

| | |
|-------------|---|
| Status | Web 認証サーバーの状態。有効 (Enabled) または無効 (Disabled) |
| TCP port | Web 認証サーバーの TCP ポート番号。デフォルトは 8080 |
| RedirectURL | Web 認証の成功後に自動的にジャンプするページの URL。最大長 128Byte。デフォルトは Null |
| Message1 | Web 認証ログイン画面の表示内容。デフォルトは Null |
| Message2 | Web 認証ログイン画面の表示内容。デフォルトは Null |
| Message3 | Web 認証ログイン画面の表示内容。デフォルトは Null |
| Message4 | Web 認証ログイン画面の表示内容。デフォルトは Null |
| Message5 | Web 認証ログイン画面の表示内容。デフォルトは Null |

表 21:

例

Web 認証サーバーの情報を表示する。

```
SHOW WEBAUTHSERVER
```

関連コマンド

DISABLE PORTAUTH (28 ページ)

SET PORTAUTH AUTHMETHOD (34 ページ)

SET PORTAUTH PORT (38 ページ)

SET WEBAUTHSERVER (47 ページ)

SHOW PORTAUTH (49 ページ)

SHOW PORTAUTH PORT AUTHENTICATOR (54 ページ)

SHOW PORTAUTH PORT SUPPLICANT (60 ページ)