802.1x サプリカントとしての Lightweight アクセス ポイントの設定

目次

概要

このドキュメントでは、Lightweight アクセス ポイントを 802.1x サプリカントとして設定して、RADIUS サーバに対して認証するための方法について説明します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- Cisco Aironet 1130、1240、または 1250 シリーズ アクセス ポイント
- IOS® バージョン 5.1 が稼働する WLC
- Cisco IOS リリース 12.2(35)SE5 が稼働する Cisco Catalyst 3560 シリーズ スイッチ
- Cisco IOS リリース 12.2(40)SE が稼働する Cisco Catalyst 3750 シリーズ スイッチ
- Cisco IOS リリース 12.2(40)SG が稼働する Cisco Catalyst 4500 シリーズ スイッチ
- Cisco IOS リリース 12.2(33)SXH が稼働する、Supervisor Engine 32 を搭載した Cisco Catalyst 6500 シリーズ スイッチ

使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

LAP には、秘密キーで署名された X.509 証明書が出荷時に組み込まれ、これは製造時にデバイスに書き込まれます。 LAP はこの証明書を使用して、加入プロセス時に WLC との認証を行います。 詳細は、ドキュメント『Cisco 440X シリーズ ワイヤレス LAN コントローラの配備』の「LWAPP コントロール プレーンの保護」セクションを参照してください。 ここでは LAP を認証する別の方法について説明します。 WLC バージョン 5.1 では、Cisco Aironet アクセス ポイントと Cisco スイッチの間に 802.1x 認証を設定できます。 アクセス ポイントは 802.1x サプリカントとして機能し、匿名 PAC プロビジョニングによる EAP-FAST を使用する RADIUS サーバ（ACS）に対してスイッチによって認証されます。 802.1x 認証が設定されると、スイッチは、ポートに接続されたデバイスが正しく認証されるまでは、802.1x トラフィック以外のトラフィックがポートを通過することを許可しません。 アクセス ポイントの認証は、WLC に参加する前か、WLC に参加した後に実行できます。後者の場合、LAP が WLC に参加した後で 802.1x をスイッチに設定します。

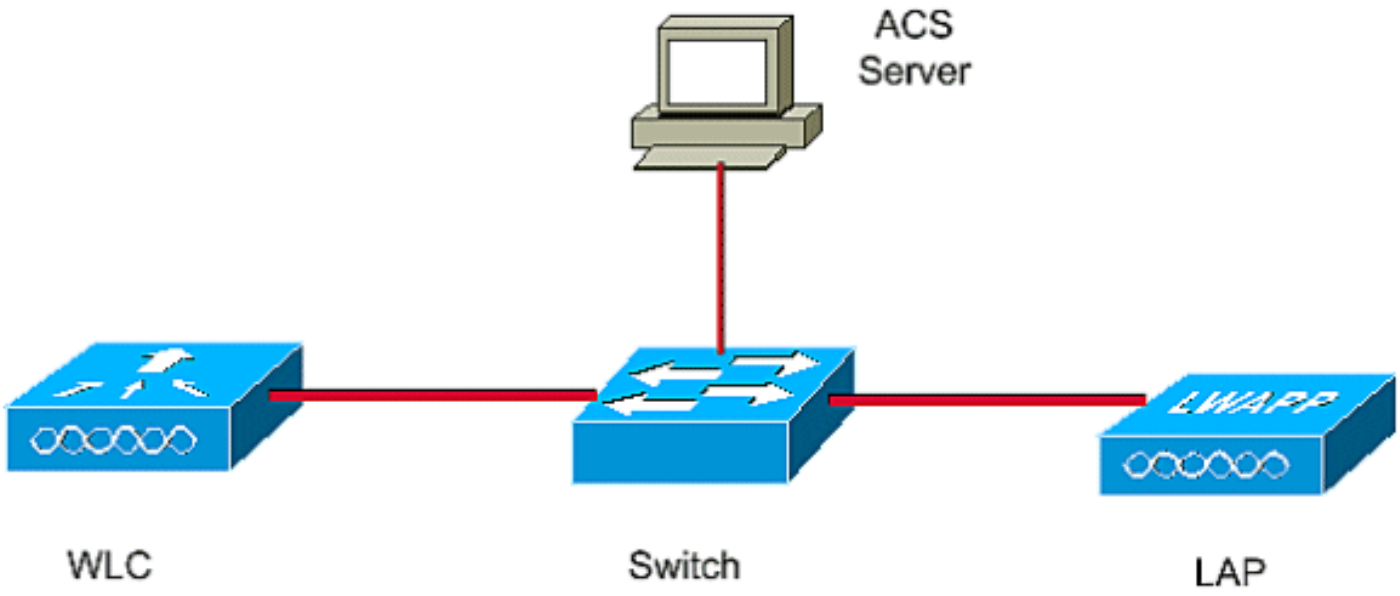
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



設定

このドキュメントでは、次の IP アドレスを使用します。

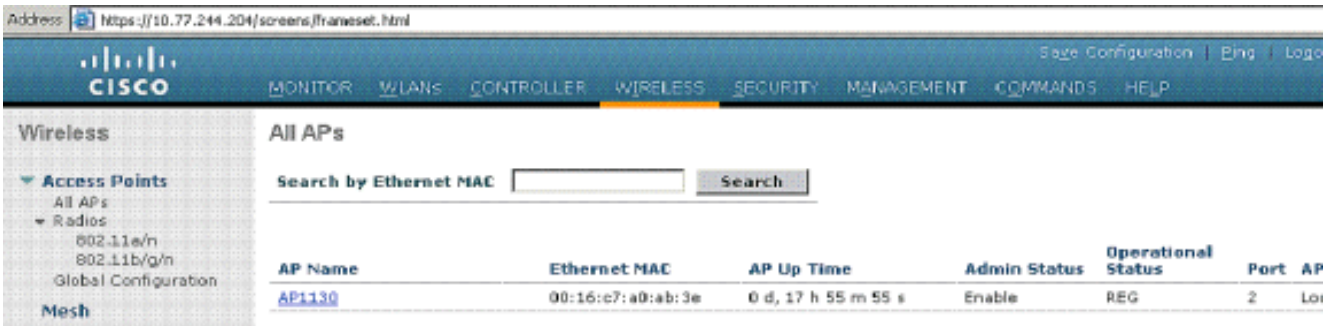
- スイッチの IP アドレスは 10.77.244.210 です。
- ACS サーバの IP アドレスは 10.77.244.196 です。
- WLC の IP アドレスは 10.77.244.204 です。

LAP の設定

このセクションでは、802.1x サプリカントとしての LAP の設定について説明しています。

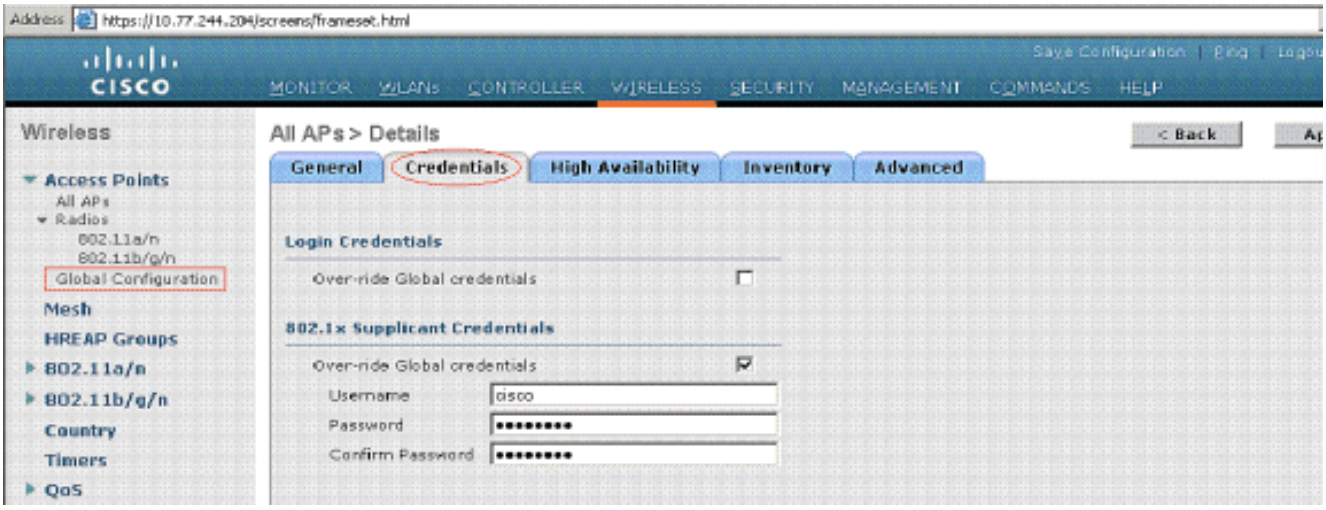
次の手順を実行します。

1. アクセス ポイントに Lightweight Recovery イメージがロードされていることを確認します。
2. LAP をスイッチに接続します。
3. LAP は加入プロセスを開始し、WLC に登録されます。 これは図 1 に示すように WLC の Wireless メニューから確認できます。**図 1**



4. [access point] をクリックし、[Credentials] タブをクリックします。
5. [802.1x Supplicant Credentials] の見出しの下にある [Over-ride Global credentials] チェックボックスにチェックマークを入れ、このアクセス ポイントについての 802.1x ユーザ名およびパスワードを設定します。 また、WLC に参加するすべてのアクセス ポイントに共通するユーザ名およびアクセス ポイントを、[Global Configuration] メニューで設定できます。 図

2 に、アクセス ポイントに対する 802.1x クレデンシャルを設定する方法を示します。**図 2**



注: アクセス ポイントの 802.1x ユーザ名およびパスワードは、WLC CLI コマンド **config ap dot1xuser add username <user> password <password> Cisco_AP (AP Name)** で設定することもできます。

6. [Apply] をクリックして、変更を確定します。
7. [Save configuration] をクリックして、クレデンシャルを保存します。**注:** これらのクレデンシャルは、いったん保存されると、WLC および AP のリブート後も保持されます。 これらは LAP が新しい WLC に加入した場合に限り変更されます。 LAP は、新しい WLC に設定されているユーザ名およびパスワードを受け入れます。
8. アクセス ポイントがまだ WLC に加入していない場合、LAP にコンソール接続してクレデンシャルを設定し、次の CLI コマンドをイネーブル モードを使用する必要があります。
   `LAP#lwapp ap dot1x username <username> password <password>` **注:** このコマンドは、5.1 リカバリ イメージを実行しているアクセス ポイントからのみ使用できます。

スイッチの設定

スイッチは LAP のオーセンティケータとして機能し、RADIUS サーバに対して LAP を認証します。 準拠したソフトウェアがスイッチにない場合、スイッチをアップグレードします。 スイッチ CLI で次のコマンドを入力して、スイッチ ポート上で 802.1X 認証を有効にします。

```
switch#configure terminal                    switch(config)dot1x system-auth-control
switch(config)aaa new-model                    switch(config)aaa authentication dot1x default
group radius                    switch(config)radius server host 10.77.244.196 key cisco!---
configures the radius server with shared secret switch(config)interface gigabitEthernet 1/0/43!-
-- 43 is the port number on which the access point is connected. switch(config-if)switchport
mode access switch(config-if)dot1x pae authenticator!--- configures dot1x authentication
switch(config-if)dot1x port-control auto!--- With this command switch initiates the 802.1x
authentication.
```

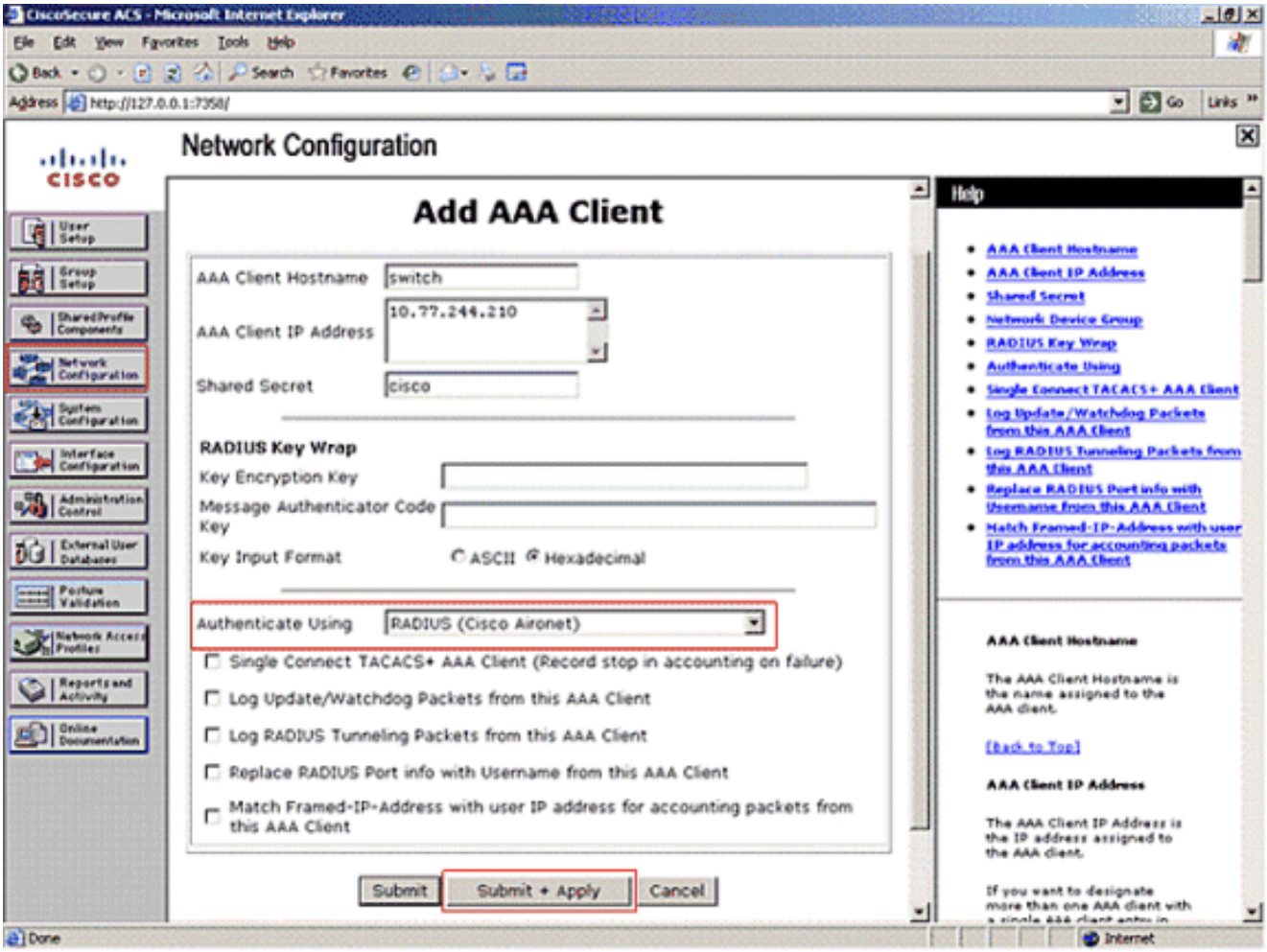
RADIUS サーバの設定

LAP は EAP-FAST で認証されます。 使用する RADIUS サーバがこの EAP 方式をサポートすることを確認してください。 この例では認証に ACS サーバを使用します。 ACS サーバで次の手順を実行します。

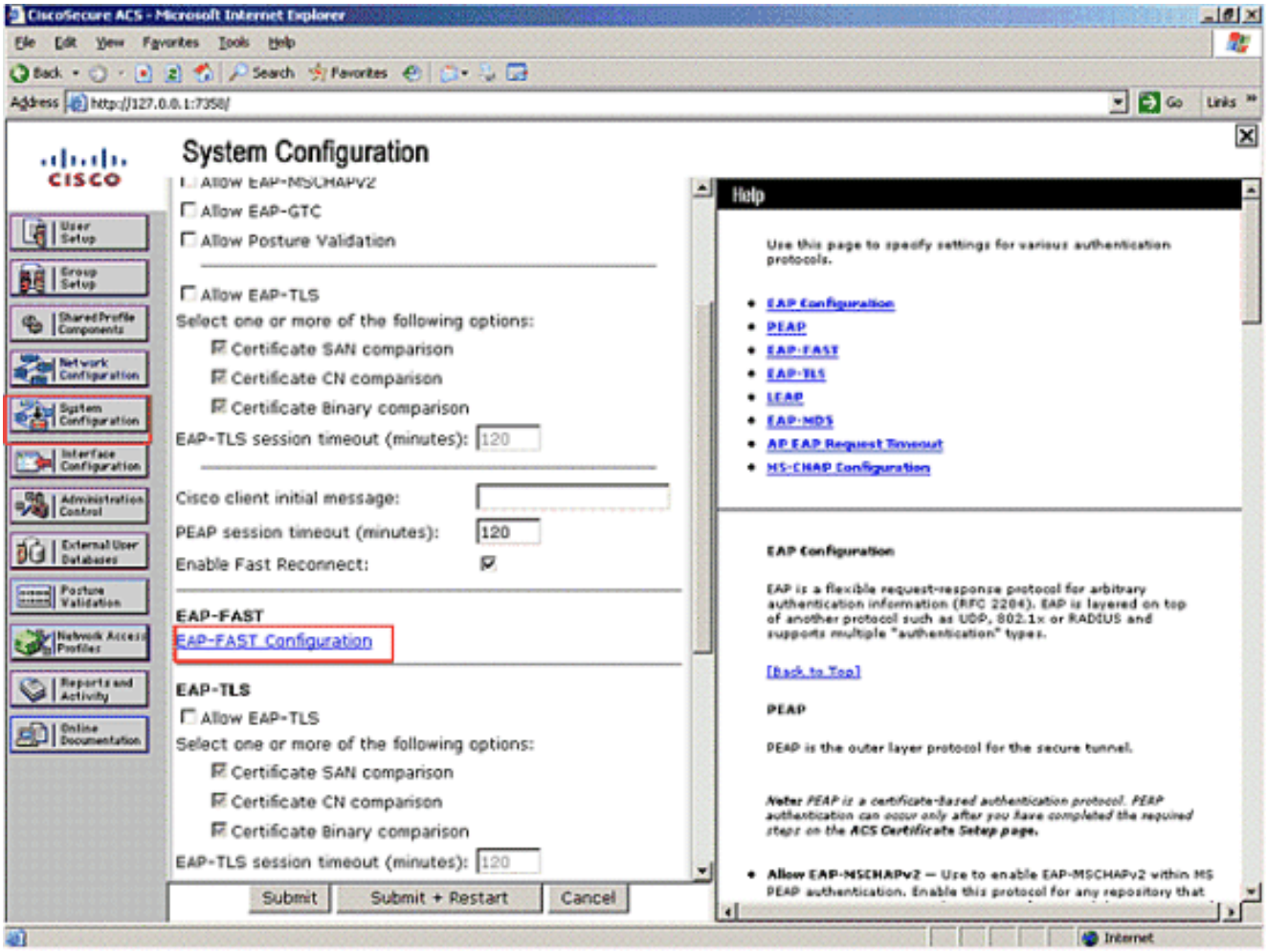
1. ACS 管理画面を起動します。
2. ACS データベース内で LAP のユーザ名およびパスワードを設定します。 ACS にユーザ アカウントを追加するには、『Cisco Secure Access Control Server 4.2 ユーザ ガイド』の「

ユーザ管理」セクションを参照してください。

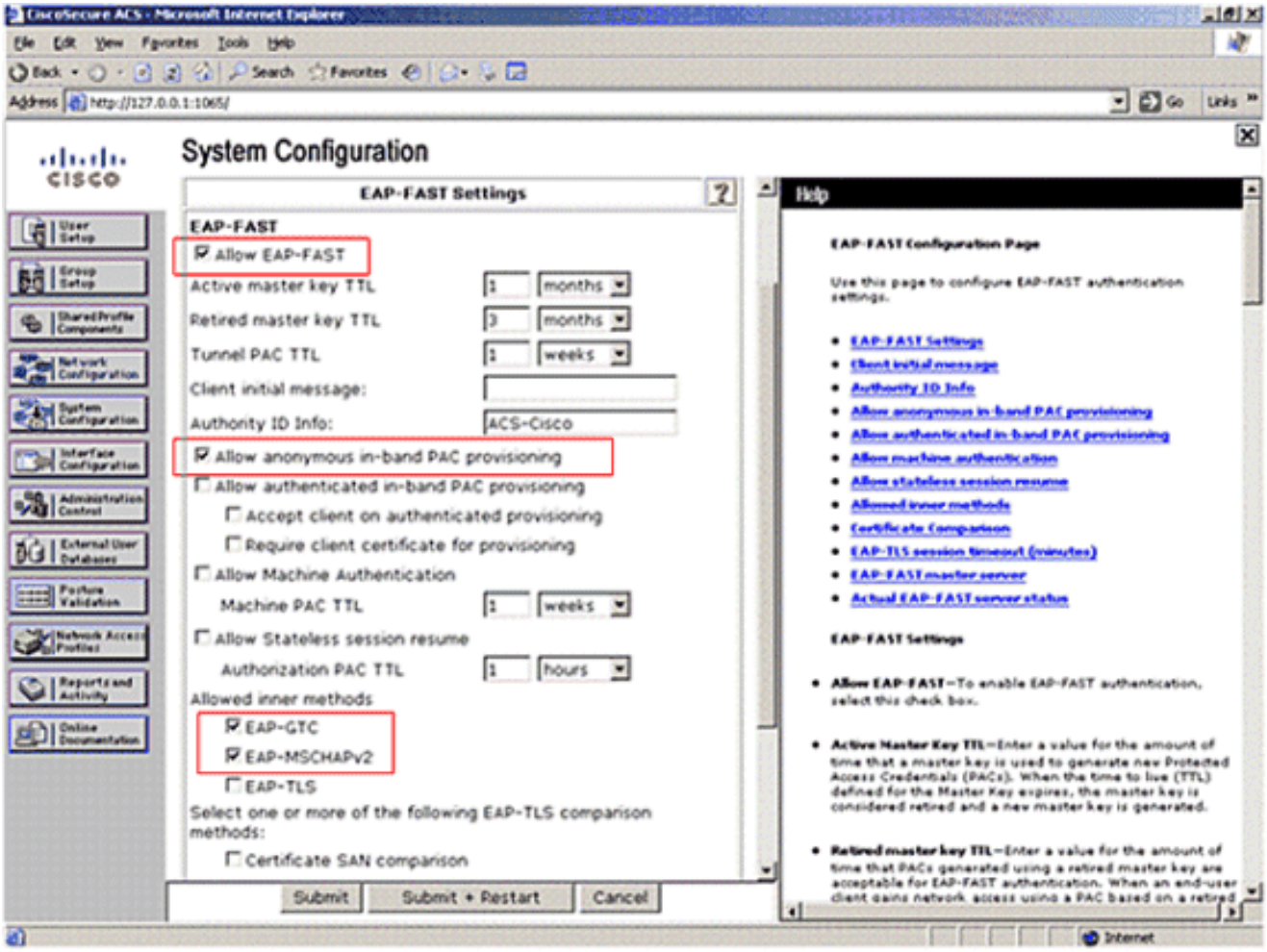
3. ACS サーバに対する AAA クライアントとしてスイッチを設定します。 ACS 管理画面で、[Network Configuration] メニューをクリックします。
4. [AAA client] セクションで、[Add New Entry] をクリックします。 次のパラメータを入力します。[AAA Client IP Address] フィールドにスイッチの IP アドレスを入力します。スイッチの共有秘密を入力します。 これはスイッチと ACS サーバでまったく同一である必要があります。[Authenticate Using] フィールドで [RADIUS Protocol] を選択します。 これはデフォルトでは TACACS+ です。**注:** RADIUS プロトコルの説明については、ACS サーバを確認してください。図 3 を参照してください。**図 3**



5. [Submit + Apply] をクリックして AAA クライアントを保存します。
6. RADIUS サーバ上で EAP-FAST を有効にする必要があります。 左側にある [System Configuration] メニューをクリックします。 [Global Authentication Setup] オプションをクリックします。**図 4**



7. 図 4 に示すように、[EAP -FAST Configuration] をクリックします。
8. [EAP-FAST Settings] ページで、[Allow EAP-FAST] ボックスにチェックマークを付けます。 LAP では、匿名 PAC プロビジョニングの EAP-FAST を使用します。 [Allow Anonymous in-band PAC provisioning] ボックスにチェックマークを付けます。 詳細については、ドキュメント『ワイヤレス LAN コントローラおよび外部 RADIUS サーバを使用する EAP-FAST 認証の設定例』を参照してください。**図 5**



9. [Allow inner methods] の下にある [EAP-GTC] および [EAP-MSCHAPv2] にチェックマークが付いていることを確認します。 図 5 に、手順 8 と 9 の設定例を示します。

確認

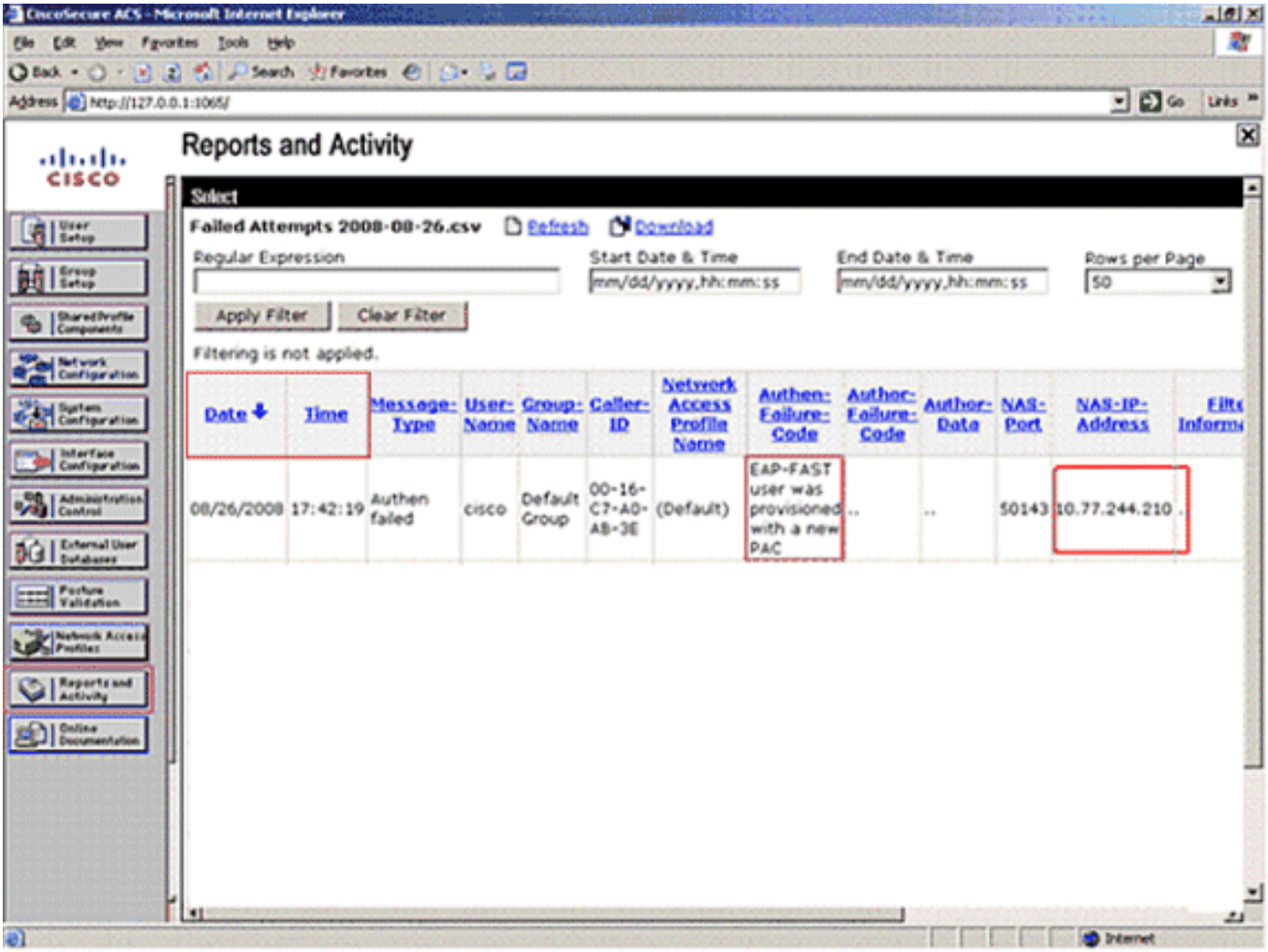
ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

802.1x がスイッチ ポートで有効になると、802.1x トラフィック以外のすべてのトラフィックがポートでブロックされます。 WLC に登録されている LAP は、アソシエーションが解除されます。 他のトラフィックは、802.1x 認証に成功した場合に限り、通過が許可されます。 802.1x がスイッチ上で有効になった後、WLC に対して LAP の登録が成功したということは、LAP 認証が成功したことを示します。

このことは ACS からも確認できます。 ACS のメイン画面で、[Reports and Authentication] メニューをクリックします。 [Failed Attempts] オプションをクリックします。 認証に成功すると、図 6 に示すように、[NAS-IP-Address] フィールドに「*EAP-FAST user was provisioned with a new PAC with IP address of the switch*」というコードが付いた「*Authentication failed*」メッセージが表示されます。 また、認証の日時も確認できます。

図 6



トラブルシューティング

ここでは、設定に関するトラブルシューティングについて説明します。

1. ping コマンドを使用して、ACS サーバにスイッチからアクセスできるかどうかを調べます。
2. スイッチが ACS サーバの AAA クライアントとして設定されていることを確認します。
3. スイッチと ACS サーバの共有秘密が同一であることを確認します。
4. ACS サーバで EAP-FAST が有効になっているかどうかを調べます。
5. デバイスのソフトウェアが準拠しているかどうかを確認します。
6. LAP に 802.1x クレデンシャルが設定されていること、および ACS サーバ上で同一であることを確認します。**注:** ユーザ名とパスワードは大文字小文字が区別されます。

トラブルシューティングのためのコマンド

この機能について現在使用できるデバッグ コマンドはありません。

関連情報

- Lightweight アクセス ポイントの制御
- IEEE 802.1x ポートベース認証の設定

- テクニカルサポートとドキュメント - Cisco Systems