

Configure Lightweight Access Point as an 802.1x Supplicant

Document ID: 107946

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

Configure

- Network Diagram
- Configurations
- Configure the LAP
- Configure the Switch
- Configure the RADIUS Server

Verify

Troubleshoot

- Troubleshooting Commands

Related Information

Introduction

This document describes how to configure a Lightweight Access Point as a 802.1x supplicant to authenticate against a RADIUS Server.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Cisco Aironet 1130, 1240, or 1250 Series access point
- WLC that runs IOS[®] Version 5.1
- Cisco Catalyst 3560 Series Switches with Cisco IOS Release 12.2(35)SE5
- Cisco Catalyst 3750 Series Switches with Cisco IOS Release 12.2(40)SE
- Cisco Catalyst 4500 Series Switches with Cisco IOS Release 12.2(40)SG
- Cisco Catalyst 6500 Series Switches with Supervisor Engine 32 that runs Cisco IOS Release 12.2(33)SXH

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

LAPs have factory installed X.509 certificates, signed by a private key, that are burned into the device at the time of manufacture. LAPs use this certificate to authenticate with the WLC at the join process. For more information, refer to Securing the LWAPP Control Plane of the document Deploying Cisco 440X Series Wireless LAN Controllers. This method describes another way to authenticate LAPs. With WLC Version 5.1, you can configure the 802.1x authentication between a Cisco Aironet access point and a Cisco switch. The access point acts as the 802.1x supplicant and is authenticated by the switch against a RADIUS Server (ACS) that uses EAP-FAST with anonymous PAC provisioning. Once it is configured for 802.1x authentication, the switch does not allow any traffic other than 802.1x traffic to pass through the port until the device connected to the port authenticates successfully. An access point can be authenticated either before it joins a WLC or after it has joined a WLC, in which case you configure 802.1x on the switch after the LAP joins the WLC.

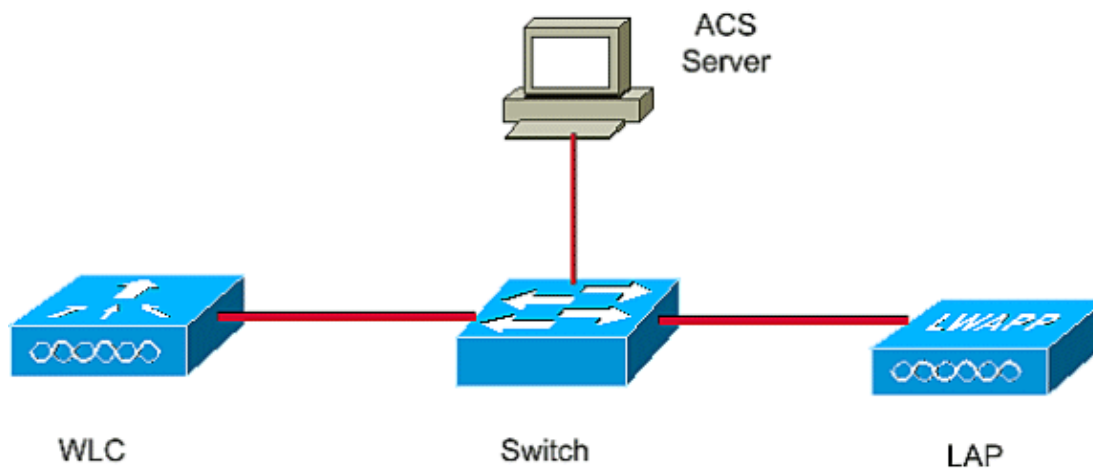
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Network Diagram

This document uses this network setup:



Configurations

This document uses these IP addresses:

- IP address of the switch is 10.77.244.210
- IP address of the ACS server is 10.77.244.196
- IP address of the WLC is 10.77.244.204

Configure the LAP

In this section, you are presented with the information to configure the LAP as a 802.1x supplicant.

Complete these steps:

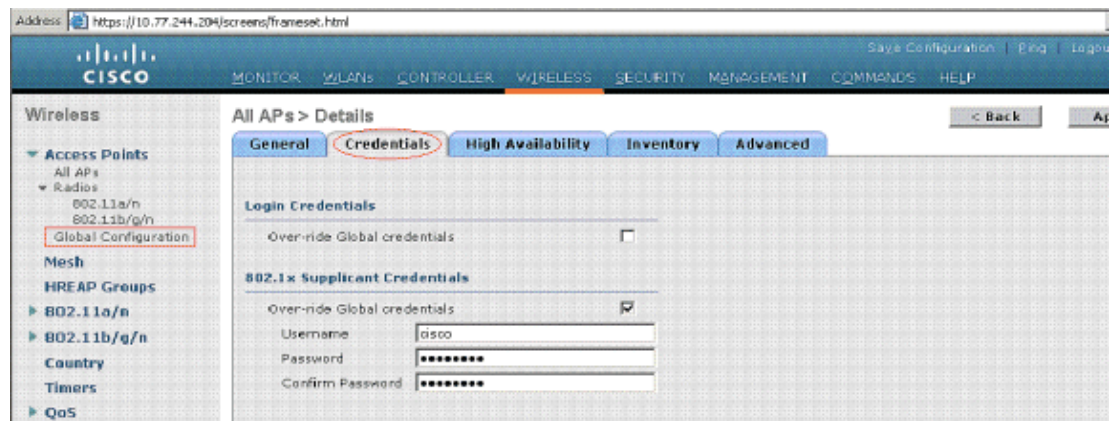
1. Make sure that the access point is loaded with a Lightweight Recovery image.
2. Connect the LAP to the switch.
3. The LAP goes through the join process and registers with the WLC. This can be checked from the Wireless menu of the WLC as shown in Figure 1.

Figure 1



4. Click the **access point**, and click the **Credentials** tab.
5. Under the 802.1x Supplicant Credentials heading, check the **Over-ride Global credentials** box to set the 802.1x username and password for this access point. You can also set the username and password in common to all the access points that join a WLC with the Global Configuration menu. Figure 2 shows how to set the 802.1x credentials for an access point.

Figure 2



Note: You can also set the 802.1x username and password for an access point with the WLC CLI command `config ap dot1xuser add username <user> password <password> Cisco_AP (AP Name)`.

6. Click **Apply** to commit your changes.
7. Click **Save configuration** to save the credentials.

Note: Once saved, these credentials are retained across WLC and AP reboots. They change only when the LAP joins a new WLC. The LAP assumes the username and password that were configured on the new WLC.

8. If the access point has not joined a WLC yet, you must console into the LAP to set the credentials and use this CLI command in the enable mode:

```
LAP#lwapp ap dot1x username <username> password <password>
```

Note: This command is available only for access points that run the 5.1 recovery image.

Configure the Switch

The switch acts as an authenticator for the LAP and authenticates the LAP against a RADIUS server. If the switch does not have the compliant software, upgrade the switch. On the switch CLI, enter these commands to enable the 802.1x authentication on a switch port:

```
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.
```

Configure the RADIUS Server

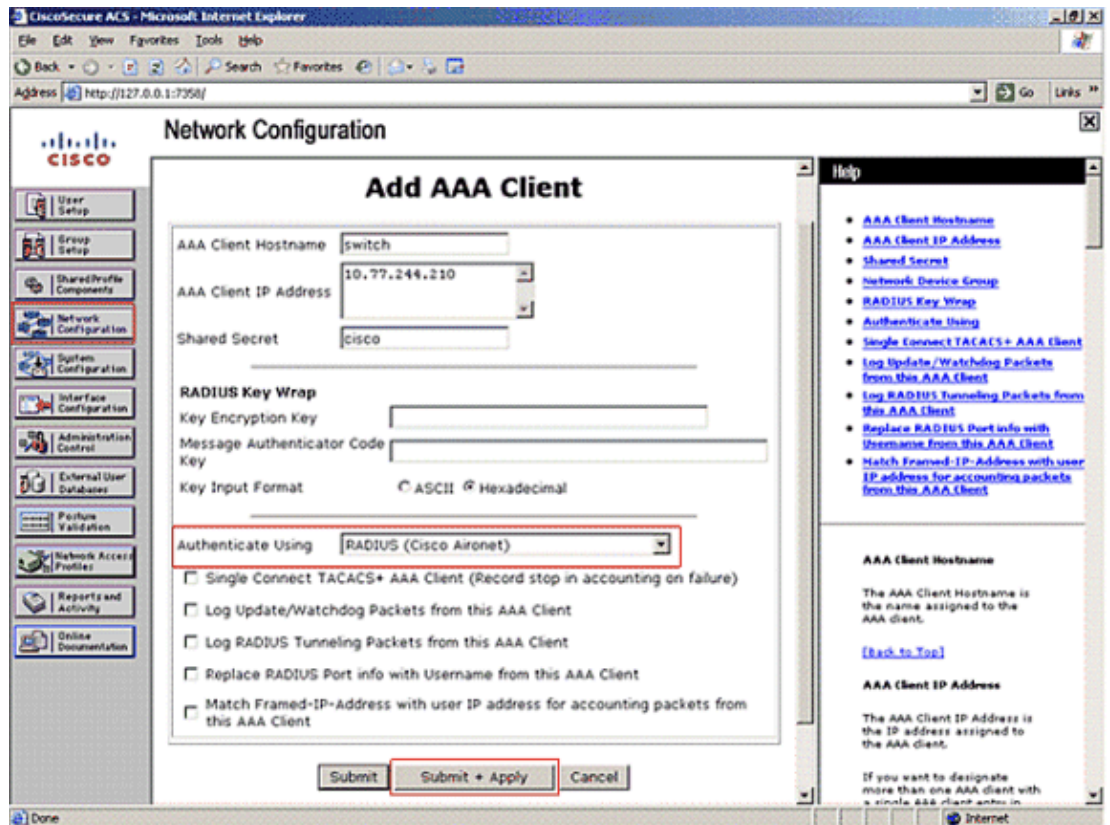
LAP is authenticated with EAP-FAST. Make sure that the RADIUS server you use supports this EAP method. In this example, the ACS server is used for authentication. Complete these steps on the ACS server:

1. Launch the ACS admin screen.
2. Configure the username and password of the LAP in the ACS database. In order to add a user account in the ACS, refer to the User Management section of the document User Guide for Cisco Secure Access Control Server 4.2.
3. Configure the Switch as an AAA client to the ACS server. On the ACS admin screen, click the **Network Configuration** menu.
4. Under the **AAA client** section, click **Add New Entry**. Enter these parameters:
 - a. Enter the IP address of the switch in the *AAA Client IP Address* field.
 - b. Enter the shared secret of the switch. This must be exactly the same on the switch and ACS server.
 - c. Choose a **RADIUS Protocol** in the *Authenticate Using* field. By default, it is TACACS+.

Note: Check the ACS server for a description of the RADIUS Protocols.

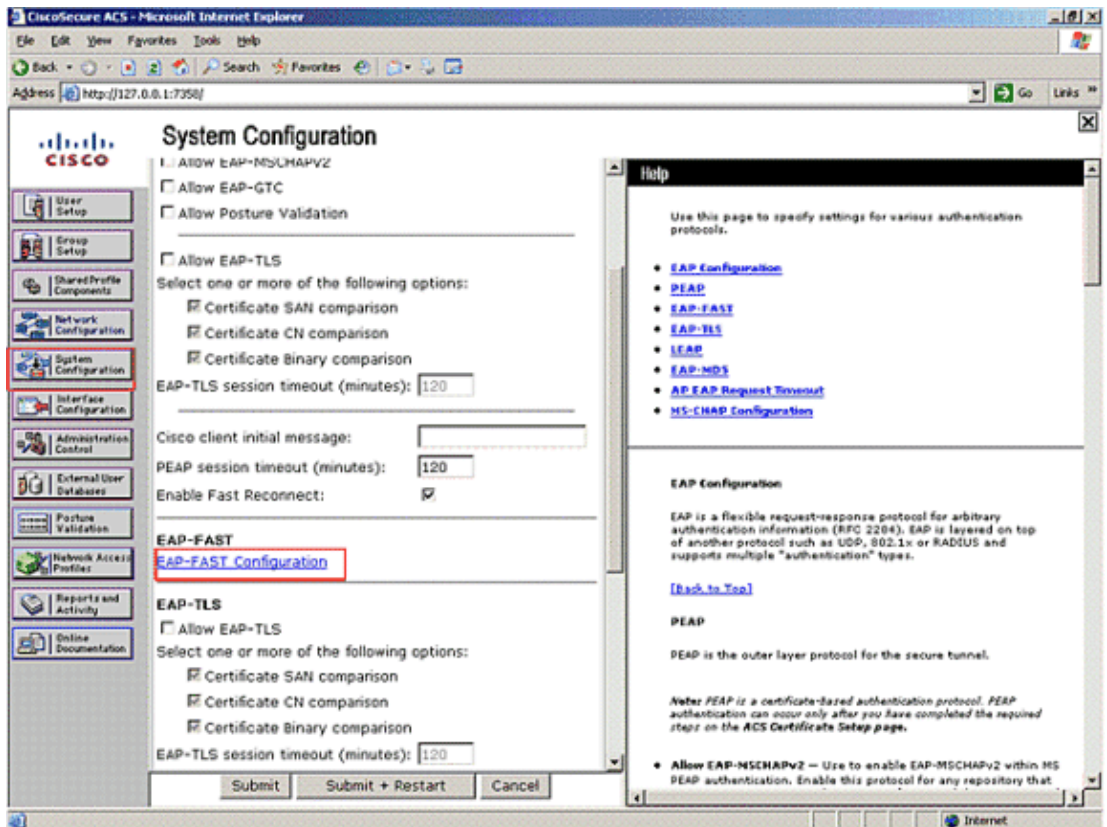
See Figure 3.

Figure 3



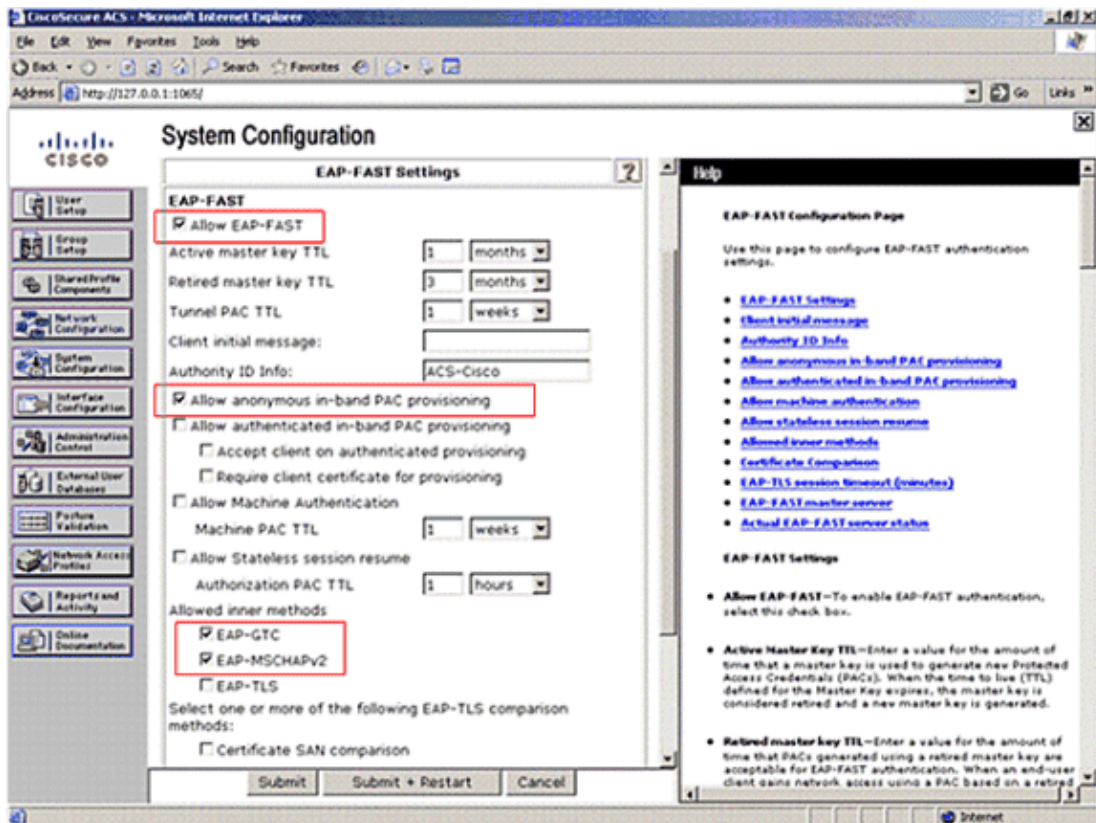
5. Click **Submit + Apply** to save the AAA client.
6. EAP-FAST has to be enabled on the RADIUS server. Click the **System Configuration** menu in the left-hand side. Click the **Global Authentication Setup** option.

Figure 4



7. Click **EAP –FAST Configuration** as shown in Figure 4.
8. On the EAP–FAST Settings page, check the **Allow EAP–FAST** box. LAP uses EAP–FAST with anonymous PAC provisioning. Check the **Allow Anonymous in–band PAC provisioning** box. For more information, refer to the document EAP–FAST Authentication with Wireless LAN Controllers and External RADIUS Server Configuration Example.

Figure 5



9. Make sure that **EAP-GTC** and **EAP-MSCHAPv2** are checked under *Allow inner methods*. Figure 5 shows a sample configuration of steps 8 and 9.

Verify

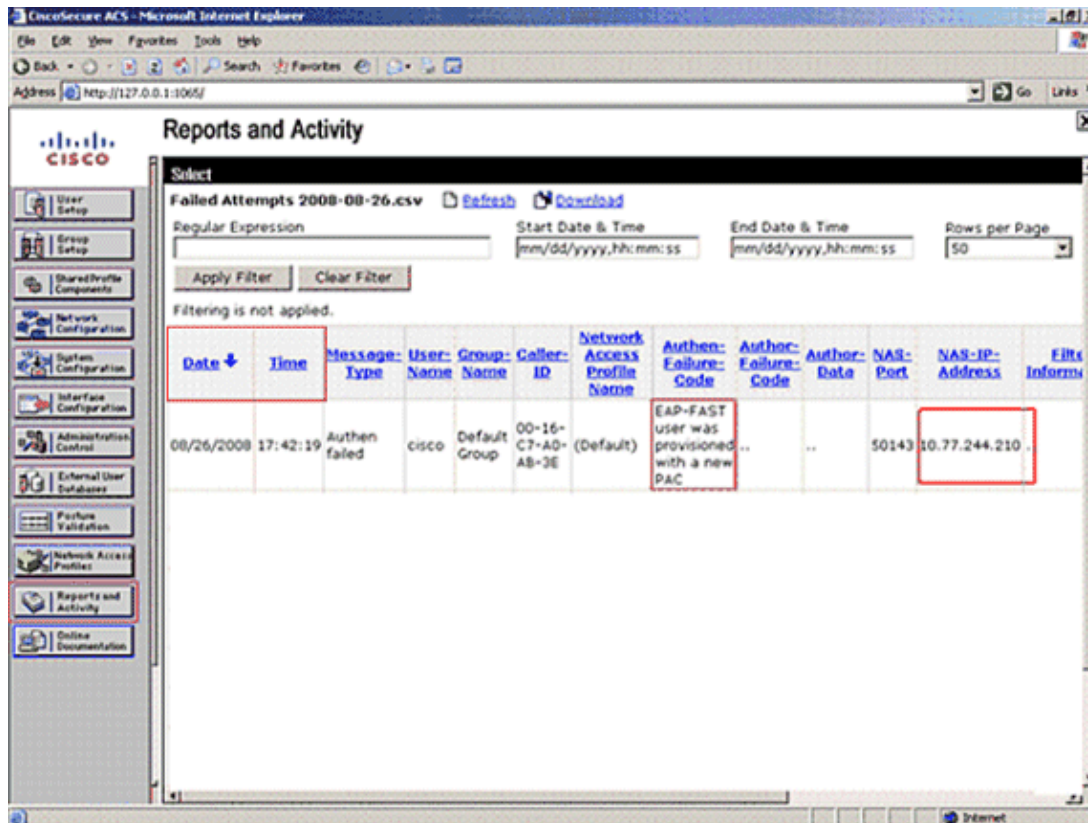
Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Once 802.1x is enabled on the switch port, all the traffic except the 802.1x traffic is blocked through the port. The LAP, which is already registered to the WLC, gets disassociated. Only after a successful 802.1x authentication is other traffic allowed to pass through. Successful registration of the LAP to the WLC after the 802.1x is enabled on the switch indicates that the LAP authentication is successful.

You can also check this from ACS. From the ACS main screen, click the **Reports and Authentication** menu. Click the **Failed Attempts** option. If the authentication is successful, you find an *Authentication failed* message with the code *EAP-FAST user was provisioned with a new PAC with IP address of the switch* in the NAS-IP-Address field as shown in Figure 6. You can also confirm with the Date and Time of authentication.

Figure 6



Troubleshoot

Use this section to troubleshoot your configuration.

1. Use the **ping** command and check if the ACS server is reachable from the switch.
2. Make sure that the switch is configured as a AAA client on the ACS server.
3. Ensure that the shared secret is the same between switch and the ACS server.
4. Check if EAP-FAST is enabled on the ACS server.
5. Check for the software compliance on the devices.
6. Check if the 802.1x credentials are configured for the LAP and are same on the ACS server.

Note: The username and password are case sensitive.

Troubleshooting Commands

There are currently no debug commands available for this feature.

Related Information

- [Controlling Lightweight Access Points](#)
- [Configuring IEEE 802.1x Port-Based Authentication](#)
- [Technical Support & Documentation – Cisco Systems](#)

