



Lab 7.1.9 Configure EAP on Cisco ACS for Windows

Estimated Time: 20 minutes

Number of Team Members: Two teams with four students per team.

Objective

In this lab, students will learn the following objectives:

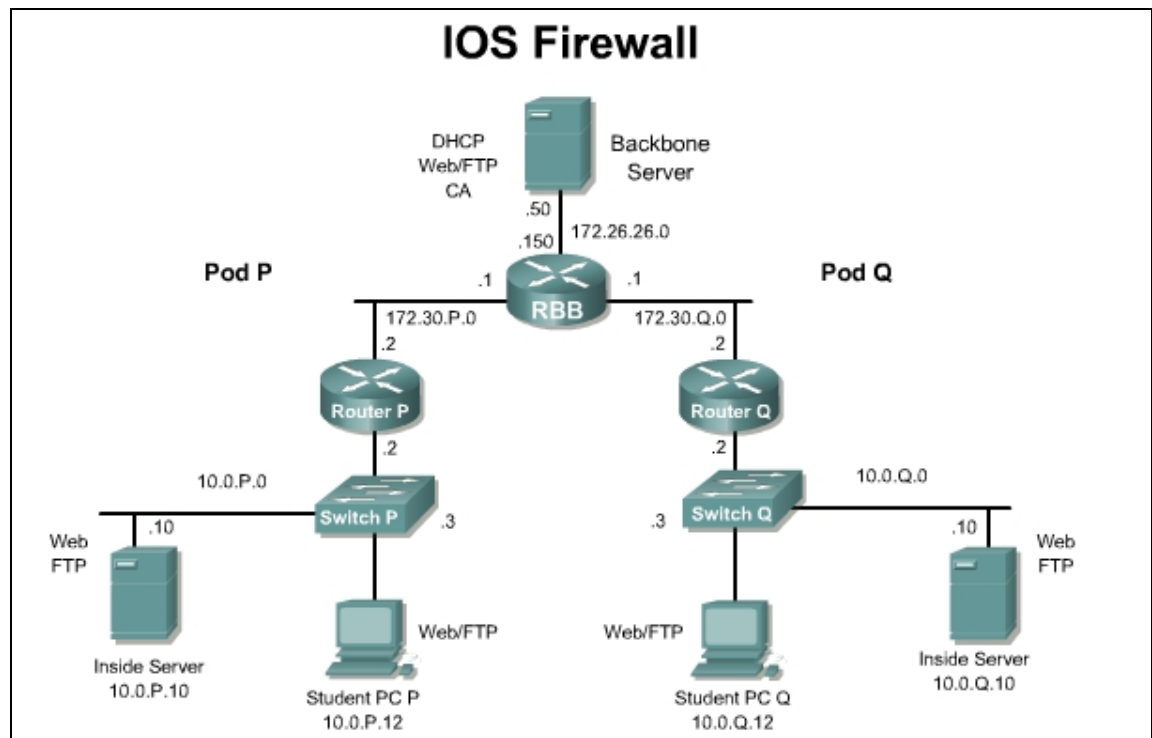
- Obtain a certificate for the ACS server.
- Configure ACS to use a certificate from storage.
- Specify additional certificate authorities that the ACS should trust.
- Restart the service and configure EAP settings on the ACS.
- Specify and configure the access point as an AAA client.
- Configure the external user databases.
- Restart the service.

Scenario

The XYZ company would like to implement 802.1x authentication on the corporate network. Before the 2950 switches can be configured to support 802.1x authentication of network clients, a RADIUS authentication server must be put in place. In this activity, students will configure Extensible Authentication Protocol (EAP) with Cisco Secure ACS for Windows so that it can be used as an authentication server in the 802.1x implementation.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod switch. Access the pod switch console port using the terminal emulator on the Windows 2000 server. If desired, save the switch configuration to a text file for later analysis. Refer back to the *Student Lab Orientation* if more help is needed.

A server certificate must be available for the Cisco Secure ACS before you can install it. With Cisco Secure ACS, certificate files must be in Base64-encoded X.509. If a server certificate is not already in storage, the procedure in Step 1 can be used to create a certificate for installation. The Cisco Secure ACS can be used to generate a self-signed digital certificate to be used for PEAP authentication protocol or for HTTPS support of Cisco Secure ACS administration. This capability supports TLS/SSL protocols and technologies without the requirement of interacting with a CA.

Tools and resources

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal

Step 1 Generate a Self-signed Certificate

- a. Create a directory for use with certificate.

```
c:>md c:\acs_server_cert
```
- b. In the navigation bar, click **System Configuration**.
- c. Click **ACS Certificate Setup**.
- d. Click **Generate Self-Signed Certificate**.
- e. type in **cn=securacs** in **Certificate Subject**
- f. type in **c:\acs_server_cert\acs_server_cert.cer** in **Certificate File**
- g. type in **c:\acs_server_cert\acs_server_cert.pvk"** in **Private Key File**
- h. type in **secur** for the private key password.
- i. In the Retype private key password box, retype the private key password.
- j. In the Key length box, select the default key length of **2048 bits**.
- k. In the Digest to sign with box, select the **SHA1** hash digest to be used to encrypt the key.
- l. To install the self-signed certificate when you submit the page, select the **Install generated certificate** option.

Note	If the Install generated certificate option is used, the Cisco Secure ACS services must be restarted after submitting this form to adopt the new settings.
-------------	--

Note	If the Install generated certificate option is not selected, the certificate file and private key file are generated and saved when Submit is clicked in the next step, but they are not installed into the local machine storage.
-------------	--

- m. Click **Submit**. The specified certificate and private key files are generated and stored, as specified. The certificate becomes operational, if the Install generated certificate option was selected, only after the Cisco Secure ACS is restarted.
- n. To restart the Cisco Secure ACS services, Click on **System Configuration** then **Service Control**, and then click on the **Restart** button.

Step 2 Configure EAP Settings

In this step, select and configure how Cisco Secure ACS handles options for authentication. In particular, use this procedure to specify and configure the varieties of EAP that are allowed, and to specify whether to allow either MS-CHAP Version 1 or MS-CHAP Version 2, or both.

- a. In the navigation bar, click **System Configuration**.
- b. Click **Global Authentication Setup**.
- c. Make sure **Allow EAP-MD5** is checked.
- d. Click **Submit**.

Note	To save any changes to the settings that have been made but are to be implemented later, click Submit . The Cisco Secure ACS services can be restarted at any time by using the Service Control page in the System Configuration section.
-------------	--

Step 3 Specify the Switch as a AAA Client

- a. Click on Network Configuration button.
- b. Click on **(Not Assigned)** under Device Groups.
- c. Click on **Add Entry** in the AAA client window.
- d. Input the following:
 - i. IP address of the pod switch, **10.0.P.3**
(Where P = pod number)
 - ii. key = **secretkey**
 - iii. authenticate using **RADIUS (IETF)**
- e. Click **Submit**. The hostname now appears in the AAA Clients window.

Step 4 Restart the Cisco Secure ACS Service

- a. Click on **System Configuration** then **Service Control**.
- b. Click on **Restart**.