Lab 8.4.5.2 Configuring LEAP/EAP using Cisco Secure ACS (OPTIONAL)

Estimated Time: 60 minutes

Number of Team Members: Students can work in teams of two.

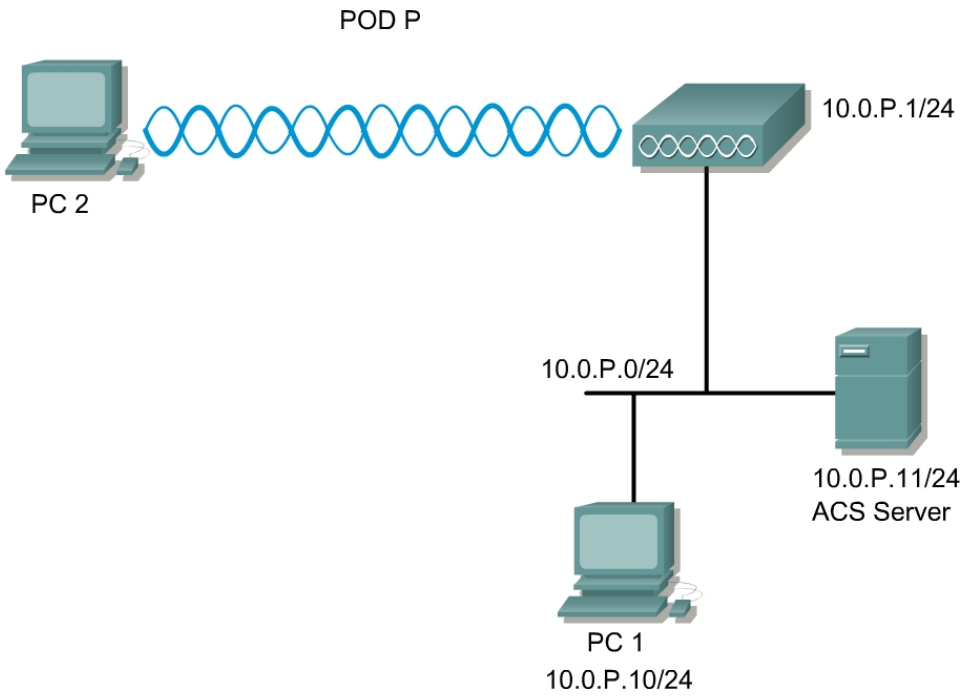
Objective

In this lab, the student will learn about the second generation of Wireless LAN security and how to implement LEAP on a Wireless LAN for secure client authentication.

The main steps to this lab are:

1. Install Cisco Secure ACS software (Instructor)
2. Configure the Cisco Secure ACS software
3. Create user accounts in the Access Control Server (ACS)
4. Configure AP WEP Key or Cipher
5. Configure LEAP/EAP on the AP
6. Configure LEAP/EAP on the client (PC2) through ACU
7. Monitor the connection and login

Topology



Scenario

One way to secure wireless LANs and improve network security is to use authentication for accessing the AP. Wireless clients can use Extensible Authentication Protocol (EAP) to authenticate though a wireless LAN. EAP can authenticate through digital certificates such as public key infrastructure (PKI) or passwords and usernames. EAP can pass authentication information onto an Authentication, Authorization, Accounting (AAA) RADIUS server, such as a Cisco Access Control Server (ACS).

The Network Authentication Process can be summarized in four main stages:

- The client adapter uses the username and password to start the authentication process.
- The AP communicates with the EAP-compliant RADIUS server to authenticate the username and password.
- If the username and password are valid, the RADIUS server and the client adapter negotiate a dynamic, session-based Wired Equivalent Privacy (WEP) key. The key, which is unique for the authenticated client, provides the client with secure network access.
- The client and AP use the WEP key for all data transmissions during the session.

Preparation

Prior to this lab, the Cisco Aironet AP should be configured to allow clients to associate. The IP address, hostname and SSID should be configured on the AP. A PC should be installed with a Cisco Aironet Client Card, and it should already be associated to the AP.

Cable the equipment according to the Topology.

A Windows 2000 Server running ACS 2.6 or above must be available.

Update the Aironet Client Utility version 6.0 or later.

Tools and Resources

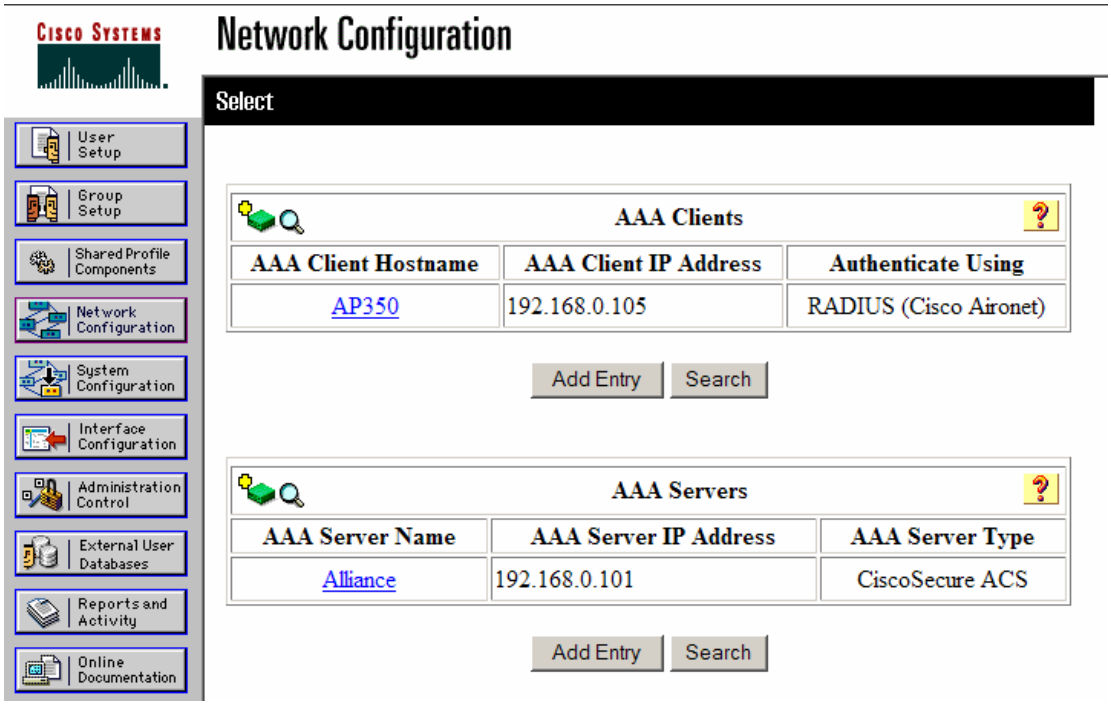
Each team of students will require the following:

- Cisco Aironet AP
- Hub or switch
- A wireless PC, laptop, or handheld (PC2) with a Cisco Aironet Client Adapter Card and utility properly installed and configured.
- Windows 2000 Server running Cisco Secure ACS 2.6 or above.
- One wired PC (PC1)

An evaluation copy of Cisco Secure ACS can be downloaded from the following link:

http://www.cisco.com/cgi-bin/tablebuild.pl/acs-win-3des

Step 1 Add a AAA client

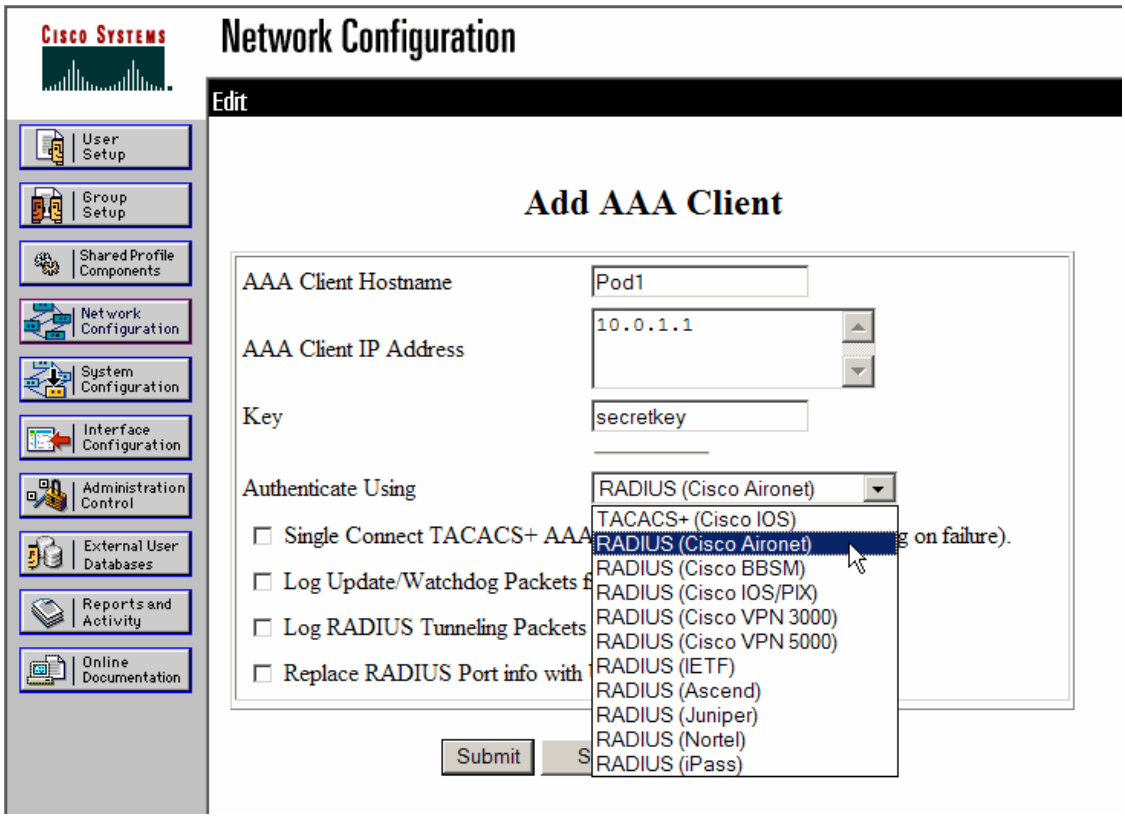


Follow these steps to include the AP as a **AAA Client** in Cisco Secure ACS:

a. After properly loading the TACACS software on the Windows Server computer, on the ACS main menu, click **Network Configuration**.

b. Click **Add New Access Server**, or it may display **Add Entry**.

Step 2 Configure AAA Client



a. In the **Network Access Server Hostname** box, type the system name of the AP. Enter ***PodP*** (where **P** is the Pod number)

b. In the **Network Access Server IP address** box, type the AP IP address. Enter **10.0.P.1** (where P is the Pod number)

c. In the **Key** box, type the shared secret that the AP and Cisco Secure ACS use to encrypt the data. For correct operation, the identical key, which is case sensitive, must be configured on the AP. For simplicity of the lab, use the word ***secretkey***.

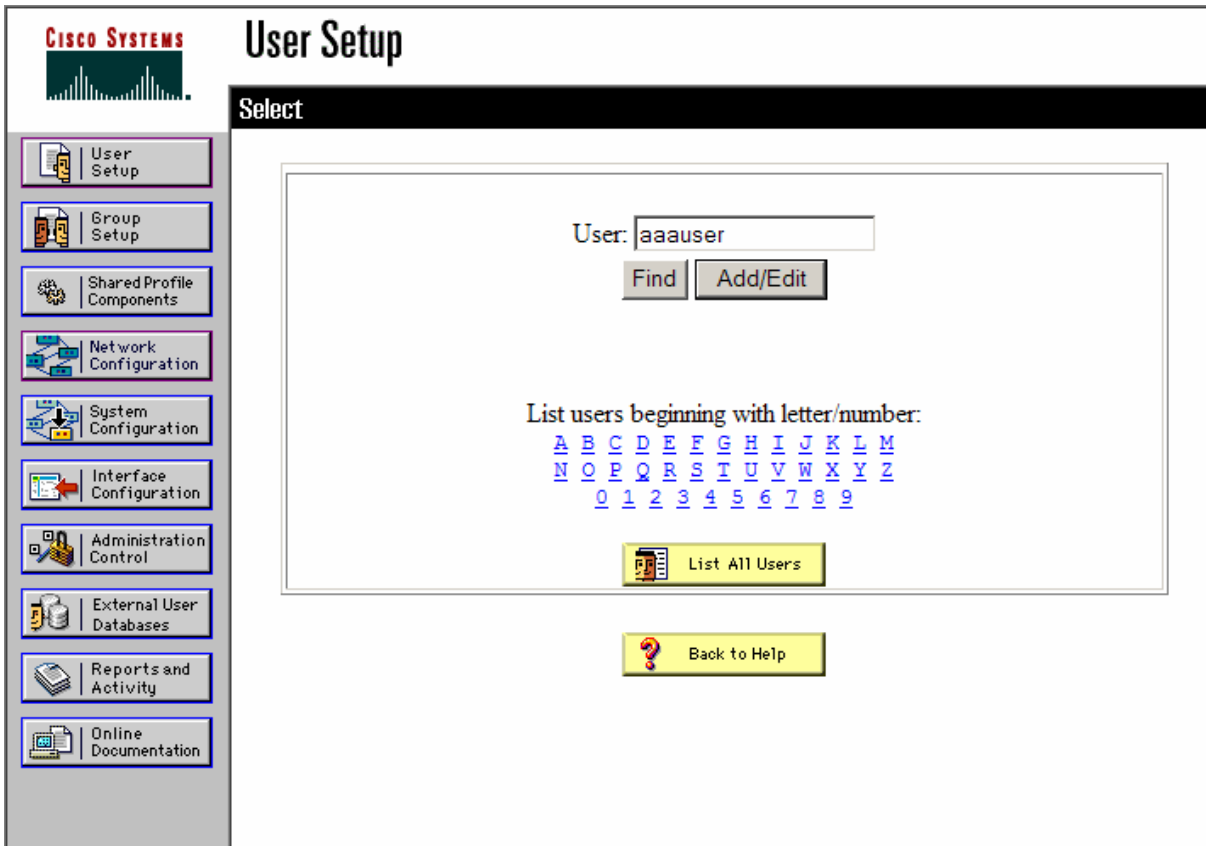
d. From the **Authenticate Using** list box, click the network security protocol. Select **RADIUS (Cisco Aironet**).

e. Each AP in the class will have to be added to this list if it will be using LEAP.

f. Remote Access Services must be started on the RADIUS Server for LEAP to work properly. To save the changes and apply them immediately, click the **Submit + Restart** button.

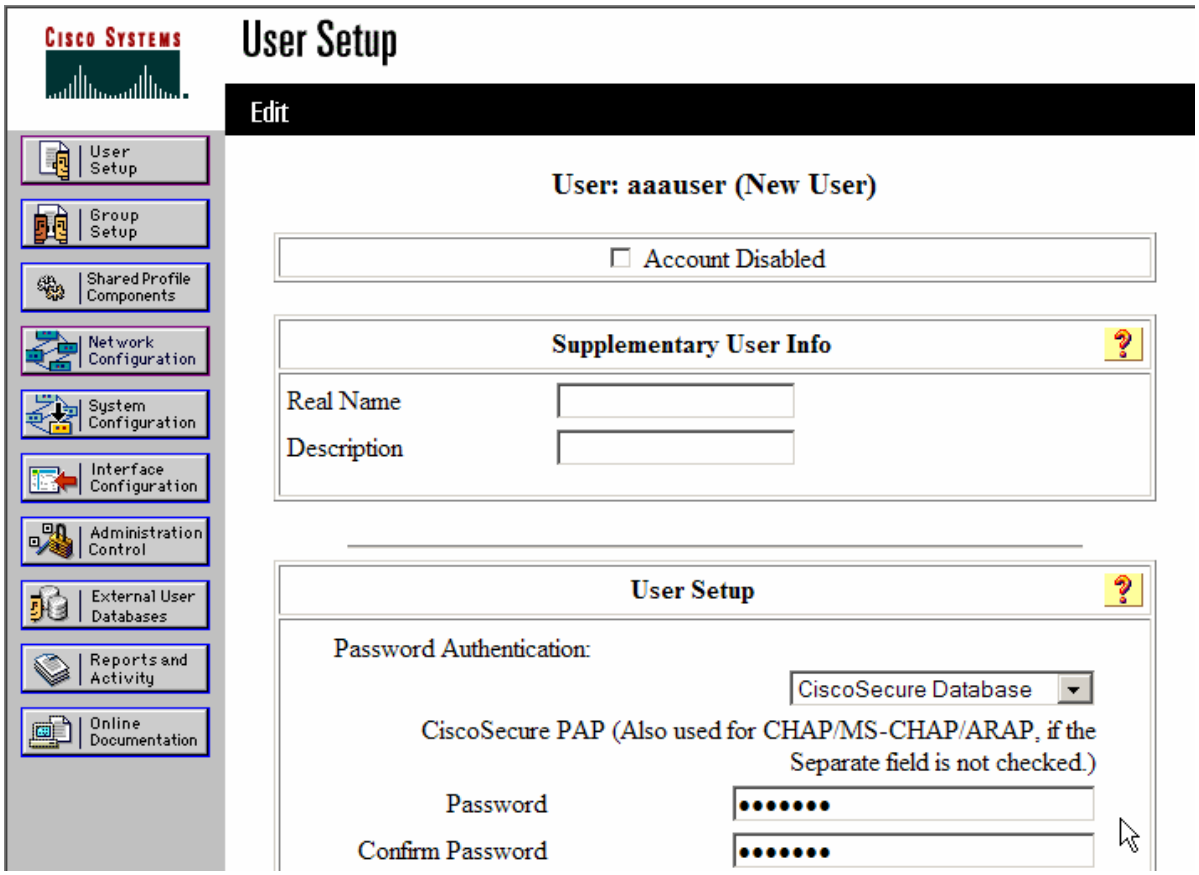
Note	It is very important to click **Submit + Restart**

Step 3 Create a user account in the Access Control Server (ACS)



a. Click on the **User Setup** button located on the left side of the ACS Home page.

b. Type the user name ***aaauser*** in the **User**: field box, and then click on the **Add/Edit** button beneath this box.

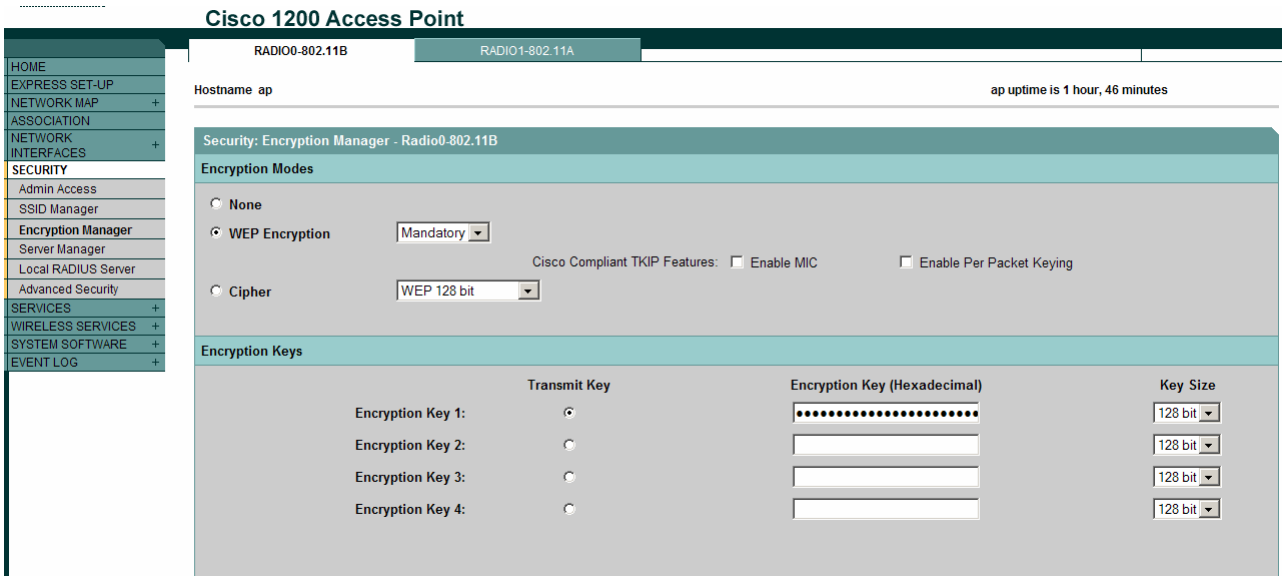


c. Type the user password ***aaapass*** in the Password: box and then type ***aaapass*** in the Confirm Password: box.

d. Click on the **Submit** button to add this entry to the user list.

e. Additional users can be added to this database list for each wireless PC client.

Step 4 Configure the AP WEP Keys or Cipher



In order to enable Cisco LEAP on the AP, WEP Encryption or a Cipher must be enabled.

a. From the **SECURITY>Encryption Manager** page of the AP, configure the Encryption Key 1.

b. Click on the WEP Encryption radio button.

c. Select Mandatory.

d. Click **Apply-All**.

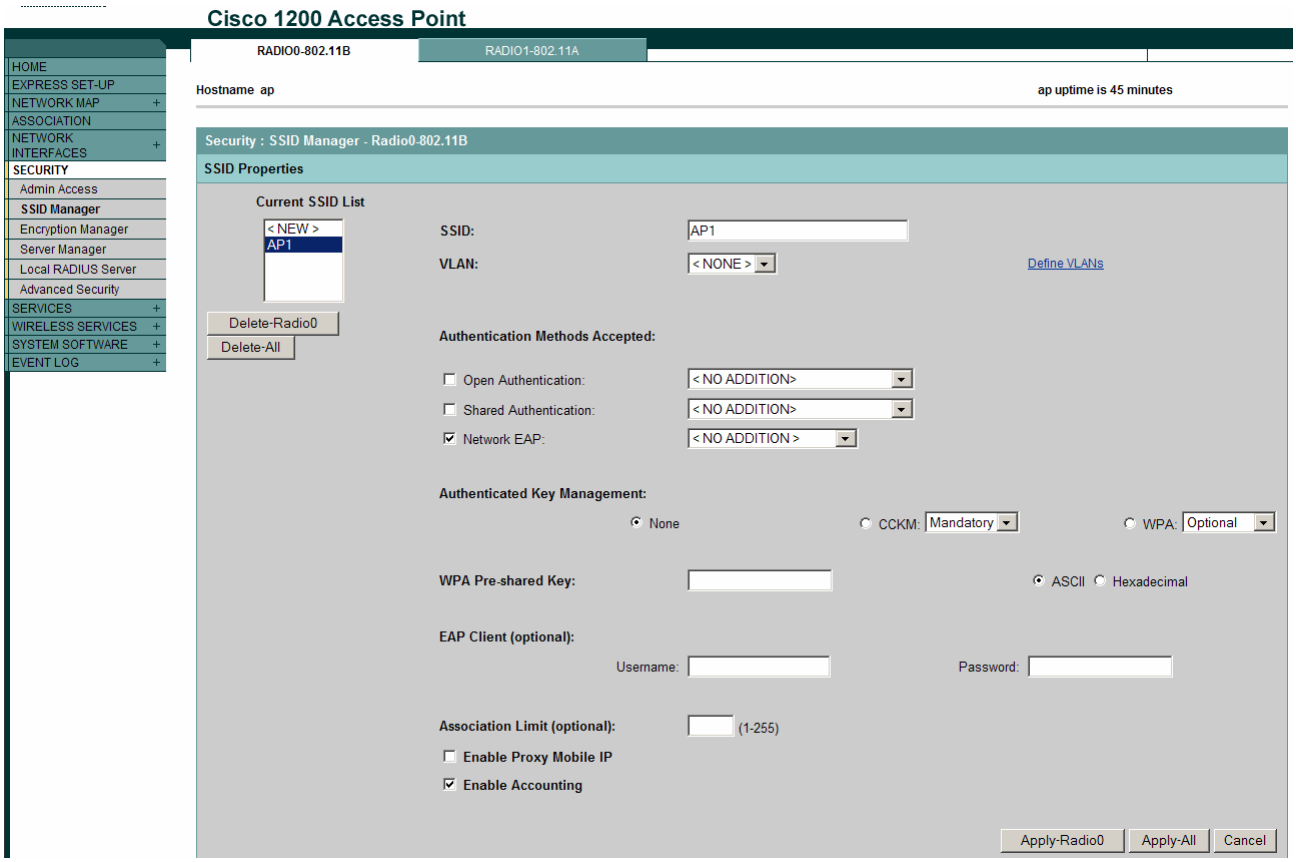
e. **The Cipher** option can be used for greater security. What options are available?

_____

_____

_____

Step 5 Configure authentication on AP



In order to enable Cisco LEAP on the AP, complete the following steps to configure the Authentication Method:

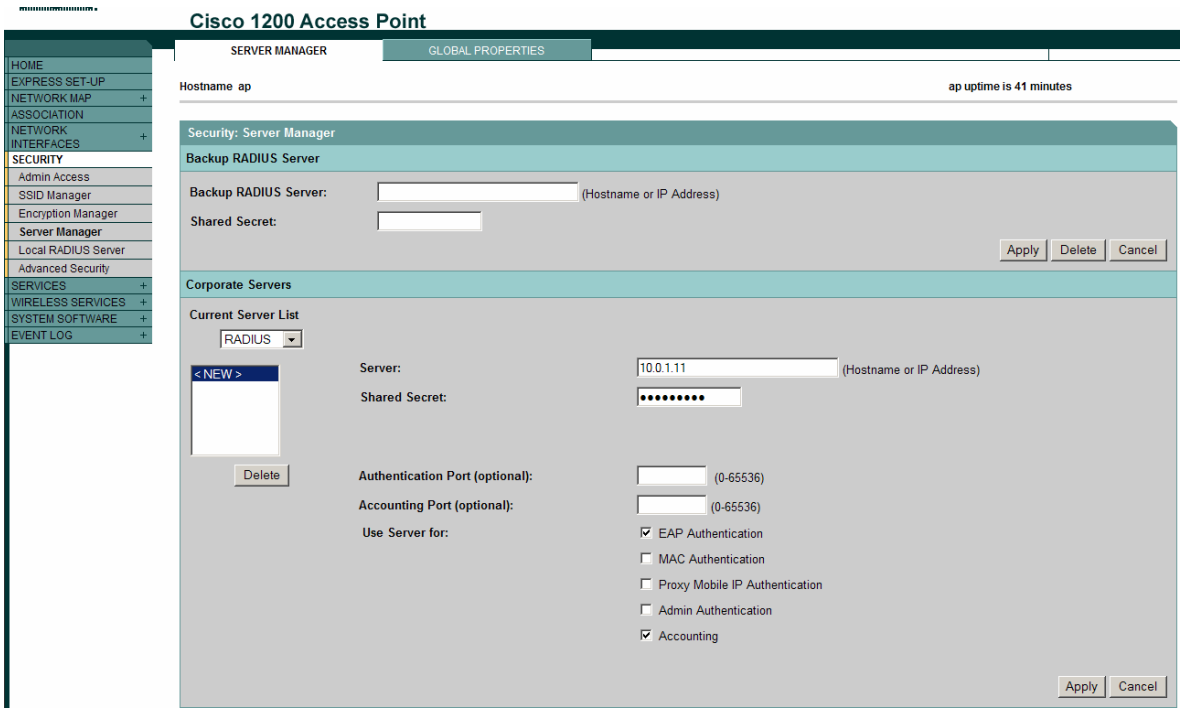
a. On the **SECURITY>SSID Manager** page of the AP, create a new SSID of AP**P** (where **P** is the Pod number)

b. Check the **Network EAP** box.

c. Check the **Enable Accounting** box.

d. Click the **Apply-All** button.

Step 6 AP RADIUS configuration



In order to enable Cisco LEAP on the AP, complete the following steps to configure a RADIUS Server from the SECURITY>**Server Manager** Page:

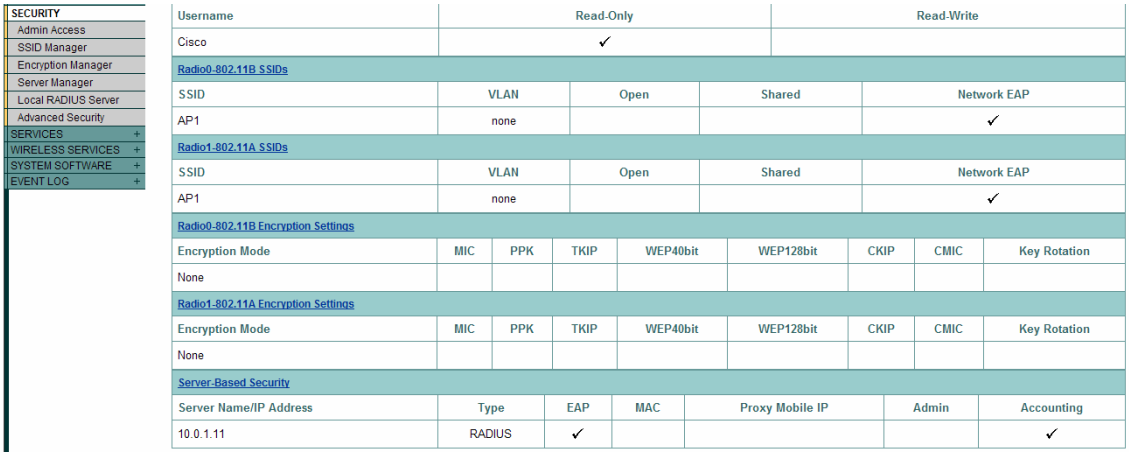
a. Enter the IP address of the RADIUS server in the Server Name/IP entry field. This will be the IP address of the Windows Server where the ACS software is running. Should be 10.0.P.11.

b. Enter the port number the RADIUS server uses for authentication. This will default to port **1645** if the field is left empty.

c. Enter the shared secret used by the RADIUS server in the Shared Secret entry field. This was configured as ***secretkey*** on ACS. The shared secret on the AP must match the shared secret on the RADIUS server.

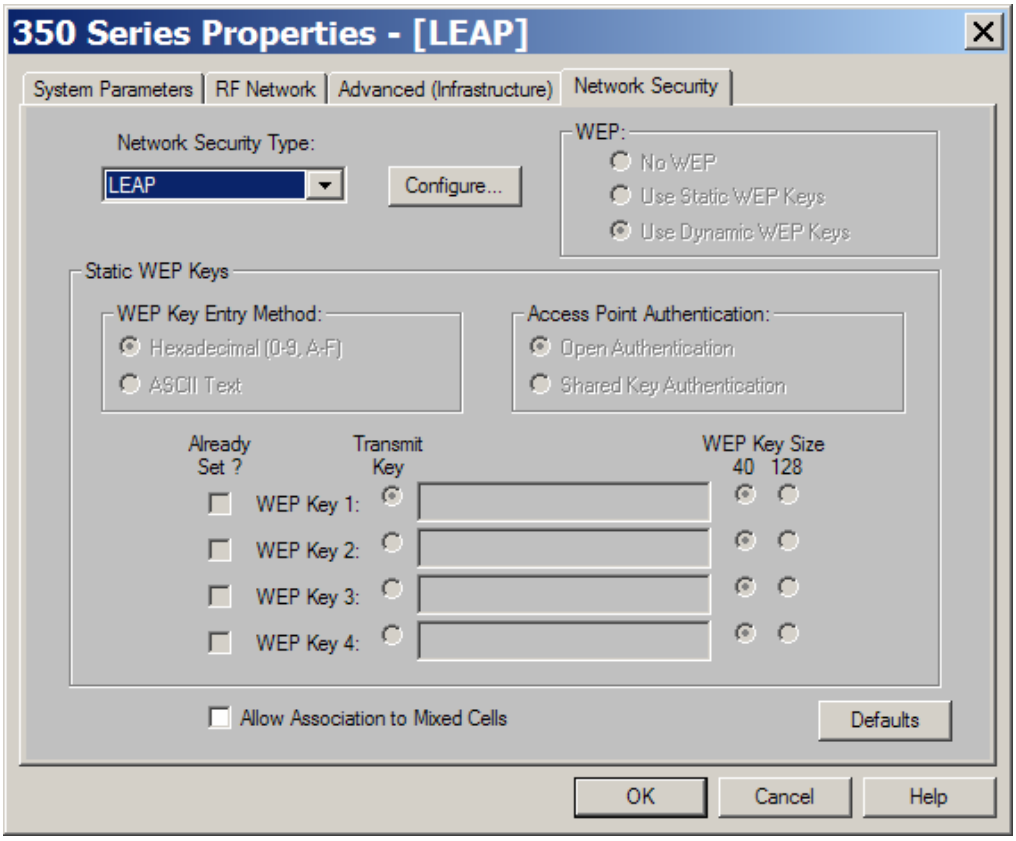
d. Check the **EAP Authentication** and **Accounting** box.

e. Click the APPLY button.



e. From the **SECURITY** Home page of the AP, verify Network EAP is checked and the only SSID. The default tsunami SSID should be deleted for security. Also verify the Server Based Security is configured correctly as shown.

Step 7 Configuring LEAP on the ACU



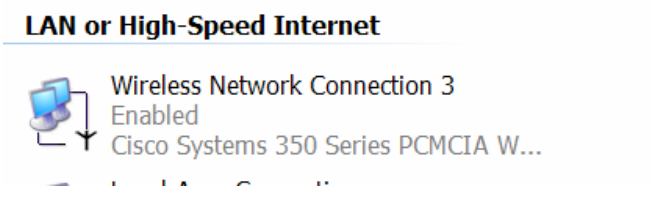
In order to enable the EAP in the Aironet client utility, complete the following steps:

a. On PC2, configure the TCP/IP settings for the **Wireless Network Connection** if a DHCP server is not available. Otherwise, when the client authenticates, the wireless PC will not be able to communicate through IP.

   i. IP address of 10.0.P.12

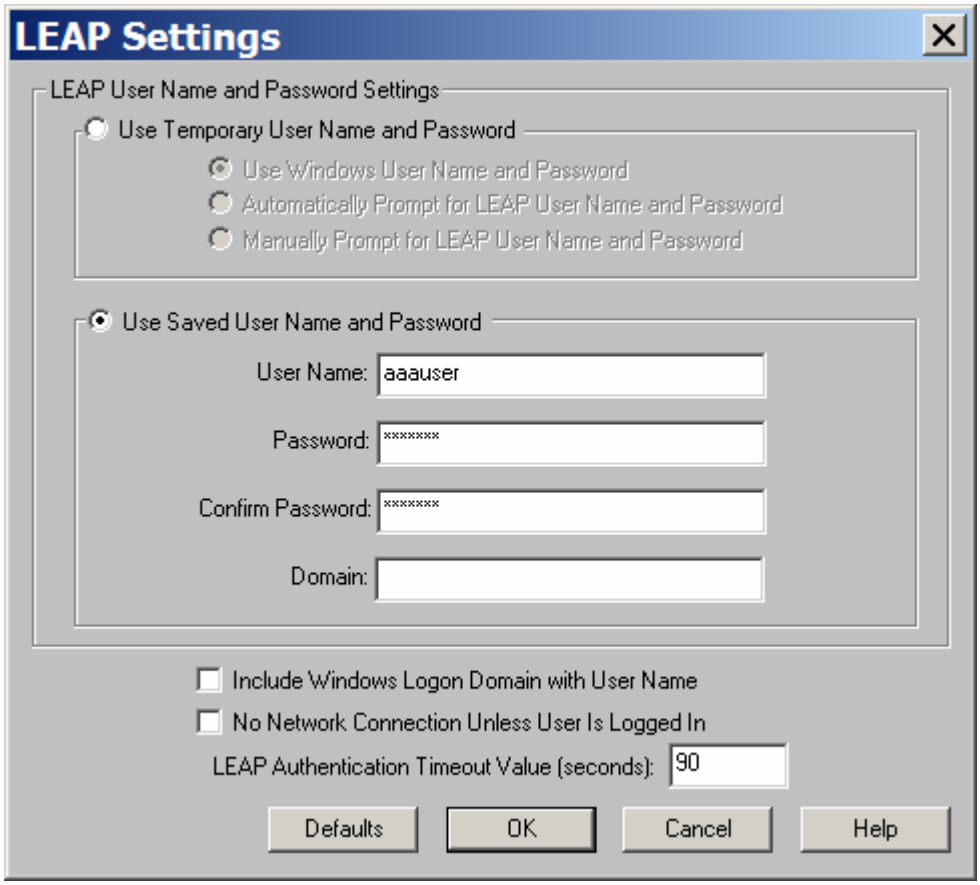
   ii. Subnet mask of 255.255.255.0

   iii. Gateway of 10.0.P.254



b. Go to the **Network Security** tab in the Aironet Client Utility on PC2 and each of the wireless client computers.

c. Select the **LEAP** from the **Network Security Type:** drop down list and click **Configure**.



d. Click on **Use Saved User Name and Password**

   i. Enter ***aaauser*** for the **User Name**

   ii. Enter ***aaapass*** for the **Password**

   iii. Enter ***aaapass*** for the **Confirm Password**

   iv. Uncheck the two checkboxes at the bottom of the LEAP Settings window

   v. Click **OK**.

e. In the profile manager, select the profile which LEAP is configured on and click OK. If a save username and password was not configured, an authentication screen should come up asking for a user ID and password. Type in the following.

   i. The username for authentication is ***aaauser***.

   ii. The password for authentication is ***aaapass***.

f. From PC1, PC2 or the ACS Server, browse to the AP **ASSOCIATION** page to verify the connection.

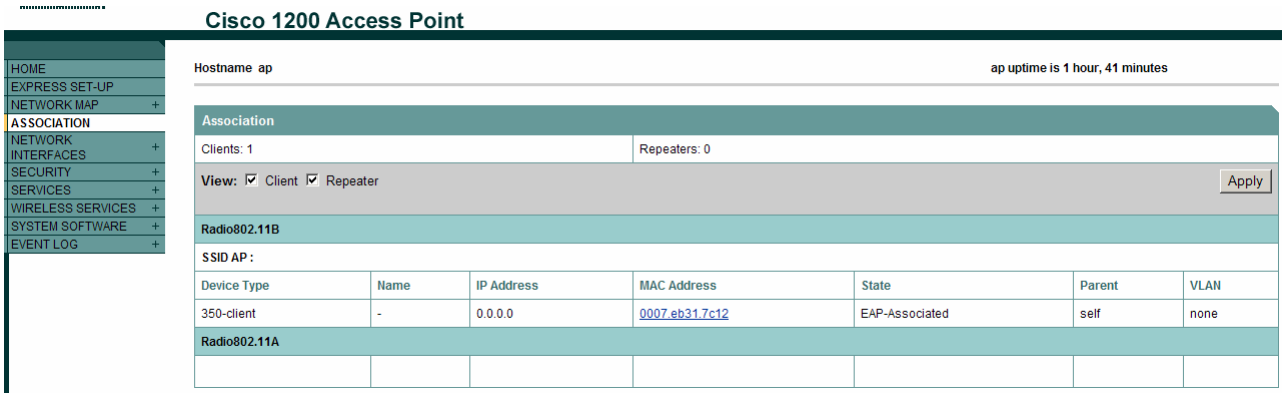
g. What are the three authentication states?

_____

_____

_____

Step 8 Verify connection

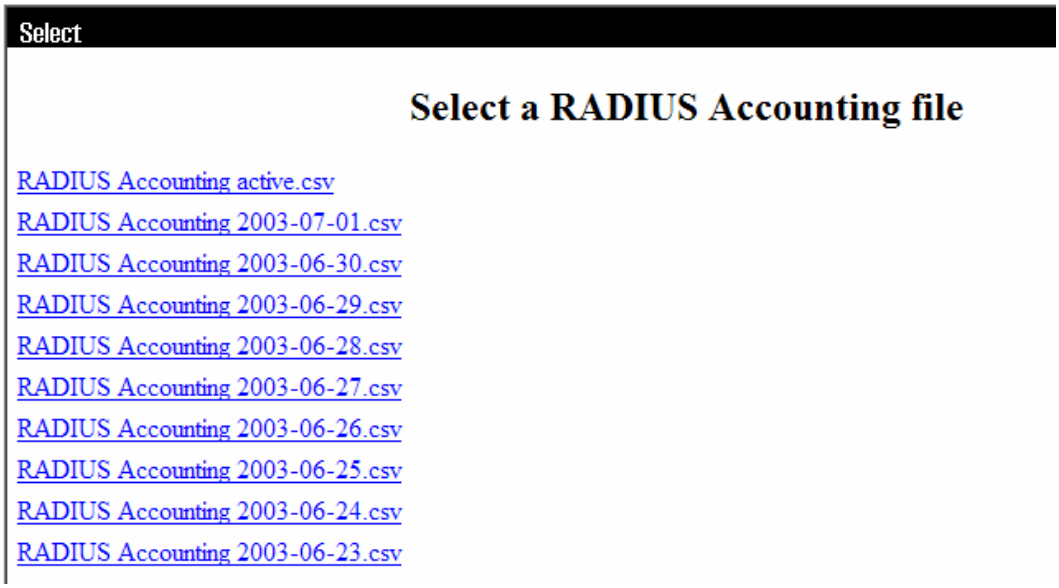


From the ASSOCIATION page of the AP, verify the association state. This should display all of the connected clients.

Step 9 Monitoring LEAP login on ACS (Optional)

a. Click on the **Reports and Activity** button located on the left side of the ACS Home page.

b. Next, click on the RADIUS Accounting link.



c. On the right hand side, select the **RADIUS Accounting active.csv** link.

d. Fill in the information found in the accounting file below.

