Lab 8.4.5.1 Configuring LEAP/EAP using Local RADIUS Authentication

Estimated Time: 40 minutes

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

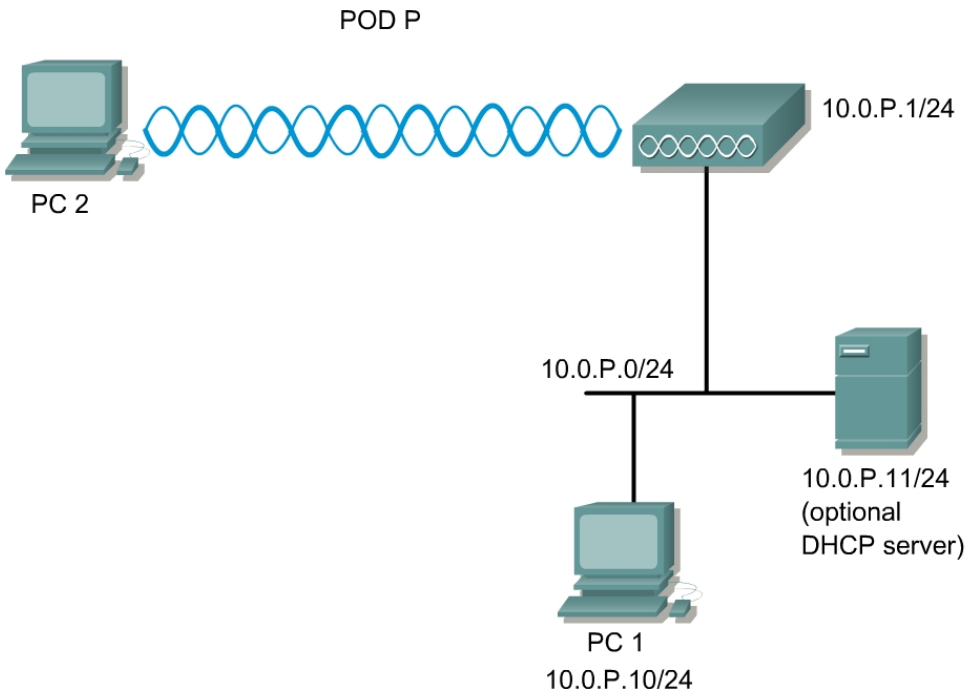
Objective

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. Configure AP WEP Key or Cipher
2. Configure RADIUS Server
3. Configure Local RADIUS Server
4. Configure Users
5. Configure and verify LEAP/EAP Authentication on the AP
6. Configure LEAP/EAP on the client (PC2) through ACU
7. Monitor the connection, login, and authentication statistics

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 to a wireless LAN. 802.1x local RADIUS authentication is available on the 1100 and 1200 APs. This allows LEAP/EAP to be used without requiring a Cisco Secure ACS Server. Furthermore, this feature provides a backup for ACS Servers in an Enterprise network.

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.

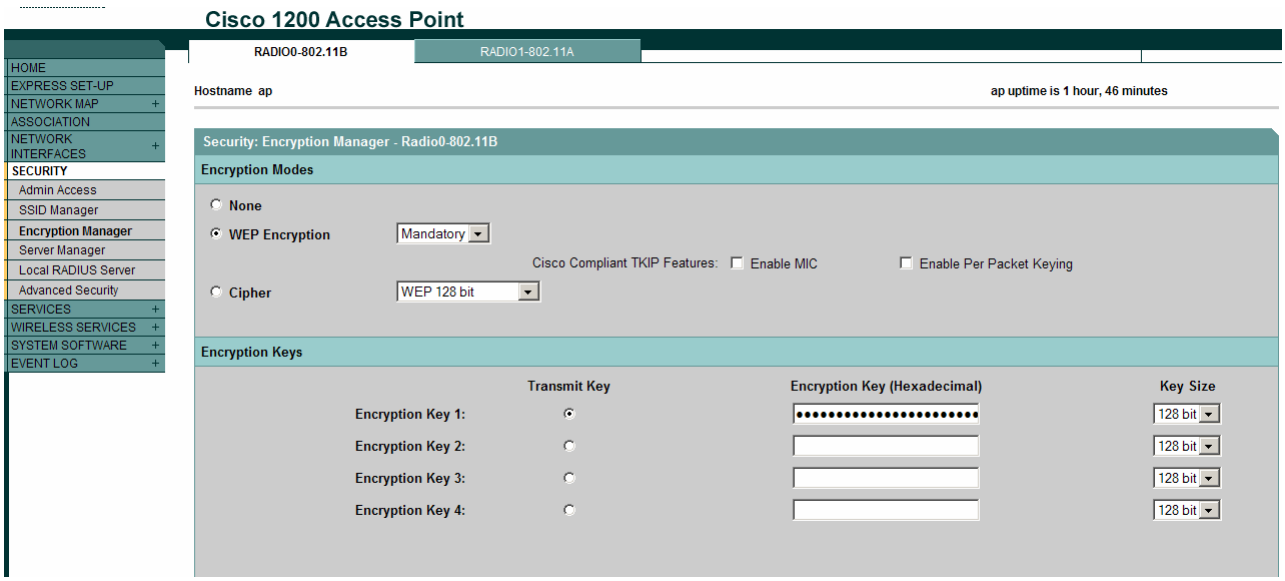
Update the Aironet Client Utility version 6.0 or later.

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.
- One wired PC (PC1)

Step 1 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**.

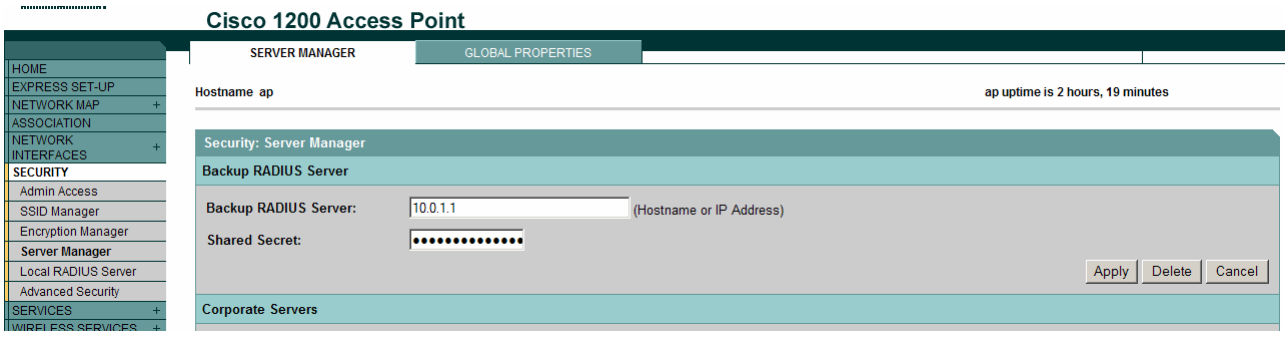
e. The **Cipher** option can be used for greater security. What options are available?

_____

_____

_____

Step 2 Configure RADIUS server



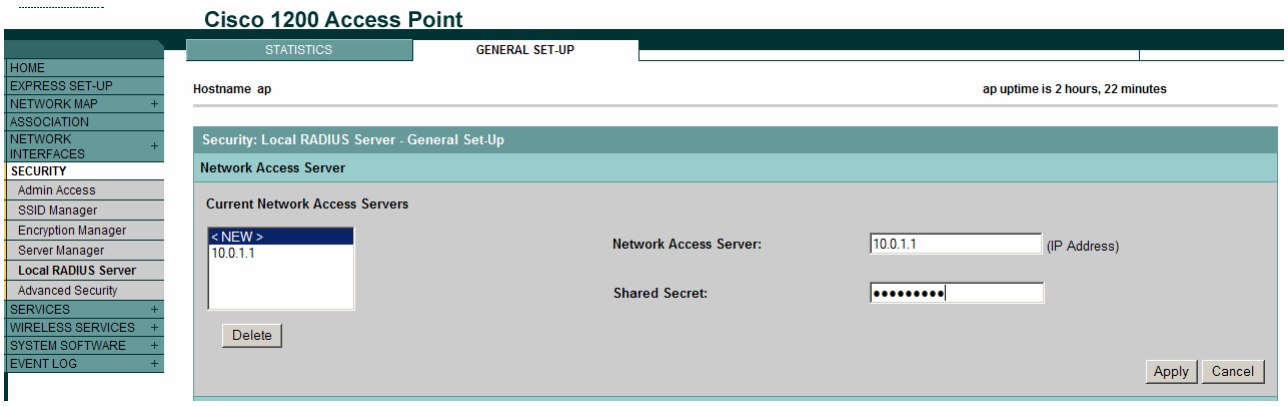
Complete the following steps to configure the Backup RADIUS Server from the **SECURITY>Server Manager** Page:

a. Enter the IP address of the Local RADIUS server in the Server Name/IP entry field. This will be the IP address of the AP where the local RADIUS database is running. Should be 10.0.P.1

b. Enter the Shared Secret key of ***secretkey***

c. Click **Apply.**

Step 3 Configure local RADIUS server



Complete the following steps to configure a Local RADIUS Server from the **SECURITY>Local RADIUS Server** Page:

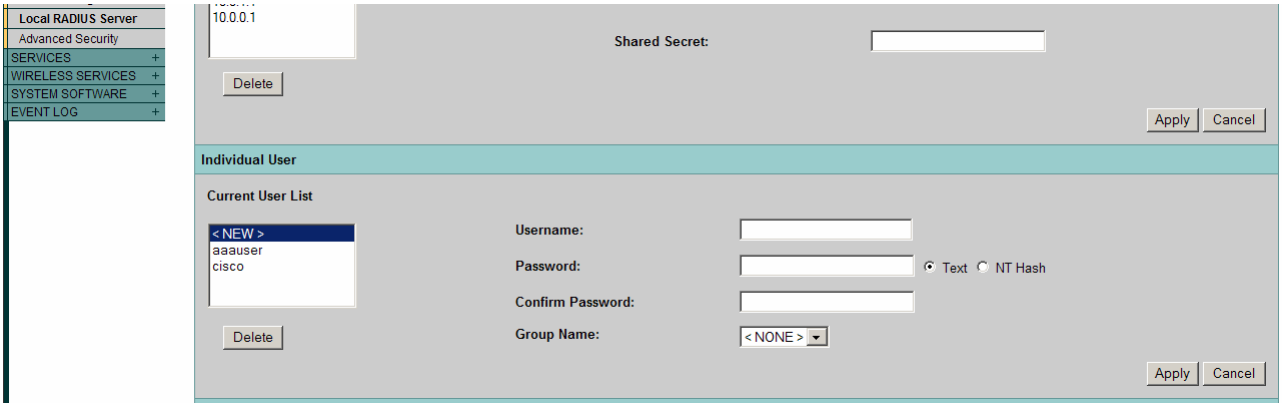
a. Click on the **GENERAL SET-UP** tab.

b. Enter the IP address of the Local RADIUS server in the Server Name/IP entry field. This will be the IP address of the AP where the local RADIUS database is running, 10.0.P.1

c. Enter the Shared Secret key of ***secretkey***

d. Click **Apply.**

Step 4 Configure users



Complete the following steps to configure users from the **SECURITY** > **Local RADIUS Server** Page:

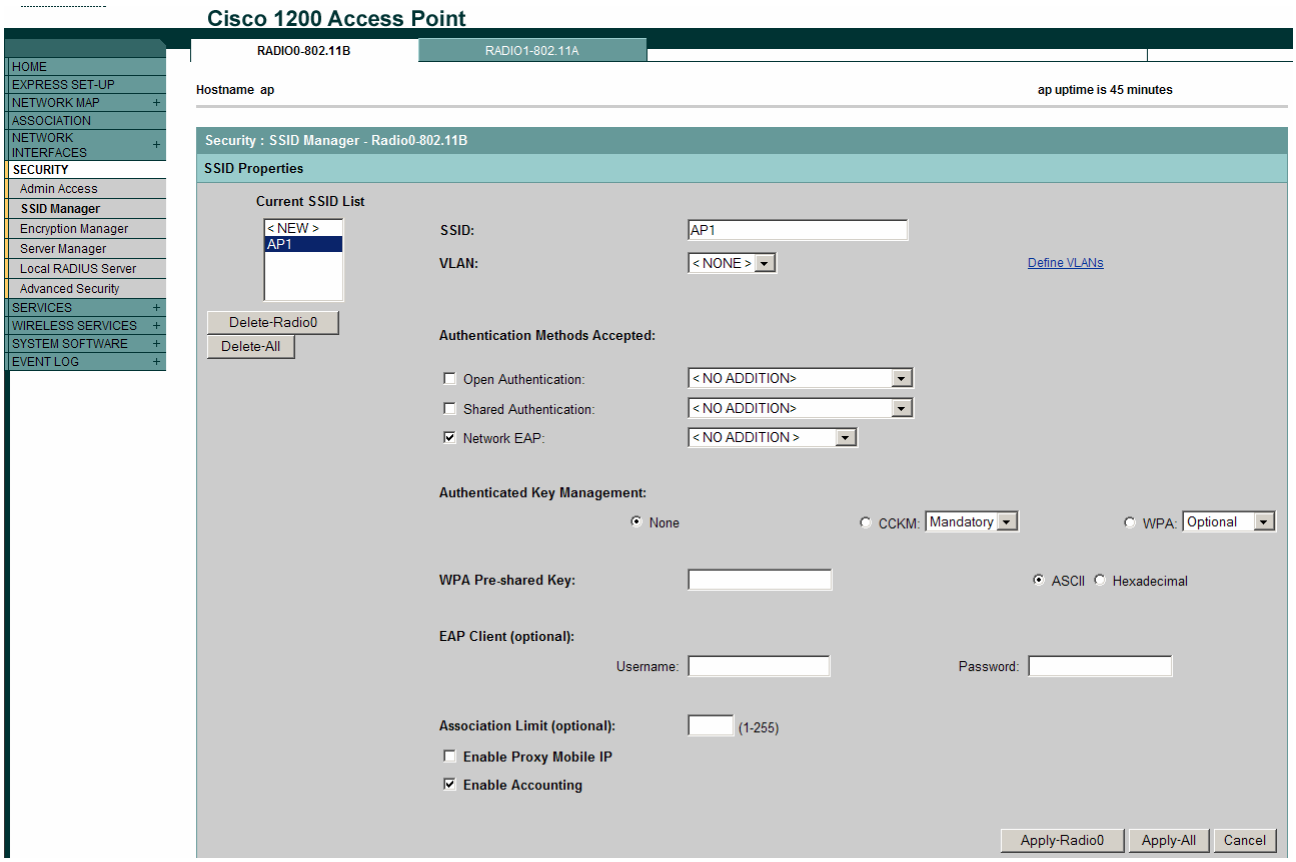
a. Continue from the **GENERAL SET-UP** tab.

b. Enter the following users:

User	Username	Password
1	aaauser	aaapass
2	Cisco1	ciscopass

c. Click **Apply**.

Step 5 Configure authentication on AP



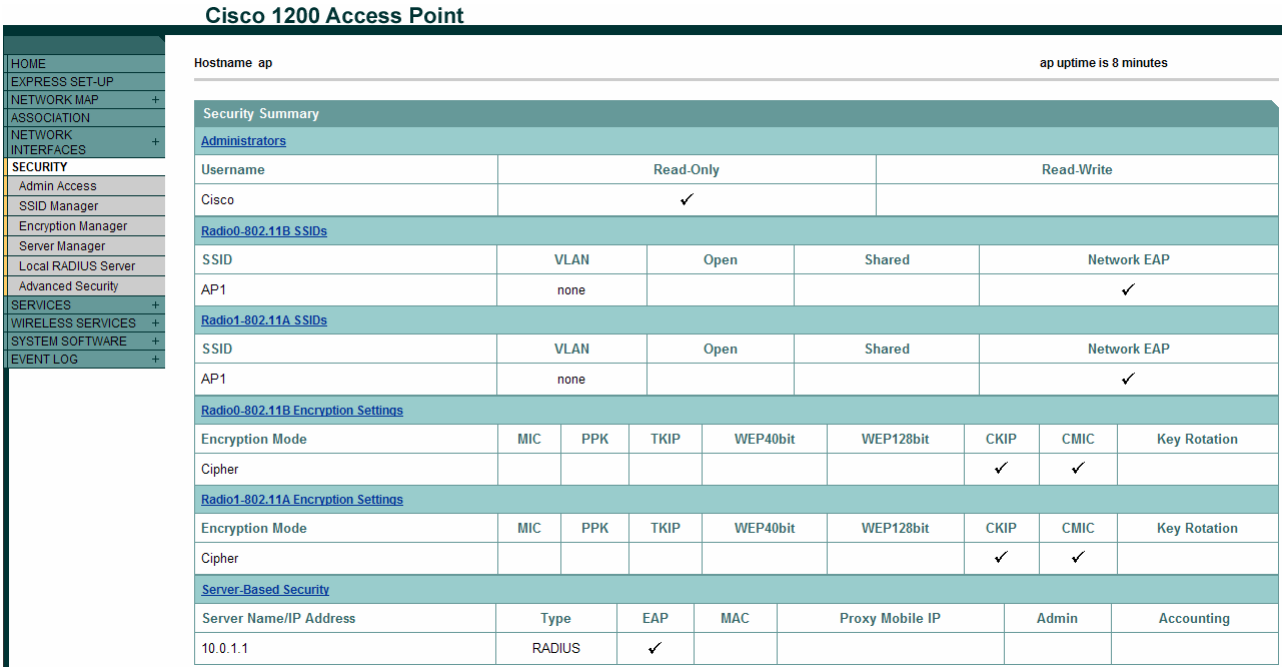
In order to enable Cisco LEAP on the AP, complete the following steps to configure the Authentication Method:

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.

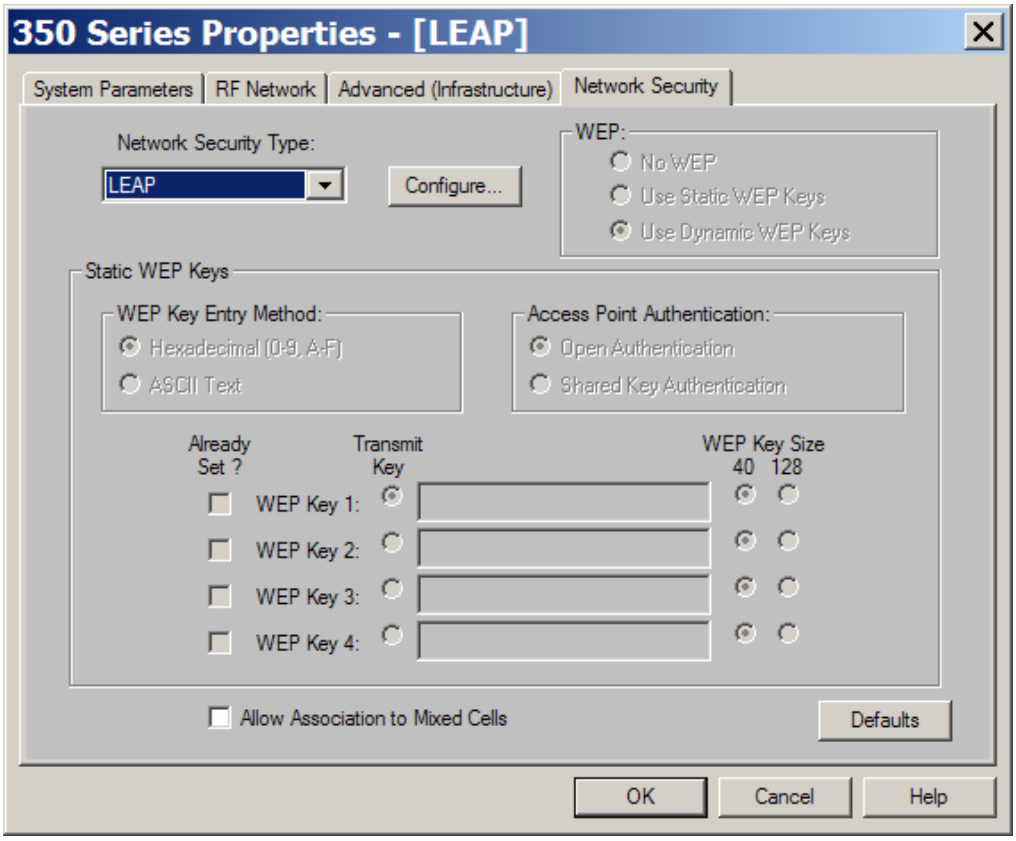
c. Click the **Apply-All** button.

Step 6 Verify the LEAP configuration



From the **SECURITY** Home page of the AP, verify Network EAP is checked and the only SSID is AP**P**. 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



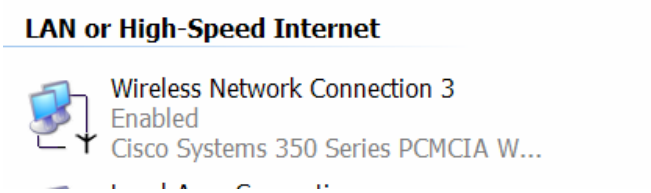
In order to enable the EAP in the Aironet client utility, complete the following steps:

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

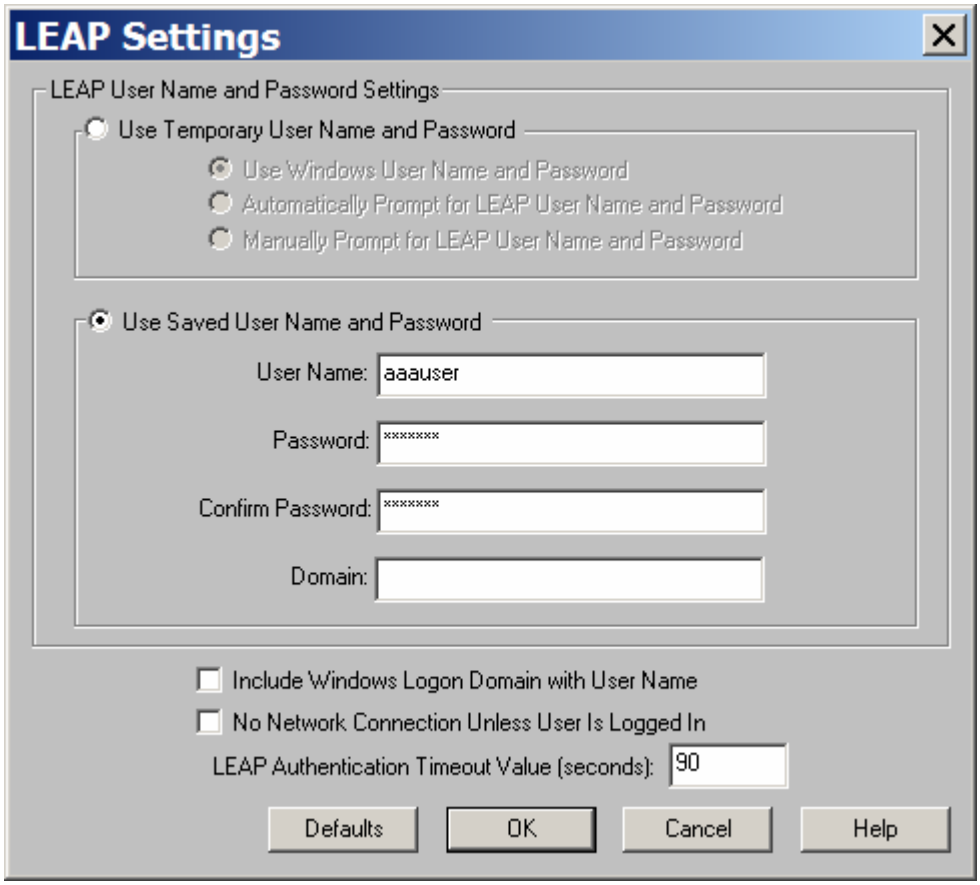
   ii. Subnet mask of 255.255.255.0

   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. The ACM icon should change to green once the authentication is complete.

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

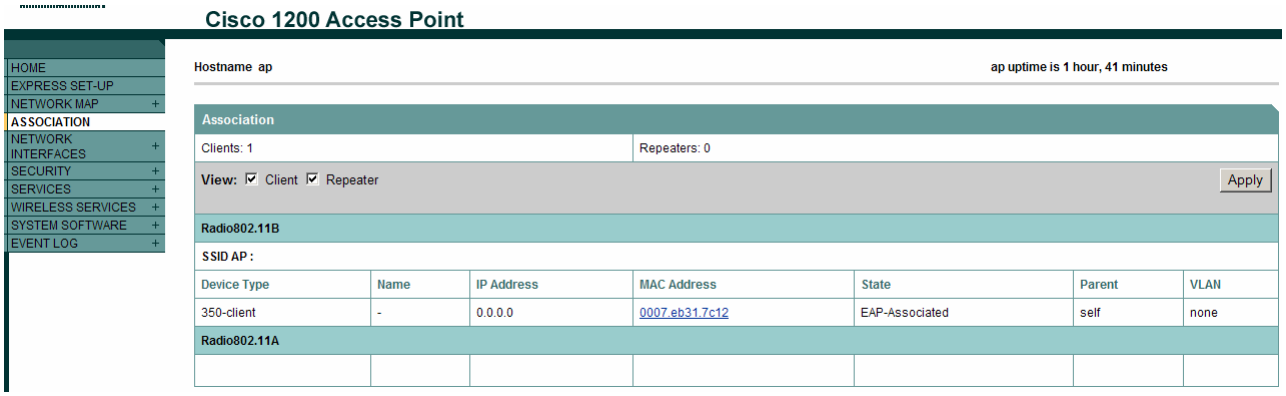
h. What are the three authentication states?

_____

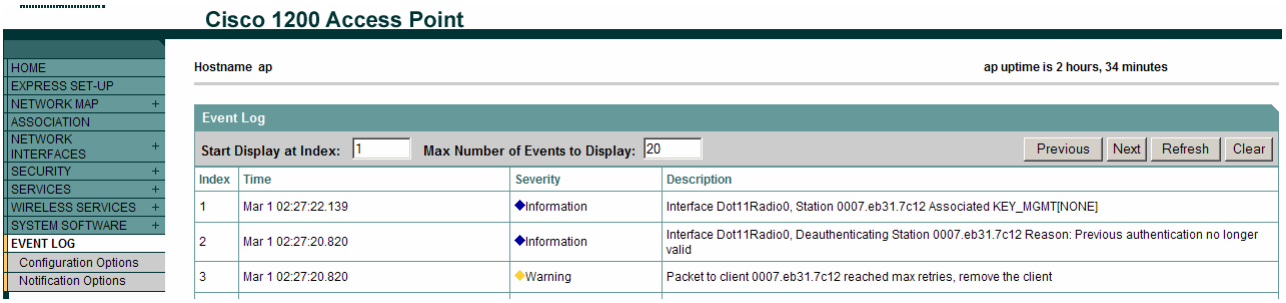
_____

_____

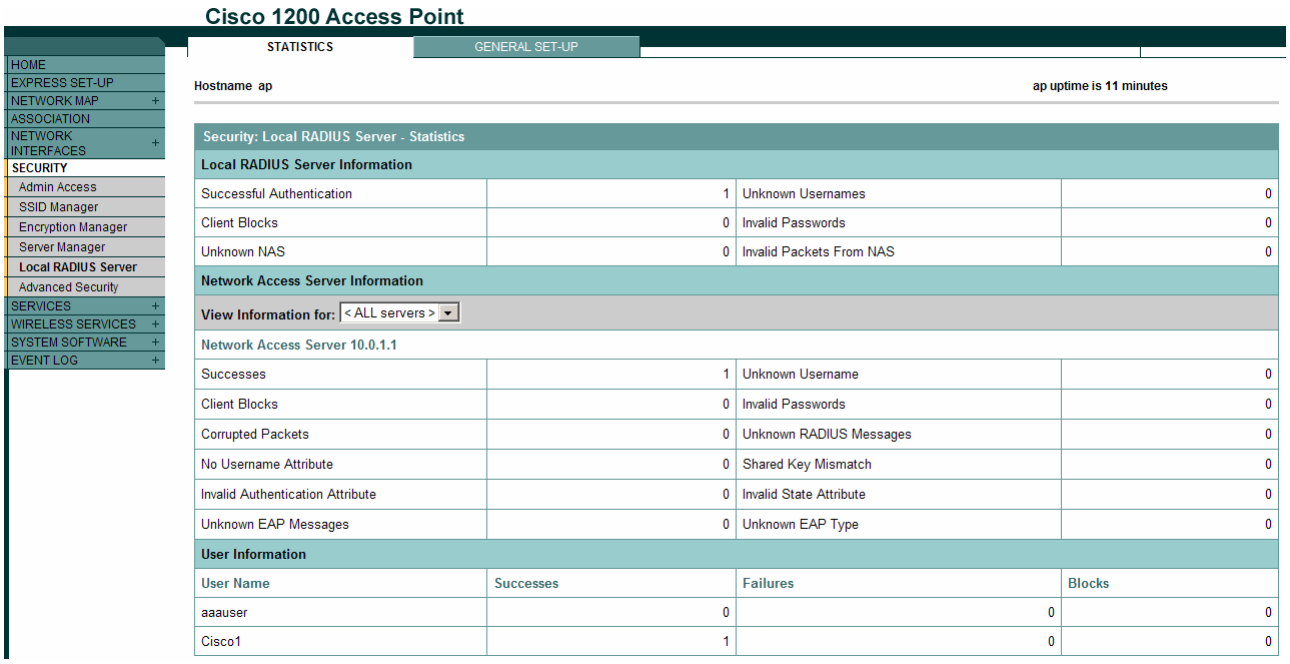
Step 8 Verify the wireless connection



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



From the **EVENT LOG** Page of the AP, check the association logs.



From the **SECURITY>Local RADIUS Server** Page of the AP, click on the **STATISTICS** tab. Verify the User Information for authentication successes, failures, and blocks.

