



## 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.

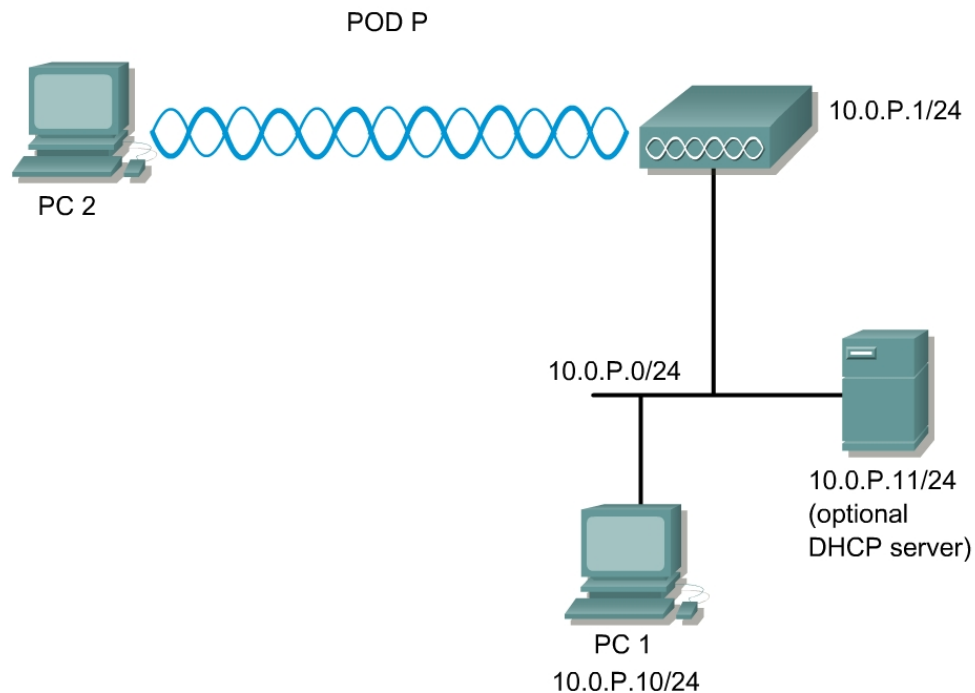
### Objective

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

The screenshot displays the configuration interface for a Cisco 1200 Access Point. The title bar reads "Cisco 1200 Access Point". Below it, there are tabs for "RADIO0-802.11B" and "RADIO1-802.11A". The "Hostname" is set to "ap", and the "ap uptime" is "1 hour, 46 minutes". The left sidebar contains a menu with the following items: HOME, EXPRESS SET-UP, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, and SERVICES. The "SECURITY" menu item is expanded, showing sub-items: Admin Access, SSID Manager, Encryption Manager (selected), Server Manager, Local RADIUS Server, and Advanced Security. The main content area is titled "Security: Encryption Manager - Radio0-802.11B". It contains two sections: "Encryption Modes" and "Encryption Keys". In the "Encryption Modes" section, the "None" radio button is unselected, and the "WEP Encryption" radio button is selected. The "Mandatory" dropdown menu is set to "Mandatory". Below this, there are checkboxes for "Cisco Compliant TKIP Features": "Enable MIC" and "Enable Per Packet Keying", both of which are unchecked. The "Cipher" radio button is unselected, and its dropdown menu is set to "WEP 128 bit". In the "Encryption Keys" section, there are four rows for "Encryption Key 1" through "Encryption Key 4". Each row has a radio button for selection and a "Key Size" dropdown menu. "Encryption Key 1" is selected, and its key size is set to "128 bit". The other three keys are unselected, and their key sizes are also set to "128 bit".

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

- From the **SECURITY>Encryption Manager** Page of the AP, configure the Encryption Key 1.
- Click on the WEP Encryption radio button.
- Select Mandatory.
- Click **Apply-All**.

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

---

---

---

## Step 2 Configure RADIUS server

Cisco 1200 Access Point

SERVER MANAGER GLOBAL PROPERTIES

Hostname ap ap uptime is 2 hours, 19 minutes

Security: Server Manager

Backup RADIUS Server

Backup RADIUS Server: 10.0.1.1 (Hostname or IP Address)

Shared Secret: .....

Apply Delete Cancel

Corporate Servers

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

- 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
- Enter the Shared Secret key of **secretkey**
- Click **Apply**.

## Step 3 Configure local RADIUS server

Cisco 1200 Access Point

STATISTICS GENERAL SET-UP

Hostname ap ap uptime is 2 hours, 22 minutes

Security: Local RADIUS Server - General Set-Up

Network Access Server

Current Network Access Servers

< NEW > 10.0.1.1

Network Access Server: 10.0.1.1 (IP Address)

Shared Secret: .....

Delete Apply Cancel

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

- Click on the **GENERAL SET-UP** tab.
- 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
- Enter the Shared Secret key of **secretkey**
- Click **Apply**.

## Step 4 Configure users

10.0.0.1

Shared Secret:

Delete Apply Cancel

**Individual User**

Current User List

< NEW >  
aaauser  
cisco

Delete

Username:

Password:  ☒ Text ☐ NT Hash

Confirm Password:

Group Name: < NONE >

Apply Cancel

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

- Continue from the **GENERAL SET-UP** tab.
- Enter the following users:

User	Username	Password
1	aaauser	aaapass
2	Cisco1	ciscopass

- Click **Apply**.

## Step 5 Configure authentication on AP

**Cisco 1200 Access Point**

RADIO0-802.11B      RADIO1-802.11A

Hostname ap      ap uptime is 45 minutes

**Security : SSID Manager - Radio0-802.11B**

**SSID Properties**

**Current SSID List**

SSID
< NEW >
AP1

Delete-Radio0  
Delete-All

SSID: AP1  
VLAN: < NONE > [Define VLANs](#)

**Authentication Methods Accepted:**

☐ Open Authentication: < NO ADDITION >  
☐ Shared Authentication: < NO ADDITION >  
☒ Network EAP: < NO ADDITION >

**Authenticated Key Management:**

☒ None      ☐ CCKM: Mandatory      ☐ WPA: Optional

WPA Pre-shared Key:      ☐ ASCII      ☐ Hexadecimal

EAP Client (optional):  
Username:      Password:

Association Limit (optional):      (1-255)

☐ Enable Proxy Mobile IP  
☒ Enable Accounting

Apply-Radio0      Apply-All      Cancel

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

- On the **SECURITY>SSID Manager** page of the AP, create a new SSID of APP, where **P** is the Pod number.
- Check the **Network EAP** box.
- Click the **Apply-All** button.

## Step 6 Verify the LEAP configuration

HOME

EXPRESS SET-UP

NETWORK MAP +

ASSOCIATION

NETWORK INTERFACES +

SECURITY

Admin Access

SSID Manager

Encryption Manager

Server Manager

Local RADIUS Server

Advanced Security

SERVICES +

WIRELESS SERVICES +

SYSTEM SOFTWARE +

EVENT LOG +

### Cisco 1200 Access Point

Hostname ap

ap uptime is 8 minutes

Security Summary

Administrators

Username	Read-Only	Read-Write
Cisco	✓	

Radio0-802.11B SSIDs

SSID	VLAN	Open	Shared	Network EAP
AP1	none			✓

Radio1-802.11A SSIDs

SSID	VLAN	Open	Shared	Network EAP
AP1	none			✓

Radio0-802.11B Encryption Settings

Encryption Mode	MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	CMIC	Key Rotation
Cipher						✓	✓	

Radio1-802.11A Encryption Settings

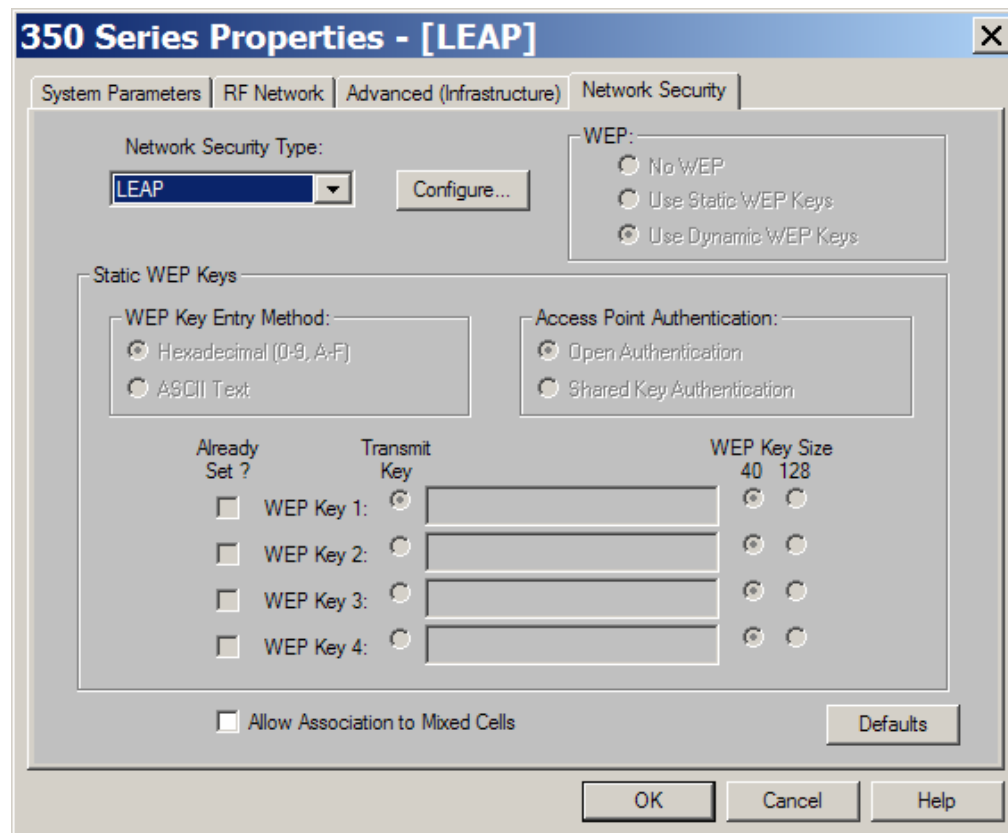
Encryption Mode	MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	CMIC	Key Rotation
Cipher						✓	✓	

Server-Based Security

Server Name/IP Address	Type	EAP	MAC	Proxy Mobile IP	Admin	Accounting
10.0.1.1	RADIUS	✓				

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

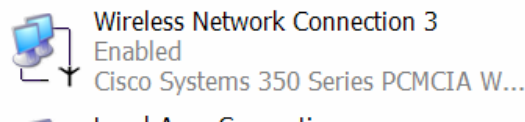
## Step 7 Configuring LEAP on the ACU



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

### LAN or High-Speed Internet



- 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

.....

### Cisco 1200 Access Point

Hostname ap ap uptime is 1 hour, 41 minutes

Association

Clients: 1 Repeater: 0

View: ☒ Client ☒ Repeater Apply

Radio802.11B

SSID AP :

Device Type	Name	IP Address	MAC Address	State	Parent	VLAN
350-client	-	0.0.0.0	<a href="#">0007.eb31.7c12</a>	EAP-Associated	self	none

Radio802.11A

Device Type	Name	IP Address	MAC Address	State	Parent	VLAN

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

.....

### Cisco 1200 Access Point

Hostname ap ap uptime is 2 hours, 34 minutes

Event Log

Start Display at Index:  Max Number of Events to Display:  Previous Next Refresh Clear

Index	Time	Severity	Description
1	Mar 1 02:27:22.139	Information	Interface Dot11Radio0, Station 0007.eb31.7c12 Associated KEY_MGMT[NONE]
2	Mar 1 02:27:20.820	Information	Interface Dot11Radio0, Deauthenticating Station 0007.eb31.7c12 Reason: Previous authentication no longer valid
3	Mar 1 02:27:20.820	Warning	Packet to client 0007.eb31.7c12 reached max retries, remove the client

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

### Cisco 1200 Access Point

STATISTICS GENERAL SET-UP

Hostname ap ap uptime is 11 minutes

Security: Local RADIUS Server - Statistics

Local RADIUS Server Information

Successful Authentication	1	Unknown Usernames	0
Client Blocks	0	Invalid Passwords	0
Unknown NAS	0	Invalid Packets From NAS	0

Network Access Server Information

View Information for:

Network Access Server 10.0.1.1

Successes	1	Unknown Username	0
Client Blocks	0	Invalid Passwords	0
Corrupted Packets	0	Unknown RADIUS Messages	0
No Username Attribute	0	Shared Key Mismatch	0
Invalid Authentication Attribute	0	Invalid State Attribute	0
Unknown EAP Messages	0	Unknown EAP Type	0

User Information

User Name	Successes	Failures	Blocks
aaauser	0	0	0
Cisco1	1	0	0

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.