Lab 8.5.4.1 Configure Enterprise Security on AP

Estimated Time: 30 minutes

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

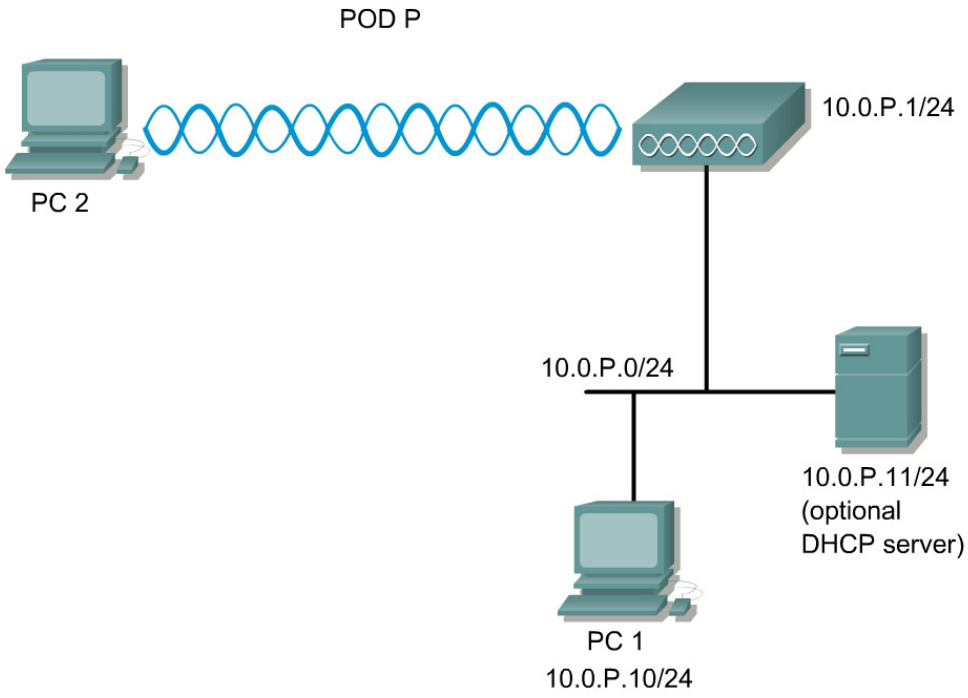
Objective

In this lab, students will demonstrate an understanding of the role of enterprise wireless network security. Additionally, students will configure MIC, TKIP and BKR on an AP.

Scenario

The purpose of WEP is to protect the privacy of transmitted data. However, WEP has inherent security weaknesses. There are many mechanisms available to provide additional security for WEP.

Topology



Preparation

The AP and PCs should be properly setup according to the topology prior to the lab. Ensure an existing wireless connection is present from PC2 to the AP.

Tools and Resources

Each team of students will require the following:

- One AP
- Wireless PC with the ACU
- Wired PC

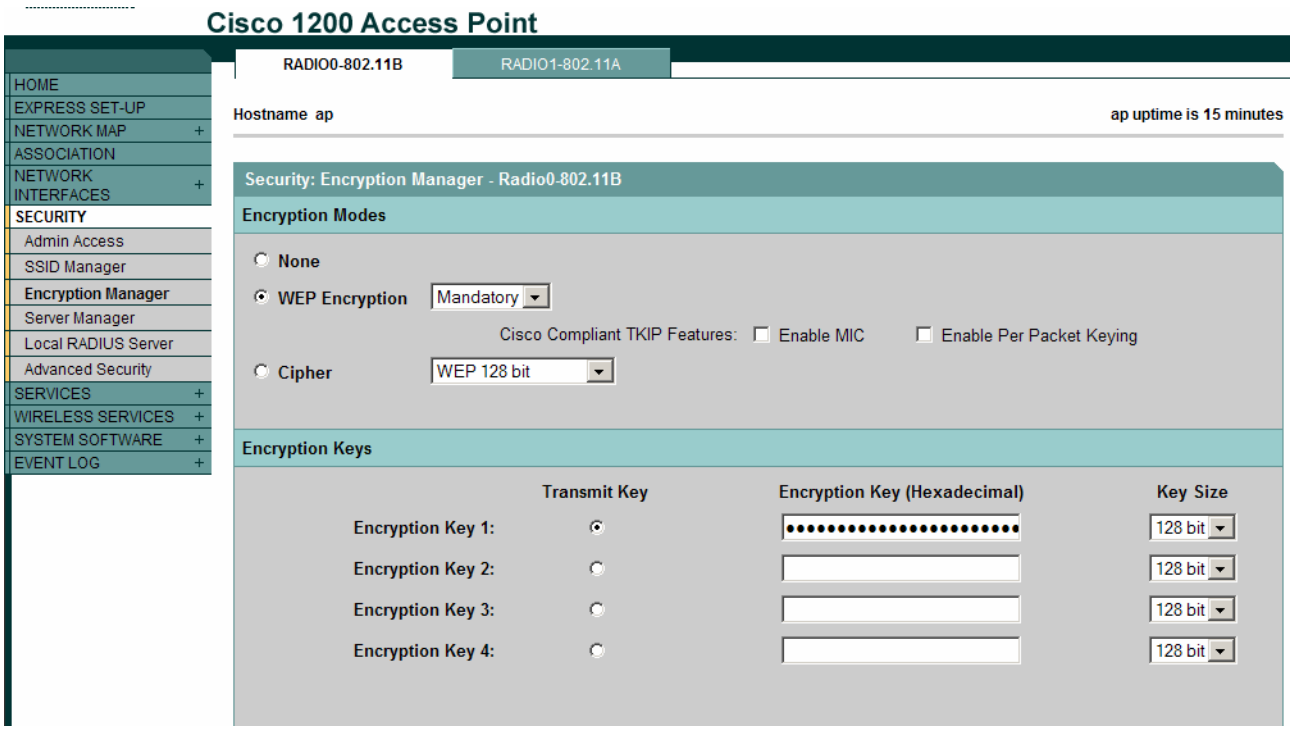
Understanding wireless security terminology:

- TKIP (Temporal Key Integrity Protocol)—TKIP is a suite of algorithms surrounding WEP that is designed to achieve the best possible security on legacy hardware built to run WEP. TKIP adds four enhancements to WEP:
  - A per-packet key mixing function to defeat weak-key attacks
  - A new IV sequencing discipline to detect replay attacks
  - A cryptographic message integrity Check (MIC), called Michael, to detect forgeries such as bit flipping and altering packet source and destination
  - An extension of IV space, to virtually eliminate the need for re-keying
- CKIP (Cisco Key Integrity Protocol)—Cisco's WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group.
- CMIC (Cisco Message Integrity Check)—Like TKIP's Michael, Cisco's message integrity check mechanism is designed to detect forgery attacks.
- Broadcast key rotation—Broadcast Key Rotation allows the AP to generate the best possible random key and update all key-management capable clients periodically.

Understanding WEP Key Restrictions

Security Configuration	WEP Key Restriction on AP
CCKM or WPA authenticated key management	Cannot configure a WEP key in key slot 1
LEAP or EAP authentication	Cannot configure a WEP key in key slot 4
Cipher suite with 40-bit WEP	Cannot configure a 128-bit key
Cipher suite with 128-bit WEP	Cannot configure a 40-bit key
Cipher suite with TKIP	Cannot configure any WEP keys
Cipher suite with TKIP and 40-bit WEP or 128-bit WEP	Cannot configure a WEP key in key slot 1 and 4
Static WEP with MIC or CMIC	AP and client devices must use the same WEP key as the transmit key, and the key must be in the same key slot on both AP and clients
Broadcast key rotation	Keys in slots 2 and 3 are overwritten by rotating broadcast keys

Step 1 Configure and verify WEP on the AP



In order to configure WEP on the AP, complete the following steps:

a. Verify connectivity from the wireless client (PC2) to the AP.

b. Open a Web browser on PC1 and type the IP address of the AP to configure in the browser address bar.

c. Go to the **Security** Setup page of the AP and click on the **Encryption Manager** option.

d. Check the radio button WEP Encryption Mode for **WEP Encryption.**

e. Use the Pull Down Menu to select **Mandatory.**

f. Select the **Transmit Key.**

g. Enter the Encryption key (for lab purposes will be) **12345678909876543210123456**.

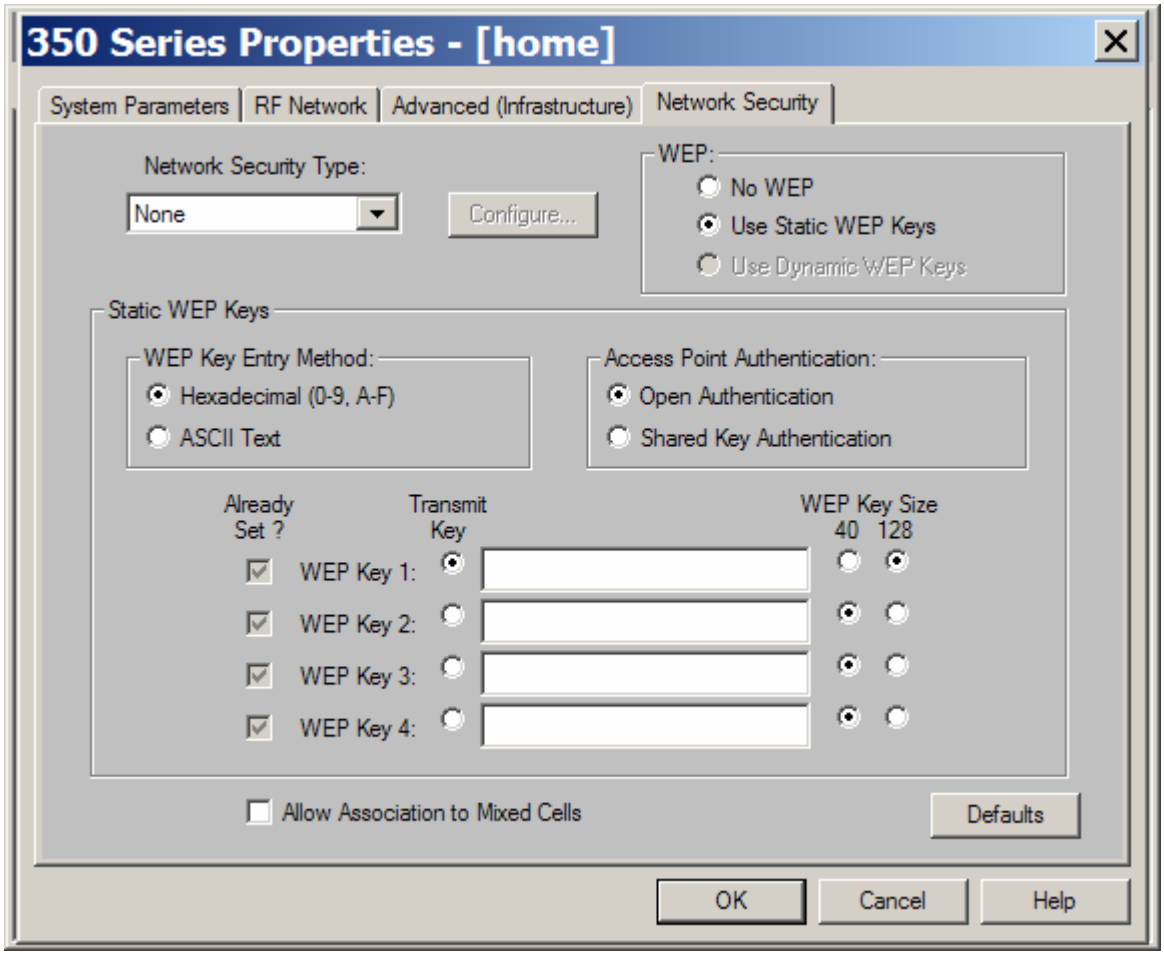
h. Select the Key size **128 bits**.

i. Click the **Apply-All** button to apply these options.

j. Once WEP is configured on the AP with a **Mandatory** option, all the clients will become disassociated to this AP.

k. View the **SECURITY>Encryption Manager** page. The WEP settings should be configured and the Encryption Key field should be stored in the AP. However, the Key field should be encrypted with asterisk symbols to prevent unauthorized users from viewing the Encryption Key.

Step 2 Configure and verify WEP on the client



a. Open the Aironet client utility by clicking on the ACU icon.

b. Click Profile Manager to edit the WEP settings.

c. Under the Profile Management section, choose the profile being used for this lab, and click Edit.

d. Go to the **Network Security** tab of the profile that is being used for the lab.

e. Configure the following settings for WEP:

   i. Select the WEP setting – **Use Static WEP keys**

   ii. Select the Static WEP key entry method – **Hexadecimal**

   iii. Select the AP Authentication – **Open authentication**

   iv. Select and enter the Transmit key [for lab purposes will be] **1234567890987654321012345 6**

   v. Select the WEP key Size – **128 bits**

   vi. Click the **OK** button to apply the WEP settings to the client

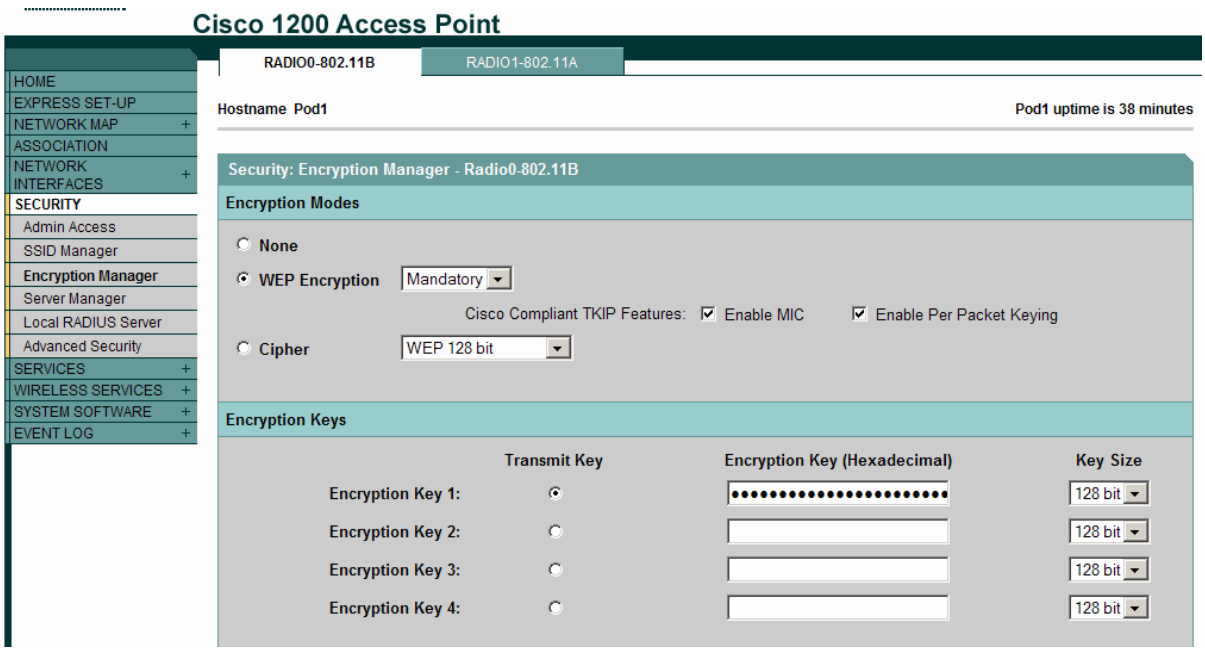
   vii. The connection should be reestablished between PC2 and the AP.

   viii. From the ACU Statistics Page, notice the “Packets Aged” and “Up-Time” values on the lower left hand corner.

Step 3 Enable MIC and TKIP

Once WEP is configured correctly, additional measures should be configured to secure the wireless link.

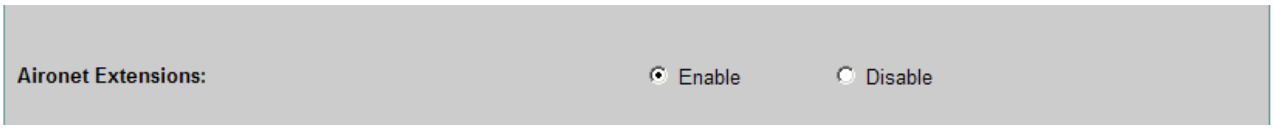
- **Message Integrity Check (MIC)**—MIC prevents attacks on encrypted packets called bit-flip attacks. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The MIC, implemented on both the AP and all associated client devices, adds a few bytes to each packet to make the packets tamper proof.
- **TKIP (Temporal Key Integrity Protocol, also known as WEP key hashing)**—This feature defends against an attack on WEP in which the intruder uses the unencrypted initialization vector (IV) in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs. On the AP, this feature is the Enable Per Packet Keying (PPK) option.



From the **SECURITY>Encryption Manager** Page, enable Cisco Compliant TKIP features.

a. Check the **Enable MIC** and **Enable Per Packet Keying (PPK).** These mechanisms can be used separately or together.

b. Click **Apply-All**

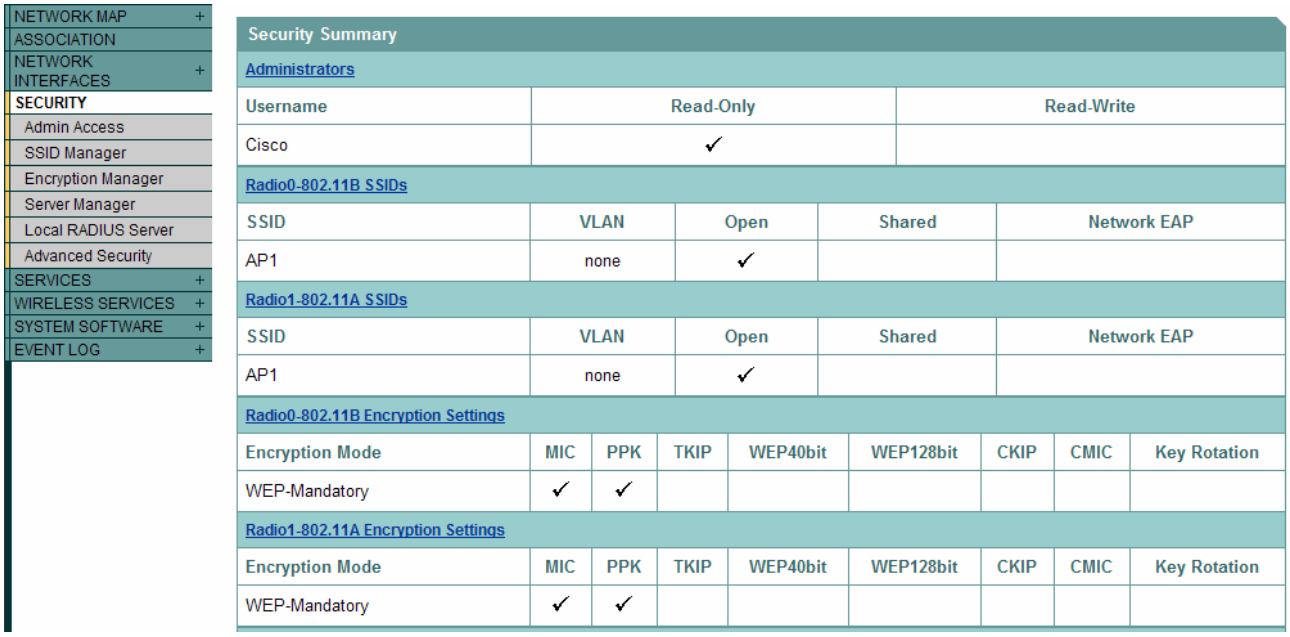


c. From the **NETWORK INTERFACES>Radio0-802.11b** Settings tab, verify the Aironet Extensions are enabled.

d. Also, check the 802.11a interface if applicable.

e. Verify the connection between PC2 and the AP

f. From the ACU Statistics Page, verify the “Packets MIC OK” statistics. The MIC statistics should now appear between the “Packets Aged” and “Up-Time” values. These values appear when MIC is enabled on the AP.



g. From the **SECURITY** Page, verify MIC and PPK are enabled.

h. What does MIC do to protect WEP?

_____

i. What attack does MIC prevent?

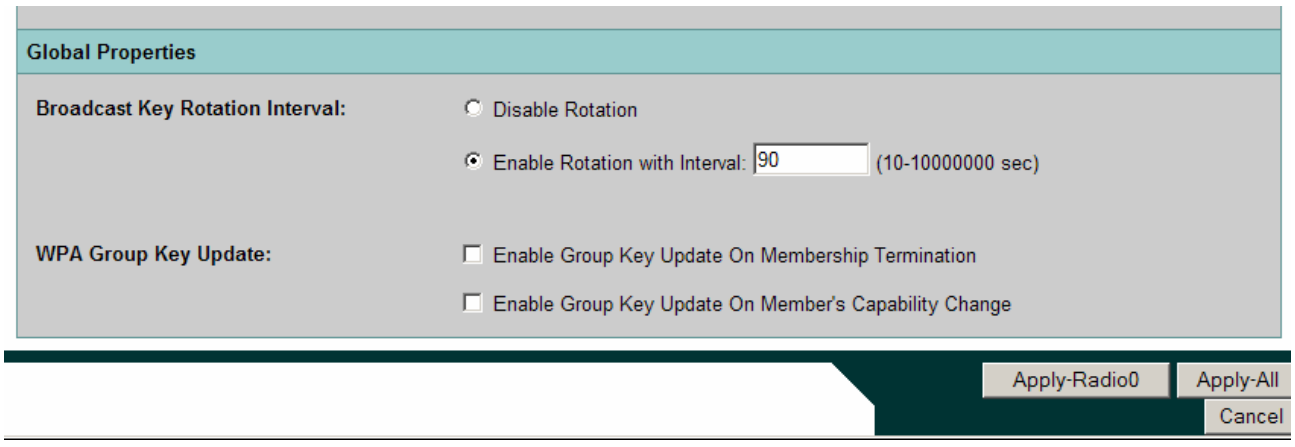
_____

j. Why do the Aironet extensions have to be used?

_____

Step 4 Enable Broadcast Key Rotation (BKR)

Broadcast key rotation (BKR)—When enabled, the AP provides a dynamic broadcast WEP key and changes it at the selected interval. Broadcast key rotation is an excellent alternative to TKIP if the wireless LAN supports wireless client devices that are not Cisco devices or that cannot be upgraded to the latest firmware for Cisco client devices.



a. Remove MIC and PPK configured from the previous step.

b. Check the **Enable Rotation with Interval** radio button.

c. Enter a value of 90 seconds.

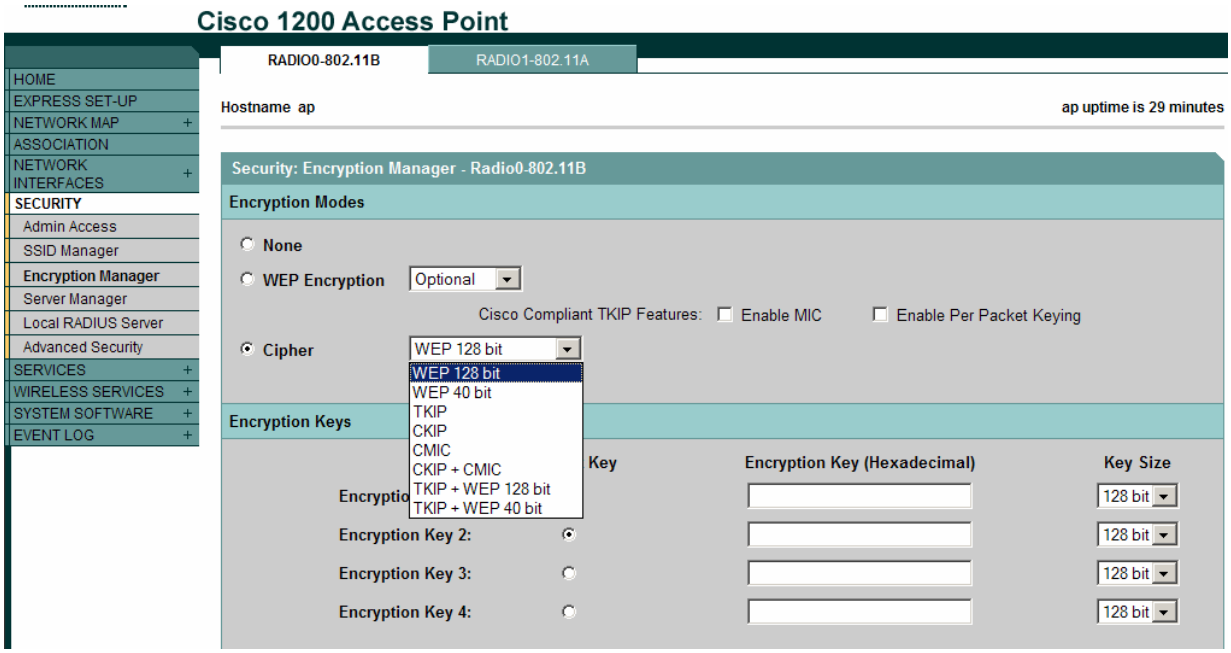
d. Click **Apply-All**

Radio0-802.11B Encryption Settings								
Encryption Mode	MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	CMIC	Key Rotation
WEP-Mandatory								✓
Radio1-802.11A Encryption Settings								
Encryption Mode	MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	CMIC	Key Rotation
WEP-Mandatory								✓

e. From the **SECURITY** Page, verify Key Rotation is enabled.

f. Verify connectivity from PC2 to the AP.

Step 5 Enable a cipher



From the **SECURITY>Encryption Manager** Page.

a. Remove Key Rotation configured from the previous step.

b. Check the **Cipher** radio button.

c. Choose the **TKIP** option in the drop down list

d. Click **Apply-All**

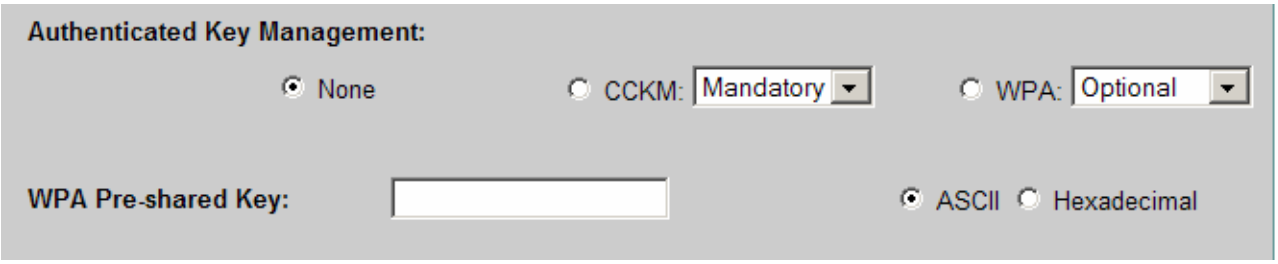
Radio0-802.11B Encryption Settings								
Encryption Mode	MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	CMIC	Key Rotation
Cipher			✓					
Radio1-802.11A Encryption Settings								
Encryption Mode	MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	CMIC	Key Rotation
Cipher			✓					

e. From the **SECURITY** Page, verify TKIP is enabled.

f. Verify the wireless connection from PC2 and the AP.

g. Return to step 5c and try some of the various Cipher settings. Verify the changes from the SECURITY Page.

Step 6 Understanding ciphers and Key Management (optional challenge)

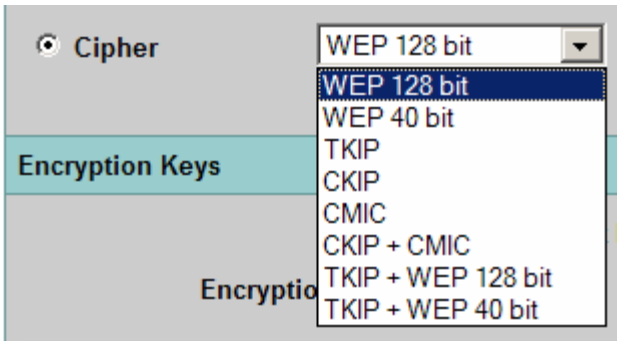


a. From the **SECURITY>SSID Manager** Page, check the **Authenticated Key Management** options.

Using Cisco Centralized Key Management (CCKM), authenticated client devices can roam from one AP to another without any perceptible delay during reassociation. An AP on the network provides Wireless Domain Services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS AP cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new AP. When a client device roams, the WDS AP forwards the client's security credentials to the new AP, and the reassociation process is reduced to a two-packet exchange between the roaming client and the new AP. Roaming clients reassociate so quickly that there is no perceptible delay in voice or other time-sensitive applications.

Wi-Fi Protected Access (WPA) is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages TKIP (Temporal Key Integrity Protocol) for data protection and 802.1X for authenticated key management.

WPA key management supports two mutually exclusive management types: WPA and WPA-Pre-shared key (WPA-PSK). Using WPA key management, clients and the authentication server authenticate to each other using an EAP authentication method, and the client and server generate a pairwise master key (PMK). Using WPA, the server generates the PMK dynamically and passes it to the AP. Using WPA-PSK, a pre-shared key must be configured on both the client and the AP, and that pre-shared key is used as the PMK.



Cipher Suites Compatible with WPA and CCKM

Authenticated Key Management Types	Compatible Cipher Suites
CCKM	• encryption mode cipher wep128 • encryption mode cipher wep40 • encryption mode cipher ckip • encryption mode cipher cmic • encryption mode cipher ckip-cmic • encryption mode cipher tkip • encryption mode cipher tkip wep128 • encryption mode cipher tkip wep40
WPA	• encryption mode cipher tkip • encryption mode cipher tkip wep128 • encryption mode cipher tkip wep40

b. Explore the different Cipher settings.

