Application Note

The Cisco Router and Security Device Manager

Wireless Application

Introduction

This document explains how to configure a Cisco Systems® fixed wireless router using the Cisco® Router and Security Device Manager (SDM) wireless application. This document contains these sections:

- Cisco Wireless Routers Supported by the Cisco Router and Security Device Manager
- Deploying Cisco Wireless Routers
- Configuring Wireless Security
- Configuring Cisco Wireless Clients and Wireless Associations

Cisco Wireless Routers Supported by the Cisco Router and Security Device Manager

Cisco wireless routers are Wi-Fi certified 802.11b-compliant, 802.11g-compliant, or 802.11a-compliant WLAN transceivers (access points). You can configure a Cisco Wireless Router as an access point (root unit) that is connected to wired LANs. For more information about Cisco wireless routers, please refer to Wireless Device/Network Configuration Examples.

The Cisco SDM supports configuring a wireless router as an access point (root unit) running Cisco IOS® Software offering these features:

- **World mode**—Use this feature to communicate the wireless router regulatory setting information, including maximum transmit power and available channels, to world mode–enabled clients. Clients using world mode can be used in countries with different regulatory settings and automatically conform to local regulations.

- **Multiple Service Set Identifiers (SSIDs)**—Create up to 16 SSIDs on the access point and assign any combination of these settings to each SSID:
  - Broadcast SSID mode for guests on your network
  - Client authentication methods
  - Maximum number of client associations
  - VLAN identifier
  - RADIUS accounting list identifier

- **VLANs**—Assign VLANs to the SSIDs on the access point (one VLAN per SSID) to differentiate policies and services among users.

- **Enhanced security**—Enable advanced security features to protect against sophisticated attacks on your wireless network Wired Equivalent Privacy (WEP) keys: Message Integrity Check (MIC), WEP key hashing, and broadcast WEP key rotation.
• **Wi-Fi Protected Access (WPA)**—WPA is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future WLAN systems.

### Deploying Cisco Wireless Routers

This document demonstrates how to configure a wireless router as an access point (root unit) that is connected to wired LANs. In this deployment scenario, company ABC plans to open a new branch office with 30 to 40 employees who use wireless as the primary connectivity. To reduce cabling costs in the new building, a Cisco 1811W Wireless Security Router with fixed configuration will be installed; the branch office also provides Internet connectivity (the "hotspot") for visiting customers.

All the employees in the branch office use 802.11g Cisco Aironet® 350 wireless LAN client adapters. These employees might travel around the building, optimizing the wireless network range that will be applied to the radio interface. The wireless network will be in routing mode to separate employee wireless subnet from the guest hotspot; firewalls will be applied to radio interfaces to prevent guests in the hotspot from accessing the company’s private LANs. Figure 1 shows the deployment topology. The traffic (in red) from the hotspot to the employee network and VLAN1 is blocked by a firewall, and all other traffic (in green) is allowed.

**Figure 1** Deployment Topology

![Deployment Topology Diagram](image)

*Note:* The information and data presented in this document were created in a lab environment. All of the devices and clients used in this document started with a cleared configuration. Collect necessary data for your live network; the data used in this document might not suit your network. If you are working in a live network, make sure that you understand the potential effects of any commands and changes.
**Prerequisites**
Before creating a wireless configuration, use Cisco SDM Express to prepare the wireless router.

**Accessing a Wireless Router the First Time**
When you access a fixed-configuration wireless router for the first time, Cisco SDM Express displays the Basic Configuration screen, then the Wireless Interface Configuration screen (Figure 2).

**Figure 2  Wireless Interface Configuration Screen**

1. Select Yes to configure your wireless interface and then click Next.

2. On the LAN Interface Configuration screen (Figure 3), make the following settings and then click Next:
   - Bridge-to interface: Vlan 1
   - IP Address: 192.168.1.1
   - Subnet Mask: 255.255.255.0
   - SSID: defense

---

1 Cisco SDM Express will configure a bridged wireless network by enabling integrated routing and bridging (IRB) and creating a bridge group virtual interface (BVI, in this case BVI1) to associate a bridge group (group 1) where VLAN1 and the wireless interfaces belong.
3. On the DHCP Server configuration screen (Figure 4), make the following settings and then click Next:

   - Enable DHCP Server on the LAN interface: check
   - Starting IP Address: 192.168.1.10
   - Ending IP Address: 192.168.1.254
   - Domain name server (DNS): skip
4. On the WAN Configuration screen (Figure 5), make the following settings and then click Next:

   o Uncheck Use CNS.

   o Select FastEthernet1 and click Add Connection icon

   o Add InterfaceFast1 Connection window appears

     § PPPoE: uncheck

     § Static IP Address: 66.1.1.213/255.255.255.0

     § Click OK to return to the WAN Configuration screen
5. On the Internet (WAN) - Advanced Options screen (Figure 6), check Enable NAT² and click Next.

² Cisco SDM Express will create a Network Address Translation (NAT) rule with FastEthernet1 as the outside interface and BV11 as the inside interface.
6. On the Firewall Configuration screen, select Yes, I want to protect my network with a firewall and click Next.

7. On the Security Configuration screen (Figure 7), use the default security configuration settings recommended by Cisco and click Next.
8. If you are satisfied with the configuration shown on the Cisco SDM Express Summary screen (Figure 8), click Finish.
9. Click OK when you finish reading and saving the Cisco SDM Express reconnection instructions.

10. Click OK to shut down Cisco SDM Express when the configuration has been delivered to the router.

Cisco SDM Express configures the wireless router as an access point for a bridged wireless network, shown in Figure 9. The wired LAN (VLAN1) and wireless network are in the same subnet: they share the same Dynamic Host Configuration Protocol (DHCP) pool, NAT rules, and BVI interface.

![Figure 9 Bridged Wireless Network Topology](image)

For a quick verification from the client side, configure a wireless client with SSID defense (refer to “Configuring Cisco Wireless Clients and Wireless Associations,” later in this document, for a configuration example) and configure the wireless client host (the laptop or the PC) to obtain an IP address automatically. The wireless client icon in the taskbar on the laptop will turn green (Figure 10), and the host will be assigned an IP address from the DHCP pool (192.168.1.x).

![Figure 10 Host Taskbar](image)

You can view the list of clients on your wireless router using the Cisco SDM wireless application. Refer to “Configuring Cisco Wireless Clients and Wireless Associations,” later in this document, to bring up the wireless association page. Figure 11 shows a wireless client, User-abc1, that is associated with SSID defense, is assigned IP address 192.168.1.10 from the DHCP pool, and belongs to no VLAN.
The bridged wireless network is easy to deploy—after the wireless clients are associated with the access point, they obtain connectivity to wired LANs and to the Internet.

**Configuring a Routed Wireless Network**

In our scenario, company ABC wants to separate the employee wireless subnet from the guest hotspot and will use the Cisco SDM wireless application to convert a bridged wireless network to a routed wireless network for better security implementation (Figure 12).

---

**Figure 11 Wireless Association Screen**

![Wireless Association Screen](image)

<table>
<thead>
<tr>
<th>Association</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Clients: 1</td>
<td>Repeaters: 0</td>
</tr>
</tbody>
</table>

**Figure 12 Routed Wireless Network Topology**

![Routed Wireless Network Topology](image)
Launching the Cisco SDM Wireless Application

Launch Cisco SDM. On the Configure Mode screen, select Interfaces and Connections, click the Create Connection tab, and select Wireless (Figure 13). The Launch Wireless Application button appears; click the button to launch the wireless application.

Figure 13  Wireless Interfaces and Connections Screen

The left side of the Cisco SDM wireless application window (Figure 14) includes a navigation bar. The configuration action buttons are at the bottom. Use the navigation bar to display other management pages and use the configuration action buttons to save or cancel changes to the configuration:

- **Wireless Express Set-up**—Allows you to optimize radio network and configure Cisco Aironet 350 Wireless LAN Client Adapter extensions.
- **Wireless Express Security**—Allows you to configure SSID and basic security settings.
- **Wireless Network Map**—Displays a list of infrastructure devices on the wireless network.
- **Wireless Association**—Displays a list of clients on your WLAN associated with the access point.
- **Wireless Interfaces**—Displays status and statistics for the radio interfaces and provides links to a configuration window for each radio interface.
- **Wireless Security**—Displays a summary of security settings and provides links to a security configuration window.
- **Wireless Services**—Provides links to a filter configuration and VLAN configuration for each radio interface.

**Figure 14 Cisco SDM Wireless Application**

Express Set-up

On the Express Set-up page (Figure 14), you can select either preconfigured settings or customized settings for the radio. Selecting Throughput maximizes the data volume handled by the device but might reduce the range. All data rates are set to Required (basic). Selecting Range maximizes the device’s range but might reduce the throughput. The lowest data rate is set to Required (basic), and the other data rates are set to Enable; if Default is selected, the data rates are set to factory default settings.

By default, the access point uses Cisco Aironet 802.11 extensions to detect the capabilities of Cisco Aironet client devices. This setting must be set to Enable for you to use features such as load balancing, MIC, or Temporal Key Integrity Protocol (TKIP). Disabling Cisco Aironet extensions sometimes improves the ability of client devices not from Cisco Systems to associate with the wireless router.

In our scenario, we optimize the radio network for range and enable the Cisco Aironet extensions to remain, because all employees use Cisco Aironet clients.
For Radio0-802.11G, follow these steps.

1. For Optimize Radio Network, choose Range.
2. For Aironet Extensions, choose Enable.
3. Click Apply, then Click OK to continue.

This document does not discuss Radio01-802.11A.

### Wireless Express Security

The Wireless Express Security pages help you configure your basic security settings. Use these pages to create unique SSIDs and assign security types to them to quickly enable the wireless network.

Click Wireless Express Security in the left navigation bar on the Cisco SDM wireless application window. You can configure a bridging connection or a routing connection.

- **Bridging**—Configures basic security settings for a bridging connection. A bridging connection uses a BVI to combine traffic from all radio interfaces into one subnetwork.
- **Routing**—Configures basic security settings for a routing connection. Make basic security settings for a routing connection on this page. A routing connection allows you to create separate networks for each radio interface and route traffic to each network.

In our scenario, the guest hotspot has to be separate from the employee wireless subnet and wired LANs. Therefore, routing will be implemented on radio interfaces. Use the Express Security Routing page to create two subnets: the guest hotspot and the employee wireless subnet. The guest hotspot will be configured with a guest mode SSID to allow client devices with no SSID to be associated to obtain Internet access.

To configure a routed wireless network, complete the following steps:

2. Scroll down to locate the SSID table (Table 1), which shows the SSID defense created for the bridged wireless network by Cisco SDM Express.
3. Delete all SSIDs created for bridged wireless networks before configuring SSIDs for a routed wireless network.
4. Click Delete.
5. Click OK to deliver the change.
### Table 1 SSID Table

<table>
<thead>
<tr>
<th>SSID</th>
<th>VLAN</th>
<th>IP Address/Netmask</th>
<th>Encryption</th>
<th>Authentication</th>
<th>Key Management</th>
<th>Native VLAN</th>
<th>Broadcast SSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>defense</td>
<td>none</td>
<td>none</td>
<td>none</td>
<td>open</td>
<td>none</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring a Routed Wireless Network

Use the Express Security Routing page (Figure 15) to configure an SSID for the hotspot subnet:

#### Figure 15 Express Security Routing Screen

<table>
<thead>
<tr>
<th>SSID Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. SSID</td>
</tr>
<tr>
<td>2. VLAN</td>
</tr>
<tr>
<td>3. IP Protocol</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>4. Security</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

© 2005 Cisco Systems, Inc. All rights reserved. Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com

Page 14 of 41
1. For SSID, enter hotspot.

2. Check Broadcast SSID in Beacon.³

3. Select Enable VLAN ID and enter 100. (Note: Static WEP key is disabled if Enable VLAN ID is selected.)

4. Check Radio0-802.11G

5. For IP Address, enter 10.10.100.1.

6. For IP Subnet Mask, enter 255.255.255.0.

7. Uncheck Radio0-802.11A.

8. Choose No Security. (Note: This document will use the Cisco SDM Wireless Application/Wireless Security page to configure more advanced security settings later.)

9. Click Apply.

10. When WARNING window appears, click OK to continue.

Use the same Express Security Routing page to configure an SSID for the employee wireless subnet:

1. For SSID, enter defense.

2. Uncheck Broadcast SSID in Beacon.

3. Select Enable VLAN ID and enter 2.

4. Check Radio0-802.11G.

5. For IP Address, enter 192.168.2.1.

6. For IP Subnet Mask, enter 255.255.255.0.

7. Uncheck Radio0-802.11A.


9. Click Apply.

10. When WARNING window appears, click OK to continue.

At the same Express Security Routing page, scroll down to the SSID table (Table 2), which shows two SSIDs, defense and hotspot, configured with VLAN 2 and VLAN 100, and IP addresses 192.168.2.1 and 10.10.100.1, respectively.

³ When you broadcast the SSID (SSID in guest mode), client devices that do not specify an SSID can associate to the root access point. This is a useful option for an SSID used by guests or by client devices in a public space. If you do not broadcast the SSID, client devices cannot associate to the access point unless their SSID matches this SSID. Only one SSID can be included in the beacon.
Table 2 SSID Table

<table>
<thead>
<tr>
<th>SSID</th>
<th>VLAN</th>
<th>IP Address/Netmask</th>
<th>Encryption</th>
<th>Authentication</th>
<th>Key Management</th>
<th>Native VLAN</th>
<th>Broadcast SSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>@</td>
<td>2</td>
<td>Dot11Radio0.2 192.168.2.2/24</td>
<td>none</td>
<td>open</td>
<td>none</td>
<td></td>
<td></td>
</tr>
<tr>
<td>@</td>
<td>100</td>
<td>Dot11Radio0.100 10.10.100.1/24</td>
<td>none</td>
<td>open</td>
<td>none</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

Configuring the Dynamic Host Control Protocol—Reducing Client Configuration Tasks

Use the Cisco SDM to configure DHCP pools to automatically assign reusable IP addresses to DHCP clients in the guest hotspot and the employee wireless subnet.

The first step is to synchronize the configuration. To do this by go to the Cisco SDM and click Refresh (Figure 16).

Figure 16 Refresh

At Configure Mode, select Additional Tasks, and select DHCP from the Tasks panel. Cisco SDM Express should create a pool named sdm-pool1 for interface BVII (Figure 17).
To add a DHCP pool for the employee wireless subnet:

1. Click Add… The Add DHCP Pool window (Figure 18) appears. Use the following settings:
   - DHCP Pool Name: employeeW
   - DHCP Pool Network: 192.168.2.0, Subnet Mask: 255.255.255.0
   - Lease Length: Never Expires
   - DHCP Options: Default Router = 192.168.1.1 (in our scenario, we use wired LAN interface)

2. Click OK to deliver the changes.

3. Click OK and return to the DHCP Pools page.
To add a DHCP pool for the hotspot subnet:

1. Click Add… The Add DHCP Pool window appears. Use the following settings:
   - DHCP Pool Name: hotspot
   - DHCP Pool Network: 10.10.100.0, Subnet Mask: 255.255.255.0
   - DHCP Pool: Starting IP: 10.10.100.10, Ending IP: 10.10.100.254
   - Lease Length: User-Defined/1 Day
   - DHCP Options: Default Router = 66.1.1.213 (in our scenario, we use WAN interface)

2. Click OK to deliver the changes.

3. Click OK.

After finishing the preceding task, at the Cisco SDM DHCP Pools page, you should see two DHCP pools, employeeW and hotspot. They are related to interfaces Dot11Radio0.2 and Dot11Radio0.100, respectively (Figure 19).
At this point, the guest hotspot and the employee wireless subnet have no connectivity to the Internet, because they are private networks, and private IP addresses are not routable in the Internet. Use the Cisco SDM to apply NAT rules to the radio interfaces to translate the private addresses into routable addresses.

Configuring Network Address Translation—Internet Connectivity

Use the Cisco SDM to apply NAT rules to the radio interfaces to translate private addresses into routable addresses. At Configure Mode, select Interfaces and Connections, the click the Edit Interface/Connection tab.

You should see two radio interfaces, Dot11Radio0.2 and Dot11Radio0.100, created by the Cisco SDM wireless application for the employee wireless subnet and the guest hotspot (Figure 20).
To configure interfaces to allow NAT, take the following steps:

1. Select Dot11Radio0.2 from the Interface List.
2. Click Edit. The Interface Feature Edit dialog box (Figure 21) appears.
3. Click the NAT tab.
   - Select inside from the drop-down box.
   - Click OK to deliver the change.
   - Click OK and return to the Edit Interface/Connection screen.
4. Repeat steps 1 through 3 for the Dot11Radio0.100 interface.

The next step is to add the traffic from the guest hotspot and the employee wireless subnet to the original address of the NAT rules. At Configure Mode, select Additional Tasks, expand ACL Editor, and select NAT Rules. You should see NAT rule number 1 created by Cisco SDM Express. This rule permits the VLAN 1 subnet (192.168.1.0/24) for NAT (Figure 22).
To add employee wireless traffic to the NAT rules (Figure 23), take the following steps:

1. Select the rule.

2. Click Edit.

3. Click Add. The Add a Standard Rule Entry window appears. Use the following values:
   - Action: Permit
   - Type: A Network
   - IP Address: 192.168.2.0
   - Wildcard Mask: 0.0.0.255
   - Description: employee wireless subnet

Figure 23  Editing a Rule
Repeat step 3 for the guest hotspot, using these values:

- **Action**: Permit
- **Type**: A Network
- **IP Address**: 10.10.100.0
- **Wildcard Mask**: 0.0.0.255
- **Description**: hotspot

4. Click OK to deliver the changes.

5. Click OK.

Now the hotspot and the employee wireless subnet obtain Internet connectivity. However, there is no firewall to block traffic from the guest hotspot to wired LANs and the employee wireless subnet.

**Network Security**

In our scenario, company ABC uses firewalls to prevent guests in the hotspot from accessing the company’s private LANs.

Use the Cisco SDM to apply firewalls to radio interfaces. At Configure Mode, select the firewall and access control list (ACL), then click the Create Firewall tab (Figure 24).

**Figure 24 Creating Firewall**

1. Select Basic Firewall, then click Launch the selected task
2. Click Next.
3. The Basic Firewall Interface Configuration screen (Figure 25) appears. Use the following values:
   - Outside (untrusted) Interface: FastEthernet1
   - Inside (trusted) Interfaces: BV11, Dot11Radio0.2, Dot11Radio0.100, then click Next

4. Click Yes if prompted by Cisco SDM Warning to disassociate the inspection rule (Figure 26).
5. Make sure you are not launching the Cisco SDM from the outside interface (Figure 27), then click OK.

Figure 27 Warning

Note: You cannot launch SDM from the following interfaces after the Firewall Wizard completes:

FastEthernet1

6. The Internet Firewall Configuration Summary appears. Click Finish if you are satisfied the configuration.

7. You will be prompted to merge or replace existing access rules. Click Merge.

8. Use the Edit a Rule tool (Figure 28) to edit the rules, if necessary. Click OK when finished.

9. Repeat steps 7 and 8 if necessary.
10. Click OK.

Next, use the Cisco SDM to edit the access rule on the interface Dot11Radio0.100 (inbound) direction to deny traffic going to BV11 and Dot11Radio0.2. At Configure Mode, select the firewall and ACL, then click the Edit Firewall Policy/ACL tab.

To block traffic from Dot11Radio0.100 to BV11, take the following steps:

1. Select a direction from Dot11Radio0.100 to FastEthernet1, then click Go.

2. The Dot11Radio0.100 inbound access rule displays (Figure 29).
3. Go to the Firewall Feature/Service section.

4. Click Add, then select Insert Before (Figure 30).

Figure 30 Insert Before Command
5. The Add an Extended Rule Entry (Figure 31) window appears. Enter the following information:

- Action: Deny
- Description: block traffic going to wired LAN
- Source Host/Network: Any IP Address
- Destination Network: 192.168.1.0/0.0.0.255
- Protocol and Service: IP Protocol = IP/any
- Click OK and go back to the Edit Firewall Policy/ACL page.

Figure 31 Add an Extended Rule Entry Screen
To block traffic from Dot11Radio0.100 to Dot11Radio0.2, repeat steps 3 to 5 with the following information:

- Action: Deny
- Source Host/Network: Any IP Address
- Destination Network: 192.168.2.0.0/0.0.0.255
- Protocol and Service: IP Protocol = IP/any
- Click OK and go back to the Edit Firewall Policy/ACL page.

6. From the Edit Firewall Policy/ACL page, click the Apply Changes button on the lower screen to deliver the changes.

7. Click OK.

Now the wired LANs and the employee wireless subnet are not accessible from the hotspot. You have successfully created a routed wireless network with a firewall, as shown in Figure 1.

Configuring Wireless Security

You can configure a wireless router to act as a local authenticator to provide authentication service for small WLANs without a RADIUS server or to provide backup authentication service in case of a WAN link or a server failure. This section describes how to configure the access point as a local authenticator to serve as a standalone authenticator for small WLANs.

In our scenario, company ABC will enable Cisco LEAP authentication with the local RADIUS server on the wireless router to provide user-based authentication to further protect its LANs. Use the Cisco SDM wireless application to enable Cisco LEAP, then click Wireless Security in the left navigation bar.

Configuring a Local RADIUS Server

1. Using Local RADIUS Server, select Local RADIUS Server, click the GENERAL SET-UP tab, and scroll down to the Network Access Servers (AAA Clients) section (Figure 32) to configure the wireless router as a network access server (NAS). Use the following settings:
   - Network Access Server: 192.168.1.1 (configure the wireless router as the NAS)
   - Shared Secret: cisco123

2. Click Apply.

3. Click OK to activate the change.

---

Cisco LEAP is an 802.1x authentication type for WLANs that supports strong mutual authentication between the client and a RADIUS server using a logon password as the shared secret. It provides dynamic per-user, per-session encryption keys to address the major vulnerabilities of 802.11 security, including:
- Weak device-only authentication: Client devices, not users, are authenticated
- Weak data encryption: WEP has been proven ineffective as a means to encrypt data
Configuring User Groups and User Credentials

RADIUS user groups may be configured to permit differentiation between groups for different access requirements. Add a new group in the User Group section under the Wireless Security/Local RADIUS Server/GENERAL-SETUP page (Figure 33). Use the following settings:
• Group Name: employeeLEAP
• Session Timeout: leave it blank to use default
• Failed Authentication before Lockout: 3
• Lockout: Internal = 60 sec
• VLAN ID: 2 (the employee wireless subnet)
• SSID: defense, then click Add
• Click Apply.
• Click OK to activate the change.

Enter the user credentials for local authentication under the Individual Users section under the Wireless Security/Local RADIUS Server/GENERAL SET-UP page (Figure 34). Use the following values:

• Username: abc1
• Password: abc1/Text (you may enter the password in text or directly as a Windows NT hash)
• Group Name: select employeeLEAP from the drop-down box
• Click Apply in the Individual Users section.
• Click OK to activate the changes and create a user in the local database.

Repeat these steps to add more user credentials.

Figure 34 Individual Users Screen
Configuring Cisco LEAP
To configure the wireless router for Cisco LEAP, click Wireless Security in the navigation bar, select Server Manager, click the SERVER MANAGER tab, and take the following steps:

1. Choose RADIUS from the Current Server List drop-down box under the Corporate Servers section (Figure 35). Use the following values:
   - Server: 192.168.1.1 (the IP address of the wireless router)
   - Shared Secret: cisco123 (same as the shared secret for the NAS)
   - Authentication Port: 1812 (the local RADIUS server listens on port 1812—required for local authenticator)
   - Accounting Port: 1813 (the local RADIUS server listens on port 1813—required for local authenticator)
   - Click Apply in this section.
   - Click OK to save the server configuration settings.

2. Choose 192.168.1.1 from the EAP Authentication drop-down box under the Default Server Priorities section.
3. Click Apply.
4. Click OK.

To configure encryption, click Wireless Security in the left navigation bar, select Encryption Manager, click the RADIO0-202.11G tab, and take the following steps (Figure 36). Use the specified values.

1. Security: Encryption Manager Radio0-802.11G
   - Set Encryption Mode and Keys for VLAN: 2 (the employee wireless subnet)
Encryption Modes: Cipher/TKIP+WEP 128 bit

Global Properties: use default value

2. Click Apply.

3. Click OK to activate the changes.

**Figure 36  Security: Encryption Manager**

<table>
<thead>
<tr>
<th>Security: Encryption Manager Radio® 802.11G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Encryption Mode and Keys for VLAN:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Encryption Modes</td>
</tr>
<tr>
<td>☐ None</td>
</tr>
<tr>
<td>☐ WEP Encryption [Optional]</td>
</tr>
<tr>
<td>☒ Cipher</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Global Properties</td>
</tr>
<tr>
<td>Broadcast Key Rotation Interval:</td>
</tr>
<tr>
<td>☐ Disable Rotation</td>
</tr>
<tr>
<td>☐ Enable Rotation with Interval [DISABLED] (10-1000000 sec)</td>
</tr>
<tr>
<td>WPA Group Key Update:</td>
</tr>
<tr>
<td>[ ] Enable Group Key Update On Membership Termination</td>
</tr>
<tr>
<td>[ ] Enable Group Key Update On Member's Capability Change</td>
</tr>
</tbody>
</table>

To configure Cisco LEAP for the employee wireless subnet (SSID = defense), click Wireless Security in the left navigation bar, select SSID Manager, click the RADIO-802.11 G tab (Figure 37), and take the following steps:

1. Choose defense from Current SSID List.

2. Use the following values for Authentication Settings:
   - Methods Accepted: check the Network EAP box with the <NO ADDITION> option (If you are using client cards not from Cisco, specify Open Authentication and specify EAP Authentication in the drop-down box. In our scenario, it is not necessary to use Open Authentication/EAP Authentication.)
   - In our scenario, use Defaults for Server Priorities

3. Authenticated key Management: skip; we do not use WPA
4. Accounting Settings: skip; we do not enable accounting

5. General Settings: skip; they are optional (Association Limit is the maximum number of clients that may associate to a particular SSID. This limit prevents access points from getting overloaded and helps to provide an adequate level of service to associated clients.)

6. Click Apply-Radio0 in the General Settings section.

7. Click OK to activate the changes.

Figure 37 SSID Properties

Security: SSID Manager Radio0.802.11G
SSID Properties

Current SSID List

<table>
<thead>
<tr>
<th>SSID</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>defense hotspot</td>
<td>&lt;NONE&gt;</td>
</tr>
</tbody>
</table>

Delete

Authentication Settings

Methods Accepted:

- Open Authentication: <NO ADDITION>
- Shared Authentication: <NO ADDITION>
- Network EAP: <NO ADDITION>

Server Priorities:

FAP Authentication Servers
- Use Defaults
- Customize
  Priority 1: <NONE>

MAC Authentication Servers
- Use Defaults
- Customize
  Priority 1: <NONE>

You have complete adding LEAP authentication to your wireless router acting as a local RADIUS server and an access point.
Configuring Cisco Wireless Clients and Wireless Associations
This document gives examples of configuring the Cisco Aironet 350 Wireless LAN Client Adapter for SSID/no security clients and Cisco LEAP clients.

Configuring SSID/No Security Clients
1. Open the Cisco Aironet Client Utility Version 6.0.
2. Click the Profile Manager icon.
3. Click Add and enter a name (defense) for the profile.
4. Click Apply.
5. On the Profile Properties screen, configure these system parameters:
   - Client Name: User-abc1 (optional)
   - SSID1: defense
   - Power Save Mode: CAM
   - Network Type: Infrastructure
6. Click the Network Security tab.
7. Choose None from the Network Security Type drop-down box.
8. For WEP: No WEP, click OK to return to the Profile Manager.
9. Click OK to create the new profile, defense.
10. From the Cisco Aironet Client Utility, click the Select Profile icon.
11. For quick deployment, select Use Selected Profile, then select defense from the drop-down box (Figure 38).
12. Click Apply. The client should start to reassociate with the access point using SSID = defense with no wireless security.
You can view your routed wireless subnets using the Cisco SDM wireless application by clicking Wireless Association in the left navigation bar to display a list of clients on your WLAN associated with the access point.

Figure 39 shows that employee User-abc1 using a Cisco Aironet 350 client is associated with the employee wireless subnet (VLAN 2), a guest using a Cisco Aironet 350 client, and an unnamed guest using a client card not from Cisco are associated with the hotspot (VLAN 100). the DHCP server assigns IP addresses to the clients automatically.

### Configuring Cisco LEAP Clients

1. Open the Cisco Aironet Client Utility Version 6.0.
2. Click the Profile Manager icon.
3. Click Add and enter a name (defenseLEAP) for the profile.

4. Click Apply.

5. On the Profile Properties screen, configure these system parameters:
   - Client Name: User-abc1 (optional)
   - SSID1: defense
   - Power Save Mode: CAM
   - Network Type: Infrastructure

7. Click the Network Security tab.

8. Choose LEAP from the Network Security Type drop-down box.

9. Click Configure…. The LEAP Settings screen appears (Figure 40).

10. Choose the desired user prompt mode for the Cisco LEAP authentication process. In our scenario, we selected Use Saved User Name and Password:
    - User Name: abc1
    - Password: abc1
    - Domain: leave it blank
11. Check Include Windows Logon Domain with User Name if single sign-on to a Microsoft domain is desired. In our scenario, uncheck it.

12. Make sure that the No Network Connection Unless User Is Logged In box is checked in order to automatically disassociate a client when a user logs off to prevent other users on a shared machine from using someone else’s credentials.

13. Configure the LEAP Authentication Timeout Value to extend the time permitted to authenticate the user to a domain controller. (The default is 90 seconds; the minimum is 10 seconds.)

14. Click OK.

15. From the Cisco Aironet Client Utility, click the Select Profile icon.

16. For quick deployment, select Use Selected Profile, then select defenseLEAP from the drop-down box (Figure 41).
17. Click Apply. The client should start to reauthenticate with the access point using Cisco LEAP (Figure 42).

You can verify your routed wireless subnets using the Cisco SDM wireless application by clicking Wireless Association in the left navigation bar to display a list of clients on your WLAN associated with the access point.

Figure 43 shows that employee User-abc1 using a Cisco Aironet 350 client is Extensible Authentication Protocol (EAP)—associated with the employee wireless subnet (VLAN 2), a guest using a Cisco Aironet 350 client, and an unnamed guest using a client card not from Cisco are associated with the hotspot (VLAN 100).
### Association

<table>
<thead>
<tr>
<th>Clients</th>
<th>Repeater</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

**View:** Client ✔ Repeater ✔

### Radio0.802.11G

#### SSID defense:

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Name</th>
<th>IP Address</th>
<th>MAC Address</th>
<th>State</th>
<th>Parent</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>350-client</td>
<td>user-acl</td>
<td>192.168.2.10</td>
<td>00d0.59e8.65c2</td>
<td>EAP-Associated</td>
<td>self</td>
<td>2</td>
</tr>
</tbody>
</table>

#### SSID hotspot:

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Name</th>
<th>IP Address</th>
<th>MAC Address</th>
<th>State</th>
<th>Parent</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>350-client</td>
<td>guest</td>
<td>10.10.100.13</td>
<td>0002.8a10.5993</td>
<td>Associated</td>
<td>self</td>
<td>100</td>
</tr>
</tbody>
</table>

- 10.10.100.15 | 001cf3.09e8e | Associated | self  | 100     |

In summary, by using the Cisco SDM and the Cisco SDM wireless application, users can quickly deploy secured bridged and routed wireless networks.
Reference

Online help for the Cisco SDM wireless application: www.cisco.com/univercd/cc/td/doc/product/software/sdm/wlanui/es_1.htm