



# CHAPTER 9

## Configuring a Wireless LAN Connection

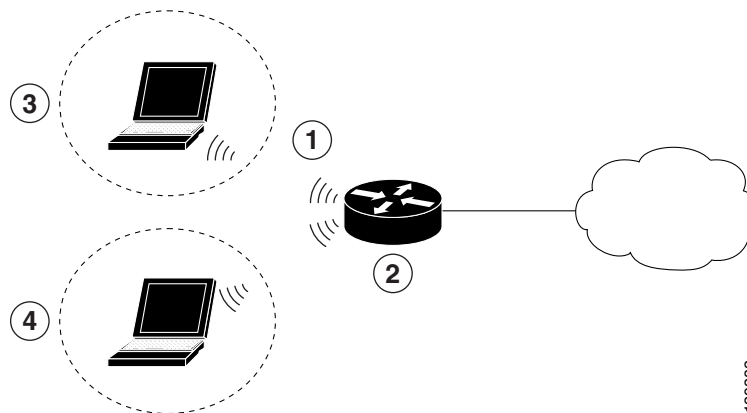
The Cisco Secure Router 520 Series routers support a secure, affordable, and easy-to-use wireless LAN solution that combines mobility and flexibility with the enterprise-class features required by networking professionals. With a management system based on Cisco IOS software, the Cisco routers act as access points, and are Wi-Fi certified, IEEE 802.11a/b/g-compliant wireless LAN transceivers.

You can configure and monitor the routers using the command-line interface (CLI), the browser-based management system, or Simple Network Management Protocol (SNMP). This chapter describes how to configure the router using the CLI. Use the **interface dot11radio** global configuration CLI command to place the device into radio configuration mode.

See the *Cisco Access Router Wireless Configuration Guide* for more detailed information about configuring these Cisco routers in a wireless LAN application.

Figure 9-1 shows a wireless network deployment.

**Figure 9-1** Wireless Connection to the Cisco Router



1	Wireless LAN (with multiple networked devices)
2	Cisco Secure Router 520 Series router connected to the Internet
3	VLAN 1
4	VLAN 2

In the configuration example that follows, a remote user is accessing the Cisco Secure Router 520 Series router using a wireless connection. Each remote user has his own VLAN.

**Configuration Tasks**

Perform the following tasks to configure this network scenario:

- [Configure the Root Radio Station](#)
- [Configure Bridging on VLANs](#)
- [Configure Radio Station Subinterfaces](#)

A configuration example showing the results of these configuration tasks is provided in the “[Configuration Example](#)” section on page 9-6.

**Note**

The procedures in this chapter assume that you have already configured basic router features as well as PPPoE or PPPoA with NAT. If you have not performed these configurations tasks, see [Chapter 1, “Basic Router Configuration,”](#) [Chapter 3, “Configuring PPP over Ethernet with NAT,”](#) and [Chapter 4, “Configuring PPP over ATM with NAT,”](#) as appropriate for your router. You may have also configured DHCP, VLANs, and secure tunnels.

## Configure the Root Radio Station

Perform these steps to create and configure the root radio station for your wireless LAN, beginning in global configuration mode:

	Command	Purpose
Step 1	<b>interface</b> <i>name number</i>  <b>Example:</b> Router(config)# <b>interface dot11radio 0</b> Router(config-if)#	Enters interface configuration mode for the radio interface.
Step 2	<b>broadcast-key</b> [ <b>vlan</b> <i>vlan-id</i> ] <b>change</b> <i>seconds</i>  <b>Example:</b> Router(config-if)# <b>broadcast-key vlan 1 change 45</b> Router(config-if)#	Specifies the time interval, in seconds, between rotations of the broadcast encryption key used for clients.  <b>Note</b> Client devices using static Wired Equivalent Privacy (WEP) cannot use the access point when you enable broadcast key rotation—only wireless client devices using 802.1x authentication (such as Light Extensible Authentication Protocol [LEAP], Extensible Authentication Protocol–Transport Layer Security [EAP-TLS], or Protected Extensible Authentication Protocol [PEAP]) can use the access point.  <b>Note</b> This command is not supported on bridges.  See the <a href="#">Cisco IOS Commands for Access Points and Bridges</a> for more details.

	Command	Purpose
Step 3	<p><b>encryption</b> <i>method algorithm key</i></p> <p><b>Example:</b>  Router(config-if)# <b>encryption</b> <b>vlan 1 mode</b>  <b>ciphers</b> <b>tkip</b>  Router(config-if)#</p>	<p>Specifies the encryption method, algorithm, and key used to access the wireless interface.</p> <p>The example uses the VLAN with optional encryption method of data ciphers.</p>
Step 4	<p><b>ssid</b> <i>name</i></p> <p><b>Example:</b>  Router(config-if)# <b>ssid</b> <b>cisco</b>  Router(config-if-ssid)#</p>	<p>Creates a Service Set ID (SSID), the public name of a wireless network.</p> <p><b>Note</b> All of the wireless devices on a WLAN must employ the same SSID to communicate with each other.</p>
Step 5	<p><b>vlan</b> <i>number</i></p> <p><b>Example:</b>  Router(config-if-ssid)# <b>vlan 1</b>  Router(config-if-ssid)#</p>	<p>Binds the SSID with a VLAN.</p>
Step 6	<p><b>authentication</b> <i>type</i></p> <p><b>Example:</b>  Router(config-if-ssid)# <b>authentication</b> <b>open</b>  Router(config-if-ssid)# <b>authentication</b>  <b>network-eap</b> <b>eap_methods</b>  Router(config-if-ssid)# <b>authentication</b>  <b>key-management</b> <b>wpa</b></p>	<p>Sets the permitted authentication methods for a user attempting access to the wireless LAN.</p> <p>More than one method can be specified, as shown in the example.</p>
Step 7	<p><b>exit</b></p> <p><b>Example:</b>  Router(config-if-ssid)# <b>exit</b>  Router(config-if)#</p>	<p>Exits SSID configuration mode, and enters interface configuration mode for the radio interface.</p>
Step 8	<p><b>speed</b> <i>rate</i></p> <p><b>Example:</b>  Router(config-if)# <b>speed</b> <b>basic-1.0 basic-2.0</b>  <b>basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0</b>  <b>36.0 48.0 54.0</b>  Router(config-if)#</p>	<p>(Optional) Specifies the required and allowed rates, in Mbps, for traffic over the wireless connection.</p>
Step 9	<p><b>rts</b> [<b>retries</b>   <b>threshold</b>]</p> <p><b>Example:</b>  Router(config-if)# <b>rts</b> <b>threshold</b> <b>2312</b>  Router(config-if)#</p>	<p>(Optional) Specifies the Request to Send (RTS) threshold or the number of times to send a request before determining the wireless LAN is unreachable.</p>

	Command	Purpose
Step 10	<p><b>power</b> [client   local] [cck [number   maximum]   ofdm [number   maximum]]</p> <p><b>Example:</b></p> <pre>Router(config-if)# power local cck 17 Router(config-if)# power local ofdm 17 Router(config-if)#</pre>	<p>(Optional) Specifies the radio transmitter power level.</p> <p>See the <i>Cisco Access Router Wireless Configuration Guide</i> for available power level values.</p>
Step 11	<p><b>channel</b> [number   least-congested]</p> <p><b>Example:</b></p> <pre>Router(config-if)# channel 2462 Router(config-if)#</pre>	<p>(Optional) Specifies the channel on which communication occurs.</p> <p>See the <i>Cisco Access Router Wireless Configuration Guide</i> for available channel numbers.</p>
Step 12	<p><b>station-role</b> [repeater   root]</p> <p><b>Example:</b></p> <pre>Router(config-if)# station-role root Router(config-if)#</pre>	<p>(Optional) Specifies the role of this radio interface.</p> <p>You must specify at least one root interface.</p>
Step 13	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>Router(config-if)# exit Router(config)#</pre>	<p>Exits interface configuration mode, and enters global configuration mode.</p>

## Configure Bridging on VLANs

Perform these steps to configure integrated routing and bridging on VLANs, beginning in global configuration mode:

	Command or Action	Purpose
Step 1	<p><b>bridge</b> [number   crb   irb   mac-address-table]</p> <p><b>Example:</b></p> <pre>Router(config)# bridge irb Router(config)#</pre>	<p>Specifies the type of bridging.</p> <p>The example specifies integrated routing and bridging.</p>
Step 2	<p><b>interface</b> name number</p> <p><b>Example:</b></p> <pre>Router(config)# interface vlan 1 Router(config-if)#</pre>	<p>Enters interface configuration mode.</p> <p>We want to set up bridging on the VLANs, so the example enters the VLAN interface configuration mode.</p>

	Command or Action	Purpose
Step 3	<b>bridge-group</b> <i>number</i>  <b>Example:</b> Router(config-if)# <b>bridge-group 1</b> Router(config-if)#	Assigns a bridge group to the interface.
Step 4	<b>bridge-group</b> <i>parameter</i>  <b>Example:</b> Router(config-if)# <b>bridge-group 1</b> <b>spanning-disabled</b> Router(config-if)#	Sets other bridge parameters for the bridging interface.
Step 5	<b>interface</b> <i>name number</i>  <b>Example:</b> Router(config-if)# <b>interface bvi 1</b> Router(config-if)#	Enters configuration mode for the virtual bridge interface.
Step 6	<b>ip address</b> <i>address mask</i>  <b>Example:</b> Router(config-if)# <b>ip address 10.0.1.1</b> <b>255.255.255.0</b> Router(config-if)#	Specifies the address for the virtual bridge interface.

Repeat [Step 2](#) through [Step 6](#) above for each VLAN that requires a wireless interface.

## Configure Radio Station Subinterfaces

Perform these steps to configure subinterfaces for each root station, beginning in global configuration mode:

	Command	Purpose
Step 1	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# <b>interface dot11radio 0.1</b> Router(config-subif)#	Enters subinterface configuration mode for the root station interface.
Step 2	<b>description</b> <i>string</i>  <b>Example:</b> Router(config-subif)# <b>description Cisco open</b> Router(config-subif)#	Provides a description of the subinterface for the administrative user.

	Command	Purpose
Step 3	<b>encapsulation dot1q <i>vlanID</i> [native   second-dot1q]</b>  <b>Example:</b> Router(config-subif)# <b>encapsulation dot1q 1 native</b> Router(config-subif)#	Specifies that IEEE 802.1Q (dot1q) encapsulation is used on the specified subinterface.
Step 4	<b>no cdp enable</b>  <b>Example:</b> Router(config-subif)# <b>no cdp enable</b> Router(config-subif)#	Disables the Cisco Discovery Protocol (CDP) on the wireless interface.
Step 5	<b>bridge-group <i>number</i></b>  <b>Example:</b> Router(config-subif)# <b>bridge-group 1</b> Router(config-subif)#	Assigns a bridge group to the subinterface.  <b>Note</b> When the bridge-group command is enabled, the following commands are automatically enabled, and cannot be disabled. If you disable these commands you may experience an interruption in wireless device communication.  <pre>           bridge-group 1           subscriber-loop-control            bridge-group 1 spanning-disabled            bridge-group 1           block-unknown-source           </pre>
Step 6	<b>exit</b>  <b>Example:</b> Router(config-subif)# <b>exit</b> Router(config)#	Exits subinterface configuration mode, and enters global configuration mode.

Repeat these steps to configure more subinterfaces, as needed.

## Configuration Example

The following configuration example shows a portion of the configuration file for the wireless LAN scenario described in the preceding sections.

```

!
bridge irb
!
interface Dot11Radio0
no ip address
!
broadcast-key vlan 1 change 45
!

```

```
!
encryption vlan 1 mode ciphers tkip
!
ssid cisco
  vlan 1
  authentication open
  wpa-psk ascii 0 cisco123
  authentication key-management wpa
!
ssid ciscowep
  vlan 2
  authentication open
!
ssid ciscowpa
  vlan 3
  authentication open
!
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
rts threshold 2312
power local cck 50
power local ofdm 30
channel 2462
station-role root
!
interface Dot11Radio0.1
description Cisco Open
encapsulation dot1Q 1 native
no cdp enable
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.2
encapsulation dot1Q 2
bridge-group 2
bridge-group 2 subscriber-loop-control
bridge-group 2 spanning-disabled
bridge-group 2 block-unknown-source
no bridge-group 2 source-learning
no bridge-group 2 unicast-flooding
!
interface Dot11Radio0.3
encapsulation dot1Q 3
bridge-group 3
bridge-group 3 subscriber-loop-control
bridge-group 3 spanning-disabled
bridge-group 3 block-unknown-source
no bridge-group 3 source-learning
no bridge-group 3 unicast-flooding
!
interface Vlan1
no ip address
bridge-group 1
bridge-group 1 spanning-disabled
!
interface Vlan2
no ip address
bridge-group 2
bridge-group 2 spanning-disabled
!
interface Vlan3
```

## ■ Configuration Example

```
no ip address
bridge-group 3
bridge-group 3 spanning-disabled
!
interface BVI1
ip address 10.0.1.1 255.255.255.0
!
interface BVI2
ip address 10.0.2.1 255.255.255.0
!
interface BVI3
ip address 10.0.3.1 255.255.255.0
!
```