Configuring a Basic Wireless LAN Connection

This module describes how to configure a wireless LAN (WLAN) connection between a wireless device, such as a laptop computer or mobile phone, and a Cisco 800, 1800 (fixed and modular), 2800, or 3800 series integrated services router, hereafter referred to as an access point or AP, using the Cisco IOS CLI. It also describes how to configure the access point in bridging or routing mode with basic authentication, and how to verify and monitor wireless LAN settings.

Upon completion of this module, you will need to configure security features on your wireless LAN such as encryption and authentication, adjust radio settings, configure VLANs, configure quality of service (QoS), and configure RADIUS servers, as needed.

Module History

This module was first published on December 15, 2005.

Information on Features in This Module

Your Cisco IOS software release may not support all features. To find information about feature support and configuration, see the "Cisco IOS Wireless LAN Features Roadmap" module.

Contents

Prerequisites for Configuring a Basic Wireless LAN Connection

The following prerequisites apply to configuring a basic wireless LAN connection using the Cisco IOS CLI:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- Read the "Wireless LAN Overview" module.
- Make sure you are using a computer connected to the same network as the access point, and obtain the following information from your network administrator:
  - The Service Set Identifier (SSID) for your wireless network
  - If your access point is not connected to a Dynamic Host Configuration Protocol (DHCP) server, a unique IP address for your access point (such as 172.17.255.115)

Information About Configuring a Basic Wireless LAN

Before you configure a basic wireless LAN, you should understand the following concepts:

- Service Set Identifiers in Wireless LANs, page 14

Service Set Identifiers in Wireless LANs

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or subnetwork can use the same SSID. SSIDs are case sensitive and can contain up to 32 alphanumeric characters.

You can create up to 16 SSIDs on Cisco 1800 series routers or routers equipped with the access point high-speed WAN interface card (AP HWIC), such as the Cisco 2800 and 3800 series routers. You can create up to 10 SSIDs on Cisco 800 series routers. Assign different configuration settings to each SSID. All the SSIDs are active at the same time; that is, client devices can associate to the access point using any of the SSIDs.

You can assign multiple SSIDs to the same interface or subinterface as long as all of the SSIDs have the same encryption. If, for example, you want to configure two SSIDs, each with its own encryption, you must configure two VLANs and assign an SSID to each VLAN.

If you want the access point to allow associations from client devices that do not specify an SSID in their configurations, you can set up a guest SSID. The access point includes the guest SSID in its beacon. However, if the network must be secure, do not create a guest mode SSID on the access point.

If your network uses VLANs, you can assign one SSID to a VLAN, and client devices using the SSID are grouped in that VLAN. See the "Configuring Wireless VLANs" module for more information.

Spaces in SSIDs

You can include spaces in an SSID, but be careful not to add spaces to an SSID accidentally, especially trailing spaces (spaces at the end of an SSID). If you add trailing spaces, it might appear that you have identical SSIDs configured on the same access point. If you think you configured identical SSIDs on the access point, enter the **show dot11 associations** command and examine the output to check your SSIDs for trailing spaces.

For example, this sample output from a **show configuration** command does not show spaces in SSIDs:

```
ssid cisco
 vlan 77
 authentication open

ssid cisco
 vlan 17
 authentication open
```

```
ssid cisco
 vlan 7
 authentication open
```

However, this sample output from a **show dot11 associations** command shows the spaces in the SSIDs:

```
SSID [anyname] :
SSID [anyname ] :
SSID [anyname] :
```

How to Configure a Basic Wireless LAN Connection

This section contains the following tasks:

- Configuring Bridging Mode and Open Authentication on an Access Point, page 15 (required, depending on desired network configuration)
- Configuring Routing Mode and Open Authentication on an Access Point, page 19 (required, depending on desired network configuration)
- Verifying and Monitoring Wireless LAN Settings, page 21 (optional)

Configuring Bridging Mode and Open Authentication on an Access Point

Perform this task to configure bridging mode and open authentication on an access point.

Bridging mode should be used on an access point if one or more of the following conditions is required:

- You want to bridge non-IP traffic (for example, IPX, AppleTalk, and SNA) between the wired and wireless devices.
- You want to configure the network so that the devices on the FastEthernet ports and the wireless clients are on the same IP subnet.

Note Configuring the network in this way limits the capability to filter traffic between the wireless devices and devices on the FastEthernet interfaces.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bridge irb**
4. **bridge** *bridge-group* **route** *protocol*
5. **interface dot11Radio** *interface*
6. **ssid** *name*
7. **authentication open** [**mac-address** *list-name*] [**eap** *list-name*]
8. **exit**
9. **bridge-group** *bridge-group*
10. **bridge-group** *bridge-group* **subscriber-loop-control**
11. **bridge-group** *bridge-group* **spanning-disabled**

12. **bridge-group** *bridge-group* **block-unknown-source**
13. **no bridge-group** *bridge-group* **source-learning**
14. **no bridge-group** *bridge-group* **unicast-flooding**
15. **no shutdown**
16. **exit**
17. **interface** *type number*
18. **bridge-group** *bridge-group*
19. **bridge-group** *bridge-group* **spanning-disabled**
20. **exit**
21. **interface** *type number*
22. **ip address** *ip-address mask* [**secondary**]
23. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enters privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`bridge irb`
	
	Example:
	`Router(config)# bridge irb`
		Enables the Cisco IOS software to route a given protocol between routed interfaces and bridge groups.

Step 4	**bridge** *bridge-group* **route** *protocol* **Example:** `Router(config)# bridge 1 route ip`	Enables the routing of a specified protocol in a specified bridge group.
Step 5	**interface dot11Radio** *interface* **Example:** `Router(config)# interface dot11Radio 0`	Identifies the router wireless module and enters interface configuration mode for the radio interface. • For the Cisco 800 and 1800 series fixed-configuration routers, the *interface* argument can be either 0, for the 2.4-GHz, 802.11b/g radio port, or 1, for the 5-GHz, 802.11a radio port. • For the Cisco 1800 series modular router and the Cisco 2800 and 3800 series routers, the *interface* argument is in module/slot/port format, for example, 0/3/0.

	Command or Action	Purpose
Step 6	**ssid** *name* **Example:** `Router(config-if)# ssid floor1`	Specifies an SSID, the public name of your wireless network, and enters SSID configuration mode. • All of the wireless devices on a WLAN must use the same SSID to communicate with each other.
Step 7	**authentication open** [**mac-address** *list-name*] [**eap** *list-name*] **Example:** `Router(config-if-ssid)# authentication open`	Configures the radio interface for the specific SSID to support open authentication, and optionally MAC address authentication or Extensible Authentication Protocol (EAP) authentication.
Step 8	**exit** **Example:** `Router(config-if-ssid)# exit`	Exits SSID configuration mode.
Step 9	**bridge-group** *bridge-group* **Example:** `Router(config-if)# bridge-group 1`	Assigns a specific bridge group to the radio interface. • The *bridge-group* argument range is from 1 to 255.
Step 10	**bridge-group** *bridge-group* **subscriber-loop-control** **Example:** `Router(config-if)# bridge-group 1 subscriber-loop-control`	Enables loop control on virtual circuits associated with a bridge group.
Step 11	**bridge-group** *bridge-group* **spanning-disabled** **Example:** `Router(config-if)# bridge-group 1 spanning-disabled`	Disables spanning tree on the radio interface.
Step 12	**bridge-group** *bridge-group* **block-unknown-source** **Example:** `Router(config-if)# bridge-group 1 block-unknown-source`	Blocks traffic that comes from unknown MAC address sources.
Step 13	**no bridge-group** *bridge-group* **source-learning** **Example:** `Router(config-if)# no bridge-group 1 source-learning`	Disables source learning.
Step 14	**no bridge-group** *bridge-group* **unicast-flooding** **Example:** `Router(config-if)# no bridge-group 1 unicast-flooding`	Disables unicast flooding.

	Command or Action	Purpose
Step 15	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the radio interface. • If an SSID has not been configured for the radio interface, the interface cannot be enabled with the **no shutdown** command.
Step 16	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode for the radio interface.
Step 17	**interface** *type number* **Example:** `Router(config)# interface vlan 1`	Enters interface configuration mode for the VLAN interface. • The *number* argument range is from 1 to 1001.
Step 18	**bridge-group** *bridge-group* **Example:** `Router(config-if)# bridge-group 1`	Assigns a specific bridge group to the VLAN interface. • The *bridge-group* argument range is from 1 to 255.
Step 19	**bridge-group** *bridge-group* **spanning-disabled** **Example:** `Router(config-if)# bridge-group 1 spanning-disabled`	Disables spanning tree on the VLAN interface.
Step 20	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode for the VLAN interface.
Step 21	**interface** *type number* **Example:** `Router(config)# interface bvi 1`	Enters interface configuration mode for the creation of a bridge virtual interface (BVI). • The *number* argument range is from 1 to 255.
Step 22	**ip address** *ip-address mask* [**secondary**] **Example:** `Router(config-if)# ip address 10.0.1.1 255.255.255.0`	Assigns an IP address and address mask to the BVI. **Note** If you are connected to the access point using a Telnet session, you lose your connection to the access point when you assign a new IP address to the BVI. If you need to continue configuring the access point using Telnet, use the new IP address to open another Telnet session to the access point.

	Command or Action	Purpose

Step 23	`end`
	
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Step 24	`copy running-config startup-config`
	
	Example:
	`Router# copy running-config startup-config`
		Saves configuration changes to NVRAM so that they are not lost if there is a system reload or power outage.

Configuring Routing Mode and Open Authentication on an Access Point

Perform this task to configure routing mode and open authentication on an access point.

Routing mode should be used on an access point if one or more of the following conditions is required:

- You want to implement routing features on the radio interface to take advantage of features such as filtering and access lists.

  The radio interface is like other Layer 3 routeable interfaces: Configuring static or dynamic routing is required to route traffic between networks.
- You want to configure the network so that the wired LAN interface is on a different IP subnet than the wireless devices.
- You want to improve network performance by using features such as Cisco Express Forwarding.
- You want to increase network security by using firewalls, for example, to separate traffic between the wired devices and the wireless devices.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dot11Radio** *interface*
4. **ip address** *ip-address mask* [**secondary**]
5. **ssid** *name*
6. **authentication open** [**mac-address** *list-name*] [**eap** *list-name*]
7. **no shutdown**
8. **end**
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface dot11Radio** *interface* **Example:** `Router(config)# interface dot11Radio 0`	Identifies the router wireless module and enters interface configuration mode for the radio interface. • For the Cisco 800 and 1800 series fixed-configuration routers, the *interface* argument can be either 0, for the 2.4-GHz, 802.11b/g radio port, or 1, for the 5-GHz, 802.11a radio port. • For the Cisco 1800 series modular router and the Cisco 2800 and 3800 series routers, the *interface* argument is in module/slot/port format, for example, 0/3/0.
Step 4	**ip address** *ip-address mask* [**secondary**] **Example:** `Router(config-if)# ip address 10.0.1.1 255.255.255.0`	Assigns an IP address and address mask to the interface.
Step 5	**ssid** *name* **Example:** `Router(config-if)# ssid anyname`	Specifies an SSID, the public name of your wireless network, and enters SSID configuration mode. • The *name* argument is a case-sensitive alphanumeric string up to 32 characters in length. • All of the wireless devices on a WLAN must use the same SSID to communicate with each other.
Step 6	**authentication open** [**mac-address** *list-name*] [**eap** *list-name*] **Example:** `Router(config-if-ssid)# authentication open`	Configures the radio interface for the specified SSID to support open authentication. • Use the **aaa authentication login** command to define the *list-name* argument for MAC address and EAP authentication.
Step 7	**no shutdown** **Example:** `Router(config-if-ssid)# no shutdown`	Enables the radio interface and returns to interface configuration mode. • If an SSID has not been configured for the radio interface, the interface cannot be enabled with the **no shutdown** command.

	Command or Action	Purpose

Step 8	`end`
	
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Step 9	`copy running-config startup-config`
	
	Example:
	`Router# copy running-config startup-config`
		Saves configuration changes to NVRAM so that they are not lost if there is a system reload or power outage.

Verifying and Monitoring Wireless LAN Settings

Perform this task to verify and montior wireless LAN settings.

SUMMARY STEPS

1. **enable**
2. **show controllers dot11Radio** *interface*
3. **show dot11 associations [client | repeater | statistics |** *mac-address* **| bss-only | all-client | cckm-statistics]**
4. **show dot11 statistics client-traffic**
5. **show dot11 statistics interface**
6. **show interfaces dot11Radio** *interface* **aaa timeout**
7. **show interfaces dot11Radio** *interface* **statistics**
8. **clear dot11 client**
9. **clear dot11 hold-list**
10. **clear dot11 statistics {dot11Radio** *interface* **|** *mac-address***}**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enters privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`show controllers dot11Radio` *interface* **Example:** `Router# show controllers dot11Radio 0/0/0`	(Optional) Displays the status of the radio controller.

	Command or Action	Purpose
Step 3	**show dot11 associations** [**client** | **repeater** | **statistics** | *mac-address* | **bss-only** | **all-client** | **cckm-statistics**] **Example:** `Router# show dot11 associations client`	(Optional) Displays the radio association table and radio association statistics. • To display specific association information, use one of the optional keywords or argument.
Step 4	**show dot11 statistics client-traffic** **Example:** `Router# show dot11 statistics client-traffic`	(Optional) Displays radio client traffic statistics.
Step 5	**show dot11 statistics interface** **Example:** `Router# show dot11 statistics interface`	(Optional) Displays statistics for all dot11Radio interfaces.
Step 6	**show interfaces dot11Radio** *interface* **aaa timeout** **Example:** `Router# show interfaces dot11Radio 0/3/0 aaa timeout`	(Optional) Displays dot11 authentication, authorization, and accounting (AAA) timeout values for a specific radio interface.
Step 7	**show interfaces dot11Radio** *interface* **statistics** **Example:** `Router# show interfaces dot11Radio 0/3/0 statistics`	(Optional) Displays statistics for a specific dot11Radio interface.
Step 8	**clear dot11 client** **Example:** `Router# clear dot11 client`	(Optional) Deauthenticates a radio client with a specified MAC address. • Before a radio client can be deactivated, the client must be directly associated with the access point, not a repeater.
Step 9	**clear dot11 hold-list** **Example:** `Router# clear dot11 hold-list`	(Optional) Resets the MAC authentication hold list.
Step 10	**clear dot11 statistics** {**dot11Radio** *interface* | *mac-address*} **Example:** `Router# clear dot11 statistics dot11Radio 0/3/0`	(Optional) Resets statistic information for a specified radio interface or a particular client with a specified MAC address.

Configuration Examples for a Basic Wireless LAN Connection

This section contains the following examples:

Access Point in Bridging Mode with Open Authentication Configuration: Example

The following configuration example shows how to:

- Configure a basic wireless LAN connection between a wireless client and a 2.4-GHz, 802.11b/g radio interface on a Cisco 800 or Cisco 1800 series fixed-configuration router (access point).
- Configure the access point in bridging mode with open authentication.
- Define a bridge group and assign it to the radio interface and a VLAN interface.
- Create a BVI and assign an IP address to that interface.
- Verify connectivity between the client and access point.

No encryption is being configured in this basic connection.

```
configure terminal
 bridge irb
 bridge 1 route ip
 interface dot11Radio 0
 ssid ssid1
 authentication open
 exit
 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
 no shutdown
 exit
 interface vlan 1
 bridge-group 1
 bridge-group 1 spanning-disabled
 exit
 interface bvi 1
 ip address 10.0.1.2 255.255.255.0
 end
 copy running-config startup-config
 show dot11 associations client
```

Access Point in Routing Mode with Open Authentication Configuration: Example

The following configuration example shows how to:

- Configure a basic wireless LAN connection between a wireless client and a 2.4-GHz, 802.11b/g radio interface on a Cisco 3800 series router (access point).
- Configure the access point in routing mode with open authentication.
- Verify connectivity between the client and access point.

No encryption is being configured in this basic connection.

```
configure terminal
 interface dot11Radio 0/3/0
 ip address 10.0.1.1 255.255.255.0
 ssid ssid2
 authentication open
 no shutdown
 end
 copy running-config startup-config
 show dot11 associations client
```

Where to Go Next

After you configure the access point in bridging or routing mode with open authentication, you must configure security features to prevent unauthorized access to your network. Because it is a radio device, the access point can communicate beyond the physical boundaries of your building. Configure some combination of the following security features to protect your network from intruders:

- Encryption, such as Wired Equivalent Privacy (WEP), which scrambles the communication between the access point and client devices to keep the communication private. See the "Securing a Wireless LAN" module for more information.
- Client authentication, such as EAP, Lightweight Extensible Authentication Protocol (LEAP), EAP with Transport Layer Security (EAP-TLS), Protected Extensible Authentication Protocol (PEAP), or MAC-based authentication. See the "Securing a Wireless LAN" module for more information.
- Unique SSIDs that are not broadcast in the access point beacon. See the "Separating a Wireless Network by Configuring Multiple SSIDs" section in the "Securing a Wireless LAN" module for information on how to configure multiple SSIDs.

Additional References

The following sections provide references related to configuring a basic wireless LAN connection.

Related Documents

Related Topic	Document Title
Cisco IOS wireless LAN commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Wireless LAN Command Reference*, Release 12.4T
Cisco IOS bridging commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Bridging Command Reference*, Release 12.4T
Cisco IOS security and AAA commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Security Command Reference*, Release 12.4T

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport