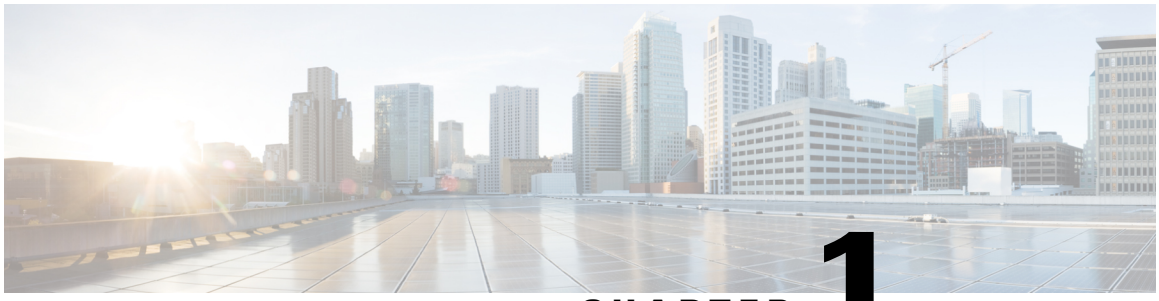
Wireless LAN Configuration Guide, Cisco IOS XE Fuji 16.7.x

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Wireless LAN Overview

A wireless LAN (WLAN) is, in some sense, nothing but a radio--with different frequencies and characteristics--acting as a medium for networks. The Cisco 800, 1800, 2800, and 3800 series integrated services routers, hereafter referred to as an access point or AP, serve as the connection point between wireless and wired networks or as the center point of a stand-alone wireless network. In large installations, wireless users within radio range of an AP can roam throughout a facility while maintaining seamless, uninterrupted access to the network.

Components of a traditional WLAN network include APs, network interface cards (NICs) or client adapters, bridges, repeaters, and antennae. Additionally, an authentication, authorization, and accounting (AAA) server (specifically a RADIUS server), network management server (NMS), and "wireless aware" switches and routers are considered as part of an enterprise WLAN network.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Wireless LANs

Purpose of This Guide

This guide provides the conceptual information, configuration tasks, and examples to help you configure and monitor a "wireless-aware" router using the Cisco IOS CLI, which can be used through a console port or Telnet session. You can also configure and monitor your router using the Security Device Manager (SDM) application or Simple Network Management Protocol (SNMP). SDM comes preinstalled on all new Cisco 850, 870, 1800, 2800, and 3800 series integrated services routers.

Organization of This Guide

This guide is organized into the following modules:

- " Configuring a Basic Wireless LAN Connection "--Describes how to configure basic wireless settings using the Cisco IOS CLI. Examples of how to configure the AP in bridging and routing mode, and how to set up basic WLAN security, such as encryption and authentication, are provided.
- " Securing a Wireless LAN "--Describes how to configure security features in a WLAN, such as Wired Equivalent Privacy (WEP) encryption and features to protect WEP keys including Wi-Fi Protected Access (WPA) authenticated key management, Message Integrity Check (MIC), Temporal Key Integrity Protocol (TKIP), and broadcast key rotation. It also describes how to configure various types of AP authentication, such as open, shared key, MAC address, and Extensible Authentication Protocol (EAP), and how to configure multiple Service Set Identifiers (SSIDs).
- " Configuring RADIUS or a Local Authenticator in a Wireless LAN "--Describes how to enable and configure RADIUS, which provides detailed accounting information and flexible administrative control over the authentication and authorization processes. This module also describes how to configure the AP to act as a local RADIUS server for your WLAN. If a WAN connection to your main RADIUS server fails, the AP acts as a backup server to authenticate wireless devices.
- " Configuring Wireless VLANs "--Describes how to configure your AP to interoperate with VLANs on your wired LAN.
- " Implementing Quality of Service in a Wireless LAN "--Describes how to configure your AP to use the quality of service (QoS) features on your wired LAN.
- " Wireless LAN Error Messages "-- Lists the WLAN CLI error and event messages.

Roaming Wireless Client Devices

If you have more than one AP in your WLAN, wireless client devices can roam seamlessly from one AP to another. The roaming functionality is based on signal quality, not proximity. When a client's signal quality drops, the client device roams to another AP.

WLAN users are sometimes concerned when a client device stays associated to a distant AP instead of roaming to a closer AP. However, if a client's signal to a distant AP remains strong and the signal quality is high, the

client will not roam to a closer AP. Checking constantly for closer APs would be inefficient, and the extra radio traffic would slow throughput on the WLAN.

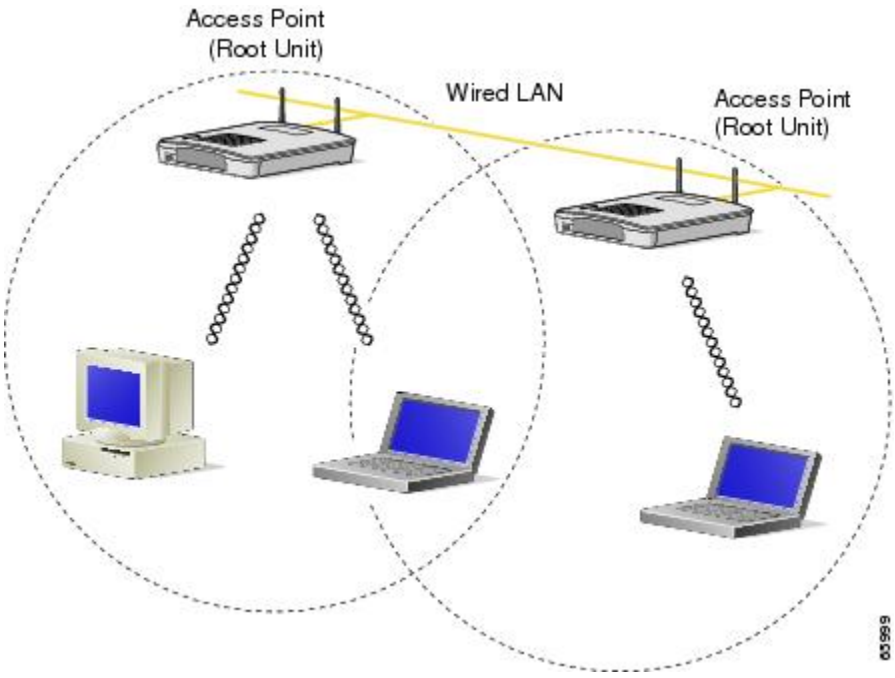
Common Wireless Network Configurations

This section describes the AP's role in three common wireless network configurations. The AP's default configuration is as a root unit connected to a wired LAN or as the central unit in an all-wireless network. The repeater role requires a specific configuration.

Root Unit on a Wired LAN

An AP connected directly to a wired LAN provides a connection point for wireless users. If more than one AP is connected to the LAN, users can roam from one area of a facility to another without losing their connection to the network. As users move out of range of one AP, they automatically associate to the network through another AP. The roaming process is seamless and transparent to the user. The figure below shows APs acting as root units on a wired LAN.

Figure 1: Access Points as Root Units on a Wired LAN

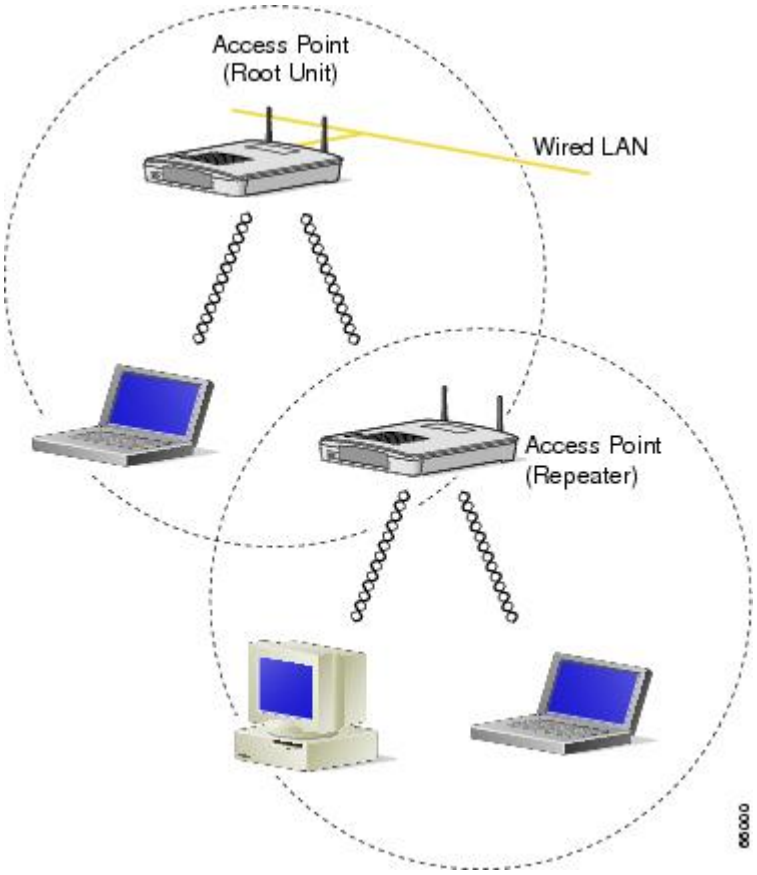


Repeater Unit That Extends Wireless Range

An AP can be configured as a standalone repeater to extend the wireless range of your infrastructure or to overcome an obstacle that blocks radio communication. The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an AP connected to the wired LAN. The data is sent through the route that provides the best performance for the client. The figure below shows an AP acting as a repeater.

Note Non-Cisco client devices might have difficulty communicating with repeater APs.

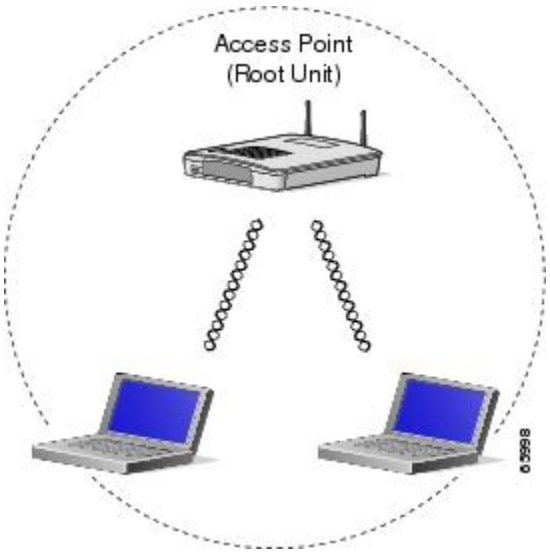
Figure 2: Access Point as a Repeater



Central Unit in an All-Wireless Network

In an all-wireless network, an AP acts as a standalone root unit. The AP is not attached to a wired LAN; it functions as a hub linking all stations. The AP serves as the focal point for communications, increasing the communication range of wireless users. The figure below shows an AP in an all-wireless network.

Figure 3: Access Point as a Central Unit in an All-Wireless Network



Additional References

The following sections provide references related to configuring and monitoring a WLAN.

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*
Configuration information for the Cisco 850 series and Cisco 870 series access routers	*Cisco 850 Series and Cisco 870 Series Access Routers* http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/85x87x/index.htm
Configuration information for the Cisco 1800 series integrated services routers (fixed)	*Cisco 1800 Series Integrated Services Routers (Fixed)* http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1800fix/index.htm
Configuration information for the Cisco 1800 series integrated services routers (modular)	*Cisco 1800 Series Integrated Services Routers (Modular)* http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1800/index.htm

Related Topic	Document Title
Configuration information for the Cisco 2800 series integrated services routers	*Cisco 2800 Series Integrated Services Routers* http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/2800/index.htm
Configuration information for the Cisco 3800 series integrated service routers	*Cisco 3800 Series Integrated Services Routers* http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/3800/index.htm
Information on SDM	*Cisco Router and Security Device Manager* http://www.cisco.com/en/US/products/sw/secursw/ps5318/tsd_products_support_series_home.html

Standards

Standard	Title
IEEE 802.11	*Part II: Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications.*
IEEE 802.11a	*Higher-Speed Physical Layer Extension in the 5-GHz Band*
IEEE 802.11b	*Higher-Speed Physical Layer Extension in the 2.4-GHz Band*
IEEE 802.11g	*Amendment 4: Further Higher Data Rate Extension in the 2.4-GHz Band*

MIBs

MIB	MIBs Link
• CISCO-DOT11-ASSOCIATION-MIB • CISCO-DOT11-IF-MIB • CISCO-IETF-DOT11-QOS-EXT-MIB • CISCO-IETF-DOT11-QOS-MIB • CISCO-TBRIDGE-DEV-IF-MIB • CISCO-WLAN-VLAN-MIB	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

Glossary

access point --An AP operates within a specific frequency spectrum and uses an 802.11 standard modulation technique. It also informs the wireless clients of its availability and authenticates and associates wireless clients to the wireless network. An AP also coordinates the wireless clients' use of wired resources. It should be noted that there are several kinds of APs, including single radio and multiple radios, based on different 802.11 technologies.

antenna --An antenna radiates the modulated signal through the air so that wireless clients can receive it. Characteristics of an antenna are defined by propagation pattern (directional versus omnidirectional), gain, transmit power, and so on. Antennas are needed on the APs, bridges, and clients.

client adapter --A PC or workstation uses a client adapter or wireless NIC to connect to the wireless network. The NIC scans the available frequency spectrum for connectivity and associates to the AP or another wireless client. The NIC is coupled to the PC or workstation operating system (OS) using a software driver. Various client adapters are available from Cisco.

EAP --Extensible Authentication Protocol. EAP is a flexible protocol used to carry authentication information. It is defined in RFC 2284.

IEEE --The Institute of Electrical and Electronic Engineers is, among other things, a standards body. IEEE publishes standards for many types of systems, and is well known for its standards on information exchange between computers--from best practices to IT infrastructure to LAN and MAN standards to portable applications standards.

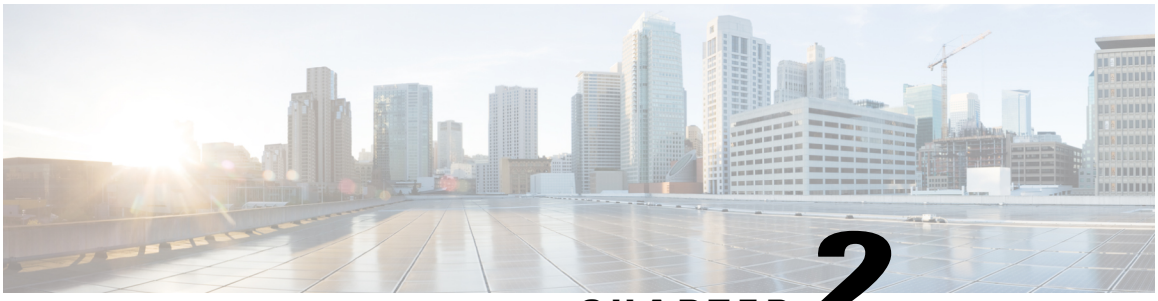
MAC --Media Access Control address. A unique 48-bit number used in Ethernet data packets to identify an Ethernet device, such as an AP or client adapter.

MIC --Message Integrity Check algorithm.

SSID --Service Set Identifier. A unique identifier used to identify a radio network and which stations must use to be able to communicate with each other or with an AP.

TKIP --Temporal Key Integrity Protocol. Developed to fix the problems with WEP. TKIP consists of three protocols: a cryptographic message integrity algorithm, a key mixing algorithm, and an enhancement to the initialization vector (IV).

WEP --Wired Equivalent Privacy. An optional security mechanism defined within the 802.11 standard designed to make the link integrity of wireless devices equal to that of a wired Ethernet.



CHAPTER 2

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.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring a Basic Wireless LAN Connection

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

- 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

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

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. **end**
24. **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.

	Command or Action	Purpose
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.
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.

	Command or Action	Purpose
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.
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*	Enters interface configuration mode for the VLAN interface.

	Command or Action	Purpose
	Example: `Router(config)# interface vlan 1`	• 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.
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.

	Command or Action	Purpose
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.
Step 8	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
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.

	Command or Action	Purpose
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

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*
Cisco IOS bridging commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Bridging Command Reference*

Related Topic	Document Title
Cisco IOS security and AAA commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Security Command Reference*

Standards

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

MIBs

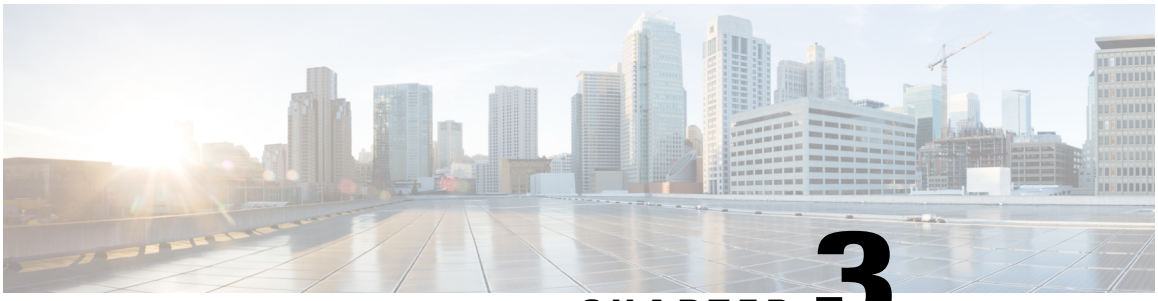
MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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



CHAPTER 3

Configuring Multiple Basic Service Set Identifiers and Microsoft WPS IE SSIDL

This module describes how to configure multiple basic service set identifiers (BSSID) on a Cisco 800, 1800, 2800, or 3800 series integrated services router, hereafter referred to as an access point (AP).

Access point 802.11a and 802.11g radios support up to 16 BSSIDs which are similar to MAC addresses. You use multiple BSSIDs to broadcast more than one SSID in beacons.

Devices on your wireless LAN that are configured to associate to a specific access point based on the access point MAC address (for example, client devices, repeaters, hot standby units, or workgroup bridges) might lose their association when you add or delete a multiple BSSID. When you add or delete a multiple BSSID, check the association status of devices configured to associate to a specific access point. If necessary, reconfigure the disassociated device to use the BSSID's new MAC address.

This module also describes how to configure the Microsoft WPS IE SSIDL feature. This feature allows an access point to broadcast a list of configured SSIDs such as SSID Lists (SSIDL) in the Microsoft Wireless Provisioning Services information element (WPS IE). A client with the ability to read the SSIDL can alert the user to the availability of the SSIDs.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Multiple Basic Service Set Identifiers and Microsoft WPS IE SSIDL

The following prerequisites apply to configuring multiple BSSIDs and Microsoft WPS IE SSIDL:

- VLANs must be configured.
- Access points must run Cisco IOS Release 12.4(15)T or a later release.
- Access points must contain an 802.11a or 802.11g radio that supports multiple BSSIDs. To determine whether a radio supports multiple basic SSIDs, enter the show controllers radio-interface command. The radio supports multiple basic SSIDs if the results include this line:

Number of supported simultaneous BSSID on radio-interface: 8

Information About Configuring Multiple Basic Service Set Identifiers and Microsoft WPS IE SSIDL

Guidelines for Using Multiple BSSIDs

Remember these guidelines when configuring multiple BSSIDs:

- RADIUS-assigned VLANs are not supported when you enable multiple BSSIDs.
- When you enable BSSIDs, the access point automatically maps a BSSID to each SSID. You cannot manually map a BSSID to a specific SSID.
- When multiple BSSIDs are enabled on the access point, the SSIDL IE does not contain a list of SSIDs; it contains only extended capabilities.
- Any Wi-Fi certified client device can associate to an access point using multiple BSSIDs.
- You can enable multiple BSSIDs on access points that participate in WDS.

How to Configure Multiple BSSIDs and Include an SSID in an SSIDL IE

Configuring Multiple BSSIDs on an Access Point

Perform this task to configure multiple BSSIDs on an access point.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot11 mbssid**
4. **dot11 ssid** *name*
5. **exit**
6. **interface dot11Radio** *interface*
7. **ssid** *name*
8. **end**
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dot11 mbssid** **Example:** `Router(config)# dot11 mbssid`	Enables multiple basic SSIDs on all access point radio interfaces.
Step 4	**dot11 ssid** *name* **Example:** `Router(config)# dot11 ssid guest`	Creates a global SSID. • The SSID is inactive until you use the **ssid** interface configuration command to assign the SSID to a specific radio interface.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-ssid)# exit`	Exits SSID configuration mode.
Step 6	**interface dot11Radio** *interface* **Example:** `Router(config)# interface dot11Radio 0/3/0`	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 7	**ssid** *name* **Example:** `Router(config-if)# ssid guest`	Creates an SSID for a radio interface.
Step 8	**end** **Example:** `Router(config-if-ssid)# end`	Returns to privileged EXEC mode.
Step 9	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Including an SSID in an SSIDL IE

The access point or bridge beacon can advertise only one broadcast SSID. However, you can use SSIDL information elements (SSIDL IEs) in the access point or bridge beacon to alert client devices of additional SSIDs on the access point or bridge. When you designate an SSID to be included in an SSIDL IE, client devices detect that the SSID is available, and they also detect the security settings required to associate using that SSID.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot11 ssid** *name*
4. **information-element ssidl [advertisement wps]**
5. Repeat Steps 3 and 4 for each SSID you want included in the information element.
6. **exit**
7. **interface dot11Radio** *interface*
8. **ssid** *name*
9. **end**
10. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dot11 ssid** *name* **Example:** `Router(config)# dot11 ssid guest`	Creates a global SSID. • The SSID is inactive until you use the **ssid** interface configuration command to assign the SSID to a specific radio interface.
Step 4	**information-element ssidl [advertisement wps]** **Example:** `Router(config-ssid)# information-element ssidl advertisement`	Designates an SSID for inclusion in an SSIDL IE that the access point includes in its beacons.
Step 5	Repeat Steps 3 and 4 for each SSID you want included in the information element.	--

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-ssid)# exit`	Exits SSID configuration mode.
Step 7	**interface dot11Radio** *interface* **Example:** `Router(config)# interface dot11Radio 0/3/0`	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 8	**ssid** *name* **Example:** `Router(config-if)# ssid guest`	Assigns a globally configured SSID to a radio interface and enters SSID configuration mode. • If you created more than one global SSID in Step 3, you would repeat this command for each SSID name.
Step 9	**end** **Example:** `Router(config-if-ssid)# end`	Returns to privileged EXEC mode.
Step 10	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuration Examples for Configuring Multiple Basic Service Set Identifiers

Configuring Multiple BSSIDs on an Access Point Example

This example shows the CLI commands that you use to enable multiple BSSIDs on a radio interface, create an SSID named visitor, designate the SSID as a BSSID, specify that the BSSID is included in beacons, and assign the SSID visitor to the radio interface:

```
configure terminal
 dot11 mbssid
 dot11 ssid visitor
 exit
 interface dot11 0
 ssid visitor
 end
```

Additional References

The following sections provide references related to configuring Multiple BSSIDs:

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*

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified by this feature.	--

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

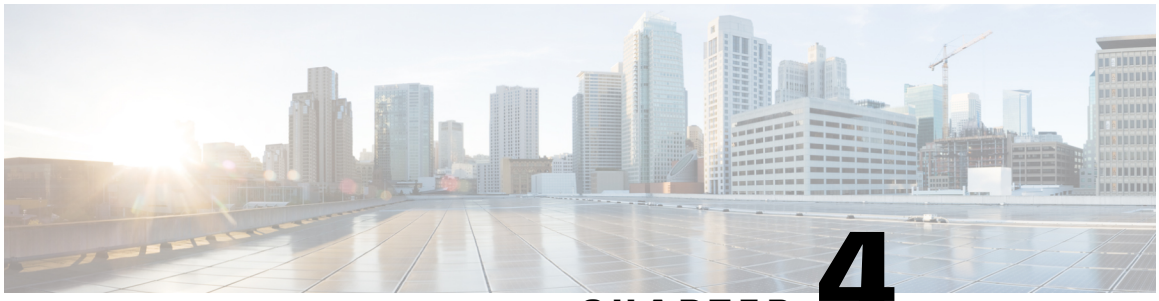
Feature Information for Configuring Multiple Basic Service Set Identifiers and Microsoft WPS IE SSIDL

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Configuring Multiple Basic Service Set Identifiers (BSSIDs)

Feature Name	Releases	Feature Information
Microsoft WPS IE SSIDL	12.4(15)T	This feature allows an access point to broadcast a list of configured SSIDs such as SSID Lists (SSIDL) in the Microsoft Wireless Provisioning Services Information Element (WPS IE). A client with the ability to read the SSIDL can alert the user to the availability of the SSIDs.
Multiple Basic Service Set ID (BSSID)	12.4(15)T	This feature permits a single access point (AP) to appear to the wireless LAN (WLAN) as multiple virtual APs.



CHAPTER 4

Securing a Wireless LAN

This module describes how to apply strong wireless security mechanisms on a Cisco 800, 1800, 2800, or 3800 series integrated services router, hereafter referred to as an access point (AP), to ensure that a wireless LAN is protected against unauthorized access and eavesdropping.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the Feature Information for Securing a Wireless LAN, on page 68.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To

find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Securing a Wireless LAN

The following prerequisites apply to securing a wireless LAN:

- Read the "Wireless LAN Overview" module.
- Read the "Configuring a Basic Wireless LAN Connection" module.

Information About Securing a Wireless LAN

Wired Equivalent Privacy in a Wireless LAN

The first, most basic level of a secure wireless LAN is the presence of a Wired Equivalent Privacy (WEP) key. The WEP key is unique to the client and provides the client with the appropriate level of network access. WEP keys encrypt both unicast and multicast messages. Because WEP is the first line of defense against intruders, we recommend that you use full encryption on your wireless network.

WEP Weaknesses

WEP is vulnerable to attack for several reasons:

- Distributing WEP keys manually is a time-intensive, laborious task. Because it is tedious to manually rekey the WEP code, the keys are not likely to change frequently. Therefore, an attacker probably has enough time to decipher the key.
- When keys are not changed often, attackers can compile so-called *decryption dictionaries* . These are huge collections of frames, encrypted with the same key. These frames can then be analyzed and used for attack.
- Standardized WEP implementations use 64- or 128-bit shared keys. Although the 128-bit key sounds excessively durable, it is still possible to crack a key this size within a short interval with sustained traffic.
- WEP uses Rivest Cipher 4 (RC4) for encryption. Of all the possible RC4 keys, the statistics for the first few bytes of output are nonrandom, which can provide information about the key.

Note RC4 is the most widely used software stream cipher. In addition to WEP, it is used in Secure Socket Layer (SSL), the encryption medium used for web pages. Although widely deployed and adequate for web use, it is generally not considered a good means of encryption for WLANs.

Wi-Fi Protected Access in a Wireless LAN

Wi-Fi Protected Access (WPA) was designed as a more secure replacement for WEP. The Temporal Key Integrity Protocol (TKIP), also known as *WEP key hashing* , is an improvement over WEP. It causes keys to automatically change, and when used in conjunction with a larger initialization vector (IV), it makes discovering keys highly unlikely.

Note An IV is a block of bits added to the first block of data of a block cipher. This block is added--or hashed--with the base key and is used with other types of ciphers. This block strengthens security because the same transmissions with the same key yield the same output. As a result, attackers can notice the similarities and derive both the messages and the keys being used.

In addition to improving authentication and encryption, WPA secures the payload better than in WEP. With WEP, cyclic redundancy checks (CRC) are used to ensure packet integrity. However, it is possible to alter the payload and update the message CRC without knowing the WEP key because the CRC is not encrypted. WPA uses Message Integrity Check (MIC) to ensure packet integrity. The MICs also employ a frame counter, which prevents replay attacks.

Note A replay attack occurs when an intruder intercepts an encrypted transmission, and then rebroadcasts that transmission at a later time. For example, if a password is intercepted, the attacker need not know how to read the message; the attacker can simply rebroadcast it later, and then gain access using the victim's credentials.

Breaking into a WLAN that uses WPA is more difficult than breaking into one that uses WEP because the IVs are larger, there are more keys in use, and there is a sturdier message verification system.

WPA 2 is the next generation of Wi-Fi security. WPA 2 is the Wi-Fi Alliance interoperable implementation of the ratified IEEE 802.11i standard. WPA 2 implements the Advanced Encryption Standard (AES) encryption algorithm with the use of Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). AES Counter Mode is a block cipher that encrypts 128-bit blocks of data at a time with a 128-bit encryption key. The CCMP algorithm produces a message integrity code (MIC) that provides data origin authentication and data integrity for the wireless frame.

Note CCMP is also referred to as CBC-MAC.

WPA 2 offers a higher level of security than WPA because AES offers stronger encryption than Temporal Key Integrity Protocol (TKIP). TKIP is the encryption algorithm that WPA uses. WPA 2 creates fresh session keys on every association. The encryption keys that are used for each client on the network are unique and specific to that client. Ultimately, every packet that is sent over the air is encrypted with a unique key. Security is enhanced with the use of a new and unique encryption key because there is no key reuse.

For more information on WPA 2, refer to Configuration of WPA/WPA2 with Pre-Shared Key.

Broadcast Key Rotation in a Wireless LAN

Extensible Authentication Protocol (EAP) authentication provides dynamic unicast WEP keys for client devices but uses static broadcast keys. When you enable broadcast key rotation, the access point provides a dynamic broadcast WEP key and changes it at the interval you select. Because broadcast key rotation is used to protect multicast traffic and TKIP is used to protect unicast traffic, they can be enabled at the same time on a wireless LAN. You should enable broadcast key rotation if you are running multicast applications on your wireless LAN.

Client devices using static WEP cannot use the access point when you enable broadcast key rotation. Only wireless client devices using 802.1x authentication, such as Lightweight Extensible Authentication Protocol (LEAP), EAP with Transport Layer Security (EAP-TLS), or Protected Extensible Authentication Protocol (PEAP), can use the access point when you enable broadcast key rotation.

Types of Access Point Authentication

This section describes the authentication types that you can configure to the access point. The authentication types correspond to the SSIDs that you configure for the access point. If you want to serve different types of client devices with the same access point, you can configure multiple SSIDs. See the Separating a Wireless Network by Configuring Multiple SSIDs, on page 52 section for instructions on how to configure multiple SSIDs.

Before a wireless client device can communicate on your network through the access point, it must authenticate to the access point using open or shared-key authentication. For maximum security, client devices should also authenticate to your network using MAC-address or EAP authentication, authentication types that rely on an authentication server on your network.

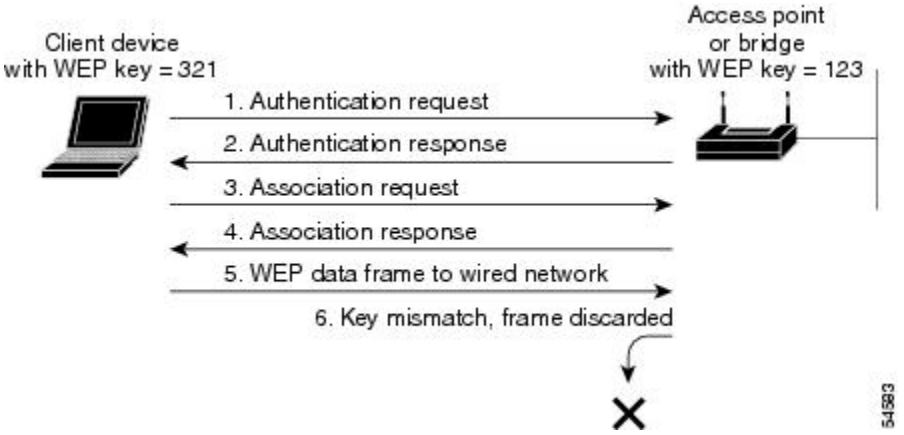
The access point uses four authentication mechanisms or types and can use more than one at the same time. The following sections explain each authentication type:

Open Authentication to the Access Point

Open authentication allows any device to authenticate and then attempt to communicate with the access point. If encryption is enabled, any wireless device using open authentication can authenticate to the access point, but the device can communicate only if its WEP keys match the access point's. Open authentication with no encryption is normally used for guest access. Any wireless client can communicate with the AP if open authentication and no encryption are configured. Devices not using WEP do not attempt to authenticate with an access point that is using WEP. Open authentication does not rely on a RADIUS server on your network.

The figure below shows the authentication sequence between a device trying to authenticate and an access point using open authentication. In this example, the device's WEP key does not match the access point's key, so it can authenticate but not pass data.

Figure 4: Sequence for Open Authentication



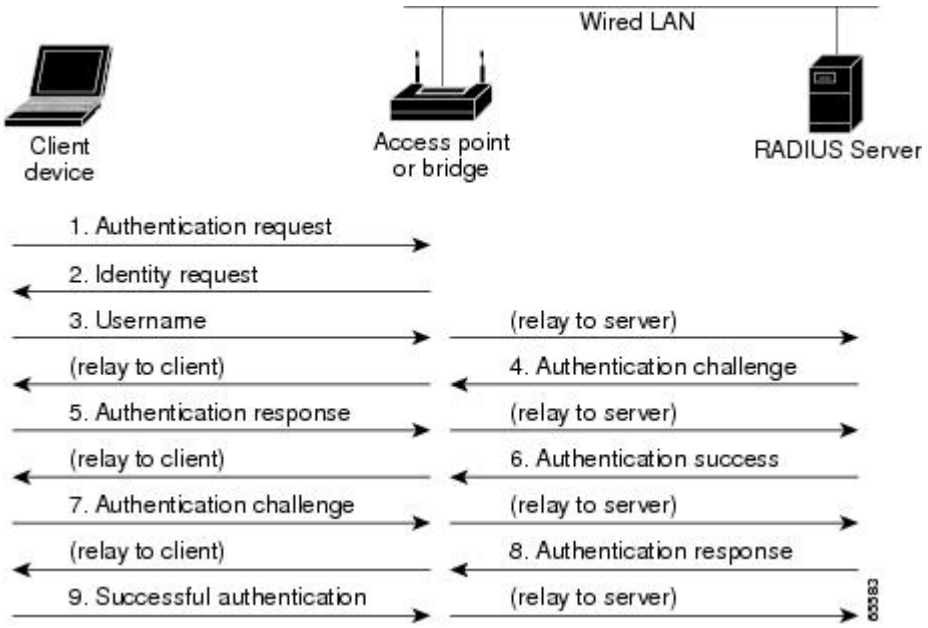
EAP Authentication to the Access Point

EAP provides the highest level of security for a wireless network. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless client device and the RADIUS server to perform mutual authentication and derive a dynamic unicast WEP key. The RADIUS server sends the WEP key to the access point, which uses it for all unicast data signals that it sends to or receives from the client. The access point also encrypts its broadcast WEP key (entered in the access point's WEP key slot 1) with the client's unicast key and sends it to the client.

EAP authentication provides dynamic WEP keys to wireless users. Dynamic WEP keys are more secure than static, or unchanging, WEP keys. If an intruder passively receives enough packets encrypted by the same WEP key, the intruder can perform a calculation to learn the key and use it to join a network. Because they change frequently, dynamic WEP keys prevent intruders from performing the calculation and learning the key.

When you enable EAP on your access points and client devices, authentication to the network occurs in the sequence shown in the figure below.

Figure 5: Sequence for EAP Authentication



In Steps 1 through 9 in the above figure, a wireless client device and a RADIUS server on the wired LAN use 802.1x and EAP to perform a mutual authentication through the access point. The RADIUS server sends an authentication challenge to the client. The client uses a one-way encryption of the user-supplied password to generate a response to the challenge and sends that response to the RADIUS server. Using information from its user database, the RADIUS server creates its own response and compares that to the response from the client. When the RADIUS server authenticates the client, the process repeats in reverse, and the client authenticates the RADIUS server.

When mutual authentication is complete, the RADIUS server and the client determine a WEP key that is unique to the client and provides the client with the appropriate level of network access, thereby approximating the level of security in a wired switched segment to an individual desktop. The client loads this key and prepares to use it for the login session.

During the login session, the RADIUS server encrypts and sends the WEP key, called a session key, over the wired LAN to the access point. The access point encrypts its broadcast key with the session key and sends the encrypted broadcast key to the client, which uses the session key to decrypt it. The client and access point activate WEP and use the session and broadcast WEP keys for all communications during the remainder of the session.

There is more than one type of EAP authentication, but the access point behaves the same way for each type: It relays authentication messages from the wireless client device to the RADIUS server and from the RADIUS server to the wireless client device.

To set up EAP authentication on the access point, see the Separating a Wireless Network by Configuring Multiple SSIDs, on page 52 task.

Note If you use EAP authentication, you can select open or shared key authentication, but you need not. EAP authentication controls authentication both to your access point and to your network.

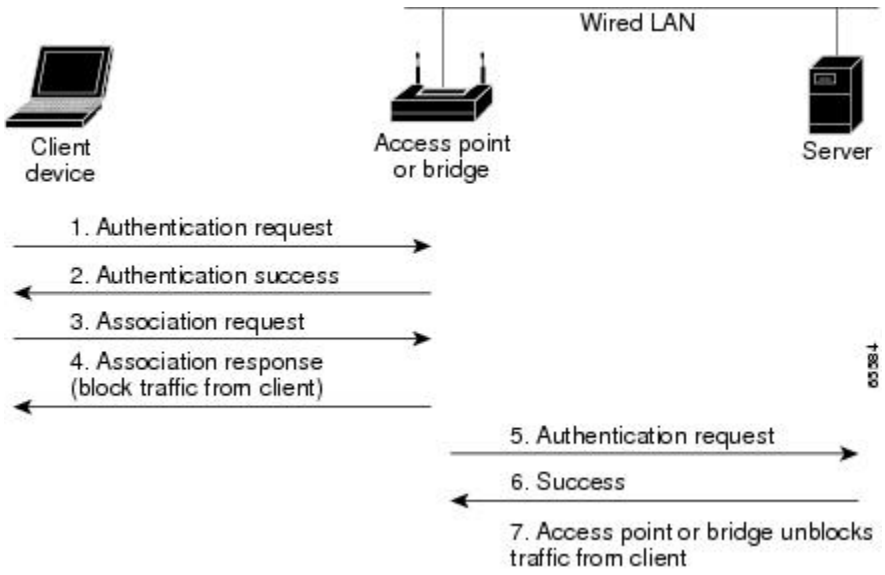
MAC Address Authentication to the Access Point

The access point relays the wireless client device's MAC address to a RADIUS server on your network, and the server compares the address to a list of allowed MAC addresses. Intruders can create counterfeit MAC addresses, so MAC-based authentication is less secure than EAP authentication. However, MAC-based authentication provides an alternate authentication method for client devices that do not have EAP capability. See the Separating a Wireless Network by Configuring Multiple SSIDs, on page 52 section for instructions on enabling MAC-based authentication.

If you do not have a RADIUS server on your network, you can create a list of allowed MAC addresses on the access point. Devices with MAC addresses not on the list are not allowed to authenticate. When you create the list of allowed MAC addresses, use lowercase for all letters in the addresses that you enter.

The figure below shows the authentication sequence for MAC-based authentication.

Figure 6: Sequence for MAC-Based Authentication



MAC-Based EAP and Open Authentication

You can set up the access point to authenticate client devices using a combination of MAC-based and EAP authentication. When you enable this feature, client devices that associate to the access point using 802.11 open authentication first attempt MAC authentication; if MAC authentication succeeds, the client device joins the network. If MAC authentication fails, the access point waits for the client device to attempt EAP authentication. See the "Assigning Authentication Types to SSIDs" section for instructions on setting up this combination of authentications.

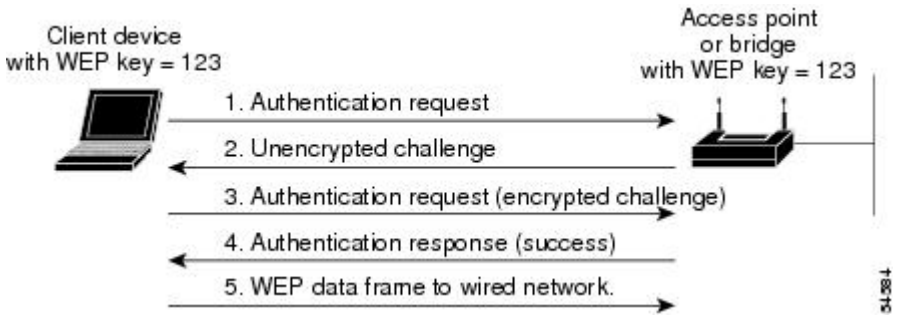
Shared Key Authentication to the Access Point

Note Cisco provides shared key authentication to comply with the IEEE 802.11b standard. However, because of shared key's security flaws, we recommend that you avoid using it.

During shared key authentication, the access point sends an unencrypted challenge text string to any device attempting to communicate with the access point. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. Both the unencrypted challenge and the encrypted challenge can be monitored, however, which leaves the access point open to attack from an intruder that calculates the WEP key by comparing the unencrypted and encrypted text strings. Because of this weakness, shared key authentication can be less secure than open authentication. Like open authentication, shared key authentication does not rely on a RADIUS server on your network.

The figure below shows the authentication sequence between a device trying to authenticate and an access point using shared key authentication. In this example the device's WEP key matches the access point's key, so it can authenticate and communicate.

Figure 7: Sequence for Shared Key Authentication



Correspondence Between Access Point and Client Authentication Types

The authentication settings on the access point must match the authentication settings on the clients that associate to the access point. Refer to the installation guide for your wireless LAN client adapter for instructions on setting authentication types.

Note Some non-Cisco client adapters do not perform 802.1x authentication to the access point unless you configure open authentication with EAP. To allow both Cisco clients using LEAP and non-Cisco clients using LEAP to associate using the same SSID, it might be necessary to configure the SSID for both network EAP authentication and open authentication with EAP.

The table below lists the client and access point settings required for each authentication type.

Table 2: Client and Access Point Settings for Authentication

Authentication Type	Client Setting	Access Point Setting
Static WEP with open authentication	Create a WEP key and enable Use Static WEP Keys and Open Authentication.	Configure WEP and enable open authentication for the Service Set Identifier (SSID).
Static WEP with shared key authentication	Create a WEP key and enable Use Static WEP Keys and Shared Key Authentication.	Configure WEP and enable shared key authentication for the SSID.
LEAP authentication	Enable LEAP on Cisco clients. Use the vendor authentication application for non-Cisco clients.	Configure WEP and enable network EAP for the SSID[1].
802.1x authentication	Enable EAP-TLS, PEAP MS-CHAP v2, or EAP-FAST.	Enable mandatory WEP. Enable open authentication with EAP for the SSID.
802.1x authentication and WPA	Enable any 802.1x authentication method and WPA.	Choose TKIP as the cipher suite and enable open authentication with EAP and/or network EAP for the SSID. You can enable network EAP authentication in addition to or instead of open authentication. To allow both WPA clients and non-WPA clients to use the SSID, enable optional WPA. If WPA is set as mandatory, TKIP is the only valid cipher suite. If WPA is set as optional, the only available ciphers are TKIP+WEP40 or TKIP+WEP128.
WPA-PSK authentication	Enable WPA-PSK and configure a preshared key.	Choose a cipher suite and enable open authentication and WPA for the SSID. Enter a WPA preshared key. To allow both WPA clients and non-WPA clients to use the SSID, enable optional WPA.
EAP-TLS Authentication		

Authentication Type	Client Setting	Access Point Setting
If using ACU to configure card	Enable Host Based EAP and Use Dynamic WEP Keys in ACU and choose Enable network access control using IEEE 802.1X and Smart Card or Other Certificate as the EAP Type in Windows 2000 (with Service Pack 3) or Windows XP.	Configure WEP and enable open authentication with EAP for the SSID.
If using Windows XP to configure card	Select Enable network access control using IEEE 802.1X and Smart Card or other Certificate as the EAP type.	Configure WEP and enable open authentication with EAP for the SSID.
PEAP Authentication		
If using Aironet Client Utility (ACU) to configure card	Enable Host Based EAP and Use Dynamic WEP Keys in ACU and choose Enable network access control using IEEE 802.1X and PEAP as the EAP type in Windows 2000 (with Service Pack 3) or Windows XP.	Configure WEP and enable open authentication with EAP for the SSID.
If using Windows XP to configure card	Choose Enable network access control using IEEE 802.1X and PEAP as the EAP type.	Configure WEP and enable open authentication with EAP for the SSID.

[1] Some non-Cisco Aironet client adapters do not perform 802.1x authentication to the access point unless you configure open authentication with EAP. To allow both Cisco Aironet clients using LEAP and non-Cisco Aironet clients using LEAP to associate using the same SSID, you might need to configure the SSID for both network EAP authentication and open authentication with EAP.

MAC Address and IP Filters on Access Point Interfaces

In addition to managing access to a WLAN through WEP keys or authentication, you can configure access to be restricted according to device; to do this, you use the MAC address or IP address. For example, you can employ filtering on your APs to keep out clients that do not have an authorized client adapter. Without an explicitly approved MAC address on the network adapter, it does not matter if the correct username and password are presented because the AP does not allow access.

Simply put, filtering checks a wireless client's MAC or IP address against a list of authorized MAC or IP addresses maintained on the access point. When a client tries to connect to the access point, it must be on the list. If it is not, the client cannot connect.

Filtering should not be the only security measure, however. Both MAC and IP addresses can be spoofed, thus circumventing this layer of security.

To configure filters, you use access control lists (ACLs) and bridge groups.

Note You can include filters in the access point's quality of service policies. Refer to the "Implementing Quality of Service in a Wireless LAN" module for detailed instructions on configuring QoS policies on an access point.

MAC Address Filters

MAC address filters allow or disallow the forwarding of unicast and multicast packets either sent from or addressed to specific MAC addresses. You can create a filter that passes or blocks traffic to all MAC addresses except those you specify. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.

MAC address filters are powerful, and you can lock yourself out of the access point if you make a mistake setting up the filters. If you accidentally lock yourself out of your access point, you may need to attach to the AP using a console, disable the filters, then correct each filter accordingly.

Note Client devices with blocked MAC addresses cannot send or receive data through the access point, but they might remain in the Association Table as unauthenticated client devices. Client devices with blocked MAC addresses disappear from the Association Table when the access point stops monitoring them, when the access point reboots, or when the clients associate with another access point.

IP Filters

You can limit access to your AP with IP filters. IP filters can be applied based on IP address, IP protocol, and IP port. IP filters prevent or allow the use of specific protocols through the access point's Ethernet and radio ports, and IP address filters allow or prevent the forwarding of unicast and multicast packets either sent from or addressed to specific IP addresses. You can create a filter that passes traffic to all addresses except those you specify, or you can create a filter that blocks traffic to all addresses except those you specify. You can create filters that contain elements of one, two, or all three IP filtering methods. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.

Note If you create an IP filter and intend to block traffic to all IP addresses except those specified, make sure you include the IP address of your own computer in the list of specified exceptions; otherwise, your computer is shut out from the access point.

How to Secure a Wireless LAN

Configuring WEP Encryption and Key Management Features

Perform this task to configure WEP encryption and additional key management features, such as MIC, TKIP, and broadcast key rotation.

Configure static WEP keys only if the access point must support client devices that use static WEP. If all the client devices that associate to the access point use key management (WPA or 802.1x authentication) you do not need to configure static WEP keys.

WEP, TKIP, MIC, and broadcast key rotation are disabled by default.

Before You Begin

Determine if all the clients that will associate to the access point are capable of key management. If they are, use the **encryption mode ciphers** command rather than the **encryption mode wep** command to configure WEP. See the relevant command pages in the Cisco IOS Wireless LAN Command Reference for more details.

Note The table below lists WEP key restrictions based on your security configuration.

Table 3: WEP Key Restrictions

Security Configuration	WEP Key Restriction
WPA authenticated key management	Cannot configure a WEP key in key slot 1
LEAP or EAP authentication	Cannot configure a WEP transmit 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 transmit key in key slot 1 and 4
Broadcast key rotation	Keys in slots 2 and 3 are overwritten by rotating broadcast keys **Note** Client devices using static WEP cannot use the access point when you enable broadcast key rotation. When you enable broadcast key rotation, only wireless client devices using 802.1x authentication (such as LEAP, EAP-TLS, or PEAP) can use the access point.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dot11Radio** *interface*
4. **encryption** [**vlan** *vlan-id*] **mode wep**[**mandatory** | **optional**]
5. **encryption** [**vlan** *vlan-id*] **key** *number* **size** {**40bit** | **128bit**} [**0** | **7**] *encryption-key* [**transmit-key**]
6. **encryption** [**vlan** *vlan-id*] **mode ciphers {aes-ccm tkip}**[**wep128** | **wep40**]
7. **broadcast-key** [**vlan** *vlan-id*][**change** *seconds*] [**membership-termination**] [**capability-change**]
8. **end**
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables 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 0/3/0`	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	**encryption** [**vlan** *vlan-id*] **mode wep**[**mandatory**	**optional**] **Example:** `Router(config-if)# encryption vlan 1 mode wep`	Enables WEP encryption on the wireless LAN or a specific VLAN.
Step 5	**encryption** [**vlan** *vlan-id*] **key** *number* **size** {**40bit**	**128bit**} [**0**	**7**] *encryption-key* [**transmit-key**]	Defines the WEP key used for data encryption on the wireless LAN or on a specific VLAN. • When you have configured the encryption key for static WEP clients, skip to Step 8.

	Command or Action	Purpose
	Example: `Router(config-if)# encryption vlan 1 key 1 size 40bit 11aa33bb55 transmit-key`	
Step 6	**encryption** [**vlan** *vlan-id*] **mode ciphers** {**aes-ccm tkip**}[**wep128** | **wep40**] **Example:** `Router(config-if)# encryption vlan 10 mode ciphers tkip wep40`	Enables WEP encryption and a cipher suite that contains Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Code Protocol (AES-CCMP) or TKIP, which provides better security for your wireless LAN. • When you configure the TKIP cipher and AES-CCM (not TKIP + WEP 128 or TKIP + WEP 40) for an SSID, the SSID must use WPA key management. Client authentication fails on an SSID that uses the TKIP cipher without enabling WPA key management. See the Separating a Wireless Network by Configuring Multiple SSIDs, on page 52 section for more information on configuring WPA.
Step 7	**broadcast-key** [**vlan** *vlan-id*][**change** *seconds*] [**membership-termination**] [**capability-change**] **Example:** `Router(config-if)# broadcast key vlan 10 change 300`	(Optional) Enables broadcast key rotation--the time interval between rotations of the broadcast encryption key used for clients. • Client devices using static WEP cannot access the access point when you enable broadcast key rotation. Only wireless client devices using 802.1x authentication, such as LEAP, EAP-TLS, or PEAP, can use the access point when you enable broadcast key rotation.
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`	(Optional) Saves your entries in the configuration file.

What to Do Next

After you have configured encryption, configure authentication mechanisms as shown in the Controlling Access to a Wireless Network by Using Authentication Mechanisms, on page 49 section.

Controlling Access to a Wireless Network by Using Authentication Mechanisms

In a wireless network, you need to ascertain the identity of the users and devices using authentication mechanisms. This is important because access control is established depending on the user's identity.

Perform this task to configure authentication mechanisms.

Before You Begin

The following prerequisites apply to using authentication mechanisms:

- If you are going to use 802.1*x* authentication mechanisms (for example, network EAP), an EAP-compatible RADIUS server must be configured and accessible in the network to provide AAA services.
- If you are going to use MAC address or EAP authentication, you need to define the MAC and EAP address lists using the **aaa authentication login** command, which can be found in the *Cisco IOS Security Command Reference* , Release 12.4T.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot11 ssid** *name*
4. **authentication open [mac-address** *list-name* **] [eap** *list-name* **]**
5. **authentication shared [mac-address** *list-name* **] [eap** *list-name* **]**
6. **authentication network-eap** *list-name* **[mac-address** *list-name* **]**
7. **authentication key-management wpa** [**optional**]
8. **exit**
9. **interface dot11Radio** *interface*
10. **ssid** *name*
11. **end**
12. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dot11 ssid** *name* **Example:** `Router(config)# dot11 ssid anyname`	Creates a global SSID. • The *name* argument is a case-sensitive alphanumeric string up to 32 characters in length. • The SSID is inactive until you use the ssid command in interface configuration mode to assign the SSID to a specific radio interface.
Step 4	**authentication open [mac-address** *list-name* **] [eap** *list-name* **]** **Example:** `Router(config-ssid)# authentication open`	(Optional) Sets the authentication type to open for this SSID. • The **mac-address** keyword sets the SSIDs authentication type to open with MAC address authentication. This requires all clients to perform MAC address authentication before joining the network. • The **eap** keyword sets the SSIDs authentication type to open with EAP authentication. The AP requires all clients to perform EAP authentication before joining the network. • For the *list-name* argument, specify the authentication method list.
Step 5	**authentication shared [mac-address** *list-name* **] [eap** *list-name* **]** **Example:** `Router(config-ssid)# authentication shared mac-address mac-list1`	(Optional) Sets the authentication type for this SSID to shared key. • The **mac-address** keyword sets the SSID's authentication type to shared key with MAC address authentication. For the *list-name*argument, specify the authentication method list. • The **eap** keyword sets the SSID's authentication type to shared key with EAP authentication. • For the *list-name*argument,specify the authentication method list. **Note** Cisco provides shared key authentication to comply with the IEEE 802.11b standard. However, because of shared key's security flaws, we recommend that you avoid using it.
Step 6	**authentication network-eap** *list-name* **[mac-address** *list-name* **]** **Example:** `Router(config-ssid)# authentication network-eap list1`	(Optional) Sets the authentication type for this SSID to Network-EAP. • This command is used to authenticate an EAP client with an EAP-compatible RADIUS server. • The SSID's authentication type can be altered so that it also requires MAC address authentication. For the *list-name* argument, specify the authentication method list.
Step 7	**authentication key-management wpa** [**optional**]	(Optional) Sets the authentication type for the SSID to WPA.

	Command or Action	Purpose
	Example: `Router(config-ssid)# authentication key-management wpa`	• If you use the **optional** keyword, clients that do not use WPA are allowed to use the SSID. However, if **optional** is not used, clients must use WPA to connect. • To enable WPA for an SSID, you must also enable open authentication, network EAP, or both.
Step 8	**exit** **Example:** `Router(config-ssid)# exit`	Exits SSID configuration mode.
Step 9	**interface dot11Radio** *interface* **Example:** `Router(config)# interface dot11Radio 0/3/0`	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 10	**ssid** *name* **Example:** `Router(config-if)# ssid anyname`	Creates an SSID and enters SSID configuration mode. • The *name* argument is a case-sensitive alphanumeric string up to 32 characters.
Step 11	**end** **Example:** `Router(config-if-ssid)# end`	Returns to privileged EXEC mode.
Step 12	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to Do Next

After you configure authentication mechanisms, you can configure authentication timeouts and reauthentication periods on the access point by completing the optional task in the Configuring Authentication Timeouts and Reauthentication Periods, on page 54 section.

Separating a Wireless Network by Configuring Multiple SSIDs

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. You can configure up to 10 SSIDs on the Cisco 800 and 1800 series fixed-configuration routers and up to 16 SSIDs on the Cisco 1800 modular, 2800, and 3800 series routers and 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.

These are the settings you can assign to each SSID:

- VLAN--You can use VLANs to configure different security features for each user or group in the wireless network. For example, users in VLAN 1 may be forced to use MAC authentication while users in VLAN 2 do not have that requirement.
- Client authentication method--You can apply separate authentication methods to different user groups on the wireless network.
- Guest mode--If you want an 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. The access point's default SSID is set to guest mode. However, to keep your network secure, you should disable the guest mode SSID on most access points.
- Repeater mode, including authentication username and password--If your access point will be a repeater or will be a root access point that acts as a parent for a repeater, you can set up an SSID for use in repeater mode. You can assign an authentication username and password to the repeater-mode SSID to allow the repeater to authenticate to your network like a client device.

Note If your network uses VLANs, you must assign, or bind, each SSID to an individual VLAN. Client devices using the SSID are grouped in that VLAN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot11 ssid** *name*
4. **vlan** *vlan-id*
5. **exit**
6. **interface dot11Radio** *interface*
7. **ssid** *name*
8. Repeat Step 2 through Step 7 for each SSID you want to create.
9. **end**
10. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dot11 ssid** *name* **Example:** `Router(config)# dot11 ssid floor2`	Creates a global SSID. • The *name* argument is a case-sensitive alphanumeric string up to 32 characters in length. • The SSID is inactive until you use the ssid command in interface configuration mode to assign the SSID to a specific radio interface.
Step 4	**vlan** *vlan-id* **Example:** `Router(config-ssid)# vlan 1`	Assigns the SSID to a VLAN on your network. • Client devices that associate using the SSID are grouped into this VLAN. • The *vlan-id* argument range is from 1 to 4095.
Step 5	**exit** **Example:** `Router(config-ssid)# exit`	Exits SSID configuration mode and returns to global configuration mode.
Step 6	**interface dot11Radio** *interface* **Example:** `Router(config)# interface dot11Radio 0/3/0`	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 7	**ssid** *name* **Example:** `Router(config-if)# ssid floor2`	Creates an SSID and enters SSID configuration mode. • The *name* argument is a case-sensitive alphanumeric string up to 32 characters in length.

	Command or Action	Purpose
Step 8	Repeat Step 2 through Step 7 for each SSID you want to create.	--
Step 9	**end** **Example:** `Router(config-if-ssid)# end`	Returns to privileged EXEC mode.
Step 10	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to Do Next

After you have configured the SSIDs, configure authentication mechanisms by completing the task in the Controlling Access to a Wireless Network by Using Authentication Mechanisms, on page 49 section.

Configuring Authentication Timeouts and Reauthentication Periods

Perform this task to configure authentication timeouts and reauthentication periods for client devices authenticating through your access point.

This task is optional and can be used only if 802.1*x* authentication is configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dot11Radio** *interface*
4. **dot1x client-timeout** *seconds*
5. **dot1x reauth-period {** *seconds* **| server}**
6. **end**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• 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 0/3/0`	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	**dot1x client-timeout** *seconds* **Example:** `Router(config-if)# dot1x client-timeout 120`	Specifies the length of time, in seconds, the access point waits for a reply from a client attempting to authenticate before the authentication fails.
Step 5	**dot1x reauth-period {** *seconds* **| server}** **Example:** `Router(config-if)# dot1x reauth-period 120`	Specifies the length of time, in seconds, the access point waits before forcing an authenticated client to reauthenticate. • Use the server keyword to configure the access point to use the reauthentication period specified by the authentication server. If you use this option, configure your authentication server with RADIUS attribute 27, Session-Timeout. This attribute sets the maximum number of seconds of service to be provided to the client before termination of the session or prompt. The server sends this attribute to the access point when a client device performs EAP authentication.
Step 6	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuration Examples for Securing a Wireless LAN

Configuring an Access Point in Bridging Mode with Open Authentication and Static WEP Encryption Example

The following configuration example shows how to:

- Configure a Cisco 3800 series access point in bridging mode with open authentication and static WEP encryption.
- Define a bridge group and assign it to the radio interface and a VLAN interface.
- Create a bridge virtual interface (BVI) and assign an IP address to that interface.

- Save the new entries in the configuration file.

```
configure terminal
 bridge irb
 bridge 1 route ip
 dot11 ssid ssid1
 authentication open
 exit
 interface dot11Radio 0/0/0
 encryption mode wep mandatory
 encryption key 1 size 40bit 11aa33bb55
 ssid ssid1
 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
```

Configuring an Access Point in Bridging Mode with WPA-PSK Example

The following example shows how to:

- Configure a Cisco 1800, 2800, or 3800 series modular router (access point) in bridging mode with authenticated key management and encryption that uses a cipher suite that contains TKIP and a WPA preshared key.
- 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.
- Save the new configuration to NVRAM.

```
configure terminal
 bridge irb
 bridge 1 route ip
 dot11 ssid ssid1
 authentication open
 authentication key-management wpa
 wpa-psk ascii shared-key-name
 exit
 interface dot11Radio 0/3/0
 encryption mode ciphers tkip
 ssid ssid1
 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
```

Configuring an Access Point in Bridging Mode with MAC Authentication Example

The following example shows how to:

- Configure a Cisco 1800, 2800, or 3800 series modular router (access point) in bridging mode with open authentication and MAC authentication using a local MAC address list.
- 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.
- Save the new configuration to NVRAM.

```
configure terminal
 bridge irb
 bridge 1 route ip
 dot11 ssid ssid1
 authentication open mac-address maclist1
 exit
 interface dot11Radio 0/3/0
 ssid ssid1
 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
 configure terminal
 username 000011111111 password 000011111111
 aaa new-model
 aaa authentication login maclist1 local
 end
 copy running-config startup-config
```

This example shows how to:

- Configure a Cisco 1800, 2800, or 3800 series modular router (access point) in bridging mode with open authentication and MAC authentication using a MAC address list located on an external RADIUS server.
- 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.

- Save the new configuration to NVRAM.

```
configure terminal
 bridge irb
 bridge 1 route ip
 dot11 ssid ssid1
 authentication open mac-address maclist1
 exit
 interface dot11Radio 0/3/0
 ssid ssid1
 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
 configure terminal
 aaa new-model
 ip radius source-interface bvi 1
 radius-server host 11.2.0.1 auth-port 1812 acct-port 1813 key sharedsecret
 aaa group server radius rad_mac
 server 11.2.0.1 auth-port 1812 acct-port 1813
 exit
 aaa authentication login maclist1 group rad_mac
 end
 copy running-config startup-config
```

Configuring an Access Point in Bridging Mode with 802.1x Authentication Example

The following example shows how to:

- Configure a Cisco 1800, 2800, or 3800 series modular router (access point) in bridging mode with 802.1*x* (network EAP) authentication.
- Define a bridge group and assign it to the radio interface and VLAN interface.
- Create a BVI and assign an IP address to that interface.
- Save the new configuration to NVRAM.

```
configure terminal
 bridge irb
 bridge 1 route ip
 dot11 ssid ssid1
 authentication network-eap eaplist1
 authentication open eap eaplist1
 exit
 interface dot11Radio 0/3/0
 ssid ssid1
 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
```

Configuring an Access Point in Routing Mode with Open Authentication and Static WEP Encryption Example

The following example shows how to:

- Configure a Cisco 1800, 2800, or 3800 series modular router (access point) in routing mode with open authentication and static WEP encryption.
- Assign an IP address to the radio interface.
- Create an SSID for the access point.
- Save the new configuration to NVRAM.

```
configure terminal
 dot11 ssid ssid2
 authentication open
 exit
 interface dot11Radio 0/3/0
 ip address 10.0.1.1 255.255.255.0
 encryption mode wep mandatory
 encryption key 1 size 40bit 11aa33bb55
 ssid ssid2
 no shutdown
 end
 copy running-config startup-config
```

Configuring an Access Point in Routing Mode with WPA-PSK Example

The following example shows how to:

- Configure a Cisco 1800, 2800, or 3800 series modular router (access point) in routing mode with authenticated key management and encryption that uses a cipher suite that contains TKIP and a WPA preshared key.
- Assign an IP address to the radio interface.

- Save the new configuration to NVRAM.

```
configure terminal
 dot11 ssid ssid2
 authentication key-management wpa
 wpa-psk ascii shared-key-name
 authentication open
 exit
 interface dot11Radio 0/3/0
 ip address 10.0.1.1 255.255.255.0
 encryption mode ciphers tkip
 ssid ssid2
 no shutdown
 end
 copy running-config startup-config
```

Configuring an Access Point in Routing Mode with MAC Authentication Example

The following example shows how to:

- Configure a Cisco 1800, 2800, or 3800 series modular router (access point) in routing mode with MAC authentication using a local list.
- Assign an IP address to the radio interface.

- Save the new configuration to NVRAM.

```
configure terminal
 dot11 ssid ssid2
 authentication open mac-address maclist1
 exit
 interface dot11Radio 0/3/0
 ip address 10.0.1.1 255.255.255.0
 ssid ssid2
 no shutdown
 end
 configure terminal
 username 000011111111 password 000011111111
 aaa new-model
 aaa authentication login maclist1 local
 end
 copy running-config startup-config
```

This example shows how to:

- Configure a Cisco 1800, 2800, or 3800 series modular router (access point) in routing mode with MAC authentication using a MAC address list located on an external RADIUS server.
- Assign an IP address to the radio interface.

- Save the new configuration to NVRAM.

```
configure terminal
 dot11 ssid2
 authentication open mac-address maclist1
 exit
 interface dot11Radio 0/3/0
 ip address 10.0.1.1 255.255.255.0
 ssid ssid2
 no shutdown
 end
 configure terminal
 aaa new-model
 ip radius source-interface bvi 1
 radius-server host 11.2.0.1 auth-port 1812 acct-port 1813 key sharedsecret
 aaa group server radius rad_mac
 server 11.2.0.1 auth-port 1812 acct-port 1813
 exit
 aaa authentication login maclist1 group rad_mac
 end
 copy running-config startup-config
```

Configuring an Access Point in Routing Mode with 802.1x Authentication Example

The following example shows how to:

- Configure a Cisco 1800, 2800, or 3800 series modular router (access point) in routing mode with 802.1*x* (network EAP) authentication.
- Assign an IP address to the radio interface.

- Save the new configuration to NVRAM.

```
configure terminal
 dot11 ssid ssid2
 authentication open eap eaplist1
 authentication network-eap eaplist1
 exit
 interface dot11Radio 0/3/0
 ip address 10.0.1.1 255.255.255.0
 ssid ssid2
 no shutdown
 end
 copy running-config startup-config
```

Where to Go Next

- If you are using a RADIUS server in your wireless LAN for AAA services, or you need to configure an access point to serve as a local authenticator, see the "Configuring RADIUS or a Local Authenticator in a Wireless LAN" module.
- If you want to configure quality of service (QoS) settings on an access point, see the "Implementing Quality of Service in a Wireless LAN" module.
- If you want to configure wireless VLANs, see the "Configuring Wireless VLANs" module.

Additional References

The following sections provide references related to securing a wireless LAN.

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
Cisco IOS security commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS Security Command Reference

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

Feature Information for Securing a Wireless LAN

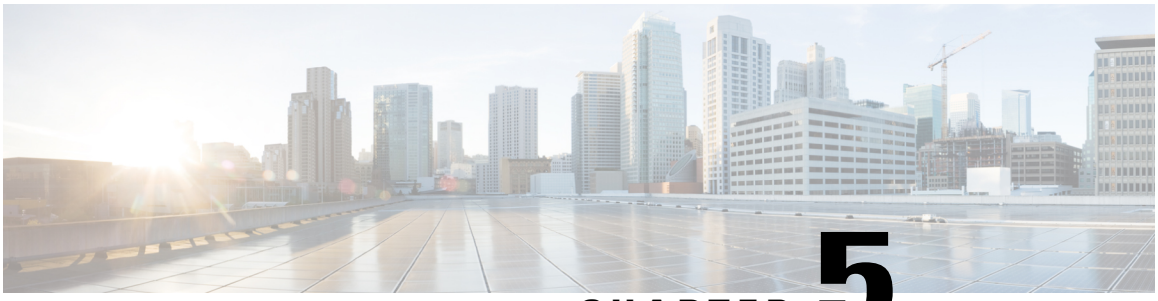
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4: Feature Information for Securing a Wireless LAN

Feature Name	Releases	Feature Information
Advanced Encryption Standard (AES) - CCMP	12.4(15)T	AES-CCMP is a symmetric block cipher that can encrypt and decrypt data using keys of 128, 192, and 256 bits. AES-CCMP is a superior to WEP encryption and is defined in the IEEE 802.11i standard.
Broadcast Key Rotation	12.4T	This feature allows a user to set a timeout for the shared broadcast key.
IEEE 802.11 Wireless Standards Support	12.4T	This feature provides support for 802.11 standards, which allows you to set authentication types and security based on WEP, among other configurable fields.
IEEE 802.11a Support	12.4T	This feature provides support for 802.11a standards, which allows you to set authentication types and security based on WEP, among other configurable fields.
IEEE 802.11b Support	12.4T	This feature provides support for 802.11b standards, which allows you to set authentication types and security based on WEP, among other configurable fields.
IEEE 802.11g Support	12.4T	This feature provides support for 802.11g standards, which allows you to set authentication types and security based on WEP, among other configurable fields.
MAC Address Local Authentication	12.4T	This feature provides support for MAC authentication of users on an access point.

Feature Name	Releases	Feature Information
Multiple SSIDs	12.4T	This feature allows a user to configure up to 10 SSIDs on the Cisco 800 and 1800 series fixed-configuration routers and up to 16 SSIDs on the Cisco 1800 modular, 2800, and 3800 series routers and assign different configuration settings to each SSID.
Wi-Fi Protected Access (WPA)	12.4T	This feature provides support for wireless fidelity protected access, which is a standards-based, interoperable security enhancement that greatly increases the level of data protection and access control for existing and future wireless LAN systems.



CHAPTER 5

Configuring RADIUS or a Local Authenticator in a Wireless LAN

This module describes how to enable and configure RADIUS in a wireless LAN (WLAN), which is a protocol that provides detailed accounting information and flexible administrative control over the authentication and authorization processes. RADIUS is facilitated through authentication, authorization, and accounting (AAA) and can be enabled only through AAA commands.

This module also describes how to configure a Cisco 800, 1800, 2800, or 3800 series integrated services router, hereafter referred to as an access point or AP, as a local authenticator. The AP can serve as a standalone authenticator for a small wireless LAN or provide backup authentication service. As a local authenticator, an AP performs Lightweight Extensible Authentication Protocol (LEAP) and MAC-based authentication for up to 50 client devices.

You can configure your APs to use the local authenticator when they cannot reach the main servers, or you can configure your APs to use the local authenticator or as the main authenticator if you do not have a RADIUS server. When you configure the local authenticator as a backup to your main servers, the APs periodically check the link to the main servers and stop using the local authenticator automatically when the link to the main servers is restored.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the Feature Information for Configuring RADIUS or a Local Authenticator in a Wireless LAN, on page 95.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring RADIUS or a Local Authenticator in a Wireless LAN

The following prerequisites apply to configuring RADIUS or a local authenticator in a wireless LAN:

- Read the "Wireless LAN Overview" module.
- Read the "Configuring a Basic Wireless LAN Connection" module.

Information About Configuring RADIUS or a Local Authenticator in a Wireless LAN

Network Environments Recommended to Use RADIUS for Access Security in a Wireless LAN

RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on supported Cisco devices and send authentication requests to a central RADIUS server, which contains all user authentication and network service access information. The RADIUS host is normally a multiuser system running RADIUS server software from Cisco (Cisco Secure Access Control Server version 3.0), Livingston, Merit, Microsoft, or another software provider. For more information, refer to the RADIUS server documentation.

Use RADIUS in these network environments, which require access security:

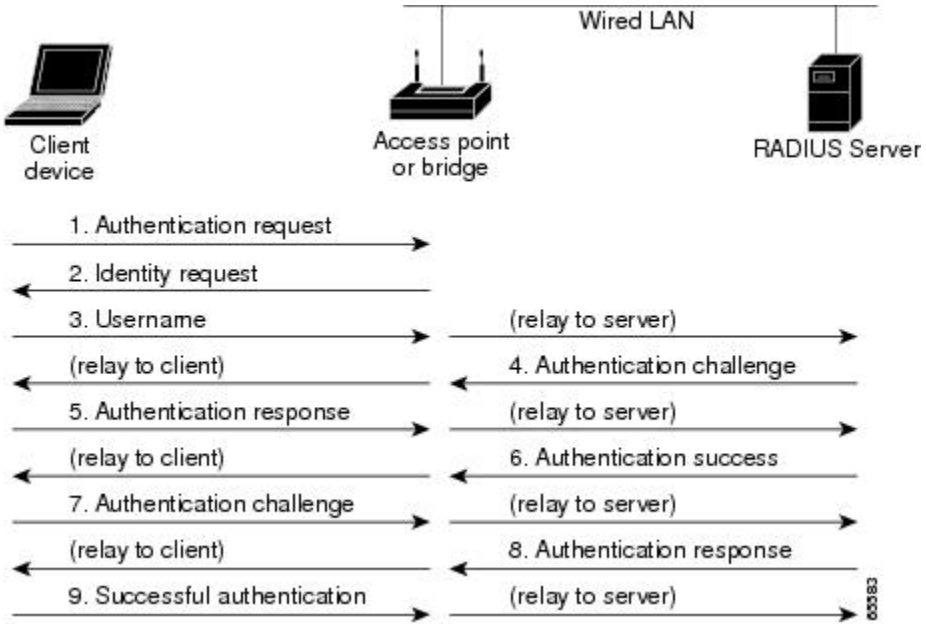
- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server that is customized to work with the Kerberos security system.

- Turnkey network security environments in which applications support the RADIUS protocol, such as an access environment that uses a *smart card* access control system. In one case, RADIUS has been used with Enigma's security cards to validate users and to grant access to network resources.
- Networks already using RADIUS. You can add a Cisco AP containing a RADIUS client to the network.
- Networks that require resource accounting. You can use RADIUS accounting independently of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, showing the amount of resources (such as time, packets, bytes, and so forth) used during the session. An Internet service provider might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.

RADIUS Operation in a Wireless LAN

When a wireless user attempts to log in and authenticate to an AP whose access is controlled by a RADIUS server, authentication to the network occurs in the steps shown in the figure below.

Figure 8: Sequence for EAP Authentication



In Steps 1 through 9 in the above figure, a wireless client device and a RADIUS server on the wired LAN use 802.1x and Extensible Authentication Protocol (EAP) to perform a mutual authentication through the AP. The RADIUS server sends an authentication challenge to the client. The client uses a one-way encryption of the user-supplied password to generate a response to the challenge and sends that response to the RADIUS server. Using information from its user database, the RADIUS server creates its own response and compares that to the response from the client. When the RADIUS server authenticates the client, the process repeats in reverse, and the client authenticates the RADIUS server.

When mutual authentication is complete, the RADIUS server and the client determine a Wired Equivalent Privacy (WEP) key that is unique to the client and provides the client with the appropriate level of network access, thereby approximating the level of security in a wired switched segment to an individual desktop. The client loads this key and prepares to use it for the login session.

During the login session, the RADIUS server encrypts and sends the WEP key, called a session key, over the wired LAN to the AP. The AP encrypts its broadcast key with the session key and sends the encrypted broadcast key to the client, which uses the session key to decrypt it. The client and AP activate WEP and use the session and broadcast WEP keys for all communications during the remainder of the session.

There is more than one type of EAP authentication, but the AP behaves the same way for each type: It relays authentication messages from the wireless client device to the RADIUS server and from the RADIUS server to the wireless client device. See the " Separating a Wireless Network by Configuring Multiple SSIDs " section in the " Securing a Wireless LAN " module for instructions on setting up client authentication using a RADIUS server.

Local Authentication in a Wireless LAN

To provide local authentication service or backup authentication service in case of a WAN link or a server failure, you can configure an AP to act as a local authentication server. The AP can authenticate clients using LEAP or MAC-based authentication.

The Cisco 800, 1800, 1841, and 2801 series APs can locally authenticate up to 50 clients, the Cisco 2811 and 2821 APs can authenticate up to 100 clients, the Cisco 2851 AP can authenticate up to 200 clients, the Cisco 3825 AP can authenticate up to 500 clients, and the Cisco 3845 AP can locally authenticate up to 1000 clients. The AP performs up to 5 authentications per second.

Small wireless LANs that do not have access to a RADIUS server could be made more secure with 802.1*x* authentication. Also, on wireless LANs that use 802.1x authentication, the APs rely on RADIUS servers housed at a distant location to authenticate client devices and the authentication traffic must cross a WAN link. If the WAN link fails or the APs cannot access the RADIUS servers for any other reason, client devices cannot access the wireless network even if the work they want to do is entirely local and typically authorized.

Configuration of authentication on a local authenticator must be done manually with client usernames and passwords. The local authenticatior does not synchronize its database with the RADIUS servers. Also, a VLAN and a list of SSIDs that a client is allowed to use can be configured.

Note If your wireless LAN contains only one AP, you can configure the AP as both the 802.1x authenticator and the local authenticator. However, users associated to the local authenticator might notice a decrease in performance during the authentication process.

You can configure your APs to use the local authenticator when they cannot reach the main servers, or you can configure your APs to use the local authenticator or as the main authenticator if you do not have a RADIUS server. When you configure the local authenticator as a backup to your main servers, the APs periodically check the link to the main servers and stop using the local authenticator automatically when the link to the main servers is restored.

Note The AP you use as an authenticator contains detailed authentication information for your wireless LAN. Physically secure it to protect its configuration.

Configuration Overview for a Local Authenticator in a Wireless LAN

These are the typical steps you will follow to set up a local authenticator. The task is fully described in the Configuring Local or Backup Authentication Service, on page 89 section.

1. On the local authenticator, create a list of APs authorized to use the authenticator to authenticate client devices. Each AP that uses the local authenticator is a network access server (NAS). If the local authenticator AP serves client devices directly, include the local authenticator AP as a NAS.
2. Create user groups and configure parameters to be applied to each group (optional).
3. Create a list of up to 1000 LEAP users or MAC addresses that the local authenticator is authorized to authenticate; the number of authorized users depends on the model of the AP. Verify the limit of your AP before creating the list.

You do not have to specify which type of authentication you want the local authenticator to perform. It automatically performs LEAP or MAC-address authentication for the users in its user database.

1. On the client APs that use a local authenticator AP for security, enter the local authenticator as a RADIUS server. If your local authenticator AP also serves client devices, you must enter the local authenticator as a RADIUS server in the local authenticator configuration. When a client associates to the local authenticator AP, the AP uses itself to authenticate the client.

How to Configure RADIUS or a Local Authenticator in a Wireless LAN

How to Configure RADIUS in a Wireless LAN

This section describes how to configure RADIUS in a wireless LAN.

At a minimum, you must identify the host or hosts that run the RADIUS server software and define the method lists for RADIUS authentication. You can optionally define method lists for RADIUS authorization and accounting.

A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on a user. You can use method lists to designate one or more security protocols to be used, thus ensuring a backup system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on users; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

This section contains the following tasks:

Identifying the RADIUS Server Host in a Wireless LAN

Perform this task to identify the RADIUS server host in a wireless LAN.

You also need to configure some settings on the RADIUS server. These settings include the IP address of the AP and the key string to be shared by both the server and the AP. For more information, refer to your RADIUS server documentation.

You identify RADIUS security servers by their hostname or IP address, hostname and specific User Datagram Protocol (UDP) port numbers, or their IP address and specific UDP port numbers. The combination of the IP address and the UDP port number creates a unique identifier allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address.

If two different host entries on the same RADIUS server are configured for the same service--such as accounting--the second host entry configured acts as a failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the AP tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order that they are configured.)

A RADIUS server and the AP use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the AP.

The timeout, retransmission, and encryption key values can be configured globally per server for all RADIUS servers or in some combination of global and per-server settings. To apply these settings globally to all RADIUS servers communicating with the AP, use the **radius-server timeout**, **radius-server retransmit**, and **radius-server key**commands**,**respectively. To apply these values on a specific RADIUS server, use the **radius-server host**command.

Note If you configure both global and per-server functions (timeout, retransmission, and key commands) on the AP, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands. For information on configuring these setting on all RADIUS servers, see Configuring Global Communication Settings Between an Access Point and a RADIUS Server, on page 84.

RADIUS and AAA are disabled by default.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables AAA.
Step 4	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] **Example:** `Router(config)#` **radius-server host 172.29.36.49 auth-port 1612 key rad1**	Specifies the IP address or hostname of the remote RADIUS server host. • (Optional) For **auth-port** *port-number*, specify the UDP destination port for authentication requests. • (Optional) For **acct-port** *port-number*, specify the UDP destination port for accounting requests. • (Optional) For **timeout***seconds* , specify the time interval that the AP waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the **radius-server timeout** global configuration command setting. If no timeout is set with the **radius-server host** command, the setting of the **radius-server timeout** command is used. • (Optional) For **retransmit***retries* , specify the number of times a RADIUS request is re-sent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the **radius-server host** command, the setting of the **radius-server retransmit** global configuration command is used. • (Optional) For **key***string* , specify the authentication and encryption key used between the AP and the RADIUS daemon running on the RADIUS server. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host**command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. • To configure the AP to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The AP software searches for

	Command or Action	Purpose
		hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.
Step 5	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to Do Next

After you identify the RADIUS host, configure RADIUS login authentication. See the Configuring RADIUS Login Authentication for a Wireless LAN, on page 78 section.

You can configure the AP to use AAA server groups to group existing server hosts for authentication by completing the optional task in the Defining and Associating a AAA Server Group to a RADIUS Server, on page 81 section.

Configuring RADIUS Login Authentication for a Wireless LAN

Perform this task to configure RADIUS login authentication for a wireless LAN.

To configure RADIUS authentication, you define a named list of authentication methods and then apply that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle--meaning that the security server or local username database responds by denying the user access--the authentication process stops, and no other authentication methods are attempted.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** {**default** | *list-name* } *method1* [*method2...*]
5. **line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]
6. **login authentication** {**default** | *list-name*}
7. **radius-server attribute 32 include-in-access-req format %h**
8. **end**
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables AAA.
Step 4	**aaa authentication login** {**default**	*list-name* } *method1* [*method2...*] **Example:** `Router(config)# aaa authentication login default local`	Creates a login authentication method list. • To create a default list that is used when a named list is *not* specified in the **login authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. • For the *method1 argument,* specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: • **line** --Use the line password for authentication. You must define a line password before you can use this authentication method. Use the **password** *password* line configuration command.

	Command or Action	Purpose
		• **local** --Use the local username database for authentication. You must enter username information in the database. Use the **username** *password* global configuration command. • **radius** --Use RADIUS authentication. You must identify the RADIUS server host before you can use this authentication method. For more information, see the Identifying the RADIUS Server Host in a Wireless LAN, on page 75 section.
Step 5	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*] **Example:** `Router(config)# line 10`	Configures the lines to which you want to apply the authentication list, and enters line configuration mode.
Step 6	**login authentication** {**default** | *list-name*} **Example:** `Router(config-line)# login authentication default`	Applies the authentication list to a line or set of lines. • If you specify the **default**keyword, use the default list created with the **aaa authentication login** command. • For the *list-name* argument, specify the list created with the **aaa authentication login** command.
Step 7	**radius-server attribute 32 include-in-access-req format %h** **Example:** `Router(config-line)# radius-server attribute 32 include-in-access-req format %h`	Configures the AP to send its system name in the NAS_ID attribute for authentication.
Step 8	**end** **Example:** `Router(config-line)# end`	Returns to privileged EXEC mode.
Step 9	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Defining and Associating a AAA Server Group to a RADIUS Server

Perform this task to define a AAA server group and associate a particular RADIUS server with that server group.

You can configure the AP to use AAA server groups to group existing server hosts for authentication. You select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list, which lists the IP addresses of the selected server hosts.

Server groups also can include multiple host entries for the same server if each entry has a unique identifier (the combination of the IP address and UDP port number), allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. If you configure two different host entries on the same RADIUS server for the same service (such as accounting), the second configured host entry acts as a failover backup to the first one.

You use the **server** group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional **auth-port** and **acct-port** keywords.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
5. **aaa group server radius** *group-name*
6. **server** *ip-address*
7. **end**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables AAA.
Step 4	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] **Example:** `Router(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001`	Specifies the IP address or hostname of the remote RADIUS server host. • (Optional) For **auth-port** *port-number*, specify the UDP destination port for authentication requests. • (Optional) For **acct-port** *port-number*, specify the UDP destination port for accounting requests. • (Optional) For **timeout***seconds* , specify the time interval that the AP waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the **radius-server timeout** global configuration command setting. If no timeout is set with the **radius-server host** command, the setting of the **radius-server timeout** command is used. • (Optional) For **retransmit***retries* , specify the number of times a RADIUS request is re-sent to a server if that server is not responding or responding slowly. The range is from 1 to 1000. If no retransmit value is set with the **radius-server host** command, the setting of the **radius-server retransmit** global configuration command is used. • (Optional) For **key***string* , specify the authentication and encryption key used between the AP and the RADIUS daemon running on the RADIUS server. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host**command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
Step 5	**aaa group server radius** *group-name* **Example:** `Router(config)# aaa group server radius group1`	Defines the AAA server group with a group name and places the AP in server group configuration mode.
Step 6	**server** *ip-address* **Example:** `Router(config-sg)# server 172.20.0.1`	Associates a particular RADIUS server with the defined server group. • Repeat this step for each RADIUS server in the AAA server group. • Each server in the group must be previously defined.

	Command or Action	Purpose
Step 7	**end** **Example:** `Router(config-sg)# end`	Returns to privileged EXEC mode.
Step 8	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Enabling RADIUS Accounting for a Wireless LAN

Perform this task to enable RADIUS accounting for each Cisco IOS privilege level and for network services.

The AAA accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the AP reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa accounting network start-stop radius**
4. ip radius source-interface bvi1
5. aaa accounting update periodic minutes
6. **end**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa accounting network start-stop radius** **Example:** `Router(config)# aaa accounting network start-stop radius`	Enables RADIUS accounting for all network-related service requests.
Step 4	ip radius source-interface bvi1 **Example:** `Router(config)# ip radius source-interface bvi1`	Configures the AP to send its bridge virtual interface (BVI) IP address in the NAS_IP_ADDRESS attribute for accounting records.
Step 5	aaa accounting update periodic minutes **Example:** `Router(config)# aaa accounting update periodic 5`	Specifies an accounting update interval in minutes.
Step 6	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 7	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Global Communication Settings Between an Access Point and a RADIUS Server

Perform this task to configure global communication settings between an AP and a RADIUS server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server key** {**0** *string* | **7** *string* | *string*}
4. **radius-server retransmit** *retries*
5. **radius-server deadtime** *minutes*
6. **end**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server key** {**0** *string*	**7** *string*	*string*} **Example:** `Router(config)# radius-server key anykey`	Specifies the shared secret text string used between the AP and all RADIUS servers. • The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
Step 4	**radius-server retransmit** *retries* **Example:** `Router(config)# radius-server retransmit 5`	Specifies the number of times the AP sends each RADIUS request to the server before giving up. • The range is from 1 to 1000; the default is 3.
Step 5	**radius-server deadtime** *minutes* **Example:** `Router(config)# radius-server deadtime 5`	Causes the Cisco IOS software to mark as "dead" any RADIUS servers that fail to respond to authentication requests, thus avoiding the wait for the request to time out before the software tries the next configured server. • A RADIUS server marked as dead is omitted in additional requests for the duration of minutes that you specify, up to a maximum of 1440 minutes (24 hours).

	Command or Action	Purpose
		Note If you set up more than one RADIUS server, you must configure the RADIUS server deadtime for optimal performance.
Step 6	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 7	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring the Access Point to Recognize and Use Vendor-Specific Attributes

Perform this task to configure the AP to recognize and use vendor-specific attributes (VSAs).

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the AP and the RADIUS server by using the vendor-specific attribute (attribute 26). A VSA allows a vendor to support its own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option by using the format recommended in the specification. Cisco's vendor ID is 9, and the supported option has vendor type 1, which is named *cisco-avpair* . The value is a string with this format:

```
protocol : attribute sep value *
```

Protocol is a value of the Cisco protocol attribute for a particular type of authorization. *Attribute* and *value* are an appropriate AV pair, and *sep* is = for mandatory attributes and the asterisk (*) for optional attributes. This allows the full set of features to be used for RADIUS.

For example, the following AV pair activates Cisco's *Multiple Named IP Address Pools* feature during IP authorization (during PPP's IPCP address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

The following example shows how to provide a user logging in from an AP with immediate access to privileged EXEC commands:

```
cisco-avpair= "shell:priv-lvl=15"
```

Other vendors have their own unique vendor IDs, options, and associated VSAs. For more information about vendor IDs and VSAs, refer to RFC 2138, Remote Authentication Dial-In User Service (RADIUS).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server vsa send** [**accounting** | **authentication**]
4. **end**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server vsa send** [**accounting** | **authentication**] **Example:** `Router(config)# radius-server vsa send`	Configures the AP to recognize and use VSAs as defined by RADIUS IETF attribute 26. • (Optional) Use the **accounting** keyword to limit the set of recognized vendor-specific attributes to only accounting attributes. • (Optional) Use the **authentication** keyword to limit the set of recognized vendor-specific attributes to only authentication attributes. • If you enter this command without keywords, both accounting and authentication vendor-specific attributes are used.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring a Vendor-Proprietary RADIUS Server Host

Perform this task to configure a vendor-proprietary RADIUS server host and a shared secret text string.

Although an IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the AP and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. Cisco IOS software supports a subset of vendor-proprietary RADIUS attributes.

To configure RADIUS (whether vendor-proprietary or IETF draft-compliant), you must specify the host running the RADIUS server daemon and the secret text string it shares with the AP. You specify the RADIUS host and secret text string by using the **radius-server** global configuration commands.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. radius-server host {hostname | ip-address} non-standard
4. **end**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	radius-server host {hostname | ip-address} non-standard **Example:** `Router(config)# radius-server host samplehost non-standard`	Specifies the IP address or hostname of the remote RADIUS server host and identifies that it is using a vendor-proprietary implementation of RADIUS.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 5	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

How to Configure a Local Authenticator in a Wireless LAN

This section describes how to configure an access point in a wireless LAN as a local authenticator.

This section contains the following task:

Configuring Local or Backup Authentication Service

Perform this task to configure local or backup authentication service.

You can configure your APs to use a local authenticator when they cannot reach the main servers, or you can configure your APs to use the local authenticator or as the main authenticator if you do not have a RADIUS server. When you configure the local authenticator as a backup to your main servers, the APs periodically check the link to the main servers and stop using the local authenticator automatically when the link to the main servers is restored.

When you configure an AP as a local authenticator, use an AP that does not serve a large number of client devices. When the AP acts as an authenticator, performance might degrade for associated client devices. Also, the AP you use as an authenticator contains detailed authentication information for your wireless LAN. Physically secure it to protect its configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. radius-server local
5. **nas** *ip-address* **key** *shared-key*
6. Repeat Step 5 to add each AP that uses the local authenticator.
7. **group** *group-name*
8. **vlan** *vlan*
9. **ssid** *name*
10. **reauthentication time** *seconds*
11. **block count** *count* **time** {*seconds* | **infinite**}
12. **exit**
13. **user** *username* {**password** | **nthash**} *password* [**group** *group-name*] [**mac-auth-only**]
14. **end**
15. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA access control system.
Step 4	radius-server local **Example:** `Router(config)# radius-server local`	Configures the AP or wireless-aware router as a local authentication server, and enters authenticator configuration mode.
Step 5	**nas** *ip-address* **key** *shared-key*	Adds an AP to the list of devices that use the local authentication server.

	Command or Action	Purpose
	Example: `Router(config-radsrv)# nas 10.91.6.159 key 110337`	• Enter the AP IP address and the shared key used to authenticate communication between the local authenticator and other APs. • You must enter this shared key on the APs that use the local authenticator. If your local authenticator also serves client devices, you must enter the local authenticator AP as a NAS. • Leading spaces in the shared key string are ignored, but spaces within and at the end of the key are used. If you use spaces in your shared key, do not enclose the key in quotation marks unless the quotation marks are part of the shared key.
Step 6	Repeat Step 5 to add each AP that uses the local authenticator.	--
Step 7	**group** *group-name* **Example:** `Router(config-radsrv)# group clerks`	(Optional) Configures a user group to which you can assign shared settings, and enters user group configuration mode.
Step 8	**vlan** *vlan* **Example:** `Router(config-radsrv-group)# vlan 87`	(Optional) Specifies a VLAN to be used by members of the user group. • The AP moves group members into a VLAN, overriding other VLAN assignments. • You can assign only one VLAN to the group.
Step 9	**ssid** *name* **Example:** `Router(config-radsrv-group)# ssid anyname`	(Optional) Creates an SSID for a radio interface. • Enter up to 20 SSIDs to limit members of the user group to those SSIDs. • The AP checks that the SSID that the client used to associate matches one of the SSIDs in the list. If the SSID does not match, the client is disassociated.
Step 10	**reauthentication time** *seconds* **Example:** `Router(config-radsrv-group)# reauthentication time 1800`	(Optional) Specifies the number of seconds after which the AP should reauthenticate members of the group. • The reauthentication provides users with a new encryption key. The default setting is 0, which means that group members are never required to reauthenticate.
Step 11	**block count** *count* **time** {*seconds* | **infinite**} **Example:** `Router(config-radsrv-group)# block count 3 time infinite`	(Optional) To help protect against password guessing attacks, locks out members of a user group for a length of time after a set number of incorrect passwords. • *count* --The number of failed passwords that triggers a lockout of the username.

	Command or Action	Purpose
		• *seconds* --The number of seconds the lockout should last. If you use the infinite keyword, an administrator must manually unblock the locked username. • See the **clear radius local-server** command for information on how to unblock a locked username.
Step 12	**exit** **Example:** `Router(config-radsrv-group)# exit`	Exits user group configuration mode and returns to authenticator configuration mode.
Step 13	**user** *username* {**password** | **nthash**} *password* [**group** *group-name*] [**mac-auth-only**] **Example:** `Router(config-radsrv)# user anyuser password pwd1234 group clerks`	Specifies the LEAP users allowed to authenticate using the local authenticator. • Enter a username and password for each user. If you do not know the user password, look up the NT value of the password in the authentication server database, and enter the NT hash as a hexadecimal string. • To add a client device for MAC-based authentication, enter the client MAC address as both the username and password. Enter 12 hexadecimal digits without a dot or dash between the numbers as the username and the password. For example, for the MAC address 0009.5125.d02b, enter *00095125d02b* as both the username and the password. • (Optional) To add the user to a user group, enter the group name. If you do not specify a group, the user is not assigned to a specific VLAN and is never forced to reauthenticate. • (Optional) To limit the user to MAC authentication only, enter mac-auth-only.
Step 14	**end** **Example:** `Router(config-radsrv)# end`	Returns to privileged EXEC mode.
Step 15	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuration Examples for a RADIUS Server or a Local Authenticator in a Wireless LAN

Configuring a Local Authenticator in a Wireless LAN Example

The following example shows how to:

- Configure a local authenticator in a wireless LAN used by three APs all sharing the same key.
- Configure three user groups: sales, marketing, and managers.
- Configure individual users, each of which will authenticate to the AP using either a personal password or a MAC address.

```
configure terminal
 radius-server local
 nas 10.91.6.159 key 110337
 nas 10.91.6.162 key 110337
 nas 10.91.6.181 key 110337
 group sales
 vlan 87
 ssid name1
 ssid name2
 reauthentication time 1800
 block count 2 time 600
 group marketing
 vlan 97
 ssid name3
 ssid name4
 ssid name5
 reauthentication time 1800
 block count 2 time 600
 group managers
 vlan 77
 ssid name6
 ssid name7
 reauthentication time 1800
 block count 2 time 600
 exit
! The following three users will authenticate using their own passwords.
 user username1 password pwd1 group sales
 user username2 password pwd2 group sales
 user username3 password pwd3 group sales
! These three users will authenticate using their MAC addresses.
 user 00095125d02b password 00095125d02b group marketing mac-auth-only
 user 00095125d02b password 00095125d02b group sales mac-auth-only
 user 00079431f04a password 00079431f04a group sales mac-auth-only
 user username4 password 272165 group managers
 user username5 password 383981 group managers
 end
 copy running-config startup-config
```

Additional References

The following sections provide references related to configuring a RADIUS server or a local authenticator.

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*

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

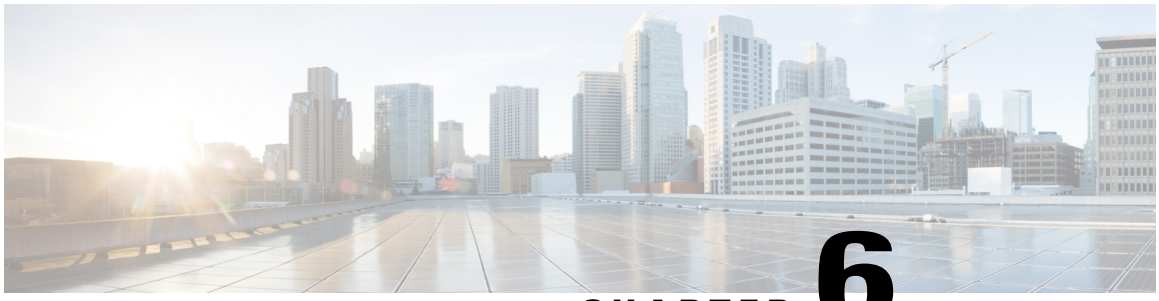
Feature Information for Configuring RADIUS or a Local Authenticator in a Wireless LAN

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5: Feature Information for Configuring RADIUS or a Local Authenticator in a Wireless LAN

Feature Name	Releases	Feature Information
RADIUS Server per SSID	12.4T	This feature allows RADIUS servers to be specified on a per-SSID basis.



CHAPTER 6

Configuring Radio Settings on an Access Point

This module describes how to configure radio settings on a Cisco 800, 1800, 2800, or 3800 series integrated services router, hereafter referred to as an access point (AP).

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the Feature Information for Configuring Radio Settings on an Access Point, on page 124.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Configuring Radio Settings on an Access Point

Wireless Device Roles in a Radio Network

The table below shows the role in the radio network for each of the following devices.

Note Universal client mode is not supported on the 85x ISRs.

Table 6: Device Role in Radio Network Configuration

Role in Radio Network	Cisco 800 Series ISRs	Cisco 1800 Series ISRs	Cisco 1841 Series ISRs	Cisco 2800 Series ISRs	Cisco 3800 Series ISRs
Root access point	X	X	X	X	X
Root bridge with or without clients	-	-	X	X	X
Nonroot bridge without clients	-	-	X	X	X
Universal client mode	X	X	X	X	X
Support of Workgroup bridge clients	X	X	X	X	X

Data Rate Settings

You use the data rate settings to choose the data rates the AP uses for data transmission. The rates are expressed in megabits per second. The AP always attempts to transmit at the highest data rate set to Basic, also called Require on the browser-based interface. If there are obstacles or interference, the AP steps down to the highest rate that allows data transmission. You can set each data rate (1, 2, 5.5, and 11 megabits per second) to one of three states:

- Basic (this is the default state for all data rates)--Allows transmission at this rate for all packets, both unicast and multicast. At least one of the access point's data rates must be set to Basic.

- Enabled--The AP transmits only unicast packets at this rate; multicast packets are sent at one of the data rates set to Basic.
- Disabled--The AP does not transmit data at this rate.

Note At least one data rate must be set to basic.

You can use the data rate settings to set up an AP to serve client devices operating at specific data rates. For example, to set up the 2.4-GHz radio for 11 megabits per second (Mbps) service only, set the 11-Mbps rate to Basic and set the other data rates to Enabled. To set up the AP to serve only client devices operating at 1 and 2 Mbps, set 1 and 2 to Basic and set the rest of the data rates to Enabled. To set up the 5-GHz radio for 54 Mbps service only, set the 54-Mbps rate to Basic and set the other data rates to Enabled.

You can also configure the AP to set the data rates automatically to optimize either range or throughput. When you enter range for the data rate setting, the AP sets the 1 Mbps rate to basic and the other rates to enabled. When you enter throughput for the data rate setting, the AP sets all four data rates to basic.

Universal Client Mode

Universal client mode is a wireless radio station role that allows the radio to act as a wireless client to another access point or repeater. This feature is exclusive to the integrated radio running in the Cisco 870, 1800, 2800, and 3800 integrated service routers (ISRs).

Universal client mode has the following features and limitations:

- You can configure universal client mode on the main dot11radio interface only, subinterfaces are not supported.
- Universal client can associate to access points with radio VLANs.
- Layer-3 routing is supported over the radio interface. However, there is no support for layer 2 (L2) bridging. The user cannot configure a dot11radio interface with a bridge-group when in universal client mode.
- Service Set Identifiers (SSIDs) are required to be configured on the dot11 interface operating as a universal client; association to an access point running in guest mode is not supported.
- The universal client can associate to Cisco access points, third party access points, and repeaters. It cannot associate to Cisco root bridges or Cisco workgroup bridges.
- Easy VPN does not support universal client mode using DHCP.

How to Configure Radio Settings on an Access Point

Configuring Universal Client Mode

Perform this task to configure universal client mode.

You can configure universal client mode on a Cisco ISR series router by setting the radio interface station role to nonroot. This is different from configuring the dot11radio interface to operate in non-root bridge mode,

which requires specifying the word bridge at the end of the command, for example, station-role non-root bridge.

Note In other Cisco wireless products such as the Cisco AP1232, the station-role non-root command operates the same as station-role non-root bridge command. On the ISRs, the two commands are different: station-role non-root is considered the universal client mode and station-role non-root bridge is considered the nonroot bridge mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dot11Radio** *interface*
4. **station-role {root [access-point | ap-only | bridge [wireless-clients]] | non-root [bridge]}**
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables 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 0/3/0`	Enters configuration mode for the radio interface. • The *interface* argument is in module/slot/port format, except for the Cisco 800 series and Cisco 1800 series fixed-configuration routers, where the *interface* argument is either 0 or 1. • The 2.4-GHz radio is port 0, and the 5-GHz radio is port 1.
Step 4	**station-role {root [access-point | ap-only | bridge [wireless-clients]] | non-root [bridge]}** **Example:** `Router(config-if)# station-role non-root`	Sets the role of the radio interface.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Radio Data Rates on an Access Point

Perform this task to configure radio data rates.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dot11Radio** *interface*
4. **speed** {*data-rates* | **default** | **ofdm-throughput** | **range** | **throughput**}
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables 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*	Enters configuration mode for the radio interface.

	Command or Action	Purpose
	Example: `Router(config)# interface dot11Radio 0/3/0`	• The *interface* argument is in module/slot/port format, except for the Cisco 800 series and Cisco 1800 series fixed-configuration routers, where the *interface* argument is either 0 or 1. • The 2.4-GHz radio is port 0, and the 5-GHz radio is port 1.
Step 4	**speed** {*data-rates* | **default** | **ofdm-throughput** | **range** | **throughput**} **Example:** `Router(config-if)# speed throughput`	Configures the data rates supported by the access point. • Use the no form of the speed command to disable data rates. When you use the no form of the command, all data rates are disabled except the rates you name in the command.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Radio and Client Device Power Levels on an Access Point

Perform this task to set the transmit power on your AP and the power level on client devices that associate to the access point.

When a client device associates to the access point, the AP sends the maximum power level setting to the client.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dot11Radio** *interface*
4. **power local {cck | ofdm} {** *milliwatt* **| maximum}** or**power local {** *milliwatt* | **maximum}**
5. **power client** {*milliwatt*| **maximum**}
6. **end**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables 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 0/3/0`	Enters radio interface configuration mode. • The *interface* argument is in module/slot/port format, except for the Cisco 800 series and Cisco 1800 series fixed-configuration routers, where the *interface* argument is either 0 or 1. • The 2.4-GHz radio is port 0, and the 5-GHz radio is port 1.
Step 4	**power local {cck | ofdm} {** *milliwatt* **| maximum}** or**power local {** *milliwatt* **| maximum}** **Example:** `Router(config-if)# power local 20`	(Optional) Specifies the local transmit power level, which reduces the radio cell size and interference between cells, on a 2.4-GHz, 802.11b/g radio. or Specifies the local transmit power level on a 5-GHz, 802.11a radio. • On the 2.4-GHz radio, you can set CCK and OFDM power levels. On the 5-GHz radio, these keywords are not supported. • For the 802.11b/g radio, the *milliwatt* argument can be 7, 10, 13, 15, 17, or 20. For the 802.11a radio, the *milliwatt*argument can be 4, 7, 10, 13, or 16. • Use the **maximum** keyword to specify the maximum power level. This is the default setting.
Step 5	**power client** {*milliwatt*| **maximum**} **Example:** `Router(config-if)# power client 20`	(Optional) Specifies the maximum power level that clients should use for radio transmissions to the access point. • For the 802.11b/g radio, the *milliwatt* value can be 7, 10, 13, 15, 17, or 20. For the 802.11a radio, the *milliwatt*value can be 4, 7, 10, 13, or 16. • Use the **maximum** keyword to specify the maximum power level. • The default is for the AP to specify no specific client power level.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Radio Channel Settings on an Access Point

Perform this task to set the access point's radio channel.

The default channel setting for the AP radios is least congested; at startup, the AP scans for and selects the least-congested channel. For most consistent performance after a site survey, however, we recommend that you assign a static channel setting for each access point. The channel settings on your AP correspond to the frequencies available in your regulatory domain.

Each 2.4-GHz channel covers 22 MHz. The bandwidth for channels 1, 6, and 11 does not overlap, so you can set up multiple access points in the same vicinity without causing interference.

The 5-GHz radio operates on up to 27 channels from 5170 to 5850 MHz. Each channel covers 20 MHz, and the bandwidth for the channels overlaps slightly. For best performance, use channels that are not adjacent (44 and 46, for example) for radios that are close to each other.

Note Too many access points in the same vicinity creates radio congestion that can reduce throughput. A careful site survey can determine the best placement of access points for maximum radio coverage and throughput.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dot11Radio** *interface*
4. **channel** { *number* | *MHz* | **least-congested** }
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables 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 0/3/0`	Enters radio interface configuration mode. • The *interface* argument is in module/slot/port format, except for the Cisco 800 series and Cisco 1800 series fixed-configuration routers, where the *interface* argument is either 0 or 1. • The 2.4-GHz radio is port 0, and the 5-GHz radio is port 1.
Step 4	**channel** { *number* | *MHz* | **least-congested** } **Example:** `Router(config-if)# channel 2457`	(Optional) Sets the default channel for the AP radio.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Dynamic Frequency Selection on an Access Point

Perform this task to configure DFS on an access point with a 5-GHz radio.

This section applies only to wireless access points shipped to Europe and Japan with 5-GHz radios running Cisco IOS version 12.4(6)T. Access points shipped to Europe and Japan with 5-GHz radios are required to use DFS to detect and avoid interfering with radar signals to comply with that regulatory domain.

The access point automatically sets the operating frequency on a DFS-enabled 5-GHz radio. A specific channel cannot be configured for DFS-enabled 5-GHz radios; the **channel** command is disabled.

Note If the access point is set to use DFS and it is deployed in a regulatory domain that does not allow or does not require the use of DFS, disable DFS by using the **no dfs band block**interface configuration command.

DFS-enabled 5-GHz radios monitor the operating frequency for radar signals. If radar signals are detected on the channel, the access point takes these steps:

- Blocks new transmissions on the channel.
- Flushes the power-save client queues.
- Broadcasts an 802.11h channel-switch announcement.
- Disassociates remaining client devices.
- Randomly selects a different channel:
  - If the access point does not select a DFS-required channel, the access point enables beacons and accepts client associations.
  - If the access point selects a DFS required channel, the access point scans the new channel for radar signals for 60 seconds. If there are no radar signals on the new channel, the access point enables beacons and accepts client associations. If a radar signal is detected, the access point selects a different channel.

When a DFS-enabled 5-GHz radio operates on one of the following 15 channels, the access point automatically uses DFS to set the operating frequency:

- 52 (5260 MHz)
- 56 (5280 MHz)
- 60 (5300 MHz)
- 64 (5320 MHz)
- 100 (5500 MHz)
- 104 (5520 MHz)
- 108 (5540 MHz)
- 112 (5560 MHz)
- 116 (5580 MHz)
- 120 (5600 MHz)
- 124 (5620 MHz)
- 128 (5640 MHz)
- 132 (5660 MHz)

- 136 (5680 MHz)
- 140 (5700 MHz)

The maximum legal transmit power is greater for some 5-GHz channels than for others. When the access point randomly selects a 5-GHz channel on which power is restricted, the access point automatically reduces transmit power to comply with power limits for that channel.

Note Cisco recommends using the world-mode dot11d country-code interface configuration command to configure a country code on DFS-enabled radios. The IEEE 802.11h protocol requires access points to include the country information element (IE) in beacons and probe responses. By default, however, the country code in the IE is blank. Use the world-mode command to populate the country code IE.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dot11Radio** *interface*
4. **dfs band** *frequency-group* **block**
5. **end**
6. **show controllers dot11Radio** *interface*
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables 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 0/3/1`	Enters interface configuration mode. • The *interface* argument is in module/slot/port format, except for the Cisco 1800 series fixed-configuration routers, where the *interface* argument is either 0 or 1. • The 5-GHz radio is port 1.

	Command or Action	Purpose

Step 4	**dfs band** *frequency-group* **block**
	
	Example:
	`Router(config-if)# dfs band 1 2 block`
		Prevents an access point from selecting a specific group of frequencies during DFS.
		• The *frequency-group*value can be **1**, **2**, **3**, or **4**:
		  • **1** specifies frequencies 5.150 to 5.250 GHz.
		  • **2** specifies frequencies 5.250 to 5.350 GHz.
		  • **3** specifies frequencies 5.470 to 5.725 GHz.
		  • **4** specifies frequencies 5.725 to 5.825 GHz.
		• At least one group of frequencies must be specified. Multiple groups are allowed.

Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show controllers dot11Radio** *interface* **Example:** `Router# show controllers dot11Radio 0/0/1`	(Optional) Displays radio controller status. • The Current Frequency line of the output displays the status of DFS, for example: Current Frequency: 5300 MHz Channel 60 (DFS enabled)
Step 7	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Enabling and Disabling World Mode on an Access Point

Perform this task to configure the AP to support 802.11d world mode or Cisco legacy world mode.

When you enable world mode, the AP adds channel carrier set information to its beacon. Client devices with world mode enabled receive the carrier set information and adjust their settings automatically. For example, a client device used primarily in Japan could rely on world mode to adjust its channel and power settings automatically when it travels to Italy and joins a network there. World mode is disabled by default.

Aironet extensions must be enabled for world mode operation. Aironet extensions are enabled by default.

Note World mode is not supported on the 5-GHz radio.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dot11Radio** *interface*
4. **world-mode {legacy | dot11d country-code code} {indoor | outdoor | both}**
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables 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 0/3/0`	Enters radio interface configuration mode. • The *interface* argument is in module/slot/port format, except for the Cisco 800 series and Cisco 1800 series fixed-configuration routers, where the *interface* argument is either 0 or 1. • The 2.4-GHz radio is port 0, and the 5-GHz radio is port 1.
Step 4	**world-mode {legacy | dot11d country-code code} {indoor | outdoor | both}** **Example:** `Router(config-if)# world-mode legacy indoor`	Enables AP world mode operation. • The example enables Cisco legacy world mode and specifies that the AP is indoors.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Enabling and Disabling Short Radio Preambles on an Access Point

Perform this task to enable or disable short radio preambles.

The radio preamble (sometimes called a header) is a section of data at the head of a packet that contains information that the AP and client devices need when sending and receiving packets. You can set the radio preamble to long or short:

- Short--A short preamble improves throughput performance. Cisco Aironet Wireless LAN Client Adapters support short preambles. Early models of Cisco Aironet's Wireless LAN Adapter (PC4800 and PC4800A) require long preambles.
- Long--A long preamble ensures compatibility between the AP and all early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A). If these client devices do not associate to your access points, you should use short preambles.

Note You cannot configure short or long radio preambles on the 5-GHz radio.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dot11Radio** *interface*
4. **preamble-short**
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface dot11Radio** *interface* **Example:** `Router(config)# interface dot11Radio 0/3/0`	Enters radio interface configuration mode. • The *interface* argument is in module/slot/port format, except for the Cisco 800 series and Cisco 1800 series fixed-configuration routers, where the *interface* argument is either 0 or 1. • The 2.4-GHz radio is port 0, and the 5-GHz radio is port 1.
Step 4	**preamble-short** **Example:** `Router(config-if)# no preamble-short`	Disables short preambles and enables long preambles. • Short preambles are enabled by default. Use the **preamble-short** command to reenable short preambles if they are disabled.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Transmit and Receive Antennas on an Access Point

Perform this task to select the antenna the AP uses to transmit and receive data.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dot11Radio** *interface*
4. **antenna { receive | transmit} { diversity | left | right }**
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables 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 0/3/0`	Enters radio interface configuration mode. • The *interface* argument is in module/slot/port format, except for the Cisco 800 series and Cisco 1800 series fixed-configuration routers, where the *interface* argument is either 0 or 1. • The 2.4-GHz radio is port 0, and the 5-GHz radio is port 1.
Step 4	**antenna { receive | transmit} { diversity | left | right }** **Example:** `Router(config-if)# antenna receive right`	Sets the transmit or receive antenna to diversity, left, or right. **Note** For best performance, leave the transmit antenna setting at the default setting, **diversity**.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Enabling and Disabling Aironet Extensions on an Access Point

Perform this task to enable or disable Cisco Aironet extensions to the IEEE 802.11b standard.

Aironet extensions are enabled by default.

By default, the AP uses Cisco Aironet 802.11 extensions to detect the capabilities of Cisco Aironet client devices and to support features that require specific interaction between the AP and associated client devices. Aironet extensions must be enabled to support these features:

- Load balancing--The AP uses Aironet extensions to direct client devices to an AP that provides the best connection to the network based on factors such as number of users, bit error rates, and signal strength.
- Message Integrity Check (MIC)--MIC is an additional WEP security feature that prevents attacks on encrypted packets called bit-flip attacks. 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.
- Temporal Key Integrity Protocol (TKIP)--TKIP, also known as WEP key hashing, is an additional WEP security feature that defends against an attack on WEP in which the intruder uses an unencrypted segment called the initialization vector (IV) in encrypted packets to calculate the WEP key.
- Repeater mode--Aironet extensions must be enabled on repeater access points and on the root access points to which they associate.
- World mode--Client devices with world mode enabled receive carrier set information from the AP and adjust their settings automatically.
- Limiting the power level on associated client devices--When a client device associates to the access point, the AP sends the maximum allowed power level setting to the client.

Disabling Aironet extensions disables the features listed above, but it sometimes improves the ability of non-Cisco client devices to associate to the access point.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dot11Radio** *interface*
4. **no dot11 extension aironet**
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables 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*	Enters radio interface configuration mode.

	Command or Action	Purpose
	Example: `Router(config)# interface dot11Radio 0/3/0`	• The *interface* argument is in module/slot/port format, except for the Cisco 800 series and Cisco 1800 series fixed-configuration routers, where the *interface* argument is either 0 or 1. • The 2.4-GHz radio is port 0, and the 5-GHz radio is port 1.
Step 4	**no dot11 extension aironet** **Example:** `Router(config-if)# no dot11 extension aironet`	Disables Aironet extensions. • Use the **dot11 extension aironet** command to enable Aironet extensions if they are disabled.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Ethernet Encapsulation Transformation Method on an Access Point

Perform this task to configure the encapsulation transformation method.

When the AP receives data packets that are not 802.3 packets, the AP must format the packets to 802.3 using an encapsulation transformation method. These are the two transformation methods:

- dot1h (802.1H)--This method provides optimum performance for Cisco Aironet wireless products.
- RFC 1042--Use this setting to ensure interoperability with non-Cisco Aironet wireless equipment. RFC 1042 does not provide the interoperability advantages of 802.1H but is used by other manufacturers of wireless equipment. This is the default setting.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dot11Radio** *interface*
4. **payload-encapsulation { rfc1042 | dot1h }**
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables 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 0/3/0`	Enters radio interface configuration mode. • The *interface* argument is in module/slot/port format, except for the Cisco 800 series and Cisco 1800 series fixed-configuration routers, where the *interface* argument is either 0 or 1. • The 2.4-GHz radio is port 0, and the 5-GHz radio is port 1.
Step 4	**payload-encapsulation { rfc1042 | dot1h }** **Example:** `Router(config-if)# no dot11 extension aironet`	Specifies the encapsulation transformation method to RFC 1042 (SNAP) or dot1h (IEEE 802.1h).
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Beacon Period and DTIM on an Access Point

Perform this task to configure the beacon period and delivery traffic indication message (DTIM).

The beacon period is the amount of time between AP beacons in Kilo microseconds. One kilomicrosecond equals 1,024 microseconds. The Data Beacon Rate, always a multiple of the beacon period, determines how often the beacon contains a DTIM. The DTIM tells power-save client devices that a packet is waiting for them.

For example, if the beacon period is set at 100, its default setting, and the data beacon rate is set at 2, its default setting, then the AP sends a beacon containing a DTIM every 200 kilomicroseconds.

The default beacon period is 100, and the default DTIM is 2.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dot11Radio** *interface*
4. **beacon** { **period** *microseconds* | **dtim-period** *period-count* }
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables 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*	Enters configuration mode for the radio interface.

	Command or Action	Purpose
	Example: `Router(config)# interface dot11Radio 0/3/0`	• The *interface* argument is in module/slot/port format, except for the Cisco 800 series and Cisco 1800 series fixed-configuration routers, where the *interface* argument is either 0 or 1. • The 2.4-GHz radio is port 0, and the 5-GHz radio is port 1.
Step 4	**beacon { period** *microseconds* **| dtim-period** *period-count* **}** **Example:** `Router(config-if)# beacon period 15`	Specifies how often the beacon contains a Delivery Traffic Indicator Message (DTIM).
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring RTS Threshold and Retries on an Access Point

Perform this task to set the Request-to-Send (RTS) threshold and number of retries.

The RTS threshold determines the packet size at which the AP issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the access point, or in areas where the clients are far apart and can detect only the AP and not each other. You can enter a setting ranging from 0 to 2347 bytes.

Maximum RTS Retries is the maximum number of times the AP issues an RTS before stopping the attempt to send the packet over the radio. Enter a value from 1 to 128.

The default RTS threshold is 2312, and the default maximum RTS retries setting is 32.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dot11Radio** *interface*
4. **rts** {**threshold** *bytes* | **retries** *number*}
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables 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 0/3/0`	Enters radio interface configuration mode. • The *interface* argument is in module/slot/port format, except for the Cisco 800 series and Cisco 1800 series fixed-configuration routers, where the *interface* argument is either 0 or 1. • The 2.4-GHz radio is port 0, and the 5-GHz radio is port 1.
Step 4	**rts** {**threshold** *bytes*	**retries** *number*} **Example:** `Router(config-if)# rts retries 30`	Sets the RTS threshold or maximum RTS retries number.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Maximum Data Retry on an Access Point

Perform this task to specify the number of attempts the AP makes to send a packet before giving up and dropping the packet.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dot11Radio** *interface*
4. **packet retries** *number*
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables 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 0/3/0`	Enters radio interface configuration mode. • The *interface* argument is in module/slot/port format, except for the Cisco 800 series and Cisco 1800 series fixed-configuration routers, where the *interface* argument is either 0 or 1. • The 2.4-GHz radio is port 0, and the 5-GHz radio is port 1.
Step 4	**packet retries** *number* **Example:** `Router(config-if)# rts retries 30`	Specifies the number of attempts the AP makes to send a packet before giving up and dropping the packet.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Packet Fragmentation Threshold on an Access Point

Perform this task to configure the size at which packets are fragmented (sent as several pieces instead of as one block).

Use a low setting in areas where communication is poor or where there is a great deal of radio interference.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dot11Radio** *interface*
4. **fragment-threshold** *bytes*
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables 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*	Enters radio interface configuration mode.

	Command or Action	Purpose
	Example: `Router(config)# interface dot11Radio 0/3/0`	• The *interface* argument is in module/slot/port format, except for the Cisco 800 series and Cisco 1800 series fixed-configuration routers, where the *interface* argument is either 0 or 1. • The 2.4-GHz radio is port 0, and the 5-GHz radio is port 1.
Step 4	**fragment-threshold** *bytes* **Example:** `Router(config-if)# rts retries 30`	Sets the size at which packets are fragmented.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring IP Phone Support on an Access Point

Perform this task to enable 802.11 compliance phone support.

Enabling IEEE 802.11 compliance phone support adds information to the AP beacons and probe responses. This information helps some 802.11 phones make intelligent choices about the AP to which they should associate. Some phones do not associate with an AP without this additional information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot11 phone**
4. **end**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dot11 phone** **Example:** `Router(config)# dot11 phone`	Enables IEEE 802.11 compliance phone support.
Step 4	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 5	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuration Examples for Radio Settings on an Access Point

Configuring Radio Data Rates Example

The following example shows how to disable the 1-Mbps data rate and set the rest of the data rates to **basic**:

```
configure terminal
 interface dot11radio 0
 no speed basic-2.0 basic-5.5 basic-11.0
 end
 copy running-config startup-config
```

Additional References

The following sections provide references related to configuring radio settings on an access point.

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*

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

Feature Information for Configuring Radio Settings on an Access Point

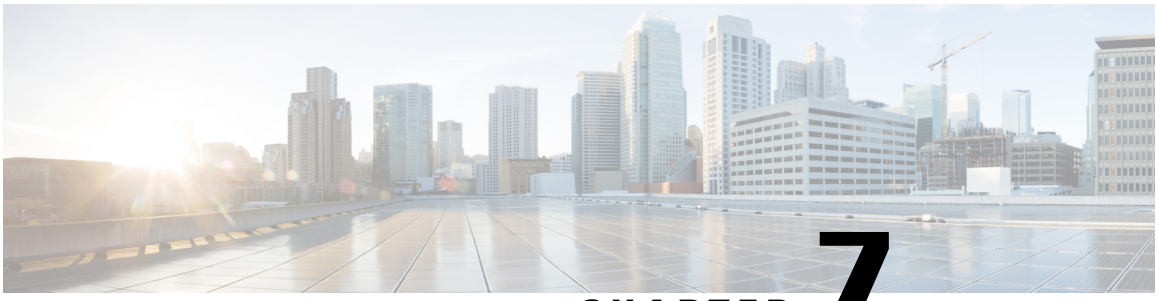
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 7: Feature Information for Configuring Radio Settings on an Access Point

Feature Name	Releases	Feature Information
Access Point Link Role Flexibility	12.4(15)T	This feature allows access point radios to operate in a combination of radio roles, such as access point root, access point repeater, bridge root (with or without clients), bridge nonroot (with or without clients), and WGB.
Universal Client Mode	12.4(15)T	This feature allows a wireless device to associate to other Cisco and third-party APs.
Wireless Non-Root Bridge	12.4(15)T	This feature allows a wireless device to operate as the remote node in a point-to-point or point-to-multi-point network.
Cisco Compatible Extensions Information Element	12.4T	This feature allows a Cisco access point to inform Cisco Compatible Extension client devices about the Cisco-compatible release version that the access point supports.
Configurable Radio Transmit Power	12.4T	This feature allows a user to set the transmit power of the access point.
Dynamic Frequency Selection (DFS) and IEEE 802.11h Transmit Power Control	12.4T	This feature allows a user to block groups of channels to prevent an access point from selecting them when DFS is enabled.

Feature Name	Releases	Feature Information
IEEE 802.11 Wireless Standards Support	12.4T	This feature provides support for 802.11 standards, which allows you to set channels, transmission rates, and power-save mode, among other configurable fields.
IEEE 802.11a Support	12.4T	This feature provides support for 802.11a standards, which allows you to set channels, transmission rates, and power-save mode, among other configurable fields.
IEEE 802.11b Support	12.4T	This feature provides support for 802.11b standards, which allows you to set channels, transmission rates, and power-save mode, among other configurable fields.
IEEE 802.11d Support	12.4T	This feature provides support for 802.11d standards, which allows you to set channels, transmission rates, and power-save mode, among other configurable fields.
IEEE 802.11g Support	12.4T	This feature provides support for 802.11g standards, which allows you to set channels, transmission rates, and power-save mode, among other configurable fields.
Transmit Power Control	12.4T	This feature allows client devices to calculate the path loss and the transmit power necessary for the client to reach the access point, thereby extending client device battery life.
Wireless Access Point High-Speed WAN Interface Card	12.4T	This feature provides support for two new AP HWICs.
World Mode	12.4T	This feature automates client configuration of channel and transmit power settings allowing world-mode-enabled access points to configure the settings on world-mode-enabled clients. World mode is supported only on the 2.4-GHz radio.



CHAPTER 7

NAC—L2 IEEE 802.1x

This feature extends NAC support to Layer 2 switches and wireless access points.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About NAC—L2 IEEE 802.1x

Network Admission Control

The NAC layer 2 (L2) IEEE 802.1x feature extends NAC support to Layer 2 switches and wireless access points. Network admission control (NAC) is a Cisco Systems sponsored initiative that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources, thereby limiting damage from viruses and worms.

Using NAC, you can provide network access to endpoint devices such as PCs, PDAs, and servers that are verified to be fully compliant with an established security policy. NAC can also identify noncompliant devices and deny them access, place them in a quarantined area, or give them restricted access to computing resources.

Additional References for NAC—L2 IEEE 802.1x

The following sections provide references related to NAC—L2 IEEE 802.1x.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco IOS wireless LAN commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS Wireless LAN Command Reference
VLAN conceptual information	*Cisco IOS LAN Switching Configuration Guide*

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 Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

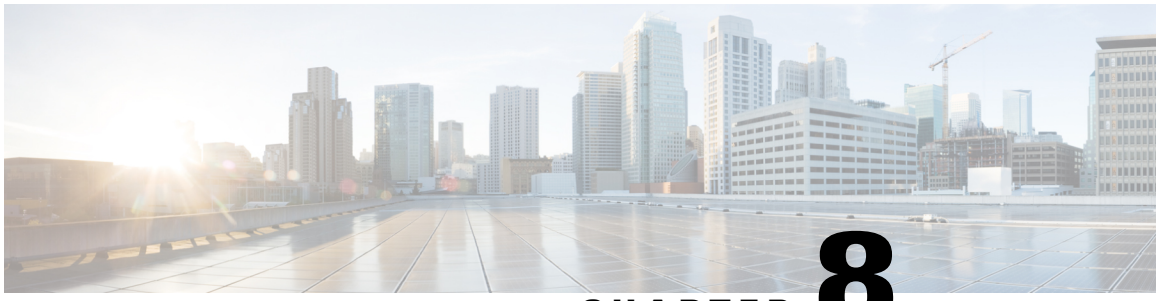
Feature Information for NAC—L2 IEEE 802.1x

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 8: Feature Information for NAC—L2 IEEE 802.1x

Feature Name	Releases	Feature Information
NAC—L2 IEEE 802.1x	12.4(15)T	This feature extends NAC support to Layer 2 switches and wireless access points. There are no new or modified commands associated with this feature.



CHAPTER 8

VLAN Assignment by Name

This feature provides the ability for the RADIUS server to assign an 802.1x client to a VLAN identified by name. This module describes how to configure wireless VLANs on a Cisco 800, 1800, 2800, or 3800 series integrated services router (ISR), hereafter referred to as an access point (AP).

This feature provides the ability for the RADIUS server to assign an 802.1x client to a VLAN identified by name.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About VLAN Assignment by Name

VLANs Overview

A VLAN is a switched network that is logically segmented by functions, project teams, or applications rather than on a physical or geographical basis. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN, regardless of their physical connections to the network or whether they are intermingled with other teams. You use VLANs to reconfigure the network through software rather than physically unplugging and moving devices or wires.

A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment such as LAN switches that operate bridging protocols between them with a separate group for each VLAN.

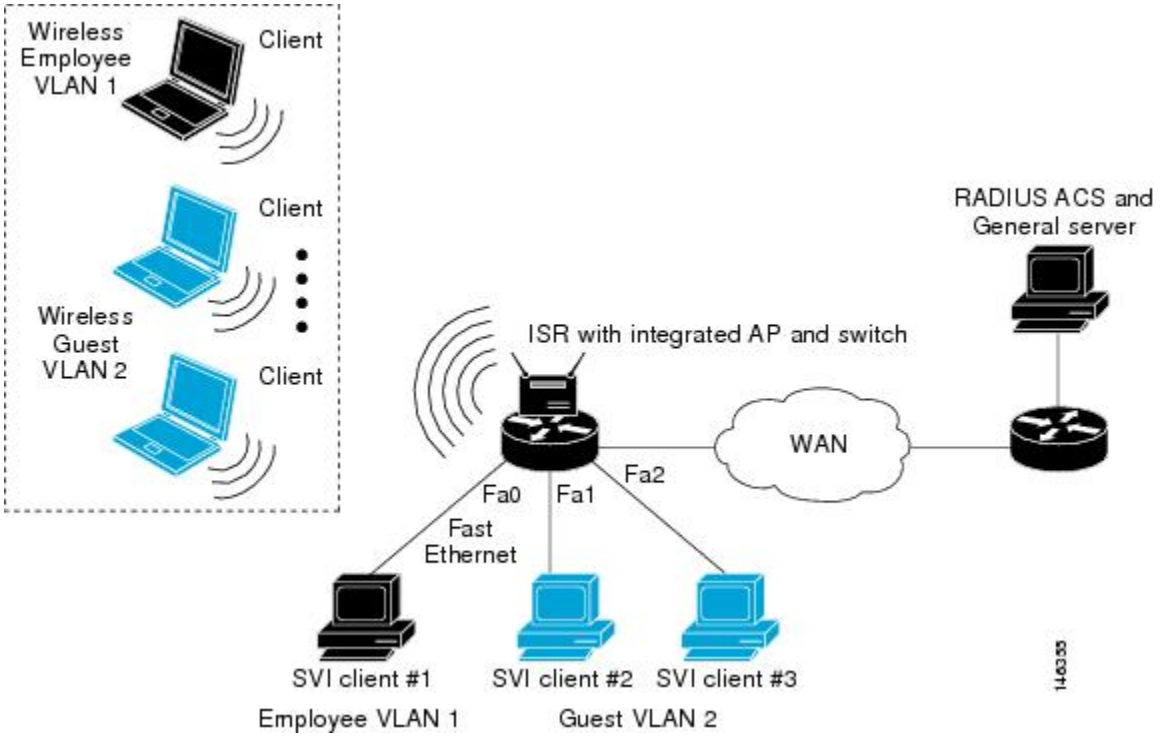
VLANs provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address scalability, security, and network management. You should consider several key issues when designing and building switched LAN networks:

- LAN segmentation
- Security
- Broadcast control
- Performance
- Network management
- Communication between VLANs

You extend VLANs into a wireless LAN by adding IEEE 802.11q tag awareness to the AP. Frames destined for different VLANs are transmitted by the AP wirelessly on different service set identifiers (SSIDs). Only the clients associated with that VLAN receive those packets. Each SSID can have one VLAN assigned to it. The benefit of using multiple SSIDs and VLANs is that you can configure different security features for each group. For example, users in VLAN 1 might be forced to use MAC authentication while users in VLAN 2 are not.

The figure below shows both wired and wireless VLANs coexisting on a router with an integrated AP and switch.

Figure 9: LAN and VLAN Segmentation with Wireless Devices



Wireless Device Deployment in VLANs

The basic wireless components of a VLAN consist of an AP and a client associated to it using wireless technology.

You configure an AP to connect to a specific VLAN by configuring its SSID to recognize that VLAN. Because VLANs are identified by a VLAN ID, it follows that if the SSID on an AP is configured to recognize a specific VLAN ID, a connection to the VLAN is established. When this connection is made, associated wireless client devices having the same SSID can access the VLAN through the AP. The VLAN processes data to and from the clients the same way that it processes data to and from wired connections.

You can configure up to 10 SSIDs or VLANs on the Cisco 800 series routers, and up to 16 SSIDs or VLANs on the Cisco 1800 series fixed-configuration routers and the Cisco 1841, 2800 and 3800 series modular routers with an AP high-speed WAN interface card (HWIC). You can assign only one SSID to a VLAN.

The limits for the 16 configurable VLANs on routers with an AP HWIC are:

- 1 static and 15 dynamic VLANs
- 1 static and 15 unsecured VLANs
- 16 dynamic VLANs
- 16 unsecured VLANs

The limits for the 16 configurable VLANs on the Cisco 1800 series fixed-configuration routers are:

- 1 static Wired Equivalent Privacy (WEP) encrypted VLAN, 7 dynamic WEP VLANs, and 8 unsecured VLANs
- 1 static and 15 unsecured VLANs
- 8 dynamic and 8 unsecured VLANs
- 16 unsecured VLANs

The limits for the 10 configurable VLANs on the Cisco 800 series routers are:

- 1 static WEP encrypted VLAN, 3 dynamic WEP VLANs, and 6 unencrypted VLANs

You can use the VLAN feature to deploy wireless devices with greater efficiency and flexibility. For example, one AP can handle the specific requirements of multiple users having widely varied network access and permissions. Without VLAN capability, multiple APs would be needed to serve classes of users based on the access and permissions they were assigned.

These are two common strategies for deploying wireless VLANs:

- Segmentation by user groups: You can segment your wireless LAN user community and enforce a different security policy for each user group. For example, you can create wired and wireless VLANs in an enterprise environment for full-time and part-time employees and also provide guest access.
- Segmentation by device types: You can segment your wireless LAN to allow different devices with different security capabilities to join the network. For example, some wireless users might have handheld devices that support only static WEP, and some wireless users might have more sophisticated devices using dynamic WEP. You can group and isolate these devices into separate VLANs.

Assignment of Users to VLANs Using a RADIUS Server

You can configure your RADIUS authentication server to assign users or groups of users to a specific VLAN when they authenticate to the network.

The VLAN-mapping process consists of these steps:

1. A client device associates to the AP using any SSID configured on the AP.
2. The client begins RADIUS authentication.
3. When the client authenticates, the RADIUS server maps the client to a specific VLAN, regardless of the VLAN mapping defined for the SSID the client is using on the AP. If the server does not return any VLAN attribute for the client, the client is assigned to the VLAN specified by the SSID mapped locally on the AP.

These are the RADIUS user attributes used for VLAN ID assignment. Each attribute must have a common tag value to identify the grouped relationship.

- IETF 64 (Tunnel Type): Set this attribute to VLAN.
- IETF 65 (Tunnel Medium Type): Set this attribute to 802.
- IETF 81 (Tunnel Private Group ID): Set this attribute to a VLAN ID.

How to Configure Wireless VLANs

Configuring a Wireless VLAN

Using the LAN and VLAN Segmentation with Wireless Devices figure as a reference, perform this task to configure a VLAN on an AP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot11 ssid** *name*
4. **vlan** *vlan-id*
5. **exit**
6. **interface dot11Radio** *interface*
7. **ssid** *name*
8. **exit**
9. **exit**
10. **interface dot11Radio** *interface.x*
11. **encapsulation dot1q** *vlan-id* [**native**]
12. **end**
13. **copy running-config startup-config**
14. **show vlans**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dot11 ssid** *name* **Example:** `Device(config)# dot11 ssid anyname`	Creates a global SSID. • The *name* argument is a case-sensitive alphanumeric string up to 32 characters in length.

	Command or Action	Purpose
		• The SSID is inactive until you use the **ssid** command in interface configuration mode to assign the SSID to a specific radio interface.
Step 4	**vlan** *vlan-id* **Example:** `Device(config-ssid)# vlan 1`	Assigns the SSID to a VLAN on your network. • Client devices that associate using the SSID are grouped into this VLAN. • Enter a VLAN ID from 1 to 4095.
Step 5	**exit** **Example:** `Device(config-ssid)# exit`	Exits SSID configuration mode and returns to global configuration mode.
Step 6	**interface dot11Radio** *interface* **Example:** `Device(config)# interface dot11Radio 0/3/0`	Enters interface configuration mode for the radio interface. • The *interface* argument is in module/slot/port format, except for the Cisco 800 and Cisco 1800 fixed-configuration series routers, where the *interface* argument is either 0 or 1. • The 2.4-GHz radio port is 0. The 5-GHz radio port is 1.
Step 7	**ssid** *name* **Example:** `Device(config-if)# ssid anyname`	Assigns an SSID to a specific radio interface. • The *name* argument is a case-sensitive alphanumeric string up to 32 characters in length.
Step 8	**exit** **Example:** `Device(config-if-ssid)# exit`	Exits SSID configuration mode.
Step 9	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.
Step 10	**interface dot11Radio** *interface.x* **Example:** `Device(config)# interface dot11Radio 0/3/0.1`	Enters configuration mode for the Ethernet VLAN subinterface. • On the Cisco 800 and Cisco 1800 fixed-configuration series routers, the *interface* argument is either 0 or 1, which means this command would be entered as **interface dot11Radio 0.1**.

	Command or Action	Purpose
Step 11	**encapsulation dot1q** *vlan-id* [**native**] **Example:** `Device(config-subif)# encapsulation dot1q 1 native`	Sets the encapsulation type for an interface.
Step 12	**end** **Example:** `Device(config-subif)# end`	Returns to privileged EXEC mode.
Step 13	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.
Step 14	**show vlans** **Example:** `Device# show vlans`	(Optional) Displays the VLANs that the AP supports.

Assigning Names to VLANs

You can assign a name to a VLAN in addition to its numerical ID. VLAN names can contain up to 32 ASCII characters. The access point stores each VLAN name and ID pair in a table.

Remember these guidelines when using VLAN names:

- The mapping of a VLAN name to a VLAN ID is local to each access point, so across your network, you can assign the same VLAN name to a different VLAN ID.

Note If clients on your wireless LAN require seamless roaming, we recommend that you assign the same VLAN name to the same VLAN ID across all access points, or that you use only VLAN IDs without names.

- Every VLAN configured on your access point must have an ID, but VLAN names are optional.
- VLAN names can contain up to 32 ASCII characters in length. However, a VLAN name cannot be a number from 1 to 4095. For example, vlan4095 is a valid VLAN name, but 4095 is not. The access point reserves the numbers 1 through 4095 for VLAN IDs.

Assigning a Name to a VLAN

Perform this task to assign a name to a VLAN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot11 vlan-name** *name* **vlan** *vlan-id*
4. **end**
5. **copy running-config startup-config**
6. **show dot11 vlan-name** [*vlan-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dot11 vlan-name** *name* **vlan** *vlan-id* **Example:** `Device(config)# dot11 vlan-name vlan1 vlan 121`	Assigns a name to a VLAN in addition to its numerical ID.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 5	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
Step 6	**show dot11 vlan-name** [*vlan-name*] **Example:** `Device# show dot11 vlan-name`	(Optional) Displays VLAN names and ID pairs configured on the access point.

Configuration Examples for VLAN Assignment by Name

Example: VLAN Configuration Scenario

The following VLAN configuration scenario shows how to use VLANs to manage wireless devices in a typical branch office. In this example, two levels of access are available through VLANs configured on the network:

- Employee access—Users can access all company files, databases, and sensitive information. Employees are required to authenticate using Cisco Light Extensible Authentication Protocol (LEAP).
- Guess access—Users can access only the Internet and any external files stored specifically for guest users.

In this scenario, a minimum of two VLAN connections are required, one for each level of access. Because the AP can support up to 16 SSIDs on the AP HWIC and Cisco 1800 fixed-configuration routers, and up to 10 SSIDs on the Cisco 800 series routers, you can use the basic design shown in the table below.

Table 9: VLAN Basic Design

Level of Access	SSID	VLAN ID
Employee	employee	1
Guest	guest	2

Employees configure their wireless client adapters to use the SSID named employee and guests configure their client adapters to use the SSID named guest. When these clients associate to the AP, they automatically belong to the correct VLAN. Wired clients attached to the router through the integrated switch can also belong to a specific VLAN. Wireless VLAN clients and wired VLAN clients can share subnets or they can belong to completely different subnets. This type of configuration can be accomplished using bridging or integrated routing and bridging (IRB) or routing on the dot11 interface.

The following examples show two configuration methods:

1. Bridge traffic between wireless VLANs and wired VLANs using IRB and route traffic from these networks through the bridged virtual interface (BVI). The clients in the wireless VLANs and wired VLANs will be in the same respective subnets as the IP address of the BVI interfaces.
2. Use routing to keep the wireless and wired VLANs in separate subnets.

Example: Configuring Wireless VLANs on an Access Point in Bridging Mode

Using the VLAN configuration scenario above, this example shows how to configure VLAN 1 and VLAN 2 on an AP in bridging mode. When the AP has been configured, the example shows how to configure each client device to recognize either the employee SSID or the guest SSID.

This example shows the following configuration steps:

- Create a global SSID.
- Assign a VLAN to each configured SSID.
- Assign authentication types to each SSID.
- Configure subinterfaces and 802.1q encapsulation for each VLAN under the dot11 interface.
- Assign a bridge group for each subinterface.
- Assign the same bridge group to the relevant wired VLAN.
- Create a BVI interface and assign an IP address for each bridge group.
- Configure the protocol to route each bridge group.

```
configure terminal
 dot11 ssid employee
  vlan 1
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa
   exit
  interface dot11Radio 0/0/0
   no ip address
   encryption vlan 1 mode ciphers aes-ccm
   ssid employee
   exit
  exit
 dot11 ssid guest
  vlan 2
  authentication open
  exit
 interface dot11Radio 0/0/0.1
 encapsulation dot1q 1 native
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
 exit
 interface dot11Radio 0/0/0.2
 encapsulation dot1q 2
 bridge-group 2
 exit
interface FastEthernet 0/1/2
 switchport access vlan 2
 exit
interface FastEthernet 0/1/3
 switchport access vlan 2
 exit
 interface vlan 1
 bridge group 1
 exit
interface vlan 2
 bridge group 2
 exit
```

```
 interface bvi 1
 ip address 10.10.10.1 255.255.255.0
 exit
interface bvi 2
 ip address 20.20.20.1 255.255.255.0
 exit
bridge 1 route ip
bridge 2 route ip
exit
 copy running-config to startup-config
```

Example: Configuring Wireless VLANs on an Access Point in Routing Mode

Using the VLAN configuration scenario described in the previous section, this example shows how to configure VLAN 1 and VLAN 2 on an AP in routing mode. Routing can be used to keep the wireless and wired VLANs on separate subnets. After the AP has been configured, the example shows how to configure each client device to recognize either the employee SSID or the guest SSID.

This example shows the following configuration steps:

- Create a global SSID.
- Assign a VLAN to each configured SSID.
- Assign authentication types to each SSID.
- Configure subinterfaces and 802.1q encapsulation for each VLAN under the dot11 interface.
- Configure an IP address for each subinterface.

```
configure terminal
 dot11 ssid employee
 vlan 1
 authentication open eap eap_methods
 authentication network-eap eap_methods
 authentication key-management wpa
 exit
 interface dot11Radio 0/0/0
 no ip address
 encryption vlan 1 mode ciphers aes-ccm
 ssid employee
 exit
exit
 dot11 ssid guest
 vlan 2
 authentication open
 exit
 interface dot11Radio 0/0/0
 ssid guest
 exit
exit
 interface dot11Radio 0/0/0.1
 encapsulation dot1Q 1 native
 ip address 10.10.10.1 255.255.255.0
exit
 interface dot11Radio 0/0/0.2
 encapsulation dot1q 2
 ip address 50.50.50.1 255.255.255.0
end
 copy running-config startup-config
```

Where to Go Next

If you want to configure quality of service (QoS) parameters on an AP, see the "Configuring QoS on an Access Point" module.

Additional References for VLAN Assignment by Name

The following sections provide references related to configuring VLANs for wireless LANs.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco IOS wireless LAN commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS Wireless LAN Command Reference
VLAN conceptual information	*Cisco IOS LAN Switching Configuration Guide*

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 Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

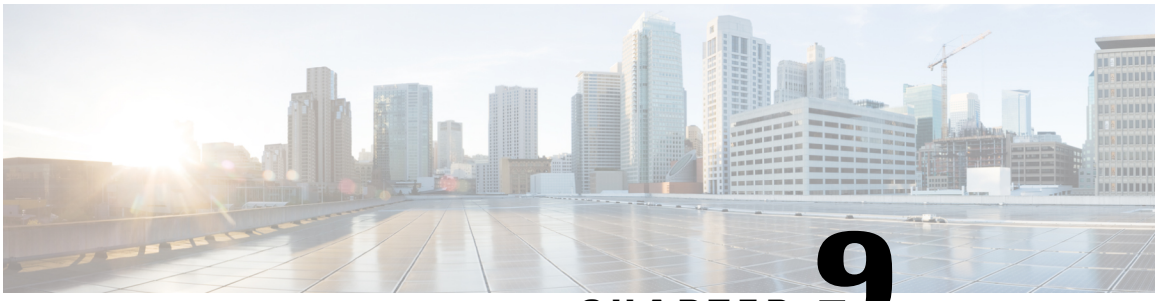
Feature Information for VLAN Assignment By Name

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 10: Feature Information for Configuring Wireless VLANs

Feature Name	Releases	Feature Information
VLAN Assignment by Name	12.4(15)T	This feature provides the ability for the RADIUS server to assign an 802.1x client to a VLAN identified by name.



CHAPTER 9

Implementing Quality of Service in a Wireless LAN

This module describes how to implement quality of service (QoS) features on a Cisco 800, 1800, 2800, or 3800 series integrated services router, hereafter referred to as an access point or AP.

QoS enables you to use congestion management and avoidance tools, which prevent traffic from slowing down on your wireless LAN (WLAN).

In a wired network, routers or switches primarily enforce QoS. In a WLAN, however, the access point manages QoS duties for traffic to wireless clients.

Without QoS, the access point offers best-effort service to each packet, regardless of the packet contents or size. It sends the packets without any assurance of reliability, delay bounds, or throughput.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the Feature Information for Implementing Quality of Service in a Wireless LAN, on page 156.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Implementing QoS in a Wireless LAN

The following prerequisites apply to implementing QoS in a wireless LAN:

- If you use VLANs on your wireless LAN, make sure the necessary VLANs are configured on your access point before configuring QoS.
- Be familiar with the traffic on your wireless LAN. If you know the applications used by wireless client devices, the sensitivity of applications to delay, and the amount of traffic associated with the applications, configuring QoS improves performance.
- QoS does not create additional bandwidth on a wireless LAN; it helps control the allocation of bandwidth. If there is enough bandwidth on your wireless LAN, it might not be necessary to configure QoS.

Information About Implementing QoS in a Wireless LAN

QoS for Wireless LANs

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

When you configure QoS on the access point, you can select specific network traffic, prioritize it, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. Implementing QoS in your wireless LAN makes network performance more predictable and bandwidth utilization more effective.

When you configure QoS, you create QoS policies and apply the policies to the VLANs configured on your access point. If you do not use VLANs on your network, you can apply your QoS policies to the access point's Ethernet and radio ports.

QoS for Wireless LANs Compared to QoS on Wired LANs

The QoS implementation for wireless LANs differs from QoS implementations on other Cisco devices. With QoS enabled, access points have the following behavior:

- They do not classify packets; they prioritize packets based on the Dynamic Host Configuration Protocol (DSCP) value, client type (such as a wireless phone), or the priority value in the 802.1q or 802.1p tag.

- They do not match packets using access control lists (ACL); they use only Modular QoS CLI (MQC) class maps for matching clauses.
- They do not construct internal DSCP values; they support mapping only by assigning IP DSCP, Precedence, or Protocol values to Layer 2 Class of Service (CoS) values.
- They carry out Enhanced Distributed Coordination Function (EDCF) like queueing on the radio egress port only.
- They do only First In First Out (FIFO) queueing on the Ethernet egress port.
- They support only 802.1q/p tagged packets. Access points do not support Inter-Switch Link (ISL).
- They support only MQC policy-map set cos action.
- They prioritize the traffic from voice clients (such as Symbol phones) over traffic from other clients when the QoS Element for Wireless Phones feature is enabled.
- They support Spectralink phones using the class-map IP protocol clause with the protocol value set to 119.

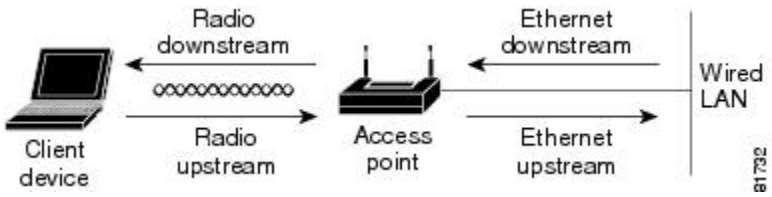
Impact of QoS on a Wireless LAN

Wireless LAN QoS features area subset of the 802.11e draft. QoS on wireless LANs provides prioritization of traffic from the access point over the WLAN based on traffic classification.

Just as in other media, you might not notice the effects of QoS on a lightly loaded wireless LAN. The benefits of QoS become more obvious as the load on the wireless LAN increases, keeping the latency, jitter, and loss for selected traffic types within an acceptable range.

QoS on the wireless LAN focuses on downstream prioritization from the access point. The figure below shows the upstream and downstream traffic flow.

Figure 10: Upstream and Downstream Traffic Flow



The radio downstream flow is traffic transmitted out the access point radio to a wireless client device. This traffic is the main focus for QoS on a wireless LAN.

The radio upstream flow is traffic transmitted out the wireless client device to the access point. QoS for wireless LANs does not affect this traffic.

The Ethernet downstream flow is traffic sent from a switch or a router to the Ethernet port on the access point. If QoS is enabled on the switch or router, the switch or router might prioritize and rate-limit traffic to the access point.

The Ethernet upstream flow is traffic sent from the access point Ethernet port to a switch or router on the wired LAN. The access point does not prioritize traffic that it sends to the wired LAN based on traffic classification.

Precedence of QoS Settings

When you enable QoS, the access point queues packets based on the CoS value for each packet. If a packet matches one of the filter types based on its current precedence, the packet is classified based on the matching filter and no other filters are applied.

There are three levels of precedence for QoS filters.

- 0--Dynamically created VoIP client filter. Traffic from voice clients takes priority over other traffic regardless of other policy settings. This setting takes precedence over all other policies, second only to previously assigned packet classifications.
- 1--User configured class-map match clause (except match any). QoS policies configured for and that apply to VLANs or to the access point interfaces are third in precedence after previously classified packets and the QoS element for wireless phones setting.
- 2--User configured class-map match any clause (match VLAN). If a default classification for all packets on a VLAN is set, that policy is fourth in the precedence list.

Precedence number zero is the highest.

QoS Configuration Guidelines for Wireless LANs

An access point is essentially a Layer 2 transparent bridge between wired and wireless networks. Typically, bandwidth on the wireless side constrains the wired side. For example, 802.11b offers 6 Mbps half duplex and 100BASE-T offers 100 Mbps full duplex.

A Cisco access point uses ACLs for forwarding or blocking packets on selective basis, as designated by the user for the purpose of:

- Providing QoS for Voice-over-IP (VoIP) phones.
- Mapping IP precedence values into 802.1p/q CoS values for downlink traffic.
- Providing Layer 2 and Layer 3 ACL features to the bridging path and access point host receive path.

802.11 VoIP Phone Support

The Symbol element is advertised by the access point. This helps a Symbol phone to make an association decision if there are multiple access points serving the area. The current packet rate is the calculation of average means of number of packets transmitted per second for the past 8 seconds.

After the normal 802.11 association process, a Symbol phone sends a proprietary Symbol 802.11 phone registration message (WNMP) to the access point to complete the association.

The Symbol phone does not associate to an access point if the advertised packet rate is above the threshold of the access point. The Symbol phone uses its Symbol element as optional information. Basic operation does not require an access point to send Symbol elements.

Cisco Wireless IP Phone 7920 Support

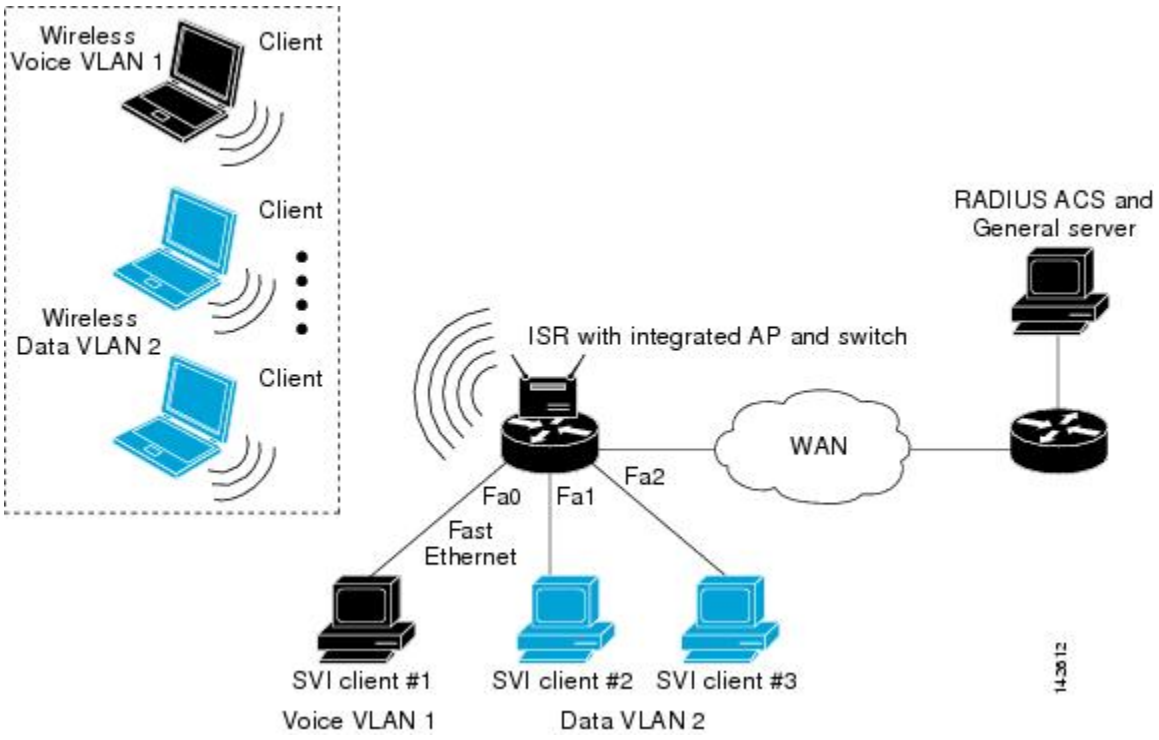
The wireless IP Phone 7920 uses Cisco Discovery Protocol (CDP) messages with Appliance VLAN-ID TLV to inform the access point of its presence. The access point intercepts the CDP messages sent from the client, and if it contains the Appliance VLAN-ID Type-Length-Value (TLV), it should flag the client as VoIP phone client.

If a VLAN is enabled, we recommend that all phone clients be associated to a single voice VLAN and that all data clients be associated to a separate data VLAN. If a VLAN is not enabled, we recommend that all the VoIP packets be classified by using the same user_priority value (6).

The access point always uses DIFS with minimum contention window (CW) value derived from the CWmax and CWmin range parameters to prioritize voice traffic.

The figure below shows the difference between traditional physical LAN segmentation and logical VLAN segmentation with wireless devices connected.

Figure 11: LAN and VLAN Segmentation with Wireless Devices



Radio Interface Transmit Queues

The access point radio maintains four priority queues, one for each traffic category, and 802.11e EDCF to provide differentiate Distributed Coordination Function (DCF) access to the wireless medium. An EDCF-aware access point is assigned distinct pairs of CWmin and CWmax parameters for each traffic category. The CWmin and CWmax parameters can be modified through the CLI.

Radio Access Categories

The access point uses the radio access categories to calculate backoff times for each packet. As a rule, high-priority packets have short backoff times.

The default values in the minimum and maximum contention window fields, and in the slot time fields, are based on settings recommended in IEEE Draft Standard 802.11e. For detailed information on these values, consult the standard.

We recommend that you use the default settings. Changing these values can lead to unexpected blockages of traffic on your wireless LAN, and the blockages might be difficult to diagnose.

Ethernet Interface Transmit Queue

Because the Ethernet interface always has a larger bandwidth than radio interface, there is no need to maintain priority queues for Ethernet interface. There will be only one transmit queue per Ethernet interface.

802.1Q Untagged Voice Packets

If a VLAN is enabled, Cisco IOS bridging code adds 802.11q tags into the untagged voice packets. The CoS value should be part of the VLAN configuration. For a voice VLAN, the CoS should be (6).

If a VLAN is not enabled, the access point relies on the DSCP-to-CoS filter configured by the user to assign CoS value to the packet.

CoS Values on a VLAN

The default CoS value for all the VLANs is zero (best effort). This ensures that the access point provides differentiate services based on VLAN IDs. Packets sent to these clients are queued into the appropriate priority queue based on their VLAN CoS value.

If a VLAN is enabled, and packets from a wireless client must be forwarded to the wired network, a 802.1q tag is added by the forwarding module.

Access Control Lists

ACLs are applied on either outbound or inbound interfaces. For standard inbound access lists, after receiving a packet, the Cisco IOS software checks the source address of the packet against the access list. If the access list permits the address, the software continues to process the packet. If the access list rejects the address, the software discards the packet and returns an Internet Control Message Protocol (ICMP) host unreachable message.

For extended access lists, the router also checks the destination access list. If the access list permits the address, the software continues to process the packet. If the access list rejects the address, the software discards the packet and returns an ICMP host unreachable message.

For standard outbound access lists, after receiving and routing a packet to a controlled interface, the software checks the source address of the packet against the access list. For extended access lists, the router also checks the destination access list. If the access list permits the address, the software sends the packet. If the access list rejects the address, the software discards the packet and returns an ICMP host unreachable message.

If the specified access list does not exist, all packets are passed.

When you enable outbound access lists, you automatically disable autonomous switching for that interface. When you enable input access lists on any CBus or CxBus interface, you automatically disable autonomous switching for all interfaces (with one exception--a Storage Services Enabler (SSE) configured with simple access lists can still switch packets, on output only).

When you apply an access list that has not yet been defined to an interface, the software will act as if the access list has not been applied to the interface and will accept all packets. Remember this behavior if you use undefined access lists as a means of security in your network.

Wi-Fi Multimedia Mode

When you enable QoS, the access point uses Wi-Fi Multimedia (WMM) mode by default. WMM provides these enhancements over basic QoS mode:

- The access point adds each packet's class of service to the packet's 802.11 header to be passed to the receiving station.
- Each access class has its own 802.11 sequence number. The sequence number allows a high-priority packet to interrupt the retries of a lower-priority packet without overflowing the duplicate checking buffer on the receiving side.
- For access classes that are configured to allow it, transmitters that are qualified to transmit through the normal backoff procedure are allowed to send a set of pending packets during the configured transmit opportunity (a specific number of microseconds). Sending a set of pending packets improves throughput because each packet does not have to wait for a backoff to gain access; instead, the packets can be transmitted immediately one after the other.

The access point uses WMM enhancements in packets sent to client devices that support WMM. The access point applies basic QoS policies to packets sent to clients that do not support WMM.

To disable WMM, use the no dot11 qos mode wmm command in interface configuration mode.

How to Implement QoS on a Wireless LAN

Implementing QoS on a Wireless LAN

Perform this task to implement QoS features on a wireless LAN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot11 phone**
4. **interface dot11Radio** *interface*
5. **ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**}
6. **bridge-group** *bridge-group* **input-address-list** *access-list-number*
7. **l2-filter bridge-group-acl**
8. **traffic-class {best-effort | background | video | voice} [cw-min min-value | cw-max max-value | fixed-slot backoff-interval]**
9. **end**
10. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dot11 phone** **Example:** `Router(config)# dot11 phone`	Enables 802.11 compliance phone support.
Step 4	**interface dot11Radio** *interface* **Example:** `Router(config)# interface dot11Radio 0`	(Optional) Enters interface configuration mode for the radio interface.
Step 5	**ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**} **Example:** `Router(config-if)# ip access-group 101 out`	(Optional) Controls access to an interface. • The example shows how to apply access list 101 on packets outbound from an interface.

	Command or Action	Purpose
Step 6	**bridge-group** *bridge-group* **input-address-list** *access-list-number* **Example:** `Router(config-if)# bridge-group 1 input-address-list 700`	(Optional) Assigns an access list to a particular interface. • This access list is used to filter packets received on that interface based on their MAC source addresses.
Step 7	**l2-filter bridge-group-acl** **Example:** `Router(config-if)# l2-filter bridge-group-acl`	(Optional) Applies a Layer 2 ACL filter to bridge group incoming and outgoing packets between the access point and the host (upper layer). • If this command is enabled, and any Layer 2 ACLs are installed in ingress or egress, the same ACLs are applied to packets received or sent by the access point host stack.
Step 8	**traffic-class {best-effort | background | video | voice} [cw-min min-value | cw-max max-value | fixed-slot backoff-interval]** **Example:** `Router(config-if)#` **traffic-class best-effort cw-min 4 cw-max 10 fixed-slot 2**	(Optional) Configures the radio interface QoS traffic class parameters for each of the four traffic types. • Backoff parameters control how the radio accesses the airwaves. The **cw-min** and **cw-max** keywords specify the collision window as a power of 2. For example, if the value is set to 3, the contention window is 0 to 7 backoff slots (2 to the power 3 minus 1). The **fixed-slot** keyword specifies the number of backoff slots that are counted before the random backoff counter starts to count down.
Step 9	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 10	**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.

Configuration Examples for Implementing QoS on a Wireless LAN

Configuring QoS on a Wireless LAN Example

The following example shows how to:

- Enable 802.11 compliance phone support.
- Configure the best effort traffic class for contention windows and fixed-slot backoff values.

Each time the backoff for best effort is started, the backoff logic waits a minimum of the 802.11 Short Inter-Frame Space (SIFS) time plus two backoff slots. It then begins counting down the 0 to 15 backoff slots in the contention window.

- Save your entries in the configuration file.

```
configure terminal
 dot11 phone
 interface dot11Radio 0/3/0
 traffic-class best-effort cw-min 4 cw-max 10 fixed-slot 2
 end
 copy running-config startup-config
```

Configuring QoS for a Voice VLAN on an Access Point in Routing Mode Example

Using LAN and VLAN Segmentation with Wireless Devices figure as a reference, this example shows how to create a VLAN for voice traffic on an access point in routing mode and apply QoS parameters to that voice VLAN:

```
configure terminal

 class-map match-any voice_vlan

 match vlan 2

 policy-map voice
 class voice_vlan
 set cos 6

 exit

 exit

 interface Dot11Radio 0/3/0
 no ip address
```

```
ssid serialvoicevlan
vlan 2
authentication open

exit

exit

interface Dot11Radio 0/3/0.2
encapsulation dot1Q 2
ip address 10.2.1.1 255.255.255.0
service-policy output voice

end

copy running-config startup-config
```

Additional References

The following sections provide references related to implementing QoS on a wireless LAN.

Related Documents

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

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified by this feature.	--

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

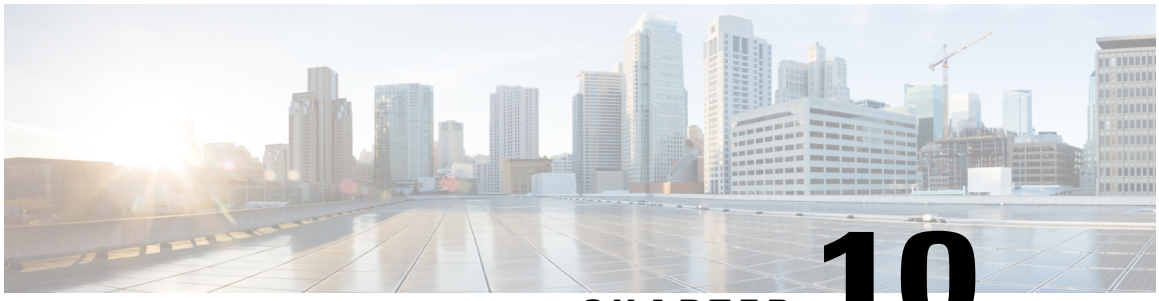
Feature Information for Implementing Quality of Service in a Wireless LAN

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 11: Feature Information for Implementing Quality of Service in a Wireless LAN

Feature Name	Releases	Feature Information
Wi-Fi Multimedia (WMM) Required Elements	12.4(15)T	WMM provides enhancements over basic QoS mode.



CHAPTER 10

Wireless LAN Error Messages

This module lists wireless LAN (WLAN) error messages for the Cisco 800, 1800, 2800, and 3800 series integrated services routers, hereafter referred to as an access point or AP.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Wireless LAN Error Messages

Association Management Messages

Error Message

```
DOT11-3-BADSTATE: [mac-address] [chars] [chars] -> [chars]
```

Explanation - 802.11 Association and management uses a table-driven state machine to track and transition an association through various states. A state transition occurs when an association receives one of many possible events. When this error occurs, it means that an association received an event that it did not expect while in this state.

Recommended Action - The system can continue but may lose the association that generates this error. Copy the message exactly as it appears and report it to your technical service representative.

Error Message

```
DOT11-6-ASSOC: Interface [interface], Station [char] [mac] Associated
```
Explanation - A station associated to an access point.

Recommended Action - None.

Error Message

```
DOT11-6-ADD: Interface [interface], Station [mac] Associated to Parent [mac]
```
Explanation - A station associated to an access point.

Recommended Action - None.

Error Message

```
DOT11-6-DISASSOC: Interface [interface], Deauthenticating Station [mac] [char]
```
Explanation - A station disassociated from an access point.

Recommended Action - None.

802.11 Subsystem Messages

Error Message

```
DOT11-6-FREQ_INUSE: Radio frequency [int] is in use
```
Explanation - When scanning for an unused frequency, the unit recognized another radio using the displayed frequency.

Recommended Action - None.

Error Message

```
DOT11-6-FREQ_USED: Radio frequency [int] selected
```
Explanation - After scanning for an unused frequency, the unit selected the displayed frequency.

Recommended Action - None.

Error Message

```
DOT11-4-NO_SSID: No SSIDs configured, radio not started
```
Explanation - All Service Set Identifiers (SSIDs) were deleted from the configuration. At least one must be configured for the radio to run.

Recommended Action - Configure at least one SSID on the access point.

Error Message

```
DOT11-2-RADIO_FAILED: Interface [interface] failed -- [chars]
```
Explanation - The radio driver found a severe error and is shutting down.

Recommended Action - None.

Error Message

```
DOT11-4-CANT_ASSOC: Cannot associate: [chars]
```

Explanation - The unit could not establish a connection to a parent access point for the displayed reason.

Recommended Action - Verify that the basic configuration settings (SSID, Wired Equivalent Privacy [WEP], and others) of the parent access point and this unit match.

Error Message

```
DOT11-4-MAXRETRIES: Packet to client [mac] reached max retries, remove the client
```

Explanation - Delivery of a packet sent to the client failed many times, and the maximum retries limit has been reached. The client is deleted from the association table.

Recommended Action - None.

Error Message

```
DOT11-AUTH_FAILED: Station [mac-address] authentication failed
```

Explanation - The station failed authentication.

Recommended Action - Verify that the user entered the correct username and password, and check that the authentication server is online.

Error Message

```
DOT11-TKIP_MIC_FAILURE: TKIP Michael MIC failure was detected on a packet (TSC=0x0) received
 from [mac-address]
```

Explanation - TKIP Michael MIC failure was detected on a unicast frame decrypted locally with the pairwise key.

Recommended Action - A failure of the Michael MIC in a packet usually indicates an active attack on your network. Search for and remove potential rogue devices from your wireless LAN.

Error Message

```
DOT11-TKIP_MIC_FAILURE_REPORT: Received TKIP Michael MIC failure report from the station
[mac-address] on the packet (TSC=0x0) encrypted and protected by [key] key
```

Explanation - The access point received an EAPOL-key from a station notifying the access point that TKIP Michael MIC failed on a packet sent by this access point.

Recommended Action - None.

Error Message

```
DOT11-TKIP_MIC_FAILURE_REPEATED: Two TKIP Michael MIC failures were detected within [number]
 seconds on [interface] interface. The interface will be put on MIC failure hold state for
 next [number] seconds
```

Explanation - Because MIC failures usually indicate an active attack on your network, the interface will be put on hold for the configured time. During this hold time, stations using TKIP ciphers are disassociated and cannot reassociate until the hold time ends. At the end of the hold time, the interface operates normally.

Recommended Action - Michael MIC failures usually indicate an active attack on your network. Search for and remove potential rogue devices from your wireless LAN. If this is a false alarm and the interface should not be on hold this long, use the **countermeasure tkip hold-time** command to adjust the hold time.

Error Message

```
Multicast received for AP sa [mac-address], da [mac-address], ra cbcb.cbcb.cbcb ta
[mac-address]
```

Explanation - The access point received a direct broadcast or multicast frame in which the dot11 MAC header's RA address field is a broadcast or multicast address.

Recommended Action - None. However, if your access point displays this message frequently, capture these frames with a sniffer for further analysis.

Local Authenticator Messages

Error Message

```
RADSRV-4-NAS_UNKNOWN: Unknown authenticator: [ip-address]
```

Explanation - The local RADIUS server received an authentication request but does not recognize the IP address of the network access server (NAS) that forwarded the request.

Recommended Action - Make sure that every access point on your wireless LAN is configured as a NAS on your local RADIUS server.

Additional References

The following sections provide references related to error and event messages.

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*

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