



Configuring WLANs

This chapter describes how to configure up to 16 wireless LANs for your Cisco Wireless LAN Solution. This chapter contains these sections:

- [Wireless LAN Overview, page 6-2](#)
- [Configuring Wireless LANs, page 6-2](#)

Wireless LAN Overview

The Cisco Wireless LAN Solution can control up to 16 wireless LANs for lightweight access points. Each wireless LAN has a separate wireless LAN ID (1 through 16), a separate wireless LAN SSID (wireless LAN name), and can be assigned unique security policies.

Lightweight access points broadcast all active Cisco Wireless LAN Solution wireless LAN SSIDs and enforce the policies that you define for each wireless LAN.



Note

Cisco recommends that you assign one set of VLANs for wireless LANs and a different set of VLANs for Management Interfaces to ensure that controllers properly route VLAN traffic.

Configuring Wireless LANs

These sections describe how to configure wireless LANs:

- [Displaying, Creating, Disabling, and Deleting Wireless LANs, page 6-2](#)
- [Activating Wireless LANs, page 6-3](#)
- [Assigning a Wireless LAN to a DHCP Server, page 6-3](#)
- [Configuring MAC Filtering for Wireless LANs, page 6-3](#)
- [Assigning Wireless LANs to VLANs, page 6-4](#)
- [Configuring Layer 2 Security, page 6-4](#)
- [Configuring Layer 3 Security, page 6-6](#)
- [Configuring Quality of Service, page 6-8](#)

Displaying, Creating, Disabling, and Deleting Wireless LANs

On the controller CLI, enter these commands to display, create, disable, and delete wireless LANs:

- Enter **show wlan summary** to display existing wireless LANs and whether they are enabled or disabled. Note that each wireless LAN is assigned a wireless LAN ID from 1 to 16.
- Enter **config wlan create *wlan-id* *wlan-name*** to create a new wireless LAN. For *wlan-id*, enter an ID from 1 to 16. For *wlan-name*, enter an SSID of up to 31 alphanumeric characters.



Note

When wireless LAN 1 is created in the Configuration Wizard, it is created in enabled mode; disable it until you have finished configuring it. When you create a new wireless LAN using the **config wlan create** command, it is created in disabled mode; leave it disabled until you have finished configuring it.

- If you need to modify an enabled wireless LAN, disable it first using the **config wlan disable *wlan-id*** command. Leave wireless LANs in disabled mode until you finish configuring them.
- Enter **config wlan enable *wlan-id*** to enable a wireless LAN.
- Enter **config wlan delete *wlan-id*** to delete a wireless LAN.

Activating Wireless LANs

After you have completely configured your wireless LAN settings, enter **config wlan enable *wlan-id*** to activate the wireless LAN.

Assigning a Wireless LAN to a DHCP Server

Each wireless LAN can be assigned to a DHCP server. Any or all wireless LANs can be assigned to the same DHCP server, and each wireless LAN can be assigned to different DHCP servers.



Note

DHCP servers must be assigned for wireless LANs that allow management through a wireless connection.

- Enter this command to assign a wireless LAN to a DHCP server:
config wlan dhcp_server *wlan-id dhcp-server-ip-address*
- Enter **show wlan** to verify that the wireless LAN is assigned to the DHCP server.

Configuring MAC Filtering for Wireless LANs

When you use MAC filtering for client or administrator authorization, you need to enable it at the wireless LAN level first. If you plan to use local MAC address filtering for any wireless LAN, use the commands in this section to configure MAC filtering for a wireless LAN.

Enabling MAC Filtering

Use these commands to enable MAC filtering on a wireless LAN:

- Enter **config wlan mac-filtering enable *wlan-id*** to enable MAC filtering.
- Enter **show wlan** to verify that you have MAC filtering enabled for the wireless LAN.

When you enable MAC filtering, only the MAC addresses that you add to the wireless LAN are allowed to join the wireless LAN. MAC addresses that have not been added are not allowed to join the wireless LAN.

Creating a Local MAC Filter

Cisco Wireless LAN Controllers have built-in MAC filtering capability, similar to that provided by a RADIUS authorization server.

Use these commands to add MAC addresses to a wireless LAN MAC filter:

- Enter **show macfilter** to view MAC addresses assigned to wireless LANs.
- Enter **config macfilter add *mac-addr wlan-id*** to assign a MAC address to a wireless LAN MAC filter.
- Enter **show macfilter** to verify that MAC addresses are assigned to the wireless LAN.

Configuring a Timeout for Disabled Clients

You can configure a timeout for disabled clients. Clients who fail to authenticate three times when attempting to associate are automatically disabled from further association attempts. After the timeout period expires, the client is allowed to retry authentication until it associates or fails authentication and is excluded again. Use these commands to configure a timeout for disabled clients:

- Enter **config wlan blacklist** *wlan-id timeout* to configure the timeout for disabled clients. Enter a timeout from **1** to **65535** seconds, or enter **0** to permanently disable the client.
- Use the **show wlan** command to verify the current timeout.

Assigning Wireless LANs to VLANs

Use these commands to assign a wireless LAN to a VLAN:

- Enter this command to assign a wireless LAN to a VLAN:

```
config wlan vlan wlan-id { default | untagged | vlan-id controller-vlan-ip-address vlan-netmask vlan-gateway }
```

 - Use the **default** option to assign the wireless LAN to the VLAN configured on the network port.
 - Use the **untagged** option to assign the wireless LAN to VLAN 0.
 - Use the *vlan-id*, *controller-vlan-ip-address*, *vlan-netmask*, and *vlan-gateway* options to assign the wireless LAN to a specific VLAN and to specify the controller VLAN IP address, the local IP netmask for the VLAN, and the local IP gateway for the VLAN.
- Enter **show wlan** to verify VLAN assignment status.



Note

Cisco recommends that you assign one set of VLANs for wireless LANs and a different set of VLANs for management interfaces to ensure that controllers properly route VLAN traffic.

- To remove a VLAN assignment from a wireless LAN, use this command:

```
config wlan vlan wlan-id untagged
```

Configuring Layer 2 Security

This section explains how to assign Layer 2 security settings to wireless LANs.

Dynamic 802.1X Keys and Authorization

Cisco Wireless LAN Controllers can control 802.1X dynamic WEP keys using EAP (extensible authentication protocol) across access points, and support 802.1X dynamic key settings for wireless LANs.

- Enter **show wlan** *wlan-id* to check the security settings of each wireless LAN. The default security setting for new wireless LANs is 802.1X with dynamic keys enabled. To maintain robust Layer 2 security, leave 802.1X configured on your wireless LANs.
- To disable or enable the 802.1X configuration, use this command:

```
config wlan security 802.1X { enable | disable } wlan-id
```

- If you want to change the 802.1X encryption level for a wireless LAN, use this command:
config wlan security 802.1X encryption *wlan-id* [40 | 104 | 128]
 - Use the 40 option to specify 40/64-bit encryption.
 - Use the 104 option to specify 104/128-bit encryption. (This is the default encryption setting.)
 - Use the 128 option to specify 128/152-bit encryption.

WEP Keys

Cisco Wireless LAN Controllers can control static WEP keys across access points. Use these commands to configure static WEP for wireless LANs:

- Enter this command to disable 802.1X encryption:
config wlan security 802.1X disable *wlan-id*
- Enter this command to configure 40/64, 104/128, or 128/152-bit WEP keys:
config wlan security static-wep-key encryption *wlan-id* {40 | 104 | 128} {hex | ascii} *key* *key-index*
 - Use the **40**, **104**, or **128** options to specify 40/64-bit, 104/128-bit, or 128/152-bit encryption. The default setting is 104/128.
 - Use the **hex** or **ascii** option to specify the character format for the WEP key.
 - Enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F) or five printable ASCII characters for 40-bit/64-bit WEP keys; enter 26 hexadecimal or 13 ASCII characters for 104-bit/128-bit keys; enter 32 hexadecimal or 16 ASCII characters for 128-bit/152-bit keys.
 - Enter a key index (sometimes called a key slot) **1** through **4**.



Note One unique WEP key index must be applied to each wireless LAN that uses static WEP. Because there are only four key indexes, only four wireless LANs can be configured for static WEP Layer 2 encryption. Also note that some legacy clients can only access key index 1 through 3 but cannot access key index 4.

Dynamic WPA Keys and Encryption

Cisco Wireless LAN Controllers can control WPA (Wi-Fi Protected Access) across access points. Enter these commands to configure WPA for a wireless LAN:

- Enter this command to disable 802.1X encryption:
config wlan security 802.1X disable *wlan-id*
- Enter these commands to configure authorization and dynamic key exchange on a wireless LAN:
 - **config wlan security wpa enable *wlan-id***
 - **config wlan security wpa encryption aes-ocb *wlan-id***
 - **config wlan security wpa encryption tkip *wlan-id***
 - **config wlan security wpa encryption wep *wlan-id* {40 | 104 | 128}**
- Enter **show wlan** to verify that you have WPA enabled.

Configuring a Wireless LAN for Both Static and Dynamic WEP

You can configure up to four wireless LANs to support static WEP keys, and you can also configure dynamic WEP on any of these static-WEP wireless LANs. Follow these guidelines when configuring a wireless LAN for both static and dynamic WEP:

- The static WEP key and the dynamic WEP key must be the same length.
- When you configure static and dynamic WEP as the Layer-2 security policy, no other security policies can be specified. For example, when you configure only dynamic WEP or only static WEP, you can also configure web authentication or IPSec. However, when you configure both static and dynamic WEP, you cannot also configure web authentication or IPSec.

Configuring Layer 3 Security

This section explains how to assign Layer 3 security settings to wireless LANs.



Note

To use Layer 3 security on a Cisco 4100 Series Wireless LAN Controller, the controller must be equipped with a VPN/Enhanced Security Module (Crypto Module). The module plugs into the back of the controller and provides the extra processing power needed for processor-intensive security algorithms.

IPSec

IPSec (Internet Protocol Security) supports many Layer 3 security protocols. Enter these commands to enable IPSec on a wireless LAN:

- **config wlan security ipsec {enable | disable} wlan-id**
- Enter **show wlan** to verify that IPSec is enabled.

IPSec Authentication

IPSec uses hmac-sha-1 authentication as the default for encrypting wireless LAN data, but can also use hmac-md5, or no authentication. Enter this command to configure the IPSec IP authentication method:

- **config wlan security ipsec authentication {hmac-md5 | hmac-sha-1 | none} wlan-id**
- Enter **show wlan** to verify that the IPSec authentication method is configured.

IPSec Encryption

IPSec uses 3DES encryption as the default for encrypting wireless LAN data, but can also use AES, DES, or no encryption. Enter this command to configure the IPSec encryption method:

- **config wlan security ipsec encryption {3des | aes | des | none} wlan-id**
- Enter **show wlan** to verify that the IPSec encryption method is configured.

IKE Authentication

IPSec IKE (Internet Key Exchange) uses pre-shared key exchanges, x.509 (RSA Signatures) certificates, and XAuth-psk for authentication. Enter these commands to enable IPSec IKE on a wireless LAN that uses IPSec:

- **config wlan security ipsec ike authentication certificates** *wlan-id*
 - Use the **certificates** option to specify RSA signatures.
- **config wlan security ipsec ike authentication xauth-psk** *wlan-id key*
 - Use the **xauth-psk** option to specify XAuth pre-shared key.
 - For key, enter a pre-shared key from 8 to 255 case-sensitive ASCII characters.
- **config wlan security ipsec ike authentication pre-shared-key** *wlan-id key*
- Enter **show wlan** to verify that IPSec IKE is enabled.

IKE Diffie-Hellman Group

IPSec IKE uses Diffie-Hellman groups to block easily-decrypted keys. Enter these commands to configure the Diffie-Hellman group on a wireless LAN with IPSec enabled:

- **config wlan security ipsec ike DH-Group** *wlan-id group-id*
 - For *group-id*, enter **group-1**, **group-2** (this is the default setting), or **group-5**.
- Enter **show wlan** to verify that IPSec IKE DH group is configured.

IKE Phase 1 Aggressive and Main Modes

IPSec IKE uses the Phase 1 Aggressive (faster) or Main (more secure) mode to set up encryption between clients and the controller. Enter these commands to specify the Phase 1 encryption mode for a wireless LAN with IPSec enabled:

- **config wlan security ipsec ike phase1** { **aggressive** | **main** } *wlan-id*
- Enter **show wlan** to verify that the Phase 1 encryption mode is configured.

IKE Lifetime Timeout

IPSec IKE uses its timeout to limit the time that an IKE key is active. Enter these commands to configure an IKE lifetime timeout:

- **config wlan security ipsec ike lifetime** *wlan-id seconds*
 - For seconds, enter a number of seconds from 1800 to 345600 seconds. The default timeout is 28800 seconds.
- Enter **show wlan** to verify that the key timeout is configured.

IPSec Passthrough

IPSec IKE uses IPSec Passthrough to allow IPSec-capable clients to communicate directly with other IPSec equipment. IPSec Passthrough is also known as VPN Passthrough. Enter this command to enable IPSec Passthrough for a wireless LAN:

- `config wlan security passthru {enable | disable} wlan-id gateway`
 - For *gateway*, enter the IP address of the IPSec (VPN) passthrough gateway.
- Enter **show wlan** to verify that the passthrough is enabled.

Web-Based Authentication

Wireless LANs can use web authentication if IPSec is not enabled on the controller. Web Authentication is simple to set up and use, and can be used with SSL to improve the overall security of the wireless LAN. Enter these commands to enable web authentication for a wireless LAN:

- `config wlan security web {enable | disable} wlan-id`
- Enter **show wlan** to verify that web authentication is enabled.

Local Netuser

Cisco Wireless LAN Controllers have built-in network client authentication capability, similar to that provided by a RADIUS authentication server. Enter these commands to create a list of usernames and passwords allowed access to the wireless LAN:

- Enter **show netuser** to display client names assigned to wireless LANs.
- Enter `config netuser add username password wlan-id` to add a user to a wireless LAN.
- Enter `config netuser wlan-id username wlan-id` to add a user to a wireless LAN without specifying a password for the user.
- Enter `config netuser password username password` to create or change a password for a particular user.
- Enter `config netuser delete username` to delete a user from the wireless LAN.

Configuring Quality of Service

Cisco WLAN Solution wireless LANs support four levels of QoS: Platinum/Voice, Gold/Video, Silver/Best Effort (default), and Bronze/Background. You can configure the voice traffic wireless LAN to use Platinum QoS, assign the low-bandwidth wireless LAN to use Bronze QoS, and assign all other traffic between the remaining QoS levels. Enter these commands to assign a QoS level to a wireless LAN:

- `config wlan qos wlan-id {bronze | silver | gold | platinum}`
- Enter **show wlan** to verify that you have QoS properly set for each wireless LAN.

The wireless LAN QoS level (platinum, gold, silver, or bronze) defines a specific 802.11e user priority (UP) for over-the-air traffic. This UP is used to derive the over-the-wire priorities for non-WMM traffic, and it also acts as the ceiling when managing WMM traffic with various levels of priorities. The access point uses this QoS-profile-specific UP in accordance with the values in [Table 6-1](#) to derive the IP DSCP value that is visible on the wired LAN.

Table 6-1 Access Point QoS Translation Values

AVVID 802.1p UP-Based Traffic Type	AVVID IP DSCP	AVVID 802.1p UP	IEEE 802.11e UP
Network control	–	7	–
Inter-network control (LWAPP control, 802.11 management)	48	6	7
Voice	46 (EF)	5	6
Video	34 (AF41)	4	5
Voice control	26 (AF31)	3	4
Background (Gold)	18 (AF21)	2	2
Background (Gold)	20 (AF22)	2	2
Background (Gold)	22 (AF23)	2	2
Background (Silver)	10 (AF11)	1	1
Background (Silver)	12 (AF12)	1	1
Background (Silver)	14 (AF13)	1	1
Best Effort	0 (BE)	0	0, 3
Background	2	0	1
Background	4	0	1
Background	6	0	1

Configuring QoS Enhanced BSS (QBSS)

You can enable QBSS in these two modes:

- Wireless Multimedia (WMM) mode, which supports devices that meet the 802.11E QBSS standard
- 7920 support mode, which supports Cisco 7920 IP telephones on your 802.11b/g network

QBSS is disabled by default.

Enabling WMM Mode

Enter this command to enable WMM mode:

```
config wlan wmm {disabled | allowed | required} wlan-id
```

- The **allowed** option allows client devices to use WMM on the wireless LAN.
- The **required** option requires client devices to use WMM; devices that do not support WMM cannot join the wireless LAN.



Note Do not enable WMM mode if Cisco 7920 phones are used on your network.

Enabling 7920 Support Mode

The 7920 support mode contains two options:

- Support for 7920 phones that require call admission control (CAC) to be configured on and advertised by the client device (these are typically older 7920 phones)
- Support for 7920 phones that require CAC to be configured on and advertised by the access point (these are typically newer 7920 phones)



Note When access-point-controlled CAC is enabled, the access point sends out a Cisco proprietary CAC Information Element (IE) and does not send out the standard QBSS IE.

Enter this command to enable 7920 support mode for phones that require client-controlled CAC:

```
config wlan 7920-support client-cac-limit {enabled | disabled} wlan-id
```



Note You cannot enable both WMM mode and client-controlled CAC mode on the same wireless LAN.

Enter this command to enable 7920 support mode for phones that require access-point-controlled CAC:

```
config wlan 7920-support ap-cac-limit {enabled | disabled} wlan-id
```

QBSS Information Elements Sometimes Degrade 7920 Phone Performance

If your wireless LAN contains both 1000 series access points and Cisco 7920 wireless phones, do not enable the WMM or AP-CAC-LIMIT QBSS information elements. Do not enter either of these commands:

```
config wlan 7920-support ap-cac-limit enable wlan-id
```

```
config wlan wmm [allow | require] wlan-id
```

The information sent by 1000 series access points in the WMM and AP-CAC-LIMIT QBSS information elements is inaccurate and could result in degradation of voice quality 7920 wireless phones. This issue does not affect the CLIENT-CAC-LIMIT QBSS IE, which you enable using this command:

```
config wlan 7920-support client-cac-limit enable wlan-id
```

The CLIENT-CAC-LIMIT QBSS IE is the only QBSS IE that should be used in networks containing both 1000 series access points and 7920 wireless phones.