Configuring WLANs

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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

Prerequisites for WLANs

- You can associate up to 16 WLANs with each access point group and assign specific access points to each group. Each access point advertises only the enabled WLANs that belong to its access point group. The access point (AP) does not advertise disabled WLANs in its access point group or WLANs that belong to another group.

- We recommend that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that switches properly route VLAN traffic.
- The switch uses different attributes to differentiate between WLANs with the same Service Set Identifier (SSID).
  - WLANs with the same SSID and same Layer 2 policy cannot be created if the WLAN ID is lower than 17.
  - Two WLANs with IDs that are greater than 17 and that have the same SSID and same Layer 2 policy is allowed if WLANs are added in different AP groups.

Note This requirement ensures that clients never detect the SSID present on the same access point radio.

Related Topics

Creating WLANs (CLI), on page 7
Creating WLANs (GUI), on page 8
Configuring General WLAN Properties (CLI), on page 12
Configuring General WLAN Properties (GUI), on page 15
Deleting WLANs (CLI), on page 9
Configuring Advanced WLAN Properties (CLI), on page 16
Configuring Advanced WLAN Properties (GUI), on page 19
Band Selection, on page 4
Off-Channel Scanning Defer
DTIM Period
Session Timeout
Cisco Client Extensions, on page 5
Peer-to-Peer Blocking, on page 6
Diagnostic Channel
Client Count Per WLAN
Enabling WLANs (CLI), on page 11
Disabling WLANs (CLI), on page 12

Restrictions for WLANs

- Peer-to-peer blocking does not apply to multicast traffic.
- You can configure a maximum of up to 1000 clients.
- The WLAN name and SSID can have up to 32 characters. Spaces are not allowed in the WLAN profile name and SSID.
- You cannot map a WLAN to VLAN0, and you cannot map VLANs 1002 to 1006.

- Dual stack clients with a static-IPv4 address is not supported.
- When creating a WLAN with the same SSID, you must create a unique profile name for each WLAN.
- When multiple WLANs with the same SSID get assigned to the same AP radio, you must have a unique Layer 2 security policy so that clients can safely select between them.

Caution Some clients might not be able to connect to WLANs properly if they detect the same SSID with multiple security policies. Use this feature with care.

Related Topics

Creating WLANs (CLI), on page 7
Creating WLANs (GUI), on page 8
Configuring General WLAN Properties (CLI), on page 12
Configuring General WLAN Properties (GUI), on page 15
Deleting WLANs (CLI), on page 9
Configuring Advanced WLAN Properties (CLI), on page 16
Configuring Advanced WLAN Properties (GUI), on page 19
Band Selection, on page 4
Off-Channel Scanning Defer
DTIM Period
Session Timeout
Cisco Client Extensions, on page 5
Peer-to-Peer Blocking, on page 6
Diagnostic Channel
Client Count Per WLAN
Enabling WLANs (CLI), on page 11
Disabling WLANs (CLI), on page 12

Information About WLANs

This feature enables you to control up to 64 WLANs for lightweight access points. Each WLAN has a separate WLAN ID, a separate profile name, and a WLAN SSID. All switches publish up to 16 WLANs to each connected access point, but you can create up to the maximum number of WLANs supported and then selectively publish these WLANs (using access point groups) to different access points to better manage your wireless network.

You can configure WLANs with different SSIDs or with the same SSID. An SSID identifies the specific wireless network that you want the switch to access.

Band Selection

Band selection enables client radios that are capable of dual-band (2.4- and 5-GHz) operation to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of three nonoverlapping channels. To prevent these sources of interference and improve overall network performance, you can configure band selection on the switch.

Band selection works by regulating probe responses to clients. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels.

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 16

Configuring Advanced WLAN Properties (GUI), on page 19

Prerequisites for WLANs, on page 1

Restrictions for WLANs, on page 2

Off-Channel Scanning Defer

In deployments with certain power-save clients, you sometimes need to defer the Radio Resource Management's (RRM) normal off-channel scanning to avoid missing critical information from low-volume clients (for example, medical devices that use power-save mode and periodically send telemetry information). This feature improves the way that Quality of Service (QoS) interacts with the RRM scan defer feature.

You can use a client's Wi-Fi Multimedia (WMM) UP marking to configure the access point to defer off-channel scanning for a configurable period of time if it receives a packet marked UP.

Off-Channel Scanning Defer is essential to the operation of RRM, which gathers information about alternate channel choices such as noise and interference. Additionally, Off-Channel Scanning Defer is responsible for rogue detection. Devices that need to defer Off-Channel Scanning Defer should use the same WLAN as often as possible. If there are many of these devices (and the possibility exists that Off-Channel Defer scanning could be completely disabled by the use of this feature), you should implement an alternative to local AP Off-Channel Scanning Defer, such as monitoring access points, or other access points in the same location that do not have this WLAN assigned.

You can assign a QoS policy (bronze, silver, gold, and platinum) to a WLAN to affect how packets are marked on the downlink connection from the access point regardless of how they were received on the uplink from the client. UP=1,2 is the lowest priority, and UP=0,3 is the next higher priority. The marking results of each QoS policy are as follows:

- Bronze marks all downlink traffic to UP= 1.
- Silver marks all downlink traffic to UP= 0.
- Gold marks all downlink traffic to UP=4.
- Platinum marks all downlink traffic to UP=6.

DTIM Period

In the 802.11 networks, lightweight access points broadcast a beacon at regular intervals, which coincides with the Delivery Traffic Indication Map (DTIM). After the access point broadcasts the beacon, it transmits any buffered broadcast and multicast frames based on the value set for the DTIM period. This feature allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.

Typically, the DTIM value is set to 1 (to transmit broadcast and multicast frames after every beacon) or 2 (to transmit after every other beacon). For instance, if the beacon period of the 802.11 network is 100 ms and the DTIM value is set to 1, the access point transmits buffered broadcast and multicast frames 10 times per second. If the beacon period is 100 ms and the DTIM value is set to 2, the access point transmits buffered broadcast and multicast frames 5 times per second. Either of these settings are suitable for applications, including Voice Over IP (VoIP), that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (to transmit broadcast and multicast frames after every 255th beacon) if all 802.11 clients have power save enabled. Because the clients have to listen only when the DTIM period is reached, they can be set to listen for broadcasts and multicasts less frequently which results in a longer battery life. For example, if the beacon period is 100 ms and you set the DTIM value to 100, the access point transmits buffered broadcast and multicast frames once every 10 seconds. This rate allows the power-saving clients to sleep longer before they have to wake up and listen for broadcasts and multicasts, which results in a longer battery life.

Note A beacon period, which is specified in milliseconds on the switch, is converted internally by the software to 802.11 Time Units (TUs), where 1 TU = 1.024 milliseconds. On Cisco's 802.11n access points, this value is rounded to the nearest multiple of 17 TUs. For example, a configured beacon period of 100 ms results in an actual beacon period of 104 ms.

Many applications cannot tolerate a long time between broadcast and multicast messages, which results in poor protocol and application performance. We recommend that you set a low DTIM value for 802.11 networks that support such clients.

Session Timeouts

You can configure a WLAN with a session timeout. The session timeout is the maximum time for a client session to remain active before requiring reauthorization.

Cisco Client Extensions

The Cisco Client Extensions (CCX) software is licensed to manufacturers and vendors of third-party client devices. The CCX code resident on these clients enables them to communicate wirelessly with Cisco access points and to support Cisco features that other client devices do not, including those features that are related to increased security, enhanced performance, fast roaming, and power management.

- The software supports CCX versions 1 through 5, which enables switches and their access points to communicate wirelessly with third-party client devices that support CCX. CCX support is enabled automatically for every WLAN on the switch and cannot be disabled. However, you can configure Aironet information elements (IEs).

- If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the switch sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the controller and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 16
Configuring Advanced WLAN Properties (GUI), on page 19
Prerequisites for WLANs, on page 1
Restrictions for WLANs, on page 2

Peer-to-Peer Blocking

Peer-to-peer blocking is applied to individual WLANs, and each client inherits the peer-to-peer blocking setting of the WLAN to which it is associated. Peer-to-Peer enables you to have more control over how traffic is directed. For example, you can choose to have traffic bridged locally within the switch, dropped by the switch, or forwarded to the upstream VLAN.

Peer-to-peer blocking is supported for clients that are associated with the local switching WLAN.

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 16
Configuring Advanced WLAN Properties (GUI), on page 19
Prerequisites for WLANs, on page 1
Restrictions for WLANs, on page 2

Diagnostic Channel

You can choose a diagnostic channel to troubleshoot why the client is having communication problems with a WLAN. You can test the client and access points to identify the difficulties that the client is experiencing and allow corrective measures to be taken to make the client operational on the network. You can use the switch GUI or CLI to enable the diagnostic channel, and you can use the switch CLI to run the diagnostic tests.

Note We recommend that you enable the diagnostic channel feature only for nonanchored SSIDs that use the management interface.

Per-WLAN Radius Source Support

By default, the switch sources all RADIUS traffic from the IP address on its management interface, which means that even if a WLAN has specific RADIUS servers configured instead of the global list, the identity used is the management interface IP address.

If you want to filter WLANs, you can use the callStationID that is set by RFC 3580 to be in the APMAC:SSID format. You can also extend the filtering on the authentication server to be on a per-WLAN source interface by using the NAS-IP-Address attribute.

When you enable the per-WLAN RADIUS source support, the switch sources all RADIUS traffic for a particular WLAN by using the dynamic interface that is configured. Also, RADIUS attributes are modified accordingly to match the identity. This feature virtualizes the switch on the per-WLAN RADIUS traffic, where each WLAN can have a separate layer 3 identity. This feature is useful in deployments that integrate with ACS Network Access Restrictions and Network Access Profiles.

You can combine per-WLAN RADIUS source support with the normal RADIUS traffic source and some WLANs that use the management interface and others using the per-WLAN dynamic interface as the address source.

How to Configure WLANs

Creating WLANs (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name wlan-id* [*ssid*]
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id* [*ssid*] **Example:** `Switch(config)# wlan mywlan 34 mywlan-ssid`	Specifies the WLAN name and ID: • For the *profile-name*, enter the profile name. The range is from 1 to 32 alphanumeric characters. • For the *wlan-id*, enter the WLAN ID. The range is from 1 to 512. • For the *ssid*, enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID. **Note** By default, the WLAN is disabled.

	Command or Action	Purpose
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for WLANs, on page 1
Restrictions for WLANs, on page 2

Creating WLANs (GUI)

Step 1 Click **Configuration** > **Wireless**.
The **WLANs** page is displayed.

Step 2 Click **New** to create a WLAN.
The **WLANs** > **Create New** page is displayed.

Step 3 Enter the following parameters:

Parameter	Description
WLAN ID	WLAN identifier. The value ranges from 1 to 512.
SSID	Broadcast name of the WLAN.
Profile	WLAN profile name.

Step 4 Click **Apply**.

Related Topics

Prerequisites for WLANs, on page 1
Restrictions for WLANs, on page 2

Deleting WLANs (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **no wlan** *wlan-name wlan-id ssid*
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**no wlan** *wlan-name wlan-id ssid* **Example:** `Switch(config)# no wlan test2`	Deletes the WLAN. The arguments are as follows: • The *wlan-name* is the WLAN profile name. • The *wlan-id* is the WLAN ID. • The *ssid* is the WLAN SSID name configured for the WLAN. **Note** If you delete a WLAN that is part of an AP group, the WLAN is removed from the AP group and from the AP's radio.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for WLANs, on page 1
Restrictions for WLANs, on page 2

Deleting WLANs (GUI)

Step 1 Click **Configuration** > **Wireless**.
The **WLANs** page is displayed.

Step 2 Select the checkbox corresponding to the WLAN you want to delete.
Note If you delete a WLAN that is part of an AP group, the WLAN is removed from the AP group and from the AP's radio.

Step 3 Click **Remove**.

Searching WLANs (CLI)

SUMMARY STEPS

1. **show wlan summary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show wlan summary** **Example:** `Switch# show wlan summary`	Displays the list of all WLANs configured on the device. You can search for the WLAN in the output.

```
Switch# show wlan summary
Number of WLANs: 4

WLAN Profile Name                     SSID                           VLAN Status
-------------------------------------------------------------------------------
1    test1                             test1-ssid                     137  UP
3    test2                             test2-ssid                     136  UP
2    test3                             test3-ssid                     1    UP
45   test4                             test4-ssid                     1    DOWN
```

You can also use wild cards to search WLANs. For example **show wlan summary include** | *variable*. Where variable is any search string in the output.

```
Switch# show wlan summary | include test-wlan-ssid
1    test-wlan                        test-wlan-ssid                   137   UP
```

Searching WLANs (GUI)

Step 1 Click **Configuration** > **Wireless**.
The **WLANs** page is displayed.

Step 2 Type the first few characters in the text box above the column you are searching. Fo For example, to search the WLAN based on the **Profile**, type the first few characters of the profile name.
You can search a WLAN based on the following criteria:

- **Profile**
- **ID**
- **SSID**

- **VLAN**
- **Status**

If a WLAN exists, it would appear based on the accuracy of the match.

Enabling WLANs (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **no shutdown**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Enables the WLAN.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for WLANs, on page 1
Restrictions for WLANs, on page 2

Disabling WLANs (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **shutdown**
4. **end**
5. **show wlan summary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**shutdown** **Example:** `Switch(config-wlan)# shutdown`	Disables the WLAN.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 5	**show wlan summary** **Example:** `Switch# show wlan summary`	Displays the list of all WLANs configured on the device. You can search for the WLAN in the output.

Related Topics

Prerequisites for WLANs, on page 1
Restrictions for WLANs, on page 2

Configuring General WLAN Properties (CLI)

You can configure the following properties:

- Media stream
- Broadcast SSID
- Call Snooping
- Radio
- Interface
- Status

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **shutdown**
4. **broadcast-ssid**
5. **radio** {**all** | **dot11a** | **dot11ag** | **dot11bg** | **dot11g**}
6. **client vlan** *vlan-identifier*
7. **ip multicast vlan** *vlan-name*
8. **media-stream multicast-direct**
9. **call-snoop**
10. **no shutdown**
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**shutdown** **Example:** `Switch# shutdown`	Disables the WLAN before configuring the parameters.
Step 4	**broadcast-ssid** **Example:** `Switch(config-wlan)# broadcast-ssid`	Broadcasts the SSID for this WLAN. This field is enabled by default.

	Command or Action	Purpose
Step 5	**radio** {**all** | **dot11a** | **dot11ag** | **dot11bg** | **dot11g**} **Example:** `Switch# radio all`	Enables radios on the WLAN. The keywords are as follows: • **all**—Configures the WLAN on all radio bands. • **dot1a**—Configures the WLAN on only 802.11a radio bands. • **dot11g**—Configures the WLAN on 802.11ag radio bands. • **dot11bg**—Configures the WLAN on only 802.11b/g radio bands (only 802.11b if 802.11g is disabled). • **dot11ag**— Configures the wireless LAN on 802.11g radio bands only.
Step 6	**client vlan** *vlan-identifier* **Example:** `Switch# client vlan test-vlan`	Enables an interface group on the WLAN. *vlan-identifier*—Specifies the VLAN identifier. This can be the VLAN name, VLAN ID, or VLAN group name.
Step 7	**ip multicast vlan** *vlan-name* **Example:** `Switch(config-wlan)# ip multicast vlan test`	Enables IP multicast on a WLAN. The keywords are as follows: • **vlan**—Specifies the VLAN ID. • *vlan-name*—Specifies the VLAN name.
Step 8	**media-stream multicast-direct** **Example:** `Switch(config-wlan)# media-stream multicast-direct`	Enables multicast VLANs on this WLAN.
Step 9	**call-snoop** **Example:** `Switch(config-wlan)# call-snoop`	Enables call-snooping support.
Step 10	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Enables the WLAN.
Step 11	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for WLANs, on page 1
Restrictions for WLANs, on page 2

Configuring General WLAN Properties (GUI)

Use this procedure to perform the following actions on a WLAN:

- Set WLAN Status
- Configure Radio Policies
- Assign Interface/Interface Groups
- Enable or Disable Multicast VLAN Feature
- Enable or Disable Broadcast SSID Feature

Before You Begin

Step 1 Click **Configuration** > **Wireless**.
The **WLANs** page is displayed.

Step 2 Locate the WLAN you want to configure by using the search mechanisms on the page.

Step 3 Click on the **WLAN Profile** of the WLAN.
The **WLAN** > **Edit** page is displayed.

Step 4 Click the **General** tab. This tab is displayed by default.

Step 5 Configure the **General** parameters.

Parameter	Description
Profile Name	Displays the configured profile name of the WLAN.
Type	Displays the configured LAN type.
SSID	Displays the configured SSID of the WLAN.
Status	Check box to enable the WLAN. The default value is enabled.
Security Policies	WLAN security policies set using the Security tab.
Radio Policy	WLAN radio policy to enable radios on the WLAN. Values are the following: • All • 802.11a only • 802.11g only • 802.11a/g only • 802.11b/g only

Parameter	Description
Interface/Interface Group	Interface or interface group that you want this WLAN to be mapped. Displays the non-service port and non-virtual interface names configured on the **Interfaces** page. **Note** This field displays a drop down box only when the VLAN for a WLAN is mapped using a existing VLAN name on the switch.
Broadcast SSID	Check box to broadcast this SSID. The default is enabled.
Multicast VLAN Feature	Check box to enable the multicast VLAN. The default is disabled. **Note** The Multicast Interface field appears only after you enable the Multicast VLAN feature text box. **Note** You have to configure the multicast VLAN feature only once if you want to use the multicast feature.

Step 6 Click **Apply**.

What to Do Next

Proceed to configure the Security, QoS, and Advanced Properties.

Related Topics

Prerequisites for WLANs, on page 1
Restrictions for WLANs, on page 2

Configuring Advanced WLAN Properties (CLI)

You can configure the following advanced properties:

- AAA Override
- Coverage Hole Detection
- Session Timeout
- Cisco Client Extensions
- Diagnostic Channels
- Interface Override ACLs
- P2P Blocking
- Client Exclusion
- Maximum Clients Per WLAN
- Off Channel Scan Defer

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **aaa-override**
4. **chd**
5. **session-timeout** *time-in-seconds*
6. **ccx aironet-iesupport**
7. **diag-channel**
8. **ip access-group** [web] *acl-name*
9. **peer-blocking** [**drop** | **forward-upstream**]
10. **exclusionlist** *time-in-seconds*
11. **client association limit** *max-number-of-clients*
12. **channel-scan defer-priority** {**defer-priority** {**0-7**} | **defer-time** {**0 - 6000**}}
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**aaa-override** **Example:** `Switch(config-wlan)# aaa-override`	Enables AAA override.
Step 4	**chd** **Example:** `Switch(config-wlan)# chd`	Enables coverage hole detection for this WLAN. This field is enabled by default.
Step 5	**session-timeout** *time-in-seconds* **Example:** `Switch(config-wlan)# session-timeout 450`	Sets the session timeout in seconds. The range and default values vary according to the security configuration. If the WLAN security is configured to dot1x, the range is 300 to 86400 seconds and the default value is 1800 seconds. For all other WLAN security configurations, the range is 1 to 65535 seconds and the default value is 0 seconds. A value of 0 indicates no session timeout.

	Command or Action	Purpose
Step 6	**ccx aironet-iesupport** **Example:** `Switch(config-wlan)# ccx aironet-iesupport`	Enables support for Aironet IEs for this WLAN. This field is enabled by default.
Step 7	**diag-channel** **Example:** `Switch(config-wlan)# diag-channel`	Enables diagnostic channel support to troubleshoot client communication issues on a WLAN.
Step 8	**ip access-group** [web] *acl-name* **Example:** `Switch(config)# ip access-group test-acl-name`	Configures the WLAN ACL group. The variable *acl-name* specifies the user-defined IPv4 ACL name. The keyword **web** specifies the IPv4 web ACL.
Step 9	**peer-blocking** [**drop** | **forward-upstream**] **Example:** `Switch(config)# peer-blocking drop`	Configures peer to peer blocking parameters. The keywords are as follows: • **drop—**Enables peer-to-peer blocking on the drop action. • **forward-upstream—**Enables peer-to-peer blocking on the forward upstream action.
Step 10	**exclusionlist** *time-in-seconds* **Example:** `Switch(config)# exclusionlist 10`	Specifies the timeout in seconds. The valid range is from 0 to 2147483647. Enter 0 for no timeout. A zero (0) timeout indicates that the client is permanently added to the exclusion list.
Step 11	**client association limit** *max-number-of-clients* **Example:** `Switch(config)# client association limit 200`	Sets the maximum number of clients that can be configured on a WLAN.
Step 12	**channel-scan defer-priority** {**defer-priority** {**0-7**} | **defer-time** {**0 - 6000**}} **Example:** `Switch(config)# channel-scan defer-priority 6`	Sets the channel scan defer priority and defer time. The arguments are as follows: • **defer-priority—**Specifies the priority markings for packets that can defer off-channel scanning. The range is from 0 to 7. The default is 3. • **defer-time—**Deferral time in milliseconds. The range is from 0 to 6000. The default is 100.
Step 13	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Band Selection, on page 4
Off-Channel Scanning Defer
DTIM Period
Session Timeout
Cisco Client Extensions, on page 5
Peer-to-Peer Blocking, on page 6
Diagnostic Channel
Client Count Per WLAN
Prerequisites for WLANs, on page 1
Restrictions for WLANs, on page 2
Information About AAA Override
Prerequisites for Layer 2 Security

Configuring Advanced WLAN Properties (GUI)

Before You Begin

Step 1 Click **Configuration** > **Wireless**.
The **WLANs** page is displayed.

Step 2 Locate the WLAN you want to configure by using the search mechanisms on the page.

Step 3 Click on the **WLAN Profile** of the WLAN.
The **WLAN** > **Edit** page is displayed.

Step 4 Click on the **Advanced Properties** tab.

Step 5 Configure the **Advanced** properties.

Parameter	Description
Allow AAA Override	AAA override for global WLAN parameters that you can enable or disable. When AAA Override is enabled, and a client has conflicting AAA and switches WLAN authentication parameters, client authentication is performed by the AAA server. As part of this authentication, the operating system moves clients from the default Cisco WLAN Solution WLAN VLAN to a VLAN returned by the AAA server and predefined in the switches interface configuration. In all cases, the operating system also uses QoS, DSCP, 802.1p priority tag values, and ACLs provided by the AAA server, if they are predefined in the switches interface configuration. (This VLAN switching by AAA Override is also referred to as Identity Networking.) If the Corporate WLAN primarily uses a Management Interface assigned to VLAN 2, and if AAA Override returns a redirect to VLAN 100, the operating system redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned. When AAA Override is disabled, all client authentication defaults to the switches authentication parameter settings, and authentication is performed only by the AAA server if the switches WLAN does not contain any client-specific authentication parameters. The AAA override values might come from a RADIUS server, for example.
Coverage Hole Detection	Coverage hole detection (CHD) on this WLAN that you can enable or disable. By default, CHD is enabled on all WLANs on the switches. You can disable CHD on a WLAN. When you disable CHD on a WLAN, a coverage hole alert is still sent to the Switch, but no other processing is done to mitigate the coverage hole. This feature is useful for guest WLANs where guests are connected to your network for short periods of time and are likely to be highly mobile.
Session Timeout	Configure a WLAN with a session timeout in seconds. The session timeout is the maximum time for a client session to remain active before requiring reauthorization. Entering zero denotes the session will never expire.
Aironet IE	Support of Aironet IEs per WLAN that you can enable or disable. The default is disabled.
Diagnostic Channel	Diagnostic channel support on the WLAN that you can enable or disable. The default is disabled.
P2P Blocking Action	Peer-to-peer blocking settings that you can choose from the following: • Disabled—(Default) Disables peer-to-peer blocking and bridges traffic locally within the switch whenever possible. • Drop—Causes the switches to discard the packets. • Forward-UpStream—Causes the packets to be forwarded on the upstream VLAN. The device above the switches decides what action to take regarding the packets.

Parameter	Description
Client Exclusion	Timeout in seconds for disabled client machines that you can enable or disable. Client machines are disabled by their MAC address and their status can be observed on the Clients > Details page. A timeout setting of 0 indicates that the client is disabled permanently. Administrative control is required to reenable the client. The default is enabled and the timeout setting is configured as 60 seconds.
Timeout Value (secs)	
Max Allowed Client	Maximum clients allowed per Switch. You can set a limit to the number of clients that can connect to a WLAN. This feature is useful in scenarios where you have a limited number of clients that can connect to a Switch. You can set a limit on the number of guest clients that can access a given WLAN. The number of clients that you can configure per WLAN depends on the platform that you are using. A maximum of up to 12000 clients are supported. **Note** The maximum number of clients per WLAN feature is supported only for access points that are in connected mode.
DHCP	
DHCP Server IP Address	Enter the DHCP server on the WLAN that overrides the DHCP server address on the interface assigned to the WLAN.
DHCP Address Assignment Required	Enables the DHCP address assignment and makes it mandatory for clients to get their IP address from the DHCP server.
DHCP Option 82	Enables the DHCP82 payload on the WLAN.
DHCP option 82 Format	Specifies the DHCP option 82 format. Valus are as follows: • add-ssid— Set RemoteID format that is the AP radio MAC address and SSID. • ap-ethmac—Set RemoteID format that is the AP Ethernet MAC address. **Note** If the format option is not configured, only the AP radio MAC address is used.
DHCP Option ASCII Mode	Configures ASCII for DHCP Option 82. If this is not configured, the option 82 format is set to ASCII format.
DHCP Option 82 RID Mode	Adds the Cisco 2 byte RID for DHCP option 82.
NAC	
NAC State	Enables the NAC on the WLAN.
Off Channel Scanning Defer	

Parameter	Description
Scan Differ Priority	Defer priority for the channel scan that you can assign by clicking on the priority argument. The valid range for the priority is 0 to 7. The priority is 0 to 7 (this value should be set to 6 on the client and on the WLAN). Multiple values can be set. The default values are 4, 5 and 6.
Scan Differ Time	Channel scan defer time in milliseconds that you can assign. The valid range is 100 (default) to 60000 (60 seconds). This setting should match the requirements of the equipment on your wireless LAN.
Override Interface ACL	
IPv4 ACL	The WLANs IPv4 ACL group. Values are as follow: • Un-configured • Pre-auth_ipv4_acl
IPv6 ACL	The WLANs IPv6 ACL group. Values are as follow: • Un-configured • Pre-auth_ipv6_acl

Step 6 Click **Apply**.

Related Topics

Band Selection, on page 4
Off-Channel Scanning Defer
DTIM Period
Session Timeout
Cisco Client Extensions, on page 5
Peer-to-Peer Blocking, on page 6
Diagnostic Channel
Client Count Per WLAN
Prerequisites for WLANs, on page 1
Restrictions for WLANs, on page 2
Information About the Dynamic Host Configuration Protocol
Internal DHCP Servers
External DHCP Servers
DHCP Assignments
Information About DHCP Option 82

Applying a QoS Policy on a WLAN (GUI)

Step 1 Choose **Configuration** > **Wireless**.

Step 2 Expand the **WLAN** node by clicking on the left pane and choose **WLANs**.
The **WLANs** page is displayed.

Step 3 Select the WLAN for which you want to configure the QoS policies by clicking on the WLAN **Profile**.

Step 4 Click the QoS tab to configure the QoS policies on the WLAN.
The following options are available:

Parameter	Description
QoS SSID Policy	
Downstream QoS Policy	QoS downstream policy configuration. The **Existing Policy** column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the **Assign Policy** column.
Upstream QoS Policy	QoS upstream policy configuration. The **Existing Policy** column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the **Assign Policy** column.
QoS Client Policy	
Downstream QoS Policy	QoS downstream policy configuration. The **Existing Policy** column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the **Assign Policy** column.
Upstream QoS Policy	QoS upstream policy configuration. The **Existing Policy** column displays the current applied policy. To change the existing policy, select the policy from the drop-down list in the **Assign Policy** column.
WMM	
WMM Policy	WMM Policy. Values are the following: • Disabled—Disables this WMM policy. • Allowed—Allows the clients to communicate with the WLAN. • Required—Ensures that it is mandatory for the clients to have WMM features enabled on them to communicate with the WLAN.

Step 5 Click **Apply**.

Monitoring WLAN Properties (CLI)

Command	Description
show wlan id *wlan-id*	Displays WLAN properties based on the WLAN ID.
show wlan name *wlan-name*	Displays WLAN properties based on the WLAN name.
show wlan all	Displays WLAN properties of all configured WLANs.
show wlan summary	Displays a summary of all WLANs. The summary details includes the following information: • WLAN ID • Profile name • SSID • VLAN • Status
show running-config wlan *wlan-name*	Displays the running configuration of a WLAN based on the WLAN name.
show running-config *wlan*	Displays the running configuration of all WLANs.

Viewing WLAN Properties (GUI)

Before You Begin

- You must have administrator privileges.

Step 1 Select **Configuration** > **WLAN**
The WLANs page is displayed.

Step 2 Click the **WLAN Profile** link.

The **WLANs** > **Edit** page is displayed. The WLANs page contains the following tabs:

- General : Displays the WLAN general properties.
- Security: Displays the security properties. The properties include Layer 2, Layer 3, and AAA properties.
- QoS: Displays the QoS configuration properties.
- Advanced: Displays the advanced properties.

Where to Go Next

Proceed to configure DHCP for WLANs.

Additional References

Related Documents

Related Topic	Document Title
WLAN command reference	*WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*
Mobility Anchor configuration	*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*
WebAuth Configuration	*Security Configuration Guide (Catalyst 3650 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All supported MIBs for this release.	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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for WLANs

This table lists the features in this module and provides links to specific configuration information:

Feature	Release	Modification
WLAN Functionality	Cisco IOS XE 3.3SE	This feature was introduced.