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 controllers properly route VLAN traffic.

- The controller 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.

Restrictions for WLANs

The following restrictions apply when configuring WLANs:

- Peer-to-peer blocking does not apply to multicast traffic.
- You can configure a maximum of 3000 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 Static-IPv4 address is not supported.
- When creating a WLAN with the same SSID, you must create a unique profile name for each WLAN.

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 controller.

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 10

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.

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 10

DTIM Period

In 802.11a/n and 802.11b/g/n 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 802.11a/n or 802.11b/g/n 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 802.11a/n or 802.11b/g/n 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 controller, 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 802.11a/n and 802.11b/g/n networks that support such clients.

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 10

Session Timeout

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.

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 10

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 controllers 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 controller 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 controller 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 10

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 10

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 controller GUI or CLI to enable the diagnostic channel, and you can use the controller 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.

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 10

Client Count Per WLAN

You can set a limit to the number of clients that can connect to a WLAN, which is useful in scenarios where you have a limited number of clients that can connect to a controller. For example, consider a scenario where the controller can serve up to 256 clients on a WLAN and these clients can be shared between enterprise users (employees) and guest users. 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 for each WLAN depends on the platform that you are using.

Related Topics

Configuring Advanced WLAN Properties (CLI), on page 10

Per-WLAN RADIUS Source Support

By default, the controller 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 controller 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 controller on the per-WLAN RADIUS traffic, where each WLAN can have a separate layer 3 identity. This feature is useful in ACS Network Access Restrictions and Network Access Profiles.

You can be 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** *wlan-name wlan-id* [*ssid*]
3. **end**
4. (Optional) **show wlan summary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id* [*ssid*] **Example:** `Switch(config)# wlan mywlan 34 mywlan-ssid`	Specifies the WLAN name and ID: • For the *wlan-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.

	Command or Action	Purpose
		• 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.
Step 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.
Step 4	**show wlan summary** **Example:** `Switch# show wlan summary`	(Optional) Displays a summary of WLANs that are created on the device.

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

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
```

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** *wlan-name*
3. **shutdown**
4. **media-stream multicast-direct**
5. **broadcast-ssid**
6. **call-snoop**
7. **radio** {**all** | **dot11a** | **dot11ag** | **dot11bg** | **dot11g**}
8. **client vlan** *vlan-identifier*
9. **ip multicast vlan** *vlan-name*
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** *wlan-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *wlan-name* is the profile name of the configured WLAN.
Step 3	**shutdown** **Example:** `Switch# shutdown`	Disables the WLAN before configuring the parameters.
Step 4	**media-stream multicast-direct** **Example:** `Switch(config-wlan)# media-stream multicast-direct`	Enables multicast VLANs on this WLAN.
Step 5	**broadcast-ssid** **Example:** `Switch(config-wlan)# broadcast-ssid`	Broadcasts the SSID for this WLAN. This field is enabled by default.
Step 6	**call-snoop** **Example:** `Switch(config-wlan)# call-snoop`	Enables call-snooping support.
Step 7	**radio** {**all** | **dot11a** | **dot11ag** | **dot11bg** | **dot11g**}	Enables radios on the WLAN. The keywords are as follows: • **all—**Configures the WLAN on all radio bands.

	Command or Action	Purpose
	Example: `Switch# radio all`	• **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 8	**client vlan** *vlan-identifier* **Example:** `Switch# client vlan test-vlan`	Enables an interface group on the WLAN. The arguments are as follows: • *vlan-identifier***—**Specifies the VLAN ID. • **name—**Specifies the VLAN name.
Step 9	**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 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.

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** *wlan-name*
3. **aaa-override**
4. **chd**
5. **session-timeout** *time-in-seconds*
6. **ccx aironet-iesupport**
7. **diag-channel**
8. **ip access-group** *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** { [**0-7**] | **defer-value**}
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *wlan-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.

	Command or Action	Purpose
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.
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** *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.
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`	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** { [**0-7**] | **defer-value**} **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 60000. The default is 100.

	Command or Action	Purpose
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 2
Off-Channel Scanning Defer, on page 3
DTIM Period, on page 3
Session Timeout, on page 4
Cisco Client Extensions, on page 4
Peer-to-Peer Blocking, on page 5
Diagnostic Channel, on page 5
Client Count Per WLAN, on page 5
Information About AAA Override

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.

Command	Description
show running-config *wlan*	Displays the running configuration of all WLANs.

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 3850 Switches)*

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 Name	Release	Feature Information
WLAN functionality	Cisco IOS XE 3.2SE	This feature was introduced.