WLANs

Information About WLANs

This feature enables you to control WLANs for lightweight access points. Each WLAN has a separate WLAN ID, a separate profile name, and a WLAN SSID. All access points can advertise up to 16 WLANs. However, you can create up to 4096 WLANs and then selectively advertise these WLANs (using profiles and tags) to different access points for better manageability.

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

Note The **wireless client max-user-login concurrent** command will work as intended even if the **no configure max-user-identity response** command is configured.

Note We recommend that you configure the **password encryption aes** and the **key config-key password-encrypt** *key* commands to encrypt your password.

Note For C9105, C9115, and C9120 APs, when a new WLAN is pushed from the controller and if the existing WLAN functional parameters are changed, the other WLAN clients will disconnect and reconnect.

Band Selection

Band select enables client radios that are capable of dual-band (2.4 and 5-GHz) operations 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 3 nonoverlapping channels. To prevent these sources of interference and improve overall network performance, configure band selection on the device.

Off-Channel Scanning Deferral

A lightweight access point, in normal operational conditions, periodically goes off-channel and scans another channel. This is in order to perform RRM operations such as the following:

- Transmitting and receiving Neighbor Discovery Protocol (NDP) packets with other APs.
- Detecting rogue APs and clients.
- Measuring noise and interference.

During the off-channel period, which normally is about 70 milliseconds, the AP is unable to transmit or receive data on its serving channel. Therefore, there is a slight impact on its performance and some client transmissions might be dropped.

While the AP is sending and receiving important data, it is possible to configure off-channel scanning deferral so that the AP does not go off-channel and its normal operation is not impacted. You can configure off-channel scanning deferral on a per-WLAN basis, per WMM UP class basis, with a specified time threshold in milliseconds. If the AP sends or receives, on a particular WLAN, a data frame marked with the given UP class within the specified threshold, the AP defers its next RRM off-channel scan. For example, by default, off-channel scanning deferral is enabled for UP classes 4, 5, and 6, with a time threshold of 100 millseconds. Therefore, when RRM is about to perform an off-channel scan, a data frame marked with UP 4, 5, or 6 is received within the last 100 milliseconds, RRM defers going off-channel. The AP radio does not go off-channel when a voice call sending and receiving audio samples is marked as UP class 6 for every active 20 milliseconds.

Off-channel scanning deferral does come with a tradeoff. Off-channel scanning can impact throughput by 2 percent or more, depending on the configuration, traffic patterns, and so on. Throughput can be slightly improved if you enable off-channel scanning deferral for all traffic classes and increase the time threshold. However, by not going off-channel, RRM can fail to identify AP neighbors and rogues, resulting in negative impact to security, DCA, TPC, and 802.11k messages.

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 broadcast and multicast frames 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 for 10 times every 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 for 5 times every 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). The only recommended DTIM values are 1 and 2; higher DTIM values will likely cause communications problems.

Note A beacon period, which is specified in milliseconds on the device, is converted internally by the software to 802.11 Time Units (TUs), where 1 TU = 1.024 milliseconds. Depending on the AP model, the actual beacon period may vary slightly; for example, a beacon period of 100 ms may in practice equate to 104.448 ms.

Prerequisites for Configuring Cisco Client Extensions

- The software supports CCX versions 1 through 5, which enables devices 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 device 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 device sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the device and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.

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 device, dropped by the device, or forwarded to the upstream VLAN.

Peer-to-peer blocking is supported for clients that are associated with local and central switching WLANs.

Note Peer-to-peer blocking feature is VLAN-based. WLANs using the same VLAN has an impact, if Peer-to-peer blocking feature is enabled.

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 device GUI or CLI to enable the diagnostic channel, and you can use the device **diag-channel** CLI to run the diagnostic tests.

Note We recommend that you enable the diagnostic channel feature only for non-anchored SSIDs that use the management interface. CCX Diagnostic feature has been tested only with clients having Cisco ADU card

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 devices properly route VLAN traffic.

Restrictions for WLANs

- Do not configure PSK and CCKM in a WLAN, as this configuration is not supported and impacts client join flow.
- Ensure that TKIP or AES ciphers are enabled with WPA1 configuration, else ISSU may break during upgrade process.
- When you change the WLAN profile name, then FlexConnect APs (using AP-specific VLAN mapping) will become WLAN-specific. If FlexConnect Groups are configured, the VLAN mapping will become Group-specific.
- Do not enable IEEE 802.1X Fast Transition on Flex Local Authentication enabled WLAN, as client association is not supported with Fast Transition 802.1X key management.
- Peer-to-peer blocking does not apply to multicast traffic.
- In FlexConnect, peer-to-peer blocking configuration cannot be applied only to a particular FlexConnect AP or a subset of APs. It is applied to all the FlexConnect APs that broadcast the SSID.
- The WLAN name and SSID can have up to 32 characters.
- WLAN and SSID names support only the following ASCII characters:
  - Numerals: 48 through 57 hex (0 to 9)
  - Alphabets (uppercase): 65 through 90 hex (A to Z)
  - Alphabets (lowercase): 97 through 122 hex (a to z)
  - ASCII space: 20 hex
  - Printable special characters: 21 through 2F, 3A through 40, and 5B through 60 hex, that is: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
- WLAN name cannot be a keyword; for example, if you try to create a WLAN with the name as 's' by entering the **wlan s** command, it results in shutting down all WLANs because 's' is used as a keyword for shutdown.
- You cannot map a WLAN to VLAN 0. Similarly, you cannot map a WLAN to VLANs 1002 to 1006.
- Dual stack clients with a static-IPv4 address is not supported.

- In a dual-stack with IPv4 and IPv6 configured in the Cisco 9800 controller, if an AP tries to join controller with IPv6 tunnel before its IPv4 tunnel gets cleaned, you would see a traceback and AP join will fail.
- 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.
- The SSID that is sent as part of the user profile will work only if **aaa override** command is configured.
- RADIUS server overwrite is not configured on a per WLAN basis, but rather on a per AAA server group basis.
- Downloadable ACL (DACL) is supported only on the central switching mode. It is not supported for Flex Local switching or on the Cisco Embedded Wireless Controller.
- You cannot mix open configuration models with CLI-based, GUI-based, or Catalyst Center-based configurations. However, if you decide to use multiple model types, they must remain independent of each other. For example, in open configuration models, you can only manage configurations that have been created using an open configuration model, not a CLI-based or GUI-based model. Configurations that are created using open configuration models cannot be modified using a GUI-based model, or CLI-based model, or any other model.

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

How to Configure WLANs

Creating WLANs (GUI)

Procedure

Step 1 In the **Configuration** > **Tags & Profiles** > **WLANs** page, click **Add**.

The **Add WLAN** window is displayed.

Step 2 Under the **General** tab and **Profile Name** field, enter the name of the WLAN. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 3 Click **Save & Apply to Device**.

Creating WLANs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id* [*ssid*] **Example:** `Device(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** • You can create SSID using GUI or CLI. However, we recommend that you use CLI to create SSID. • By default, the WLAN is disabled.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Deleting WLANs (GUI)

Procedure

Step 1 In the **Configuration** > **Tags & Profiles** > **WLANs** page, check the checkbox adjacent to the WLAN you want to delete.

To delete multiple WLANs, select multiple WLANs checkboxes.

Step 2 Click **Delete**.

Step 3 Click **Yes** on the confirmation window to delete the WLAN.

Deleting WLANs

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**no wlan** *wlan-name wlan-id ssid* **Example:** `Device(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:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Searching WLANs (CLI)

To verify the list of all WLANs configured on the controller, use the following show command:

```
Device# 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
```

To use wild cards and search for WLANs, use the following `show` command:

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

Enabling WLANs (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 On the **WLANs** page, click the WLAN name.

Step 3 In the **Edit WLAN** window, toggle the **Status** button to **ENABLED**.

Step 4 Click **Update & Apply to Device**.

Enabling WLANs (CLI)

Procedure

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

Disabling WLANs (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 In the **WLANs** window, click the WLAN name.

Step 3 In the **Edit WLAN** window, set the **Status** toggle button as **DISABLED**.

Step 4 Click **Update & Apply to Device**.

Disabling WLANs (CLI)

Procedure

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

Configuring General WLAN Properties (CLI)

You can configure the following properties:

- Media stream
- Broadcast SSID
- Radio

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device(config)# wlan test4`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.

	Command or Action	Purpose
Step 3	**shutdown** **Example:** `Device(config-wlan)# shutdown`	Disables the WLAN.
Step 4	**broadcast-ssid** **Example:** `Device(config-wlan)# broadcast-ssid`	Broadcasts the SSID for this WLAN.
Step 5	**dot11bg 11g** **Example:** `Device(config-wlan)# dot11bg 11g`	Configures the WLAN radio policy for dot11 radios.
Step 6	**media-stream multicast-direct** **Example:** `Device(config-wlan)# media-stream multicast-direct`	Enables multicast VLANs on this WLAN.
Step 7	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 8	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.

Configuring Advanced WLAN Properties (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device(config)# wlan test4`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**chd** **Example:** `Device(config-wlan)# chd`	Enables coverage hole detection for this WLAN.

	Command or Action	Purpose
Step 4	**ccx aironet-iesupport** **Example:** `Device(config-wlan)# ccx aironet-iesupport`	Enables support for Aironet IEs for this WLAN.
Step 5	**client association limit** {*clients-per-wlan* | **ap** *clients-per-ap-per-wlan* | **radio***clients-per-ap-radio--per-wlan*} **Example:** `Device(config-wlan)# client association limit ap 400`	Sets the maximum number of clients, clients per AP, or clients per AP radio that can be configured on a WLAN.
Step 6	**ip access-group web** *acl-name* **Example:** `Device(config-wlan)# ip access-group web test-acl-name`	Configures the IPv4 WLAN web ACL. The variable *acl-name* specifies the user-defined IPv4 ACL name.
Step 7	**peer-blocking** [**allow-private-group** | **drop** | **forward-upstream**] **Example:** `Device(config-wlan)# peer-blocking drop`	Configures peer to peer blocking parameters. The keywords are as follows: • **allow-private-group**—Enables peer-to-peer blocking on the Allow Private Group action. • **drop**—Enables peer-to-peer blocking on the drop action. • **forward-upstream**—No action is taken and forwards packets to the upstream. **Note** The **forward-upstream** option is not supported for Flex local switching. Traffic is dropped even if this option is configured. Also, peer to peer blocking for local switching SSIDs are available only for the clients on the same AP.
Step 8	**channel-scan** {**defer-priority** {**0-7**} | **defer-time** {**0 - 6000**}} **Example:** `Device(config-wlan)# 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.

	Command or Action	Purpose
Step 9	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.

Configuring Advanced WLAN Properties (GUI)

Before you begin

Ensure that you have configured an AP Join Profile prior to configuring the primary and backup controllers.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs** .

Step 2 Click **Add**.

Step 3 Under the **Advanced** tab, check the **Coverage Hole Detection** check box.

Step 4 Check the **Aironet IE** check box to enable Aironet IE on the WLAN.

Step 5 Check the **Diagnostic Channel** check box to enable diagnostic channel on the WLAN.

Step 6 From the **P2P Blocking Action** drop-down list, choose the required value.

Step 7 Set the **Multicast Buffer** toggle button as enabled or diabled.

Step 8 Check the **Media Stream Multicast-Direct** check box to enable the feature.

Step 9 In the **Max Client Connections** section, specify the maximum number of client connections for the following:

- In the **Per WLAN** field, enter a value. The valid range is between 0 and 10000.
- In the **Per AP Per WLAN** field, enter a value. The valid range is between 0 and 400.
- In the **Per AP Radio Per WLAN** field, enter a value. The valid range is between 0 and 200.

Step 10 In the **11v BSS Transition Support** section, perform the following configuration tasks:

a) Check the BSS Transition check box to enable 802.11v BSS Transition support.
b) In the **Disassociation Imminent** field, enter a value. The valid range is between 0 and 3000.
c) In the **Optimized Roaming Disassociation Timer** field, enter a value. The valid range is between 0 and 40.
d) Select the check box to enable the following:

- BSS Max Idle Service
- BSS Max Idle Protected
- Disassociation Imminent Service
- Directed Multicast Service
- Universal Admin
- Load Balance

- Band Select
- IP Source Guard

Step 11 From the **WMM Policy** drop-down list, choose the policy as Allowed, Disabled, or Required. By default, the WMM policy is Allowed.

Step 12 In the **Off Channel Scanning Defer** section, choose the appropriate **Defer Priority** values and then specify the required Scan Defer Time value in milliseconds.

Step 13 In the **Assisted Roaming (11k)** section, choose the appropriate status for the following:

- Prediction Optimization
- Neighbor List
- Dual-Band Neighbor List

Step 14 In the **DTIM Period (in beacon intervals)** section, specify a value for 802.11a/n and 802.11b/g/n radios. The valid range is from 1 to 255.

Step 15 Click **Apply to Device**.

Verifying WLAN Properties (CLI)

To verify the WLAN properties based on the WLAN ID, use the following `show` command:

```
Device# show wlan id wlan-id
```

To verify the WLAN properties based on the WLAN name, use the following `show` command:

```
Device# show wlan name wlan-name
```

To verify the WLAN properties of all the configured WLANs, use the following `show` command:

```
Device# show wlan all
```

To verify the summary of all WLANs, use the following `show` command:

```
Device# show wlan summary
```

To verify the running configuration of a WLAN based on the WLAN name, use the following `show` command:

```
Device# show running-config wlan wlan-name
```

To verify the running configuration of all WLANs, use the following `show` command:

```
Device# show running-config wlan
```