Converged Access: WLAN Configuration

This chapter provides information about configuring and enabling wireless LANs (WLAN) on your converged access deployment and the recommended WLAN configuration on a switch. It also provides information about how to configure and advertise WLANs for the clients to join. This document also describes how to enhance the functionality of WLANs by enabling various features, and leverage the security policies created in the deployment process for wireless authentication.

WLAN Features

DHCP Server

By default, clients either assign their IP addresses statically or by an enterprise DHCP server. We recommend that the wireless clients get their IP addresses through a DHCP server. This allows addressing policies to be leveraged on the DHCP server, prevent the use of duplicate network addresses, and enhance security.

To configure WLANs such that clients receive their IP addresses through a DHCP server, use the following commands:

```
Device(config)# wlan profile-name
Device(config-wlan)# ip dhcp required
```

To verify the configuration on a per-WLAN basis, use the following command:

```
Device# show wlan id wlan-id
.
.
.
DHCP Address Assignment Required               : Enabled
.
.
.
```

For more information on DHCP in WLANs, refer to the Configuring DHCP for WLANs section in the WLAN Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches).

Protected Management Frame

Control and Management frames are transmitted unencrypted, so that they are understood by all clients. The 802.11w Protected Management frames protect the wireless medium from attacks by adding cryptographic information into control frames for clients that support the standard.

To configure a protected management frame for clients that support the standard, use the following command:

```
Device(config-wlan)# security pmf optional
```

To verify that the protected management frame is configured properly on the WLAN, use the following command:

```
Device# show wlan id wlan_id
.
.
.
    PMF Support                                : Optional
        PMF Association Comeback Timeout       : 1
        PMF SA Query Time                      : 200
.
.
.
```

For more information about DHCP in WLANs, refer to theConfiguring DHCP for WLANs section in the WLAN Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) WLAN Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches).

Band Selection

Band Selection is a feature that encourages dual-band clients to connect to a 5-GHz network over a 2.4-GHz network advertising the same SSID. This is preferred because 5-GHz networks exhibit less interference on wireless channels. The band selection algorithm works by slightly delaying probe responses to clients on 2.4-GHz channels, thus making the 5-GHz channels more attractive to clients.

Note Band selection only affects the operation of dual-band clients and requires both the radios on the corresponding access point to be operational.

Tip Band selection should not be used with WLANs that provide latency-sensitive services, such as real-time voice or video because of the potential for slightly increased roaming delay. If you are provisioning a WLAN for voice or video, do not enable band selection.

To enable band selection on WLANs used to support data clients, use the following commands:

```
Device(config)# wlan profile-name
Device(config-wlan)# band-select
```

To verify that band selection is configured on a WLAN, use the following command:

```
Device# show wlan id wlan-id

WLAN Profile Name     : profile_name
.
```

```
.
.
Band Select                                     : Enabled
.
.
.
```

Assisted Roaming

The Assisted Roaming feature helps reduce the need for active and passive scanning by 802.11k-enabled clients, and optimizes roaming for 802.11k-compliant and non-802.11k clients. For 802.11k clients, assisted roaming allows clients to request neighbor reports with information about access points that are roaming candidates. For non-802.11k clients, the switch maintains a prediction neighbor list and attempts to ensure that clients roam to the access point with the best signal by denying association requests to less desirable access points.

To configure assisted roaming on data WLANs, use the following commands:

```
Device(config)# wlan profile-name
Device(wlan)# assisted-roaming neighbor-list
Device(wlan)# assisted-roaming dual-list
Device(wlan)# assisted-roaming prediction
```

To verify that assisted roaming is configured on a WLAN, use the following command:

```
Device# show wlan id wlan-id
.
.
.
Assisted-Roaming
    Neighbor List                               : Enabled
    Prediction List                             : Enabled
    Dual Band Support                           : Enabled
```

Tip The Assisted Roaming Prediction feature can potentially deny association requests to access points. This is not considered to be the best candidate for the client roam and may induce extra delay during an active client roam. We do not recommend Assisted Roaming Prediction or WLANs that provide real-time or latency-sensitive services, such as voice or real-time video.

Peer-to-Peer Blocking

Peer-to-peer blocking gives an administrator more control to handle wireless-to-wireless client traffic on a switch. For example, one wireless user downloading a shared file from another user, or two phones connected to one another in an enterprise environment are scenarios that are acceptable and expected. However, on a guest WLAN or a hotspot-style WLAN, wireless-to-wireless traffic may be a security hazard and should be blocked.

For enterprise WLANs, the peer-to-peer feature is disabled by default.

To enable peer-to-peer blocking on a guest WLAN with the drop option, use the following commands on the corresponding WLAN:

```
Device(config)# wlan profile-name
```

```
Device(config-wlan)# peer-blocking drop
```

To verify that peer-to-peer blocking is enabled with the drop action for the guest WLAN, use the following command:

```
Device# show wlan id wlan-id
.
.
.
Peer-to-Peer Blocking Action                    : Drop
.
.
.
```

Wi-Fi Direct Client Policy

Wi-Fi Direct is a client feature that allows clients to form ad hoc connections with one another to conveniently transfer data or provide a service. Devices that are Wi-Fi Direct capable can connect directly to each other quickly and conveniently to do tasks such as printing, synchronization, and sharing of data. Wi-Fi Direct devices may associate with multiple peer-to-peer (P2P) devices and with infrastructure wireless LANs (WLANs) concurrently.

However, this represents a potential security risk because devices connected through Wi-Fi Direct lack any identity information because they do not connect to the wireless infrastructure. Policy decisions cannot be easily applied to the devices connected on the Wi-Fi Direct devices. As a result, we recommend that you do not allow the devices connected through Wi-Fi Direct to access the wireless network in an enterprise environment.

To stop Wi-Fi devices from connecting to enterprise WLAN, use the following commands:

```
Device(config)# wlan profile-name
Device(config-wlan)# wifidirect policy deny
```

To ensure that the Wi-Fi Direct policy is set to Deny a WLAN, use the following command:

```
Device# show wlan id wlan-id
.
.
.
WifiDirect                                      : Deny
.
.
.
```

Roaming Fast Transition (802.11r)

802.11r is an IEEE standard to help accelerate client roaming while creating a more seamless experience for a roaming client. Fast-transition roaming works by associating a client and an access point before the client roams to the target AP, such that all the wireless keys are ready for use before roam association actually takes place.

Note By default, fast transition is disabled.

Tip Clients with drivers that do not support 802.11r will not be able to associate to a WLAN with fast transition enabled. Therefore, ensure that fast transition is disabled. If fast transition is required, create a separate SSID. Disabling or enabling fast transition by creating a separate SSID allows even legacy devices to access the enterprise WLAN.

To configure fast transition and an associated SSID, use the following commands:

```
Device(config)# wlan profile-name
Device(config-wlan)# security ft
```

To verify that fast transition is enabled on the appropriate WLAN, use the following command:

```
Device# show wlan id wlan-id
.
.
.
    FT Support                                  : Enabled
        FT Reassociation Timeout                : 20
        FT Over-The-DS mode                     : Enabled
.
.
.
```

For more information about 802.11r fast transition, refer to the Configuring 802.11r BSS Fast Transition guide.

Media Session Snooping

Media session snooping is configured on a per-WLAN basis and allows access points to detect Session Initiation Protocol (SIP) sessions, session establishment, and session termination. An access point reports statistics to the controller, which collects data about VoIP calls for a management station such as Cisco Prime Infrastructure. Further, when media session snooping is enabled, the controller generates a trap log for failed calls, indicating the time and reason for failure.

Tip For successful operation, media session snooping requires call control and establishment to be handled through the SIP. Media session snooping may not operate as expected if call control is performed through Signaling Connection Control Part (SCCP) or a SIP that is noncompliant with RFC 3261.

To configure media session snooping, use the following commands. Ensure that a voice WLAN is configured and SIP is used as a call control mechanism before using the commands.

```
Device(config)# wlan profile-name
Device(config-wlan)# call-snoop
```

To verify that media session snooping is enabled on a voice WLAN, use the following command:

```
Device# show wlan id wlan-id
.
.
.
Call Snooping                               : Enabled
.
.
.
```

Quality of Service

For information about enabling quality of service (QoS) on the WLANs that service your enterprise network and configuration of QoS feature, see the Wireless QoS chapter.

Deploying WLANs

Defining WLANs

The wireless functionality in the Cisco Catalyst 3850 Series Switches and the Cisco Catalyst 3650 Series Switches supports up to 64 WLANs for lightweight access points (APs). Similarly, the Cisco 5700 Series Wireless Controllers support up to 512 WLANs for lightweight APs. Each WLAN ID has an associated profile name, WLAN identifier, and Service Set Identifier (SSID). A switch can publish up to 16 WLANs to a given AP.

Tip You can select the WLANs to be deployed to a given AP by placing the APs into access-point groups and then publishing the WLANs to that AP group. This helps you to segment and manage your wireless network in larger deployments.

To define a WLAN for corporate users, use the following command:

```
Device(config)# wlan profile-name wlan-id [ssid]
```

Note If you do not provide the SSID option, the *SSID* will be the same as the WLAN profile name.

To associate a WLAN with a client VLAN after the WLAN is created, use the following command:

```
Device(config-wlan)# client vlan vlan-id
```

After you run the command, any client joining the WLAN is placed into the specified VLAN. The *vlan-id* can be the VLAN name, numeric VLAN identifier, or a VLAN group name.

WLAN Security

AAA policies authenticate and authorize clients. To attach a configured AAA client authentication policy to a WLAN, use the following commands:

```
Device(config)# wlan profile-name
Device(config-wlan)# security dot1x authentication-list aaa-method-list
```

Tip WPA2 security with Advanced Encryption Standard (AES) ciphers is the default security for a new WLAN. To configure WPA security, for example, if you changed the security policy, use the **security wpa wpa2 ciphers aes** command.
For more information on WLAN security and configuring additional features, refer to the Configuring WLAN Security guide.

To verify the configuration, use the following command:

```
Device# show wlan id wlan-id
.
.
.
802.1x authentication list name                : aaa_method_list
.
.
.
    Wi-Fi Protected Access (WPA/WPA2)          : Enabled
        WPA (SSN IE)                           : Disabled
        WPA2 (RSN IE)                          : Enabled
            TKIP Cipher                        : Disabled
            AES Cipher                         : Enabled
```

Enabling a WLAN

By default, WLANs are shut down after they are created. This chapter describes how to make configuration changes to a WLAN while it is in the disabled state. Each configuration change to a WLAN requires pushing that configuration to the access points. Therefore, configurations on a WLAN requires the WLAN to be shut down.

To enable a WLAN in order to allow clients to connect, use the following command:

```
Device(config)# wlan profile-name
Device(config-wlan)# no shutdown
```

To verify that the WLAN is operational, check the controller WLAN summary using the following command:

```
Device# show wlan summary

Number of WLANs: 1

WLAN Profile Name                    SSID                           VLAN Status
-------------------------------------------------------------------------------
id   profile_name                    ssid                           vlan UP
```