Best Practices

Infrastructure

Disable Aironet IE

- Description— Aironet IE is a Cisco proprietary attribute used by Cisco devices for better connectivity. It contains information, such as the access point name, load, number of associated clients, and so on sent out by the access point (AP) in the beacon and probe responses of the Cisco Catalyst 9800 Series Wireless Controller. The Cisco Client Extensions (CCX) clients use this information to choose the best AP with which to associate.

  The 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 APs and to support Cisco features that other client devices do not. The features are related to increased security, enhanced performance, fast roaming, and power management.

  Aironet IE is optional for CCX based clients, however it can cause compatibility issues with some types of wireless clients. The recommendation is to enable for WGB and Cisco voice, but for general production network, it can be beneficial to disable Aironet IE after testing.

  CCX Aironet IE feature should be disabled.

- Status:
  - Selected—CCX Aironet IE must be disabled on one or more *ACTIVE* WLANs.
  - Unselected—CCX Aironet IE enabled on all *ACTIVE* WLANs.

- CLI Option—Enable support for Aironet IEs for a particular WLAN by entering this command:

```
Device# conf t

Device(config)# wlan <profile-name> <wlan-id> <ssid>

Device(config-wlan)# ccx aironet-iesupport
```

- CLI Option—Disable support for Aironet IEs for a particular WLAN by entering this command:

  ```
  Device# conf t
  
  Device(config)# wlan <profile-name> <wlan-id> <ssid>
  
  Device(config-wlan)# no ccx aironet-iesupport
  ```

Disable Management over Wireless

- Description—The Cisco WLAN solution Disable Management over Wireless feature allows Cisco WLAN solution operators to monitor and configure local controller using a wireless client.

  Management over wireless should be disabled for security reasons. Clicking **Fix it Now** disables management over wireless.

- Status:
  - Selected—Enabled
  - Unselected—Disabled

- CLI Option—Disable management over wireless by entering this command:

  ```
  Device(config)# no wireless mgmt-via-wireless
  ```

  CLI Option—Enable management over wireless by entering this command:

  ```
  Device(config)# wireless mgmt-via-wireless
  ```

HTTPs for Management

- Description—HTTPs for management provides greater security by allowing secure access.

  Secure Web Access (HTTPS) should be enabled for managing the Cisco Catalyst 9800 Series Wireless Controller. Web Access (HTTP) should be disabled.

- Status:
  - Selected—HTTPS enabled; HTTP disabled
  - Unselected—HTTPS enabled, HTTP enabled or HTTPS disabled, HTTP enabled

- CLI Options:
  - Disable the web mode to deny users to access the controller GUI using http://ip-address, by entering this command:

    ```
    Device# conf t
    Device(config)# no ip http secure-server
    ```

  - Enable Secure Web Access mode to allow users to access the controller GUI using https://ip-address, by entering this command:

    ```
    Device# conf t
    Device(config)# ip http secure-server
    ```

Configuring HTTPS to Use a Specific Trustpoint

If a device is configured with more than one crypto trustpoint (which could be for a self-signed or identity certificate), enter the following CLI command to use a specific trustpoint for HTTPS communication:

```
Device # conf t
Device (config)# ip http secure-trustpoint trustpoint-name
```

If the preceding CLI is not configured, HTTPS can use any configured trustpoint. HTTPS chooses the trustpoint in the following order:

1. Identity certificate
2. Self-signed certificate
3. CA certificate

Load Balancing

- Description—In dense production networks, controllers have been verified to function optimally with load balancing ON and window size set at 5 or higher. In practical, this means load balancing behavior is only enabled when, for example, a large group of people congregate in a conference room or open area (meeting or class). Load balancing is very useful to spread these users between various available APs in such scenarios.

  Load balancing should be enabled. For time sensitive application such as voice, it can cause roaming issues. Therefore, it is recommended to test before enabling load balancing on the Cisco Catalyst 9800 Series Wireless Controller. Clicking **Restore Default** enables load balancing on the Cisco Catalyst 9800 Series Wireless Controller, which may impact service at the time.

- Status:
  - Selected—Load balancing disabled on all active WLANs.
  - Unselected—Load balancing enabled on one or more active WLANs.

- CLI Option—Enable load balancing on a WLAN by entering this command:

  ```
  Device# conf t
  Device(config)# wlan <profile-name> <wlan-id> <ssid>
  Device(config-wlan)# load-balance
  ```

  CLI Option—Disable load balancing on a WLAN by entering this command:

  ```
  Device# conf t
  Device(config)# wlan <profile-name> <wlan-id> <ssid>
  Device(config-wlan)# no load-balance
  ```

NTP

- Description—Network Time Protocol (NTP) is very important for several features. It is mandatory to use NTP synchronization on the Cisco Catalyst 9800 Series Wireless Controller if you use any of these features: Location, SNMPv3, access point authentication, or MFP. The controller supports synchronization with NTP.

The NTP server is used to sync the Cisco Catalyst 9800 Series wireless controller's time.

- Status—If disabled, click **Manual Configuration** to manually configure the syncing with the NTP server.
  - Selected—NTP is configured on the Cisco Catalyst 9800 Series wireless controller.
  - Unselected—NTP is not configured on the Cisco Catalyst 9800 Series wireless controller.
- CLI Option:
  - Enable NTP server by entering this command:

```
Device# conf t
Device(config)# ntp server <server-name>
```

Virtual Gateway IP

- Description: Virtual gateway IP should be enabled. Clicking **Fix it Now** enables virtual gateway IP.
- Status:
  - Selected: Enabled
  - Unselected: Disabled

Local Profiling

- Description—The controller in Cisco Catalyst 9800 series-enabled APs can determine the client type from the information received when a client device associates with the controller. This controller acts as the collector of the information, and either displays the information directly on the Cisco Catalyst 9800 Series Wireless Controller GUI dashboard or sends required data to the ISE optimally.

  Local profiling (DHCP/HTTP) should be enabled on the Cisco Catalyst 9800 Series wireless controller.
- CLI Option—Enable local profiling (DHCP/HTTP) on all WLANs by entering this command:

Note Disable policy profile before you enable local profiling.

```
Device# conf t
Device(config)# wireless profile policy <policy name>
Device(config-wireless-policy)# http-tlv-caching
Device(config-wireless-policy)# dhcp-tlv-caching
Device(config-wireless-policy)# radius-profiling
```

Note To disable local profiling on all WLANs, use the same CLIs with a **no** command. For instance:

```
Device# conf t
Device(config)# wireless profile policy <policy name>
Device(config-wireless-policy)# no http-tlv-caching
Device(config-wireless-policy)# no dhcp-tlv-caching
Device(config-wireless-policy)# no radius-profiling
```

VRF and Routing Protocol

Cisco Catalyst 9800 Series Wireless Controller does not support VRFs or routing protocols. The controller should not be used as a router for wireless clients.

The only exception is the mgmt-vrf on the management port on physical appliances.

Site Tag

- We recommend that you use a custom site-tag instead of the default-site-tag for APs.
- For APs in local mode (or local site-tag), we recommend that you limit the number of APs per site-tag to 500. For example, if you have more than 500 APs in a building, use two site-tags for the building. Seamless and fast-roaming is supported across site-tags. You can configure more or less APs per site-tag, but the recommendation is not to exceed these numbers:

Platform	Maximum Number of APs per Local Site-Tag
C9800-80, C9800-CL (medium and large)	1600
C9800-40	800
Other C9800 platforms	Equal to the maximum number of APs supported

- For FlexConnect APs and related remote site-tags, if seamless roaming is required, the limit is 100 APs per site-tag.

Security

WLAN with WPA3, WPA2 or 802.1X

- Description—WLAN should be using 802.1x or WPA2 or WPA3 security. You can enable this from the linked WLAN page. The default day 0 setting does not mandate configuring 802.1x.
- Status—If disabled, click **Manual Configuration** to specify the security setting of the WLAN.
  - Selected—Either 802.1x or WPA2 is enabled on at least one WLAN.

  - Unselected—Neither security is enabled on any WLAN.

- CLI option—Enable WLAN with WPA2 or 802.1x security by entering this command:

```
Device# configure terminal
Device(config)# wlan wlan-demo 1 ssid-demo
Device(config-wlan)# security wpa wpa2 ciphers aes
Device(config-wlan)# security wpa akm dot1x
```

Client Exclusion

- Description—When the client fails to authenticate, the controller excludes the client. The client cannot connect to the network until the exclusion timer expires or is manually overridden by the administrator.

  Client exclusion detects authentication attempts made by a single device. When the device exceeds a maximum number of failures, that MAC address is not allowed to associate any longer to the controller.

  When you click **Fix it**, the following components are enabled:

  - Excessive 802.11 Association Failures
  - Excessive 802.1X Authentication Failures
  - Excessive 802.1X Authentication Timeout
  - IP Theft or IP Reuse
  - Excessive Web Authentication Failures

- Status:

  - Selected—Client exclusion is enabled for all events
  - Unselected—Client exclusion is disabled for all events

- CLI Option—Enable client exclusion for all events by entering this command:

```
Device# conf t
Device (config)# wireless profile policy <default-policy-profile>
! This is per-profile and needs to be done in all the profiles.
Device (config-wireless-policy)# exclusionlist timeout <secs>
```

Note The valid values for exclusion-list timeout ranges between 0 and 2147483647 seconds. Here, 0 refers to no timeout.

CLI Option—Disable client exclusion for all events by entering this command:

```
Device# conf t
Device (config)# wireless profile policy <default-policy-profile>
Device (config-wireless-policy)# exclusionlist timeout 0
```

Note To deauthenticate the client, use the following command:

```
Device# wireless client mac-address xxxx.xxxx.xxxx deauthenticate
```

You must use the wireless exclusion list client mac address to manually add clients to the exclusion list and use the no form of the command to remove the client from the exclusion list. However; the no form of the command does not remove the clients that are dynamically added to the exclusion list.

User Login Policies

- Description—The user login policies are provided to limit the number of concurrent logins to the controller. You can limit the number of concurrent logins, and the recommendation is greater than default of 0 (unlimited).
- Status:
  - Selected—User login policies enabled only if the login count is set to either 0 or 8.
  - Unselected—User login policies disabled only if the login count is set to either 0 or 8.

  Note 0 refers to unlimited restrictions for user login policies.

- CLI Option:
  - Verify the user login policies by entering this command:

    ```
    Device# show run | i max-user-login
    ```

  - Configure user login policies by entering this command:

    ```
    Device# conf t
    Device(config)# wireless client max-user-login ?
       <0-8>  Maximum number of login sessions for a single user, 0-8 (0=Unlimited)
    ```

RF Management

Auto Coverage Hole Detection

- Description—Auto CHD should be enabled.

  The controller uses the quality of client signal levels reported by the APs to determine if the power level of that AP needs to be increased. Coverage Hole Detection (CHD) is controller independent, so the RF group leader is not involved in those calculations. The controller knows how many clients are associated with a particular AP and what are the signal-to-noise ratio (SNR) values for each client.

If a client SNR drops below the configured threshold value on the controller, the AP increases its power level to try to compensate for the client. The SNR threshold is based on the transmit power of the AP and the coverage profile settings on the controller.

For instructions on how to configure auto CHD, see the *Cisco Catalyst 9800 Seriess Wireless Controller Software Configuration Guide, Cisco IOS XE Gibraltar 16.12.x*.

- Status:
  - Selected—CHD enabled
  - Unselected— None or one enabled
- CLI Option—Enable auto CHD by entering this command:

```
Device# conf t
Device (config)# ap dot11 24ghz/5gHz rrm coverage
```

CLI Option—Disable auto CHD by entering this command:

```
Device# conf t
Device (config)# no ap dot11 24ghz/5gHz rrm coverage
```

Auto Dynamic Channel Assignment

- Description—Auto DCA should be enabled to allow RRM to select best channels for each radio.

  When a wireless network is first initialized, all radios participating require a channel assignment to operate without interference - optimizing the channel assignments to allow for interference free operation is DCA's job. Wireless network does this using the air metrics reported by each radio on every possible channel, and providing a solution that maximizes channel bandwidth and minimizes RF interference from all sources - Self (signal), other networks (foreign interference), Noise (everything else).

  DCA is enabled by default and provides a global solution to channel planning for your network.
- Status:
  - Selected—DCA is enabled for 2.4 / 5 GHz
  - Unselected—None or one is enabled
- CLI Option—Enable auto DCA by entering this command:

```
Device# conf t
Device (config)# ap dot11 5ghz/24ghz rrm channel dca global auto
```

CLI Option—Disable auto DCA by entering this command:

```
Device# conf t
Device (config)# no ap dot11 5ghz/24ghz rrm channel dca global auto
```

Auto Transmit Power Control

- Description—The controller dynamically controls the access point transmit power based on real-time wireless LAN conditions. You can choose between two versions of transmit power control: TPCv1 and TPCv2. With TPCv1, power can be kept low to gain extra capacity and reduce interference. With TPCv2, transmit power is dynamically adjusted with the goal of minimum interference. TPCv2 is suitable for dense networks. In this mode, there could be higher roaming delays and coverage hole incidents.

  Auto TPC is enabled by default to allow RRM to select best transmit power for each radio.

  The Transmit Power Control (TPC) algorithm increases and decreases the power of an access poin (AP) in response to changes in the RF environment. In most instances, TPC seeks to lower the power of the AP to reduce interference. But, in the case of a sudden change in the RF coverage-for example, if the AP fails or becomes disabled-TPC can also increase power of the surrounding APs. This feature is different from coverage hole detection, which is primarily concerned with clients. TPC provides enough RF power to achieve desired coverage levels while avoiding channel interference between APs.

  Note For optimal performance, use the Automatic setting to allow best transmit power for each radio.

- Status:
  - Selected—TPC enabled for 2.4 / 5 GHz
  - Unselected—None or one enabled

- CLI Option—Enable Auto TPC by entering this command:

```
Device# conf t
Device (config)# ap dot11 5ghz rrm txpower auto

Device (config)# ap dot11 24ghz rrm txpower auto
```

CleanAir Detection

- Description—CleanAir should be enabled.

  To effectively detect and mitigate RF interference, enable CleanAir whenever possible. There are recommendations to various sources of interference to trigger security alerts, such as generic DECT phones, jammer, and so on.

  Note Not all Cisco access points support CleanAir. Consult the data sheet of your Cisco AP model to see whether it supports CleanAir.

- Status:
  - Selected—Enabled
  - Unselected—Disabled

- CLI Option:
  - Enables CleanAir functionality on a network by entering this command:

    ```
    Device# configure terminal
    Device(config)# ap dot11 {5ghz | 24ghz} cleanair {alarm | device}
    ```

  - Enables interference detection specifically for jammer by entering this command:

    ```
    Device# configure terminal
    Device(config)# ap dot11 {5ghz | 24ghz} cleanair device jammer
    ```

Event Driven RRM

- Description—Spontaneous interference is interference that appears suddenly on a network, perhaps jamming a channel or a range of channels completely. The Cisco CleanAir spectrum event-driven radio resource management (RRM) feature allows you to set a threshold for air quality (AQ) that, if exceeded, triggers an immediate channel change for the affected access point. Most RF management systems can avoid interference, but this information takes time to propagate through the system. Cisco CleanAir relies on AQ measurements to continuously evaluate the spectrum and can trigger a move within 30 seconds. For example, if an access point detects interference from a video camera, it can recover by changing channels within 30 seconds of the camera becoming active. Cisco CleanAir also identifies and locates the source of interference so that more permanent mitigation of the device can be performed at a later time.

  Note Spectrum EDRRM can be triggered, to detect a significant level of interference, only by Cisco CleanAir-enabled access points in local mode.

  Event driven RRM is enabled by default.

- Status:
  - Selected—Event driven RRM is disabled on both 5GHz and 2.4GHz.
  - Unselected—Event driven RRM is enabled on either 5GHz or 2.4GHz.

- CLI Option—Enable Cisco CleanAir spectrum event-driven RRM by entering this command:

  ```
  Device# conf t
  Device (config)# ap dot11 {5ghz | 24ghz} rrm channel cleanair-event
  ```

WiFi Interference

- Description—To improve handling of WiFi Interference, Rogue Severity was added to the ED-RRM metrics. If a rogue access point is generating interference above a given threshold, this feature changes channels immediately instead of waiting until the next DCA cycle.

  This should be used when ED-RRM is enabled. It should be avoided on buildings with very large number of collocated WiFi networks (multi-tenant buildings) that are 100% overlapping.

- Status
  - Selected—WiFi interference is enabled.
  - Unselected—WiFi interference is disabled.
- CLI Option:
  - Verify the WiFi interference by entering this command:

    ```
    Device# show ap dot11 24ghz cleanair config
    ```

  - To enable WiFi interference, you need to perform the following:
    - Configure duty cycle by entering this command:

      ```
      Device# conf t
      Device (config)# ap dot11 24ghz rrm channel cleanair-event rogue-contribution
      dutycycle 80
      ```

    - Enable EDRRM by entering this command:

      ```
      Device# conf t
      Device (config)# ap dot11 24ghz rrm channel cleanair-event
      ```

    - Enable Rogue contribution by entering this command:

      ```
      Device# conf t
      Device (config)# ap dot11 24ghz rrm channel cleanair-event rogue-contribution
      ```

DCA Cisco AP Load

- Description—Avoid using this option to avoid frequent changes in DCA due to varying load conditions, this is disabled by default.
- Status
  - Selected—AP Load is disabled.
  - Unselected—AP Load is enabled.
- CLI Option:
  - Verify the current status by entering this command:

    ```
    Device# show ap dot11 24ghz channel | include Load
    ```

  - Enable DCA Cisco AP Load by entering this command:

    ```
    Device# conf t
    Device(config)# ap dot11 24ghz rrm channel load
    ```

  - Disable DCA Cisco AP Load by entering this command:

    ```
    Device# conf t
    Device(config)# no ap dot11 24ghz rrm channel load
    ```

Best Channel Width

- Description—Dynamic bandwidth selection selects the widest channel width with the highest client data rates and lowest channel utilization per radio. This minimizes data retries and CRC errors on the 5 GHz band while avoiding rogue APs and CleanAir Interferers.
- Status:
  - Selected—Channel width is selected as Best on both bands.
  - Unselected—Channel width is not selected as Best on both bands.
- CLI Option—Enable best channel width by entering this command:

```
Device# conf t
Device (config)# ap dot11 5ghz rrm channel dca chan-width best
```

Flexible Radio Assignment

- Description—Flexible radio assignment (FRA) enables automatic assignment of the XOR 2.4GHz radios to other roles such as 5 GHz and Monitor.

  We recommend that you enable FRA when you have APs such as the Cisco Aironet 2800 and 3800 Series that support XOR operation.
- Status:
  - Selected—FRA is disabled.
  - Unselected—FRA is enabled.
- CLI Option: Enable FRA by entering this command:

```
Device# conf t
Device (config)# ap fra
```

High SSID Counts

- Description—Number of WLANs should be less than 4.

  We recommend limiting the number of service set identifiers (SSIDs) configured at the controller. You can configure 16 simultaneous SSIDs (per radio on each AP), but as each WLAN/SSID needs separate probe responses and beaconing, the RF pollution increases as more SSIDs are added. Furthermore, some smaller wireless stations like PDA, WiFi Phones, and barcode scanners cannot cope with a high number of basic SSID (BSSID) information. This results in lockups, reloads, or association failures. Also the more SSIDs, the more beaconing needed, so less RF time is available for real data transmits. Cisco recommends one to three SSIDs for corporate, and one SSID for high-density designs. AAA override can be leveraged for per user VLAN/ settings on a single SSID scenario.

  The AP must beacon at the lowest mandatory speed set for each WLAN, in order to be able to reach the farthest stations irrespective of their location. This reduces available air time for client traffic.

- Status—Click **Manual Configuration** to manually configure the number of service set identifiers (SSIDs) configured at the controller.
  - Selected—Active SSID count is 4 or less.
  - Unselected—Active SSID count is more than 4.
- CLI Option:
  - Verify the number of WLANs by entering this command:

    ```
    (Cisco Controller) >show wlan summary
    ```

  - Disable unwanted WLANs by entering this command:

    ```
    Device# conf t
    Device (config)# no wlan <wlan-name> <wlan-id> <ssid-name>
    ```

Client Band Select

- Description—Band selection should be enabled. However, if there is interactive traffic such as voice or video on the WLAN, do not use band selection. Clicking **Enable** turns band selection on.

  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 AP. 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 APs because of the 802.11b/g limit of three non-overlapping channels. To prevent these sources of interference and improve overall network performance, you can configure band selection on controller:

  - Band selection is enabled globally by default.
  - 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.
  - Evaluate band selection for voice, particularly focusing on roaming performance. See below for further explanation.
  - Most newer model clients prefer 5 GHz by default if the 5 GHz signal of the AP is equal to or stronger than the 2.4-GHz signal.
  - Band select should be enabled for high-density designs

  Also, in high-density designs, the study of available UNII-2 channels should be made. Those channels that are unaffected by Radar and also usable by the client base should be added to the RRM DCA list as usable channels.

  Dual-band roaming can be slow depending on the client. If a majority of the base of voice clients exhibits a slow roaming behavior, it is more likely that the client sticks to 2.4 GHz. In this case, it has scanning issues on 5 GHz. Generally when a client decides to roam, it scans its current channel and band first. The clients generally scan for an AP that has a significantly better signal level, maybe as much as 20 dB and/or a significantly better SNR. Failing such available connection, the client may remain with its current AP. In this case, if the CU on 2.4 GHz is low and the call quality is not poor, then disabling the selected band is acceptable. However, the preferred design is to enable band selection on 5 GHz with all data rates enabled and 6 Mbps as mandatory. Then, set the 5 GHz RRM minimum Tx power level 6 dBm higher than the average 2.4 GHz power level set by RRM.

The goal of this configuration recommendation is to enable the client to obtain a band and channel with better SNR and Tx power initially. As already stated, generally when a client decides to roam, it scans its current channel and band first. So, if the client initially joins the 5 GHz band, then it is more likely to stay on the band if there are good power levels on 5 GHz. SNR levels on 5 GHz are generally better than 2.4 GHz because 2.4 GHz has only three Wi-Fi channels and is more susceptible to interference such as Bluetooth, iBeacons, and microwave signals.

802.11k is recommended to be enabled with dual-band reporting. This enables all 11k enabled clients to have the benefit of assisted roaming. With dual-band reporting enabled, the client receives a list of the best 2.4-GHz and 5-GHz APs upon a directed request from the client. Here, the client most likely looks at the top of the list for an AP on the same channel, and then on the same band as the client is currently on. This logic reduces scan times and saves battery power. Having 802.11k enabled on the WLC does not have a downside effect for non-802.11k clients.

- Status:
  - Selected—Client band select disabled on all active WLANs.
  - Unselected—Client band select enabled on one or more active WLANs.
- CLI Option:
  - Verify Band Select by entering this command:

    ```
    Device# show wlan all
    ```

  - Enable Band Select on a WLAN by entering this command:

    ```
    Device# conf t
    Device (config)# wlan <wlan-name> <wlan-id> <ssid-name>
    Device (config-wlan)# band-select
    ```

5GHz Low Data Rates

- Description—We recommend that low data rates of 6 and 9 Mbps are disabled on 5GHz for better performance.

  Note Low data rates should not be disabled for low density deployments where these data rates are expected to be present.

- Status:
  - Selected—Low data rates of 6 and 9 Mbps are disabled on 5GHz.
  - Unselected—Low data rates of 6 and 9 Mbps are enabled on 5GHz.
- CLI Option:
  - Disable 6Mbps on 5GHz by entering this command:

```
Device# conf t
Device (config)# ap dot11 5ghz rate RATE_6M disable
```

- Disable 9Mbps on 5GHz by entering this command:

```
Device# conf t
Device (config)# ap dot11 5ghz rate RATE_9M disable
```

2.4GHz Low Data Rates

- Description—Low data rates of 1, 2, and 5.5 Mbps should be disabled on 2.4Ghz and 11 Mbps set to *not mandatory* on 2.4Ghz for better performance.

Note Low data rates should not be disabled for low density deployments where these data rates are expected to be present.

- Status:
  - Selected—Low data rates of 1, 2 or 5.5 Mbps are disabled on 2.4GHz or 11 Mbps is set to *not mandatory*.
  - Unselected—Low data rates of 1, 2 or 5.5 Mbps are enabled on 2.4GHz or 11 Mbps is set to *mandatory*.

- CLI Option:
  - Disable 1Mbps on 2.4GHz by entering this command:

```
Device# conf t
Device (config)# ap dot11 24ghz rate RATE_1M disable
```

  - Disable 2Mbps on 2.4GHz by entering this command:

```
Device# conf t
Device (config)# ap dot11 24ghz rate RATE_2M disable
```

  - Disable 5.5Mbps on 2.4GHz by entering this command:

```
Device# conf t
Device (config)# ap dot11 24ghz rate RATE_5_5M disable
```

  - Configure or disable 11Mbps on 2.4GHz by entering this command:

```
Device# conf t
Device (config)# ap dot11 24ghz rate RATE_11M {disable | supported}
```

Apple Devices

WLAN Configuration

- Description—Allows you to identify if the WLAN is configured with recommended L2 security, QoS, and Advanced settings for Apple devices. Application Visibility should be enabled.
- Status—Click **Detailed** to manually configure the L2 security, QoS, and advanced settings for Apple devices for individual, active WLANs.
    - Selected—At least one WLAN is compliant with all the recommended WLAN configurations for Apple devices.
    - Unselected—None of the active WLANs are compliant with all the recommended WLAN configurations for Apple devices.
- Recommended configurations:
    - Security—Fast Transition should be adaptive enabled or enabled. If Fast transition is enabled, the Authentication Key Management should be **psk** or **dot1x**. Layer 3 security should be none. Over the DS needs to be disabled.
    - QOS—WMM policy should be set to required.
    - Advanced—11k Neighbor List or Dual Band should be enabled. 11v BSS Transition should be enabled. WLAN Radio policy should be all or 802.11a or 802.11 a/g. mDNS should be set to gateway mode.
    - Policy—Fastlane should be set in AutoQOS. Egress and Ingress QOS SSID policy should be set to platinum.

Optimized Roaming Disabled

- Description—Optimized roaming should be disabled because Apple devices use the newer 802.11r, 802.11k, or 802.11v roaming improvement.
- Status:
    - Selected—Optimized roaming is disabled.
    - Unselected—Optimized roaming is enabled.
- CLI Option:
    - Enable optimized roaming by entering this command:

```
Device# conf t
Device(config)# ap dot11 5ghz rrm optimized-roam
```

    - Disable optimized roaming by entering this command:

```
Device# conf t
Device(config)# no ap dot11 5ghz rrm optimized-roam
```

5GHz EDCA Fastlane

- Description—Configuring the EDCA Profile as Fastlane improves Apple device performance on 5GHz networks.
- Status:
  - Selected—The 5GHz EDCA Profile is configured as Fastlane.
  - Unselected—The 5GHz EDCA Profile is not configured as Fastlane.
- CLI Option:
  - Enable Fastlane by entering this command:

```
Device# conf t
Device(config)# ap dot11 5ghz edca-parameters fastlane
```

  - Disable Fastlane by entering this command:

```
Device# conf t
Device(config)# no ap dot11 5ghz edca-parameters fastlane
```

5GHz Enabled

- Description—Enable the 5GHz radio to provide a faster and less interfering network for Apple devices.
- Status:
  - Selected—5GHz radio is enabled on the network.
  - Unselected—5GHz radio is disabled on the network.

5GHz MCS Rates

- Description—All the MCS Rates (0-31) should be enabled on the 5GHz networks to help improve the performance of Apple client devices.
- Status:
  - Selected—All the MCS rates are enabled on the 5GHz network.
  - Unselected—Some of the MCS rates are disabled on the 5GHz network.