Client Roaming

In an 802.11 network with multiple APs, the selection of which AP to roam to is primarily made by the client. However, various configurations on the controller and APs can influence the client's roaming choices. Various protocols can inform the client regarding AP availability. Also, the wireless infrastructure can reject client association attempts in efforts to steer the client to a better AP.

Fast SSID Changing

By default, when a client roams between SSIDs, the controller enforces a delay of a few seconds before that client is permitted to associate to the new SSID.

When fast SSID changing is enabled, the controller allows clients to move faster between SSIDs. When fast SSID is enabled, the client entry is not cleared and the delay is not enforced.

This section contains the following subsections:

Configuring Fast SSID Changing (GUI)

Procedure

Step 1 Choose **Controller** to open the General page.

Step 2 From the Fast SSID Change drop-down list, choose **Enabled** to enable this feature or **Disabled** to disable it.

By default, fast SSID changing feature is in disabled state.

Step 3 Click **Apply** to commit your changes.

Step 4 Click **Save Configuration** to save your changes.

Configuring Fast SSID Changing (CLI)

Procedure

Step 1 Enable or disable fast SSID changing by entering this command:

config network fast-ssid-change {**enable** | **disable**}

By default, fast SSID changing feature is in disabled state.

Step 2 Save your changes by entering this command:

save config

802.11k Neighbor List and Assisted Roaming

The 802.11k standard allows an AP to inform 802.11k-capable clients of neighboring BSSIDs (APs in the same SSID). This can help the client to optimize its scanning and roaming behavior. Additionally, the Assisted Roaming Prediction Optimization feature can be used with non-802.11k clients, to discourage them from roaming to suboptimal APs.

Note We recommend not configuring two SSIDs with the same name in the controller, which may cause roaming issues.

Prediction Based Roaming - Assisted Roaming for Non-802.11k Clients

You can optimize roaming for non-802.11k clients by generating a prediction neighbor list for each client without sending an 802.11k neighbor list request. When prediction based roaming enables a WLAN, after each successful client association/re-association, the same neighbor list optimization applies on the non-802.11k client to generate and store the neighbor list in the mobile station software data structure. Clients at different locations have different lists because the client probes are seen with different RSSI values by the different neighbors as the clients usually probe before any association or re-association. This list is created with the most updated probe data and predicts the next AP that the client is likely to roam to.

The wireless infrastructure discourages clients from roaming to those less desirable neighbors by denying association if the association request to an AP does not match the entries on the stored prediction neighbor list.

- Denial count: Maximum number of times a client is refused association.
- Prediction threshold: Minimum number of entries required in the prediction list for the assisted roaming feature to activate.

For more information, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/Enterprise-Mobility-8-5-Design-Guide/Enterprise_Mobility_8-5_Deployment_Guide/Chapter-11.html#pgfId-1140097.

Restrictions for Assisted Roaming

- This feature must be implemented only if you are using one controller. The assisted roaming feature is not supported across multiple controllers.
- This feature is supported only on 802.11n capable indoor access points. For a single band configuration, a maximum of 6 neighbors are visible in a neighbor list. For dual band configuration, a maximum of 12 neighbors are visible.
- You can configure assisted roaming only using the controller CLI. Configuration using the controller GUI is not supported.

Configuring Assisted Roaming (GUI)

Procedure

Step 1 Choose **WLANs**.

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

Step 3 In the **WLANs > Edit** window, click the **Advanced** tab.

Step 4 In the **11k** area, check the **Neighbor List** and **Neighbor List Dual Band** check boxes.

Step 5 Check the **Assisted Roaming Prediction Optimization** check box if you want to optimize roaming for non-802.11k clients by generating a prediction neighbor list for each client without sending an 802.11k neighbor list request.

Step 6 Save the configuration.

Configuring Assisted Roaming (CLI)

Procedure

- Configure an 802.11k neighbor list for a WLAN by entering this command:

  config wlan assisted-roaming neighbor-list {**enable** | **disable**} *wlan-id*

- Configure neighbor floor label bias by entering this command:

  config assisted-roaming floor-bias *dBm*

- Configure a dual-band 802.11k neighbor list for a WLAN by entering this command:

  config wlan assisted-roaming dual-list {**enable** | **disable**} *wlan-id*

Note Default is the band which the client is using to associate.

- Configure Assisted Roaming Prediction List feature for a WLAN by entering this command:

  config wlan assisted-roaming prediction {**enable** | **disable**} *wlan-id*

Note A warning message is displayed and load balancing is disabled for the WLAN if load balancing is already enabled for the WLAN.

- Configure the minimum number of predicted APs required for the prediction list feature to be activated by entering this command:

  config assisted-roaming prediction-minimum *count*

Note If the number of APs in the prediction assigned to a client is less than the number that you specify, the assisted roaming feature will not apply on this roam.

- Configure the maximum number of times a client can be denied association if the association request that is sent to an AP does not match any AP in the prediction list by entering this command:

  config assisted-roaming denial-maximum *count*

- Debug a client for assisted roaming by entering this command:

  debug mac addr *client-mac-addr*

- Configure debugging of all of 802.11k events by entering this command:

  debug 11k all {**enable** | **disable**}

- Configure debugging of neighbor details by entering this command:

  debug 11k detail {**enable** | **disable**}

- Configure debugging of 802.11k errors by entering this command:

  debug 11k errors {**enable** | **disable**}

- Verify if the neighbor requests are being received by entering this command:

  debug 11k events {**enable** | **disable**}

- Configure debugging of the roaming history of clients by entering this command:

  debug 11k history {**enable** | **disable**}

- Configure debugging of 802.11k optimizations by entering this command:

  debug 11k optimization {**enable** | **disable**}

- Get details of the client-roaming parameters that are to be imported for offline simulation by entering this command:

  debug 11k simulation {**enable** | **disable**}

802.11v

From Release 8.1, controller supports 802.11v amendment for wireless networks, which describes numerous enhancements to wireless network management.

One such enhancement is Network assisted Power Savings which helps clients to improve battery life by enabling them to sleep longer. As an example, mobile devices typically use a certain amount of idle period to ensure that they remain connected to access points and therefore consume more power when performing the following tasks while in a wireless network.

Another enhancement is Network assisted Roaming which enables the WLAN to send requests to associated clients, advising the clients as to better APs to associate to. This is useful for both load balancing and in directing poorly connected clients.

Enabling 802.11v Network Assisted Power Savings

Wireless devices consume battery to maintain their connection to the clients, in several ways:

- By waking up at regular intervals to listen to the access point beacons containing a DTIM, which indicates buffered broadcast or multicast traffic that the access point will deliver to the clients.
- By sending null frames to the access points, in the form of keepalive messages– to maintain connection with access points.
- Devices also periodically listen to beacons (even in the absence of DTIM fields) to synchronize their clock to that of the corresponding access point.

All these processes consume battery and this consumption particularly impacts devices (such as Apple), because these devices use a conservative session timeout estimation, and therefore, wake up often to send keepalive messages. The 802.11 standard, without 802.11v, does not include any mechanism for the controller or the access points to communicate to wireless clients about the session timeout for the local client.

To save the power of clients due to the mentioned tasks in wireless network, the following features in the 802.11v standard are used:

- Directed Multicast Service
- Base Station Subsystem (BSS) Max Idle Period

Directed Multicast Service

Using Directed Multicast Service (DMS), the client requests the access point to transmit the required multicast packet as unicast frames. This allows the client to receive the multicast packets it has ignored while in sleep mode and also ensures Layer 2 reliability. Furthermore, the unicast frame will be transmitted to the client at a potentially higher wireless link rate which enables the client to receive the packet quickly by enabling the radio for a shorter duration, thus also saving battery power. Since the wireless client also does not have to wake up at each DTIM interval in order to receive multicast traffic, longer sleeping intervals are allowed.

BSS Max Idle Period

The BSS Max Idle period is the timeframe during which an access point (AP) does not disassociate a client due to nonreceipt of frames from the connected client. This helps ensure that the client device does not send keepalive messages frequently. The idle period timer value is transmitted using the association and reassociation response frame from the access point to the client. The idle time value indicates the maximum time a client can remain idle without transmitting any frame to an access point. As a result, the clients remain in sleep mode for a longer duration without transmitting the keepalive messages often. This in turn contributes to saving battery power.

Restrictions

- If you have enabled optimized roaming, the controller sends a BSS Transition Management (BTM) query to forcibly roam a client. This will enable the dissociation imminent field, irrespective of the WLAN configuration. Load balancing and XOR roaming adhere to the disassociation imminent configuration of the WLAN.

This section contains the following subsections:

Prerequisites for Configuring 802.11v

- This feature is applicable to Apple clients like Apple iPad, iPhone and so on that run on Apple iOS version 7 or later.
- This feature supports local mode; also supports FlexConnect access points in central authentication modes only.
- Not all Cisco APs support all 802.11v features. For more information about which APs support 802.11v, see https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-matrix.html.

Configuring 802.11v Network Assisted Power Savings (CLI)

Procedure

- Configure the value of BSS Max Idle period by entering these commands:
  - **config wlan usertimeout** *wlan-id*
  - **config wlan bssmaxidle** {**enable** | **disable**} *wlan-id*
- Configure DMS by entering this command:

  config wlan dms {**enable** | **disable**} *wlan-id*

Monitoring 802.11v Network Assisted Power Savings (CLI)

Execute the commands described in this section to monitor the DMS and BSS Max Idle time using the CLI.

- Display DMS information on each radio slot on an access point by entering the **show controller d1/d0 | begin DMS** command on the access point.
- Track the DMS requests processed by the controller by entering the following commands:
  - **debug 11v all** {**enable** | **disable**}
  - **debug 11v errors** {**enable** | **disable**}
  - **debug 11v detail** {**enable** | **disable**}
- Enable or disable 802.11v debug by entering the **debug 11v detail** command on the controller.
- Track the DMS requests processed by an access point by entering the **debug dot11 dot11v** command on the access point.

Configuration Examples for 802.11v Network Assisted Power Savings

The following example displays a sample output for the **show wlan** *wlan-id* command with 802.11v parameters:

```
WLAN Identifier.................4
Profile Name...................Mynet
802.11v Directed Multicast Service........Disabled
802.11v BSS Max Idle Service..............Enabled
802.11v BSS Max Idle Protected Mode..............Disabled
802.11v TFS Service..............Disabled
802.11v BSS Transition Service..............Disabled
802.11v WNM Sleep Mode Service..............Disabled
DMS DB is emptyTag: BSS Max Idle Period
Tag number: BSS Max Idle Period (90)
Tag Length: 3
BSS Max Idle Period (1000 TUS) :300
... ...0 = BSS Max Idle Period Options : Protected Keep-Alive Required:0
```

Enabling 802.11v BSS Transition Management

802.11v BSS Transtion is applied in the following three scenarios:

- Solicited request—Client can send an 802.11v Basic Service Set (BSS) Transition Management Query before roaming for a better option of AP to reassociate with.
- Unsolicited Load Balancing request—If an AP is heavily loaded, it sends out an 802.11v BSS Transition Management Request to an associated client.
- Unsolicited Optimized Roaming request—If a client's RSSI and rate do not meet the requirements, the corresponding AP sends out an 802.11v BSS Transition Management Request to this client.

Note 802.11v BSS Transition Management Request is a suggestion (or advice) given to a client, which the client can choose to follow or ignore. To force the task of disassociating a client, turn on the disassociation-imminent function. This disassociates the client after a period of time if the client is not reassociated to another AP.

Guidelines and Restrictions

- Client needs to support 802.11v BSS Transition.
- The disassociation imminent is set to **True** by default when optimized roaming is enabled. This value is set to **True** even when the disassociation imminent disabled in a WLAN.

Enable 802.11v BSS Transition Management on the Controller

To enable 802.11v BSS transition management on a controller, enter the following commands:

config wlan bss-transition enable *wlan-id*

config wlan disassociation-imminent enable *wlan-id*

Troubleshooting

To troubleshoot 802.11v BSS transition, enter the following command:

debug 11v all

Optimized Roaming

Optimized roaming resolves the problem of sticky clients that remain associated to access points that are far away and outbound clients that attempt to connect to a Wi-Fi network without having a stable connection. This feature disassociates clients based on the RSSI of the client data packets and data rate. The client is disassociated if the RSSI alarm condition is met and the current data rate of the client is lower than the optimized roaming data rate threshold. You can disable the data rate option so that only RSSI is used for disassociating clients.

Optimized roaming also prevents client association when the client's RSSI is low. This feature checks the RSSI of the incoming client against the RSSI threshold. This check prevents the clients from connecting to a Wi-Fi network unless the client has a viable connection. In many scenarios, even though clients can hear beacons and connect to a Wi-Fi network, the signal might not be strong enough to support a stable connection.

You can also configure the client coverage reporting interval for a radio by using optimized roaming. The client coverage statistics include data packet RSSIs, Coverage Hole Detection and Mitigation (CHDM) pre-alarm failures, retransmission requests, and current data rates.

Optimized roaming is useful in the following scenarios:

- Addresses the sticky client challenge by proactively disconnecting clients.
- Actively monitors data RSSI packets.
- Disassociates client when the RSSI is lower than the set threshold.

This section contains the following subsections:

Restrictions for Optimized Roaming

- You cannot configure the optimized roaming interval until you disable the 802.11a/b network.
- When basic service set (*BSS*) transition is sent to 802.11v-capable clients, and if the clients are not transitioned to other BSS before the disconnect timer expires, the corresponding client is disconnected forcefully. BSS transition is enabled by default for 802.11v-capable clients.
- We recommend that you do not use the optimized roaming feature with RSSI low check.

Configuring Optimized Roaming (GUI)

Procedure

Step 1 Choose **Wireless > Advanced > Optimized Roaming**. The Optimized Roaming page is displayed.

Step 2 To enable optimized roaming for an 802.11 band, check the **Enable** check box.

You can configure the optimized roaming interval and data rate threshold values only after you enable optimized roaming for an 802.11 band.

Step 3 In the **Optimized Roaming Interval** text box, enter a value for the interval at which an access point reports the client coverage statistics to the controller.

The client coverage statistics include data packet RSSIs, Coverage Hole Detection and Mitigation (CHDM) pre-alarm failures, retransmission requests, and current data rates. The range is from 5 to 90 seconds. The default value is 90 seconds.

Note You must disable the 802.11a/b network before you configure the optimized roaming reporting interval. If you configure a low value for the reporting interval, the network can get overloaded with coverage report messages.

The access point sends the client statistics to the controller based on the following conditions:

- When **Optimized Roaming Interval** is set to 90 seconds by default.
- When **Optimized Roaming Interval** is configured (for instance to 10 secs) only during optimized roaming failure due to Coverage Hole Detection (CHD) RED ALARM.

Step 4 In the **Optimized Roaming Data Rate Threshold** text box, enter a value for the threshold data rate of the client.

The following data rates are available:

- 802.11a—6, 9, 12, 18, 24, 36, 48, and 54.
- 802.11b—1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, and 54.

Optimized roaming disassociates clients based on the RSSI of the client data packet and data rate. The client is disassociated if the current data rate of the client is lower than the Optimized Roaming Data Rate Threshold.

What to do next

Optimized roaming checks the client RSSI at the time of an association. This RSSI value is verified against the configured CHDM RSSI with a 6 db hysteresis. To verify the RSSI threshold configured for coverage hole detection, choose **Wireless > 802.11a/n/ac** or **802.11b/g/n > RRM > Coverage** to open the 802.11a/ac (or 802.11b/g/n) > RRM > Coverage page.

Configuring Optimized Roaming (CLI)

Procedure

Step 1 Enable optimized roaming by entering this command:

ap dot11 5ghz rrm optimized-roam

By default, optimized roaming is disabled.

Step 2 Configure the client coverage reporting interval for 802.11a networks by entering this command:

ap dot11 5ghz rrm optimized-roam reporting-interval *interval-seconds*

The range is from 5 to 90 seconds. The default value is 90 seconds.

Note You must disable the 802.11a network before you configure the optimized roaming reporting interval.

Step 3 Configure the threshold data rate for 802.11a networks by entering this command:

ap dot11 5ghz rrm optimized-roam data-rate-threshold *mbps*

For 802.11a, the configurable data rates are 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54. You can configure DISABLE to disable the data rate.

Step 4 View information about optimized roaming for each band by entering this command:

show ap dot11 5ghz optimized-roaming

```
(Cisco Controller) > show ap dot11 5ghz optimized-roaming
802.11a OptimizedRoaming

  Mode                                  : Disabled
  Reporting Interval                    : 90 seconds
  Rate Threshold                        : Disabled
```

Step 5 View information about optimized roaming statistics by entering this command:

show ap dot11 5ghz optimized-roaming statistics

```
(Cisco Controller) > show ap dot11 5ghz optimized-roaming statistics
802.11a OptimizedRoaming statistics

  Disassociations                       : 0
  Rejections                            : 0
```

Band Select

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 controller.

Band select works by regulating probe responses to clients and it can be enabled on a per-WLAN basis. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels. In an access point, the band select table can be viewed by running the **show dot11 band-select** command. It can also be viewed by running the **show cont d0/d1 | begin Lru** command.

Band Select Algorithm

The band select algorithm affects clients that use 2.4-GHz band. Initially, when a client sends a probe request to an access point, the corresponding client probe's Active and Count values (as seen from the band select table) become 1. The algorithm functions based on the following scenarios:

- Scenario1: Client RSSI (as seen from the **show cont d0/d1** | **begin RSSI**command output) is greater than both Mid RSSI and Acceptable Client RSSI.

- Dual-band clients: No 2.4-GHz probe responses are seen at any time; 5-GHz probe responses are seen for all 5-GHz probe requests.
- Single-band (2.4-GHz) clients: 2.4-GHz probe responses are seen only after the probe suppression cycle.
- After the client's probe count reaches the configured probe cycle count, the algorithm waits for the Age Out Suppression time and then marks the client probe's Active value as 0. Then, the algorithm is restarted.

- Scenario2: Client RSSI (as seen from **show cont d0/d1** | **begin RSSI**) lies between Mid-RSSI and Acceptable Client RSSI.
  - All 2.4-GHz and 5-GHz probe requests are responded to without any restrictions.
  - This scenario is similar to the band select disabled.

Note The client RSSI value (as seen in the **sh cont d0** | **begin RSSI** command output) is the average of the client packets received, and the Mid RSSI feature is the instantaneous RSSI value of the probe packets. As a result, the client RSSI is seen as weaker than the configured Mid RSSI value (7-dB delta). The 802.11b probes from the client are suppressed to push the client to associate with the 802.11a band.

Restrictions for Band Selection

- Band selection-enabled WLANs do not support time-sensitive applications such as voice and video because of roaming delays.
- Band selection is not supported in Cisco Aironet 1600 Series APs.
- Mid-RSSI is unsupported on Cisco Aironet 1600 Series APs.
- Band selection is unsupported on Cisco Aironet 1040, OEAP 600 Series APs.
- Band selection is unsupported on Cisco Aironet 1040, OEAP 600 Series APs.
- Band selection operates only on access points that are connected to a controller. A FlexConnect access point without a controller connection does not perform band selection after a reboot.
- The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.
- You can enable both band selection and aggressive load balancing on the controller. They run independently and do not impact one another.
- It is not possible to enable or disable band selection and client load balancing globally through the controller GUI or CLI. You can, however, enable or disable band selection and client load balancing for a particular WLAN.
- We recommend that you do not use Band Select in high-density areas such as stadiums.

Configuring Band Selection (GUI)

Procedure

Step 1 Choose **Wireless** > **Advanced > Band Select** to open the **Band Select** page.

Step 2 In the **Probe Cycle Count** text box, enter a value between 1 and 10. This cycle count sets the number of 2.4 GHz probe suppression cycles. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.

Step 3 In the **Scan Cycle Period Threshold (milliseconds)** text box, enter a value between 1 and 1000 milliseconds for the scan cycle period threshold. This setting determines the time threshold during which new probe requests from a client come from a new scanning cycle (i.e. only if the time difference between the successive probe requests is greater than this configured value, then the count value in the band select table increases). The default cycle threshold is 200 milliseconds.

Step 4 In the **Age Out Suppression (seconds)** text box, enter a value between 10 and 200 seconds. Age-out suppression sets the expiration time for pruning previously known 802.11b/g/n clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 5 In the **Age Out Dual Band (seconds)** text box, enter a value between 10 and 300 seconds. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 60 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 6 In the **Acceptable Client RSSI (dBm)** text box, enter a value between –20 and –90 dBm. This parameter sets the minimum RSSI for a client to respond to a probe. The default value is –80 dBm.

Step 7 In the **Acceptable Client Mid RSSI (dBm)** text box, enter a value between –20 and –90 dBm. This parameter sets the mid-RSSI, whose value can be used for toggling 2.4 GHz probe suppression based on the RSSI value. The default value is –60 dBm.

Step 8 Click **Apply**.

Step 9 Click **Save Configuration**.

Step 10 To enable or disable band selection on specific WLANs, choose **WLANs** > **WLAN ID**. The **WLANs > Edit** page appears.

Step 11 Click the **Advanced** tab.

Step 12 In the **Load Balancing and Band Select** text area, if you want to enable band selection, select the **Client Band Select** check box. If you want to disable band selection, leave the check box unselected. The default value is disabled.

Step 13 Click **Save Configuration**.

Configuring Band Selection (CLI)

Procedure

Step 1 Set the probe cycle count for band select by entering this command:

config band-select cycle-count *cycle_count*

You can enter a value between 1 and 10 for the *cycle_count* parameter.

Step 2 Set the time threshold for a new scanning cycle period by entering this command:

config band-select cycle-threshold *milliseconds*

You can enter a value for threshold between 1 and 1000 for the *milliseconds* parameter.

Step 3 Set the suppression expire to the band select by entering this command:

config band-select expire suppression *seconds*

You can enter a value for suppression between 10 to 200 for the *seconds* parameter.

Step 4 Set the dual band expire by entering this command:

config band-select expire dual-band *seconds*

You can enter a value for dual band between 10 and 300 for the *seconds* parameter.

Step 5 Set the client RSSI threshold by entering this command:

config band-select client-rssi *client_rssi*

You can enter a value for minimum dBm of a client RSSI to respond to a probe between -20 and -90 for the *client_rssi* parameter.

Step 6 Set the client mid RSSI threshold by entering this command:

config band-select client-mid-rssi *client_mid_rssi*

You can enter a value for mid RSSI between -20 and -90 for the *client_mid_rssi* parameter.

Step 7 Enter the **save config** command to save your changes.

Step 8 Enable or disable band selection on specific WLANs by entering this command:

config wlan band-select allow {**enable** | **disable**} *wlan_ID*

You can enter a value between 1 and 512 for *wlan_ID* parameter.

Step 9 Verify your settings by entering this command:

show band-select

Information similar to the following appears:

```
Band Select Probe Response..................... Enabled
   Cycle Count................................. 3 cycles
   Cycle Threshold............................. 300 milliseconds
   Age Out Suppression......................... 20 seconds
   Age Out Dual Band........................... 20 seconds
   Client RSSI................................. -30 dBm
   Client Mid RSSI............................. -80 dBm
```

Step 10 Enter the **save config** command to save your changes.