Client Roaming

Fast SSID Changing

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.

When fast SSID changing is disabled, the controller enforces a delay before clients are allowed to move to a new SSID. When fast SSID is disabled and the client sends a new association for a different SSID, the client entry in the controller connection table is cleared before the client is added to the new SSID.

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. The default value is disabled.

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**}

Step 2 Save your changes by entering this command:

save config

Assisted Roaming

The 802.11k standard allows clients to request neighbor reports containing information about known neighbor access points that are candidates for a service set transition. The use of the 802.11k neighbor list can limit the need for active and passive scanning.

The assisted roaming feature is based on an intelligent and client optimized neighbor list.

Unlike the Cisco Client Extension (CCX) neighbor list, the 802.11k neighbor list is generated dynamically on-demand and is not maintained on the controller. The 802.11k neighbor list is based on the location of the clients without requiring the mobility services engine (MSE). Two clients on the same controller but different APs can have different neighbor lists delivered depending on their individual relationship with the surrounding APs.

By default, the neighbor list contains only neighbors in the same band with which the client is associated. However, a switch exists that allows 802.11k to return neighbors in both bands.

Clients send requests for neighbor lists only after associating with the APs that advertize the RRM (Radio Resource Management) capability information element (IE) in the beacon. The neighbor list includes information about BSSID, channel, and operation details of the neighboring radios.

Assembling and Optimizing the Neighbor List

When the controller receives a request for an 802.11k neighbor list, the following occurs:

1. The controller searches the RRM neighbor table for a list of neighbors on the same band as the AP with which the client is currently associated with.
2. The controller checks the neighbors according to the RSSI (Received Signal Strength Indication) between the APs, the current location of the present AP, the floor information of the neighboring AP from Cisco Prime Infrastructure, and roaming history information on the controller to reduce the list of neighbors to six per band. The list is optimized for APs on the same floor.

Assisted Roaming for Non-802.11k Clients

It is also possible to optimize roaming for non-802.11k clients. You can generate a prediction neighbor list for each client without the client requiring to send an 802.11k neighbor list request. When this is enabled on a WLAN, after each successful client association/reassociation, the same neighbor list optimization is applied

on the non-802.11k client to generate the neighbor list and store the 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 different neighbors. Because clients usually probe before any association or reassociation, this list is constructed with the most updated probe data and predicts the next AP that the client is likely to roam to.

We discourage 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.

Similar to aggressive load balancing, there is a switch to turn on the assisted roaming feature both on a per-WLAN basis and globally. The following options are available:

- 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 be activated.

Because both load balancing and assisted roaming are designed to influence the AP that a client associates with, it is not possible to enable both the options at the same time on a WLAN.

This section contains the following subsections:

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 (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.

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 WLC.
- 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 BSS Max Idle period value seen in an access point's association and reassociation response:

```
  Tag: 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
```

The following example displays the DMS information (if enabled) for each client in an access point:

```
Global DMS - requests:1 uc:0 drop:0
DMS enabled on WLAN(s): 11v
DMS Database:
Entry 1: mask=0x55 version=4 dstIp=0xE00000FB srcIp=0x00000000 dstPort=9 srcPort=0 dcsp=0
protocol=17
{Client, SSID}: {8C:29:37:7B:D0:4E, 11v},
```

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 Cisco WLC

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

802.11 Bands

You can configure the 802.11b/g/n (2.4 GHz) and 802.11a/n/ac (5 GHz) bands for the controller to comply with the regulatory requirements in your country. By default, both 802.11b/g/n and 802.11a/n/ac are enabled.

When a controller is configured to allow only 802.11g traffic, 802.11b client devices are able to successfully connect to an access point, but cannot pass traffic. When you configure the controller only for 802.11g traffic, you must mark 11g rates as mandatory.

Note The Block Acks in a Cisco 2800, 3800, 1560 APs are sent at configured mandatory data rates in controller for 2.4 GHz radio.

This section contains the following subsections:

Configuring the 802.11 Bands (GUI)

Procedure

Step 1 Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Network** to open the **Global Parameters** page.

Step 2 Select the **802.11a** (or **802.11b/g**) **Network Status** check box to enable the 802.11a or 802.11b/g band. To disable the band, unselect the check box. The default value is enabled. You can enable both the 802.11a and 802.11b/g bands.

Step 3 If you enabled the 802.11b/g band in *Step 2*, select the **802.11g Support** check box if you want to enable 802.11g network support. The default value is enabled. If you disable this feature, the 802.11b band is enabled without 802.11g support.

Step 4 Specify the period at which the SSID is broadcast by the access point by entering a value between 20 and 1000 milliseconds (inclusive) in the Beacon Period text box. The default value is 100 milliseconds.

Note The beacon period in controllers is listed in terms of milliseconds. The beacon period can also be measured in time units, where one time unit equals 1024 microseconds or 102.4 milliseconds. If a beacon interval is listed as 100 milliseconds in a controller, it is only a rounded off value for 102.4 milliseconds. Due to hardware limitation in certain radios, even though the beacon interval is, say 100 time units, it is adjusted to 102 time units, which roughly equals 104.448 milliseconds. When the beacon period is to be represented in terms of time units, the value is adjusted to the nearest multiple of 17.

Step 5 Specify the size at which packets are fragmented by entering a value between 256 and 2346 bytes (inclusive) in the Fragmentation Threshold text box. Enter a low number for areas where communication is poor or where there is a great deal of radio interference.

Step 6 Make access points advertise their channel and transmit power level in beacons and probe responses for CCX clients. Select the **DTPC Support** check box. Otherwise, unselect this check box. The default value is enabled.

Client devices using dynamic transmit power control (DTPC) receive the channel and power level information from the access points and adjust their settings automatically. For example, a client device used primarily in Japan could rely on DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there.

Note On access points that run Cisco IOS software, this feature is called *world mode*.

Note DTPC and 801.11h power constraint cannot be enabled simultaneously.

Step 7 Specify the maximum allowed clients by entering a value between 1 to 200 in the Maximum Allowed Client text box. The default value is 200.

Step 8 Select or unselect the **RSSI Low Check** check box to enable or disable the RSSI Low Check feature.

Step 9 Enter the **RSSI Threshold** value.

The default value is –80 dBm.

Step 10 Use the Data Rates options to specify the rates at which data can be transmitted between the access point and the client. These data rates are available:

- 802.11a—6, 9, 12, 18, 24, 36, 48, and 54 Mbps
- 802.11b/g—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps

For each data rate, choose one of these options:

- **Mandatory**—Clients must support this data rate in order to associate to an access point on the controller.
- **Supported**—Any associated clients that support this data rate may communicate with the access point using that rate. However, the clients are not required to be able to use this rate in order to associate.
- **Disabled**—The clients specify the data rates used for communication.

Step 11 Click **Apply**.

Step 12 Click **Save Configuration**.

Configuring the 802.11 Bands (CLI)

Procedure

Step 1 Disable the 802.11a band by entering this command:

config 802.11a disable network

Note The 802.11a band must be disabled before you can configure the 802.11a network parameters in this section.

Step 2 Disable the 802.11b/g band by entering this command:

config 802.11b disable network

Note The 802.11b band must be disabled before you can configure the 802.11b network parameters in this section.

Step 3 Specify the rate at which the SSID is broadcast by the access point by entering this command:

config {**802.11a** | **802.11b**} **beaconperiod** *time_unit*

where *time_unit* is the beacon interval in time units (TUs). One TU is 1024 microseconds. You can configure the access point to send a beacon every 20 to 1000 milliseconds.

Step 4 Specify the size at which packets are fragmented by entering this command:

config {**802.11a** | **802.11b**} **fragmentation** *threshold*

where *threshold* is a value between 256 and 2346 bytes (inclusive). Specify a low number for areas where communication is poor or where there is a great deal of radio interference.

Step 5 Make access points advertise their channel and transmit power level in beacons and probe responses by entering this command:

config {**802.11a** | **802.11b** } **dtpc** {**enable** | **disable**}

The default value is enabled. Client devices using dynamic transmit power control (DTPC) receive the channel and power level information from the access points and adjust their settings automatically. For example, a client device used primarily in Japan could rely on DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there.

Note On access points that run Cisco IOS software, this feature is called *world mode*.

Step 6 Specify the maximum allowed clients that can be configured by entering this command:

config {**802.11a** | **802.11b**} **max-clients** *max_allow_clients*

The valid range is between 1 to 200.

Step 7 Configure the RSSI Low Check feature by entering this command:

config 802.11{**a** | **b**} **rssi-check** {**enable** | **disable**}

Step 8 Configure the RSSI Threshold value by entering this command:

config 802.11{**a** | **b**} **rssi-threshold** *value-in-dBm*

Note The default value is –80 dBm.

Step 9 Specify the rates at which data can be transmitted between the controller and the client by entering this command:

config {**802.11a** | **802.11b**} **rate** {**disabled** | **mandatory** | **supported**} *rate*

where

- **disabled**—Clients specify the data rates used for communication.
- **mandatory**—Clients support this data rate in order to associate to an access point on the controller.
- **supported**—Any associated clients that support this data rate may communicate with the access point using that rate. However, the clients are not required to be able to use this rate in order to associate.
- *rate*—The rate at which data is transmitted:
  - 6, 9, 12, 18, 24, 36, 48, and 54 Mbps (802.11a)
  - 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps (802.11b/g)

Step 10 Enable the 802.11a band by entering this command:

config 802.11a enable network

The default value is enabled.

Step 11 Enable the 802.11b band by entering this command:

config 802.11b enable network

The default value is enabled.

Step 12 Enable or disable 802.11g network support by entering this command:

config 802.11b 11gSupport {**enable** | **disable**}

The default value is enabled. You can use this command only if the 802.11b band is enabled. If you disable this feature, the 802.11b band is enabled without 802.11g support.

Step 13 Enter the **save config** command to save your changes.

Step 14 View the configuration settings for the 802.11a or 802.11b/g band by entering this command:

show {**802.11a** | **802.11b**}

Information similar to the following appears:

```
802.11a Network.............................. Enabled
11nSupport................................... Enabled
      802.11a Low Band....................... Enabled
      802.11a Mid Band....................... Enabled
      802.11a High Band...................... Enabled
802.11a Operational Rates
    802.11a 6M Rate.......................... Mandatory
    802.11a 9M Rate.......................... Supported
    802.11a 12M Rate......................... Mandatory
    802.11a 18M Rate......................... Supported
    802.11a 24M Rate......................... Mandatory
    802.11a 36M Rate......................... Supported
```

```
    802.11a 48M Rate.............................. Supported
    802.11a 54M Rate.............................. Supported
...
Beacon Interval.................................. 100
...
Default Channel.............................. 36
Default Tx Power Level....................... 1
DTPC Status.................................. Enabled
Fragmentation Threshold...................... 2346
Maximum Number of Clients per AP................. 200
```

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) prealarm 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 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.
- The Cisco Catalyst 9800 controller increments the 80211v smart roam failed counter while disconnecting the client due to optimized roaming.
- When CPU utilization is high, the controller drops the packets. Whenever roaming fails and clients try to re-authenticate the CPU usage is very high. When the 802.11r client roams, high CPU utilization is

consumed and the controller receives RFID packets at a high rate. The packets then get dropped due to high CPU utilization. As packets are droppped randomly at the queue, it results in roam failure. Ideally, you must limit the rate of RFID traffic by changing the low priority queue size to 500.

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
```

CCX Layer 2 Client Roaming

The controller supports five CCX Layer 2 client roaming enhancements:

- Access point assisted roaming—This feature helps clients save scanning time. When a CCXv2 client associates to an access point, it sends an information packet to the new access point listing the characteristics of its previous access point. Roaming time decreases when the client recognizes and uses

an access point list built by compiling all previous access points to which each client was associated and sent (unicast) to the client immediately after association. The access point list contains the channels, BSSIDs of neighbor access points that support the client's current SSID(s), and time elapsed since disassociation.

- Enhanced neighbor list—This feature focuses on improving a CCXv4 client's roam experience and network edge performance, especially when servicing voice applications. The access point provides its associated client information about its neighbors using a neighbor-list update unicast message.
- Enhanced neighbor list request (E2E)—The End-2-End specification is a Cisco and Intel joint program that defines new protocols and interfaces to improve the overall voice and roaming experience. It applies only to Intel clients in a CCX environment. Specifically, it enables Intel clients to request a neighbor list at will. When this occurs, the access point forwards the request to the controller. The controller receives the request and replies with the current CCX roaming sublist of neighbors for the access point to which the client is associated.

Note To see whether a particular client supports E2E, choose **Wireless** > **Clients** on the controller GUI, click the **Detail** link for the desired client, and look at the E2E Version text box in the Client Properties area.

- Roam reason report—This feature enables CCXv4 clients to report the reason why they roamed to a new access point. It also allows network administrators to build and monitor a roam history.
- Directed roam request—This feature enables the controller to send directed roam requests to the client in situations when the controller can better service the client on an access point different from the one to which it is associated. In this case, the controller sends the client a list of the best access points that it can join. The client can either honor or ignore the directed roam request. Non-CCX clients and clients running CCXv3 or below must not take any action. No configuration is required for this feature.

This section contains the following subsections:

Restrictions for Client Roaming

- CCX versions 1 through 5 are supported. CCX support is enabled automatically for every WLAN on the controller and cannot be disabled. The controller stores the CCX version of the client in its client database and uses it to generate and respond to CCX frames appropriately. Clients must support CCXv4 or v5 (or CCXv2 for access point assisted roaming) in order to utilize these roaming enhancements.

  The roaming enhancements mentioned above are enabled automatically, with the appropriate CCX support.
- FlexConnect access points in standalone mode do not support CCX Layer 2 roaming.
- Seamless L2 and L3 roaming is not supported between a Cisco and a third-party wireless infrastructure, which also includes a Cisco IOS access point.

Configuring CCX Client Roaming Parameters (GUI)

Procedure

Step 1 Choose **Wireless** > **802.11a/n/ac or 802.11b/g/n** > **Client Roaming**. The 802.11a (802.11b) > Client Roaming page appears.

Step 2 If you want to fine-tune the RF parameters that affect client roaming, choose **Custom** from the **Mode** drop-down list and go to *Step 3*. If you want to leave the RF parameters at their default values, choose **Default** and go to *Step 8*.

Step 3 In the **Minimum RSSI** text box, enter a value for the minimum received signal strength indicator (RSSI) required for the client to associate to an access point. If the client's average received signal power dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.

The range is –90 to –50 dBm.

The default is –85 dBm.

Step 4 In the **Hysteresis** text box, enter a value to indicate how much greater the signal strength of a neighboring access point must be in order for the client to roam to it. This parameter is intended to reduce the amount of roaming between access points if the client is physically located on or near the border between two access points.

The range is 3 to 20 dB.

The default is 3 dB.

Step 5 In the **Scan Threshold** text box, enter the minimum RSSI that is allowed before the client should roam to a better access point. When the RSSI drops below the specified value, the client must be able to roam to a better access point within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when the RSSI is below the threshold.

The range is –90 to –50 dBm.

The default is –72 dBm.

Step 6 In the **Transition Time** text box, enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client's associated access point is below the scan threshold.

The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.

The range is 1 to 5 seconds.

The default is 5 seconds.

Step 7 Click **Apply**.

Step 8 Click **Save Configuration**.

Step 9 Repeat this procedure if you want to configure client roaming for another radio band.

Configuring CCX Client Roaming Parameters (CLI)

Configure CCX Layer 2 client roaming parameters by entering this command:

config {**802.11a** | **802.11b**} **l2roam rf-params** {**default** | **custom** *min_rssi roam_hyst scan_thresh trans_time*}

Obtaining CCX Client Roaming Information (CLI)

Procedure

Step 1 View the current RF parameters configured for client roaming for the 802.11a or 802.11b/g network by entering this command:

show {**802.11a** | **802.11b**} **l2roam rf-param**

Step 2 View the CCX Layer 2 client roaming statistics for a particular access point by entering this command:

show {**802.11a** | **802.11b**} **l2roam statistics** *ap_mac*

This command provides the following information:

- The number of roam reason reports received
- The number of neighbor list requests received
- The number of neighbor list reports sent
- The number of broadcast neighbor updates sent

Step 3 View the roaming history for a particular client by entering this command:

show client roam-history *client_mac*

This command provides the following information:

- The time when the report was received
- The MAC address of the access point to which the client is currently associated
- The MAC address of the access point to which the client was previously associated
- The channel of the access point to which the client was previously associated
- The SSID of the access point to which the client was previously associated
- The time when the client disassociated from the previous access point
- The reason for the client roam

Debugging CCX Client Roaming Issues (CLI)

If you experience any problems with CCX Layer 2 client roaming, enter this command:

debug l2roam [**detail** | **error** | **packet** | **all]** {**enable** | **disable**}