Configuring RF Groups

Information About RF Groups

An RF group is a logical collection of Cisco WLCs that coordinate to perform RRM in a globally optimized manner to perform network calculations on a per-radio basis. An RF group exists for each 802.11 network type. Clustering Cisco WLCs into a single RF group enable the RRM algorithms to scale beyond the capabilities of a single Cisco WLC.

RF group is created based on following parameters:

- User-configured RF network name.
- Neighbor discovery performed at the radio level.
- Country list configured on MC.

RF grouping runs between MCs.

Lightweight access points periodically send out neighbor messages over the air. Access points using the the same RF group name validate messages from each other.

When access points on different Cisco WLCs hear validated neighbor messages at a signal strength of −80 dBm or stronger, the Cisco WLCs dynamically form an RF neighborhood in auto mode. In static mode, the leader is manually selected and the members are added to the RF Group. To know more about RF Group modes, RF Group Leader.

Note   RF groups and mobility groups are similar in that they both define clusters of Cisco WLCs, but they are different in terms of their use. An RF group facilitates scalable, system-wide dynamic RF management while a mobility group facilitates scalable, system-wide mobility and Cisco WLC redundancy.

RF Group Leader

Starting in the 7.0.116.0 release, the RF Group Leader can be configured in two ways as follows:

- Auto Mode—In this mode, the members of an RF group elect an RF group leader to maintain a "master" power and channel scheme for the group. The RF grouping algorithm dynamically chooses the RF group leader and ensures that an RF group leader is always present. Group leader assignments can and do change (for instance, if the current RF group leader becomes inoperable or if RF group members experience major changes).

- Static Mode—In this mode, the user selects a Cisco WLC as an RF group leader manually. In this mode, the leader and the members are manually configured and are therefore fixed. If the members are unable to join the RF group, the reason is indicated. The leader tries to establish a connection with a member every 1 minute if the member has not joined in the previous attempt.

The RF group leader analyzes real-time radio data collected by the system, calculates the power and channel assignments, and sends them to each of the Cisco WLCs in the RF group. The RRM algorithms ensure system-wide stability and restrain channel and power scheme changes to the appropriate local RF neighborhoods.

In Cisco WLC software releases prior to 6.0, the dynamic channel assignment (DCA) search algorithm attempts to find a good channel plan for the radios associated to Cisco WLCs in the RF group, but it does not adopt a new channel plan unless it is considerably better than the current plan. The channel metric of the worst radio in both plans determines which plan is adopted. Using the worst-performing radio as the single criterion for adopting a new channel plan can result in pinning or cascading problems.

Pinning occurs when the algorithm could find a better channel plan for some of the radios in an RF group but is prevented from pursuing such a channel plan change because the worst radio in the network does not have any better channel options. The worst radio in the RF group could potentially prevent other radios in the group from seeking better channel plans. The larger the network, the more likely pinning becomes.

Cascading occurs when one radio's channel change results in successive channel changes to optimize the remaining radios in the RF neighborhood. Optimizing these radios could lead to their neighbors and their neighbors' neighbors having a suboptimal channel plan and triggering their channel optimization. This effect could propagate across multiple floors or even multiple buildings, if all the access point radios belong to the same RF group. This change results in considerable client confusion and network instability.

The main cause of both pinning and cascading is the way in which the search for a new channel plan is performed and that any potential channel plan changes are controlled by the RF circumstances of a single radio. In Cisco WLC software release 6.0, the DCA algorithm has been redesigned to prevent both pinning and cascading. The following changes have been implemented:

- Multiple local searches—The DCA search algorithm performs multiple local searches initiated by different radios within the same DCA run rather than performing a single global search driven by a single radio. This change addresses both pinning and cascading while maintaining the desired flexibility and adaptability of DCA and without jeopardizing stability.

- Multiple channel plan change initiators (CPCIs)—Previously, the single worst radio was the sole initiator of a channel plan change. Now each radio within the RF group is evaluated and prioritized as a potential initiator. Intelligent randomization of the resulting list ensures that every radio is eventually evaluated, which eliminates the potential for pinning.

- Limiting the propagation of channel plan changes (Localization)—For each CPCI radio, the DCA algorithm performs a local search for a better channel plan, but only the CPCI radio itself and its one-hop

neighboring access points are actually allowed to change their current transmit channels. The impact of an access point triggering a channel plan change is felt only to within two RF hops from that access point, and the actual channel plan changes are confined to within a one-hop RF neighborhood. Because this limitation applies across all CPCI radios, cascading cannot occur.

- Non-RSSI-based cumulative cost metric—A cumulative cost metric measures how well an entire region, neighborhood, or network performs with respect to a given channel plan. The individual cost metrics of all access points in that area are considered in order to provide an overall understanding of the channel plan's quality. These metrics ensure that the improvement or deterioration of each single radio is factored into any channel plan change. The objective is to prevent channel plan changes in which a single radio improves but at the expense of multiple other radios experiencing a considerable performance decline.

The RRM algorithms run at a specified updated interval, which is 600 seconds by default. Between update intervals, the RF group leader sends keepalive messages to each of the RF group members and collects real-time RF data.

Note Several monitoring intervals are also available. See the Configuring RRM section for details.

RF Group Name

A Cisco WLC is configured with an RF group name, which is sent to all access points joined to the Cisco WLC and used by the access points as the shared secret for generating the hashed MIC in the neighbor messages. To create an RF group, you configure all of the Cisco WLCs to be included in the group with the same RF group name.

If there is any possibility that an access point joined to a Cisco WLC may hear RF transmissions from an access point on a different Cisco WLC, you should configure the Cisco WLCs with the same RF group name. If RF transmissions between access points can be heard, then system-wide RRM is recommended to avoid 802.11 interference and contention as much as possible.

Controllers and APs in RF Groups

- Controller software supports up to 20 controllers and 6000 access points in an RF group.

- The RF group members are added based on the following criteria:

  ◦ Maximum number of APs Supported: The maximum limit for the number of access points in an RF group is 6000. The number of access points supported is determined by the number of APs licensed to operate on the controller.

  ◦ Twenty controllers: Only 20 controllers (including the leader) can be part of an RF group if the sum of the access points of all controllers combined is less than or equal to the upper access point limit.

Table 1: Controller Model Information

	8500	7500	5500	WiSM2
Maximum APs per RRM Group	6000	6000	1000	2000
Maximum AP Groups	6000	6000	500	500

Configuring RF Groups

This section describes how to configure RF groups through either the GUI or the CLI.

> **Note** The RF group name is generally set at deployment time through the Startup Wizard. However, you can change it as necessary.

> **Note** When the multiple-country feature is being used, all Cisco WLCs intended to join the same RF group must be configured with the same set of countries, configured in the same order.

> **Note** You can also configure RF groups using the Cisco Prime Infrastructure.

Configuring an RF Group Name (GUI)

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

Step 2 Enter a name for the RF group in the RF-Network Name text box. The name can contain up to 19 ASCII characters.

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

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

Step 5 Repeat this procedure for each controller that you want to include in the RF group.

Configuring an RF Group Name (CLI)

Step 1 Create an RF group by entering the **config network rf-network-name name** command:

Note   Enter up to 19 ASCII characters for the group name.

Step 2   See the RF group by entering the **show network** command.

Step 3   Save your settings by entering the **save config** command.

Step 4   Repeat this procedure for each controller that you want to include in the RF group.

Viewing the RF Group Status

This section describes how to view the status of the RF group through either the GUI or the CLI.

Note   You can also view the status of RF groups using the Cisco Prime Infrastructure.

Viewing the RF Group Status (GUI)

Step 1   Choose **Wireless** > **802.11a/n/ac** > **or 802.11b/g/n > RRM** > **RF Grouping** to open the 802.11a/n/ac (or 802.11b/g/n) RRM > RF Grouping page.

This page shows the details of the RF group, displaying the configurable parameter **RF Group mode**, the **RF Group role** of this Cisco WLC, the **Update Interval** and the Cisco WLC name and IP address of the **Group Leader** to this Cisco WLC.

Note   RF grouping mode can be set using the **Group Mode** drop-down list.

Tip Once a Cisco WLC has joined as a static member and you want to change the grouping mode, we recommend that you remove the member from the configured static-leader and also make sure that a member Cisco WLC has not been configured to be a member on multiple static leaders. This is to avoid repeated join attempts from one or more RF static leaders.

Step 2   (Optional) Repeat this procedure for the network type that you did not select (802.11a/n/ac or 802.11b/g/n).

Viewing the RF Group Status (CLI)

Step 1   See which Cisco WLC is the RF group leader for the 802.11a RF network by entering this command:
show advanced 802.11a group

Information similar to the following appears:

```
Radio RF Grouping
   802.11a Group Mode.............................. STATIC
   802.11a Group Update Interval.................. 600 seconds
   802.11a Group Leader........................... test (209.165.200.225)
      802.11a Group Member........................ test (209.165.200.225)
   802.11a Last Run.............................. 397 seconds ago
```

This output shows the details of the RF group, specifically the grouping mode for the Cisco WLC, how often the group information is updated (600 seconds by default), the IP address of the RF group leader, the IP address of this Cisco WLC, and the last time the group information was updated.

Note   If the IP addresses of the group leader and the group member are identical, this Cisco WLC is currently the group leader.

Note   A * indicates that the Cisco WLC has not joined as a static member.

Step 2   See which Cisco WLC is the RF group leader for the 802.11b/g RF network by entering this command:
show advanced 802.11b group

Configuring Rogue Access Point Detection in RF Groups

Information About Rogue Access Point Detection in RF Groups

After you have created an RF group of Cisco WLCs, you need to configure the access points connected to the Cisco WLCs to detect rogue access points. The access points will then select the beacon/probe-response frames in neighboring access point messages to see if they contain an authentication information element (IE) that matches that of the RF group. If the select is successful, the frames are authenticated. Otherwise, the authorized access point reports the neighboring access point as a rogue, records its BSSID in a rogue table, and sends the table to the Cisco WLC.

Configuring Rogue Access Point Detection in RF Groups

Enabling Rogue Access Point Detection in RF Groups (GUI)

Step 1   Make sure that each Cisco WLC in the RF group has been configured with the same RF group name.
Note   The name is used to verify the authentication IE in all beacon frames. If the Cisco WLCs have different names, false alarms will occur.

Step 2   Choose **Wireless** to open the All APs page.

Step 3   Click the name of an access point to open the All APs > Details page.

Step 4   Choose either **local** or **monitor** from the AP Mode drop-down list and click **Apply** to commit your changes.

Step 5   Click **Save Configuration** to save your changes.

Step 6   Repeat Step 2 through Step 5 for every access point connected to the Cisco WLC.

Step 7   Choose **Security** > **Wireless Protection Policies** > **AP Authentication/MFP** to open the AP Authentication Policy page.
The name of the RF group to which this Cisco WLC belongs appears at the top of the page.

Step 8   Choose **AP Authentication** from the Protection Type drop-down list to enable rogue access point detection.

Step 9   Enter a number in the Alarm Trigger Threshold edit box to specify when a rogue access point alarm is generated. An alarm occurs when the threshold value (which specifies the number of access point frames with an invalid authentication IE) is met or exceeded within the detection period.
   Note   The valid threshold range is from1 to 255, and the default threshold value is 1. To avoid false alarms, you may want to set the threshold to a higher value.

Step 10   Click **Apply** to commit your changes.

Step 11   Click **Save Configuration** to save your changes.

Step 12   Repeat this procedure on every Cisco WLC in the RF group.
   Note   If rogue access point detection is not enabled on every Cisco WLC in the RF group, the access points on the Cisco WLCs with this feature disabled are reported as rogues.

Configuring Rogue Access Point Detection in RF Groups (CLI)

Step 1   Make sure that each Cisco WLC in the RF group has been configured with the same RF group name.
   Note   The name is used to verify the authentication IE in all beacon frames. If the Cisco WLCs have different names, false alarms will occur.

Step 2   Configure a particular access point for local (normal) mode or monitor (listen-only) mode by entering this command:
config ap mode local *Cisco_AP* or **config ap mode monitor** *Cisco_AP*

Step 3   Save your changes by entering this command:
save config

Step 4   Repeat *Step 2* and *Step 3* for every access point connected to the Cisco WLC.

Step 5   Enable rogue access point detection by entering this command:
config wps ap-authentication

Step 6   Specify when a rogue access point alarm is generated by entering this command. An alarm occurs when the threshold value (which specifies the number of access point frames with an invalid authentication IE) is met or exceeded within the detection period.
config wps ap-authentication *threshold*

   Note   The valid threshold range is from 1 to 255, and the default threshold value is 1. To avoid false alarms, you may want to set the threshold to a higher value.

Step 7   Save your changes by entering this command:

save config

Step 8   Repeat *Step 5* through *Step 7* on every Cisco WLC in the RF group.

Note   If rogue access point detection is not enabled on every Cisco WLC in the RF group, the access points on the Cisco WLCs with this feature disabled are reported as rogues.