



## Configuring RF Groups

---

- [Information About RF Groups, on page 1](#)
- [Controllers and APs in RF Groups, on page 4](#)
- [Configuring RF Groups, on page 5](#)
- [Viewing the RF Group Status, on page 5](#)
- [Configuring Rogue Access Point Detection in RF Groups, on page 7](#)

## Information About RF Groups

An RF group is a logical collection of controllers that coordinate to perform RRM in a globally optimized manner to perform network calculations on a per-radio basis. Separate RF groups exist for 2.4-GHz and 5-GHz networks. Clustering WLCs into a single RF group enables the RRM algorithms to scale beyond the capabilities of a single WLC .

An RF group is created based on the following parameters:

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

RF grouping runs between MCs.

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

When access points on different controllers hear validated neighbor messages at a signal strength of  $-80$  dBm or stronger, the controllers 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.



---

**Note**

RF groups and mobility groups are similar, in that, they both define clusters of controllers , 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 controller redundancy.

---

## RF Group Leader

RF Group Leader can be configured in two ways as follows:



### Note

RF Group Leader is chosen on the basis of the controller with the greatest AP capacity (platform limit.) If multiple controllers have the same capacity, the leader is the one with the highest management IP address.

- **Auto Mode:** In this mode, the members of an RF group elect an RF group leader to maintain a *primary* 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 RF group members experience major changes).
- **Static Mode:** In this mode, a user selects a controller as an RF group leader manually. In this mode, the leader and the members are manually configured and 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 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 controllers in the RF group. The RRM algorithms ensure system-wide stability, and restrain channel and power scheme changes to the appropriate local RF neighborhoods.



### Note

When a controller becomes both leader and member for a specific radio, you get to view the IPv4 and IPv6 address as part of the group leader.

When a Controller A becomes a member and Controller B becomes a leader, the Controller A displays either IPv4 or IPv6 address of Controller B using the address it is connected.

So, if both leader and member are not the same, you get to view only one IPv4 or IPv6 address as a group leader in the member.

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 Grouping Failure Reason Codes

RF Grouping failure reason codes and their explanations are listed below:

Table 1: RF Grouping Failure Reason Codes

Reason Code	Description
1	Maximum number (20) of controllers are already present in the group.
2	If the following conditions are met: <ul style="list-style-type: none"> <li>• The request is from a similar powered controller and, <ul style="list-style-type: none"> <li>• Controller is the leader for the other band,</li> </ul> OR <ul style="list-style-type: none"> <li>• Requestor group is larger.</li> </ul> </li> </ul>
3	Group ID do not match.
4	Request does not include source type.
5	Group spilt message to all member while group is being reformed.
6	Auto leader is joining a static leader, during the process deletes all the members.
9	Grouping mode is turned off.
11	Country code does not match.
12	Controller is up in hierarchy compared to sender of join command (static mode). Requestor is up in hierarchy (auto mode).
13	Controller is configured as static leader and receives join request from another static leader.
14	Controller is already a member of static group and receives a join request from another static leader.
15	Controller is a static leader and receives join request from non-static member.
16	Join request is not intended to the controller. Controller name and IP do not match.
18	RF domain do not match.
19	Controller received a Hello packet at incorrect state.
20	Controller has already joined Auto leader, now gets a join request from static leader.

Reason Code	Description
21	Group mode change. Domain name change from CLI. Static member is removed from CLI.
22	Max switch size (350) is reached

### Additional Reference

*Radio Resource Management White Paper:* [https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b\\_RRM\\_White\\_Paper/b\\_RRM\\_White\\_Paper\\_chapter\\_011.html](https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_RRM_White_Paper/b_RRM_White_Paper_chapter_011.html)

## RF Group Name

A controller is configured in an RF group name, which is sent to all the access points joined to the controller 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 controllers to be included in the group with the same RF group name.

If there is any possibility that an access point joined to a controller might hear RF transmissions from an access point on a different controller, you should configure the controller 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 that are 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 2: Controller Model Information**

	8500	7500	5500	WiSM2
Maximum APs per RRM Group	6000	6000	1000	1000
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 controllers 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** For the group name, the limit is 19 ASCII characters.
- Step 2** See the RF group by entering the **show network summary** 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 > or 802.11b/g/n > RRM > RF Grouping** to open the 802.11a/n (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 or 802.11b/g/n).

## Viewing the RF Group Status (CLI)

**Step 1** See which controller 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 controller, how often the group information is updated (600 seconds by default), the IP address of the RF group leader, the IP address of this controller, 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 controller is currently the group leader.

**Note** A \* indicates that the controller has not joined as a static member.

**Step 2** See which controller 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

## Rogue Access Point Detection in RF Groups

After you have created an RF group of controller , you need to configure the access points connected to the controller to detect rogue access points. The access points will then select the beacon or 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 selection 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 controller .

## Configuring Rogue Access Point Detection in RF Groups

### Enabling Rogue Access Point Detection in RF Groups (GUI)

---

- Step 1** Make sure that each controller 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 controllers 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 controller.
- 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 controller 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 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 10** Click **Apply** to commit your changes.
- Step 11** Click **Save Configuration** to save your changes.
- Step 12** Repeat this procedure on every controller in the RF group.

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

---

## Configuring Rogue Access Point Detection in RF Groups (CLI)

---

**Step 1** Make sure that each controller 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 controllers 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 controller.

**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 controller in the RF group.

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

---