



# Radio Resource Management–Radio Frequency Grouping Algorithm

**Last Updated: November, 2013**

**Release: Radio Resource Management-Radio Frequency Grouping Algorithm, Release 7.4**

## Common Terms and Acronyms for Radio Resource Management

Term	Acronym/Description
RRM	Radio Resource Management
RF Group Name	The Radio Frequency (RF) Group Name is a user assigned name that will be shared with all other Wireless LAN Controllers (WLCs) and Access Points (APs) which are to be included in the RF Network.
RF Grouping	An algorithm that organizes WLCs and APs that share the same RF Group name.
RF Neighborhood	A group of APs that belong to the same RF Group that can physically hear one another's neighbor messages above -80 dBm.
NDP	Neighbor Discovery Protocol
TPC	Transmit Power Control algorithm
DCA	Dynamic Channel Assignment algorithm
CHDM	Coverage Hole Detection and Mitigation algorithm
DFS	Dynamic Frequency Selection channels



# RRM Data Collection Activities

The RRM processes collect data so that it can be used in organizing RRM. The data collected through the processes is also used for processing channel and power selections for connected APs. A base understanding of where and how RRM gets its information and why it is essential to understand the algorithms involved is required. The process of how and where to configure monitoring tasks and what these translate to in an operational environment will be covered in this section. For each RRM algorithm discussed, the data used and how it is used will also be covered in this discussion.

The channel list to be monitored is configured under **Wireless > 802.11a/b > RRM > General > Noise/Interference/Rogue/CleanAir Monitoring channels**

The screenshot shows the Cisco RRM configuration interface. The left sidebar lists various configuration categories under 'Wireless', with '802.11a/b' selected. The main content area is titled '802.11a > RRM > General'. It contains several sections: 'Profile Threshold For Traps' with input fields for Interference (10), Clients (12), Noise (-70), and Utilization (80); 'Noise/Interference/Rogue/CleanAir Monitoring Channels' with a 'Channel List' dropdown menu; 'Monitor Intervals (60 to 3600 secs)' with 'Channel Scan Interval' (180) and 'Neighbor Packet Frequency' (60); and a 'Factory Default' section with a 'Set to Factory Default' button. A 'Foot Notes' section at the bottom states: '1. CleanAir monitoring is done on these channels only when the AP is in monitor mode.'

From the **Channel List** drop-down list, choose one of the following options to specify the set of channels that APs will use for RRM scanning:

1. All Channels—RRM channel scanning occurs on all channels supported by the selected radio, which includes channels not allowed in the country of operation. (Passive only)
2. Country Channels—RRM channel scanning occurs only on the data channels in the country of operation. This is the default value.
3. DCA Channels—RRM channel scanning occurs only on the channel set used by the DCA algorithm, which by default includes all of the non-overlapping channels allowed in the country of operation. However, you can specify the channel set to be used by DCA if desired.

Two types of off-Channel events are defined:

1. Passive Dwell—It is used to detect Rogues and collect noise and interference metrics. The dwell time is 50 ms.
2. Neighbor Discovery Protocol Tx—It is used to send NDP messages from all channels supported for transmit by the radio. For All Channels, this will be the same as Country Channels.

Under **Monitor Intervals (Wireless > 802.11a/b > RRM > General)**, the default value of Channel Scan Frequency is 180 seconds. This means that all channel dwells must be completed within 180 seconds. So depending on the number of channels defined by the selection in the Monitor list, the interval between dwells will increase or decrease.

For instance:

- Channel List = DCA, slot = 0 (2.4 GHz)—DCA defines channels 1, 6, 11 for a total of 3 channels. So  $180 \text{ (seconds)} / 3 \text{ (channels)} = 60$ , the AP will go off channel every 60 seconds to listen.
- Channel List = Country, slot = 1 (5 GHz)—In the -A regulatory domain (US) there are 21 channels defined. So,  $180 \text{ (seconds)} / 21 \text{ (channels)} = 8.57$ , the AP will go off channel every 8-9 seconds or so to listen for 50 ms.

Neighbor Packet Frequency is also defined on the same page; the default value is 60 seconds. This means that the radio must go off channel and send a single NDP packet for every channel defined by the channel monitoring list within 60 seconds. Using the same example from above where Channel List = Country and slot=1 (5 GHz), this translates to  $60 \text{ (seconds)} / 21 \text{ (channels)} = 3$  seconds. So, every 3 seconds the radio is sending an NDP packet.

Both the Channel Scan Interval and Neighbor Packet Frequency should be left at the default values. By default, the Monitoring Channels list is set to use country channels and this is best for wIPS configurations. However, if wIPS is not a primary concern, you can select DCA channels and reduce off channel activity to just the channels that you are using.

## RF Grouping

RRM RF Grouping is a central function for RRM. RF Grouping forms the basis for two management domains within the RF Network—the administrative and the physical domain.

- Administrative domain—For RRM to work properly it must know which APs and controllers are under administrative control. The RF Group name is an ASCII string that all controllers and APs within the group will share.
- Physical RF Domain – For RRM to calculate channel plans and power settings it is essential that RRM is aware of the RF Location of the APs and their relation to one another. Neighbor messaging uses the RF Group Name in a special broadcast message that allows the APs in the RF group to identify one another and to measure their RF Proximity. This information is then used to form RF Neighborhoods within the RF Group.

Each RF Group must have at least one RF Group Leader per band. The RF Group Leader is the physical device responsible for:

- Configuration
- Running active algorithms
- Collection and storage of RF Group Data and metrics

There will be a minimum of two RF Group Leaders, one for each band—802.11b and 802.11a (2.4 and 5 GHz), respectively. While RF Group Leaders for different bands can coexist on the same physical WLC, they often do not. It is also not uncommon for there to be more than one group leader per band in larger systems that have geographic diversity.

Two modes of the RF grouping algorithm exist in the system today. RF Group Leaders can be selected automatically (legacy mode) or assigned statically. Both methods of assignment were overhauled with the addition of static RF Grouping in version 7.0 of the Cisco Unified Wireless Networking (CUWN) code.

### How RF Groups are Formed

When the WLC is initialized, it creates a unique Group ID using the IP address of the WLC and a Priority Code. The Priority Code is assigned based on the controller model and MAX license count (hardware limit) to create a hierarchical model and ensure that the controller with the most processing capacity is assigned the job of Group Leader (GL). The Group ID and RF Group Name will be used together in messages to other WLCs and APs to identify them. Devices having the same RF Group Name will interoperate as members of the same RF Group.

The current controller hierarchy in terms of capacity is as such:

**8500 > 7500 > 5760 > WiSM2 > 5508 > vWLC > 3850 > 2500**

When comparing Group IDs for leader election, the priority code is the primary criteria and the IP address is secondary. For instance, if there are three other controllers with same priority code, the one with the highest IP address assumes the GL role.

For two WLCs to form an RF Group, there is an infrastructure as well as OTA (Over The Air) component:

- WLCs must be reachable to one another on the distribution network.
- They must each have at least one AP that can hear other's NDP messages above -80 dBm.

The distribution network communicates over unicast UDP:

	Source Port	Destination Port
RRM Manger 11b (11a)	12134 (12135)	12124(12125)
RRM Client 11b (11a)	12124 (12125)	12134 (12135)

The OTA component relies on two functions—NDP and collection of off channel metrics. Assume that NDP is the Off Channel TX cycle and monitoring of off channel metrics is the off channel RX cycle. In general, both NDP and monitoring are critical to the topic of RF Grouping and RRM .

## NDP

One of the most unique features about Cisco's RRM implementation is that it uses OTA messages and operates in a centralized manner even in large deployments. This advantage allows monitoring and managing of all APs and their RF experience from a single point in the network, as well as understanding how every AP relates to any other AP in the RF Group/Neighborhood. This feature is unique in the industry because most other implementations run AP to AP at the edge in a distributed fashion with only configuration elements being managed centrally.

NDP is sent from every AP/Radio/Channel every 60 seconds or less. The NDP packet is a special broadcast message that all APs listen for and it allows us to understand how every radio on every channel hears every other radio. It also gives the RF group the actual RF path loss between APs.

Neighbor messages are sent to a special Multicast address 01:0B:85:00:00:00, and are done so at:

- The Highest Power allowed for the Channel/Band.
- The Lowest data rate supported in the band.

For 802.11b, this means that the message is sent at power level 1 (always the highest power for a particular radio)@ 1 Mbps, and for 5 GHz radio's 6 Mbps. This function is hard coded into the radio firmware and there is no user control. NDP power and modulation are not changed by user configured data rates or power levels.

Max power and min data rate facilitate the maximum propagation of an NDP packet, that is, the RF Group will know the farthest reach that any AP in the group is capable of achieving.

An NDP message contains the following information:

Field name	Description
Radio Identifier	Slot ID for the sending radio
Group ID	IP Address and Priority Code of senders WLC
Hash	RF Group name converted to a hash for authentication
IP Address	The IP address of the sending Ap's RRM Group Leader
Encrypted?	Are we using Encrypted NDP
Version	Version of NDP
AP's Channel	The operating channel of the sending radio
Encryption Key Length	Key Length
Encryption Key Name	Key Name
Message Channel	The channel the NDP was sent on
Message Power	The power (in dBm) the message was sent at
Antenna	Antenna pattern of the sending radio

When an AP receives an NDP message, it:

- Validates that the message is from a member of its RF Group (hash); if not, it is dropped.
- If valid, the AP forwards the message along with the received channel and RSSI to the controller.

The forwarded message is added to the neighbor database, which in turn is forwarded to the RF group leader periodically. For each AP, each radio can store up to 34 neighbors ordered by RSSI high to low.

The following two distinct measurements are developed for each AP in the RF Group:

- RX Neighbors—How the selected AP hears other APs.
- TX Neighbors—How other APs hear the selected AP.

Neighbor entries on the controller are pruned every 60 minutes. If a new neighbor is discovered, the list is flushed and refreshed in its entirety to capture what the new neighbor can contribute.



#### Note

You must be mindful of the pruning interval. If an AP is disabled, it could be up to 60 minutes before it is flushed from the neighbor list.

You can observe neighbor messages over the air by using a packet capture tool and filtering on the multicast address 01:0B:85:00:00:00.

18	Airespace:52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:00:00:00
24	Airespace:52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:01:00.005975
29	Airespace:52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:01:59.910124
34	Airespace:52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:02:59.915850
40	Airespace:52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:03:59.922653
46	Airespace:52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:04:59.930237
51	Airespace:52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:05:59.935790
56	Airespace:52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:06:59.946686
62	Airespace:52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:07:59.950317
68	Airespace:52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:08:59.955871
74	Airespace:52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:09:59.964819
80	Airespace:52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:10:59.971166
96	Airespace:52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:13:59.990219
101	Airespace:52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:14:59.994158
115	Airespace:52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:17:59.911287
120	Airespace:52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:18:59.919573
125	Airespace:52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0:19:59.925931

Neighbor packets being sent out at 60 second intervals



#### Warning

Unless you use the AP sniffer mode to capture the packets, the RSSI values you see in your capture tool will likely be different from what is recorded in the neighbor lists – AND – the neighbor list will quite likely have more entries than what an external tool will hear, simply because the AP's radio sensitivity and position are generally favorable (on the ceiling) to a mobile tool's.

## NDP and DFS

NDP is transmitted on all regulatory channels selected under monitor channels list. However DFS channels represent a special case. In order to transmit on a DFS channel, a station must either be a Master, or in the case of a client—conversing directly with a legal Master. In order to become a Master, an AP must monitor the channel for 60 seconds to verify that no Radar is present before transmitting on that channel. A client hearing a beacon on a DFS channel will infer that the channel is owned by a master and transmit to that Master. For an AP to transmit NDP on a channel in the DFS bands in which it is not currently the master of, the AP needs to first hear either a Beacon or directed Probe from a client in order to mark that channel as clear. The AP can then follow up with a transmitted NDP packet. If there are no other APs and clients on other DFS channels, the AP will not send NDP on any DFS channel except the one on which it is the Master of.

## NDP Usage

NDP forms the foundation of RF Propagation Domain and inherent path losses encountered within the RF Domain. NDP is very important to RRM, and if the NDP is broken, RRM is broken. NDP is used first by the RF Grouping algorithm, and also by:

- TPC (Transmit Power Control)
- Rogue Detection: Any AP that is either not sending NDP, or sends an unintelligible NDP is considered a rogue.
- CleanAir Merging and Psuedo-MACs (PMAC) functions: CleanAir uses neighbor relations to understand if interference reports are coming from APs that are close enough to all hear the same interference device.

A detailed understanding of where the APs are in relation to each other in RF is required.

To view neighbor relations for each AP on the WLC, navigate to **Monitor > Access Points > 802.11a/b > details > RX Neighbors Information**

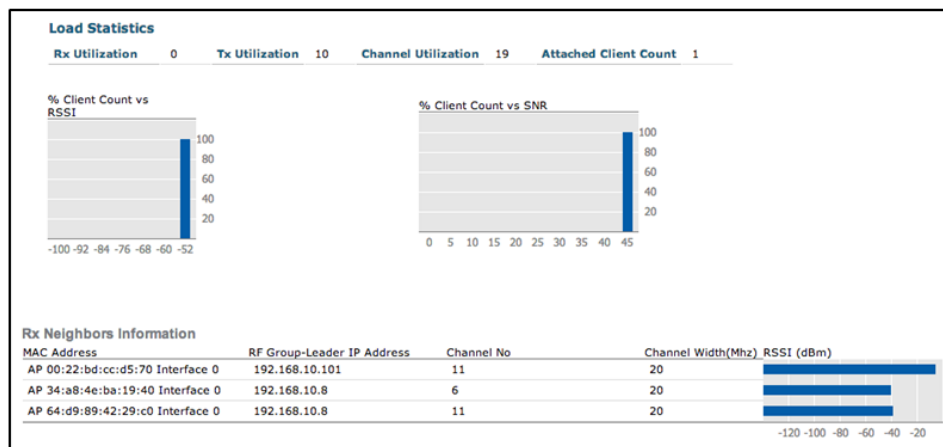
**802.11b/g/n Radios** Entries 1 - 4 of 4

Current Filter: None [\[Change Filter\]](#) [\[Clear Filter\]](#)

AP Name	Radio Slot#	Base Radio MAC	Operational Status	Load Profile	Noise Profile	Interference Profile	Coverage Profile	CleanAir Admin Status	CleanAir Oper Status
1602I_.560e.1b97	0	34:a8:4e:ba:19:40	UP	Passed	Passed	Passed	Passed	NA	NA
AP44d3.ca42.30aa	0	64:d9:89:42:29:c0	UP	Passed	Passed	Passed	Passed	Enable	UP
Base_2602E.039a.9767	0	3c:ce:73:1a:f6:30	UP	Passed	Passed	Failed	Passed	Enable	UP
NOS.ca42.55a7	0	64:d9:89:46:7f:b0	UP	Passed	Passed	Passed	Passed	Enable	

[Detail](#)  
[CleanAir](#)

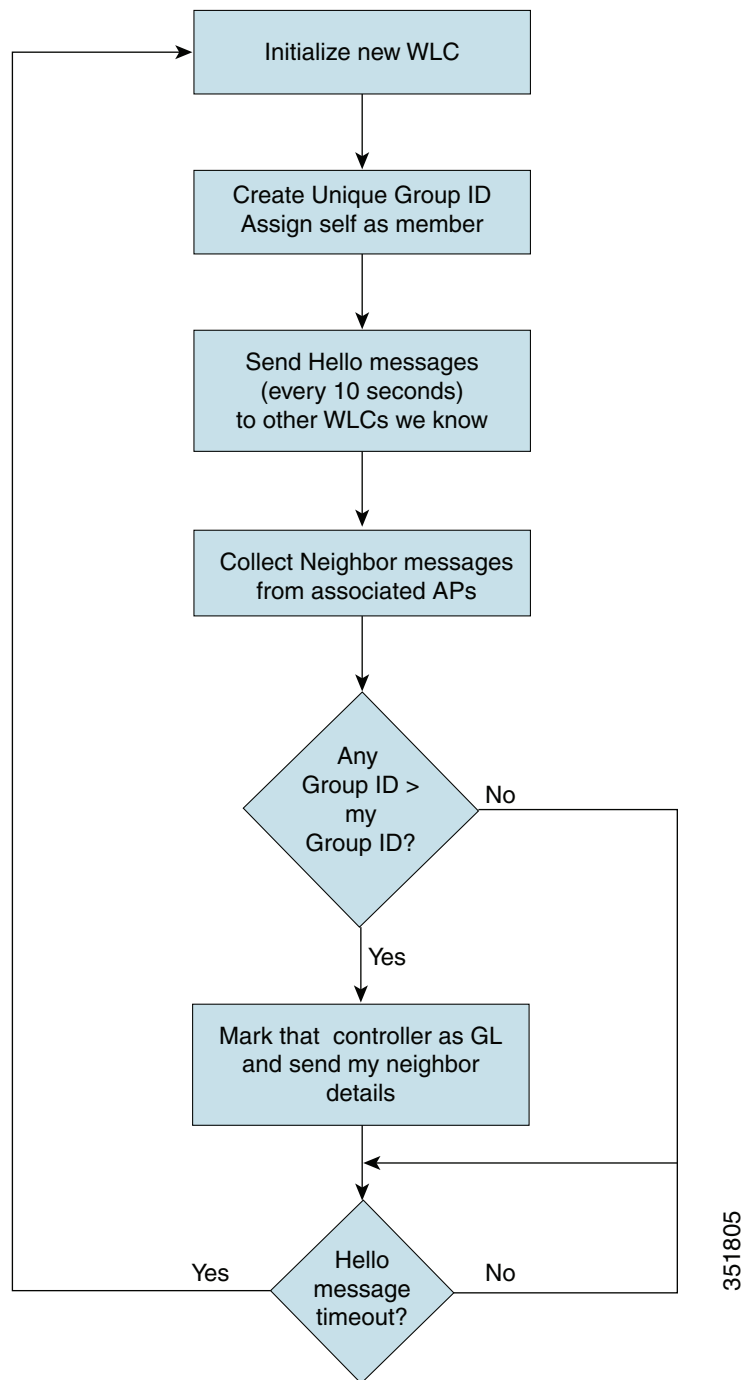
351797



To view neighbor relations for a given AP from the WLC command line, use—[Cisco Controller] show ap auto-rf 802.11b {AP\_Name}

## RF Group Leader Election

Now that we've discussed the components, let's have a look at what happens when a brand new controller is initialized and an RF group is formed. We'll cover automatic Grouping first, and then identify how this differs with Static Grouping assignment. See the flow chart below for the RRM state machine initialization and discussion.



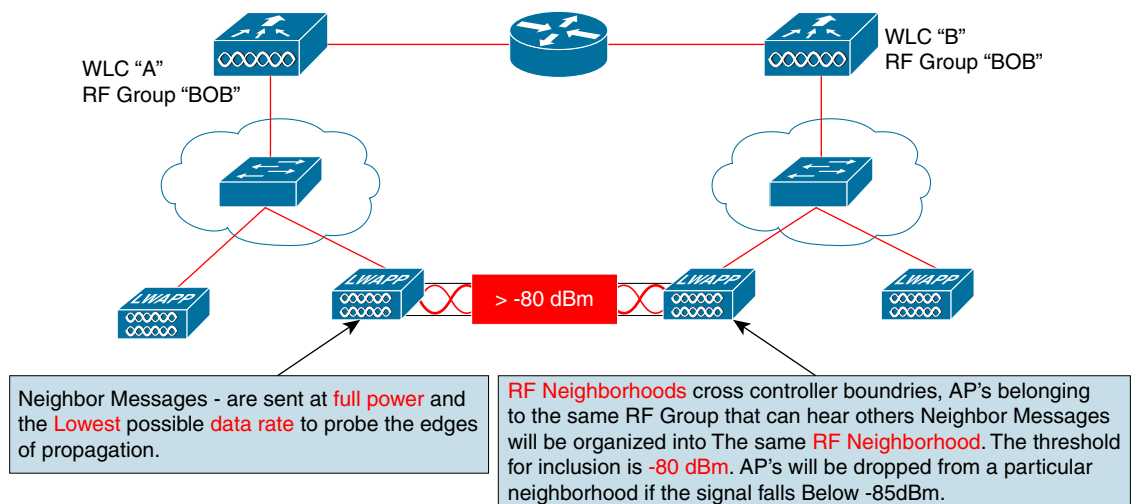
When a WLC is initialized for the first time, the only WLC that it is aware of is itself. The WLC generates the Group ID and initially assumes the role of the Group Leader taking the RF Group name entered during initial startup configuration. The new leader will have itself as a member. The WLC initializes the Hello Timers and begins sending hello messages and NDPs to other WLCs that it is aware of. The Hello message is a unicast that is sent to all WLCs stored in the RF Group History. For now, the RF Group history list will be empty because the WLC was just initialized.



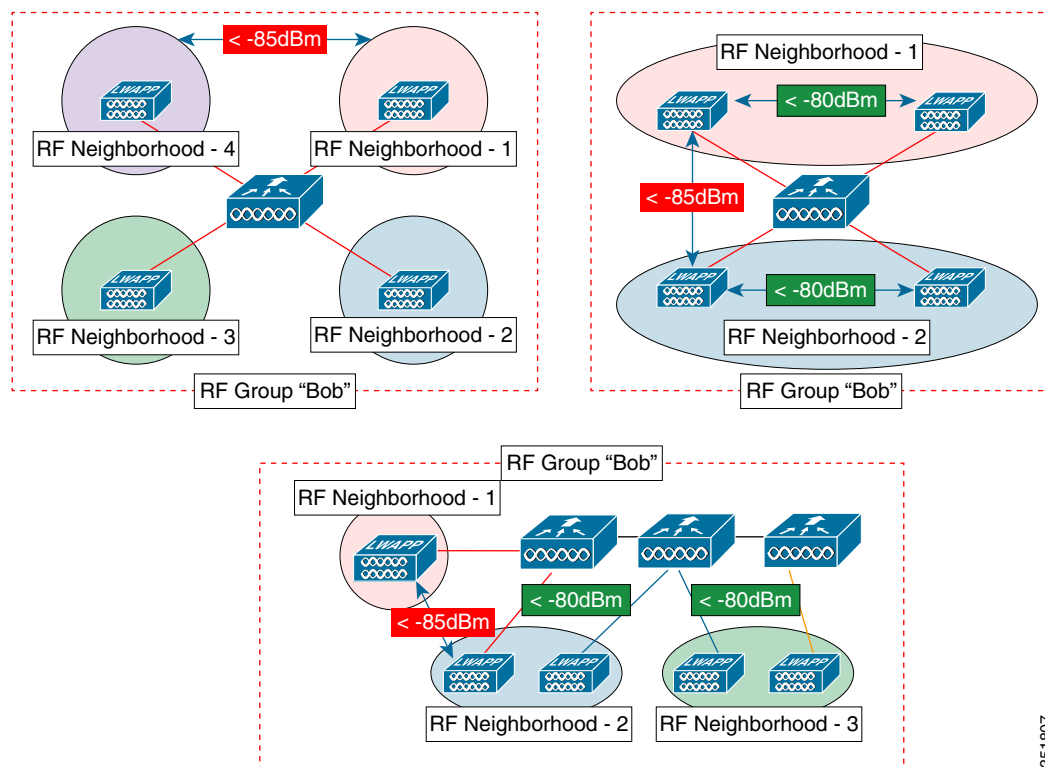
The WLC learns about the environment from NDP broadcast messages received by associated APs. The NDP message contains the sender's WLC Group ID and RF Group Hash, as well as the IP address of the sender's RF Group leader. The new WLC compares all received Group IDs, and the WLC having a larger value becomes the Group Leader. This completes the RF Grouping process and the election process ends. Every ten seconds all WLCs in the same RF group will receive a hello message from its Group Leader. If the Hello messages stop coming, then a WLC will assume that the RF Group has changed and the election process begins again. By this time the RF Group Leader normally has a list of WLCs to send Hello packets to.

Once the Group Leader (GL) is established, neighbor lists from all members will be sent to the GL. The APs in the group will be formed into RF Neighborhoods or groups of APs that are close enough to require RF Power, and channels will be calculated together. For any AP to belong to the same neighborhood, its NDP needs to be seen at or above -80 dBm by an existing member of that neighborhood. Once an AP is added to a neighborhood, as long as the neighbor message is at or above -85 dBm, it remains part of the neighborhood. Any neighbor message below -85 dBm is dropped. The neighbor list purges every 60 minutes, so any AP that remains consistently below -85 dBm will be purged from the list and neighborhood. This process is followed to identify groups of APs that are in the same geographic location.

WLC's having the same RF Group Name participate as the same RF Network. This ascii value is used by AP's attached to these controllers in Neighbor Messages Sent over the air, and allows AP's to identify one another as belonging to the same RF Network.



RF Neighborhoods can span multiple controllers, or a single controller can be managing multiple neighborhoods. A few examples are presented below.



351807

## RF Grouping Automatic Mode

The default mode of RF grouping is the legacy method of forming RF Groups. You can view the current status of the RF grouping algorithm, and learn the identity of the GL and members on the WLC:

Navigate to **Wireless > 802.11a/b > RRM > RF Grouping > Group Mode**

802.11a > RRM > RF Grouping

**RF Grouping Algorithm**

Group Mode:

Group Role: Auto-Leader

Group Update Interval: 600 secs

Group Leader: Cisco\_69:9a:64 (192.168.10.8)

Last Group Update: 97 secs ago

**RF Group Members**

\*If the member has not joined the group, the reason of failure will be shown in brackets

Controller Name	IP Address
Cisco_69:9a:64	192.168.10.8

351799

## Static RF Grouping

In version 7.0, a static method of selecting an RF Group Leader was introduced. This allows a more deterministic outcome to the grouping process. The Group ID is not required here (Priority Code and IP address of the WLC), but the Priority Code will be compared to members. This prevents a lower capacity WLC from becoming the GL of a higher capacity WLC.

The current controller hierarchy in terms of capacity is as such:

**8500 > 7500 > 5760 > WiSM2 > 5508 > vWLC > 3850 > 2500**



**Note**

You cannot assign a model 2504 WLC to be the Group Leader of a model 5508 WLC.

Static grouping allows a user to designate a particular WLC as the Static leader, and manually add the members to be managed. Members must be in auto mode and running a compatible version of RRM. Once the Static leader is assigned, members are assigned to it and a special join message is sent to prospective members that overrides the automatic function and provides the member with a new Group leader assignment.

Navigate to **Wireless > 802.11a/b > RRM > RF Grouping**

802.11a > RRM > RF Grouping

**RF Grouping Algorithm**

Group Mode: leader (1) Restart

Group Role: Static-Leader

Group Update Interval: 600 secs

Group Leader: Cisco\_dc:bb:24 (192.168.10.30)

Last Group Update: 129 secs ago

**RF Group Members**

Controller Name IP Address Add

\*If the member has not joined the group, the reason of failure will be shown in brackets

Controller Name	IP Address
Cisco_dc:bb:24	192.168.10.30
Cisco_dd:f8:e4	192.168.10.20

Changing the group mode to leader and hitting apply opens the member assignment dialogue. You must then assign members and when that is completed, select restart to re-initialize GL elections for new assignments. The new GL controller is automatically added as the first member. At any time, additional members can be added manually. Once the RF Group is restarted, member controllers should stabilize within 10 minutes or so.

## RF Group Scalability

The maximum size of any RF Group depends on the model of the controller and the number of APs physically connected to it. Group member counts are counted by connected APs and not by license count. The maximum size for RF groups can be calculated by using the following rules. An RF Group can contain up to twenty WLCs, and have the noted Maximum APs.

Group Leader HW Platform	Max AP's	Max AP RF Group Size
2500	50	500
WLCM2	50	500
3850	50	500
vWLC	200	1000
5508	500	1000
WiSM2	1000	2000
5760	1000	2000
7500	3000/(6000 with 7.3)	6000
8500	6000	6000

351801

If you exceed the maximum allowed number of APs for a given RF Group, the group simply splits and creates a new RF Group Leader using the same RF Group Name on the same controller receiving the exceeding request.

The downside of having two or more RF Groups is that there are more RF group leaders that have to be addressed when you want to make configuration changes (additional GLs for both 802.11a and 802.11b assuming dual radio APs). This adds some complexity, but is easily managed with controller templates and configuration audit tools.

The RF Group Leader stores the global RRM parameters for the RF Group and if a new Group Leader is created, that WLC's RRM configurations govern the global group settings. If you've not taken advantage of config audit features under **Monitor > RRM** in NCS or Prime Infrastructure, it is possible that you have different configurations on the new GL. This could be quite disruptive if the configurations are out of synch. However if the configurations match, DCA and TPC will mitigate the boundary quite seamlessly.

Refer to [DCA](#) and [TPC](#) sections in Radio Resource Management under Unified Wireless Networks for more details.

When planning your network keep these points in mind:

1. Groups of APs that are close enough to hear one another as neighbors (above -80 dBm) should reside in the same RF Group.
2. Two groups of APs require only a single common AP to join together.
3. If you have two groups of APs that are joined together by only a few APs, you can force a split by creating a second RF group. This will change the RF group advertised in NDP messages and separate the two groups.

## Troubleshooting

### RRM Data Collection

Data Collection at the AP level can be viewed by using the debug command—`debug capwap rm measurements`—This command is used to compare the periods of different intervals at the AP level.

AP44d3.ca42.30aa#deb capwap rm measurements

```
CAPWAP RM Measurements display debugging is on
AP44d3.ca42.30aa#
```

```
*Jan 14 11:36:57.403: CAPWAP_RM: Timer expiry
*Jan 14 11:36:57.403: CAPWAP_RM: Interference onchannel timer expired, slot 1, band 0
*Jan 14 11:36:57.403: CAPWAP_RM: Starting rx activity timer slot 1 band 0
*Jan 14 11:36:57.419: CAPWAP_RM: RRM measurement completed. Request 2003, slot 1 status
TUNED
*Jan 14 11:36:57.483: CAPWAP_RM: RRM measurement completed. Request 2003, slot 1 status
SUCCESS
*Jan 14 11:36:57.483: CAPWAP_RM: noise measurement channel 48 noise 93
*Jan 14 11:37:06.355: CAPWAP_RM: Timer expiry
*Jan 14 11:37:06.355: CAPWAP_RM: Interference onchannel timer expired, slot 1, band 0
*Jan 14 11:37:06.355: CAPWAP_RM: Starting rx activity timer slot 1 band 0
*Jan 14 11:37:06.423: CAPWAP_RM: RRM measurement completed. Request 2004, slot 1 status
TUNED
*Jan 14 11:37:06.487: CAPWAP_RM: RRM measurement completed. Request 2004, slot 1 status
SUCCESS
*Jan 14 11:37:06.487: CAPWAP_RM: noise measurement channel 52 noise 92
*Jan 14 11:37:08.711: CAPWAP_RM: Timer expiry
*Jan 14 11:37:08.711: CAPWAP_RM: Neighbor interval timer expired, slot 0, band 0
*Jan 14 11:37:08.711: CAPWAP_RM: Scheduling neighbor request on ch index:
*Jan 14 11:37:08.711: CAPWAP_RM: Sending neighbor packet #2 on channel 11 with power 1
slot 0
*Jan 14 11:37:08.823: CAPWAP_RM: Request id: 4011, slot: 0, status 1
```

For a granular look at the neighbor activity at the AP, use the debug command—`Debug capwap rm neighbors`

```
*Jan 14 17:29:36.683: LWAPP NEIGHBOR: NDP Rx: From 64d9.8946.7fb0 RSSI
[raw:norm:avg]=[-37:-39:-38] Channel [Srv:Tx]=[1 :6 ] TxPower [Srv:Tx]=[4 :22 ]
```

// This debug entry is about NDP packets received from other APs in our RF Group.

NDP RX from x.x.x.x RSSI (raw:norm:avg)=(n:n:n) Channel (Srv:Tx) SRV is the channel the sending AP is serving clients on, TX is the channel the message was sent on. TxPower (Srv:Tx) Srv is the power in dBm that the AP is currently serving clients at and Tx is the power in dBm that the NDP message was sent at.

```
*Jan 14 17:29:37.007: LWAPP NEIGHBOR: NDP Tx: Channel [Srv:Tx]=[64 :64 ] TxPower
[Srv:Tx]=[2 :17 ]
```

NDP TX is our AP sending NDP message, channel (Srv:Tx) Srv is the channel the AP is serving clients on, Tx is the channel the AP sends NDP message on. TxPower (Srv:Tx) Srv is power in dBm the AP is serving clients at, Tx is the power in dBm that the AP sends messages at.

```
*Jan 14 17:29:40.007: LWAPP NEIGHBOR: skipping chan 100; not clear for DFS
```

```
*Jan 14 17:29:43.007: LWAPP NEIGHBOR: skipping chan 104; not clear for DFS
```

```
*Jan 14 17:29:46.007: LWAPP NEIGHBOR: skipping chan 108; not clear for DFS
```

//Channels that do not have a DFS Clear for TX flag.

```
*Jan 14 17:29:48.299: LWAPP NEIGHBOR: Updating existing neighbor 34a8.4eba.194f(1), rssi
-51 on channel: 48 with encryption: 0
```

```
*Jan 14 17:29:48.299: LWAPP NEIGHBOR: Neighbor update 34a8.4eba.194f(avg -45), new rssi
-45, channel 48
```

//An update about a change in a neighbor's information is sent to the controller and ultimately the RF Group Leader.

Neighbor messaging issues are easy to spot, if NDP is broken, then APs that are next to one another will not have a neighbor relationship.

## RF Grouping Trouble

Most often the reason for trouble with RF groups is compatibility. With the version 7.0 code update and the introduction of Static Grouping, there have been many changes to RRM and how it behaves. Backward compatibility has been preserved where it could be; however, changes in the RRM header were required to implement these changes and the header version number is checked on grouping.

RRM Header version 30.0 was used through version 7.0. Version 30.1 was introduced with release 7.2 and RF Profiles. Version 7.3 added more structure to RF Profiles and also saw the introduction of Converged Access Architecture, and the header version changed to 30.2. This is the last change required for the foreseeable future.

CUWN Service	4.2.x	5.0.x	5.1.x	6.0.x	7.0.x.x	7.2.x.x	7.3.x.x	CA 10.1	7.4.x.x
Radio Resource Management (RRM)	X	-	-	X	X	-1	-2	-3	-2

351802



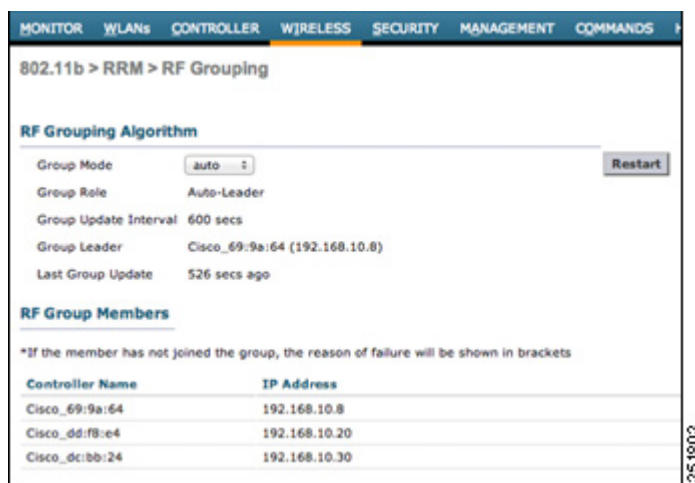
### Note

- In the 7.2.x.x release, RF Groups and Profiles were introduced. RRM for 7.2.x.x and later releases is not compatible with RRM for any previous release.
- In the 7.3.x.x release, changes were made to RF Profiles that were not backwardly compatible with 7.2.
- Converged Access 10.1 release will form RF groups with release 7.3.101.0; however, there is no support for RF Profiles.

RF Grouping functions can be observed on the controller by using the `sh advanced 802.11a/b group` command.

```
(controller) > show advanced 802.11b group
Radio RF Grouping
 802.11b Group Mode..... STATIC
 802.11b Group Update Interval..... 600 seconds
 802.11b Group Leader..... GRP_Leader (1.2.3.4)
   802.11b Group Member..... GRP_Member (1.2.3.4)
   802.11b Group Member..... GRP_Member (1.2.3.5)
 802.11b Last Run..... 594 seconds ago
```

To view the status on the WLC GUI, navigate to **Wireless > 802.11a/b > RRM > RF Grouping**



For Automatic RF Grouping, if a WLC does not join an RF Group, it is mostly because:

- The RF Group size is above capacity.
- The RF Group Name assigned to the WLC is different.
- There is no network path for Hello Messages.

For Static RF Grouping, if an assigned member does not join the statically assigned Group Leader, the most common reasons are version compatibility, RF Group Name, and Controller Hierarchy.

#### Useful Debugs that can be Executed at the WLC CLI

`debug airwave-director error` : Displays all errors for RRM and RF Grouping.

`debug airwave-director group` : Shows RF Grouping activities in a steady state network; this equates to a split calculation ensuring that the RF Group still meets the criteria on size and neighbor relations.

You can force a re-grouping to occur by selecting the reset button on the **Wireless > 802.11a/b > RRM > RF Grouping** menu.

The given example shows how a RF group is formed:

```
*emWeb: Jan 16 18:46:49.717: Airewave Director: Group 802.11bg attempting to remove entry C0.A8.0A.14.00.4B, IP Addr 192.168.10.20
```

```
*emWeb: Jan 16 18:46:49.717: Airewave Director: removing entry C0.A8.0A.14.00.4B from 802.11bg group
```

```
*emWeb: Jan 16 18:46:49.719: Airewave Director: Group 802.11bg attempting to remove entry C0.A8.0A.1E.00.32, IP Addr 192.168.10.30
```

```
*emWeb: Jan 16 18:46:49.719: Airewave Director: removing entry C0.A8.0A.1E.00.32 from 802.11bg group
```

\\Deleting the current members.

```
*RRM-MGR-2_4: Jan 16 18:46:49.746: Airewave Director: adding entry C0.A8.0A.08.01.F4 (500) to 802.11bg group
```

\\Current Group Leader adding itself as a member.

```
*RRM-MGR-2_4: Jan 16 18:49:03.614: Airewave Director: Group received Join Request from 802.11bg group C0.A8.0A.14.00.4B(63131), IP addr 192.168.10.20
```

\\The RF Group Leader receives a Join Request.

```
*RRM-MGR-2_4: Jan 16 18:49:03.614: Airewave Director: Deny join request from IP addr 192.168.10.20 to 802.11bg group C0.A8.0A.14.00.4B(63131) with reason Non matching group ID
```

\\Join is Denied because the group ID does not match.

```
*RRM-MGR-2_4: Jan 16 18:51:07.651: Airewave Director: Group received Join Request from
802.11bg group C0.A8.0A.14.00.4B(63131), IP addr 192.168.10.20
```

\\Second Join Request received.

```
*RRM-MGR-2_4: Jan 16 18:51:07.651: Airewave Director: Member in join request from source
IP addr 192.168.10.20 to 802.11bg group, member IP 192.168.10.20 our Id 500 srcType 75
*RRM-MGR-2_4: Jan 16 18:51:07.651: Airewave Director: adding entry C0.A8.0A.14.00.4B (75)
to 802.11bg group
```

\\The request is honored and the WLC is added to the group.

```
*RRM-MGR-2_4: Jan 16 18:56:59.958: Airewave Director: Group received Join Request from
802.11bg group C0.A8.0A.1E.00.32(63131), IP addr 192.168.10.30
```

\\A second WLC sends its join request.

```
*RRM-MGR-2_4: Jan 16 18:56:59.958: Airewave Director: Member in join request from source
IP addr 192.168.10.30 to 802.11bg group, member IP 192.168.10.30 our Id 500 srcType 50
*RRM-MGR-2_4: Jan 16 18:56:59.958: Airewave Director: adding entry C0.A8.0A.1E.00.32 (50)
to 802.11bg group
```

\\And the second WLC is added to the group (Complete).

```
*RRM-MGR-2_4-GRP: Jan 16 18:57:20.909: Airewave Director: prep to join 802.11bg group
C0.A8.0A.65.03.E8(63126) due to rssi -8
*RRM-MGR-2_4: Jan 16 18:57:36.839: Airewave Director: Group 802.11bg attempting to join
group IP Address 192.168.10.101, ctrl count 3
```

\\Now the GL attempts to join another WLC whose Group ID is higher—with a controller count of 3 (The GL plus the two new WLC additions).

```
*RRM-MGR-2_4: Jan 16 18:57:36.857: Airewave Director: Group received join failure from
802.11bg C0.A8.0A.65.03.E8(63126) (192.168.10.101) for reason Not a configured static
member
*RRM-MGR-2_4: Jan 16 18:57:36.857: Airewave Director: Group validated join failure from
802.11bg C0.A8.0A.65.03.E8(63126) for reason Not a configured static member
```

\\But access is denied—192.168.10.101 is configured as a static GL, and the GL attempting to join is not configured as members under that static GL.

## Summary of the Reason Codes

1. Invalid IP: This suggests that the controller IP is invalid or does not match the controller system name.
2. Group Size exceeded: When the operational limits of a Leader controller is reached either because of AP numbers or number of member controllers addition, the Leader rejects addition of more controllers and display this reason for rejection.
3. Invalid Group order: This error message is displayed for the following reasons:
  - If the grouping order is not in the way it has been formulated for reasons such as memory corruption.
  - If the data-structures have been corrupted during transmission.
  - If an unknown controller type is attempting to join.
4. Source Not Included: No valid source identification.
5. Weak Signal Strength: Nearest neighbor is not close enough. (Not applicable to static RF grouping)



6. **Join Pending:** When a member controller is waiting to complete and exit from one RRM state and join as a member to another RRM state.
7. **Not a Manager:** When a RF group member is wrongly being acknowledged as a RF leader. (Unlikely scenario)
8. **RRM Assigning:** In progress
9. **Grouping disabled:** When RF Grouping is not enabled (switched “OFF”) on the controller that this message is displayed for.
10. **Invalid Protocol Version:** If the RF member controller image is of an incompatible version or if there is a version mismatch.
11. **Country code mismatch:** Configured country code on the WLC does not match other WLCs in the RF group.
12. **Invalid hierarchy:** This error occurs when a lower priority controller tries to add a higher priority controller.
13. **Already a static leader:** Trying to add a member who is already been manually configured to be a static leader.
14. **Already Static Member:** This error message occurs when RF Group Leader tries to add a member who has already been accepted as a static member by another RF leader.
15. **Non-Static Member**
16. **Not Intended**
17. **Member Deletion Error:** The error is specifically known to occur due to improper memory allocation or de-allocation.
18. **RF-domain mismatch:** If the RF domain of the configured member and the RF leader does not match.
19. **Split for invalid-state request:** This error state occurs if there is a member split because of a RRM state transition that was not expected.
20. **Transitioning to static from auto:** While moving from auto to static state.
21. **Split due to user action:** When there is a user triggered transition because of reset while modifying country code, sys-name change, or other user actions.
22. **Switch Size Exceeded**

