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.

- Administrative domain–For RRM to work properly it must know which APs and controllers are under our administrative control. The RF Group name is an ascii string that all controllers and APs within the group will share.
- Physical RF Domain–In order for RRM to calculate channel plans and power settings it is essential that RRM be aware of the RF Location of our 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 (A group of AP's that belong to the same RF Group that can physically hear one another's neighbor messages above -80 dBm) 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 the 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's also not uncommon for there to be more than one group leader per band in larger systems that have geographic diversity.

Two modes of 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 CUWN code.

How RF Groups are formed

When the WLC initializes as new, 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 GL (Group Leader). The Group ID and the RF Group Name will be used together in messages to other WLC's and AP's to identify them. Devices having the same RF Group Name will interoperate as members of the same RF Group.

The current controller hierarchy is as such:

8500 > 7500 > vWLC(large) > 5520 > 5760 > WiSM2 > 5508 > vWLC(small) > 3850 > 2500

Note See Table 1: Ports required for RRM operationbelow along with RF group scalability numbers below.

When comparing Group IDs for leader election, the priority code is primary criteria and IP address is secondary. For instance, if there are 3 other controllers, none of which has the same or higher priority code than myself - I become the Group Leader. If all 3 have the same priority code as myself, then the one with the highest IP address wins and 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 also have at least one AP that can hear the other's NDP messages above -80 dBm

The distribution network communicates over unicast UDP:

Table 1: Ports required for RRM operation

	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 - Neighbor Discovery Protocol and collection of off channel metrics. Think of NDP as the Off Channel TX cycle, and monitoring of off channel metrics as the off channel RX cycle. Both NDP and monitoring are critical to the topic of RF Grouping and RRM in general, so we'll discuss them here before going any deeper.

Neighbor Discovery Protocol–NDP

One of the most unique things about Cisco's RRM implementation is that it uses Over The Air (OTA) messages and runs centralized even in large deployments. This gives us the advantage of being able to monitor and manage all APs and their RF experience from a single point in the network. Not only manage - but understand how every AP relates to any other AP in the RF Group/Neighborhood. This is unique in the industry as most other implementations run AP to AP at the edge in a distributed fashion with only configuration elements being managed centrally.

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

Neighbor messages are sent to a special Multicast address of **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) at 1 Mbps, and for 5 GHz radio's 6 Mbps. This function is hard coded into the radio firmware, there is no user control. NDP power and modulation is not changed by user configured data rates or power levels.

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

An NDP message contains the following information:

Table 2: Contents of NDP Packet

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
APs 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 hears an NDP message, it:

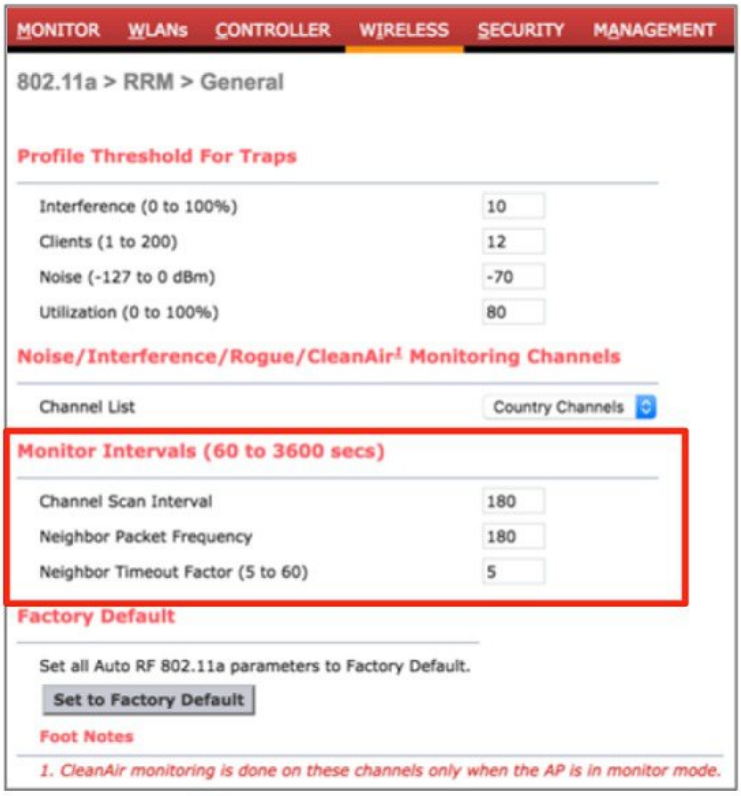
- Validates that the message is from a member of its RF Group (hash); if not it is dropped
- If valid forwards the message along with the received channel and RSSI to the controller

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.

Post processing of this information develops 2 distinct measurements:

- RX Neighbors: How I hear other APs
- TX Neighbors: How other APs hear me

Neighbor entries on the controller are pruned at different default intervals depending on your code release. Before 8.0 the pruning interval is fixed at 60 Minutes. In 8.0, it is hard coded for 15 minutes. In 8.1 and above there is a new function–Neighbor Timeout Factor. On the GUI wireless=>802.11a/802.11b=>RRM=>General.



The Neighbor Timeout Factor allows the user to directly configure how long to maintain the neighbor list on the controller.

Neighbor Timeout Factor is the multiplier that will be applied to Neighbor Packet Frequency (seconds) - NTFxNPF= Pruning interval in seconds. In the example above, the Neighbor Packet Frequency is 180 seconds; the Neighbor Timeout Factor is 5, so **5x180=900 seconds/15 Minutes (Default Configuration)**.

Note 15 Minutes is the default pruning interval in WLC version 8.0 and above. This is fine in most installations. Under sustained heavy loads (high client density, Channel Utilization consistently 60% or higher), or in environments that enjoy a lot of neighbor interference this may be inadequate to ensure stable neighbor resolution. Channel Changes will increase if NDP is changing between DCA cycles (default 10 minutes). If an AP's neighbors are changing then DCA will supply a different answer to the new equation. Changing the Neighbor Timeout Factor to 20 restores 3600 second (1 hour) the legacy interval.

The Neighbor Pruning interval affects the stability of everything that displays or uses neighbor information. Cisco Prime maps and show auto RF outputs use the neighbor list. NDP is a packet sent over the air interface,

and if off channel transmission is suspended it simply waits 180 (default - should never be longer) seconds to get back to the channel and retry the off channel Tx . High Channel Utilization and poor SNR in a busier network will lower the opportunities NDP has to transmit. A Voice SSID will defer off channel activity any time there is has been traffic in the voice QOS que within the last 100 ms. Retaining the historical information over a period of time compensates for short duration inconsistencies.

What does this mean in terms of monitoring performance? If a radio is admin disabled or disconnected, that radio will exist in the neighbor list until the NDP pruning interval kicks in. You will still see it in all lists and reports - until it times out. If a new neighbor is discovered the list is flushed and refreshed in its entirety to capture what the new neighbor can contribute.

What does all this mean? In short, leave the default values alone unless you have a reason to change them, and then only longer - not shorter than 15 minutes. When to set the interval to longer? If you upgrade from 7.x to 8.x and see a definite increase in channel changes after reaching steady state operations (no new bandwidth changes, DBS added, DCA start up isn't running) then increase the Neighbor Timeout Factor in increments of 5 (fifteen minutes for each increase of 5) until you see "Your" normal operations.

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

Figure 1: Sample Packet Capture of NDP Messaging

Caution 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 you can hear simply because the APs 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 as in order to transmit on a DFS channel a station must either be a Primary, or in the case of the client - associated directly to a legal Primary. In order to become a Primary, 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 can infer that the channel is owned by a Primary and transmit to that Primary. In order for us to transmit NDP on a channel in the DFS bands that we are not the Primary of, we need to first hear either a Beacon or a directed Probe from a client in order to mark that channel as clear, then we can follow up with a transmitted NDP packet within 5 seconds. If there are no other APs, and there are no clients on other DFS channels, we will never send an NDP on any DFS channel except the one on which we are the Primary.

What do we use NDP for?

NDP forms the foundation for our understanding of the RF Propagation domain and inherent path losses encountered within the deployment. NDP is very important to RRM, and as such it should go without saying then that if NDP is broken, RRM is broken. NDP is used first by the RF Grouping algorithm, but also by:

- TPC (Transmit Power Control) - third neighbor opinion of our NDP or the basis for calculation as in TPCv2
- FRA (Flexible Radio Assignment) NDP messages from all AP's are the basis for Coverage Overlap Factor
- Rogue Detection–any AP that is either not sending NDP, or sends an unintelligible NDP is considered a rogue
- CleanAir Merging and PMAC functions–CleanAir uses neighbor relations to understand if interference reports are coming from AP's that are close enough to all hear the same interference device
- CMX–for AP RF Distance and pathloss measurements

All of these things require a detailed understanding of where the APs are in relation to each other in RF. And, that's what NDP does.

You can see neighbor relations in several places within the system, on the WLC select **Monitor=>Access Points=>802.11a/b=>details=> RX Neighbors Information**

Figure 2: Examples of where to see Neighbor Relations per AP

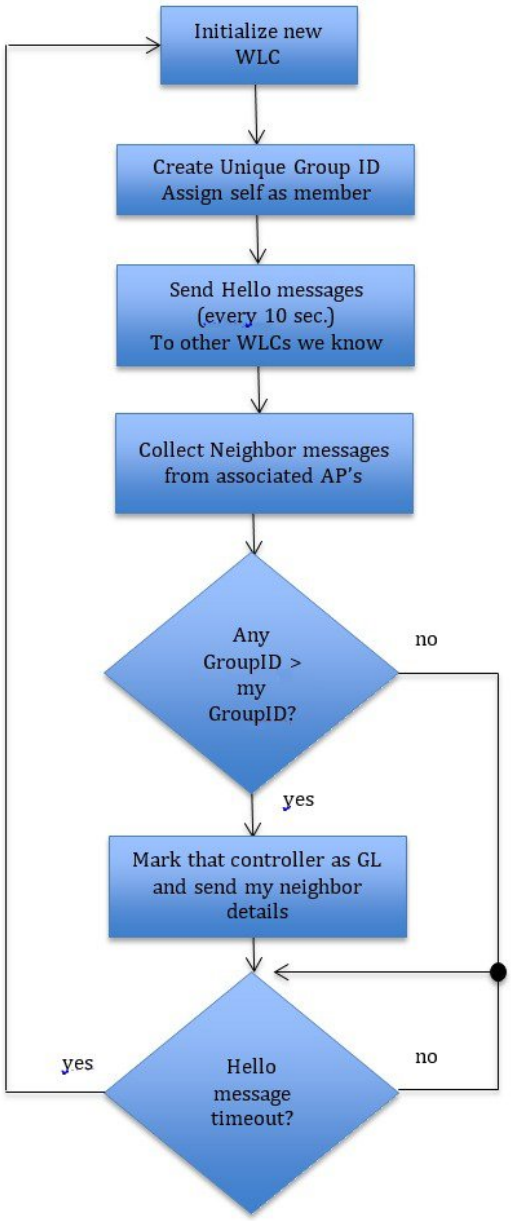
Or from the command line:

```
(Cisco Controller) show ap auto-rf 802.11a/b {AP_Name}
(Cisco Controller) show ap auto-rf 802.11-abgn {AP_Name} (for Flexible Radios)
```

RF Group Leader Election

Now that we've discussed the components, lets 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 last. See the flow chart below for RRM state machine initialization:

Figure 3: RF Grouping Process Flow Chart



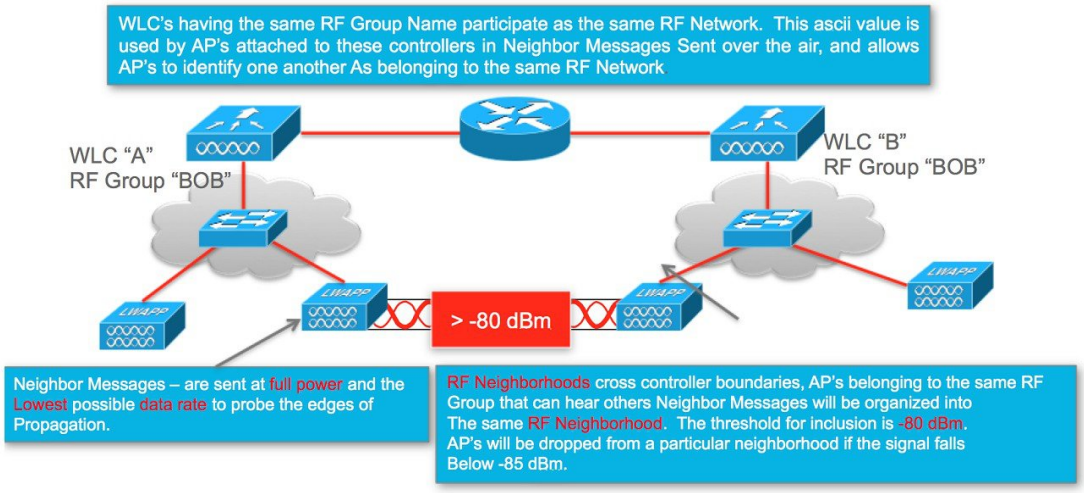
When a WLC is initialized for the first time the only WLC that its aware of is itself. The WLC generates the GroupID and initially assumes the roll of Group Leader taking the RF Group name entered during initial

startup configuration and passing this to any connected AP's for use in their neighbor string. The new leader will have itself as a member. The WLC initializes the hello timers and begins sending over the wire to other WLCs that it knows about. The Hello message is a unicast that is sent to all WLCs stored in the RF Group History. If Auto Grouping, having just been initialized, this list is empty. If Static configuration, then the list is or will be populated by manual assignment.

For Auto Grouping, the received OTA NDP message contains the sender's WLC Group ID and RF Group Hash as well as the IP address of the senders RF Group leader. The new WLC compares all received Group IDs, and any one having a larger value than our own then becomes our Group Leader. RF Grouping completes and the election process ends. Every 10 seconds we'll receive a hello message from our Group Leader that serves as a heartbeat for the RF group. If the Hello messages stop coming - we'll assume that the RF Group has changed - and the election process begins again. By this time we'll normally have a list of WLCs to send Hello packets.

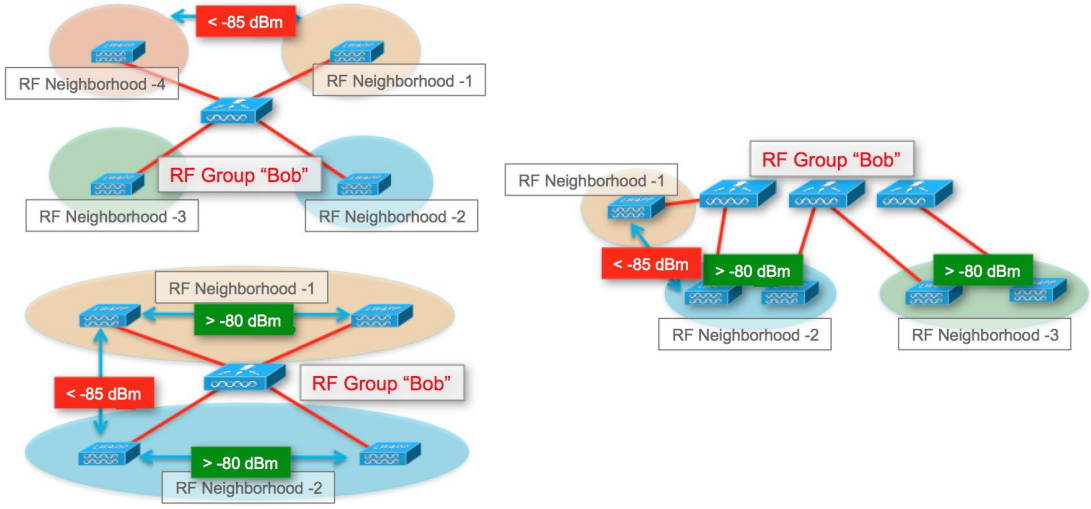
Once the Group Leader is established, neighbor lists from all members will be sent to the GL and APs in the group will be formed into RF Neighborhoods or groups of APs that are close enough to require RF Power and channel be calculated together. For another AP to belong in our neighborhood we'll need to see that APs neighbor message at -80 dBm or above. Once an AP is added to a neighborhood, as long as we see the neighbor message 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 up through version 8.0 code. In 8.1 the neighbor retention time was adjusted to match 3x the scan interval (so at default 180 seconds, the neighbor list will be purged every 15 minutes). Any AP that remains consistently below -85 dBm will be purged from the list and the neighborhood. In this way, we identify groups of APs that are in the same geographic location.

Figure 4: RF Group and Neighborhood example



RF Neighborhoods can span multiple controllers, or a single controller can be managing multiple neighborhoods, some examples are presented here.

Figure 5: Examples of how RF Neighborhoods are organized

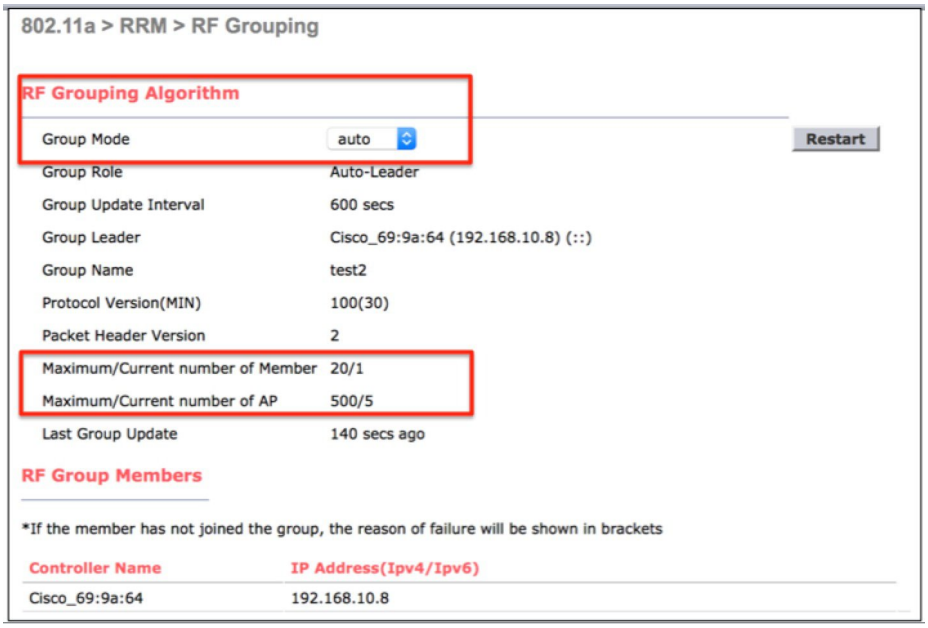


RF Grouping Automatic mode

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, learn the identity of the Group Leader and members, and on the RF Group leader WLC see a count of current WLC's and AP's contained in the group on the WLC:

Wireless=>802.11a/b=>RRM=>RF Grouping =>group mode

Figure 6: RF Grouping Configuration Dialogue



Static RF Grouping

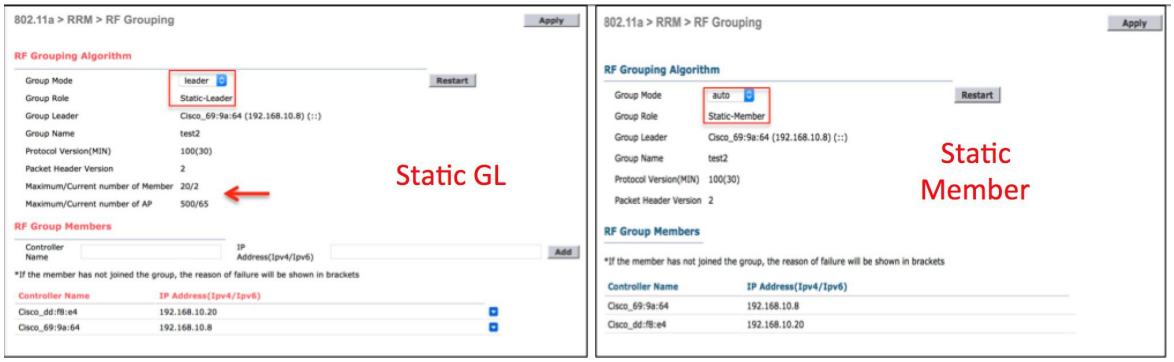
In version 7.0 a static method of selecting an RF group leader was introduced. This allows a more deterministic outcome to the grouping process. The Group ID is not needed here (Priority Code and IP address of the WLC) but the Priority Code will be compared to members; this prevents a lower capacity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

Note You cannot assign a 2504 to be the group leader and have a 5508 added as a member.

Static grouping allows the 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.

Under **Wireless=>802.11a/b=>RRM=>RF Grouping**

Figure 7: Example of Static and Automatic RF Grouping Configurations



Changing the group mode to leader, and hitting apply opens the member assignment dialogue. You then assign members and when complete select restart to re-initialize group leader elections for the new assignments. In order for a member to be added, the prospective member must be in Auto grouping mode - else it assumes it is it's own leader. The new Group Leader controller is automatically added as the first member. Additional members can be added manually at any time. Member controllers should stabilize within 10 minutes or so once the RF Group is restarted.

There are no rules on spectrums, meaning leaving 5 GHz in Auto, and 2.4 GHz as Static is just fine. Or do both static, but on different controllers, your choice. The sky is the limit as both interfaces are different RF Group instances. However, and this is always good advice, Cisco best practice is keep it simple.

RF Group Scalability

The maximum size for an RF Group is dependent on the model of the controller and the number of APs physically connected. The maximum sizes for RF groups can be calculated using the following rules. An RF Group can contain up to 20 WLCs, and have the noted Maximum APs.

Table 3: WLC RF Grouping Hierarchy and Scalability

Group Leader WLC	Maximum APs	Maximum AP per RF Group
2500	75	500
WLCM2	50	500
3850	50	500
vWLC (small)	200	1000
5508	500	1000
5520	1500	3000
WiSM2	1000	2000
5760	1000	2000
vWLC (large)	2000	2000
7500	6000	6000
8500 /8540	6000	6000

What happens if I exceed the RF group size? A popular question, relax, the world does not come to an end, please read on.

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 controller that the AP joined to create the condition. This sounds a lot worse than it is, and in practice most folks are generally not even aware of it until they look for the RF Group Leaders and notice that there is more than one per band.

What's the downside of having two or more RF Groups? There are now 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. Two AP's belonging to two different RF groups will not see one another as neighbors as they have different hashes of the same RF Group name. For this reason, some planning of which AP's go to which controllers is important. It is best to plan for AP's that are co-located to be on the same controller or under the same RF Group Leader.

The RF Group Leader stores the global RRM parameters for the RF Group and if a new Group Leader is created, that new WLC's RRM configurations will 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 (the worst case scenario). This could be quite disruptive if the configurations are seriously out of synch. However if the configurations are matching, DCA and TPC will mitigate the boundary quite seamlessly.

When planning your network keep these things 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. If you have multiple controllers, geographically group your AP’s on like RF Groups of controllers – depending on your configuration static assignment of GL’s and members may be the best approach.

3. Two otherwise diverse groups of APs only require a single AP in common to join together and form a neighborhood.
4. 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.

RF Group Backward Compatibility

In version 7.2 RF Profiles where introduced. This represented a major change to how RRM operated. RF Profiles assigned to AP groups could be configured differently from the global RF Group. Versions from 7.2 and forward are not compatible in an RF Group with older versions. About the same time Converged Access was introduced, and feature parity (RF Profiles) was not achieved immediately. Check the Cisco Wireless Solutions Software Compatibility Matrix Inter Release Controller Mobility table to ensure compatibility for mixed release integrations. Pay attention to the notes. From version 7.5 on, there are feature differences, however all can be successfully included in a single RF Grouping.

WSSI and WSM, WSM2 Modules and RRM

One of the great additions to make if you own a 3 series AP (3600, 3700, 3800) and can install a module is the Wireless Security Module which contains radios strictly dedicated to monitoring. There are two models of this module now, but both operate with respect to RRM in the same way - they off load the off channel functions of the serving radios to the module. This allows the serving radios to remain dedicated to the channel they are serving and increases the dwell time on each channel based on the role of the dwell (i.e. off channel, location, wIPS, CleanAir). This offloading is a benefit in almost every situation in that it brings a higher resolution to the data that is being collected with longer and more frequent dwells driving the collection. The module relies on it's own internal antenna's for collection and the antenna pattern is matched with that of an internal antenna AP model.

One caveat to this approach however is external highly directional antennas used in High Density designs (most omni patch antenna's are just fine and this does not apply to them). The data that is being collected relies on the over the air results matching what the AP and serving interfaces actually see. In a High Density solution using the Stadium antennas, this will differ significantly. For this reason, achieving a good channel plan for the antennas used in the design requires shutting down the module and collecting over the air metrics using the AP's native interfaces and antenna to develop a good channel solution. Once this has been done, freezing DCA will allow the module to continue driving benefit without negatively impacting the channel and power solution.

Troubleshooting RF Grouping

RRM Data Collection

Data Collection at the AP level can be viewed using debugs.

debug capwap rm measurements–the output should be self explanatory. This is useful to compare the intervals of different intervals at the AP.

```
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 specifically: 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 is about the NDP received from a neighbor.

NDP RX from x.x.x.x RSSI (raw:norm:avg)=(n:n:n) Channel (Srv:Tx) SRV = the channel the sending AP is serving clients on, TX= the channel the message was sent on. TxPower (Srv:Tx) Srv= the power in dBm that the AP is currently serving clients at Tx = 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-this sends a NDP message, channel (Srv:Tx) Srv - the channel we are serving clients on, Tx - the channel we sent the NDP message on. TxPower (Srv:Tx) Srv - power in dBm we are serving clients at, Tx - the power in dBm that we sent the message 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 not clear for transmit for DFS:

```
*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 of a change in a neighbor's information being sent to the controller and ultimately the RF Group Leader.

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

RF Grouping Trouble

Often the reason for trouble with RF groups is simply compatibility. Since version 7.0 of code 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 some of 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. 7.3 added more structure to RF Profiles and also saw the introduction of Converged Access Architecture, the header version changed to 30.2. This is the last change required for the foreseeable future.

Table 4: Excerpt of IRCM RRM compatibility matrix

CUWN Service	4.2x	5.0x	5.1x	6.0x	7.0x.x	7.2.x.x	7.3.x.x	CA10.1	7.4.x.x
Radio Resource Management (RRM)	X	–	–	X	X	-1	-2	-3	-2

Note

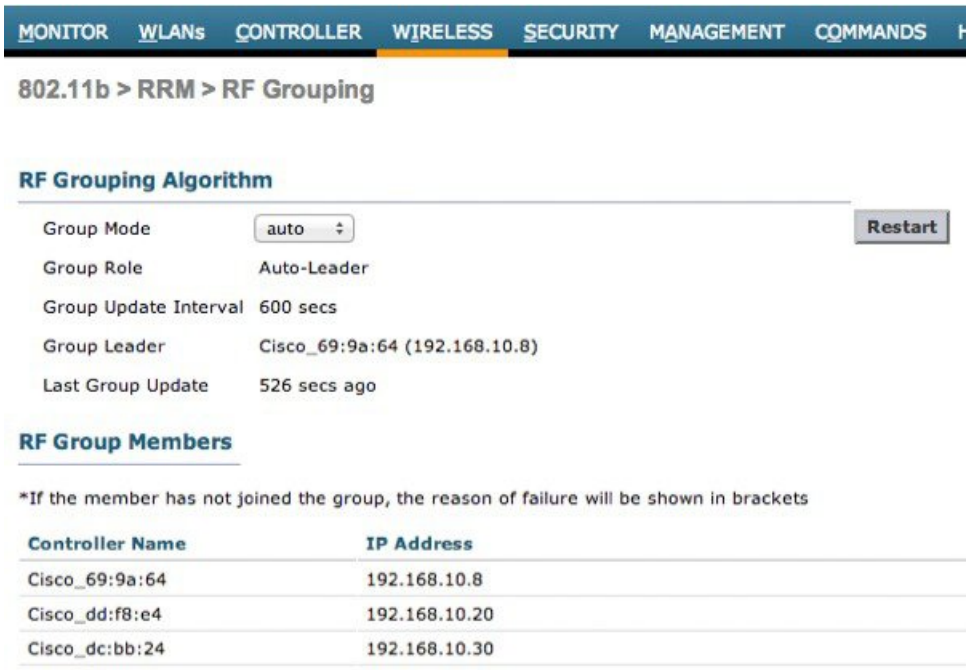
1. In the 7.2.x.x release, RF Groups and Profiles were introduced. RRM for 7.2.x.x and later releases is not compatible with RRM for any previous release.
2. In the 7.3.x.x release changes where made to RF Profiles, not backwardly compatible with 7.2.
3. CA 10.1 release will form RF groups with 7.3.101.0 - however there is NO support for RF Profiles.

RF Grouping functions can be observed on the controller 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
```

You can view the status on the **WLC GUI at Wireless=>802.11a/b=>RRM=>RF Grouping**:

Figure 8: RF Grouping information on the WLC GUI



For Automatic RF Grouping, if a WLC that you feel certain should be in an RF Group somehow will just not join, it is either 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 will not join the statically assigned group leader - the most common reason is version compatibility, RF Group Name and Controller Hierarchy are high on the list to evaluate.

Useful Debugs from the WLC console

- 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**

Watch the RF group form

```
*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
```

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 Denied, non matching group ID

```
*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 we add the WLC 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
```

The second WLC sends it's 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 it 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 our group leader attempts to join another WLC whose Group ID is higher than ours - with a controller count of 3 (himself and the two new 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 we are denied access - 192.168.10.101 is configured as a static Group leader, and we are not configured as members under that group.

Summary of the Reason Codes

1. Invalid IP: This suggests that the controller IP is invalid or doesn't match against the controller system name.
2. Group Size exceeded: When the operational limits of a leader controller has reached either because of AP numbers or number of member controllers additions, the leader rejects addition of more controllers and display this reason for rejection.
3. Invalid Group order: If the grouping order is not in the way they have been formulated for reasons such as memory corruption or if the data-structures have been corrupted while transmission or a unknown controller type is attempting to join –Then this error msg is displayed.
4. **Source Not Included**: No valid source identification.
5. **Weak Signal Strength**: (Not applicable to static RF grouping) nearest neighbor is not close enough
6. **Join Pending**: When a member controller is waiting to complete and exit one RRM state to another, when it can join as a member.
7. **Not a Manager**: An unlikely scenario, When a RF group member is wrongly being acknowledged as a RF leader.
8. **RRM Assigning**: in progress
9. **Grouping disabled**: When RF grouping is switched "OFF" at the configured member
10. **Invalid Protocol Version**: If the RF member controller image is of an incompatible version or if there's a version mismatch.
11. **Country code mismatch**: Configured country mismatch
12. **Invalid hierarchy**: if lower priority controller is trying to add higher priority controller.
13. **Already a static leader**: If trying to add a member who's already been manually configured to be a static leader.
14. **Already Static Member**: When trying to add a member who's already been accepted a static member of another RF leader.
15. **Non-Static Member**:
16. **Not Intended**:
17. **Member Deletion Error**: If error is specifically known to occur due to improper memory allocation of de-allocation.
18. **RF-domain mismatch**: If the RF domain of the configured member and the RF leader is different.
19. **Split for invalid-state request**: An error state if there's a member split because of an 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's a user triggered transition because of reset while modifying country code, sys-name change or other
22. **Switch Size Exceeded**: