

# Radio Resource Management under Unified Wireless Networks

Document ID: 71113

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used
- Conventions

Upgrading to 4.1.185.0 or Later: What to Change or Verify?

### Radio Resource Management: Tips and Best Practices

- RF Grouping and Tx Power Threshold
- Coverage Profile and Client SNR Cut-Off
- Neighbor Message Frequency (RF Group Formation)
- Use of On-Demand Option
- Load Balancing Window

### Radio Resource Management: Introduction

#### Radio Resource Management: Concepts

- Key Terms
- A Bird's-Eye View of RRM
- RF Grouping Algorithm
- Dynamic Channel Assignment Algorithm
- Transmit Power Control Algorithm
- Coverage Hole Detection and Correction Algorithm

#### Radio Resource Management: Configuration Parameters

- RF Grouping Settings via the WLC GUI
- RF Channel Assignment Settings via the WLC GUI
- Tx Power Level Assignment Settings via the WLC GUI
- Profile Thresholds: WLC GUI

#### Radio Resource Management: Troubleshooting

- Verifying Dynamic Channel Assignment
- Verifying Transmit Power Control Changes
- Transmit Power Control Algorithm Workflow Example
- Coverage Hole Detection and Correction Algorithm Workflow Example
- Debug and Show Commands

### APPENDIX A: WLC Release 4.1.185.0 RRM Enhancements

- RF Grouping Algorithm
- Dynamic Channel Assignment Algorithm
- Tx Power Control Algorithm
- Coverage Hole Algorithm
- SNMP Trap Enhancements
- Cosmetic/Other Enhancements
- Load-Balancing Changes

### APPENDIX B: WLC Release 6.0.188.0 RRM Enhancements

- RRM Fixes for Medical Devices

### Related Information

# Introduction

This document details the functionality and operation of Radio Resource Management (RRM) and provides an in-depth discussion of the algorithms behind this feature.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Lightweight Access Point Protocol (LWAPP)
- Common wireless LAN (WLAN)/radio frequency (RF) design considerations (knowledge comparable to that of the Planet 3 Wireless CWNA certification)

**Note:** Client Aggressive Load-Balancing and Rogue Detection/Containment (and other Cisco Intrusion Detection System [IDS]/Cisco IOS® Intrusion Prevention System [IPS] features) are not functions of RRM and are beyond the scope of this document.

### Components Used

This document is not restricted to specific software and hardware versions.

### Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

## Upgrading to 4.1.185.0 or Later: What to Change or Verify?

1. From the CLI, check:

```
show advanced [802.11b|802.11a] txpower
```

The new default value is -70dbm. If it has been modified, revert to the defaults since this new value has been shown to be optimal under a range of conditions. This value needs to be the same on all the controllers in an RF group. Remember to save the configuration after making changes.

In order to change this value, issue this command:

```
config advanced [802.11b|802.11a] tx-power-control-thresh 70
```

2. From the CLI, check:

```
show advanced [802.11a|802.11b] profile global
```

The results should be:

```
802.11b Global coverage threshold..... 12 dB for 802.11b
802.11a Global coverage threshold..... 16 dB for 802.11a
```

If the results are different, then you use these commands:

```
config advanced 802.11b profile coverage global 12
config advanced 802.11a profile coverage global 16
```

The client SNR cut-off parameter that determines if the client is in violation, and if the Coverage Hole algorithm's mitigation kicks in, called Coverage should be reverted back to the defaults for optimum results.

3. From the CLI, check:

```
show load-balancing
```

The default state of load-balancing is now *Disabled*. If enabled, the default window is now 5. This is the amount of clients that need to be associated to a radio before load-balancing upon association will take place. Load-balancing can be very useful in a high density client environment, and the use of this feature must be a decision from the administrator so client association and distribution behavior is understood.

## Radio Resource Management: Tips and Best Practices

### RF Grouping and Tx Power Threshold

#### TIPS:

- Ensure that the Tx power threshold is configured the same on all controllers that share the RF Group Name.
- In versions earlier than 4.1.185.0, the default Tx power threshold was  $-65\text{dBm}$ , but this threshold value of  $-65\text{dBm}$  can be too hot for most deployments. Better results have been observed with this threshold set between  $-68\text{dBm}$  and  $-75\text{dBm}$ . With Version 4.1.185.0, the default Tx power threshold is now  $-70\text{dBm}$ . With 4.1.185.0 or later, it is strongly advised that users change the Tx power threshold to  $-70$  and verify if the results are satisfactory. This is a strong recommendation since various RRM enhancements can cause your current setting to be sub-optimal now.

#### WHY:

The RF Group Name is an ASCII string configured per wireless LAN controller (WLC). The grouping algorithm elects the RF Group leader that, in turn, calculates the Transmit Power Control (TPC) and Dynamic Channel Assignment (DCA) for the entire RF Group. The exception is Coverage Hole algorithm (CHA), which is run per WLC. Because RF Grouping is dynamic, and the algorithm runs at 600-second intervals by default, there might be an instance where new neighbors are heard (or existing neighbors are no longer heard). This causes a change in the RF Group that could result in the election of a new Leader (for one or multiple logical RF Groups). At this instance, the Tx Power Threshold of the new group leader is used in the TPC algorithm. If the value of this threshold is inconsistent across multiple controllers that share the same RF Group Name, this can result in discrepancies in resultant Tx power levels when the TPC is run.

### Coverage Profile and Client SNR Cut-Off

#### TIP:

- Set the Coverage measurement (defaults to 12dB) to 3dB for most deployments.

**Note:** With Version 4.1.185.0, enhancements such as the Tx Power Up Control and User-configurable number of SNR profile threshold-violating clients, the defaults of 12dB for 802.11b/g and 16dB for 802.11a should work fine in most environments.

#### WHY:

The Coverage measurement, 12 dB by default, is used to arrive at the maximum tolerable SNR per client. If the client SNR exceeds this value, and if even one client exceeds this value, the CHA is triggered by the WLC whose access point (AP) detects the client with poor SNR. In cases where legacy clients are present (who often have poor roaming logic), tuning the tolerable noise floor down to 3dB results provides a short-term fix (this fix is not required in 4.1.185.0 or later).

This is further described under *Sticky Client Power-up Consideration* in the Coverage Hole Detection and Correction Algorithm section.

## Neighbor Message Frequency (RF Group Formation)

### TIPS:

- The longer the configured interval between transmitting neighbor messages, the slower convergence/stabilization time will be throughout the system.
- If an existing neighbor is not heard for 20 minutes, the AP is pruned out of the neighbor list.

**Note:** With Version 4.1.185.0, the neighbor list pruning interval is now extended to keep the neighbor from whom a neighbor packet has not been heard for up to 60 minutes.

### WHY:

Neighbor messages, by default, are sent every 60 seconds. This frequency is controlled by the Signal Measurement (termed Neighbor Packet Frequency in 4.1.185.0 and later) under the Monitor Intervals section on the Auto RF page (see Figure 15 for reference). It is important to understand that neighbor messages communicate the list of neighbors that an AP hears, which is then communicated to their respective WLCs, who in turn form the RF Group (this assumes that the RF Group name is configured the same). The RF convergence time entirely depends on the frequency of neighbor messages and this parameter must be appropriately set.

## Use of On-Demand Option

### TIP:

- Use the On-Demand button for finer control, and deterministic RRM behavior.

**Note:** With Version 4.1.185.0, predictability can be achieved via the usage of DCA s anchor-time, interval and sensitivity configuration.

### WHY:

For users that desire predictability on algorithmic changes throughout the system, RRM can be run in on-demand mode. When used, RRM algorithms compute optimum channel and power settings to be applied at the next 600-second interval. The algorithms are then dormant until the next time on-demand option is used; the system is in a freeze state. See Figure 11 and Figure 12, and the respective descriptions for more information.

## Load Balancing Window

### TIP:

- The default setting for load-balancing is ON, with the load-balancing window set to 0. This window should be changed to a higher number, such as 10 or 12.

**Note:** In release 4.1.185.0 and later, the default setting for load-balancing is OFF and if enabled, the window size defaults to 5.

## **WHY:**

Although not related to RRM, aggressive load-balancing can result in sub-optimal client roaming results for legacy clients with poor roaming logic, which makes them sticky clients. This can have adverse effects on the CHA. The default load-balancing window setting on the WLC is set to 0, which is not a good thing. This is interpreted as the minimum number of clients that should be on the AP before the load-balancing mechanism kicks in. Internal research and observation has shown that this default should be changed to a more practical value, such as 10 or 12. Naturally, every deployment presents a different need and the window should therefore be set appropriately. This is the command-line syntax:

```
(WLC) >config load-balancing window ?  
<client count> Number of clients (0 to 20)
```

In dense production networks, the controllers have been verified to function optimally with load-balancing ON and window size set at 10. In practical terms, this means load-balancing behavior is only enabled when, for example, a large group of people congregate in a conference room or open area (meeting or class). Load-balancing is very useful to spread these users between various available APs in such scenarios.

**Note:** Users are never thrown off the wireless network. Load-balancing only occurs upon association and the system will try to encourage a client towards a more lightly loaded AP. If the client is persistent, it will be allowed to join and never left stranded.

## **Radio Resource Management: Introduction**

Along with the marked increase in the adoption of WLAN technologies, deployment issues have similarly risen. The 802.11 specification was originally architected primarily with a home, single-cell use in mind. The contemplation of the channel and power settings for a single AP was a trivial exercise, but as pervasive WLAN coverage became one of users' expectations, determining each AP's settings necessitated a thorough site survey. Thanks to the shared nature of 802.11's bandwidth, the applications that are now run over the wireless segment are pushing customers to move to more capacity-oriented deployments. The addition of capacity to a WLAN is an issue unlike that of wired networks where common practice is to throw bandwidth at the problem. Additional APs are required to add capacity, but if configured incorrectly, can actually lower system capacity due to interference and other factors. As large-scale, dense WLANs have become the norm, administrators have continuously been challenged with these RF configuration issues that can increase operating costs. If handled improperly, this can lead to WLAN instability and a poor end user experience.

With finite spectrum (a limited number of non-overlapping channels) to play with and given RF's innate desire to bleed through walls and floors, designing a WLAN of any size has historically proven to be a daunting task. Even given a flawless site survey, RF is ever-changing and what might be an optimal AP channel and power schema one moment, might prove to be less-than-functional the next.

Enter Cisco's RRM. RRM allows Cisco's Unified WLAN Architecture to continuously analyze the existing RF environment, automatically adjusting APs' power levels and channel configurations to help mitigate such things as co-channel interference and signal coverage problems. RRM reduces the need to perform exhaustive site surveys, increases system capacity, and provides automated self-healing functionality to compensate for RF dead zones and AP failures.

## **Radio Resource Management: Concepts**

## Key Terms

Readers should fully understand these terms used throughout this document:

- **Signal:** any airborne RF energy.
- **dBm:** an absolute, logarithmic mathematical representation of the strength of an RF signal. dBm is directly correlated to milliwatts, but is commonly used to easily represent output power in the very low values common in wireless networking. For example, the value of  $-60$  dBm is equal to  $0.000001$  milliwatts.
- **Received Signal Strength Indicator (RSSI):** an absolute, numeric measurement of the strength of the signal. Not all 802.11 radios report RSSI the same, but for the purposes of this document, RSSI is assumed to directly correlate with received signal as indicated in dBm.
- **Noise:** any signal that cannot be decoded as an 802.11 signal. This can either be from a non-802.11 source (such as a microwave or Bluetooth device) or from an 802.11 source whose signal has been invalidated due to collision or any other retarding of the signal.
- **Noise floor:** the existing signal level (expressed in dBm) below which received signals are unintelligible.
- **SNR:** the ratio of signal strength to noise floor. This value is a relative value and as such is measured in decibels (dB).
- **Interference:** unwanted RF signals in the same frequency band that can lead to a degradation or loss of service. These signals can either be from 802.11 or non-802.11 sources.

## A Bird's-Eye View of RRM

Before getting into the details of how RRM algorithms work, it is important to first understand a basic work-flow of how an RRM system collaborates to form an RF Grouping, as well as understand what RF computations happen where. This is an outline of the steps that Cisco's Unified Solution goes through in learning, grouping, and then computing all RRM features:

1. Controllers (whose APs need to have RF configuration computed as a single group) are provisioned with the same RF Group Name. An RF Group Name is an ASCII string each AP will use to determine if the other APs they hear are a part of the same system.
2. APs periodically send out Neighbor Messages, sharing information about themselves, their controllers, and their RF Group Name. These neighbor messages can then be authenticated by other APs sharing the same RF Group Name.
3. APs that can hear these Neighbor Messages and authenticate them based on the shared RF Group Name, pass this information (consisting primarily of controller IP address and information on the AP transmitting the neighbor message) up to the controllers to which they are connected.
4. The controllers, now understanding which other controllers are to be a part of the RF Group, then form a logical group to share this RF information and subsequently elect a group leader.
5. Equipped with information detailing the RF environment for every AP in the RF Group, a series of RRM algorithms aimed at optimizing AP configurations related to the following are run at the RF Group Leader (with the exception of Coverage Hole Detection and Correction algorithm which is run at the controller local to the APs):
  - ◆ DCA
  - ◆ TPC

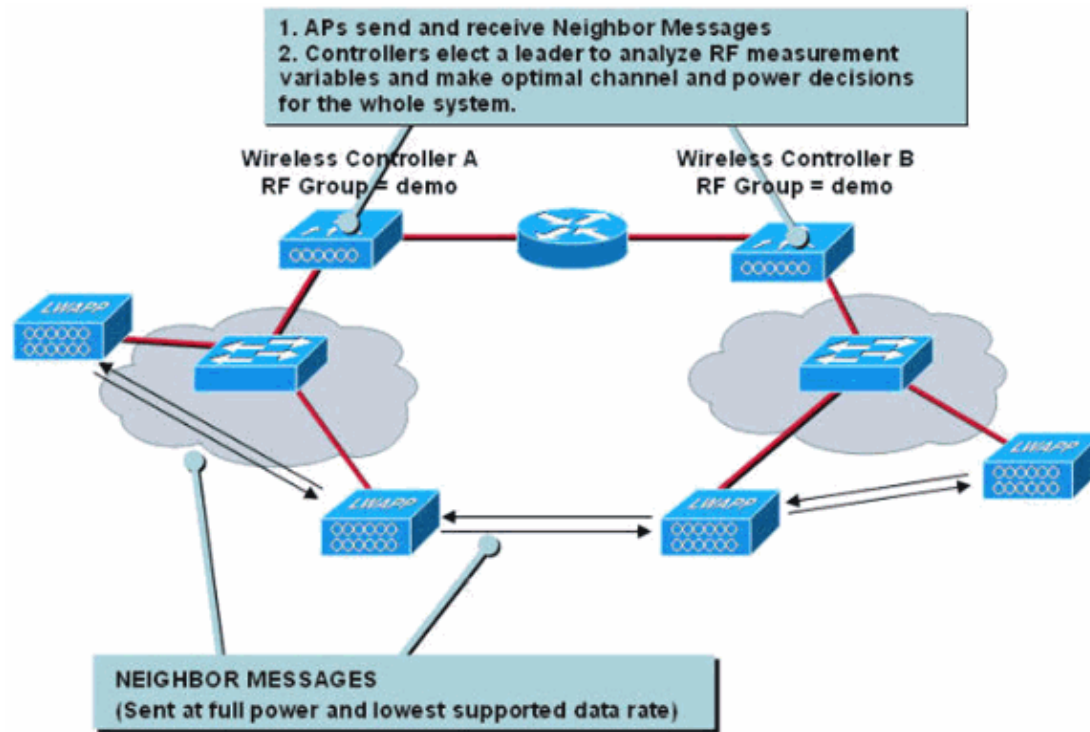
**Note:** RRM (and RF Grouping) is a separate function from inter-controller mobility (and Mobility Grouping). The only similarity is the use of a common ASCII string assigned to both group names during the initial controller configuration wizard. This is done for a simplified setup process and can be changed later.

**Note:** It is normal for multiple logical RF groups to exist. An AP on a given controller will help join their

controller with another controller only if an AP can hear another AP from another controller. In large environments and college campuses it is normal for multiple RF groups to exist, spanning small clusters of buildings but not across the entire domain.

This is a graphical representation of these steps:

**Figure 1: Neighbor Messages from APs give WLCs a system-wide RF view to make channel and power adjustments.**



**Functionality Performed at/by:** RF Grouping WLCs elect the Group Leader Dynamic Channel Assignment Group Leader Transmit Power Control Group Leader Coverage Hole Detection and Correction WLC

## RF Grouping Algorithm

RF Groups are clusters of controllers who not only share the same RF Group Name, but whose APs hear each other.

AP logical collocation, and thus controller RF Grouping, is determined by APs receiving other APs Neighbor Messages. These messages include information about the transmitting AP and its WLC (along with additional information detailed in Table 1) and are authenticated by a hash.

**Field Name Description** Radio Identifier APs with multiple radios use this to identify which radio is being used to transmit Neighbor Messages Group ID A Counter and MAC Address of the WLC WLC IP Address Management IP Address of the RF Group Leader AP s Channel Native channel on which the AP services clients Neighbor Message Channel Channel on which the neighbor packet is transmitted Power Not currently used Antenna Pattern Not currently used

When an AP receives a Neighbor Message (transmitted every 60 seconds, on all serviced channels, at maximum power, and at the lowest supported data rate), it sends the frame up to its WLC to determine whether the AP is a part of the same RF Group by verifying the embedded hash. An AP that either sends

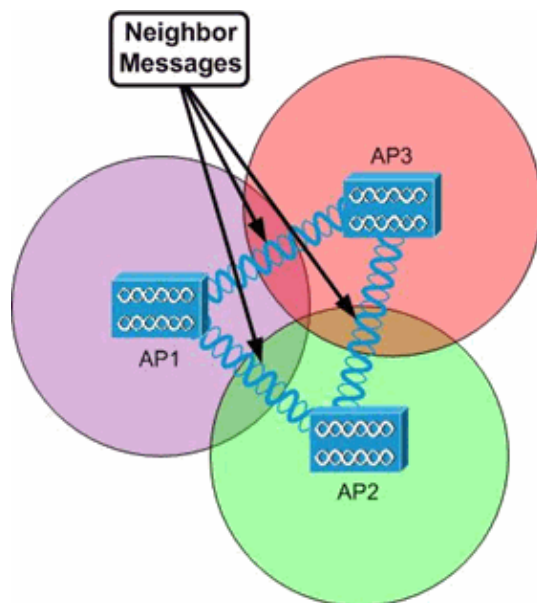
undecipherable Neighbor Messages (indicating a foreign RF Group Name is being used) or sends no Neighbor Messages at all, is determined to be a rogue AP.

**Figure 2: Neighbor Messages are sent every 60 seconds to the multicast address of 01:0B:85:00:00:00.**

18	Airespace:52:A0:A0	01:0B:85:00:00:00	802.11 Data	SNAP	0.000000
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

Given all controllers share the same RF Group Name, in order for an RF Group to form, a WLC need only have a single AP hear one AP from another WLC (see Figures 3 through 8 for further details).

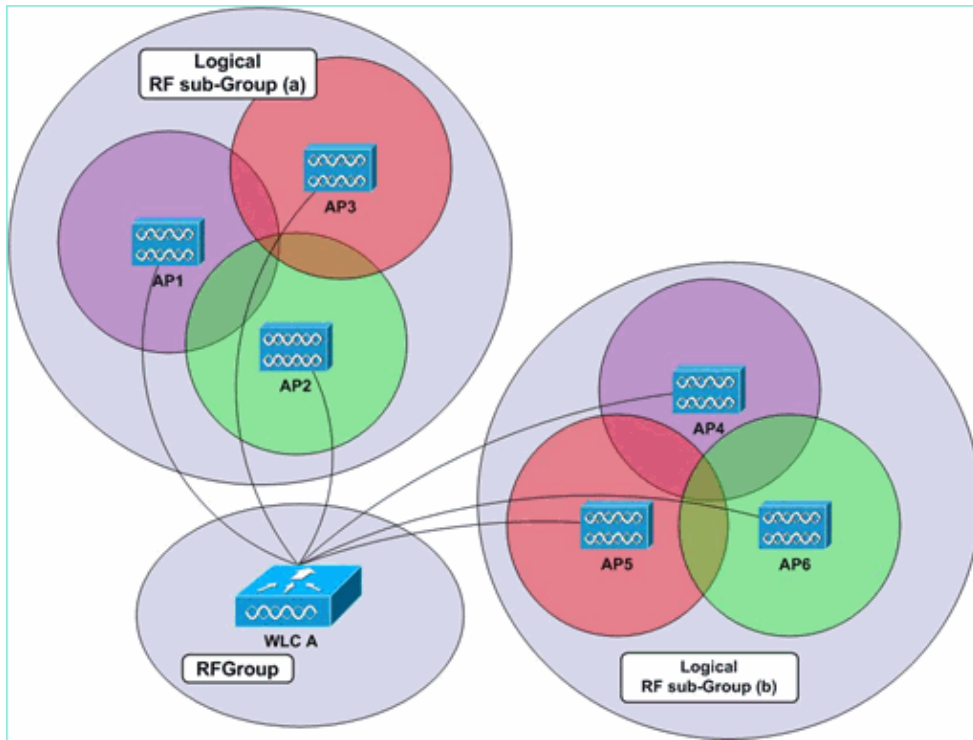
**Figure 3: APs send and receive Neighbor Messages which are then forwarded to their controller(s) to form RF Group.**



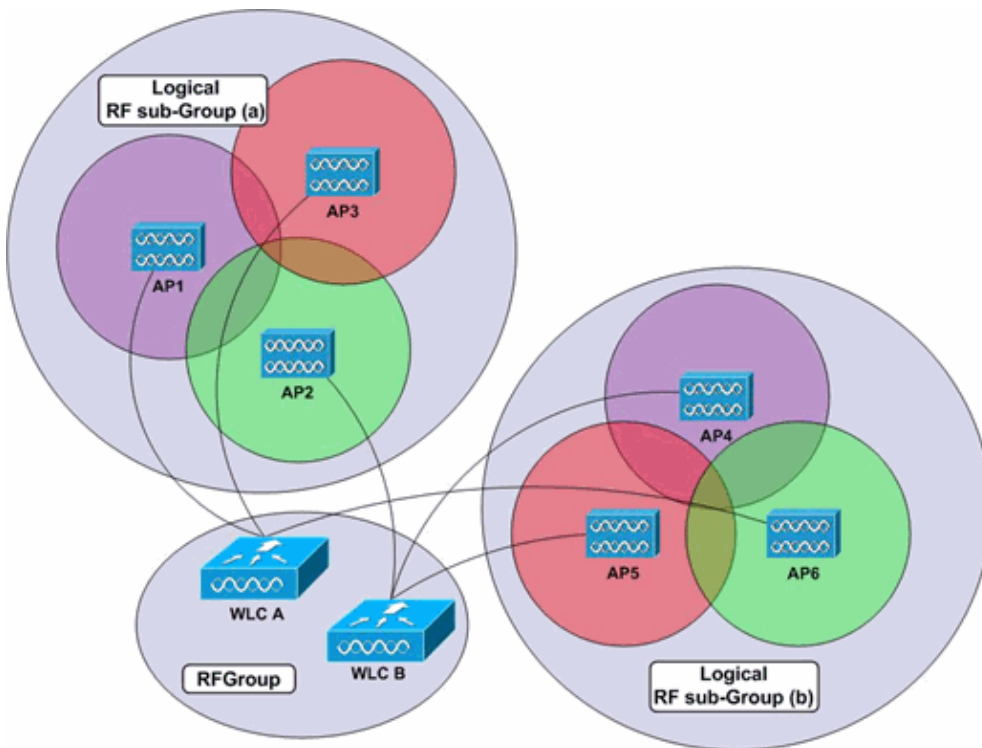
Neighbor Messages are used by receiving APs and their WLCs to determine how to create inter-WLC RF Groups, as well as to create logical RF sub-Groups which consist of only those APs who can hear each other's messages. These logical RF sub-Groups have their RRM configurations done at the RF Group Leader but independently of each other due to the fact that they do not have inter-RF sub-Group wireless connectivity (see Figures 4 and 5).

**Figure 4: All the APs are logically connected to a single WLC, but two separate logical RF sub-Groups are formed because APs 1, 2, and 3 cannot hear Neighbor Messages from APs 4, 5, and 6, and vice versa.**



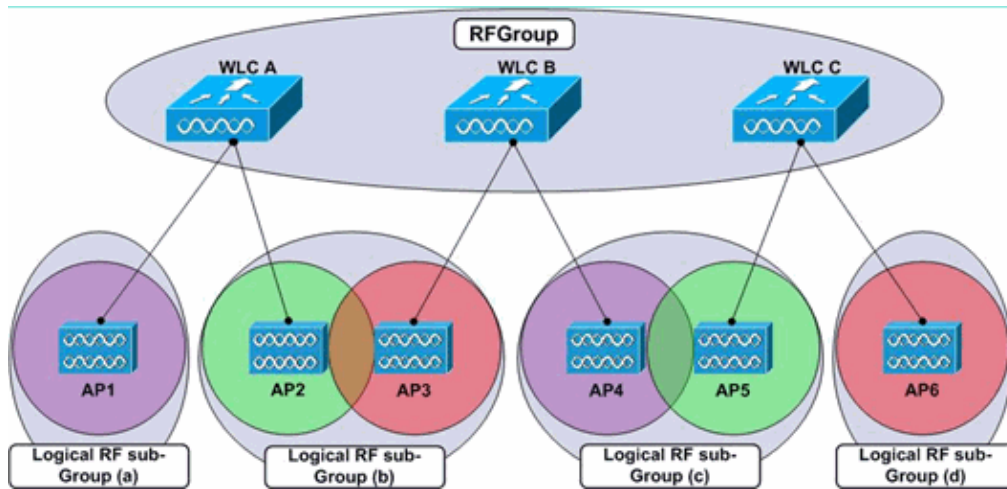


**Figure 5: APs in the same logical RF sub-Group can share a single WLC, each be on a separate WLC, or be on a mix of WLCs. RRM functionality is performed on a system-wide level, so as long as APs can hear each other, their controllers will automatically be grouped. In this example, WLCs A and B are in the same RF Group and their APs are in two different logical RF sub-Groups.**



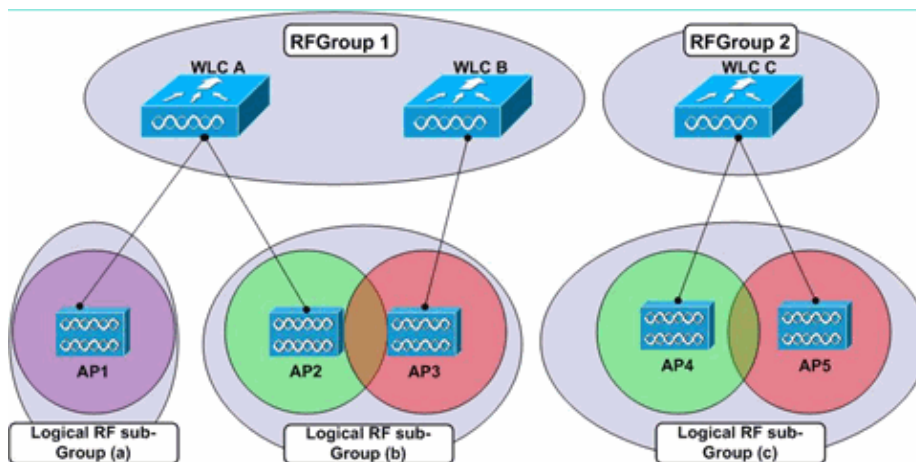
In an environment with many WLCs and many APs, not all APs need to hear each other in order for the whole system to form a single RF Group. Each controller must have at least one AP hear another AP from any other WLC. As such, RF Grouping can occur across many controllers, regardless of each controller's localized view of neighboring APs and thus, WLCs (see Figure 6).

**Figure 6:** In this example, APs connected to WLCs A and C are not able to hear Neighbor Messages from each other. WLC B can hear both WLC A and C and can then share the other s information with them so that a single RF Group is then formed. Discrete logical RF sub-Groups are created for each group of APs that can each other s Neighbor Messages.



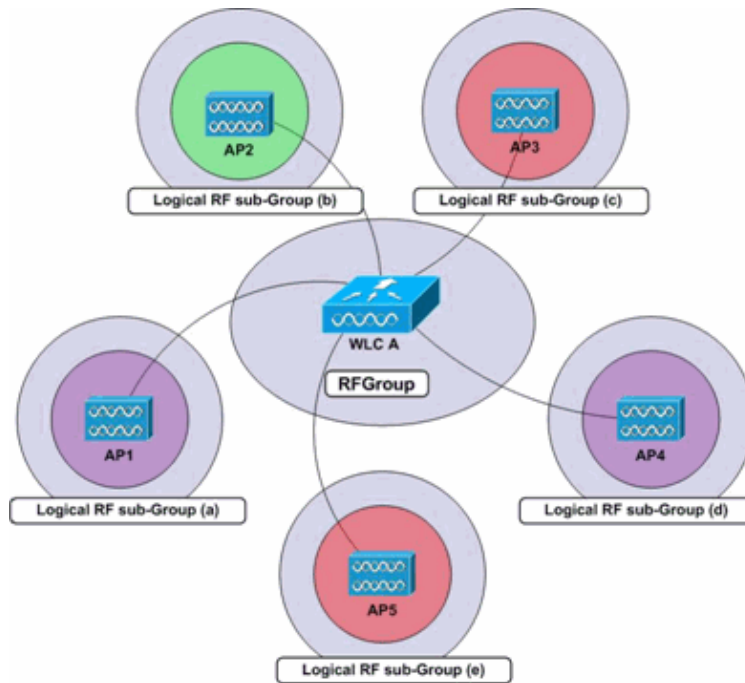
In a scenario where multiple controllers are configured with the same RF Group Name, but their respective APs cannot hear each other s Neighbor Messages, two separate (top-level) RF Groups are formed, as displayed in Figure 7.

**Figure 7:** Although the WLCs share the same RF Group Name, their APs cannot hear each other and hence two separate RF Groups are formed.



RF Grouping occurs at the controller level, which means that once APs report information on the other APs they hear (as well as the controllers to which those APs are connected) to their controllers, each respective WLC then communicates directly with the other WLCs to form a system-wide grouping. Within a single system-wide group, or RF Group, many subsets of APs would have their RF parameters set separately of each other: consider one central WLC with individual APs at remote sites. Each AP would, therefore, have its RF parameters set separately of the others, so while each AP belongs to the same controller RF Grouping, each individual AP (in this example) would be in its own logical RF sub-Group (see Figure 8).

**Figure 8:** Each AP s RF parameters are set separately of others due to their inability to hear each other s Neighbor Messages.



Each AP compiles and maintains a list of up to 34 neighboring APs (per radio) that is then reported up to their respective controllers. Each WLC maintains a list of 24 neighbors per AP radio from the Neighbor Messages sent by each AP. Once at the controller level, this per-AP, per-radio neighbor list of up to 34 APs is then pruned, which drops the ten APs with the weakest signals. WLCs then forward each AP neighbor list up to the RF Group Leader, the WLC elected by the RF Group to perform all RRM configuration decision making.

It is very important to note here that RF Grouping works per radio type. The grouping algorithm runs separately for the 802.11a and 802.11b/g radios, meaning it runs per AP, per radio, such that each AP radio is responsible for populating a list of neighbors. In order to limit flapping, whereby APs might frequently be added and pruned from this list, WLCs will add neighbors to their lists given they are heard at greater than or equal to  $-80$  dBm and will only then remove them once their signals dip below  $-85$  dBm.

**Note:** With Wireless LAN Controller software release 4.2.99.0 or later, RRM supports up to 20 controllers and 1000 access points in an RF group. For example, a Cisco WiSM controller supports up to 150 access points, so you can have up to six WiSM controllers in an RF group (150 access points times 6 controllers = 900 access points, which is less than 1000). Similarly, a 4404 controller supports up to 100 access points, so you can have up to ten 4404 controllers in an RF group (100 times 10 = 1000). The 2100-series-based controllers support a maximum of 25 access points, so you can have up to 20 of these controllers in an RF group. This 1000 limit of AP is not the actual number of APs associated to the controllers, but is calculated based on the maximum number of APs that can be supported by that specific controller model. For example, if there are 8 WiSM controllers (4 WiSMs), each with 70 APs, the actual number of APs is 560. However, the algorithm calculates it as  $8 * 150 = 1200$  (150 being the maximum number of APs supported by each WiSM controller). Therefore, the controllers get split into two groups. One group with 6 controllers and the other with 2 controllers.

Because the controller that functions as the RF Group Leader performs both, the DCA algorithm and the TPC algorithm for the entire system, controllers must be configured with the RF Group Name in a situation when it is anticipated that their neighbor messages will be heard by APs on another controller. If the APs (on different controllers) are geographically separated, at least to an extent that neighbor messages from them can not be heard at or better than  $-80$  dBm, configuring their controllers to be in an RF Group is not practical.

If the upper limit for the RF Grouping algorithm is reached, the group leader controller will not allow any new controllers or APs to join the existing group or contribute to the channel and power calculations. The system will treat this situation as a new logical RF Sub-Group and new members will be added to this new logical

group, configured with the same group name. If the environment happens to be dynamic, in nature where RF fluctuations change how neighbors are seen at periodic intervals, the likelihood of group member alterations and subsequent group leader elections will increase.

## The Group Leader

The RF Group Leader is the elected controller in the RF Group that performs the analysis of the APs' RF data, per logical RF Group, and is responsible for configuration of APs power levels and channel settings. Coverage hole detection and correction is based on client's SNR and is therefore the only RRM function performed at each local controller.

Each controller determines which WLC has the highest Group Leader priority based on the Group Identifier information element in each Neighbor Message. The Group Identifier information element advertised in each Neighbor Message is comprised of a counter value (each controller maintains a 16-bit counter that starts at 0 and increments following events such as an exit from an RF Group or a WLC reboot) and controller MAC address. Each WLC will prioritize the Group Identifier values from its neighbors based first on this counter value and then, in the event of a counter value tie, on the MAC address. Each WLC will select the one controller (either a neighboring WLC or itself) with the highest Group Identifier value, after which each controller will confer with the others to determine which single controller has the highest Group ID. That WLC will then be elected the RF Group Leader.

If the RF Group Leader goes offline, the entire group is disbanded and existing RF Group members rerun the Group Leader selection process and a new leader is chosen.

Every 10 minutes, the RF Group leader will poll each WLC in the group for APs statistics, as well as all their received Neighbor Message information. From this information, the Group Leader has visibility in to the system-wide RF environment and can then use the DCA and TPC algorithms to continuously adjust APs channel and power configurations. The Group Leader runs these algorithms every ten minutes but, as with the Coverage Hole Detection and Correction algorithm, changes are only made if determined necessary.

## Dynamic Channel Assignment Algorithm

The DCA algorithm, run by the RF Group Leader, is applied on a per-RF-Group basis to determine optimal AP channel settings for all the RF Group s APs (each set of APs who can hear each other s Neighbor Messages, referred to in this document as a logical RF sub-Group, has its channel configuration done independently of other logical RF sub-Groups due to the fact that signals do not overlap). With the DCA process, the leader considers a handful of AP-specific metrics that are taken into account when determining necessary channel changes. These metrics are:

- **Load Measurement** Every AP measures the percentage of total time occupied by transmitting or receiving 802.11 frames.
- **Noise** APs calculate noise values on every serviced channel.
- **Interference** APs report on the percentage of the medium taken up by interfering 802.11 transmissions (this can be from overlapping signals from foreign APs, as well as non-neighbors).
- **Signal Strength** Every AP listens for Neighbor Messages on all serviced channels and records the RSSI values at which these messages are heard. This AP signal strength information is the most important metric considered in the DCA calculation of channel energy.

These values are then used by the Group Leader to determine if another channel schema will result in at least a bettering of the worst performing AP by 5dB (SNR) or more. Weighting is given to APs on their operating channels such that channel adjustments are made locally, dampening changes to prevent the domino effect whereby a single change would trigger system-wide channel alterations. Preference is also given to APs based on utilization (derived from each AP s load measurement report) so that a less-used AP will have a higher likelihood of having its channel changed (as compared to a heavily utilized neighbor) in the event a

change is needed.

**Note:** Whenever an AP channel is changed, clients will be briefly disconnected. Clients can either reconnect to the same AP (on its new channel), or roam to a nearby AP, which depends on client roaming behavior. Fast, secure roaming (offered by both CCKM and PKC) will help reduce this brief disruption, given there are compatible clients.

**Note:** When APs boot up for the first time (new out of the box), they transmit on the first non-overlapping channel in the band(s) they support (channel 1 for 11b/g and channel 36 for 11a). When APs power cycle, they use their previous channel settings (stored in the AP's memory). DCA adjustments will subsequently occur as needed.

## Transmit Power Control Algorithm

The TPC algorithm, run at a fixed ten minute interval by default, is used by the RF Group Leader to determine the APs RF proximities and adjust each band's transmit power level lower to limit excessive cell overlap and co-channel interference.

**Note:** The TPC algorithm is only responsible for turning power levels down. The increase of transmission power is a part of the Coverage Hole Detection and Correction algorithm's function, which is explained in the subsequent section.

Each AP reports an RSSI-ordered list of all neighboring APs and, provided an AP has three or more neighboring APs (for TPC to work, you must have a minimum of 4 APs), the RF Group Leader will apply the TPC algorithm on a per-band, per-AP basis to adjust AP power transmit levels downward such that the third loudest neighbor AP will then be heard at a signal level of  $-70\text{dBm}$  (default value or what the configured value is) or lower and the TPC hysteresis condition is satisfied. Therefore, the TPC goes through these stages which decide if a transmit power change is necessary:

1. Determine if there is a third neighbor, and if that third neighbor is above the transmit power control threshold.
2. Determine the transmit power using this equation:  $\text{Tx\_Max for given AP} + (\text{Tx power control thresh} - \text{RSSI of 3rd highest neighbor above the threshold})$ .
3. Compare the calculation from step two with the current Tx power level and verify if it exceeds the TPC hysteresis.
  - ◆ If Tx power needs to be turned down: TPC hysteresis of at least 6dBm must be met. OR
  - ◆ If Tx power needs to be increased: TPC hysteresis of 3dBm must be met.

An example of the logic used in the TPC algorithm can be found in the Transmit Power Control Algorithm Workflow Example section.

**Note:** When all APs boot up for the first time (new out of the box), they transmit at their maximum power levels. When APs are power cycled, they use their previous power settings. TPC adjustments will subsequently occur as needed. See Table 4 for information on the supported AP transmit power levels.

**Note:** There are two main Tx power increase scenarios that can be triggered with the TPC algorithm:

- There is no third neighbor. In this case, the AP defaults back to Tx\_max, and does so right away.
- There is a third neighbor. The TPC equation actually evaluates the recommended Tx to be somewhere in between Tx\_max and Tx\_current (rather than lower than Tx\_current) as in, for example, when the third neighbor "goes away" and there is a new possible third neighbor. This results in a Tx power increase.

TPC-induced Tx decreases take place gradually, but Tx increases can take place right away. However, extra precaution has been taken in how Tx power is increased with Coverage Hole algorithm, going up, one level at a time.

## Coverage Hole Detection and Correction Algorithm

The Coverage Hole Detection and Correction algorithm is aimed at first determining coverage holes based on the quality of client signal levels and then increasing the transmit power of the APs to which those clients are connected. Because this algorithm is concerned with client statistics, it is run independently on each controller and not system-wide on the RF Group Leader.

The algorithm determines if a coverage hole exists when clients SNR levels pass below a given SNR threshold. The SNR threshold is considered on an individual AP basis and based primarily on each AP transmit power level. The higher APs power levels, the more noise is tolerated as compared to client signal strength, which means a lower tolerated SNR value.

This SNR threshold varies based on two values: AP transmit power and the controller Coverage profile value. In detail, the threshold is defined by each AP transmit power (represented in dBm), minus the constant value of 17dBm, minus the user-configurable Coverage profile value (this value is defaulted to 12 dB and is detailed on page 20). The client SNR threshold value is the absolute value (positive number) of the result of this equation.

### Coverage Hole SNR Threshold Equation:

Client SNR Cutoff Value (|dB|) = [AP Transmit Power (dBm) - Constant (17 dBm) - Coverage Profile (dB)]

Once the configured number of clients average SNR dips below this SNR threshold for at least 60 seconds, those clients AP transmit power will be increased to mitigate the SNR violation, therefore correcting the coverage hole. Each controller runs the Coverage Hole Detection and Correction algorithm for each radio on each of its APs every three minutes (the default value of 180 seconds can be changed). It is important to note that volatile environments can result in the TPC algorithm turning the power down at subsequent algorithm runs.

### Sticky Client Power-up Consideration:

Roaming implementations in legacy client drivers can result in clients sticking to an existing AP even in the presence of another AP that is better when it comes to RSSI, throughput and overall client experience. In turn, such behavior can have systemic impact on the wireless network whereby clients are perceived to experience poor SNR (because they have failed to roam) eventually resulting in a coverage hole detection. In such a situation, the algorithm powers up the AP s transmit power (to provide coverage for clients behaving badly) which results in undesirable (and higher than normal) transmit power.

Until the roaming logic is inherently improved, such situations can be mitigated by increasing the Client Min. Exception Level to a higher number (default is 3) and also increasing the tolerable client SNR value (default is 12 dB and improvements are seen when changed to 3 dB). If code version 4.1.185.0 or later is used, the default values provide optimum results in most environments.

**Note:** Although these suggestions are based on internal testing and can vary for individual deployments, the logic behind modifying these still applies.

See the Coverage Hole Detection and Correction Algorithm Example section for an example of the logic involved in the triggering.

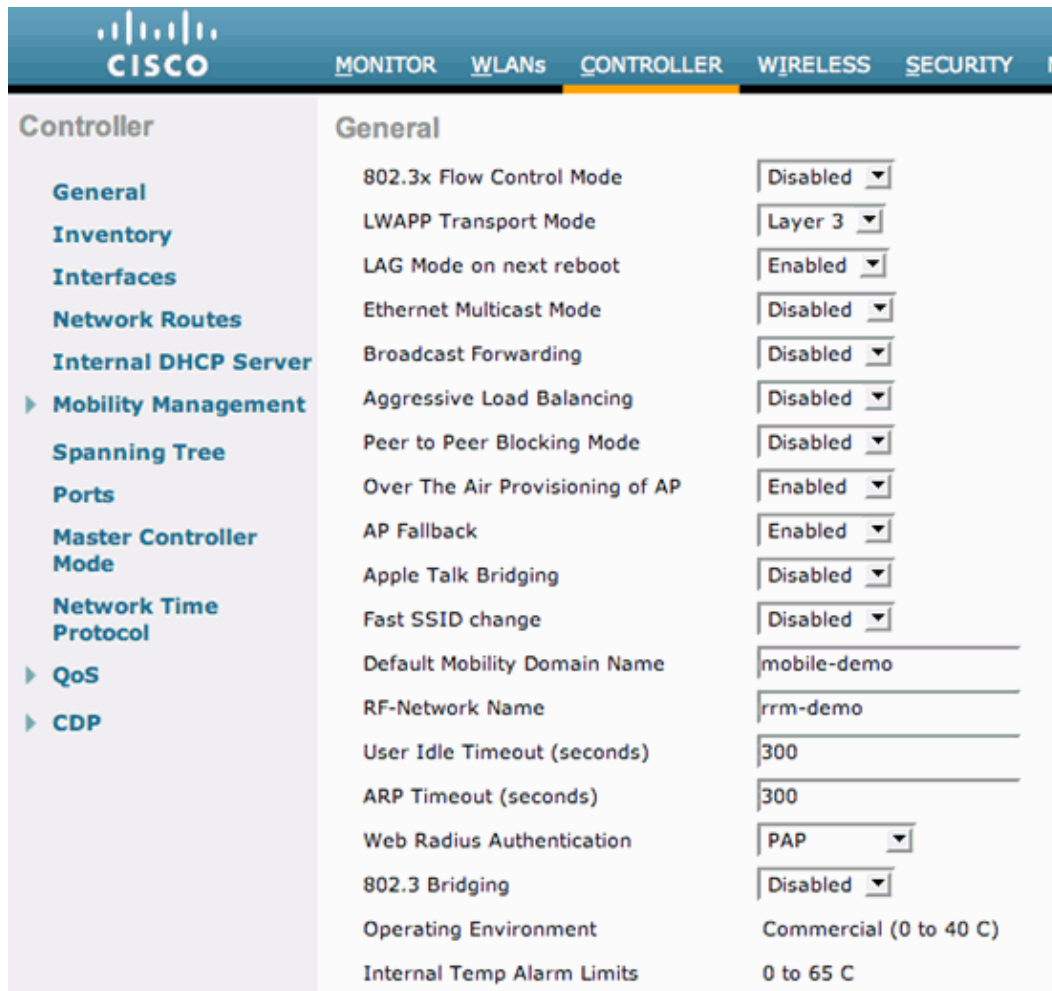
**Note:** The Coverage Hole Detection and Correction algorithm is also responsible for detecting lapses in coverage due to AP failure and powering nearby APs up as needed. This allows the network to heal around service outages.

## Radio Resource Management: Configuration Parameters

Once RRM and the algorithms are understood, the next step is to learn how to interpret and modify necessary parameters. This section details configuration operations of RRM and outlines basic reporting settings, as well.

The very first step to configure RRM is to ensure each WLC has the same RF Group Name configured. This can be done through the controller web interface if you select **Controller | General** and then input a common Group Name value. IP connectivity between WLCs in the same RF Group is a necessity, as well.

**Figure 9: RF Groups are formed based on the user-specified value of RF-Network Name, also called RF Group Name in this document. All WLCs that are required to participate in system-wide RRM operations should share this same string.**



All configuration explanations and examples in the next sections are performed through the WLC graphical interface. In the WLC GUI, go to the main heading of Wireless and select the **RRM** option for the WLAN standard of choice on the left side. Next, select the **Auto RF** in the tree. The subsequent sections reference the resulting page [Wireless | 802.11a or 802.11b/g 9 RRM | Auto RF&].

## RF Grouping Settings via the WLC GUI

- **Group Mode** The Group Mode setting allows RF Grouping to be disabled. Disabling this feature prevents the WLC from grouping with other controllers to perform system-wide RRM functionality. Disabled, all RRM decisions will be local to the controller. RF Grouping is enabled by default and the MAC addresses of other WLCs in the same RF Group are listed to the right of the Group Mode checkbox.
- **Group Update Interval** The group update interval value indicates how often the RF Grouping algorithm is run. This is a display-only field and cannot be modified.
- **Group Leader** This field displays the MAC Address of the WLC that is currently the RF Group Leader. Because RF Grouping is performed per-AP, per-radio, this value can be different for the 802.11a and 802.11b/g networks.
- **Is this controller a Group Leader** When the controller is the RF Group Leader, this field value will be "yes." If the WLC is not the leader, the previous field will indicate which WLC in the group is the leader.
- **Last Group Update** The RF Grouping algorithm runs every 600 seconds (10 minutes). This field only indicates the time (in seconds) since the algorithm last ran and not necessarily the last time a new RF Group Leader was elected.

**Figure 10: The RF Group's status, updates, and membership details are highlighted at the top of the Auto RF page.**

RF Grouping Algorithm		RF Group Members	
Group Mode	<input checked="" type="checkbox"/> Enabled	MAC Address	
Group Update Interval	600 secs	00:16:46:4b:33:40	
Group Leader	00:16:46:4b:33:40		
Is this Controller a Group Leader?	Yes		
Last Group Update	103 secs ago		

## RF Channel Assignment Settings via the WLC GUI

- **Channel Assignment Method** The DCA algorithm can be configured in one of three ways:
  - ◆ **Automatic** This is the default configuration. When RRM is enabled, the DCA algorithm runs every 600 seconds (ten minutes) and, if necessary, channel changes will be made at this interval. This is a display-only field and cannot be modified. Please note the 4.1.185.0 options in Appendix A.
  - ◆ **On Demand** This prevents the DCA algorithm from being run. The algorithm can be manually triggered by clicking on "Invoke Channel Update now" button.

**Note:** If you select **On Demand** and then click **Invoke Channel Update Now**, assuming channel changes are necessary, the DCA algorithm is run and the new channel plan is applied at the next 600 second interval.
  - ◆ **Off** This option disables all DCA functions, and is not recommended. This is typically disabled upon performing a manual site survey and subsequently configuring each AP channel settings individually. Though unrelated, this is often done alongside fixing the TPC algorithm, as well.
- **Avoid Foreign AP Interference** This field allows the co-channel interference metric to be included in DCA algorithm calculations. This field is enabled by default.
- **Avoid Cisco AP Load** This field allows the utilization of APs to be considered when determining which APs channels need changing. AP Load is a frequently changing metric and its inclusion might not be always desired in the RRM calculations. As such, this field is disabled by default.
- **Avoid non-802.11b Noise** This field allows each AP's non-802.11 noise level to be a contributing factor to the DCA algorithm. This field is enabled by default.



- **Signal Strength Contribution** Neighboring APs signal strengths are always included in DCA calculations. This is a display-only field and cannot be modified.
- **Channel Assignment Leader** This field displays the MAC address of the WLC that is currently the RF Group Leader. Because RF Grouping is performed per-AP, per-radio, this value can be different for the 802.11a and 802.11b/g networks.
- **Last Channel Assignment** The DCA algorithm runs every 600 seconds (10 minutes). This field only indicates the time (in seconds) since the algorithm last ran and not necessarily the last time a new channel assignment was made.

**Figure 11: Dynamic Channel Assignment Algorithm Configuration**

Dynamic Channel Assignment Algorithm	
Channel Assignment Method	<input checked="" type="radio"/> Automatic Interval: 600 secs AnchorTime: 0 (Hour of the day) <input type="radio"/> On Demand <span style="border: 1px solid gray; padding: 2px;">Invoke Channel Update now</span> <input type="radio"/> OFF
Avoid Foreign AP interference	<input checked="" type="checkbox"/> Enabled
Avoid Cisco AP load	<input type="checkbox"/> Enabled
Avoid non-802.11b noise	<input checked="" type="checkbox"/> Enabled
Signal Strength Contribution	Enabled
Channel Assignment Leader	00:16:46:4b:33:40
Last Channel Assignment	467 secs ago
DCA Sensitivity Level	MEDIUM (15 dB)

## Tx Power Level Assignment Settings via the WLC GUI

- **Power Level Assignment Method** The TPC algorithm can be configured in one of three ways:
  - ◆ **Automatic** This is the default configuration. When RRM is enabled, the TPC algorithm runs every ten minutes (600 seconds) and, if necessary, power setting changes will be made at this interval. This is a display-only field and cannot be modified.
  - ◆ **On Demand** This prevents the TPC algorithm from being run. The algorithm can be manually triggered if you click the **Invoke Channel Update Now** button.
 

**Note:** If you select **On Demand** and then click **Invoke Power Update Now**, assuming power changes are necessary, the TPC algorithm is run and new power settings are applied at the next 600 second interval.
  - ◆ **Fixed** This option disables all TPC functions, and is not recommended. This is typically disabled upon performing a manual site survey and subsequently configuring each AP power settings individually. Though unrelated, this is often done alongside disabling the DCA algorithm, as well.
- **Power Threshold** This value (in dBm) is the cutoff signal level at which the TPC algorithm will adjust power levels downward, such that this value is the strength at which an AP's third strongest neighbor is heard. In certain rare occasions where the RF environment has been deemed too "hot", in the sense that the APs in a probable high-density scenario are transmitting at higher-than-desired transmit power levels, the **config advanced 802.11b tx-power-control-thresh** command can be used to allow downward power adjustments. This enables the APs to hear their third neighbor with a greater degree of RF separation, which enables the neighboring AP to transmit at a lower power level. This has been an un-modifiable parameter until software release 3.2. The new configurable value ranges from -50dBm to -80dBm and can only be changed from the controller's CLI.
- **Power Neighbor Count** The minimum number of neighbors an AP must have for the TPC algorithm to run. This is a display-only field and cannot be modified.
- **Power Update Contribution** This field is not currently in use.

- **Power Assignment Leader** This field displays the MAC address of the WLC that is currently the RF Group Leader. Because RF Grouping is performed per-AP, per-radio, this value can be different for the 802.11a and 802.11b/g networks.
- **Last Power Level Assignment** The TPC algorithm runs every 600 seconds (10 minutes). This field only indicates the time (in seconds) since the algorithm last ran and not necessarily the last time a new power assignment was made.

**Figure 12: Transmit Power Control Algorithm Configuration**

Tx Power Level Assignment Algorithm	
Power Level Assignment Method	<input checked="" type="radio"/> Automatic Every 600 secs <input type="radio"/> On Demand <input type="button" value="Invoke Power Update now"/> <input type="radio"/> Fixed <input type="text" value="1"/>
Power Threshold	-70 dBm
Power Neighbor Count	3
Power Update Contribution	SNI.
Power Assignment Leader	00:16:46:4b:33:40
Last Power Level Assignment	33 secs ago

## Profile Thresholds: WLC GUI

Profile thresholds, called RRM Thresholds in wireless control systems (WCS), are used principally for alarming. When these values are exceeded, traps are sent up to WCS (or any other SNMP-based management system) for easy diagnosis of network issues. These values are used solely for the purposes of alerting and have no bearing on the functionality of the RRM algorithms whatsoever.

**Figure 13: Default alarming profile threshold values.**

Profile Threshold For Traps	
Interference (0 to 100%)	10
Clients (1 to 75)	12
Noise (-127 to 0 dBm)	-70
Utilization (0 to 100%)	80
Coverage Exception Level (0 to 100 %)	25

- **Interference (0 to 100%)** The percentage of the wireless medium occupied by interfering 802.11 signals before an alarm is triggered.
- **Clients (1 to 75)** The number of clients per-band, per-AP above which, a controller will generate a SNMP trap.
- **Noise (-127 to 0 dBm)** Used to generate a SNMP trap when the noise floor rises above the set level.
- **Coverage (3 to 50 dB)** The maximum tolerable level of SNR per client. This value is used in the generation of traps for both the Coverage Exception Level and Client Minimum Exception Level thresholds. (Part of the Coverage Hole Algorithm sub-section in 4.1.185.0 and later)
- **Utilization (0 to 100%)** The alarming value indicating the maximum desired percentage of the time an AP's radio spends both transmitting and receiving. This can be helpful to track network utilization over time.
- **Coverage Exception Level (0 to 100%)** The maximum desired percentage of clients on an AP's radio operating below the desired Coverage threshold (defined above).
- **Client Min Exception Level** Minimum desired number of clients tolerated per AP whose SNRs are below the Coverage threshold (defined above) (Part of the Coverage Hole Algorithm sub-section in

4.1.185.0 and later).

## Noise / Interference / Rogue Monitoring Channels

Cisco APs provide client data service and periodically scan for RRM (and IDS/IPS) functionality. The channels that the APs are permitted to scan are configurable.

**Channel List:** Users can specify what channel ranges APs will periodically monitor.

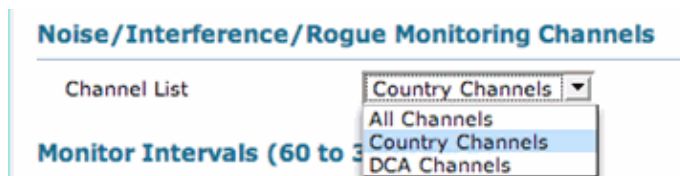
- **All Channels** This setting will direct APs to include every channel in the scanning cycle. This is primarily helpful for IDS/IPS functionality (outside the scope of this document) and does not provide additional value in RRM processes compared to the Country Channels setting.
- **Country Channels** APs will scan only those channels explicitly supported in the regulatory domain configuration of each WLC. This means that APs will periodically spend time listening on each and every channel allowed by the local regulatory body (this can include overlapping channels as well as the commonly used non-overlapping channels). This is the default configuration.
- **DCA Channels** This restricts APs scanning to only those channels to which APs will be assigned based on the DCA algorithm. This means that in the United States, 802.11b/g radios would only scan on channels 1, 6, and 11 by default. This is based on the school of thought that scanning is only focused on the channels that service is being provided on, and rogue APs are not a concern.

**Note:** The list of channels used by the DCA algorithm (both for channel monitoring and assignment) can be altered in WLC code version 4.0, or later. For example, in the United States, the DCA algorithm uses only the 11b/g channels of 1, 6, and 11 by default. In order to add channels 4 and 8, and remove channel 6 from this DCA list (**this configuration is only an example and is not recommended**), these commands need to be inputted in the controller CLI:

```
(Cisco Controller) >config advanced 802.11b channel add 4
(Cisco Controller) >config advanced 802.11b channel add 8
(Cisco Controller) >config advanced 802.11b channel delete 6
```

By scanning more channels, such as the All Channels selection, the total amount of time spent servicing data clients is slightly lessened (as compared to when fewer channels are included in the scanning process). However, information on more channels can be garnered (as compared to the DCA Channels setting). The default setting of Country Channels should be used unless IDS/IPS needs necessitate selecting All Channels, or detailed information on other channels is not needed for both threshold profile alarming and RRM algorithm detection and correction. In this case, DCA Channels is the appropriate choice.

**Figure 14: While Country Channels is the default selection, RRM monitoring channels can be set to either All or DCA channels.**



### Monitor Intervals (60 to 3600 secs)

All Cisco LWAPP-based APs deliver data to users while periodically going off channel to take RRM measurements (as well as perform other functions such as IDS/IPS and location tasks). This off-channel scanning is completely transparent to users and only limits performance by up to 1.5%, in addition to having intelligence built-in to defer scanning until the next interval upon presence of traffic in the voice queue in the last 100ms.

Adjusting Monitor Intervals will change how frequently APs take RRM measurements. The most important timer that controls the RF Groups formation is the Signal Measurement field (known as Neighbor Packet Frequency in 4.1.185.0 and later). The value specified is directly related to the frequency at which the neighbor messages are transmitted, except the EU, and other 802.11h domains, where the Noise Measurement interval is considered, as well.

Regardless of the regulatory domain, the entire scanning process takes approximately 50 ms (per radio, per channel) and runs at the default interval of 180 seconds. This interval can be changed by altering the Coverage Measurement (known as Channel Scan Duration in 4.1.185.0 and later) value. The time spent listening on each channel is a function of the non-configurable 50 ms scan time (plus, the 10ms it takes to switch channels) and number of channels to be scanned. For example, in the United States, all 11 802.11b/g channels, which includes the one channel on which data is being delivered to clients, will be scanned for 50 ms each within the 180 second interval. This means that (in the United States, for 802.11b/g) every 16 seconds, 50 ms will be spent listening on each scanned channel ( $180/11 = \sim 16$  seconds).

**Figure 15: RRM monitoring intervals, and their default values**

Monitor Intervals (60 to 3600 secs)	
Noise Measurement	180
Load Measurement	60
Neighbor Packet Frequency	60
Channel Scan Duration	180

Noise, Load, Signal, and Coverage Measurement intervals can be adjusted to provide more or less granular information to the RRM algorithms. These defaults should be maintained unless otherwise instructed by Cisco TAC.

**Note:** If any of these scanning values are changed to exceed the intervals at which the RRM algorithms are run (600 seconds for both DCA and TPC and 180 seconds for Coverage Hole Detection and Correction), RRM algorithms will still run, but possibly with stale information.

**Note:** When WLCs are configured to bond multiple gigabit Ethernet interfaces using Link Aggregation (LAG), the Coverage Measurement interval is used to trigger the User Idle Timeout function. As such, with LAG enabled, User Idle Timeout is only performed as frequently as the Coverage Measurement interval dictates. This applies only to the WLCs that run firmware versions prior to 4.1 because, in release 4.1, the Idle timeout handling is moved from the controller to the access points.

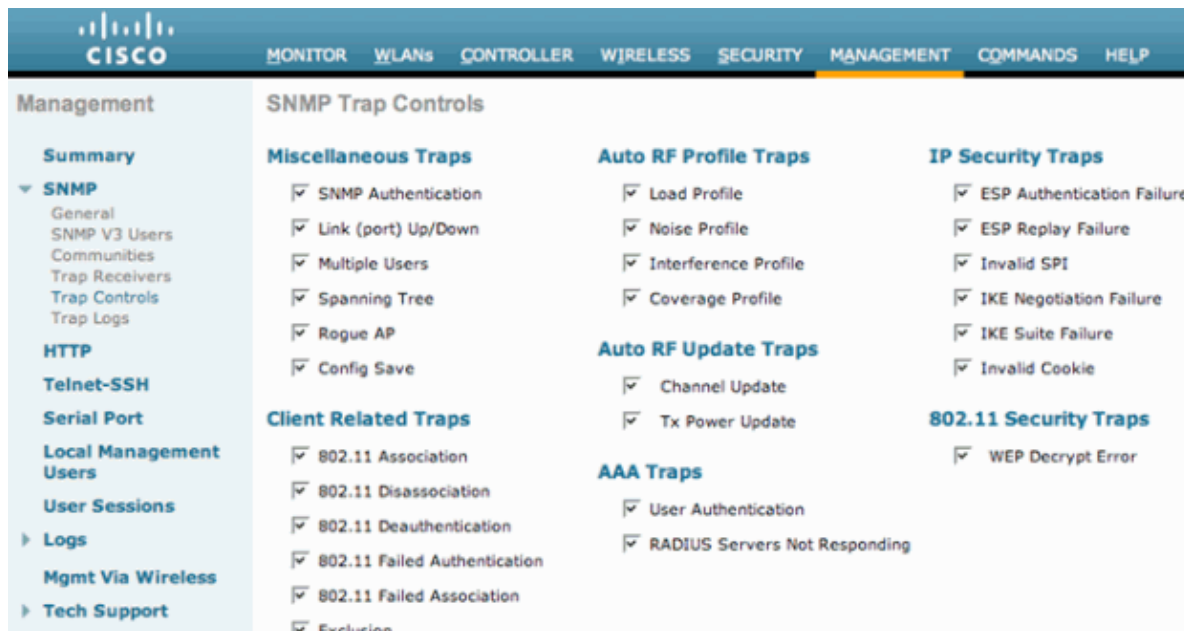
### Factory Default

In order to reset RRM values back to the default settings, click the **Set to Factory Default** button at the bottom of the page.

## Radio Resource Management: Troubleshooting

Changes made by RRM can easily be monitored by enabling the necessary SNMP traps. These settings can be accessed from the Management --> SNMP --> Trap Controls heading in the WLC GUI. All other related SNMP trap settings detailed in this section are located under the Management | SNMP heading where the links for Trap Receivers, Controls, and Logs can be found.

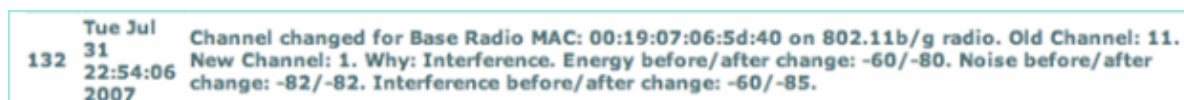
**Figure 16: Auto RF Channel and Power update traps are enabled by default.**



## Verifying Dynamic Channel Assignment

After the RF Group Leader (and the DCA algorithm) has suggested, applied and optimized channel schema, changes can easily be monitored via the Trap Logs sub-menu. An example of such a trap is displayed here:

**Figure 17: The channel change log entries contain the radio s MAC address and the new channel of operation.**



In order to view statistics that detail how long APs retain their channel settings between DCA changes, this CLI-only command provides minimum, average, and maximum values of channel dwell time on a per-controller basis.

```
(Cisco Controller) >show advanced 802.11b channel

Automatic Channel Assignment
Channel Assignment Mode..... AUTO
Channel Update Interval..... 600 seconds
Anchor time (Hour of the day)..... 0
Channel Update Contribution..... SNI.
Channel Assignment Leader..... 00:16:46:4b:33:40
Last Run..... 114 seconds ago

DCA Sensitivity Level: ..... MEDIUM (15 dB)
Channel Energy Levels
  Minimum..... unknown
  Average..... unknown
  Maximum..... unknown
Channel Dwell Times
  Minimum..... 0 days, 09 h 25 m 19 s
  Average..... 0 days, 10 h 51 m 58 s
  Maximum..... 0 days, 12 h 18 m 37 s
Auto-RF Allowed Channel List..... 1,6,11
Auto-RF Unused Channel List..... 2,3,4,5,7,8,9,10
```

## Verifying Transmit Power Control Changes

Current TPC algorithm settings, which includes the tx-power-control-thresh described earlier, can be verified using this command at the controller CLI (802.11b is displayed in this example):

```
(Cisco Controller) >show advanced 802.11b txpower

Automatic Transmit Power Assignment
Transmit Power Assignment Mode..... AUTO
Transmit Power Update Interval..... 600 seconds
Transmit Power Threshold..... -70 dBm
Transmit Power Neighbor Count..... 3 APs
Transmit Power Update Contribution..... SNI.
Transmit Power Assignment Leader..... 00:16:46:4b:33:40
Last Run..... 494 seconds ago
```

As indicated earlier in this document, a densely deployed area that results in increased cell-overlap, which results in high collision and frame retry rates due to high co-channel interference, effectively reducing the client throughput levels could warrant the use of the newly introduced **tx-power-control-thresh** command. In such atypical or anomalous scenarios, the APs hear each other better (assuming the signal propagation characteristics remain constant) compared to how the clients hear them.

Shrinking coverage areas and therefore reducing co-channel interference and the noise floor can effectively improve client experience. However, this command must be exercised with careful analysis of symptoms: high retry rates, high collision counts, lower client throughput levels and overall increased co-channel interference, on the APs in the system (rogue APs are accounted for in the DCA). Internal testing has displayed that modifying the third neighbor's perceived RSSI to  $-70$  dBm in troubleshooting such events has been an acceptable value to begin troubleshooting.

Similar to the traps generated when a channel change occurs, TPC changes generate traps, as well, which clearly indicates all necessary information associated with the new changes. A sample trap is displayed here:

**Figure 18: The Tx Power trap log indicates the new power-level of operation for the specified radio.**



## Transmit Power Control Algorithm Workflow Example

Based on the three steps/conditions defined in the TPC algorithm, the example in this section explains how the calculations are made to determine whether the transmit power of an AP needs to be changed. For the purpose of this example, these values are assumed:

- The Tx\_Max is 20
- The current transmit power is 20 dBm
- The configured TPC threshold is  $-65$  dBm
- The RSSI of the third neighbor is  $-55$  dBm

Plugging this into the three stages of the TPC algorithm results in:

- Condition one: is verified because there is a third neighbor, and it is above the transmit power control threshold.
- Condition two:  $20 + (-65 - (-55)) = 10$
- Condition three: Because the power has to be decreased one level, and a value of ten from condition two satisfies the TPC hysteresis, the Tx power is reduced by 3dB, which brings the new Tx power

down to 17dBm.

- At the next iteration of the TPC algorithm, the AP's Tx power will be lowered further to 14dBm. This assumes all other conditions remain the same. However, it is important to note that the Tx power will not be lowered further (keeping all things constant) to 11dBm because the margin at 14dBm is not 6dB or higher.

## Coverage Hole Detection and Correction Algorithm Workflow Example

In order to illustrate the decision-making process used in the Coverage Hole Detection and Correction algorithm, the example below first outlines the poor received SNR level of a single client and how the system will determine whether a change is needed, as well as what that power change might be.

Remember the Coverage Hole SNR Threshold Equation:

Client SNR Cutoff Value (dB) = [AP Transmit Power (dBm) - Constant (17 dBm) - Coverage Profile (dB)]

Consider a situation where a client might experience signal issues in a poorly covered area of a floor. In such a scenario, these can be true:

- A client has an SNR of 13dB.
- The AP to which it is connected is configured to transmit at 11 dBm (power level 4).
- That AP's WLC has a Coverage profile threshold set to the default of 12 dB.

In order to determine if the client's AP needs to be powered up, these numbers are plugged into the Coverage Hole Threshold Equation, which results in:

- Client SNR cutoff = 11dBm (AP transmit power) - 17dBm (constant value) - 12dB (Coverage threshold) = |-18dB|.
- Because the client's SNR of 13dB is in violation of the present SNR cutoff of 18dB, the Coverage Hole Detection and Correction algorithm will increase the AP's transmit power to 17dBm.
- By using the Coverage Hole SNR Threshold Equation, it is evident that the new transmit power of 17dBm will yield a Client SNR cutoff value of 12dB, which will satisfy the client SNR level of 13 dBm.
- This is the math for the previous step: Client SNR cutoff = 17dBm (AP transmit power) - 17dBm (constant value) - 12dB (Coverage threshold) = |-12dB|.

Supported power output levels in the 802.11b/g band are outlined in Table 4. In order to determine the power level outputs for 802.11a, this CLI command can be run:

```
show ap config 802.11a <ap name>
```

Supported Power Levels	Tx Power (dBm)	Tx Power (mW)
1	20	100
2	17	50
3	14	25
4	11	12.5
5	8	6.5
6	5	6.5
7	2	3.2
8	1.6	0.8
	-1	0.8

## Debug and Show Commands

The **airewave-director** debug commands can be used to further troubleshoot and verify RRM behavior. The top-level command-line hierarchy of the **debug airewave-director** command is displayed here:

```
(Cisco Controller) >debug airewave-director ?  
  
all           Configures debug of all Airewave Director logs  
channel      Configures debug of Airewave Director channel assignment protocol  
error        Configures debug of Airewave Director error logs
```

detail	Configures debug of Airewave Director detail logs
group	Configures debug of Airewave Director grouping protocol
manager	Configures debug of Airewave Director manager
message	Configures debug of Airewave Director messages
packet	Configures debug of Airewave Director packets
power	Configures debug of Airewave Director power assignment protocol
radar	Configures debug of Airewave Director radar detection/avoidance protocol
rf-change	Configures logging of Airewave Director rf changes
profile	Configures logging of Airewave Director profile events

A few important commands are explained in the next sub-sections.

## debug airewave-director all

Use of the **debug airewave-director all** command will invoke all RRM debugs which can help identify when RRM algorithms are run, what data they use, and what changes (if any) are made.

In this example, (output from the **debug airewave-director all** command has been trimmed to show the Dynamic Channel Assignment Process only), the command is run on the RF Group Leader to gain insight into the inner workings of the DCA algorithm and can be broken down into these four steps:

1. Collect and record the current statistics that will be run through the algorithm.

```
Airewave Director: Checking quality of current assignment for 802.11a
Airewave Director: 802.11a AP 00:15:C7:A9:3D:F0(1) ch 161 (before -86.91,
after -128.00)
Airewave Director: 00:15:C7:A9:3D:F0(1)( 36, -76.00)( 40, -81.75)( 44, -81.87)
( 48, -81.87)
Airewave Director: 00:15:C7:A9:3D:F0(1)( 52, -81.87)( 56, -81.85)( 60, -79.90)
( 64, -81.69)
Airewave Director: 00:15:C7:A9:3D:F0(1)(149, -81.91)(153, -81.87)(157, -81.87)
(161, -86.91)
```

2. Suggest a new channel schema and store the recommended values.

```
Airewave Director: Searching for better assignment for 802.11a
Airewave Director: 802.11a AP 00:15:C7:A9:3D:F0(1) ch 161 (before -86.91,
after -128.00)
Airewave Director: 00:15:C7:A9:3D:F0(1)( 36, -76.00)( 40, -81.75)( 44, -81.87)
( 48, -81.87)
Airewave Director: 00:15:C7:A9:3D:F0(1)( 52, -81.87)( 56, -81.85)( 60, -79.90)
( 64, -81.69)
Airewave Director: 00:15:C7:A9:3D:F0(1)(149, -81.91)(153, -81.87)(157, -81.87)
(161, -86.91)
```

3. Compare the current values against the suggested values.

```
Airewave Director: Comparing old and new assignment for 802.11a
Airewave Director: 802.11a AP 00:15:C7:A9:3D:F0(1) ch 161 (before -86.91,
after -86.91)
Airewave Director: 00:15:C7:A9:3D:F0(1)( 36, -76.00)( 40, -81.75)( 44, -81.87)
( 48, -81.87)
Airewave Director: 00:15:C7:A9:3D:F0(1)( 52, -81.87)( 56, -81.85)( 60, -79.90)
( 64, -81.69)
Airewave Director: 00:15:C7:A9:3D:F0(1)(149, -81.91)(153, -81.87)(157, -81.87)
(161, -86.91)
```

4. If necessary, apply the changes for the new channel schema to take effect.

```
Airewave Director: Before -- 802.11a energy worst -86.91, average -86.91,
best -86.91
Airewave Director: After -- 802.11a energy worst -86.91, average -86.91,
best -86.91
```



## debug airewave-director detail Explained

This command can be used to get a detailed, real-time view of RRM functioning on the controller on which it is run. These are explanations of the relevant messages:

- Keep-alive messages being sent to group members to maintain group hierarchy.

```
Airewave Director: Sending keep alive packet to 802.11a group members
```

- Load statistics being calculated on the neighbors reported.

```
Airewave Director: Processing Load data on 802.11bg AP 00:13:5F:FA:2E:00(0)
Airewave Director: Processing Load data on 802.11bg AP 00:0B:85:54:D8:10(1)
Airewave Director: Processing Load data on 802.11bg AP 00:0B:85:23:7C:30(1)
```

- Displays how strong the neighbor messages are being heard and through which APs.

```
Airewave Director: Neighbor packet from 00:0B:85:54:D8:10(1)
received by 00:13:5F:FA:2E:00(0)rssi -36
Airewave Director: Neighbor packet from 00:0B:85:23:7C:30(1)
received by 00:13:5F:FA:2E:00(0)rssi -43
```

- Noise and Interference statistics being calculated at the reported radios.

```
Airewave Director: Sending keep alive packet to
802.11bg group members
Airewave Director: Processing Interference data on
802.11bg AP 00:0B:85:54:D8:10(1)
Airewave Director: Processing noise data on
802.11bg AP 00:0B:85:54:D8:10(1)
Airewave Director: Processing Interference data on
802.11bg AP 00:0B:85:54:D8:10(1)
Airewave Director: Processing Interference data on
802.11bg AP 00:0B:85:23:7C:30(1)
Airewave Director: Processing noise data on
802.11bg AP 00:0B:85:23:7C:30(1)
Airewave Director: Processing Interference data on
802.11bg AP 00:0B:85:23:7C:30(1)
```

## debug airewave-director power

The **debug airewave-director power** command must be run on the WLC local to the AP that is being monitored for Coverage Hole corrections. The output from the command has been trimmed for the purpose of this example.

### Watching Coverage Hole Algorithm run for 802.11a

```
Airewave Director: Coverage Hole Check on
802.11a AP 00:0B:85:54:D8:10(0)
Airewave Director: Found 0 failed clients on
802.11a AP 00:0B:85:54:D8:10(0)
Airewave Director: Found 0 clients close to coverage edge on
802.11a AP 00:0B:85:54:D8:10(0)
Airewave Director: Last power increase 549 seconds ago on
802.11a AP 00:0B:85:54:D8:10(0)
Airewave Director: Set raw transmit power on
802.11a AP 00:0B:85:54:D8:10(0)
to ( 20 dBm, level 1)
```

### Watching Coverage Hole Algorithm run for 802.11b/g

```
Airewave Director: Coverage Hole Check on 802.11bg AP 00:13:5F:FA:2E:00(0)
Airewave Director: Found 0 failed clients on 802.11bg AP 00:13:5F:FA:2E:00(0)
Airewave Director: Found 0 clients close to coverage edge on 802.11bg
```

```

AP 00:13:5F:FA:2E:00(0)
Airewave Director: Last power increase 183 seconds ago on 802.11bg
AP 00:13:5F:FA:2E:00(0)
Airewave Director: Set raw transmit power on 802.11bg AP 00:13:5F:FA:2E:00(0)
to ( 20 dBm, level 1)
Airewave Director: Set adjusted transmit power on
802.11bg AP 00:13:5F:FA:2E:00(0) to ( 20 dBm, level 1)

```

## show ap auto-rf

In order to know which APs are adjacent to other APs, use the command **show ap auto-rf** from the Controller CLI. In the output of this command, there is a field called **Nearby RADs**. This field provides information on the nearby AP MAC addresses and the signal strength (RSSI) between the APs in dBm.

This is the syntax of the command:

```
show ap auto-rf {802.11a | 802.11b} Cisco_AP
```

This is an example:

```

> show ap auto-rf 802.11a AP1

Number Of Slots..... 2
Rad Name..... AP03
MAC Address..... 00:0b:85:01:18:b7
Radio Type..... RADIO_TYPE_80211a
Noise Information
  Noise Profile..... PASSED
  Channel 36..... -88 dBm
  Channel 40..... -86 dBm
  Channel 44..... -87 dBm
  Channel 48..... -85 dBm
  Channel 52..... -84 dBm
  Channel 56..... -83 dBm
  Channel 60..... -84 dBm
  Channel 64..... -85 dBm
Interference Information
  Interference Profile..... PASSED
  Channel 36..... -66 dBm @ 1% busy
  Channel 40..... -128 dBm @ 0% busy
  Channel 44..... -128 dBm @ 0% busy
  Channel 48..... -128 dBm @ 0% busy
  Channel 52..... -128 dBm @ 0% busy
  Channel 56..... -73 dBm @ 1% busy
  Channel 60..... -55 dBm @ 1% busy
  Channel 64..... -69 dBm @ 1% busy
Load Information
  Load Profile..... PASSED
  Receive Utilization..... 0%
  Transmit Utilization..... 0%
  Channel Utilization..... 1%
  Attached Clients..... 1 clients
Coverage Information
  Coverage Profile..... PASSED
  Failed Clients..... 0 clients
Client Signal Strengths
  RSSI -100 dBm..... 0 clients
  RSSI -92 dBm..... 0 clients
  RSSI -84 dBm..... 0 clients
  RSSI -76 dBm..... 0 clients
  RSSI -68 dBm..... 0 clients
  RSSI -60 dBm..... 0 clients
  RSSI -52 dBm..... 0 clients
Client Signal To Noise Ratios

```

```

SNR    0 dBm..... 0 clients
SNR    5 dBm..... 0 clients
SNR   10 dBm..... 0 clients
SNR   15 dBm..... 0 clients
SNR   20 dBm..... 0 clients
SNR   25 dBm..... 0 clients
SNR   30 dBm..... 0 clients
SNR   35 dBm..... 0 clients
SNR   40 dBm..... 0 clients
SNR   45 dBm..... 0 clients
Nearby RADs
  RAD 00:0b:85:01:05:08 slot 0..... -46 dBm on 10.1.30.170
  RAD 00:0b:85:01:12:65 slot 0..... -24 dBm on 10.1.30.170
Channel Assignment Information
  Current Channel Average Energy..... -86 dBm
  Previous Channel Average Energy..... -75 dBm
  Channel Change Count..... 109
  Last Channel Change Time..... Wed Sep 29 12:53e:34 2004
  Recommended Best Channel..... 44
RF Parameter Recommendations
  Power Level..... 1
  RTS/CTS Threshold..... 2347
  Fragmentation Threshold..... 2346
  Antenna Pattern..... 0

```

## APPENDIX A: WLC Release 4.1.185.0 RRM Enhancements

### RF Grouping Algorithm

#### Neighbor List pruning timer

Before the first maintenance release of WLC software 4.1, an AP would keep other APs in its neighbor list for up to 20 minutes from the last time they were heard. In the event of temporary changes in the RF environment, there might have been possibilities where a valid neighbor would have pruned out of a given AP's neighbor list. In order to provide for such temporary changes to the RF environment, the pruning timer for an AP's neighbor list (time since the last neighbor message was heard) has been increased to 60 minutes.

### Dynamic Channel Assignment Algorithm

#### Channel Assignment Method

While in the Automatic mode, the default behavior of DCA before 4.1.185.0 was to compute and apply (if necessary) the channel plans every 10 minutes. Volatile environments might have potentially seen numerous channel changes during the day. Therefore, the need for advanced, finer control on the frequency of DCA arose. In 4.1.185.0 and later, users wishing for finer control over the frequency have the ability to configure these:

- **Anchor Time** Users wishing to change the 10-minute default will have the option to choose an anchor time when the group leader will perform in the Start-up mode. The Start-up mode is defined as a period where the DCA operates every ten minutes for the first ten iterations (100 minutes), with the DCA sensitivity of 5dB. This is the normal mode of operation before the RRM timers were added in release 4.1. This allows for the network to stabilize initially and quickly. After the Start-up mode ends, the DCA runs at the user-defined interval. The Start-up mode operation is clearly indicated in the WLC CLI via the **show advanced 802.11[a|b]** command:

```

(Cisco Controller) >show advanced 802.11a channel

Automatic Channel Assignment

```

```

Channel Assignment Mode..... AUTO
Channel Update Interval..... 600 seconds [startup]
Anchor time (Hour of the day)..... 0
Channel Update Contribution..... SNI.
Channel Assignment Leader..... 00:16:46:4b:33:40
Last Run..... 203 seconds ago

DCA Sensitivity Level: ..... MEDIUM (5 dB)
Channel Energy Levels
  Minimum..... unknown
  Average..... unknown
  Maximum..... unknown
Channel Dwell Times
  Minimum..... unknown
  Average..... unknown
  Maximum..... unknown
Auto-RF Allowed Channel List..... 36,40,44,48,52,56,60,64,100,
  ..... 104,108,112,116,132,136,140,
  ..... 149,153,157,161
Auto-RF Unused Channel List..... 165,20,26

```

- **Interval** The interval value, with the units defined in hours, allows the users to have a predictable network and the channel plan assessments are only computed at the configured intervals. For example, if the configured interval is 3 hours, the DCA computes and assesses a new channel plan every 3 hours.
- **Sensitivity** As described in the DCA Algorithm section, the 5dB hysteresis that is accounted for in the algorithm to assess if the channel plan is improved by running the algorithm is now user-tunable. Allowed configurations are Low, Medium or High Sensitivity with a setting of low indicating the algorithm being very insensitive and a setting of high indicating the algorithm being extremely sensitive. The default sensitivity level is Medium for both bands.
  - ◆ For 802.11a, the sensitivity values equate to: Low (35dB), Medium (20dB) and High (5dB).
  - ◆ For 802.11b/g, the sensitivity values equate to: Low (30dB), Medium (15dB) and High (5dB)

## Tx Power Control Algorithm

### Default Transmit Power Control Threshold

The transmit power control threshold has always carried the responsibility of how APs hear their neighbors, which, in due course is used to decide the transmit power of the AP. As a result of the overall enhancements that have been made to the RRM algorithms in WLC software s 4.1 maintenance release, the default value of -65dBm has also been reconsidered. Therefore, the default which was deemed too hot for most deployments, has been adapted to -70dBm. This results in better cell overlap in most indoor deployments out of the box. However, this default only impacts new installations as the controller maintains the previously configured value if being upgraded from 4.1.171.0 or earlier.

## Coverage Hole Algorithm

### Minimum Clients

Up until the 4.1.185.0, only one client needed to have met the condition (worse SNR threshold than the configured value, or the defaults of 16dB for 802.11a or 12dB for 802.11b/g) for a coverage hole to be detected and the mitigation mechanisms to be kicked in. The Client Minimum Exception Level field is now directly tied to the CHA (and appropriately positioned in the newly created sub-section for the CHA) where the configured value will define how many clients have to meet the SNR threshold for the coverage hole mitigation mechanisms (increasing AP Transmit power) will kick in. It must be noted that most deployments should begin with the defaults (12dB for 802.11b/g and 16dB for 802.11a, and Client minimum exception level of 3) and adjusted only if necessary.

**Figure 19: Coverage Hole Algorithm Sub-section, separated from the Profile Thresholds, with the default values that provide optimum results in most installations**

Coverage Hole Algorithm	
Coverage (3 to 50 dB)	16
Client Min Exception Level (1 to 75)	3

## Tx-Power-Up Control

In addition to allowing the number of clients that need to be in violation for coverage hole mitigation to kick in, the algorithm has also been improved to consider AP transmit power increase in an intelligent manner. While increasing the transmit power to the maximum might have been the safe bet to ensure sufficient mitigation and overlap, it does have adverse effects with the presence of clients with poor roaming implementations. Instead of changing its association to a different AP, typically the one that provides the strongest signal, the client keeps associating to the same old AP that it has moved farther away from. As a consequence, this client is no longer receiving a good signal from the associating AP. A failed client that is a consequence of poor roaming is an example of a possible false positive coverage hole scenario. Poor roaming is not an indication that a genuine coverage hole exists. The potential coverage hole is genuine if:

- It is located within the intended coverage area, and
- Even if the client in this coverage hole were to change its association to any other available AP, the downlink signal the client would receive and the uplink signal at such an alternative AP from the client would still be below the coverage threshold.

In order to avoid and mitigate such scenarios, the AP transmit power is only raised one level at a time (per iteration), which allows genuine coverage holes to benefit from the power increase without running the network hot (avoiding co-channel interference as a result).

## SNMP Trap Enhancements

The SNMP trap generated in the event of a channel change has been enhanced to provide detailed information as to explain the reason for implementing a new channel plan. As evident from this image, the enhanced trap includes the before and after metrics used in the DCA algorithm and which one of those metrics contributed to the channel change for the given AP.

**Figure 20: Improved DCA Trap displays the reason behind a channel change**

Tue Jul 31 132 22:54:06 2007	Channel changed for Base Radio MAC: 00:19:07:06:5d:40 on 802.11b/g radio. Old Channel: 11. New Channel: 1. Why: Interference. Energy before/after change: -60/-80. Noise before/after change: -82/-82. Interference before/after change: -60/-85.
--	---

## Cosmetic/Other Enhancements

- As an undertaking to simplify configuration and improve usability, a new sub-section for the CHA was created, which separates it from the Profile Thresholds sub-section that directly controls the triggers for SNMP Trap generation.
- The terms Signal and Coverage measurements under the Monitor Intervals sub-sections have also been modified to reflect their appropriate meanings: Neighbor Packet Frequency and Channel Scan Duration respectively.

## Load-Balancing Changes

The default setting for load-balancing with 4.1.185.0 and later is OFF. When enabled, the load-balancing window will default to 5 clients.

```
(Cisco Controller) >show load-balancing

Aggressive Load Balancing..... Disabled
Aggressive Load Balancing Window..... 5 clients
```

## APPENDIX B: WLC Release 6.0.188.0 RRM Enhancements

### RRM Fixes for Medical Devices

This feature improves the way that QoS interacts with the RRM scan defer feature. In deployments with certain power-save clients, you sometimes need to defer RRM normal off-channel scanning in order to avoid missing critical information from low-volume clients, such as medical devices that use power-save mode and periodically send telemetry information.

You can use the WMM UP marking of a client in order to tell the access point to defer off-channel scanning for a configurable period of time if it receives a packet marked UP. Use this controller CLI command in order to configure this feature for a specific WLAN:

```
config wlan channel-scan defer-priority priority [enable | disable] WLAN-id
```

where priority = 0 through 7 for user priority. This value must be set to 6 on the client and on the WLAN.

Use this command in order to configure the amount of time that scanning is deferred after an UP packet in the queue:

```
config wlan channel-scan defer-time msec WLAN-id
```

Enter the time value in milliseconds (ms). The valid range is 100 (default) to 60000 (60 seconds). This setting must match the requirements of the equipment on your wireless LAN.

You can also configure this feature on the controller GUI. Select WLANs, and either edit an existing WLAN or create a new one. On the WLANs > Edit page, click the **Advanced** tab. Under Off Channel Scanning Defer, select the scan defer priorities, and enter the defer time in milliseconds.

**Note:** Off-channel scanning is essential to the operation of RRM, which gathers information about alternate channel choices, such as noise and interference. Additionally, off-channel scanning is responsible for rogue detection. Devices that need to defer off-channel scanning must use the same WLAN as often as possible. If there are many of these devices, and the possibility exists that off-channel scanning could be completely disabled by the use of this feature, you must implement an alternative to local AP off-channel scanning, such as monitor access points or other access points in the same location that do not have this WLAN assigned.

Assignment of a QoS policy (bronze, silver, gold, and platinum) to a WLAN affects how packets are marked on the downlink connection from the access point, regardless of how they were received on the uplink from the client. UP=1,2 is the lowest priority, and UP=0,3 is the next higher priority. These are the marking results of each QoS policy:

- Bronze marks all downlink traffic to UP= 1
- Silver marks all downlink traffic to UP= 0
- Gold marks all downlink traffic to UP=4

- [Platinum marks all downlink traffic to UP=6](#)

## Related Information

- [Wireless LAN Controller and IPS Integration Guide](#)
  - [Wireless LAN Controller and Lightweight Access Point Basic Configuration Example](#)
  - [Technical Support & Documentation – Cisco Systems](#)
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: May 17, 2010

Document ID: 71113

---