Radio Resource Management Configuration

Radio Resource Management Configuration

Information about Radio Resource Management

The Radio Resource Management (RRM) software embedded in the controller acts as a built-in radio frequency (RF) engineer to provide consistent, real-time RF management of your wireless network. RRM enables controllers to continually monitor their associated lightweight APs:

- **Traffic Load** - the total bandwidth used for transmitting and receiving traffic. It enables wireless LAN managers to track and plan network growth before client demand.

- **Interference** - the amount of traffic coming from other 802.11 sources.

- **Noise** - the amount of non-802.11 traffic that is interfering with the currently assigned channel.

- **Coverage** - the receiver signal strength indicator (RSSI) and signal-to-noise ratio (SNR)for all connected clients.

- **Other** - the number of nearby APs.

RRM can periodically reconfigure the 802.11 RF network for best efficiency. In order to do this, RRM performs these functions:

- Radio resource monitoring

- Transmit power control

- Dynamic channel assignment

- Coverage hole detection and correction.

For initial configuration purposes, the following covers items in the order that they occur in the current WLC GUI and focuses on predictable things that need adjustment from the default values.

RF Group Name

Assign the RF group name that RRM will use to identify members of your group and base the grouping algorithm to choose RF group leaders. Cisco recommends that you assign a distinctly different name to this test system to avoid interactions with established, production networks. In order to configure the RF Group Name, enter configuration mode at the command line of the mobility controller.

```
(config)#wireless rf-network <name> <cr>
802.11a/b network command
```

Several commands require that the network be disabled in order to execute. You can enable and disable the network very easily from the configuration terminal prompt.

```
Switch(config)#ap dot11 24/5ghz shut
Or use the no form to enable
config)# no ap dot11 24/5ghz shut)
```

This is the display of the default data-rates values. You might need to change several of these:

ap dot11 24/5ghz rate <rate> mandatory/supported/disabled:

As an example - disable 1,2,5.5,11 Mbps, enabling 24,54 Mbps as mandatory, all else supported. 5 GHz has 12, 24 Mbps as mandatory, all else supported:

```
ap dot11 2 shut
ap dot11 2 rate RATE_11M disable
ap dot11 2 rate RATE_1M disable
ap dot11 2 rate RATE_2M disable
ap dot11 2 rate RATE_5_5M disable
% Unable to modify rate, Since this is the last available BSS rate.
```

The above warning is issued since there are no other mandatory rates available – you must have at least one mandatory rate.

```
ap dot11 2 rate RATE_24M mandatory
ap dot11 2 rate RATE_5_5M disable
ap dot11 2 rate RATE_54M mandatory
no ap dot11 2 shut
ap dot11 5 shut
ap dot11 5 rate RATE_6M supported
no ap dot11 5 shut
```

The Legacy ClientLink default setting is disabled:

```
ap dot11 24/5ghz beamforming <cr>
```

Use the no form to disable.

The other Network settings are displayed for reference. Enable 802.11g support (on by default):

```
ap dot11 24ghz dot11g <cr>
```

Beacon interval - default is 100 ms - do not change:

ap dot11 24/5ghz beacon(20-1000 ms)

Short Preamble – on a Cisco AP, short preamble is enabled to allow the AP to adjust the preamble automatically. There is no way to set the preamble to always use short or long preamble. Short preamble is enabled by default. To disable short preamble, use the "no" form of the command:

ap dot11 24/5ghz preamble short<cr>

Fragmentation threshold - default 2346 - Do not change unless you have a significant reason:

ap dot11 24/5ghz fragmentation<256-2346> (bytes)

Dynamic Transmit Power Control (DTPC) support - Default is on. This tells a Cisco Compatible Extension (CCX) client the power level the AP used.

ap dot11 24/5ghz dtpc <cr>

Use the no form of the command to disable.

CCX Location Measurement Q – Default is off; enable if you use the CCX location features:

ap dot11 24/5ghz rrm ccx location-measurement <cr>

Use the no form to disable.

RRM RF Grouping and Next Generation Controller

RF Grouping can be configured for automatic or static modes. For automatic, mobility controllers negotiate with the grouping algorithm in order to choose a group leader. Static mode allows the user to choose a device that will be the group leader as well as add additional members manually. Members must be configured for automatic in order to join the static leader.

Set the RF Grouping Mode

For automatic RF grouping, use this command:

ap dot11 24/5Ghz rrm group-mode auto

For static and adding static members, member mobility controllers must be in automatic grouping mode:

ap dot11 24 rrm group-mode leader
ap dot11 24 rrm group-member Cisco_dd:f8:e4 IP address

Enter this command in order to disable/enable RRM RF Grouping:

ap dot11 24rrm group mode

RRM Transmit Power Control Configuration (TPC)

To configure RRM Transmit Power Control (TPC), choose the mode for the algorithm to operate or disable it. With the exception of the minimum/maximum commands, all TPC configurations are global commands and must be entered on the RF group leader to have an effect on the RF Group.

The default setting for TPC is configured to automatic (auto). In order to change this value, enter this command:

```
ap dot11 24 rrm txpower ?
<1-8>Enter transmit power level
autoEnables auto-RF
maxConfigures maximum auto-RF tx power
minConfigures minimum auto-RF tx power
onceEnables one-time auto-RF
```

If TPC is configured to automatic, then you may need to adjust the TPC-threshold value - (-70 dBm by default) valid range is -80 dBm to -50dBm:

```
ap dot11 24 rrm tpc threshold -70
```

Here is the command that shows the current RRM TPC configuration:

```
show ap dot11 24 txpower
```

RRM DCA Configuration

Dynamic channel assignment (DCA) is a global algorithm. Like TPC, it requires changes to be made to the RF group leader. Making changes to a member will have no effect on the algorithm, unless that member is changed to a leader.

The default DCA is configured to automatic. Other options include on-demand, as well as values for the anchor time and interval:

Use this command in order to enable DCA to run once and freeze:

```
ap dot11 24 rrm channel global once
```

Use this command in order to restore DCA to automatic:

```
ap dot11 24 rrm channel global auto
```

Use this command in order to set DCA to operate on a fixed interval other than the default of 10 minutes:

```
ap dot11 24 rrm channel dca anchor-time 1
ap dot11 24 rrm channel dca interval 8
```

These commands set the anchor time for 1 AM in the RF group leader's time zone and runs DCA every eight hours. Valid interval values are 1,2,3,4,6,8,12 and 24 hours; 0 = 10 minutes (default).

Use this command in order to set the DCA algorithm sensitivity (medium by default) use:

ap dot11 24 rrm channel dca sensitivity low

Options are medium/low/high.

Use this command to assign the channels that DCA will manage. Use one entry per channel, and run for both 2.4 and 5 Ghz bands:

```
ap dot11 24 rrm channel dca 1
ap dot11 24 rrm channel dca 6
ap dot11 24 rrm channel dca 11
```

Use the no form of the command to delete a channel from DCA control to manage options for the DCA algorithm, such as noise avoidance, foreign AP avoidance, load, CleanAir persistent device avoidance, and CleanAir Event Driven Radio Resource Management (EDRRM).

```
ap dot11 24 rrm channel ?
cleanair-event - Configure cleanair event-driven RRM parameters
dca - Config 802.11b dynamic channel assignment algorithm
device - no description - CleanAir PDA
foreign - Configure foreign AP 802.11b interference avoidance
global - Configures all 802.11b Cisco APs
load - Configure Cisco AP 802.11b load avoidance
noise - Configure 802.11b noise avoidance
```

Default values are foreign and noise.

Commands are entered one line at a time. Device, foreign, load, noise are on/off values. Use the no form of the command to turn off. The CleanAir event also has a sensitivity level associated with it. The default value is low; other options are medium and high.

The channel update contribution line indicates that our AP's Signal Noise, Interference (foreign), and Load (SNIUs) are at that moment added to DCA.

RRM Coverage Hole Detection and Mitigation

The default values for Coverage Hole Detection and Mitigation (CHDM) are sufficient for most environments. Items to change include the data/voice RSSI thresholds that determine when to consider a client in a coverage hole condition, the global coverage exception, and the percentage of failed clients per AP. There are other controls that are exposed at the command line. Unless directed, accept the defaults.

CHDM is a per controller configuration basis, and is not global. In order to enable or disable coverage hole detection, enter this command:

ap dot11 24 rrm coverage

Use the no form of the command to disable.

This command adjusts the RSSI threshold for data/voice clients:

ap dot11 24 rrm coverage data rssi-threshold -80

ap dot11 24 rrm coverage voice rssi-threshold -80

In order to set the level that a client is considered in a coverage hole, the default value is 80 dBm; valid range is -90/-60 dBm. The voice and data clients are two separate commands.

This command sets the minimum failed client count and the coverage exception level per AP:

ap dot11 `24 rrm coverage level global 3`

ap dot11 `24 rrm coverage exception global 25`

Three clients and 25% coverage exception are the default values; the available ranges are 1-75 clients and 0-100%.

The minimum failed client count and the exception level work together as a gating function for the feature. The defaults of three clients and 25% translate as a minimum of three clients must be in a coverage hole, and these three clients must represent at least 25% of the clients currently associated to the AP. This is the criterion for mitigation.

Neighbor Discovery Protocol

Neighbor Discovery Protocol (NDP) establishes RF proximity of all APs in your network. This is the basis for all calculations that RRM uses to balance the network for performance. NDP is an over-the-air open protocol by default. It is possible to secure this using encryption, but every member of the RF group must be in the same mode in order for NDP to function. In order to enable NDP protection, enter this command to every mobility agent and mobility controller on the network.

ap dot11 `24 rrm ndp-type protected`