Configuring Aggressive Load Balancing

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Aggressive Load Balancing

- You can configure aggressive load balancing only from the command-line interface.

- Aggressive load balancing is disabled by default, you must enable it manually.

- You can enable load balancing either separately or together with the band select configurations.

- When the band select is enabled on the dual-band clients, the load balancing parameter selects only the lowest load radio from 5-GHz radios. For the 2.4-GHz clients, there is no probe information of the client on 5 GHz and therefore the load balancing algorithm can only be selected between radio on 2.4 GHz.

- You can operate load balancing of clients between access points on the same switch but not for the clients between access points on the different switch.

- The load balancing uses an existing association denial mechanism based on the number of client on the radio and the band select is implemented by the distributed probe response suppression on the access point only.

Information for Configuring Aggressive Load Balancing Parameters

Aggressive Load Balancing

Enabling aggressive load balancing on the controller allows lightweight access points to load balance wireless clients across access points. You can enable aggressive load balancing using the controller.

When a wireless client attempts to associate to a lightweight access point, association response packets are sent to the client with an 802.11 response packet including status code 17. The code 17 indicates that the AP is busy. The AP does not respond with an association response bearing 'success' if the AP threshold is not met, and with code 17 (AP busy) if the AP utilization threshold is exceeded, and another less busy AP heard the client request.

For example, if the number of clients on AP1 is more than the number of clients on AP2 plus the load-balancing window, then AP1 is considered to be busier than AP2. When a client attempts to associate to AP1, it receives an 802.11 response packet with status code 17, indicating that the access point is busy, and the client attempts to associate to a different access point.

You can configure the controller to deny client associations up to 10 times (if a client attempted to associate 11 times, it would be allowed to associate on the 11th try). You can also enable or disable load balancing on a particular WLAN, which is useful if you want to disable load balancing for a select group of clients (such as time-sensitive voice clients).

Note Voice Client does not authenticate when delay is configured more than 300 ms. To avoid this configure a Central-Auth, Local Switching WLAN with CCKM, configure a Pagent Router between AP and WLC with a delay of 600 ms (300 ms UP and 300 ms DOWN and try associating the voice client

The maximum number of client associations that the access points can support is dependent upon the following factors:

- The maximum number of client associations differs for lightweight and autonomous Cisco IOS access points.
- There may be a limit per radio and an overall limit per AP.
- AP hardware (the 16-MB APs have a lower limit than the 32-MB and higher APs)

The Client Association Limits for Lightweight Access Points are as follows:

- For 16-MB APs, the limit is 128 clients per AP. This limit is applicable to 1100 and 1200 series APs.
- For 32-MB and higher APs, there is no per-AP limit.

The maximum Client Association Limits per-radio for all of the Cisco IOS APs is 200 associations.

Note With 32-MB and higher lightweight Cisco IOS APs, with two radios, up to $200 + 200 = 400$ associations are supported.

The maximum Client Association Limits per Autonomous Cisco IOS access point is around 80 to 127 clients per AP. This number varies depending on the following factors:

- AP model (whether it is 16 MB or 32 MB or higher)
- Cisco IOS software release
- Hardware configuration (two radios use more memory than one)
- Enabled features (WDS functionality in particular)

The per-radio limit is about 200 associations. One association will likely hit the per-AP limit first. Unlike Cisco Unified Wireless Network, autonomous Cisco IOS supports per-SSID/per-AP association limits. This limit is configured using the max-associations CLI, under dot11 SSID. The maximum number is 255 associations (which is also the default number).

Note For a FlexConnect AP the association is locally handled. The load-balancing decisions are taken at the Cisco WLC. A FlexConnect AP initially responds to the client before knowing the result of calculations at the Cisco WLC. Load-balancing doesn't take effect when the FlexConnect AP is in standalone mode.

FlexConnect AP does not send (re)association response with status 17 for Load-Balancing as Local mode APs do; instead, it first sends (re)association with status 0 (success) and then deauth with reason 5.

How to Configure Aggressive Load Balancing

Configuring Aggressive Load Balancing

SUMMARY STEPS

1. **configure terminal**
2. **wireless load-balancing window** *client-count*
3. **wireless load-balancing denial** *denial-count*
4. **end**
5. **wlan** *wlan_profile_name wlan_ID SSID_network_name* **load-balance**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** Switch# **configure terminal**	Enters global configuration mode.
Step 2	**wireless load-balancing window** *client-count* **Example:** Switch(config)# **wireless load-balancing window 1**	Sets the client window for aggressive load balancing. You can enter a value between 0 and 20 for the *client_count* parameter.
Step 3	**wireless load-balancing denial** *denial-count* **Example:** Switch(config)# **wireless load-balancing denial-count 1**	Sets the denial count for load balancing. You can enter a value between 0 and 10 for the *denial_count* parameter.
Step 4	**end** **Example:** Switch(config)# **end**	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 5	**wlan** *wlan_profile_name wlan_ID SSID_network_name* **load-balance** **Example:** Switch(config)# **wlan wlan1 25 ssid12** Switch(config-wlan)# **load-balance**	Enables or disables aggressive load balancing on specific WLANs. You can enter a value between 1 and 512 for the *wlan_ID* parameter. You can enter the up to 32 alphanumeric characters for *SSID_network_name* parameter.
Step 6	**end** **Example:** Switch(config)# **end**	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Monitoring Aggressive Load Balancing

This section describes the new command for aggressive load balancing.

The following command can be used to monitor aggressive load balancing on the switch.

Table 1: Monitoring Aggressive Load Balancing Command

Command	Purpose
show wireless load-balancing	Displays the status of the load-balancing feature.

Examples: Aggressive Load Balancing Configuration

This example shows how to configure the load balancing denial count:

```
Switch# configure terminal
Switch(config)# wireless load-balancing denial-count 1
Switch(config)# end
Switch# show wireless load-balancing
```

This example shows how to configure the client window for aggressive load balancing:

```
Switch# configure terminal
Switch(config)# wireless load-balancing window 1
Switch(config)# end
Switch# show wireless load-balancing
```

This example shows how to configure load balancing on specific WLAN:

```
Switch# configure terminal
Switch(config)# wlan wlan1 25 ssid12
Switch(config-wlan)# load-balance
Switch(config)# end
Switch# show wireless load-balancing
```

Additional References for Aggressive Load Balancing

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Performing Aggressive Load Balancing Configuration

Release	Feature Information
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	This feature was introduced.