Aggressive Load Balancing on Wireless LAN Controllers (WLCs) Release 6.0.182.0 and Earlier Configuration Example

Document ID: 107457

Contents

Introduction

This document explains the aggressive load−balancing feature on Wireless LAN Controllers (WLCs) in versions 6.0.182.0 and earlier.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of how to configure the Wireless LAN Controller and lightweight access point (LAP) for basic operation.
- Basic knowledge of Lightweight Access Point Protocol (LWAPP).

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 4400 Series Wireless LAN Controllers that run version 5.0.148.0
- Cisco Aironet 1250 Series Lightweight Access Points
- Cisco Aironet 802.11a/b/g (CB21AG) Wireless LAN Client adapters that run version 3.6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Aggressive Load−Balancing

Aggressive load−balancing on the WLC allows the LAPs to load−balance wireless clients across APs in an LWAPP system.

This feature can be used in order to load−balance clients across LAPs on a single controller.

Aggressive load−balancing works at the association phase. If enabled and the conditions to load−balance are met, when a wireless client attempts to associate to a LAP, association response frames are sent to the client with an 802.11 response packet that includes status code 17. This code indicates that the AP is too busy to accept any more associations.

It is the responsibility of the client to honor, process or discard that association response frame with reason code 17. Some clients ignore it, even though it is part of the 802.11 specification. The standard dictates that the client driver must look for another AP to connect to since it receives a "busy" message from the first AP it tries. Many clients do not do this and send the association request again. The client in question is allowed on to the wireless network upon subsequent attempts to associate.

In WLC versions 6.0.182.0 and earlier, the controller only sends one association response frame with reason code 17 to the client. If the client decides to discard the reason code 17, the client can try the same AP again and this time the AP allows the client to complete the association.

If the client honors the association response status code 17, the client then attempts to associate to a different AP. For example, if load−balancing is enabled and the load−balancing window is configured as five clients, when a sixth client tries to associate to the AP, the client receives an 802.11 Association Response frame with status code 17, which indicates that the AP is busy.

Configure Aggressive Load−Balancing

Aggressive load−balancing can be configured through the CLI or the GUI on the Wireless LAN Controller.

Command Line Interface

In order to enable or disable aggressive load−balancing through the CLI, complete these steps:

1. Issue this command:

   ```
   config load−balancing status {enable | disable}
   ```
2. Issue this command in order to configure the window size:

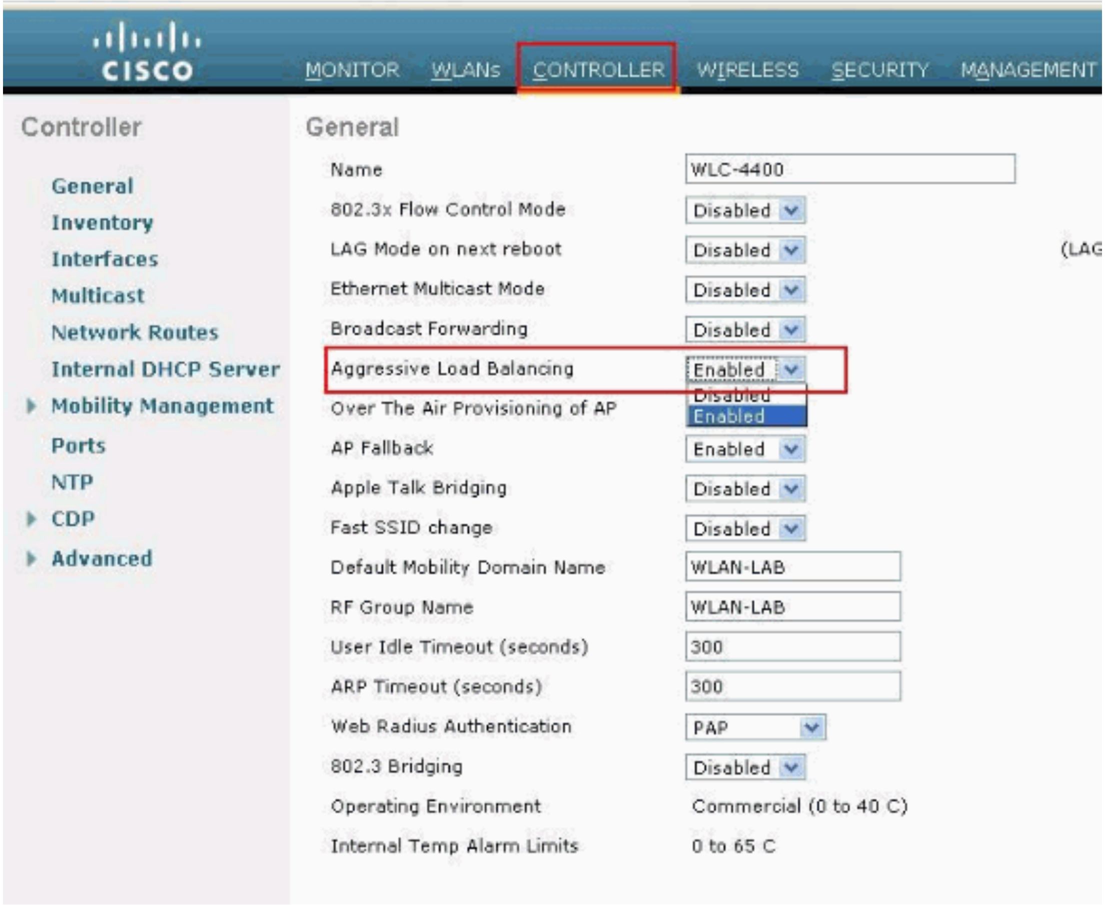
   ```
   configure load−balancing window <size>
   ```

   Note: The size of the window can be from zero to 20.

Graphical User Interface

In order to configure aggressive load−balancing through the GUI, complete these steps:

1. From the controller GUI, click **Controller > General** in order to open the **General** page.
2. From the **Aggressive Load−Balancing** drop−down box, choose either **Enabled** or **Disabled** in order to configure this feature.



General

Name	WLC-4400
802.3x Flow Control Mode	Disabled
LAG Mode on next reboot	Disabled
Ethernet Multicast Mode	Disabled
Broadcast Forwarding	Disabled
Aggressive Load Balancing	Enabled Disabled Enabled
Over The Air Provisioning of AP	
AP Fallback	Enabled
Apple Talk Bridging	Disabled
Fast SSID change	Disabled
Default Mobility Domain Name	WLAN-LAB
RF Group Name	WLAN-LAB
User Idle Timeout (seconds)	300
ARP Timeout (seconds)	300
Web Radius Authentication	PAP
802.3 Bridging	Disabled
Operating Environment	Commercial (0 to 40 C)
Internal Temp Alarm Limits	0 to 65 C

3. Click **Apply**.

Example of Aggressive Load−Balancing

The window setting controls when aggressive load−balancing starts. With a window setting of five, which is the default in version 6.0.182.0 or earlier, all clients after the sixth client are load−balanced.

Here is an example of aggressive load−balancing:

- Two APs, AP1 and AP2, have two and three clients associated to each, respectively.
- Load balancing is enabled, and the window is set to zero.

This information is obtained from debug on the controller:

```
*May 19 13:10:33.023: 00:40:96:b4:8b:ff
   Load Balancing mobile 00:40:96:b4:8b:ff 802.11bg minimum users 0, window 0
*May 19 13:10:33.023: 00:40:96:b4:8b:ff
   Load Balancing mobile 00:40:96:b4:8b:ff on AP 00:17:df:9f:0f:e0(1) band 1 has 0 users
− Good: rssi (antenna−A −31) (antenna−B −57), snr = 57
*May 19 13:10:33.023: 00:40:96:b4:8b:ff
   Load Balancing mobile 00:40:96:b4:8b:ff on AP 00:17:df:9e:ad:d0(1) band 1 has 2 users
−  Bad: rssi (antenna−A −37) (antenna−B −64), snr = 38
*May 19 13:10:33.023: 00:40:96:b4:8b:ff
   Load Balancing mobile 00:40:96:b4:8b:ff could not find acceptable 802.11a candidate
-- defaulting all
*May 19 13:10:33.023: 00:40:96:b4:8b:ff
   Load Balancing mobile 00:40:96:b4:8b:ff is denied association with AP
```

```
00:17:df:9e:ad:d0(1) (count=1)
```

If you debug on a specific client MAC address, this appears:

```
*May 19 13:14:13.432: 00:40:96:b4:8b:ff
   Sending Assoc Response to station on BSSID 00:17:df:9f:0f:e0 (status 17)
```

If the client does not honor the status code 17, and tries again on the original AP, this appears:

```
*May 19 13:14:14.042: 00:40:96:b4:8b:ff
   Load Balancing mobile 00:40:96:b4:8b:ff is permitted to associate with AP
00:17:df:9f:0f:e0(1) ( on RETRY count=1)
```

You can issue this command in order to verify the load−balancing configuration:

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

Aggressive Load Balancing........................ Disabled
Aggressive Load Balancing Window................. 10 clients
```

Note: When you use Cisco 7921 and 7920 wireless IP phones with controllers, make sure that aggressive load−balancing is disabled for each controller. Otherwise, the initial roam attempt by the phone can fail, which causes a disruption in the audio path.

Important Notes on Aggressive Load−Balancing

Here are a few additional things to consider:

- A client that has already been authenticated and associated is never removed from the system as a result of aggressive load−balancing. Load−balancing only happens at the association phase.
- This feature is implemented on a per−controller basis. This means that APs in the same geographic area must all logically connect back to the same WLC if Aggressive load−balancing is desired.

Load−balancing will not take place if:

- The threshold load−balancing window is not exceeded. That is, if the AP requested by the client is a valid candidate AP (current user count <= window + min users).
- The client sends a reassociation request to an AP which it was associated to previously.

Related Information

- **AP Load Balancing and AP Fallback in Unified Wireless Networks**
- **Technical Support & Documentation − Cisco Systems**

Updated: Aug 01, 2011 Document ID: 107457