Aggressive Client Load Balancing

- Aggressive client load balancing, on page 1
- Guidelines of aggressive client load balancing, on page 1
- Restrictions of aggressive client load balancing, on page 2
- Enable aggressive client load balancing (GUI), on page 2
- Configure aggressive client load balancing (GUI), on page 2
- Configure aggressive client load balancing (CLI), on page 3

Aggressive client load balancing

Aggressive client load balancing is a wireless network feature that

- distributes wireless clients across lightweight APs managed by the same controller
- redirects client association attempts from overutilized APs to less busy APs using standardized response codes, and
- helps optimize overall network performance by preventing AP overload.

Guidelines of aggressive client load balancing

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

If AP1 has more clients than AP2 during the load-balancing window, AP1 is considered busier. When a client attempts to associate to AP1, the client receives an 802.11 response packet with status code 17, indicating that the AP is busy, and the client attempts to associate to a different AP.

Configure the embedded wireless controller to deny client associations up to 10 times. If a client tries to connect 11 times, it will connect on the 11th attempt. Enable or disable load balancing on a particular WLAN. This option is helpful if you need to exclude time-sensitive voice clients from load balancing.

Note For a FlexConnect AP, the association is locally handled. The controller makes load-balancing decisions. A FlexConnect AP sends an initial response to the client before knowing the result of the calculations in the controller. Load balancing does not work when the FlexConnect AP is in standalone mode.

In this mode, the FlexConnect AP does not send a (re)association response with status 17 for load balancing. Instead, it first sends a (re)association response with status zero (success), and then sends a deauthentication with reason five.

Restrictions of aggressive client load balancing

- This feature is not supported on the APs joined on default-site-tag.
- This feature is not supported on the APs across different named site-tags.
- This feature is supported only on the APs within a named-site-tag.

Enable aggressive client load balancing (GUI)

Ensure clients are evenly distributed across APs to maximize WLAN performance using GUI.

Procedure

Step 1 Choose **Configuration** > **Wireless** > **WLANs** > **Wireless Networks**.

Step 2 Select a **WLAN** to view the **Edit WLAN** window.

Step 3 Click on the **Advanced** tab.

Step 4 Check the **Load Balance** check box to enable the feature.

Step 5 Click **Update & Apply to Device**.

Configure aggressive client load balancing (GUI)

Set the number of clients and denial count for aggressive load balancing to optimize wireless network performance using GUI.

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Advanced**.

The **Load Balancing** window appears.

Step 2 In the **Aggressive Load Balancing Window (clients)** field, enter the number of clients for the aggressive load balancing client window.

Step 3 In the **Aggressive Load Balancing Denial Count** field, enter the load balancing denial count.

Step 4 Click **Apply**.

Configure aggressive client load balancing (CLI)

Configure aggressive client load balancing to optimize WLAN performance and distribute clients across APs using commands.

Procedure

Step 1 Enter the global configuration mode and specify the WLAN name.

Example:

```
Device# configure terminal
Device(config)# wlan test-wlan
```

Step 2 Disable the WLAN.

Example:

```
Device(config-wlan)# shutdown
```

Step 3 Configure a guest embedded wireless controller as mobility controller, in order to enable client load balance to a particular WLAN.

Example:

```
Device(config-wlan)# load-balance
```

Configure the WLAN security settings as the WLAN requirements.

Step 4 Enable WLAN.

Example:

```
Device(config-wlan)# no shutdown
```

Step 5 Return to the privileged EXEC mode and enter the global configuration mode.

Example:

```
Device(config)# end
Device(config)# configure terminal
```

Step 6 Configure the load balancing denial count.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz} load-balancing denial 10
```

Step 7 Configure the number of clients for the aggressive load balancing client window.

Example:

```
Device(config)# ap dot11 {24ghz | 5ghz} load-balancing window 10
```

Step 8 Return to the privileged EXEC mode.

Example:

```
Device(config-wlan)# end
```

Step 9 Display a filtered section of the current configuration.

Example:

```
Device# show running-config | section test-wlan
```