

WLAN Timeouts

- Client Exclusion Timeout, on page 1
- Session Timeouts, on page 1
- User Idle Timeout, on page 3
- User Idle Timeout per WLAN, on page 4
- Address Resolution Protocol Timeout, on page 5

Client Exclusion Timeout

You can configure a timeout for disabled clients. Clients who fail to authenticate three times when attempting to associate are automatically disabled from further association attempts. After the timeout period expires, the client is allowed to retry authentication until it associates or fails authentication and is excluded again.

You can also enable or disable client exclusion on a per-WLAN basis. If enabled, you can configure the duration of the exclusion period. The activities that trigger client exclusion are configured globally. For more information, see Client Exclusion Policies.

Configuring Client Exclusion Timeout (CLI)

Procedure

- Configure the timeout for disabled clients by entering this command: command:

  config wlan exclusionlist *wlan-id timeout*

  The valid timeout range is between 1 and 2147483647 seconds. A value of 0 permanently disables the client.

- Verify the current timeout by entering this command:

  show wlan

Session Timeouts

You can configure a WLAN with a session timeout. The session timeout is the maximum time for a client session to remain active before requiring reauthorization.

If a WLAN is configured with Layer 2 security, for example WPA2-PSK, and a Layer 3 authentication is also configured, the WLAN session timeout value is overridden with the 802.1X reauthentication timeout value. If APF reauthentication timeout value is greater than 65535, the WLAN session timeout is by default set to 65535; else, the configured 802.1X reauthentication timeout value is applied as the WLAN session timeout.

This section contains the following subsections:

Configuring a Session Timeout (GUI)

Configurable session timeout range is:

- 300-86400 for 802.1X(EAP)
- 0-65535 for all other security types

Note If you configure a session-timeout of 0, it means 86400 seconds for 802.1X (EAP), and it disables the session-timeout for all other security types.

Note When a 802.1X WLAN session timeout value is modified, the associated client's PMK cache does not change to reflect the new session time out value.

Procedure

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to assign a session timeout.

Step 3 When the **WLANs > Edit** page appears, choose the **Advanced** tab. The **WLANs > Edit (Advanced)** page appears.

Step 4 Select the **Enable Session Timeout** check box to configure a session timeout for this WLAN. Not selecting the checkbox is equal to setting it to 0, which is the maximum value for a session timeout for each session type.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Configuring a Session Timeout (CLI)

Procedure

Step 1 Configure a session timeout for wireless clients on a WLAN by entering this command:

config wlan session-timeout *wlan_id timeout*

The default value for WLANs that use 802.1X (EAP) security is 1800 seconds. For all other Layer 2 security types, the default value is 0 seconds.

For 802.1X client security type, which creates the PMK cache, the maximum session timeout that can be set is 86400 seconds when the session timeout is disabled. For other client security such as open, WebAuth, and PSK for which the PMK cache is not created, the session timeout value is shown as infinite when session timeout is disabled.

Step 2 Save your changes by entering this command:

save config

Step 3 See the current session timeout value for a WLAN by entering this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 9
Profile Name..................................... test12
Network Name (SSID).............................. test12

Number of Active Clients......................... 0
Exclusionlist Timeout............................ 60 seconds
Session Timeout.............................. 1800 seconds
```

User Idle Timeout

Configuring User Idle Timeout (GUI)

This configuration is applicable to all the WLAN profiles on the controller. You can also choose to configure the user idle timeout on a per-WLAN basis. The per-WLAN configuration overrides the global configuration.

Procedure

Step 1 Choose **Controller** > **General**.

Step 2 In the **User Idle Timeout** field, enter the timeout value, in seconds. The valid range is 15 to 100000 seconds. The default value is 300 seconds.

Step 3 Save the configuration.

Configuring User Idle Timeout (CLI)

This configuration is applicable to all the WLAN profiles on the controller. You can also choose to configure the user idle timeout on a per-WLAN basis. The per-WLAN configuration overrides the global configuration.

Procedure

- Configure user idle timeout for all the WLAN profiles on the controller by entering this command:
  config network useridletimeout *timeout -in-seconds*

  The valid range is 15 to 100000 seconds. The default value is 300 seconds.

User Idle Timeout per WLAN

This is an enhancement to the present implementation of the user idle timeout feature, which is applicable to all WLAN profiles on the controller. With this enhancement, you can configure a user idle timeout for an individual WLAN profile. This user idle timeout is applicable to all the clients that belong to this WLAN profile.

You can also configure a threshold triggered timeout where if a client has not sent a threshold quota of data within the specified user idle timeout, the client is considered to be inactive and is deauthenticated. If the data sent by the client is more than the threshold quota specified within the user idle timeout, the client is considered to be active and the controller refreshes for another timeout period. If the threshold quota is exhausted within the timeout period, the timeout period is refreshed.

Suppose the user idle timeout is specified as 120 seconds and the user idle threshold is specified as 10 megabytes. After a period of 120 seconds, if the client has not sent 10 megabytes of data, the client is considered to be inactive and is deauthenticated. If the client has exhausted 10 megabytes within 120 seconds, the timeout period is refreshed.

This section contains the following subsections:

Configuring Per-WLAN User Idle Timeout (GUI)

The WLAN configuration overrides the global timeout configuration.

Procedure

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN.

Step 3 On the **WLANs > Edit** window, click the **Advanced** tab.

Step 4 Check the **Client user idle timeout** check box and enter a timeout value, in seconds. The valid range is 15 to 100000 seconds. The default value is 300 seconds.

Step 5 In the **Client user idle threshold** field, enter a threshold value, in bytes. This configures the threshold data sent by the client during the idle timeout for client sessions for the WLAN. If the client sends traffic less than the defined threshold, the client is removed upon timeout. The valid range for the threshold is 0 to 10000000 bytes. The default value is 0 bytes.

Step 6 Save the configuration.

Configuring Per-WLAN User Idle Timeout (CLI)

The WLAN configuration overrides the global timeout configuration.

Procedure

- Configure user idle timeout for a WLAN by entering this command:

  config wlan usertimeout *timeout-in-seconds wlan-id*

- Configure user idle threshold for a WLAN by entering this command:

  config wlan user-idle-threshold *value-in-bytes wlan-id*

Address Resolution Protocol Timeout

The Address Resolution Protocol (ARP) timeout is used to delete ARP entries on controller for devices learned from the network.

There are four types of ARP entries:

- Normal type: Displayed as *Host* on the CLI
- Mobile client type: Displayed as *Client* on the CLI
- Permanent type: Displayed as *Permanent* on the CLI
- Remote type: Displayed as *Client* on the CLI

Only the Normal type ARP entry can be deleted. The other three entries cannot be deleted using the ARP timeout feature.

This section contains the following subsections:

Configuring ARP Timeout (GUI)

Procedure

Step 1 Choose **Controller** > **General**.

Step 2 In the **ARP Timeout** field, enter the timeout value in seconds. By default, the timeout is set to 300 seconds; valid range is 10 to 2147483647 seconds.

Step 3 Save the configuration.

Configuring ARP Timeout (CLI)

Procedure

- Configure the ARP timeout value by entering this command:

config network arptimeout *value-in-seconds*

The default value is 300 seconds; the valid range is 10 to 2147483647 seconds.