Configuring Timeouts

Configuring a Timeout for Disabled Clients

Timeout for Disabled Clients

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. Use these commands to configure a timeout for disabled clients.

Configuring Timeout for Disabled Clients (CLI)

- Configure the timeout for disabled clients by entering the **config wlan exclusionlist** *wlan_id timeout* command. The valid timeout range is 1 to 2147483647 seconds. A value of 0 permanently disables the client.
- Verify the current timeout by entering the **show wlan** command.

Configuring Session Timeout

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 dot1x 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 dot1x 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 clients pmk-cache does not change to reflect the new session time out value.

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)

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 is 1800 seconds for the following Layer 2 security types: 802.1X, Static WEP+802.1X, WPA+WPA2 with 802.1X, CCKM, or 802.1X+CCKM authentication key management and 0 seconds for all other Layer 2 security types (Open WLAN/CKIP/Static WEP). A value of 0 is equivalent to no timeout.

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
...
```

Configuring the User Idle Timeout

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 (CLI)

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*