WLAN Timeouts

Timeouts

Timeout for Disabled Clients

Information About Configuring a 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.

Session Timeout

Information About 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.

Configuring a Session Timeout (GUI)

Configurable session timeout range is:

- 300-86400 for 802.1x.
- 0-65535 for all other security types.

Note If you configure session timeout as 0, it means disabling session-timeout, in case of open system, and 86400 seconds for all other system 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
...
```

User Idle Timeout

Information About the 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.

Configuring Per-WLAN User Idle Timeout (CLI)

- 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 Cisco WLC 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.

Configuring ARP Timeout (GUI)

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)

- 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.

Authentication for Sleeping Clients

Information About Authenticating Sleeping Clients

Clients with guest access that have had successful web authentication are allowed to sleep and wake up without having to go through another authentication process through the login page. You can configure the duration for which the sleeping clients are to be remembered for before reauthentication becomes necessary. The valid range is 10 minutes to 43200 minutes, with the default being 720 minutes. You can configure the duration on a WLAN and on a user group policy that is mapped to the WLAN. The sleeping timer becomes effective after the idle timeout. If the client timeout is lesser than the time configured on the sleeping timer of the WLAN, then the lifetime of the client is used as the sleeping time.

Note The sleeping timer expires every 6 minutes.

This feature is supported in the following FlexConnect scenario: local switching and central authentication.

Caution If the MAC address of a client that goes to sleep mode is spoofed, the fake device such as a laptop can be authenticated.

Following are some guidelines in a mobility scenario:

- L2 roaming in the same subnet is supported.
- Anchor sleeping timer is applicable.
- The sleeping client information is shared between multiple autoanchors when a sleeping client moves from one anchor to another.

From release 8.0 and later, in a High Availability scenario, the sleeping timer is synchronized between active and standby.

Supported Mobility Scenarios

A sleeping client does not require reauthentication in the following scenarios:

- Suppose there are two controllers in a mobility group. A client that is associated with one controller goes to sleep and then wakes up and gets associated with the other controller.
- Suppose there are three controllers in a mobility group. A client that is associated with the second controller that is anchored to the first controller goes to sleep, wakes up, and gets associated with the third controller.
- A client sleeps, wakes up and gets associated with the same or different export foreign controller that is anchored to the export anchor.

Restrictions for Authenticating Sleeping Clients

- The sleep client feature works only for WLAN configured with WebAuth security. Web passthrough is supported on Release 8.0 and later.
- You can configure the sleeping clients only on a per-WLAN basis.
- The authentication of sleeping clients feature is not supported with Layer 2 security and web authentication enabled.
- The authentication of sleeping clients feature is supported only on WLANs that have Layer 3 security enabled.
- With Layer 3 security, the Authentication, Passthrough, and On MAC Filter failure web policies are supported. The Conditional Web Redirect and Splash Page Web Redirect web policies are not supported.
- The central web authentication of sleeping clients is not supported.
- The authentication of sleeping clients feature is not supported on guest LANs and remote LANs.
- A guest access sleeping client that has a local user policy is not supported. In this case, the WLAN-specific timer is applied.
- In a High Availability scenario, the client entry is synchronized between active and standby, but the sleeping timer is not synchronized. If the active controller fails, the client has to get reauthenticated when it associates with the standby controller.

- The number of sleeping clients that are supported depends on the controller platform:
  - Cisco 2504 Wireless Controller—500
  - Cisco 5508 Wireless Controller—1000
  - Cisco 5520 Wireless Controller—25000
  - Cisco Flex 7510 Wireless Controller—25000 with Release 7.6 and later; 9000 in earlier releases
  - Cisco 8510 Wireless Controller—25000 with Release 7.6 and later; 9000 in earlier releases
  - Cisco 8540 Wireless Controller—64000
  - Cisco WiSM2—1000
  - Cisco Virtual Wireless LAN Controller—500
- New mobility is not supported.

Configuring Authentication for Sleeping Clients (GUI)

Step 1 Choose **WLANs**.

Step 2 Click the corresponding WLAN ID.
The **WLANs > Edit** page is displayed.

Step 3 Click the **Security** tab and then click the **Layer 3** tab.

Step 4 Select the **Sleeping Client** check box to enable authentication for sleeping clients.

Step 5 Enter the **Sleeping Client Timeout**, which is the duration for which the sleeping clients are to be remembered before reauthentication becomes necessary.
The default timeout is 12 hours.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

Configuring Authentication for Sleeping Clients (CLI)

- Enable or disable authentication for sleeping clients on a WLAN by entering this command:
  config wlan custom-web sleep-client {**enable** | **disable**} *wlan-id*
- Configure the sleeping client timeout on a WLAN by entering this command:
  config wlan custom-web sleep-client timeout *wlan-id duration*
- View the sleeping client configuration on a WLAN by entering this command:
  show wlan *wlan-id*
- Delete any unwanted sleeping client entries by entering this command:
  config custom-web sleep-client delete *client-mac-addr*

- View a summary of all the sleeping client entries by entering this command:
  show custom-web sleep-client summary
- View the details of a sleeping client entry based on the MAC address of the client by entering this command:
  show custom-web sleep-client detail *client-mac-addr*