Configuring 802.11w

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for 802.11w

- To configure 802.11w feature for optional and mandatory, you must have WPA and AKM configured.

Note The RNS (Robust Secure Network) IE must be enabled with an AES Cipher.

- To configure 802.11w as mandatory, you must enable PMF AKM in addition to WPA AKM.

Related Topics

Configuring 802.11w (CLI), on page 3

Disabling 802.11w (CLI), on page 4

Information About 802.11w, on page 2

Restrictions for 802.11w

- 802.11w cannot be applied on an open WLAN, WEP-encrypted WLAN, or a TKIP-encrypted WLAN.
- The WLAN on which 802.11w is configured must have either WPA2-PSK or WPA2-802.1x security configured.

Related Topics

Configuring 802.11w (CLI), on page 3
Disabling 802.11w (CLI), on page 4
Information About 802.11w, on page 2

Information About 802.11w

Wi-Fi is a broadcast medium that enables any device to eavesdrop and participate either as a legitimate or rogue device. Control and management frames such as authentication/deauthentication, association/disassociation, beacons, and probes are used by wireless clients to select an AP and to initiate a session for network services.

Unlike data traffic which can be encrypted to provide a level of confidentiality, these frames must be heard and understood by all clients and therefore must be transmitted as open or unencrypted. While these frames cannot be encrypted, they must be protected from forgery to protect the wireless medium from attacks. For example, an attacker could spoof management frames from an AP to tear down a session between a client and AP.

The 802.11w protocol applies only to a set of robust management frames that are protected by the Management Frame Protection (PMF) service. These include Disassociation, Deauthentication, and Robust Action frames.

Management frames that are considered as robust action and therefore protected are the following:

- Spectrum Management
- QoS
- Block Ack
- SA Query
- Vendor-specific Protected

When 802.11w is implemented in the wireless medium, the following occur:

- Client protection is added by the AP adding cryptographic protection (by including the MIC information element) to deauthentication and disassociation frames preventing them from being spoofed in a DOS attack.
- Infrastructure protection is added by adding a Security Association (SA) teardown protection mechanism consisting of an Association Comeback Time and an SA-Query procedure preventing spoofed association request from disconnecting an already connected client.

Related Topics

Configuring 802.11w (CLI), on page 3
Disabling 802.11w (CLI), on page 4
Prerequisites for 802.11w, on page 1
Restrictions for 802.11w, on page 2
Monitoring 802.11w (CLI), on page 6

How to Configure 802.11w

Configuring 802.11w (CLI)

Before you begin

WPA and AKM must be configured.

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **shutdown**
4. **security pmf** {**association-check** *association-comeback-time-in-seconds* | **mandatory** | **optional** | **saquery** *saquery-time-in-milliseconds*}
5. **no shutdown**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**shutdown** **Example:** `Switch shutdown`	Shutdown the WLAN before configuring the PMF.
Step 4	**security pmf** {**association-check** *association-comeback-time-in-seconds* | **mandatory** | **optional** | **saquery** *saquery-time-in-milliseconds*} **Example:**	Configures the PMF parameters with the following options: • **association-comeback**—Configures the 802.11w association comeback time. The range is from 1 to 20 seconds.

	Command or Action	Purpose
	`Switch(config-wlan)# security pmf saquery-retry-time 200`	• **mandatory**—Requires clients to negotiate 802.11w PMF protection on a WLAN. • **optional**—Enables 802.11w PMF protection on a WLAN. • **saquery**—Time interval identified in milliseconds before which the SA query response is expected. If the switch does not get a response, another SQ query is tried. The range is from 100 to 500 ms. The value must be specified in multiples of 100 milliseconds.
Step 5	**no shutdown** **Example:** `Switch no shutdown`	Restart the WLAN for the changes to take effect.
Step 6	**end** **Example:** `Switch(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Related Topics

Information About 802.11w, on page 2
Prerequisites for 802.11w, on page 1
Restrictions for 802.11w, on page 2
Monitoring 802.11w (CLI), on page 6

Disabling 802.11w (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **shutdown**
4. **no security pmf [association-comeback** *association-check-comback-interval-seconds* | **mandatory** | **optional** | **saquery** *saquery-time-interval-milliseconds*]
5. **no shutdown**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Switch# configure terminal`	
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**shutdown** **Example:** `Switch shutdown`	Shutdown the WLAN before configuring the PMF.
Step 4	**no security pmf [association-comeback** *association-check-comback-interval-seconds* | **mandatory** | **optional** | **saquery** *saquery-time-interval-milliseconds*] **Example:** `Switch(config-wlan)# no security pmf`	Disables PMF on the WLAN. The following attributes are available: • **association-comeback**—Disables the 802.11w association comeback time. • **mandatory**—Disables clients to negotiate 802.11w PMF protection on a WLAN. • **optional**—Disables 802.11w PMF protection on a WLAN. • **saquery**—Time interval identified in the association response to an already associated client before the association can be tried again. This time interval checks if the client is a real client and not a rogue client during the association comeback time. If the client does not respond within this time, the client association is deleted from the switch The range is from 100 to 500 ms. The value must be specified in multiples of 100 milliseconds.
Step 5	**no shutdown** **Example:** `Switch no shutdown`	Restart the WLAN for the changes to take effect.
Step 6	**end** **Example:** `Switch(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Related Topics

Information About 802.11w, on page 2
Prerequisites for 802.11w, on page 1
Restrictions for 802.11w, on page 2
Monitoring 802.11w (CLI), on page 6

Monitoring 802.11w (CLI)

The following command can be used to monitor 802.11w:

Command	Description
show wlan name *wlan-profile-name*	Displays the WLAN parameters on the WLAN. The PMF parameters are displayed. Here is an example: . . . . Auth Key Management 802.1x : Disabled PSK : Enabled CCKM : Disabled FT dot1x : Disabled FT PSK : Disabled PMF dot1x : Disabled PMF PSK : Enabled FT Support : Disabled FT Reassociation Timeout : 20 FT Over-The-DS mode : Disabled PMF Support : Required PMF Association Comeback Timeout : 9 PMF SA Query Time : 200 . . . .

Related Topics

Configuring 802.11w (CLI), on page 3
Disabling 802.11w (CLI), on page 4
Information About 802.11w, on page 2

Additional References for 802.11w

Related Documents

Related Topic	Document Title
WLAN Command Reference	*WLAN Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
WLAN Security	*Configuring WLAN Security* chapter in this book.

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
802.11w	IEEE 802.11w Protected Management Frames

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for 802.11w

This table lists the features in this module and provides links to specific configuration information:

Feature Name	Release	Feature Information
802.11w	Cisco IOS XE 3.3SE	This feature was introduced.