802.11w

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. Management frames such as authentication, de-authentication, association, dissociation, beacons, and probes are used by wireless clients to initiate and tear down sessions 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 attack a client associated with the AP.

The 802.11w protocol applies only to a set of robust management frames that are protected by the Protected Management Frames (PMF) service. These include Disassociation, De-authentication, and Robust Action frames.

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

- Spectrum Management
- QoS
- DLS
- Block Ack
- Radio Measurement
- Fast BSS Transition
- SA Query
- Protected Dual of Public Action
- Vendor-specific Protected

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

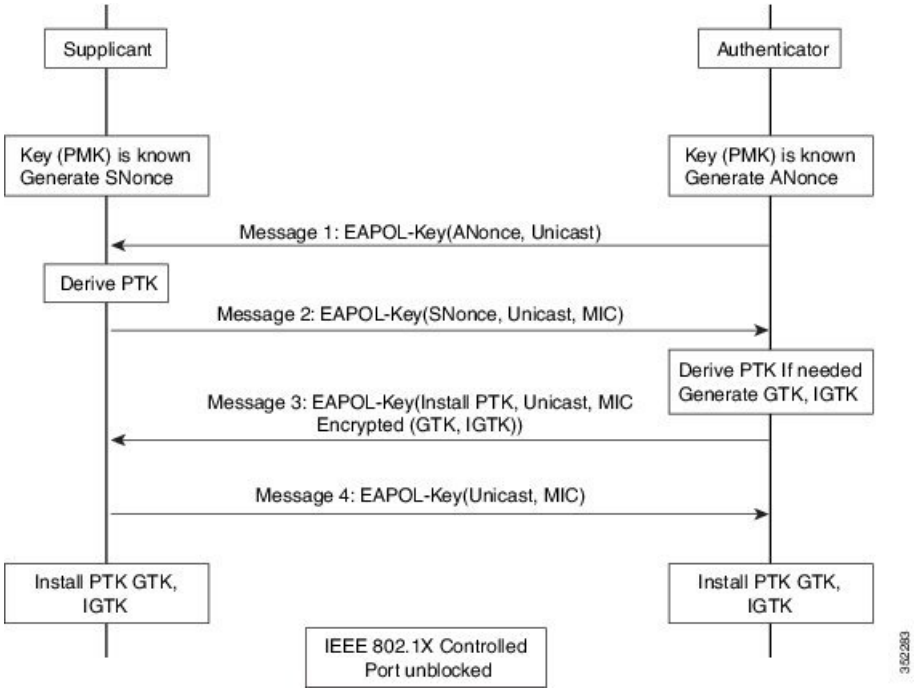
- Client protection is added by the AP adding cryptographic protection to de-authentication and dissociation frames preventing them from being spoofed in a DOS attack.
- Infrastructure protection is added by adding a Security Association (SA) tear down protection mechanism consisting of an Association Comeback Time and an SA-Query procedure preventing spoofed association request from disconnecting an already connected client.

802.11w has introduced a new IGTK Key, which is used to protect broadcast/multicast robust management frames:

- IGTK is a random value assigned by the authenticator STA (WLC) and used to protect MAC management protocol data units (MMPDUs) from that source STA.

When Management Frame Protection is negotiated, the AP encrypts the GTK and IGTK values in the EAPOL-Key frame, which is delivered in Message 3 of 4-way handshake.

Figure 1: IGTK Exchange in 4-way Handshake

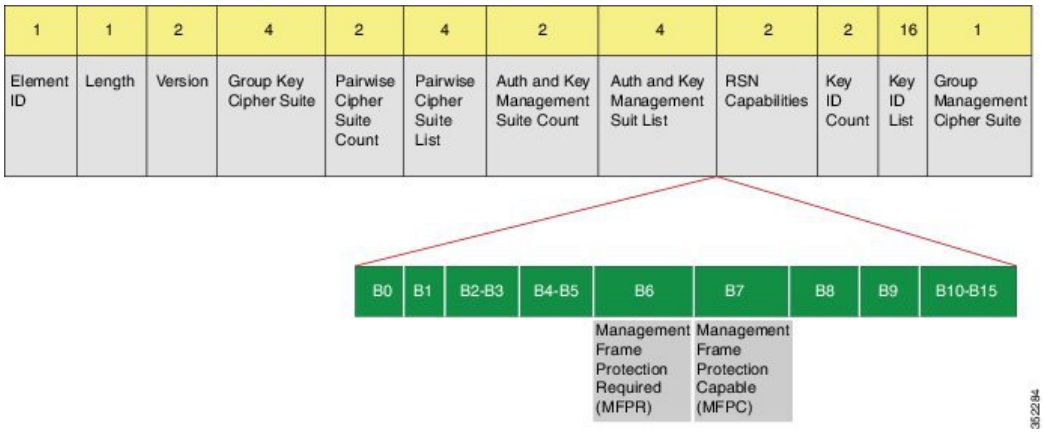


- If the AP later changes the GTK, it sends the new GTK and IGTK to the client using the Group Key Handshake .

802.11w defines a new Broadcast/Multicast Integrity Protocol (BIP) that provides data integrity and replay protection for broadcast/multicast robust management frames after successful establishment of an IGTKSA - It adds a MIC that is calculated using the shared IGTK key.

802.11w Information Elements (IEs)

Figure 2: 802.11w Information Elements

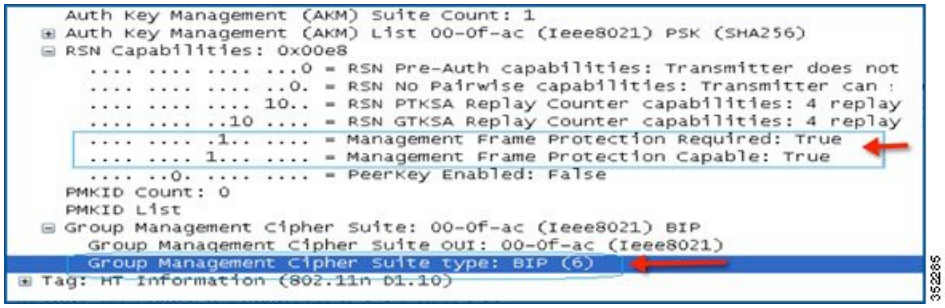


1. Modifications made in the RSN capabilities field of RSNIE.
   a. Bit 6: Management Frame Protection Required (MFPR)
   b. Bit 7: Management Frame Protection Capable (MFPC)
2. Two new AKM Suites, 5 and 6 are added for AKM Suite Selectors.
3. New Cipher Suite with type 6 is added to accommodate BIP.

The WLC adds this modified RSNIE in association and re-association responses and the APs add this modified RSNIE in beacons and probe responses.

The following Wireshark captures shows the RSNIE capabilities and the Group Management Cipher Suite elements.

Figure 3: 802.11w Information Elements



Security Association (SA) Teardown Protection

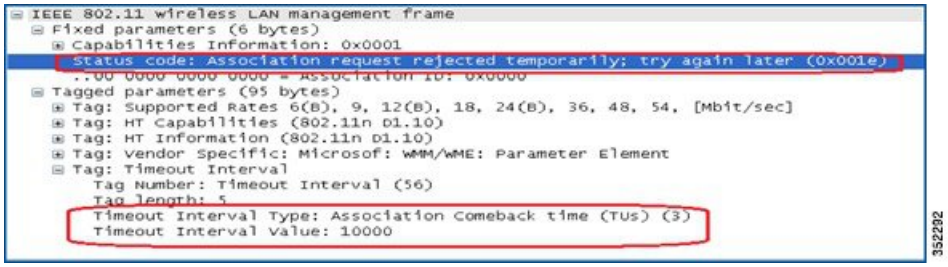
SA teardown protection is a mechanism to prevent replay attacks from tearing down the session of an existing client. It consists of an Association Comeback Time and an SA-Query procedure preventing spoofed association requests from disconnecting an already connected client.

If a client has a valid security association, and has negotiated 802.11w, the AP shall reject another Association Request with status code 30. This status code stands for "Association request rejected temporarily; Try again later". The AP should not tear down or otherwise modify the state of the existing association until the SA-Query

procedure determines that the original SA is invalid and shall include in the Association Response an Association Comeback Time information element, specifying a comeback time when the AP would be ready to accept an association with this client.

The following capture shows the Association Reject message with status code 0x1e (30) and the Association comeback time set to 10 seconds.

Figure 4: Association Reject with Comeback Time



Following this, if the AP is not already engaged in an SA Query with the client, the AP shall issue an SA Query until a matching SA Query response is received or the Association Comeback time expires. An AP may interpret reception of a valid protected frame as an indication of a successfully completed SA Query.

If a SA QUERY response with a matching transaction identifier within the time period, the AP shall allow the association process to be started without starting additional SA Query procedures.

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.

Restrictions for 802.11w

- 802.11w cannot be applied on an open WLAN, WEP-encrypted WLAN, or a TKIP-encrypted WLAN.
- Cisco Catalyst 9800 Series Wireless Controller supports 802.11w + PMF combination for non-Apple clients. But Apple iOS version 11 and earlier require fix from the Apple iOS side to resolve the association issues.
- The controller will ignore disassociation or deauthentication frames sent by the clients if they are not using 802.11w PMF. The client entry will only get deleted immediately upon reception of such a frame if the client uses PMF. This is to avoid denial of service by malicious device since there is no security on those frames without PMF.

How to Configure 802.11w

Configuring 802.11w (GUI)

Before you begin

WPA and AKM must be configured.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add** to create WLANs.

The **Add WLAN** page is displayed.

Step 3 In the **Security** > **Layer2** tab, navigate to the **Protected Management Frame** section.

Step 4 Choose **PMF** as *Disabled*, *Optional*, or *Required*. By default, the PMF is *disabled*.

If you choose **PMF** as *Optional* or *Required*, you get to view the following fields:

- **Association Comeback Timer**—Enter a value between 1 and 10 seconds to configure 802.11w association comeback time.
- **SA Query Time**—Enter a value between 100 to 500 (milliseconds). This is required for clients to negotiate 802.11w PMF protection on a WLAN.

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

Configuring 802.11w (CLI)

Before you begin

WPA and AKM must be configured.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id ssid* **Example:** `Device(config)# wlan wlan-test 12 alpha`	Configures a WLAN and enters configuration mode.

	Command or Action	Purpose
Step 3	**security wpa akm dot1x-sha256** **Example:** `Device(config-wlan)#security wpa akm dot1x-sha256`	Configures 802.1x support.
Step 4	**security pmf association-comeback** *comeback-interval* **Example:** `Device(config-wlan)# security pmf association-comeback 10`	Configures the 802.11w association comeback time.
Step 5	**security pmf mandatory** **Example:** `Device(config-wlan)# security pmf mandatory`	Requires clients to negotiate 802.11w PMF protection on a WLAN.
Step 6	**security pmf saquery-retry-time** *timeout* **Example:** `Device(config-wlan)# security pmf saquery-retry-time 100`	Time interval identified in milliseconds before which the SA query response is expected. If the device does not get a response, another SQ query is tried.

Disabling 802.11w

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id ssid* **Example:** `Device(config)# wlan wlan-test 12 alpha`	Configures a WLAN and enters configuration mode.
Step 3	**no security wpa akm dot1x-sha256** **Example:** `Device(config-wlan)# no security wpa akm dot1x-sha256`	Disables 802.1x support.
Step 4	**no security pmf association-comeback** *comeback-interval* **Example:** `Device(config-wlan)# no security pmf association-comeback 10`	Disables the 802.11w association comeback time.

	Command or Action	Purpose
Step 5	**no security pmf mandatory** **Example:** `Device(config-wlan)# no security pmf mandatory`	Disables client negotiation of 802.11w PMF protection on a WLAN.
Step 6	**no security pmf saquery-retry-time** *timeout* **Example:** `Device(config-wlan)# no security pmf saquery-retry-time 100`	Disables SQ query retry.

Monitoring 802.11w

Use the following commands to monitor 802.11w.

Procedure

Step 1 **show wlan name** *wlan-name*

Displays the WLAN parameters on the WLAN. The PMF parameters are displayed.

```
. . . .
. . . .
Auth Key Management
            802.1x                              : Disabled
            PSK                                 : Disabled
            CCKM                                : Disabled
            FT dot1x                            : Disabled
            FT PSK                              : Disabled
            FT SAE                              : Disabled
            Dot1x-SHA256                        : Enabled
            PSK-SHA256                          : Disabled
            SAE                                 : Disabled
            OWE                                 : Disabled
            SUITEB-1X                           : Disabled
            SUITEB192-1X                        : Disabled
    CCKM TSF Tolerance                          : 1000
    FT Support                                  : Adaptive
        FT Reassociation Timeout                : 20
        FT Over-The-DS mode                     : Enabled
    PMF Support                                 : Required
        PMF Association Comeback Timeout        : 1
        PMF SA Query Time                       : 500
. . . .
. . . .
```

Step 2 **show wireless client mac-address** *mac-address* **detail**

Displays the summary of the 802.11w authentication key management configuration on a client.

```
. . . .
. . . .
Policy Manager State: Run
```

```
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 497 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : 802.1x-SHA256
Encrypted Traffic Analytics : No
Management Frame Protection : No
Protected Management Frame - 802.11w : Yes
EAP Type : LEAP
VLAN : 39
Multicast VLAN : 0
Access VLAN : 39
Anchor VLAN : 0
WFD capable : No
Manged WFD capable : No
. . . .
. . . .
```