Technical white paper

WLAN 802.11w Technology

Table of contents

Overview

IEEE 802.11w-2009 is an approved amendment to the IEEE 802.11 standard to protect wireless management frames. It is also known as the Protected Management Frames (PMF) standard.

Technical background

WLAN is vulnerable to attacks because all wireless devices share the same wireless medium. Attackers can easily monitor and spoof wireless frames. To resolve the security problem, IEEE developed WEP as the authentication and encryption method, which has now been replaced by 802.11i. 802.11i uses 802.1X for authentication and CCMP for encryption. If frames are encrypted, even though attackers can still capture frames, they cannot decrypt frames to obtain the initial data.

However, 802.11i can only protect data frames. Management frames are still exposed to attacks. For example, if an attacker obtains the MAC address of a client, it can send a disassociation request to the client in the name of an AP, or send a reassociation request to an AP in the name of the client. The client will be logged off in either situation.

802.11w is developed to protect wireless management frames.

Benefits

802.11w provides the following benefits:

- **Confidentiality**—Encrypts unicast management frames.
- **Connection protection**—Security Association (SA) Query can prevent clients from going offline caused by spoofing reassociation requests.
- **Group addressed frame protection**—Broadcast/Multicast Integrity Protocol (BIP) can protect the integrity of broadcasts and multicasts, prevent replay attacks, and protect clients from spoofing broadcast/multicast attacks.

802.11w protects only specific management frames and does not affect the communication between APs and clients. It can only take effect when both APs and clients have 802.11w enabled. If 802.11w is enabled on rogue APs and rogue clients, WIPS countermeasures become invalid.

802.11w technology implementation

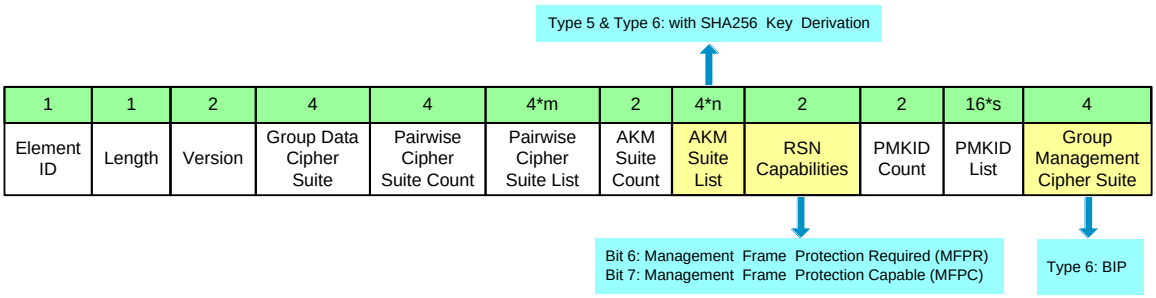
This section describes 802.11w technology implementation.

Management Frame Protection negotiation

Management Frame Protection is negotiated through RSN IE. To support Management Frame Protection negotiation, RSN IE has the following changes:

- Uses HMAC-SHA256 instead of HMAC-SHA1 as the AKM suite to protect security.
- Adds the Group Management Cipher Suite field and Type 5 and Type 6 AKM schemes. Type 6 represents protection to broadcast/multicast frames.
- Uses the RSN Capabilities field to identify Management Frame Protection capabilities.

Figure 1. RSN IE for 802.11w



Clients send RSN IE to APs through association requests and reassociation requests. APs send RSN IE to clients through beacon frames and probe responses.

Protected management frame type

802.11w enables APs to protect management frames, including deauthentication frames, disassociation frames, and action frames, as described in Table 1.

Table 1. Protected management frame type

Protected management frame type	Description
Deauthentication	Deauthentication frames.
Disassociation	Disassociation frames.
Spectrum Management	Spectrum management frames.
QoS	QoS fames.
DLS	DLS frames.
Block Ack	Block acknowledgments.
Radio measurement	Radio measurement frames.
SA Query	SA Query frames.
Protected Dual of Public Action	Protected Dual of Public Action frames.
Fast BSS Transition	Fast BSS transition frames.
Vendor-specific Protected	Reserved. Vendor-specific frames.

SA Query

When Management Frame Protection is enabled, the AP uses SA Query to secure connections with clients.
SA Query contains active and passive SA Query.

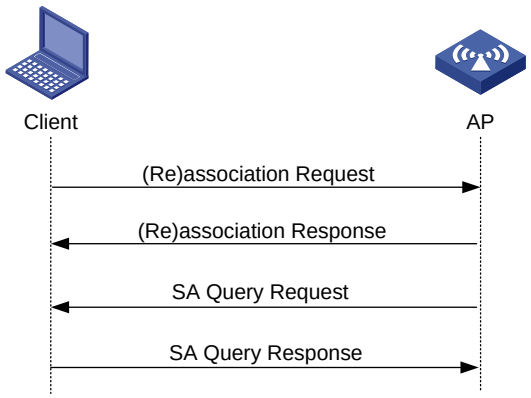
Active SA Query

If the AP receives spoofing association or reassociation requests, active SA Query can prevent the AP from responding to clients.

As shown in Figure 2, active SA Query uses the following process:

1. The client sends an association or a reassociation request to the AP.
2. Upon receiving the request, the AP sends a response to inform the client that the request is denied and the client can associate at a later time. The response contains an association comeback time.
3. The AP sends an SA Query request to the client.
   - If the AP receives an SA Query response within the timeout time, it determines that the client is online.
   - If the AP receives no SA Query response within the timeout time, it resends the request. If the AP receives an SA Query response within the retransmission time, it determines that the client is online.
   - If the client is online, the AP does not respond to any association or reassociation request from the client within the association comeback time.
   - If the AP receives no SA Query response within the retransmission time, it determines that the client is offline. The AP allows the client to reassociate.

Figure 2. Active SA Query



Passive SA Query

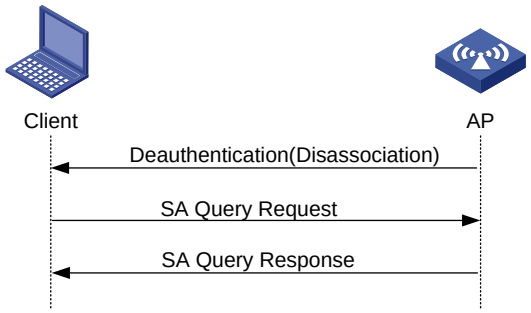
If a client receives unencrypted disassociation or deauthentication frames with failure code 6 or 7, passive SA Query can prevent the client from going offline abnormally.

As shown in Figure 3, passive SA Query uses the following process:

1. The client triggers the SA Query mechanism upon receiving an unencrypted disassociation or deauthentication frame.
2. The client sends an SA Query request to the AP.
   - If the client receives an SA Query response within the timeout time, it determines that the AP is online.
   - If the client does not receive an SA Query response within the timeout time, it resends the request. If the client receives an SA Query response within the retransmission time, it determines that the AP is online.

     If the AP is online, the client does not go offline.
   - If the client does not receive an SA Query response within the retransmission time, it determines that the AP is offline. The client goes offline.

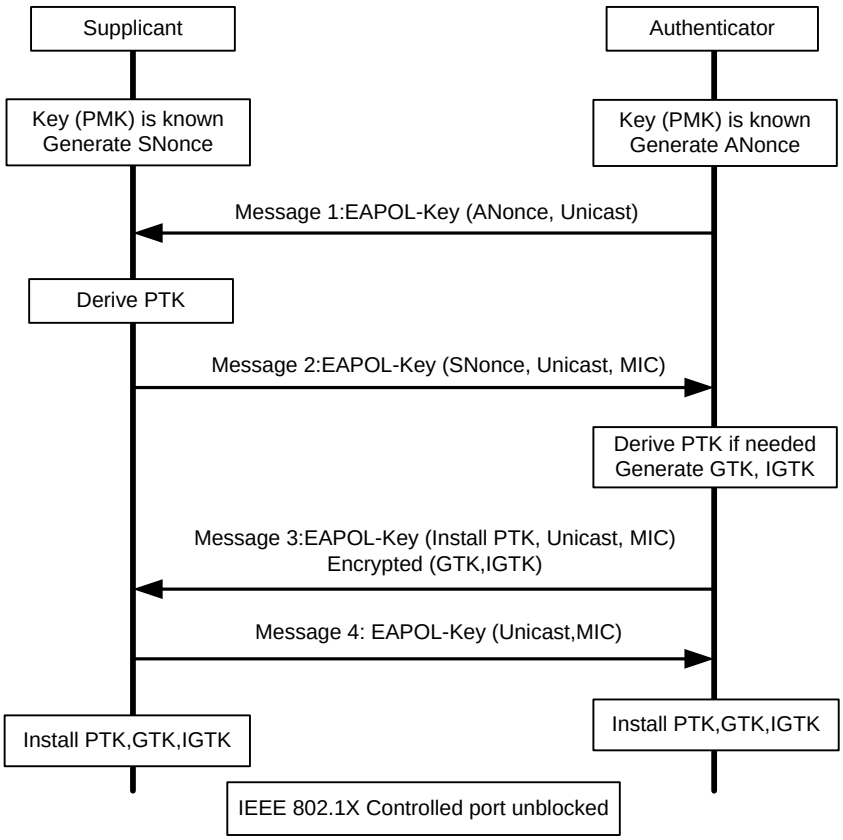
Figure 3. Passive SA Query



Broadcast and multicast management frame protection

802.11w uses Integrity Group Temporal Key (IGTK) to protect broadcast and multicast management frames. IGTK is negotiated through a 4-way handshake as shown in Figure 4.

Figure 4. IGTK negotiation

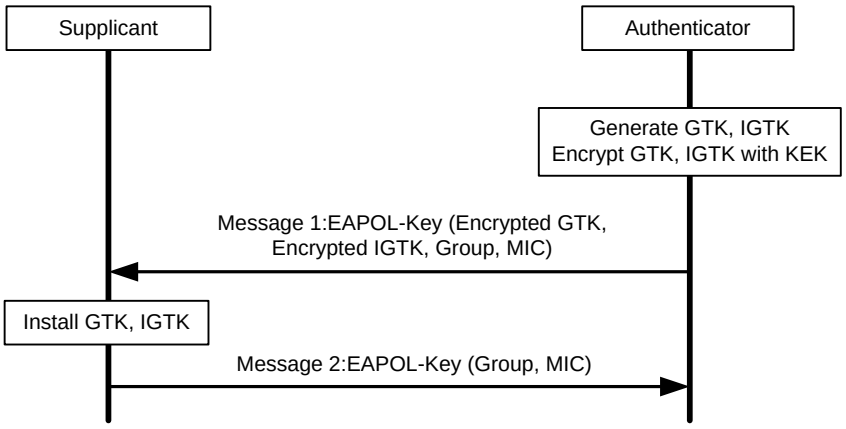


The IGTK negotiation uses the following process:

1. After the client associates with the AP, the AP sends the client an EAPOL packet that carries ANonce.
2. Upon receiving the packet, the client generates an SNonce and uses both the ANonce and the SNonce to generate the PTK.
3. The client sends the AP an EAPOL packet that carries the SNonce.
4. The AP uses the SNonce and the ANonce to generate the same PTK, then generates GTK and IGTK, and sends them to the client.
5. The client installs PTK, GTK, and IGTK, and sends a confirmation message to the AP.
6. The AP installs PTK, GTK, and IGTK.

If the GTK/IGTK changes, the AP uses Group Key Handshake to send the new GTK/IGTK to the client, as shown in Figure 5.

Figure 5. Group key handshake



After IGTK negotiation, 802.11w uses Broadcast Integrity Protocol (BIP) to protect broadcast/multicast management frames. BIP adds the Management MIC IE (MMIE) field to the management frame body. It uses the IPN and MIC in the MMIE to ensure integrity and replay protection, respectively. However, BIP cannot encrypt broadcast/multicast management frames and cannot protect confidentiality.

Figure 6. MMIE

1	1	2	6	8
Element ID	Length	KeyID	IPN	MIC

Integrity protection

The AP uses IGTK to generate a MIC value for a broadcast/multicast management frame. Then it puts the MIC value in the MMIE field. Upon receiving the frame, the client also generates a MIC value and compares the value to the MIC value in the frame. If they match, the broadcast/multicast management frame is intact.

Replay protection

Both the AP and the client maintain an IGTK Packet Number (IPN). When the AP sends a protected broadcast/multicast frame to the client, it puts an IPN in the MMIE field. The client compares the received IPN with the local IPN. If the received IPN is not larger than the local IPN, the client discards the frame.

5998-7007, November 2014