Frequently Asked Questions About Management Frame Protection (MFP)

Objective

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.

This document aims to provide answers to the frequently asked questions about Management Frame Protection (MFP).

Frequently Asked Questions

Table of Contents

1. What is MFP?

Management frames are broadcast frames used by IEEE 802.11 to permit a wireless client to negotiate with a Wireless Access Point (WAP). MFP provides security for unencrypted broadcast frames and management messages passed between wireless devices.

2. How does MFP Work?

In IEEE 802.11, management frames such as deauthentication, disassociation, beacons, and probes are always unauthenticated and unencrypted. The WAP adds Message Integrity Check Information Element (MIC IE) to each management frame it transmits. Any attempt to copy, alter, or replay the frame invalidates the MIC.

3. What are some of the things an attacker can do on a network with MFP disabled?

- The vulnerability found in management frames pose a great threat to a network by allowing an attacker to spoof a management frame from a WAP to attack a client that is associated to it. An attacker may perform the following actions:

— Run a Denial of Service (DoS) — Attackers are using evasion techniques outside of the typical volume-based attacks to avoid detection and mitigation, including "low and slow" attack techniques and SSL-based attacks. They are deploying multivulnerability attack campaigns that target every layer of the infrastructure of the victim, including the network infrastructure devices, firewalls, servers, and applications.
— Man-in-the-Middle attack on the client when reconnected — It is a form of an inductive key derivation attack which is effective in 802.11 networks because of the lack of effective message integrity. The receiver of a frame cannot verify that the frame was not tampered with during its transmission.

- Radio Frequency (RF) Jammer — Attacks with a high-power directional antenna from a distance can be carried out from the outside of your office building. Attack tools used by intruders leverage hacking techniques such as spoofed 802.11 management frames, spoofed 802.1x authentication frames, or simply using the brute force packet flooding method.
- Evil Twin Router — It is a form of phishing in which an attacker names and poses as a legitimate access point. This tricks users into connecting a mobile device to the fake access point, thus being able to cause more harm to the user.
- Run an offline dictionary attack — During a dictionary attack, variations of passwords are used to compromise the authentication credentials of the user. Most password-based authentication algorithms are vulnerable to dictionary attacks in the absence of a strong password policy.

4. What are the types of MFP?

These are the two types of MFPs:

- Infrastructure MFP — Specifically, infrastructure MFP protects 802.11 session management functions by adding MIC IE to the management frames emitted by access points and not those emitted by clients, which are validated by other access points in the network. Infrastructure MFP is passive. It can detect and report intrusions but it has no means to stop them. It protects management frames by detecting adversaries that are invoking denial-of-service attacks, flooding the network with association probes, interjecting as rogue access points, and affecting network performance by attacking the Quality of Service (QoS) and radio measurement frames.
- Client MFP — Shields authenticated clients from spoofed frames, preventing many of the common attacks against the wireless Local Area Networks (LANs) from becoming effective. Most attacks, such as de-authentication attacks, revert to simply degrading performance by contending with valid clients.

5. What are the components of Infrastructure MFP?

Infrastructure MFP has 3 components:

- Management frame protection — When management frame protection is enabled, the WAP adds MIC IE to each management frame it transmits. Any attempt to copy, alter, or replay the frame invalidates the MIC.
- Management frame validation — When management frame validation is enabled, the AP validates every management frame that it receives from other WAPs in the network. It ensures

that the MIC IE is present (when the originator is configured to transmit MFP frames) and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE from a Basic Service Set Identifier (BSSID) that belongs to a WAP, which is configured to transmit MFP frames, it reports the discrepancy to the network management system.

> **Note:** In order for the timestamps to operate properly, all Wireless LAN Controllers (WLC) must be Network Time Protocol (NTP) synchronized.

- Event reporting — The access point notifies the WLC when it detects an anomaly. WLC aggregates the anomalous events and reports it through SNMP traps to the network manager.

6. How does client MFP work?

Specifically, client MFP encrypts management frames sent between access points and Cisco Compatible Extension version 5 (CCXv5) clients so that both the access points and clients can take preventative action by dropping spoofed class 3 management frames (that is, management frames passed between an access point and a client that is authenticated and associated). Client MFP leverages the security mechanisms defined by IEEE 802.11i to protect the following types of class 3 unicast management frames: disassociation, de-authentication, and QoS (Wireless Multimedia Extenions or WMM) action. Client MFP protects a client-access point session from the most common type of denial-of-service attack. It protects class 3 management frames by using the same encryption method used for the session data frames. If a frame received by the access point or client fails decryption, it is dropped, and the event is reported to the controller.

7. How do I use client MFP?

To use client MFP, clients must support CCXv5 MFP and must negotiate Wi-Fi Protected Access version 2 (WPA2) using either Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard-Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). Extensible Authentication Protocol (EAP) or Pre-Shared Key (PSK) may be used to obtain the PMK. CCKM and controller mobility management are used to distribute session keys between access points for Layer 2 and Layer 3 fast roaming.

8. What are the components of Client MFP?

There are 3 components of Client MFP:

- Key generation and distribution — Client MFP leverages security protocols and mechanisms defined by IEEE 802.11i to protect class 3 unicast management frames:

  – Disassociation frames — A request to a client or WAP to disconnect or disassociate an authentication relationship.

  – De-authentication frames — A request to a client or WAP to disconnect or disassociate an association relationship.

  – QoS WMM action — WMM parameter is added to the beacon, probe response, and association response frames.

- Protection and validation of management frames — To prevent attacks using broadcast frames, APs that support CCXv5 do not emit any broadcast class 3 management frames. An AP in workgroup bridge mode, repeater mode, or non-root bridge mode discards broadcast

class 3 management frames if Client MFP is enabled.

- Error Reports — MFP-1 reporting mechanisms are used to report management frame de-encapsulation errors detected by access points. That is, the WLC collects MFP validation error statistics and periodically forwards collated information to the WCS.

> **Note:** MFP violation errors detected by client stations are handled by the CCXv5 Roaming and Real Time Diagnostics feature.

9. Why can’t my mobile device connect to the MFP enabled infrastructure device?

There are certain restrictions for some wireless clients to communicate with MFP-enabled infrastructure devices. MFP adds a long set of information elements to each probe request or SSID beacon. Some wireless clients such as PDAs, smartphones, barcode scanners, and so forth have limited memory and Central Processing Unit (CPU). So, you are not able to process these requests or beacons. As a result, you fail to see the SSID entirely, or you are not able to associate with these infrastructure devices, due to a misunderstanding of SSID capabilities. This issue is not specific to MFP. This also occurs with any SSID that has multiple information elements (IEs). It is always advisable to test MFP-enabled SSIDs on the environment with all your available client types before you deploy it in real time.

10. What is Broadcast Management Frame Protection?

In order to prevent attacks that use broadcast frames, APs that support CCXv5 does not transmit any broadcast class 3 management frames except for rogue containment de-authentication or disassociation frames. CCXv5 capable client stations must discard broadcast class 3 management frames. MFP sessions are assumed to be in a properly secured network (strong authentication plus TKIP or CCMP) so the disregard for rogue containment broadcasts is not an issue.

11. How to configure MFP on a Wireless Access Point (WAP)?

To learn how to configure MFP on a WAP, click here.

12. How to configure an Intel Wireless Network Card to connect to an MFP-enabled Network

To learn how to configure the Intel Wireless Network Card, click here.