Infrastructure Management Frame Protection (MFP) with WLC and LAP Configuration Example

Contents

Introduction

This document introduces a new security feature in wireless called Management Frame Protection (MFP). This document also describes how to configure MFP in infrastructure devices, such as Lightweight Access Points (LAPs) and Wireless LAN Controllers (WLCs).

Prerequisites

Requirements

- Knowledge of how to configure the WLC and LAP for basic operation
- Basic knowledge of IEEE 802.11 management frames

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 2000 Series WLC that runs firmware Release 4.1
- Cisco 1131AG LAP
- Cisco Aironet 802.11a/b/g Client Adapter that runs firmware Release 3.6
- Cisco Aironet Desktop Utility Version 3.6

Note: MFP is supported from WLC Version 4.0.155.5 and later, although Version 4.0.206.0 provides the optimal performance with MFP. Client MFP is supported on Version 4.1.171.0 and above.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

In 802.11, management frames such as (de)authentication, (dis)association, beacons, and probes are always unauthenticated and unencrypted. In other words, 802.11 management frames are always sent in an unsecured manner, unlike the data traffic, which are encrypted with protocols such as WPA, WPA2, or, at least, WEP, and so forth.

This allows an attacker to spoof a management frame from the AP to attack a client that is associated to an AP. With the spoofed management frames, an attacker can perform these actions:

- Run a Denial of Service (DOS) on the WLAN
- Attempt a Man in the Middle attack on the client when it reconnects
- Run an offline dictionary attack

MFP overcomes these pitfalls when it authenticates 802.11 management frames exchanged in the wireless network infrastructure.

Note: This document focuses on **Infrastructure and client MFP**.

Note: 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 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 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.

Note:

These are the components of Infrastructure MFP:

- **Management frame protection**—When management frame protection is enabled, AP 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. An AP, which is configured to validate MFP frames receives a frame with invalid MIC, reports it to the WLC.
- **Management frame validation**—When management frame validation is enabled, the AP validates every management frame that it receives from other APs 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 BSSID that belongs to an AP, 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 WLCs 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.

Infrastructure MFP Functionality

With MFP, all management frames are cryptographically hashed to create a Message Integrity Check (MIC). The MIC is added to the end of the frame (before the Frame Check Sequence (FCS)).

- In a centralized wireless architecture, infrastructure MFP is enabled/disabled on the WLC (global config). Protection can be selectively disabled per WLAN, and validation can be selectively disabled per AP.
- Protection can be disabled on the WLANs that are used by devices that cannot cope with extra IEs.
- Validation must be disabled on APs that are overloaded or overpowered.

When MFP is enabled on one or more WLANs configured in the WLC, the WLC sends a unique key to each radio on each registered AP. Management frames are sent by the AP over the MFP-enabled WLANs. These APs are labeled with a frame protection MIC IE. Any attempt to alter the frame invalidates the message, which causes the receiving AP that is configured to detect MFP frames to report the discrepancy to the WLAN controller.

This is a step-by-step process of MFP while implemented in a roaming environment:

1. With MFP globally enabled, the WLC generates a unique key for every AP / WLAN that is configured for MFP. WLCs communicate within themselves so that all WLCs know the keys for all the APs/BSSs in a mobility domain.**Note:** All controllers in a mobility/RF group must have MFP configured identically.
2. When an AP receives a MFP protected frame for a BSS that it does not know about, it buffers a copy of the frame and queries the WLC to get the key.
3. If the BSSID is not known on the WLC, it returns the message “Unknown BSSID” to the AP, and the AP drops the management frames received from that BSSID.
4. If the BSSID is known on the WLC, but MFP is disabled on that BSSID, the WLC returns a “Disabled BSSID.” The AP then assumes that all management frames received from that BSSID do not have an MFP MIC.

5. If the BSSID is known and has MFP enabled, the WLC returns the MFP Key to the requesting AP (over the AES encrypted LWAPP management tunnel).
6. The AP caches keys received in this way. This key is used to validate or add MIC IE.

Client MFP Functionality

Client MFP shields authenticated clients from spoofed frames, which prevents the effectiveness of many of the common attacks against wireless LANs. Most attacks, such as deauthentication attacks, revert to simply degraded performance when they contend with valid clients.

Specifically, client MFP encrypts management frames sent between access points and CCXv5 clients so that both access points and clients can take preventive action and drop 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 these types of class 3 unicast management frames: disassociation, deauthentication, and QoS (WMM) action. Client MFP can protect a client-access point session from the most common type of denial-of-service attack. It protects class 3 management frames with the same encryption method used for the data frames of the session. If a frame received by the access point or client fails decryption, it is dropped, and the event is reported to the controller.

In order to use client MFP, clients must support CCXv5 MFP and must negotiate WPA2 with either TKIP or AES-CCMP. EAP or PSK can be used to obtain the PMK. CCKM and controller mobility management are used to distribute session keys between access points or Layer 2 and Layer 3 fast roaming.

In order to prevent attacks against broadcast frames, access points that support CCXv5 do not emit any broadcast class 3 management frames (such as disassociation, deauthentication, or action). CCXv5 clients and access points must discard broadcast class 3 management frames.

Client MFP supplements infrastructure MFP rather than replaces it because infrastructure MFP continues to detect and report invalid unicast frames sent to clients that are not client-MFP capable, as well as invalid class 1 and 2 management frames. Infrastructure MFP is applied only to management frames that are not protected by client MFP.

Client MFP Components

Client MFP consists of these components:

- Key generation and distribution
- Protection and validation of management frames
- Error reports

Key Generation and Distribution

Client MFP does not use the key generation and distribution mechanisms that were derived for Infrastructure MFP. Instead, client MFP leverages the security mechanisms defined by IEEE 802.11i to also protect class 3 unicast management frames. Stations must support CCXv5 and must negotiate either TKIP or AES-CCMP to use cient MFP. EAP or PSK can be used to obtain the PMK.

Protection of Management Frames

Unicast class 3 management frames are protected with the application of either AES-CCMP or TKIP in a similar manner to that already used for data frames. Parts of the frame header are copied into the encrypted payload component of each frame for added protection, as discussed in the next sections.

These frame types are protected:

- Disassociation
- Deauthentication
- QoS (WMM) action frames

AES-CCMP- and TKIP-protected data frames include a sequence counter in the IV fields, which is used to prevent replay detection. The current transmit counter is used for both data and management frames, but a new receive counter is used for management frames. The receive counters are tested to ensure that each frame has a higher number than the last received frame (to ensure that the frames are unique and have not been replayed), so it does not matter that this scheme causes the received values to be non-sequential.

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.

MFP violation errors detected by client stations are handled by the CCXv5 Roaming and Real Time Diagnostics feature and are not in the scope of this document.

Broadcast Management Frame Protection

In order to prevent attacks that use broadcast frames, APs that support CCXv5 do not transmit any broadcast class 3 (that is, disassoc, deauth or action) management frames except for rogue containment deauthentication/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.

Similarly, APs discard inbound broadcast management frames. No inbound broadcast management frames are currently supported, so no code changes are required for this.

Supported Platforms

These platforms are supported:

- WLAN Controllers200621064400WiSM3750 with Embedded 440x Controller26/28/37/38xx Routers
- LWAPP Access PointsAP 1000AP 1100, 1130AP 1200, 1240, 1250AP 1310
- Client SoftwareADU 3.6.4 and above
- Network Management SystemsWCS

The 1500 Mesh LWAPP AP is not supported in this release.

Supported Modes

LWAPP-based Access Points that operate in these modes do support Client MFP:

Supported Access Point Modes	
Mode	**Client MFP Support**
Local	Yes
Monitor	No
Sniffer	No
Rogue Detector	No
Hybrid REAP	Yes
REAP	No
Bridge Root	Yes
WGB	No

Mixed Cell Support

Client stations that are not CCXv5 capable can associate with an MFP-2 WLAN. The access points keep track of which clients are MFP-2 capable and which are not in order to determine whether MFP-2 security measures are applied to outbound unicast management frames and expected on inbound unicast management frames.

Configure

Configure MFP on a Controller

You can globally configure MFP on a controller. When you do so, **management frame protection and validation are enabled by default for each joined access point**, and access point authentication is automatically disabled.

Perform these steps to configure MFP globally on a controller.

1. From the controller GUI, click **Security**. In the resultant screen, click **AP Authentication/MFP** under **Wireless Protection Policies**.
2. In the AP Authentication Policy, choose **Management Frame Protection** from the **Protection Type** drop-down menu and click **Apply**.

Configure MFP on WLAN

You can also enable/disable infrastructure MFP protection and client MFP on each WLAN configured on the WLC. Both are enabled by default though infrastructure MFP protection, which is only active if globally enabled, and client MFP is only active if the WLAN is configured with WPA2 security. Follow these steps in order to enable MFP on a WLAN::

1. From the WLC GUI, click **WLANs** and click **New** in order to create a new WLAN.
2. On the WLANs edit page, go to the *Advanced* tab and check the **Infrastructure MFP Protection** check box to enable the infrastructure MFP on this WLAN. In order to disable

infrastructure MFP proection for this WLAN, uncheck this check box. In order to enable Client MFP, choose the required or optional option from the drop-down menu. If you choose Client MFP= Required, make sure that all your clients have support for MFP-2 or they are not able to connect. If you choose optional, both MFP and non-MFP enabled clients can connect on the same WLAN.

Verify

In order to verify the MFP configurations from the GUI, click **Management Frame Protection** under Wireless Protection Policies from the Security page. This takes you to the MFP Settings page.

In the MFP Settings page, you can see the MFP configuration on the WLC, LAP, and WLAN. This is an example.

- The Management Frame Protection field shows if MFP is enabled globally for the WLC.
- The Controller Time Source Valid field indicates whether the WLC time is set locally (by manual entry of the time) or through an external source (such as an NTP server). If the time is set by an external source, the value of this field is "True." If the time is set locally, the value is "False." The time source is used to validate management frames between access points of different WLCs that also have mobility configured.**Note:** If MFP is enabled on all WLCs in a mobility/RF group, it is always recommended that you use an NTP server to set the WLC time in a mobility group.
- The **MFP Protection** field shows if MFP is enabled for individual WLANs.
- The **MFP Validation** field shows if MFP is enabled for individual access points.

These show commands can be helpful:

- **show wps summary** —Use this command in order to see a summary of the current wireless protection policies (which includes MFP) of the WLC.
- **show wps mfp summary**—In order to see the current global MFP setting of the WLC, enter this command.
- **show ap config general *AP_name*** —In order to see the current MFP state for a particular access point, enter this command.

This is an example of the output of the **show ap config general *AP_name*** command:

```
(Cisco Controller) >show ap config general AP

Cisco AP Identifier.............................. 4
Cisco AP Name.................................... AP
Country code..................................... US  - United States
Regulatory Domain allowed by Country.............. 802.11bg:-AB    802.11a:-AB
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-A
Switch Port Number .............................. 29
MAC Address...................................... 00:19:2f:7e:3a:30
IP Address Configuration......................... DHCP
IP Address....................................... 172.20.225.142
IP NetMask....................................... 255.255.255.248
Gateway IP Addr.................................. 172.20.225.137
Cisco AP Location................................ default location
Cisco AP Group Name.............................. default-group
```

```
Primary Cisco Switch.....................
Secondary Cisco Switch.....................
Tertiary Cisco Switch.....................
Administrative State ..................... ADMIN_ENABLED
Operation State ..................... REGISTERED
Mirroring Mode ..................... Disabled
AP Mode ..................... H-Reap
Public Safety ..................... Global: Disabled, Local: Disabled
Remote AP Debug ..................... Disabled
S/W  Version ..................... 4.1.169.24
Boot  Version ..................... 12.3.7.1
Mini IOS Version ..................... 3.0.51.0
Stats Reporting Period ..................... 180
LED State..................... Enabled
PoE Pre-Standard Switch..................... Disabled
PoE Power Injector MAC Addr..................... Disabled
Number Of Slots..................... 2
AP Model..................... AIR-LAP1242AG-A-K9
IOS Version..................... 12.4(20070414:021809)
Reset Button..................... Enabled
AP Serial Number..................... FTX1035B3QX
AP Certificate Type..................... Manufacture Installed
H-REAP Vlan mode :..................... Disabled
Management Frame Protection Validation..... Enabled
Console Login Name.....................
Console Login State..................... Unknown
Ethernet Port Duplex..................... Auto
Ethernet Port Speed..................... Auto
```

This is an example of the output of the **show wps mfp summary** command:

```
(Cisco Controller) >show wps mfp summary

Global MFP state..................... enabled
Controller Time Source Valid..... false


                                    WLAN       Infra.      Client
WLAN ID  WLAN Name                  Status     Protection  Protection
-------  -------------------------  ---------  ----------  ----------
1        secure-1                   Enabled    Enabled     Optional
2        Guest                      Enabled    Enabled     Optional but inactive
(WPA2 not configured)

                     Infra.             Operational     --Infra. Capability--
AP Name              Validation  Radio  State           Protection  Validation
-------------------  ----------  -----  --------------  ----------  ----------
AP                   Enabled     b/g    Up              Full        Full
```

These debug commands can be helpful;

- **debug wps mfp lwapp**—Shows debug information for MFP messages.
- **debug wps mfp detail**—Shows detailed debug information for MFP messages.
- **debug wps mfp report**—Shows debug information for MFP reporting.

- **debug wps mfp mm**—Shows debug information for MFP mobility (inter-controller) messages.

Note: There are also several free Wireless Packet sniffers available from the Internet, which can be used to capture and analyze the 802.11 management frames. Some example packet sniffers are Omnipeek and Wireshark.

Related Information

- **Configuring Security Solutions: WLC Configuration Guide**
- **Configuring Security Solutions in WCS**
- **EAP Authentication with WLAN Controllers (WLC) Configuration Example**
- **ACLs on Wireless LAN Controller Configuration Example**
- **External Web Authentication with Wireless LAN Controllers Configuration Example**
- **Dynamic VLAN Assignment with RADIUS Server and Wireless LAN Controller Configuration Example**
- **Cisco Secure Services Client with EAP-FAST Authentication**
- **WLC FAQ**
- **Wireless Support Page**
- **Technical Support & Documentation - Cisco Systems**