在WLC上配置802.11w管理幀保護

目錄

簡介

本檔案介紹有關IEEE 802.11w管理訊框保護以及思科無線LAN控制器(WLC)上其設定的詳細資訊。

必要條件

需求

思科建議您瞭解執行代碼7.6或更高版本的Cisco WLC。

採用元件

本檔案中的資訊是根據執行代碼7.6的WLC 5508。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

802.11w標準旨在保護控制和管理幀，以及一組強大的管理幀，防止偽造和重放攻擊。受保護的幀型別包括Disassociation、Deauthentication和Robust Action幀，例如：

- 頻譜管理
- 服務品質(QoS)

- 阻止Ack
- 無線電測量
- 快速基本服務集(BSS)過渡

802.11w不會加密幀，但是會保護管理幀。它確保報文來自合法來源。為此，必須新增消息完整性檢查(MIC)元素。802.11w引入了名為Integrity Group Temporal Key(IGTK)的新金鑰，用於保護廣播/組播魯棒管理幀。這是與無線保護訪問(WPA)一起使用的四向金鑰交握過程的一部分。這使dot1x/Pre-Shared Key(PSK)在需要使用802.11w時成為一項要求。不能與open/webauth Service Set Identifier(SSID)一起使用。

當協商管理幀保護時，接入點(AP)在EAPOL-Key幀中加密GTK和IGTK值，EAPOL-Key幀在4次握手的消息3中傳送。如果AP後來更改了GTK，則它會使用組金鑰握手將新的GTK和IGTK傳送到客戶端。它新增使用IGTK金鑰計算的MIC。

管理MIC資訊元素(MMIE)

802.11w引入了一個新的資訊元素，稱為管理MIC資訊元素。它具有如圖所示的報頭格式。

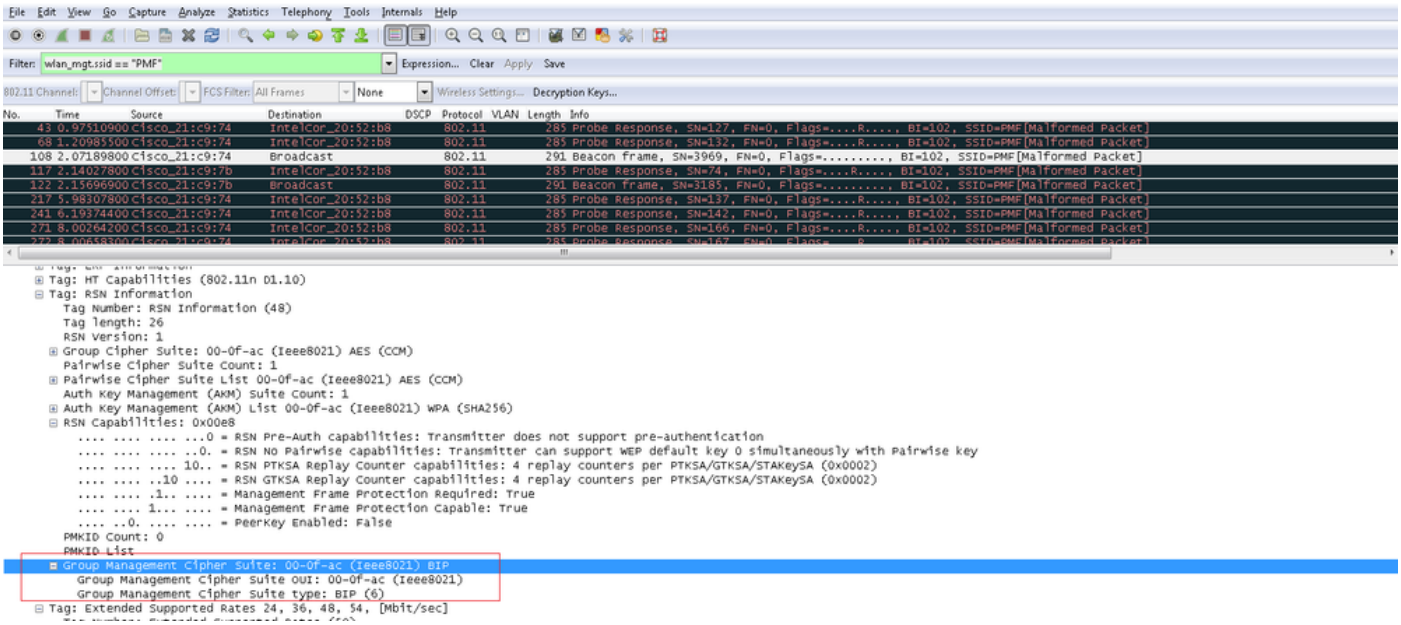
1	1	2	6	8
Element ID	Length	KeyID	IPN	MIC

此處主要關注的是元素ID和MIC。MMIE的元素ID為 0x4c 當您分析無線捕獲時，它可以作為一個有用的標識。

註:MIC — 它包含通過管理幀計算的消息完整性代碼。必須注意的是，此操作是在AP上新增的。然後，目的客戶端重新計算幀的MIC，並將其與AP傳送的資料進行比較。如果值不同，則作為無效幀將其拒絕。

對RSN IE的更改

強大的安全網路資訊元素(RSN IE)指定AP支援的安全引數。802.11w將組管理密碼套件選擇器引入到RSN IE，其中包含由AP用於保護廣播/組播強大管理幀的密碼套件選擇器。這是瞭解AP是否執行802.11w的最佳方法。這也可以驗證，如下圖所示。

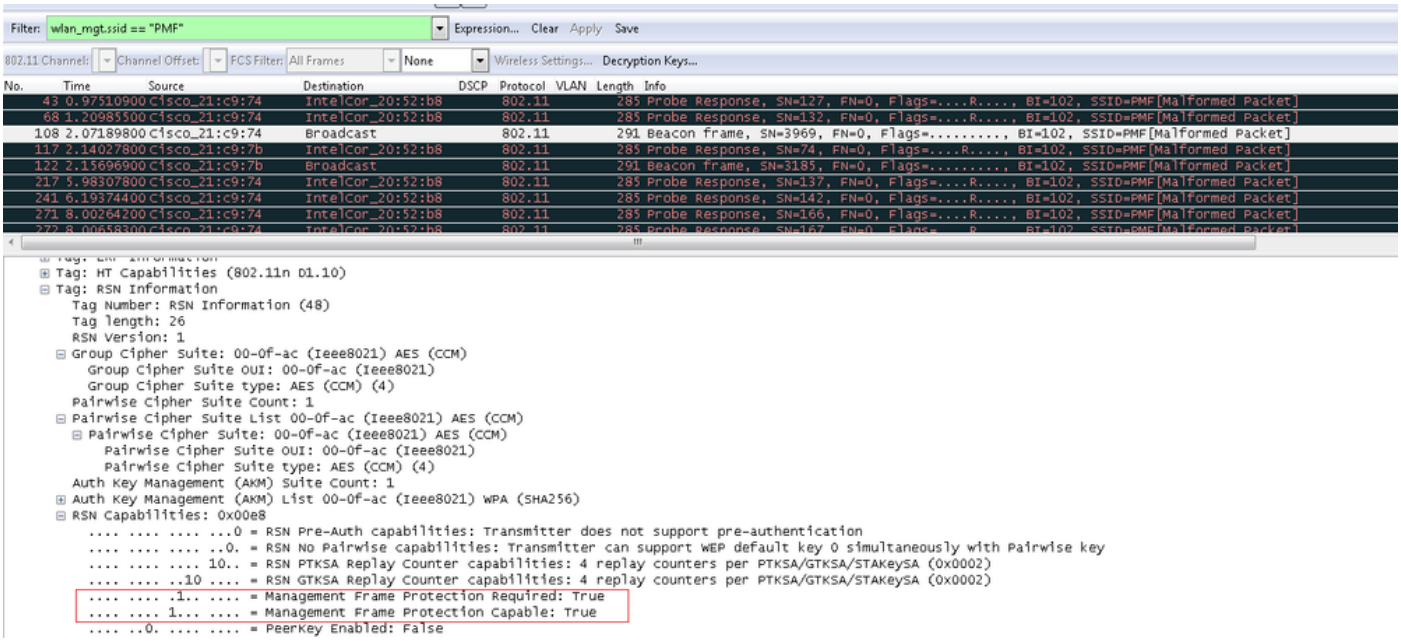


此處您可以找到group management cipher suite欄位，顯示已使用802.11w。

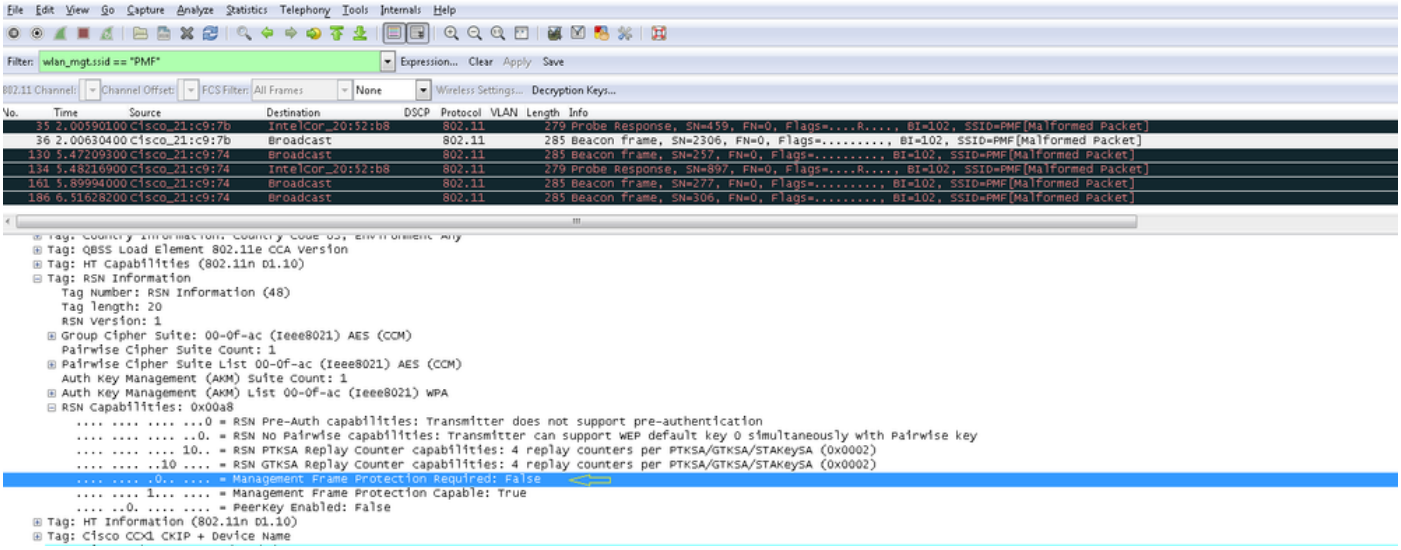
在RSN功能下也進行了更改。第6位和第7位現在用於表示802.11w的不同引數。

- 第6位：需要管理幀保護(MFPR)- STA將此位設定為1以通告必須保護強大的管理幀。
- 第7位：支援管理幀保護(MFPC)- STA將此位設定為1以通告已啟用對強健管理幀的保護。當AP設定該設定時，它會通知它支援管理幀保護。

如果在配置選項下根據需要設定管理幀保護，則同時設定第6位和第7位。如下面的封包擷取映像所示。



但是，如果將此選項設定為可選，則只設定第7位，如下圖所示。



注意:WLC在關聯/重新關聯響應中新增此修改的RSN IE，AP在信標和探測響應中新增此修改的RSN IE。

802.11w管理幀保護的優點

- 使用者端保護

這是通過向取消身份驗證和取消關聯幀新增加密保護來實現的。這可防止未經授權的使用者通過欺騙合法使用者的MAC地址並傳送deauth/disassociation幀來發起Denial of Service(DOS)攻擊。

- AP保護

通過增加由關聯恢復時間和SA-Query過程組成的安全關聯(SA)拆卸保護機制來增加基礎設施側保護。在802.11w之前，如果AP從已關聯的客戶端收到關聯或身份驗證請求，則AP將終止當前連線，然後啟動新連線。當您使用802.11w MFP時，如果STA已關聯並已協商管理幀保護，則AP將拒絕返回狀態代碼為30的關聯請求 Association request rejected temporarily; Try again later 到客戶端。

關聯響應中包括關聯回退時間資訊元素，該元素指定當AP準備接受與此STA的關聯時的回退時間。通過這種方式，您可以確保合法客戶端不會因為偽裝的關聯請求而取消關聯。

注意：如果客戶端不使用802.11w PMF，WLC（AireOS或9800）將忽略客戶端傳送的取消關聯或取消身份驗證幀。如果客戶端使用PMF，則只有在收到此類幀後才會立即刪除客戶端條目。這是為了避免惡意裝置拒絕服務，因為這些沒有PMF的幀沒有安全性。

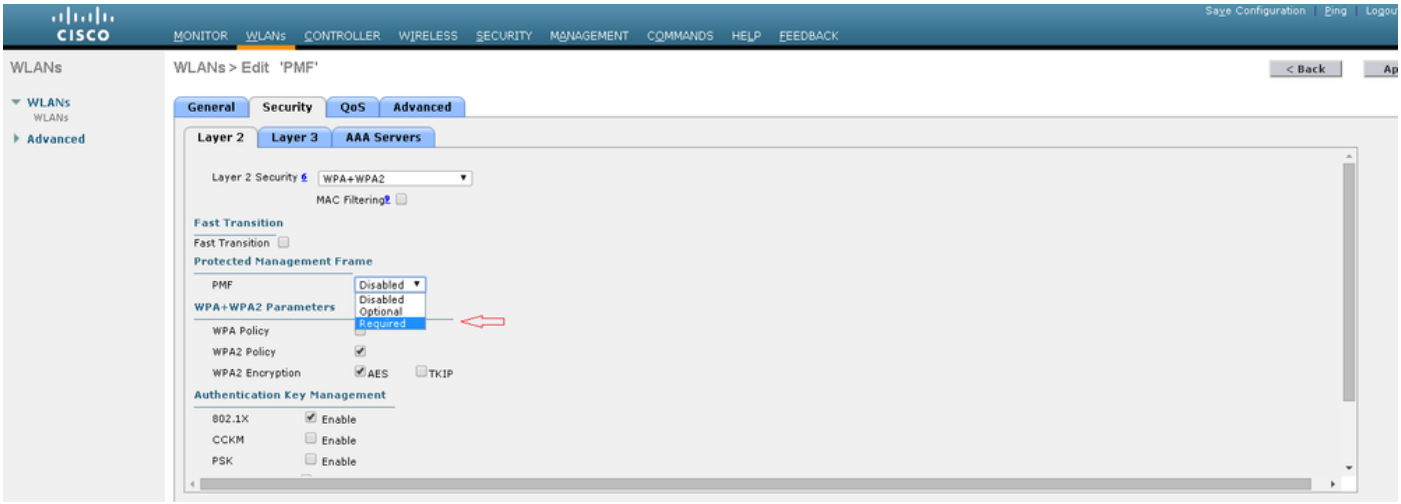
啟用802.11w的要求

- 802.11w要求使用dot1x或PSK配置SSID。
- 所有支援802.11n的AP都支援802.11w。這表示AP 1130和1240不支援802.11w。
- 7.4版本中的flexconnect AP和7510 WLC不支援802.11w。自7.5版本以來已新增支援。

設定

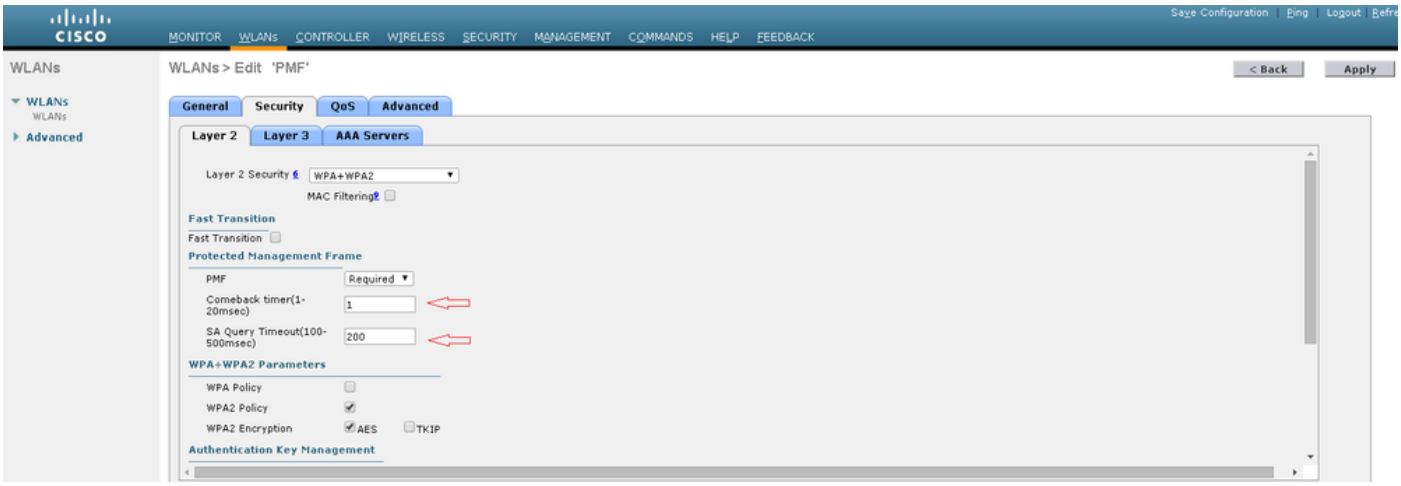
GUI

步驟 1.您需要在配置了802.1x/PSK的SSID下啟用受保護的管理幀。您可以選取三個選項，如下圖所示。

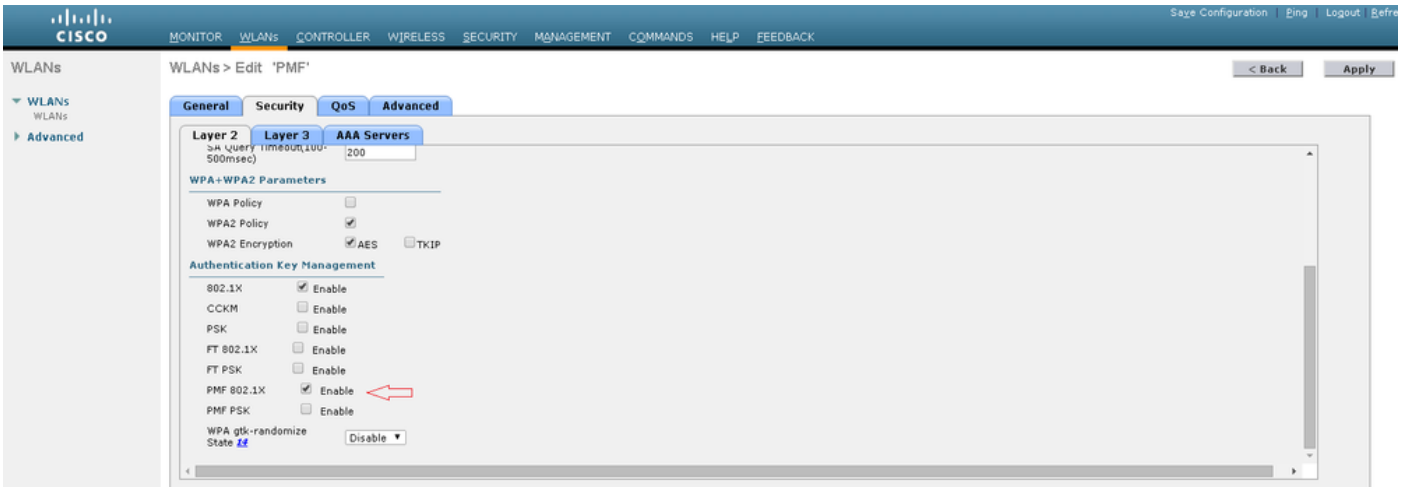


「Required」指定不允許不支援802.11w的客戶端連線。「可選」指定即使不支援802.11w的客戶端也允許連線。

步驟 2.然後，您需要指定恢復計時器和SA查詢超時。返回計時器指定當第一次被拒絕且狀態代碼為30時，關聯客戶端必須等待的時間，然後才能再次嘗試關聯。SA查詢超時指定WLC等待客戶端對查詢進程作出響應的時間。如果沒有來自客戶端的響應，其關聯將從控制器中刪除。如下圖所示。



步驟 3.如果使用802.1x作為身份驗證金鑰管理方法，則必須啟用「PMF 802.1x」。如果使用PSK，則必須選擇PMF PSK霰取方塊，如下圖所示。



CLI

- 若要啟用或停用11w功能，請運行以下命令：

config wlan security wpa akm pmf 802.1x enable/disable

config wlan security wpa akm pmf psk enable/disable

- 要啟用或禁用受保護管理幀，請運行命令：

config wlan security pmf optional/required/disable

- 關聯恢復時間設定：

config wlan security pmf 11w-association-comeback

- SA查詢重試超時設定：

config wlan security pmf saquery-retry-time

驗證

使用本節內容，確認您的組態是否正常運作。

802.11w配置可以驗證。檢查WLAN設定：

```
(wlc)>show wlan 1
Wi-Fi Protected Access (WPA/WPA2)..... Enabled
<snip>
802.1x..... Enabled
PSK..... Disabled
CCKM..... Disabled
FT-1X(802.11r)..... Disabled
FT-PSK(802.11r)..... Disabled
PMF-1X(802.11w)..... Enabled
PMF-PSK(802.11w)..... Disabled
FT Reassociation Timeout..... 20
FT Over-The-DS mode..... Enabled
GTK Randomization..... Disabled
<snip>
PMF..... Required
PMF Association Comeback Time..... 1
PMF SA Query RetryTimeout..... 200
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

以下debug指令可用於排除WLC上的802.11w問題：

- **debug 11w-pmf events enable/disable**
- debug 11w-pmf keys enable/disable
- debug 11w-pmf all enable

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。