遷移至6 GHz和Wi-Fi 7

目錄

簡介

本文檔介紹用於最佳化Wi-Fi 7效能和充分利用6 GHz頻譜的設計和配置指南。

為什麼選擇6 GHz和Wi-Fi 7

6 GHz是2020年推出的一款用於WLAN操作的新頻段，最初由Wi-Fi 6E認證開發。雖然Wi-Fi 6E仍然依賴相同的802.11ax標準（在2.4/5 GHz頻段上通過Wi-Fi 6認證），但它擴展為僅在6 GHz頻段上運行，前提是滿足特定要求。

Wi-Fi 7對應於IEEE 802.11be標準的認證，並且與Wi-Fi 6E（僅限於6 GHz）相反，它被定義用於所有三個頻段：2.4、5和6 GHz。與先前的認證相比，Wi-Fi 7還具備新功能。

6 GHz和/或Wi-Fi 7具有需要支援的特定要求，這些要求通常轉化為新的配置和RF設計，尤其是與我們在2.4/5 GHz頻段和Wi-Fi 6之前使用的要求相比。例如，就像使用WEP安全性阻止我們使用802.11標準（而不是802.11a/b/g）一樣，更新的標準具有更高的安全性先決條件，以推動採用更安全的網路。

另一方面，最新的6 GHz頻段，加上諸如Wi-Fi 6E/7等現代認證，可解鎖更清潔的頻率、更好的效能

和新的用途，甚至還可更「無憂地」實施現有使用案例（例如語音/視訊會議）。

6 GHz操作和Wi-Fi 7的基本要求

這些是6 GHz和Wi-Fi 7操作認證中寫的安全要求。

6 GHz頻段要求

6 GHz頻段只能允許WPA3或增強型開放式WLAN，這意味著以下任一安全選項：

- 採用802.1X驗證的WPA3-Enterprise
- WPA3對等同時身份驗證(SAE)（又稱WPA3 — 個人），帶密碼。SAE-FT(SAE with Fast Transition)是另一種可能的AKM，實際上建議使用，因為SAE握手並非無關緊要，並且FT允許跳過更長的交換。
- 機會無線加密(OWE)增強型開放式

根據WPA3 v3.4規範（第11.2節），6 GHz不支援增強型開放過渡模式，但許多供應商(包括思科至IOS® XE 17.18)尚未實施該模式。因此，在技術上，在5 GHz上配置開放式SSID，在5 GHz和6 GHz上配置相應的增強型開放式SSID，兩者都啟用過渡模式，而且都無需遵守標準規範。然而，在這樣的場景中，必須預期我們寧願配置不帶轉換模式且僅在6 GHz上可用的增強型開放SSID（支援6 GHz的客戶端通常也支援增強型開放），同時保持我們常規的開放SSID在5 GHz上且也不帶轉換模式。

除了802.11w/保護管理幀(PMF)實施之外，WPA3-Enterprise沒有新的特定密碼或演算法要求。許多供應商（包括思科）認為802.1X-SHA256或「FT + 802.1X」（實際上是802.1X，頂部有SHA256和快速過渡）僅符合WPA3，而普通802.1X（使用SHA1）則被視為WPA2的一部分，因此不適合/支援6 GHz。

Wi-Fi 7要求

通過802.11be標準的Wi-Fi 7認證，Wi-Fi聯盟提高了安全要求。其中一些允許使用802.11be資料速率和協定改進，而其他一些則專門支援多鏈路操作(MLO)，允許相容裝置（客戶端和/或AP）使用多個頻段，同時保持相同的關聯。

一般來說，Wi-Fi 7會要求以下安全型別之一：

- WPA3-Enterprise，帶AES(CCMP128)和802.1X-SHA256或FT + 802.1X（仍使用SHA256，即使其命名未明確顯示）。 與以前現有的6 GHz頻段的WPA3安全先決條件相比，這並不是更改。
- WPA3 — 個人，帶GCMP256和SAE-EXT-KEY和/或FT + SAE-EXT-KEY（AKM 24或25）。Wi-Fi 6E強制使用WPA3 SAE和/或FT + SAE，僅使用常規AES(CCMP128)，並且沒有額外的擴展金鑰使用，因此這是專門為Wi-Fi 7引入的新密碼。
- 使用GCMP256增強型開放/OWE。雖然仍可以在同一個SSID上配置AES(CCMP128)，但使用AES 128的客戶端不支援Wi-Fi 7。在Wi-Fi 7之前，大多數支援增強型開放的客戶端僅使用AES 128，因此這是一個新的更強要求。對於6 GHz支援，不允許轉換模式。

在所有這些情況下，還需要受保護管理幀(PMF)和信標保護來支援WLAN上的Wi-Fi 7。

Wi-Fi 7在撰寫本文時仍為最新版本，由於要儘早發佈，許多供應商從一開始就未強制執行這些安全要求。

最近，思科一直在逐步實施配置選項，以符合Wi-Fi 7認證。以下是版本特定的行為：

17.18.1及更高版本

如果WLAN的安全引數與Wi-Fi 7的要求相匹配（信標保護、PMF和前面所述的正確AKM，這取決於WLAN型別以及GCMP256的存在，以便在OWE或SAE-EXT的情況下實現Wi-Fi 7 MLO），則IOS XE 17.18及更高版本僅將給定WLAN通告為Wi-Fi 7啟用。 SSID上允許存在AES128，但使用時，它將僅提供Wi-Fi 6E，而不是Wi-Fi 7 MLO。

客戶端可以作為Wi-Fi 7進行關聯，並且無論其使用何種安全方法都可以實現Wi-Fi 7資料速率（前提是WLAN仍支援該方法）。 但是，如果客戶端符合Wi-Fi 7安全性的嚴格要求，或者被拒絕，則客戶端只能關聯為MLO功能（在一個或多個頻段上）。

17.15.3及更高版本17.15.x

在此分支中，所有WLAN都以Wi-Fi 7 SSID進行廣播，前提是Wi-Fi 7在全球範圍內啟用，且無論安全設定如何。

客戶端可以關聯為支援Wi-Fi 7，並實現Wi-Fi 7資料速率，無論其使用何種安全方法，前提是WLAN仍支援該方法。但是，如果客戶端符合Wi-Fi 7安全性的嚴格要求，或者被拒絕，則客戶端只能關聯為MLO功能（在一個或多個頻段上）。

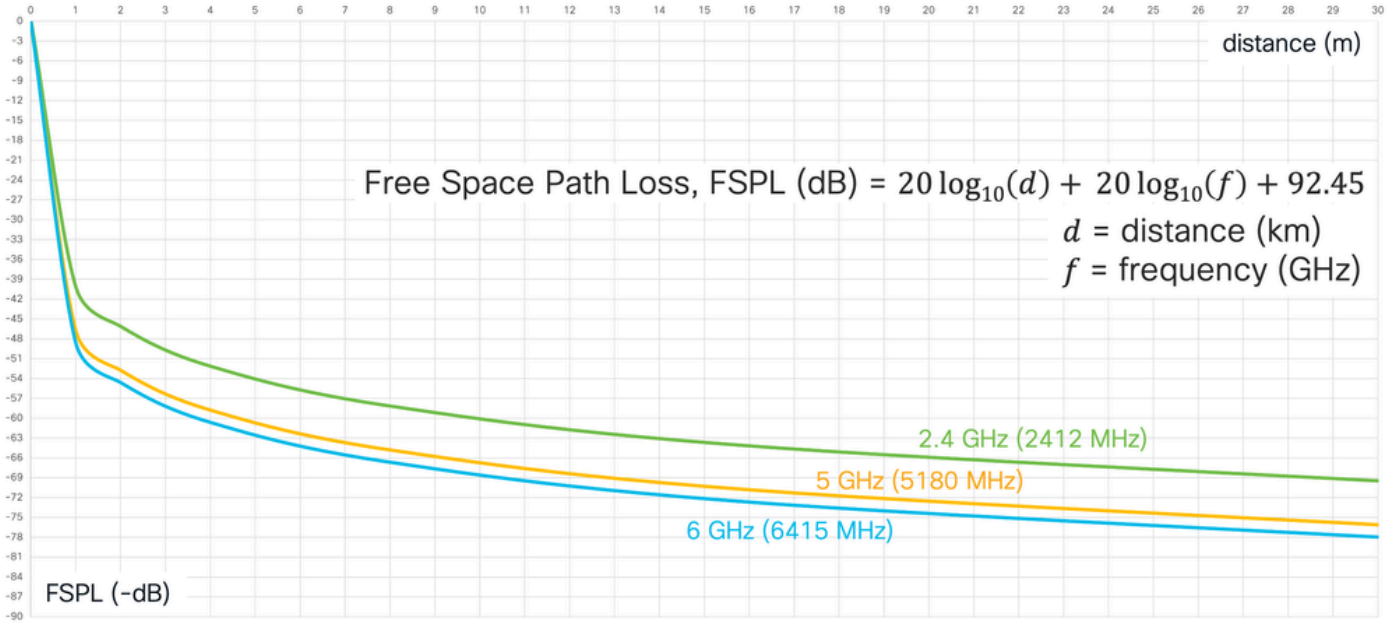
當某些早期的Wi-Fi 7客戶端無法支援更安全的密碼（如GCMP256）嘗試將Wi-Fi 7 MLO功能關聯到WLAN（其安全設定與Wi-Fi 7要求不匹配）時，這可能會造成問題。在這種情況下，由於安全設定無效（仍允許在WLAN下設定），使用者端會遭到拒絕。

6 GHz覆蓋的無線電設計注意事項

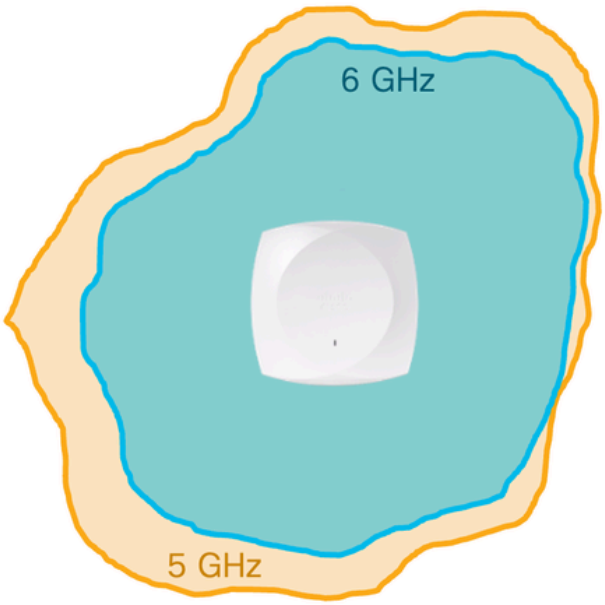
本部分無意成為現場勘測的完整規範指南，但簡要介紹為6 GHz覆蓋進行設計時的一些基本考慮事項，尤其是當已經存在要遷移到Wi-Fi 6E或7的2.4/5 GHz安裝時。
對於我們以前在2.4和/或5 GHz上使用的任何新Wi-Fi部署，6 GHz上的新無線專案也必須包括相應的專用6 GHz站點勘測。

當pre-Wi-Fi 6E/7 AP已針對特定的5 GHz覆蓋範圍和需求進行定位時，在某些情況下我們可以期望能夠用支援Wi-Fi 6E/7的AP來取代它們，並且仍然可以在6 GHz上獲得良好的覆蓋範圍。為了讓這一理論起作用，我們的現有AP必須已提供滿足預期需求（僅資料、語音、特定應用等）的正確5 GHz覆蓋範圍，同時至少已在其最大限制下有3-4個傳輸功率級別。AP通常有7到8個功率級別，每個功率級別將傳輸功率除以一半。這意味著當AP使用它們允許的傳輸功率範圍的介質時，有一個比較舒適的位置。

根據自由空間損耗計算，6GHz訊號比5GHz訊號衰減2dB。此外，6 GHz訊號受障礙物的影響也比5 GHz訊號更大。



當Cisco AP將發射功率增加/減少一個級別時，其增加/減少的幅度為3 dB。從功率級別4（例如，發射功率為11 dBm）到功率級別3的AP將其發射功率提高至14 dBm（功率級別4為11 dBm，功率級別3為14 dBm，這只是一般示例，因為對於相同的功率級別編號，不同型號/代的AP在dBm中的發射功率值可能略有不同）。



Assuming similar antenna gains/patterns and the same transmit power level, the 6 GHz radio is expected to cover slightly less than the 5 GHz radio.
The overall 6 GHz coverage throughout multiple APs could be more comparable, especially if those APs are already dense enough for good 5 GHz coverage.

例如，如果之前的Wi-Fi 6E/7 AP已經在4級電源上提供5 GHz的良好覆蓋範圍，那麼具有類似5 GHz無線電模式的較新Wi-Fi 6E/7 AP可以取代之前的AP，而不會對現有的5 GHz網路產生任何顯著影響。

此外，新型Wi-Fi 6E/7 AP的6 GHz無線電只需提高一個發射功率電平（即3 dB），就可以提供與5 GHz無線電類似的覆蓋範圍。

如果5 GHz已經被AP的5 GHz無線電正確覆蓋，其最大功率電平為3-4，因此對應的6 GHz無線電可以設定為其最大功率電平的2-3功率電平進行類似的覆蓋。

此外，如果6 GHz無線電在低於其最大功率水準的2-3個功率水準下已提供正確的覆蓋，它仍會異常地提高幾個電平，例如嘗試繞過臨時的意外覆蓋漏洞（鄰居AP故障、未通知的障礙、新的RF需求等）。

在Wi-Fi 6E/7之前的版本和Wi-Fi 6E/7 AP之間的漫遊行為

在同一個覆蓋區域部署支援不同標準和/或頻段的AP始終不是推薦的做法，尤其是當這些不同代的AP以「鹽和胡椒」方式（即在同一區域中相互混合）安裝時。

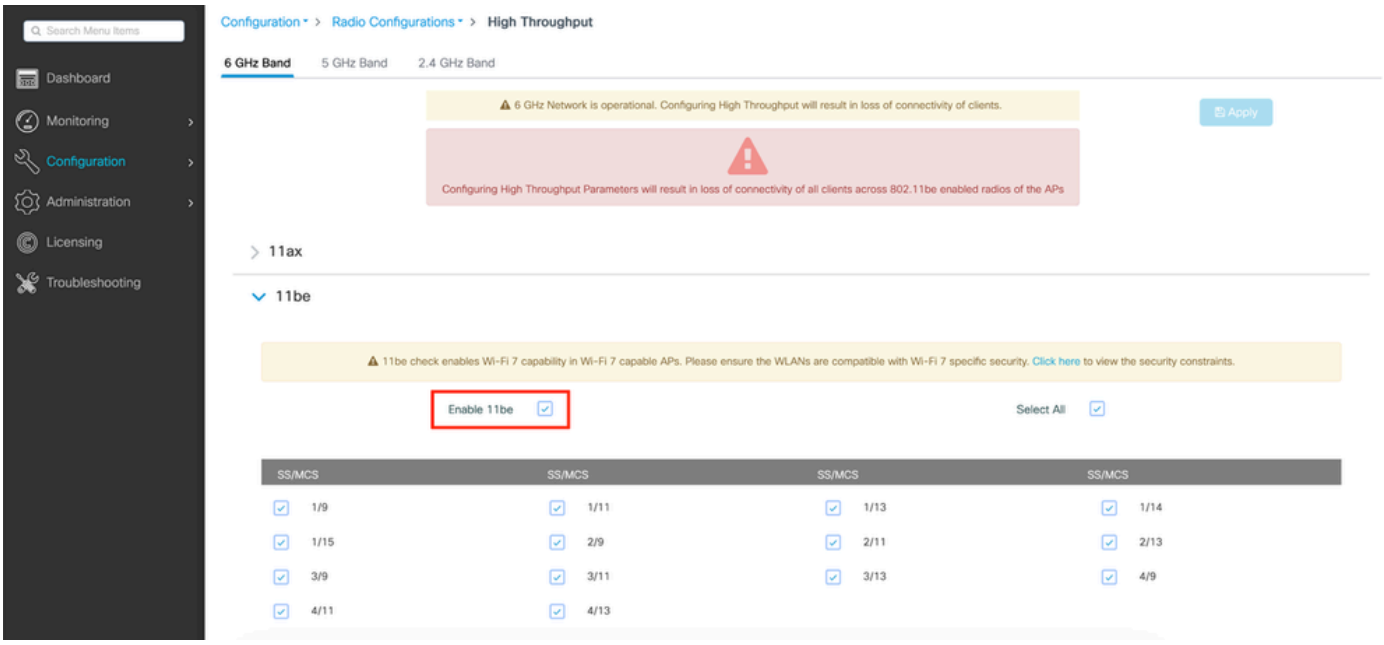
雖然無線控制器可以處理來自一組多個AP型號的操作（例如，動態通道分配、傳輸功率控制、PMK快取分配等），但在不同標準甚至不同頻帶之間移動的客戶端並不總是能夠正確處理這些操作，例如，它們可能會遇到漫遊問題。

此外，由於採用了較新的標準，Wi-Fi 6E/7 AP支援WPA3的GCMP256密碼。但是，對於某些Wi-Fi 6 AP和早期型號來說，情況並非總是如此。對於需要同時配置AES(CCMP128)和GCMP256密碼的密碼/WPA3 — 個人及增強型開放/OWE SSID，某些Wi-Fi 6（如9105、9115和9120系列）不支援GCMP256，且只能為關聯的客戶端（包括支援Wi-Fi 6E/7的客戶端）提供AES(CCMP128)密碼。如果這些Wi-Fi 6E/7客戶端需要從支援GCMP256的相鄰Wi-Fi 6E/7 AP漫遊/漫遊到相鄰Wi-Fi 6E/7 AP，它們必須經歷全新的關聯，因為透明漫遊不支援AES(CCMP128)和GCMP256之間的重新協商密碼。此外，一般而言，讓某些AP提供新功能並不理想，而同一領域的其他AP不提供這些相同功能：它不允許客戶端在移動時安全地使用這些功能，並且可能導致粘滯或斷開。
雖然此場景必須代表一個角落(corner)情況，但我們仍然要記住，在WLAN下配置了GCMP256密碼後，在9105/9115/9120 AP和9130/9124/916x/917x AP之間漫遊的Wi-Fi 6E/7客戶端將無法實現，因為這些後一個系列支援GCMP256，而前一個系列不支援。

6 GHz上40 MHz或更高的通道寬度也會導致支援6 GHz的客戶端粘性，這些客戶端可能會拒絕與其他頻段重新關聯。這肯定是不在同一漫遊區域混合使用6 GHz功能的AP和非6 GHz功能的AP的另一個原因。

在全球啟用Wi-Fi 7

安裝或升級到支援Wi-Fi 7的IOS XE版本時，預設情況下全域性禁用對Wi-Fi 7的支援。
要啟用它，我們需要導航到每個2.4/5/6 GHz頻段的High Throughput配置選單下，並選中啟用11be的覈取方塊。



另一種方法是在終端配置模式下通過SSH/控制檯運行這三個命令列：

```
ap dot11 24ghz dot11be
ap dot11 5ghz dot11be
ap dot11 6ghz dot11be
```

如警告說明所述，在嘗試修改這些設定時，更改802.11be支援的狀態會導致Wi-Fi 7 AP無線電上的所有客戶端短暫失去連線。如果您要執行MLO（這意味著客戶端同時連線到多個頻段），則需要在您希望客戶端連線的所有頻段上啟用11be。不必在所有頻段上啟用，但建議僅為效能而啟用。

使用案例

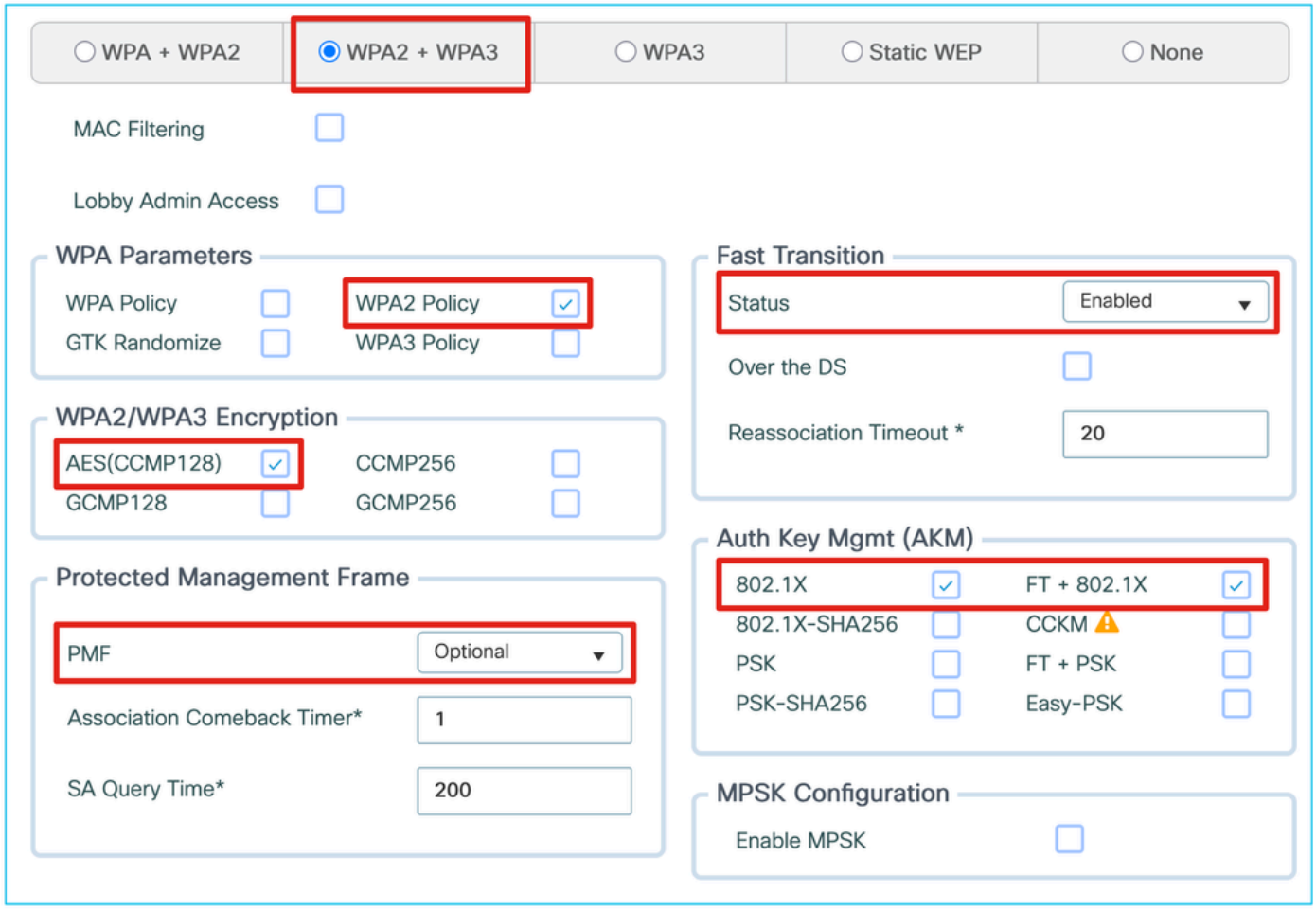
802.1X/WPA3 — 企業網路

基於具有802.1X身份驗證的WPA2/3的企業WLAN最容易遷移到6 GHz和/或Wi-Fi 7。

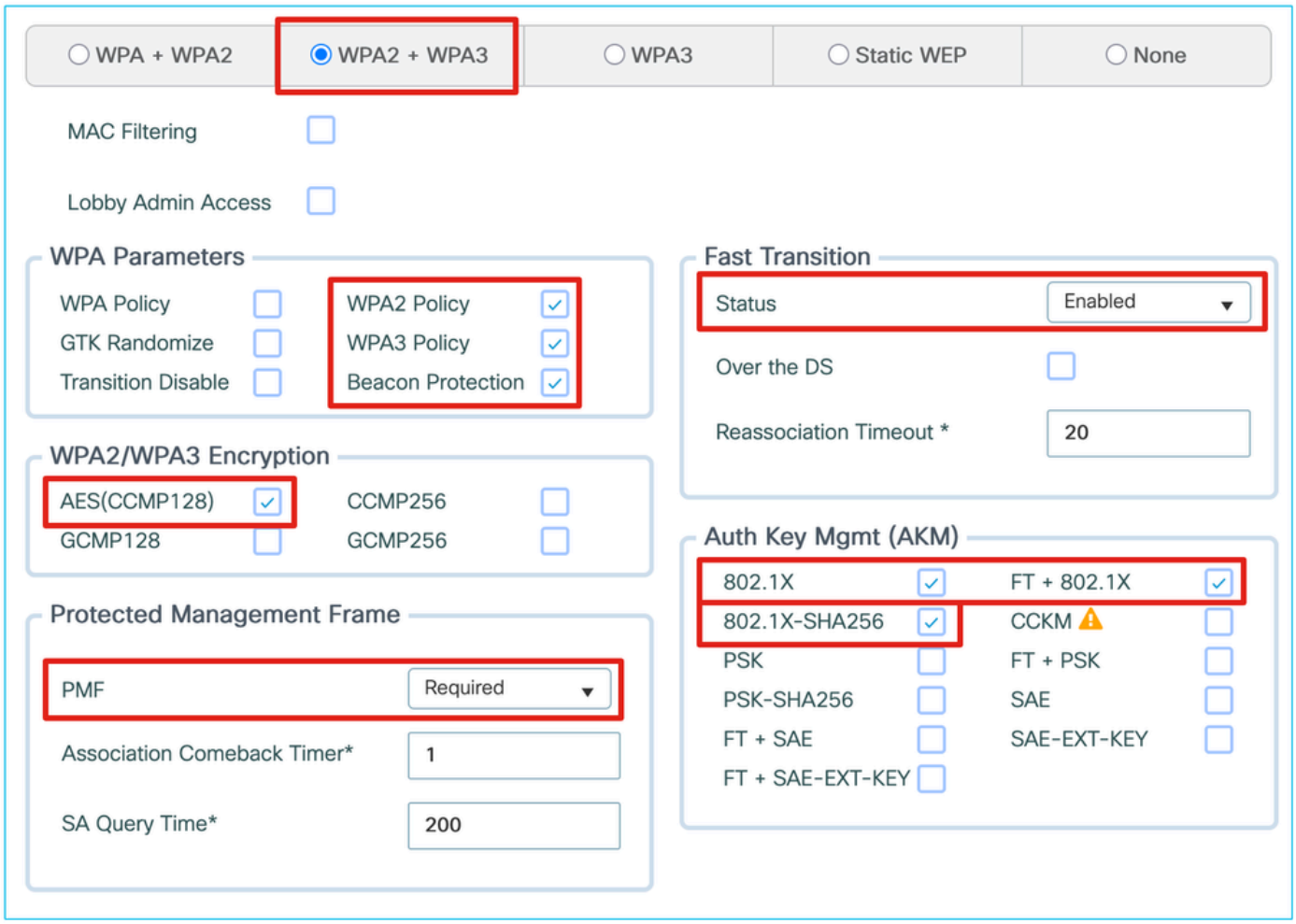
為6 GHz啟用802.1X SSID只需要啟用PMF支援（即使可選），以及802.1X-SHA256和/或FT + 802.1X AKM（兩者均符合WPA3）。

我們可以繼續在同一個WLAN上為WPA2提供標準802.1X(SHA1)。Wi-Fi 7支援要求啟用信標保護和根據要求設定PMF，而不是可選設定；WPA2 802.1X(SHA1)可以作為向後相容選項保留在WLAN中。這意味著，只要您的所有企業裝置支援802.11w/PMF（這在用於筆記型電腦和其他移動端點的當前無線網絡卡上非常常見），您就可以將其置於單個SSID下。

從具有以下L2安全設定的典型WPA2 SSID:



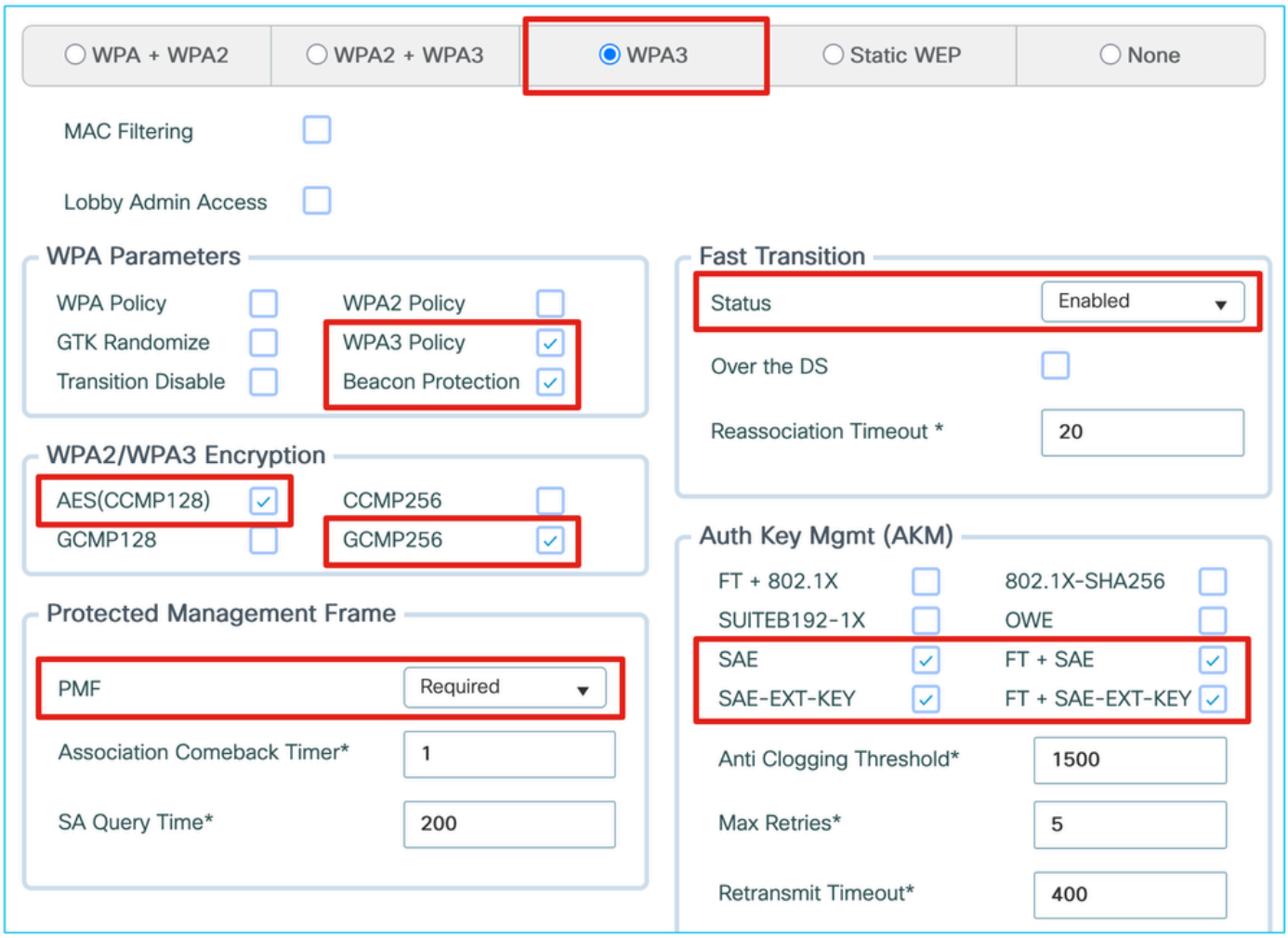
我們可以遷移WPA3、6 GHz和Wi-Fi 7支援的配置，如下所示：

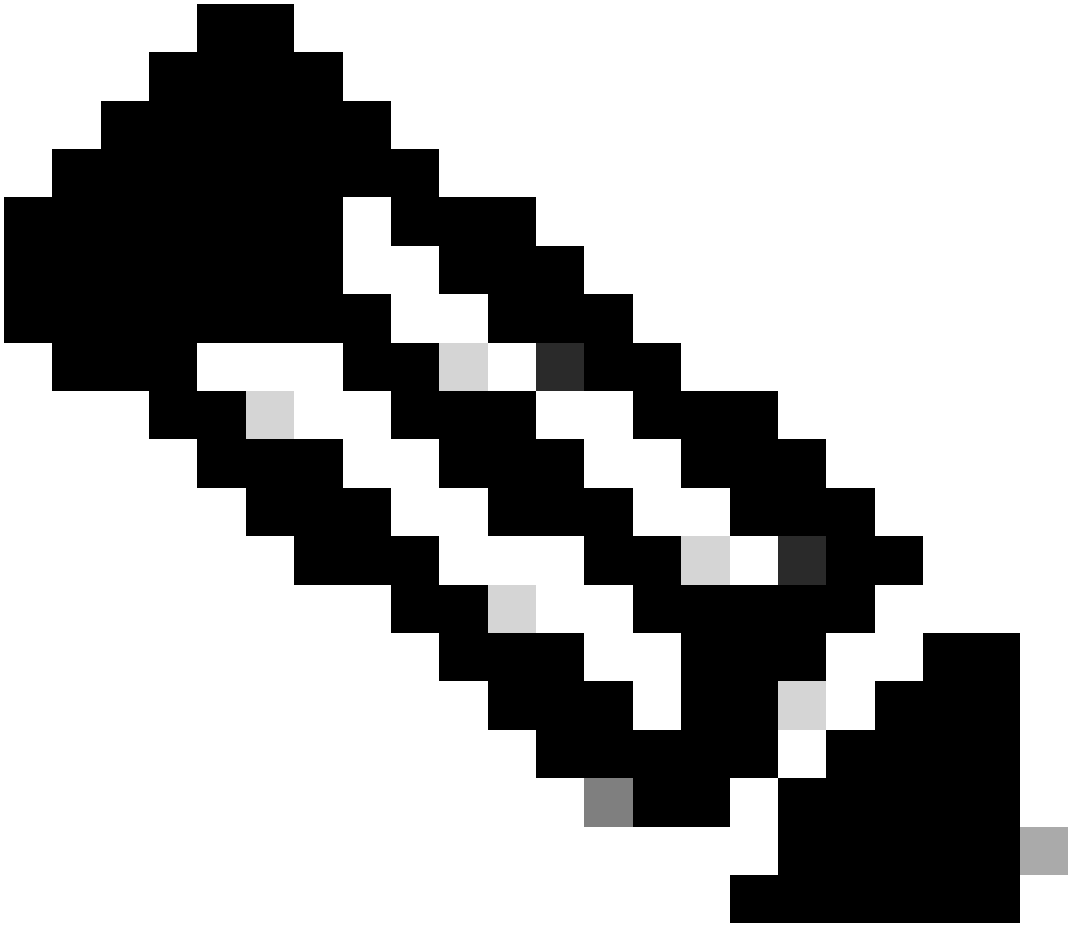


密碼短語/WPA3 — 個人/IoT網路

為6 GHz啟用密碼短語SSID（最多支援Wi-Fi 6E）非常簡單，並且如果需要，需要SAE和/或FT + SAE，以及其他WPA2 PSK AKM。但是，對於Wi-Fi 7支援，認證要求刪除任何WPA2 PSK選項，並新增SAE-EXT-KEY和/或FT + SAE-EXT-KEY AKM以及GCMP256密碼。因此，基於密碼短語的WLAN不可能同時具備較舊客戶端的最大相容性和Wi-Fi 7效能。

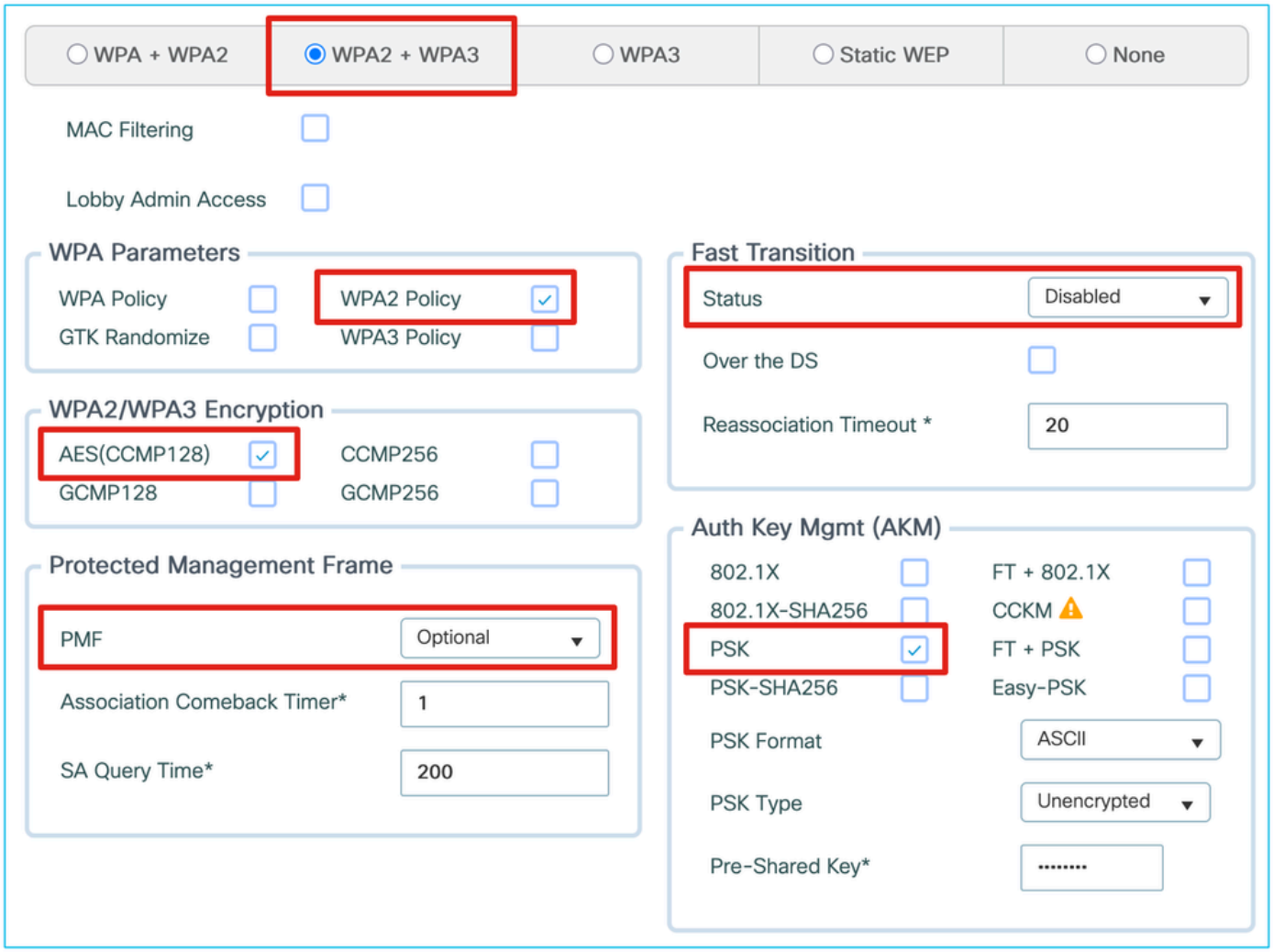
在這種情況下，我們需要為更近的Wi-Fi 6E和Wi-Fi 7客戶端配置專用僅WPA3的SSID，包括SAE、FT + SAE-EXT-KEY和FT + SAE-EXT-KEY，提供AES(CCMP128)和GCMP256密碼。


WPA + WPA2
WPA2 + WPA3
WPA3
Static WEP
None
MAC Filtering
Lobby Admin Access
WPA Parameters
WPA Policy
WPA2 Policy
GTK Randomize
WPA3 Policy
Transition Disable
Beacon Protection
WPA2/WPA3 Encryption
AES(CCMP128)
CCMP256
GCMP128
GCMP256
Protected Management Frame
PMF
Required
Association Comeback Timer*
1
SA Query Time*
200
Fast Transition
Status
Enabled
Over the DS
Reassociation Timeout *
20
Auth Key Mgmt (AKM)
FT + 802.1X
802.1X-SHA256
SUITEB192-1X
OWE
SAE
FT + SAE
SAE-EXT-KEY
FT + SAE-EXT-KEY
Anti Clogging Threshold*
1500
Max Retries*
5
Retransmit Timeout*
400



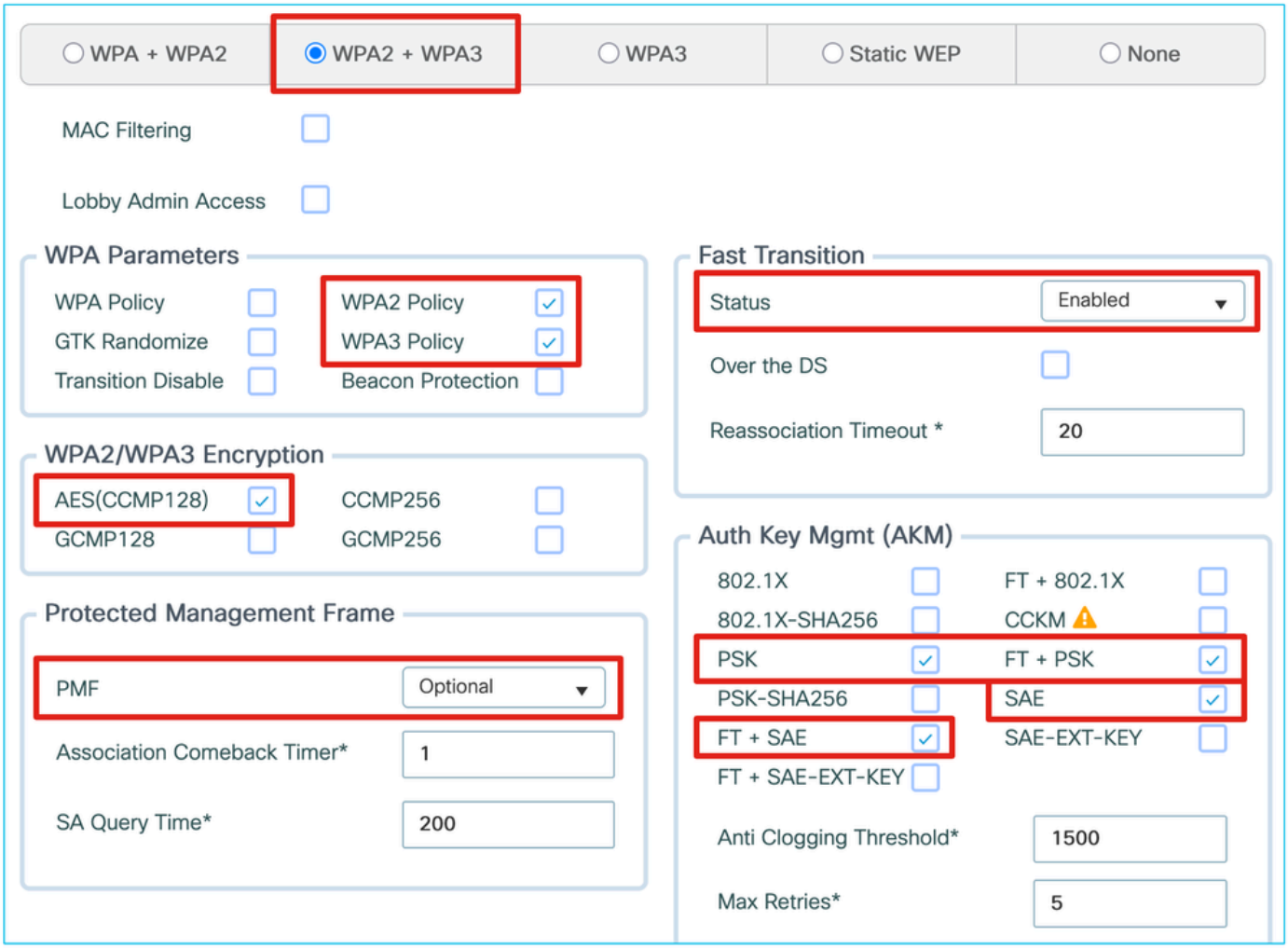
附註：如果在WLAN上啟用(FT +)SAE，並且Wi-Fi 7客戶端嘗試與其關聯而不是(FT +)SAE-EXT-KEY，則會拒絕該請求。只要(FT +)也啟用SAE-EXT-KEY，Wi-Fi 7客戶端無論如何都必須使用後一個AKM，而且此問題一定不會發生。

另一方面，另一個常規WPA2 SSID仍可容納其餘的舊客戶端。



雖然此組合會增加總SSID的數量，但它允許保持一個SSID的最大相容性，這樣我們可能也會禁用其他高級功能，這些功能可能會影響相容性，而且可能對許多IoT場景有所幫助，同時通過另一個SSID為較新的裝置提供最大特性和效能。
當然，還有一個選項是不提供Wi-Fi 7 SSID，並且只保留一個配置為WPA2 PSK和WPA3 SAE的SSID。其背後的理念可能是IoT裝置無論如何都不需要Wi-Fi 7效能。

此方法仍然支援支援Wi-Fi 6E和Wi-Fi 7客戶端的6 GHz，這些客戶端最多能連線Wi-Fi 6E效能。



在所有這些方案中，我們強烈建議使用SAE時啟用FT。與WPA2 PSK 4次握手相比，SAE幀交換在資源方面成本高昂，而且時間更長。

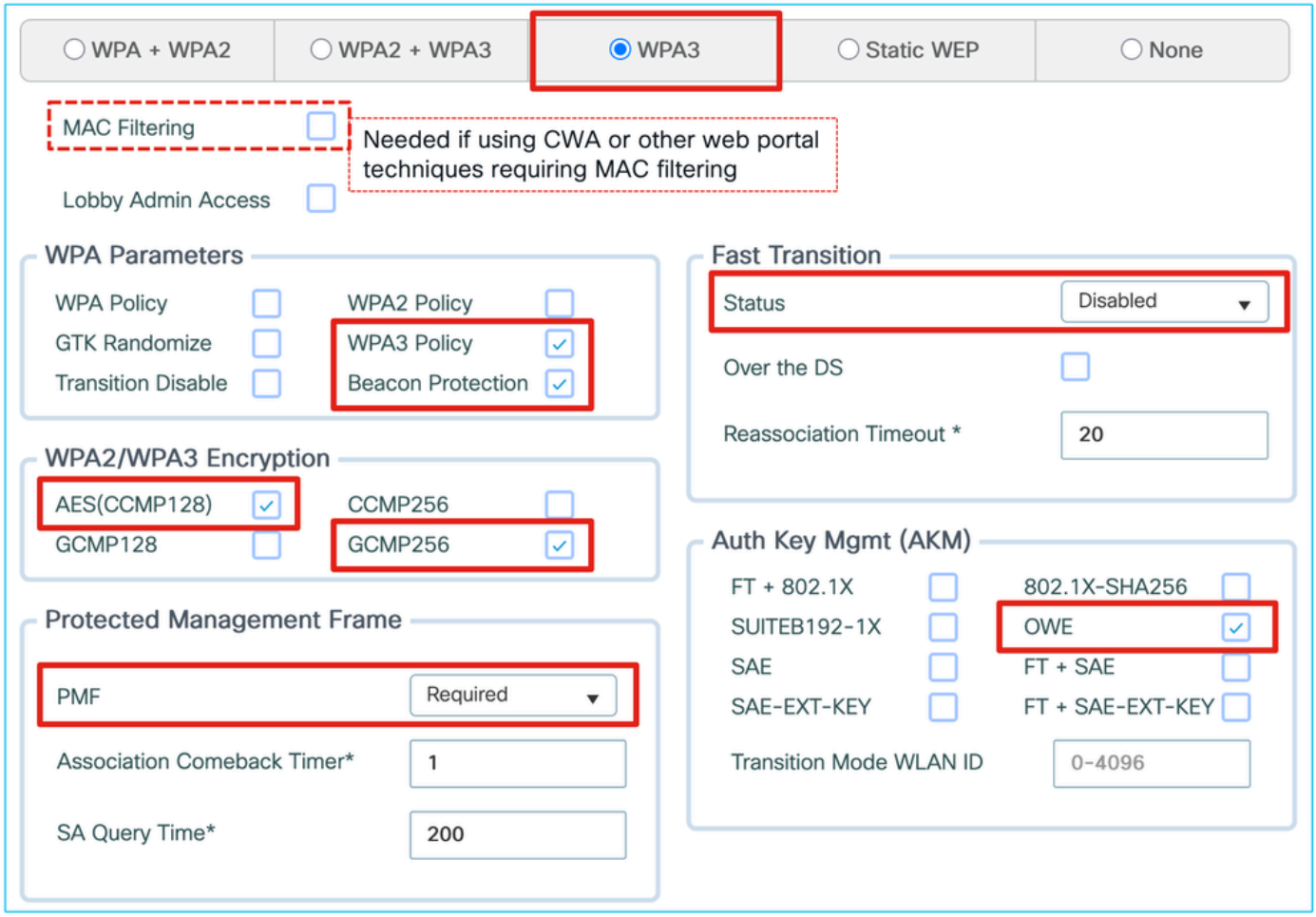
一些裝置製造商，比如蘋果，期望僅在啟用FT時使用SAE，如果不可用，可以拒絕連線。

開放/增強型開放/OWE/訪客網路

訪客網路有多種風格。通常，它們不需要802.1X憑證或密碼短語進行連線，而且可能意味著啟動顯示頁面或輸入網站，這可能要求憑證或代碼。這通常通過開放式SSID以及本地或外部訪客門戶解決方案來處理。但是，在6 GHz上或用於Wi-Fi 7支援時，不允許使用具有開放安全（無加密）的SSID。

第一種非常保守的方法是最多將訪客網路專用於5 GHz頻段和Wi-Fi 6。這就為公司裝置保留了6 GHz頻段，解決了複雜性問題並帶來了最大的相容性，儘管不高達Wi-Fi 6E/7的效能。

如果我們要向訪客提供6 GHz服務，建議使用增強型開放/OWE（機會無線加密）建立單獨的SSID。 它可以提供兩種AES(CCMP128)密碼，最大相容至Wi-Fi 6E客戶端，並為支援Wi-Fi 7的客戶端提供GCMP256位。



如果增強型開放是一款出色的隱私保護方法，同時能夠保持「開放」體驗（終端使用者無需輸入任何802.1X憑證或密碼），則直到今天，它在端點之間的支援仍然有限。某些客戶端仍不支援此功能，即使它們支援，這種技術也並不總是能順利處理（裝置可以將連線顯示為非安全，而實際上它是安全的，或者可以將其顯示為受保護的口令，即使不需要使用OWE的口令）。如果訪客網路需要在所有訪客不受控制的裝置上工作，則僅提供增強型開放SSID可能為時過早，建議通過單獨的SSID提供這兩種選項：5 GHz的開放埠和5 GHz和6 GHz的OWE埠，如果這也需要，則兩者後面都使用相同的強制網路門戶。Wi-Fi 6E、6 GHz（即使軟體上仍允許使用過渡模式）或Wi-Fi 7不支援過渡模式，因此不建議採用此解決方案。OWE仍支援所有門戶重定向技術（內部或外部Web身份驗證、中央Web身份驗證……）。

其他WPA3和相關選項

雖然WPA3選項在《WPA3部署指南》中進行了最詳細的描述和介紹，但本節介紹一些與6 GHz和Wi-Fi 7支援特別相關的WPA3額外建議。

信標保護

這是一個可解決此漏洞的功能，惡意攻擊者可在該漏洞中傳輸信標而不是合法接入點，同時修改某些欄位以更改已關聯客戶端的安全性或其他設定。信標保護是信標中的一個額外資訊元素，它充當信標本身的簽名，以證明它是合法接入點傳送的，並且沒有被篡改。只有具有WPA3加密金鑰的關聯客戶端才能驗證信標的合法性，探測客戶端無法驗證信標。信標中的其他資訊元素必須被不支援它的客戶端（非Wi-Fi 7客戶端）忽略，並且通常不會出現相容性問題（除非使用程式設計不當的客

戶端驅動程式）。

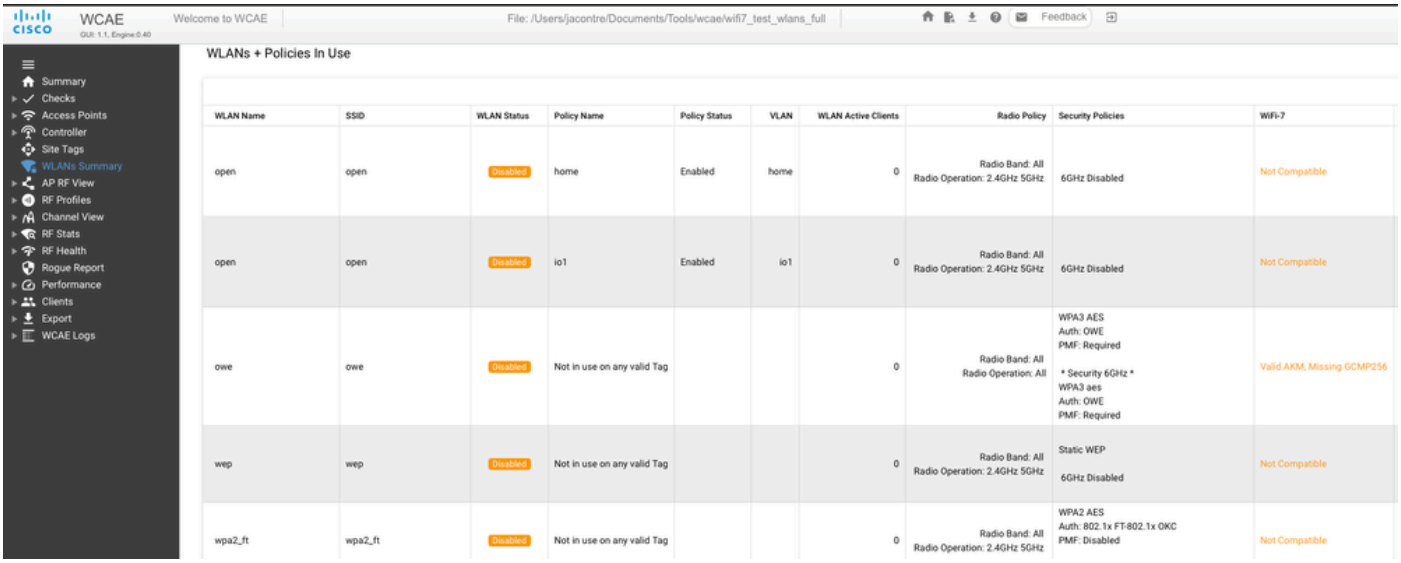
GCMP256

在Wi-Fi 7認證之前，大多數客戶端都實施AES(CCMP128)密碼加密。CCMP256和GCMP256是與SUITE-B 802.1X AKM相關的非常特殊的變體。雖然市場上的某些第一代Wi-Fi 7客戶端聲稱Wi-Fi 7支援，但它們可能仍不實施GCMP256加密，如果Wi-Fi 7 AP按照預期執行標準，阻止這些客戶端在沒有適當的GCMP256支援的情況下進行連線，那麼這可能成為一個問題。

疑難排解和驗證

Wireless Configuration Analyzer Express最新版本(https://developer.cisco.com/docs/wireless-troubleshooting-tools/wireless-config-analyzer-express-gui/)具有一個Wi-Fi 7就緒性檢查，可以評估您的9800配置是否符合上述所有Wi-Fi 7要求。

如果您仍然懷疑您的配置是否為Wi-Fi 7，則WCAE會讓您知道問題所在。



參考資料

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）。