Migrazione a 6 GHz e Wi-Fi 7

Sommario

Introduzione

Questo documento descrive le linee guida di progettazione e configurazione per ottimizzare le prestazioni di Wi-Fi 7 e sfruttare appieno lo spettro a 6 GHz.

Perché 6 GHz e Wi-Fi 7

6 GHz è una nuova banda che è diventata disponibile nel 2020 per le operazioni WLAN ed è stata inizialmente sfruttata dalla certificazione Wi-Fi 6E. Mentre Wi-Fi 6E si basa ancora sullo stesso standard 802.11ax (certificato in Wi-Fi 6 per le bande a 2,4/5 GHz), si estende per funzionare solo sulla banda a 6 GHz, a condizione che siano soddisfatti requisiti specifici.

Wi-Fi 7 corrisponde alla certificazione dello standard IEEE 802.11be e, a differenza di Wi-Fi 6E che è limitato solo a 6 GHz, è definito per l'uso in tutte e tre le bande: 2,4, 5 e 6 GHz. Wi-Fi 7 include inoltre nuove funzionalità rispetto alle certificazioni precedenti.

6 GHz e/o Wi-Fi 7 hanno requisiti specifici da supportare, che spesso si traducono in nuove configurazioni e progettazioni di RF, soprattutto rispetto a ciò che abbiamo usato fino alle bande 2.4/5 GHz e Wi-Fi 6. Ad esempio, proprio come l'uso della sicurezza WEP ci impedisce di usare

gli standard 802.11 diversi da 802.11a/b/g, gli standard più recenti hanno prerequisiti di sicurezza più elevati, per spingere l'adozione di reti più sicure.

D'altra parte, la più recente banda a 6 GHz, insieme a certificazioni moderne come Wi-Fi 6E/7, sblocca frequenze più pulite, migliori prestazioni e nuovi utilizzi, o anche un'implementazione più "senza preoccupazioni" degli attuali casi d'uso (ad esempio, conferenze voce/video).

Requisiti di base per operazioni a 6 GHz e Wi-Fi 7

Questi sono i requisiti di sicurezza indicati nelle certificazioni per le operazioni Wi-Fi 7 e 6 GHz.

Requisiti di banda a 6 GHz

La banda a 6 GHz può consentire solo WPA3 o Enhanced Open WLAN, il che significa una delle seguenti opzioni di sicurezza:

- WPA3-Enterprise con autenticazione 802.1X
- WPA3 Simultaneous Authentication of Equals (SAE) (alias WPA3-Personal) con passphrase. SAE-FT (SAE con Fast Transition) è un altro possibile AKM ed è in realtà consigliato per l'uso poiché l'handshake SAE non è banale e FT permette di saltare questo scambio più lungo.
- Apertura migliorata con crittografia wireless opportunistica (OWE)

Sebbene, come indicato nelle specifiche WPA3 v3.4 (sezione 11.2), la modalità di transizione aperta avanzata non sia supportata con 6 GHz, molti fornitori (incluso Cisco fino a IOS® XE 17.18) non la applicano ancora. Pertanto, è tecnicamente possibile configurare ad esempio un Open SSID su 5 GHz, un Enhanced Open SSID corrispondente su 5 e 6 GHz, entrambi con la modalità di transizione attivata e tutto questo senza rispettare le specifiche degli standard. In uno scenario di questo tipo, è tuttavia necessario configurare un Enhanced Open SSID senza modalità di transizione e disponibile solo su 6 GHz (i client che supportano 6 GHz supportano in genere la modalità Enhanced Open), mantenendo il nostro Open SSID standard su 5 GHz, anche senza modalità di transizione.

A parte l'imposizione 802.11w/PMF (Protected Management Frame), WPA3-Enterprise non prevede nuovi requisiti specifici per cifrari o algoritmi. Molti fornitori, tra cui Cisco, considerano lo standard 802.1X-SHA256 o "FT + 802.1X" (che in realtà è 802.1X con SHA256 e Fast Transition nella parte superiore) solo conforme allo standard WPA3 e lo standard 802.1X (che utilizza SHA1) è considerato parte di WPA2, quindi non adatto/supportato per 6 GHz.

Requisiti Wi-Fi 7

Con la certificazione Wi-Fi 7 dello standard 802.11be, la Wi-Fi Alliance ha aumentato i requisiti di sicurezza. Alcuni di essi consentono di utilizzare le velocità dati 802.11be e i miglioramenti del protocollo, mentre altri sono specifici per il supporto delle operazioni Multi-Link (MLO), consentendo ai dispositivi compatibili (client e/o access point) di utilizzare più bande di frequenza mantenendo la stessa associazione.

In generale, Wi-Fi 7 richiede uno dei seguenti tipi di protezione:

- WPA3-Enterprise con AES (CCMP128) e 802.1X-SHA256 o FT + 802.1X (che utilizza ancora SHA256, anche se non esplicito nella denominazione). Ciò non rappresenta una modifica rispetto ai prerequisiti di sicurezza WPA3 esistenti in precedenza per la banda a 6 GHz.
- WPA3-Personale con GCMP256 e SAE-EXT-KEY e/o FT + SAE-EXT-KEY (AKM 24 o 25). Wi-Fi 6E obbligatorio WPA3 SAE e/o FT + SAE solo con AES regolare (CCMP128) e nessun uso esteso di chiavi, quindi questo è un nuovo cifrario introdotto appositamente per Wi-Fi 7.
- Apertura/OWE avanzata con GCMP256. Sebbene sia ancora possibile configurare AES(CCMP128) sullo stesso SSID, i client che utilizzano AES 128 non possono supportare Wi-Fi 7. Prima di Wi-Fi 7, la maggior parte dei client che supportano AES 128 utilizzava solo AES 128, quindi questo è un nuovo requisito più avanzato. Come per il supporto a 6 GHz, non è tollerata alcuna modalità di transizione.

In tutti questi casi, per il supporto di Wi-Fi 7 sulla WLAN sono richiesti anche PMF (Protected Management Frames) e Beacon Protection.

Wi-Fi 7 era ancora recente al momento della stesura di questo documento, con una versione il più presto possibile, molti fornitori non hanno applicato tutti questi requisiti di sicurezza sin dall'inizio.

Più di recente, Cisco ha progressivamente imposto le opzioni di configurazione per essere conforme alla certificazione Wi-Fi 7. Di seguito sono riportati i comportamenti specifici della versione:

17.18.1 e successive

IOS XE 17.18 e versioni successive pubblicizzano una determinata WLAN come abilitata per Wi-Fi 7 solo se la WLAN ha parametri di sicurezza che soddisfano i requisiti Wi-Fi 7 (protezione beacon, PMF e l'AKM corretto, come descritto in precedenza, a seconda del tipo di WLAN e se esiste la GCMP256 per raggiungere il MLO di Wi-Fi 7, in caso di OWE o SAE-EXT). La presenza di AES128 è tollerata sull'SSID ma, se utilizzata, fornisce solo Wi-Fi 6E e non Wi-Fi 7 MLO.

Un client può associarsi come Wi-Fi 7 e ottenere velocità dati Wi-Fi 7 indipendentemente dal metodo di sicurezza utilizzato (a condizione che sia ancora supportato dalla WLAN). Tuttavia, il client può associarsi come MLO (su una o più bande) solo se rispetta i requisiti rigorosi per la sicurezza Wi-Fi 7, o se viene rifiutato.

17.15.3 e versioni successive 17.15.x

In questa sezione, tutte le WLAN vengono trasmesse come SSID Wi-Fi 7, a condizione che Wi-Fi 7 sia abilitato a livello globale e indipendentemente dalle impostazioni di sicurezza.

Un client può associarsi come compatibile con Wi-Fi 7 e ottenere velocità di trasmissione dati Wi-Fi 7 indipendentemente dal metodo di sicurezza utilizzato, a condizione che sia ancora supportato dalla WLAN. Tuttavia, il client può associarsi come MLO (su una o più bande) solo se rispetta i requisiti rigorosi per la sicurezza Wi-Fi 7, o altrimenti viene rifiutato.

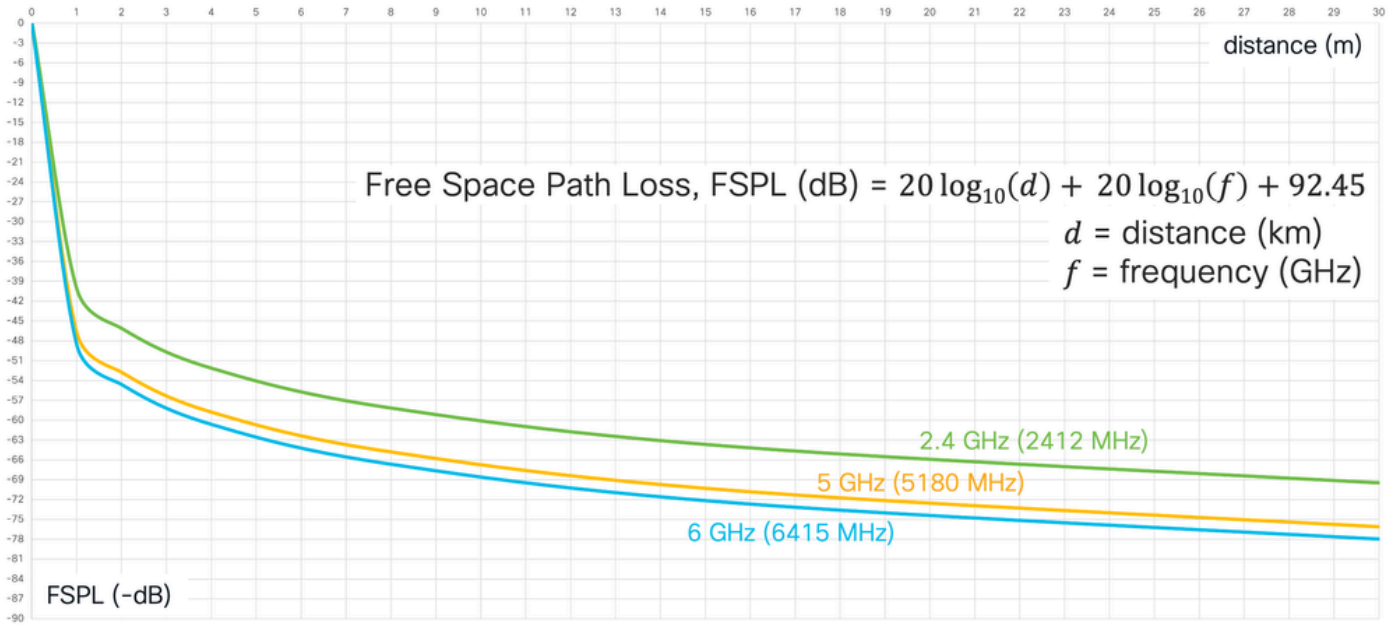
Ciò potrebbe causare problemi, quando alcuni dei primi client Wi-Fi 7 non sono in grado di supportare cifrature più sicure, come GCMP256, tentano di associarli come MLO di Wi-Fi 7 a una WLAN, le cui impostazioni di sicurezza non soddisfano i requisiti di Wi-Fi 7. In una situazione di questo tipo, il client viene rifiutato a causa di impostazioni di sicurezza non valide (ancora configurabili nella rete WLAN).

Considerazioni sulla progettazione radio per la copertura a 6 GHz

Senza voler diventare una guida prescrittiva completa sui sondaggi in loco, questa sezione descrive brevemente alcune considerazioni di base quando si progetta per la copertura a 6 GHz, soprattutto se esiste già un'installazione per 2,4/5 GHz che vorremmo migrare a Wi-Fi 6E o 7. Come per ogni nuova installazione Wi-Fi a cui eravamo abituati a 2,4 e/o 5 GHz, un nuovo progetto wireless a 6 GHz deve includere anche un corrispondente sondaggio del sito dedicato a 6 GHz.

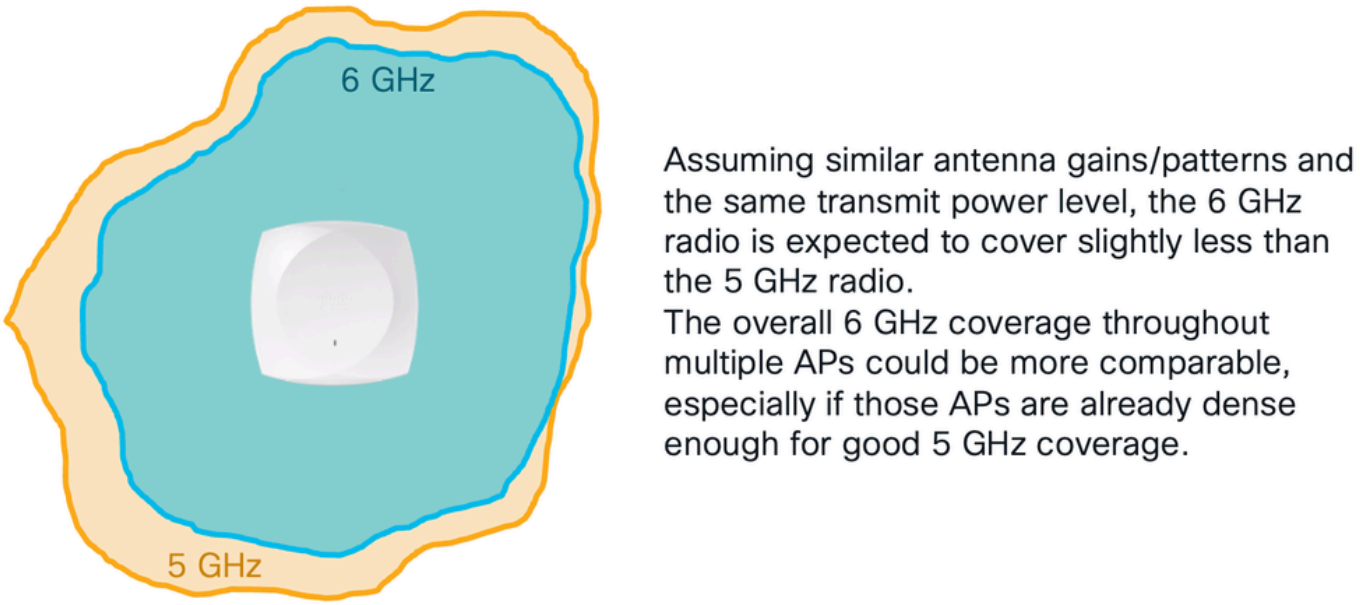
Quando i punti di accesso pre-Wi-Fi 6E/7 sono già posizionati per una copertura a 5 GHz e per esigenze specifiche, in alcuni casi possiamo aspettarci di essere in grado di sostituirli con punti di accesso compatibili con Wi-Fi 6E/7 e di ottenere comunque una buona copertura anche a 6 GHz. Affinché questa teoria funzioni, i nostri punti di accesso esistenti devono già fornire una corretta copertura a 5 GHz per le esigenze previste (solo dati, voce, applicazioni specifiche e così via), pur essendo già almeno 3-4 livelli di potenza di trasmissione sotto il loro limite massimo. I punti di accesso hanno in genere da 7 a 8 livelli di alimentazione e ogni livello di alimentazione divide la potenza di trasmissione per la metà. Ciò significa che il punto più comodo da raggiungere è quello in cui i punti di accesso utilizzano il mezzo del proprio intervallo di potenza di trasmissione consentito.

In base ai calcoli di perdita di spazio libero, i segnali a 6 GHz sono attenuati da 2 dB superiori a quelli a 5 GHz. Oltre a ciò, i segnali a 6 GHz possono anche essere maggiormente influenzati da ostacoli rispetto ai loro equivalenti a 5 GHz.



Quando un Cisco AP aumenta/diminuisce la sua potenza di trasmissione di un livello, lo fa con un

"salto" di 3 dB. Un punto di accesso che passa da un livello di potenza di 4, ad esempio con una potenza di trasmissione di 11 dBm, a un livello di potenza di 3, aumenta la potenza di trasmissione a 14 dBm (ad esempio, 11 dBm per il livello di potenza 4 e 14 dBm per il livello di potenza 3 sono solo un esempio generico, in quanto diversi modelli/generazioni di punti di accesso potrebbero avere valori di potenza di trasmissione leggermente diversi in dBm per lo stesso numero di livello di potenza).



Se un access point pre-Wi-Fi 6E/7 offre già una buona copertura a 5 GHz sul livello di alimentazione 4, ad esempio, un access point Wi-Fi 6E/7 più recente con modelli radio simili a 5 GHz potrebbe sostituire il precedente senza alcun impatto significativo sulla rete a 5 GHz esistente.

Inoltre, la radio da 6 GHz del nuovo Wi-Fi 6E/7 AP potrebbe fornire una copertura simile da 6 GHz a quella da 5 GHz solo se si trova a un livello di potenza di trasmissione (quindi 3 dB) più alto.

Se i 5 GHz sono già correttamente coperti con la radio da 5 GHz dell'access point a livelli di potenza da 3 a 4 al di sotto del suo massimo, la corrispondente radio da 6 GHz potrebbe quindi essere impostata a livelli di potenza da 2 a 3 al di sotto del suo massimo per una copertura comparabile.

Inoltre, se la radio a 6 GHz fornisce già una corretta copertura a 2-3 livelli di potenza inferiori al suo massimo, potrebbe ancora eccezionalmente andare anche di un paio di livelli più in alto, per esempio per provare a lavorare intorno a temporanei buchi di copertura inattesi (un guasto di un vicino AP, ostacoli non annunciati, nuove esigenze di RF e così via).

Comportamenti di roaming tra i punti di accesso precedenti a Wi-Fi 6E/7 e Wi-Fi 6E/7

L'installazione di punti di accesso che supportano diversi standard e/o bande di frequenza nella stessa area di copertura non è sempre stata una pratica consigliata, soprattutto se queste diverse generazioni di punti di accesso sono installate in modo "sale e pepe" (cioè mescolate tra loro nella

stessa zona).

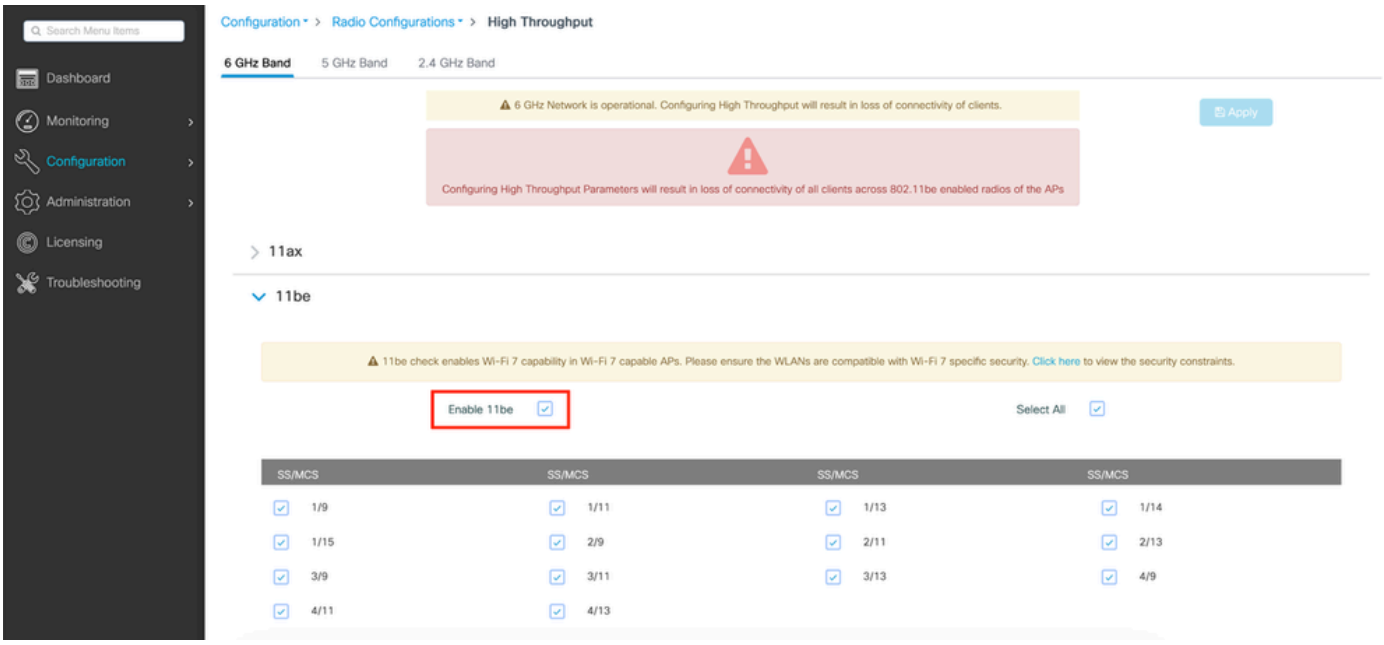
Mentre un controller wireless è in grado di gestire le operazioni (ad esempio, l'assegnazione dinamica dei canali, la trasmissione del controllo dell'alimentazione, la distribuzione della cache PMK e così via) da un gruppo di diversi modelli AP, i client che si spostano tra standard diversi e bande di frequenza diverse non sono sempre in grado di gestire questo problema in modo appropriato e potrebbero ad esempio incorrere in problemi di roaming.

Inoltre, a causa degli standard più recenti, gli access point Wi-Fi 6E/7 supportano i cifrari GCMP256 per WPA3. Lo stesso potrebbe tuttavia non essere sempre vero per alcuni access point Wi-Fi 6 e modelli precedenti. Per i passphrase/WPA3-Personal e i SSID Open/OWE avanzati che richiedono la configurazione di entrambi i cifrari AES(CCMP128) e GCMP256, alcuni Wi-Fi 6 (come la serie 9105, 9115 e 9120) non supportano GCMP256 e possono offrire cifrari AES(CCMP128) solo ai client associati, inclusi quelli compatibili con Wi-Fi 6E/7. Se questi client Wi-Fi 6E/7 necessitassero di effettuare il roaming da/verso gli access point Wi-Fi 6E/7 adiacenti che supportano GCMP256, dovrebbero passare attraverso una nuova associazione, in quanto la rinegoziazione dei cifrari tra AES (CCMP128) e GCMP256 non è supportata per il roaming trasparente. Inoltre, in generale, non è ottimale avere punti di accesso che offrono nuove funzionalità e altri punti di accesso nella stessa area che non offrono le stesse funzionalità: non consente ai client di utilizzare in modo sicuro queste funzionalità durante lo spostamento e può portare a stickyness o disconnessioni.
Anche se questo scenario deve rappresentare un caso d'angolo, vogliamo tenere presente che, con i cifrari GCMP256 configurati nella WLAN, il roaming dei client Wi-Fi 6E/7 tra i punti di accesso 9105/9115/9120 e 9130/9124/916x/917x non può essere possibile, in quanto queste serie supportano GCMP256 e le prime no.

Larghezze di canale pari o superiori a 40 MHz su 6 GHz possono inoltre causare persistenza per i client in grado di supportare 6 GHz, che possono rifiutarsi di riassociarsi ad altre bande. Questo è un motivo in più per non combinare AP da 6 GHz con AP da 6 GHz non compatibili nella stessa area di roaming.

Abilitazione di Wi-Fi 7 a livello globale

Quando si installa o si esegue l'aggiornamento a una versione di IOS XE che supporta Wi-Fi 7, per impostazione predefinita il supporto per Wi-Fi 7 è disabilitato a livello globale.
Per attivarlo, è necessario navigare nel menu di configurazione High Throughput di ciascuna banda a 2,4/5/6 GHz e selezionare la casella per abilitare 11be.



In alternativa, è possibile eseguire queste tre righe di comando tramite SSH/console nella modalità di configurazione terminale:

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

Come indicato nella nota di avviso, quando si tenta di modificare queste impostazioni, la modifica dello stato del supporto 802.11be comporta una breve perdita di connettività per tutti i client tramite le radio dei Wi-Fi 7 AP. Se si desidera eseguire MLO, ovvero i client che si connettono a più bande contemporaneamente, è necessario abilitare 11be su tutte le bande a cui si desidera connettere il client. Non è necessario attivare su tutte le bande, ma consigliato semplicemente per le prestazioni.

Scenari d'uso

Reti 802.1X / WPA3-Enterprise

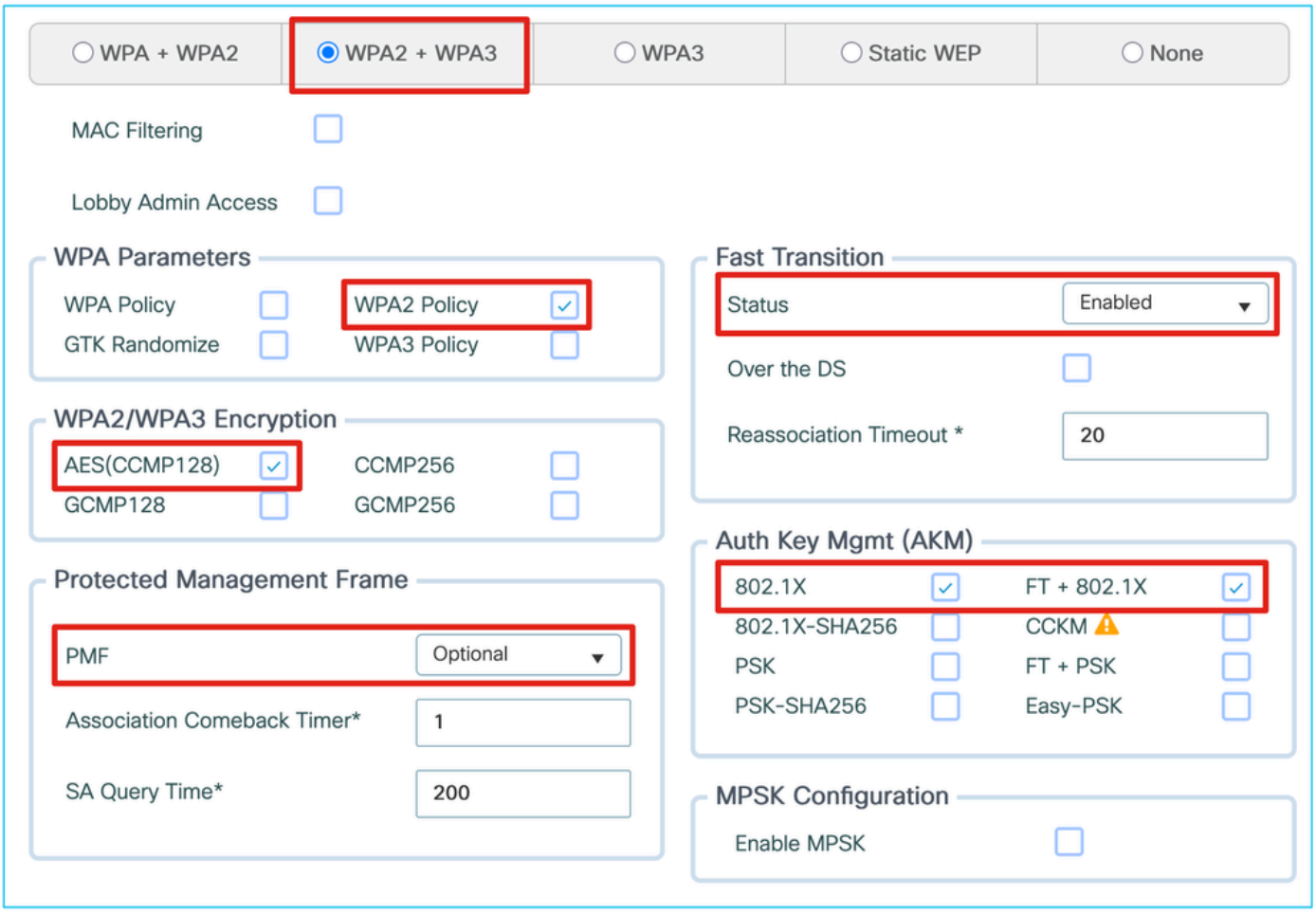
Le WLAN aziendali basate su WPA2/3 con autenticazione 802.1X sono le più facili da migrare a 6 GHz e/o Wi-Fi 7.

L'abilitazione dell'SSID 802.1X per 6 GHz richiede solo l'abilitazione del supporto PMF, anche se opzionale, nonché degli AKM 802.1X-SHA256 e/o FT + 802.1X, entrambi compatibili con WPA3.

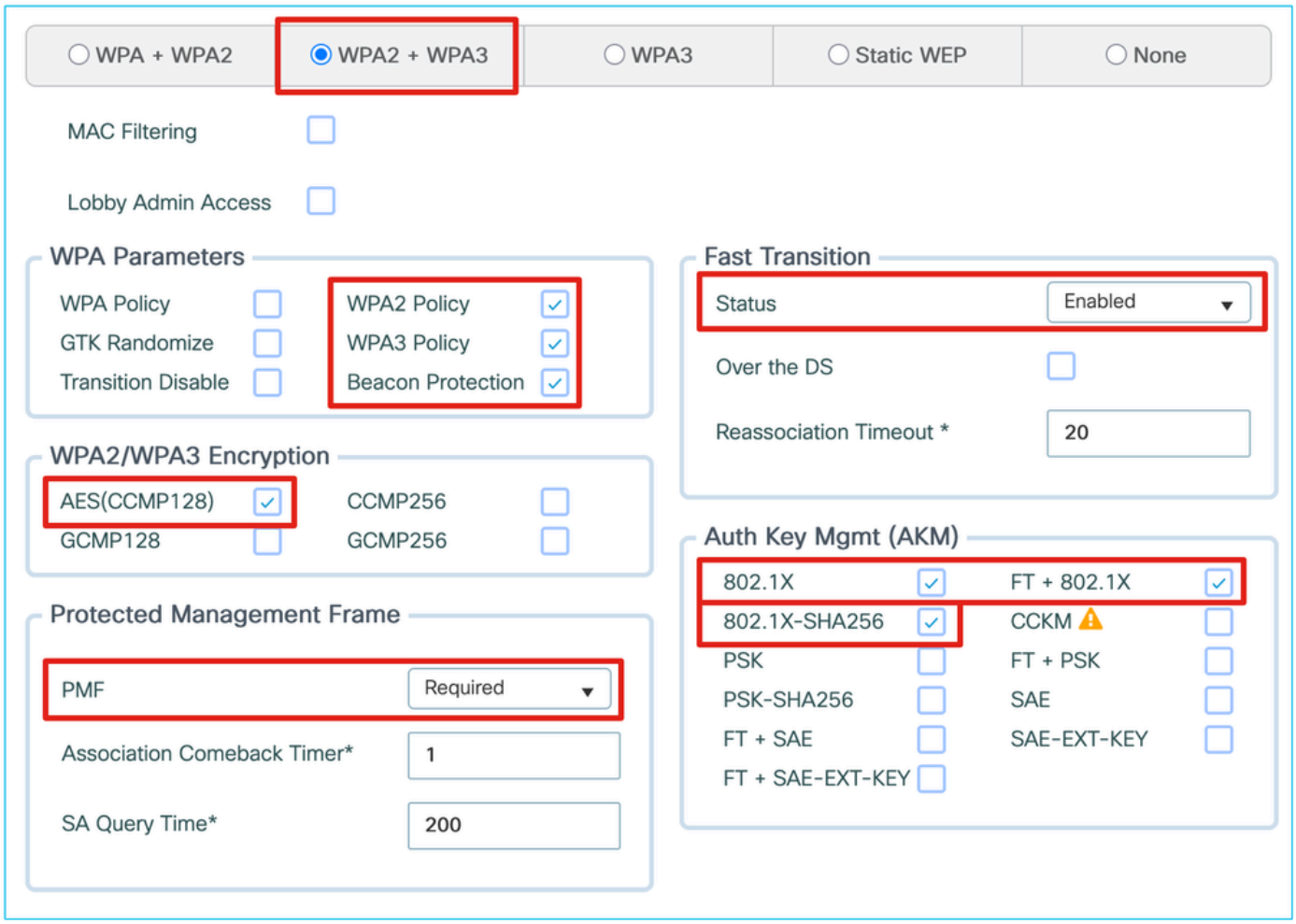
Possiamo continuare a offrire WPA2 con SHA1 802.1X standard sulla stessa WLAN. Il supporto Wi-Fi 7 richiede l'attivazione di Beacon Protection e l'impostazione di PMF come richiesto invece che come opzione; WPA2 802.1X (SHA1) può rimanere presente sulla WLAN come opzione di compatibilità con le versioni precedenti. Ciò significa che è possibile avere tutti i dispositivi

aziendali sotto un unico SSID, purché supportino lo standard 802.11w/PMF, molto comune nelle attuali schede di interfaccia di rete wireless per notebook e altri endpoint mobili.

Da un SSID WPA2 tipico con queste impostazioni di protezione L2:



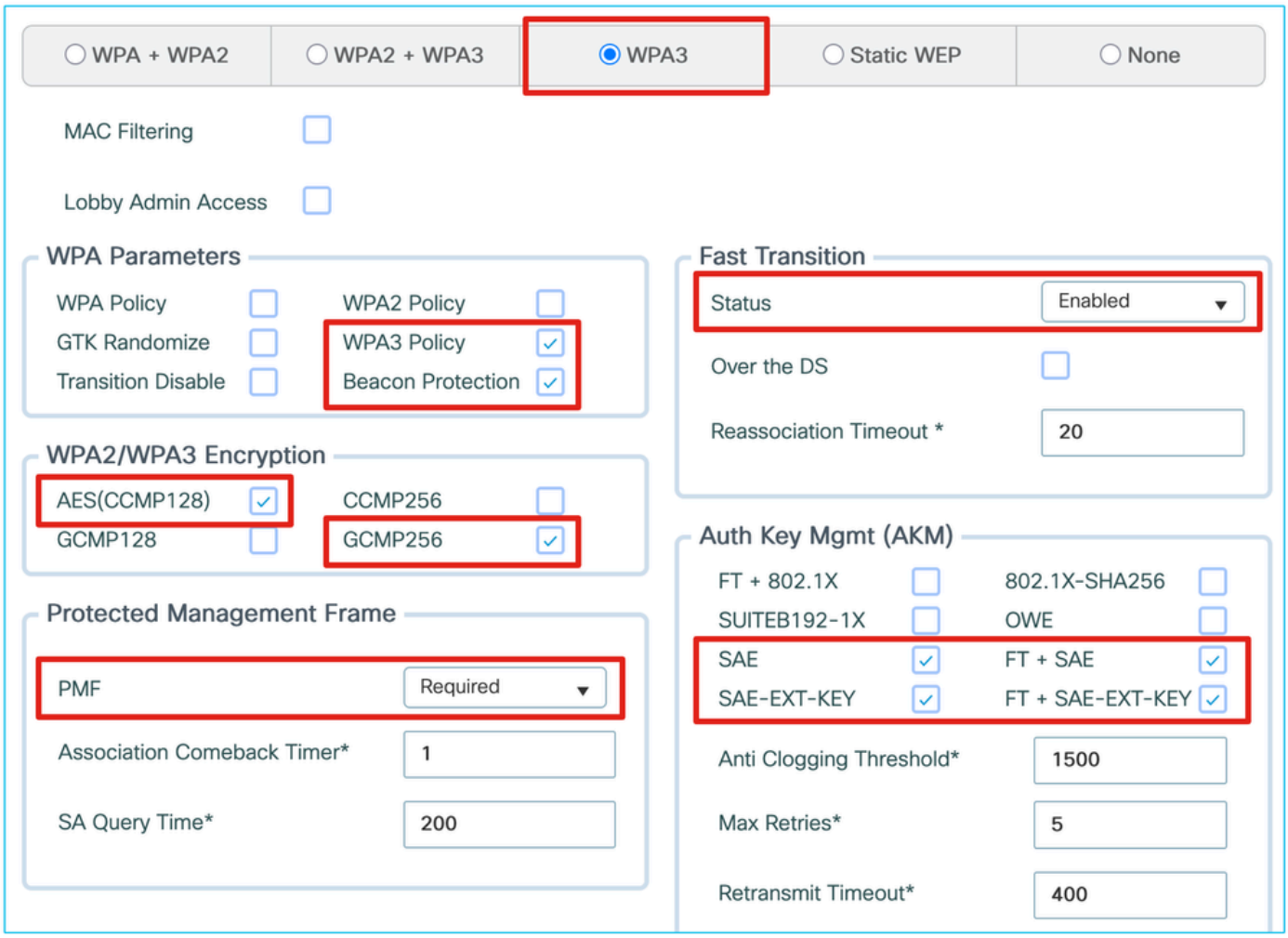
È possibile eseguire la migrazione della configurazione per il supporto di WPA3, 6 GHz e Wi-Fi 7, come mostrato di seguito:

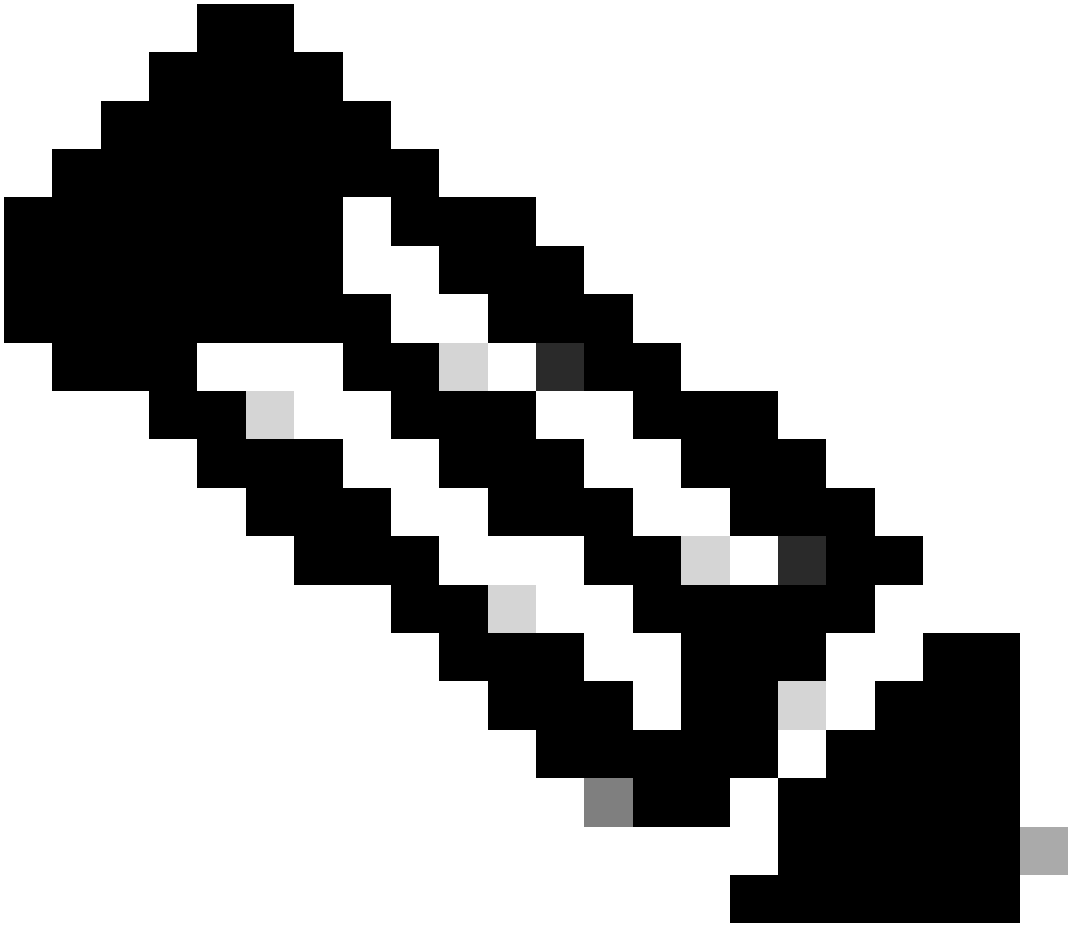


Passphrase / WPA3-Personal / Reti IoT

L'attivazione di una passphrase SSID per 6 GHz, fino al supporto Wi-Fi 6E, è semplice e richiede SAE e/o FT + SAE, insieme ad altri PSK AKM WPA2, se necessario. Tuttavia, per il supporto Wi-Fi 7, la certificazione richiede la rimozione di qualsiasi opzione WPA2 PSK e l'aggiunta di AKM SAE-EXT-KEY e/o FT + SAE-EXT-KEY, insieme alla cifratura GCMP256. Non è quindi possibile avere una WLAN basata su passphrase con la massima compatibilità sia per i client meno recenti che per le prestazioni Wi-Fi 7.

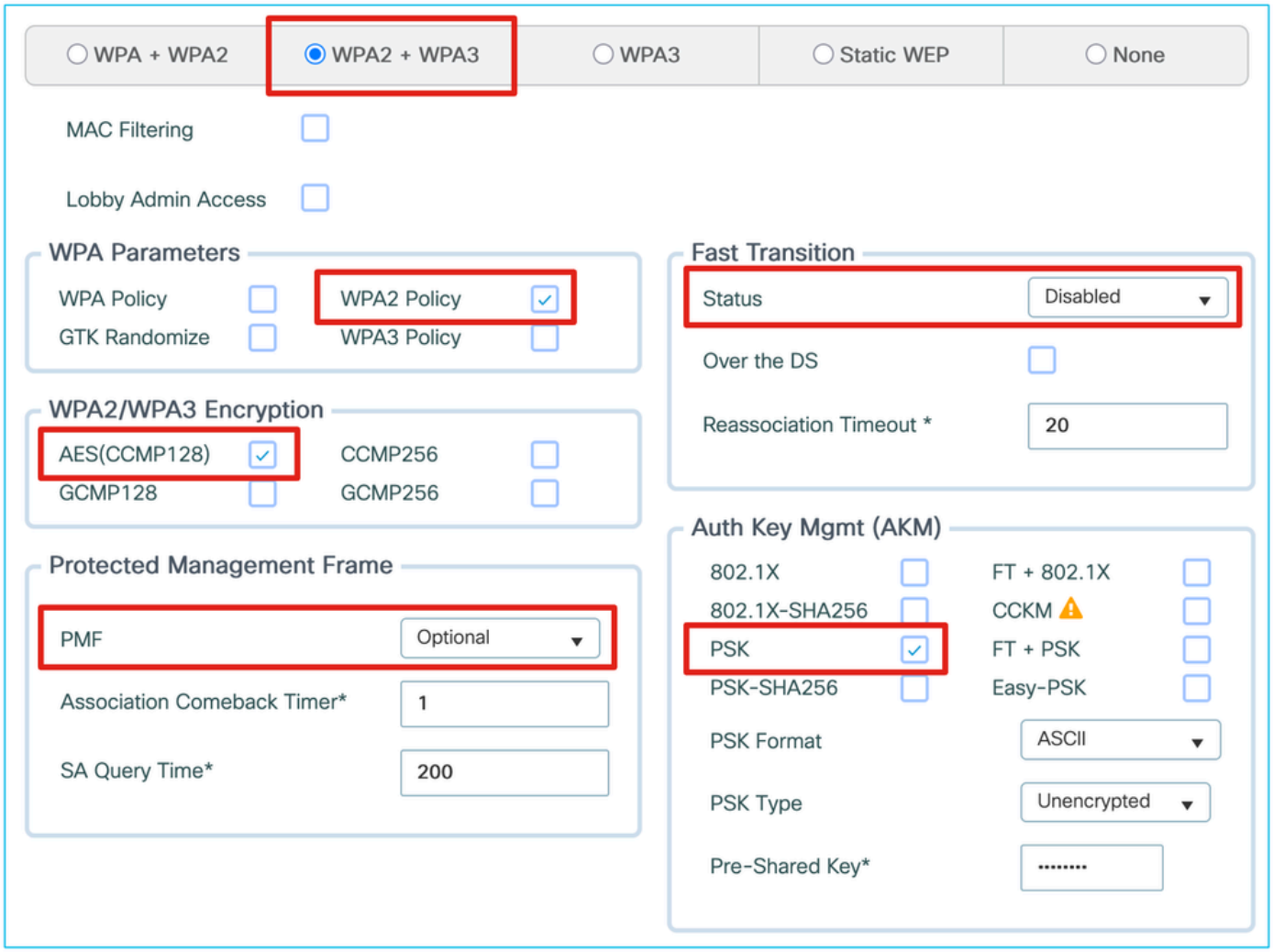
In questi casi, è necessario configurare un SSID WPA3 dedicato solo con SAE, FT + SAE, SAE-EXT-KEY e FT + SAE-EXT-KEY, che offra sia le cifrature AES(CCMP128) che GCMP256, per i client Wi-Fi 6E e Wi-Fi 7 più recenti.


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



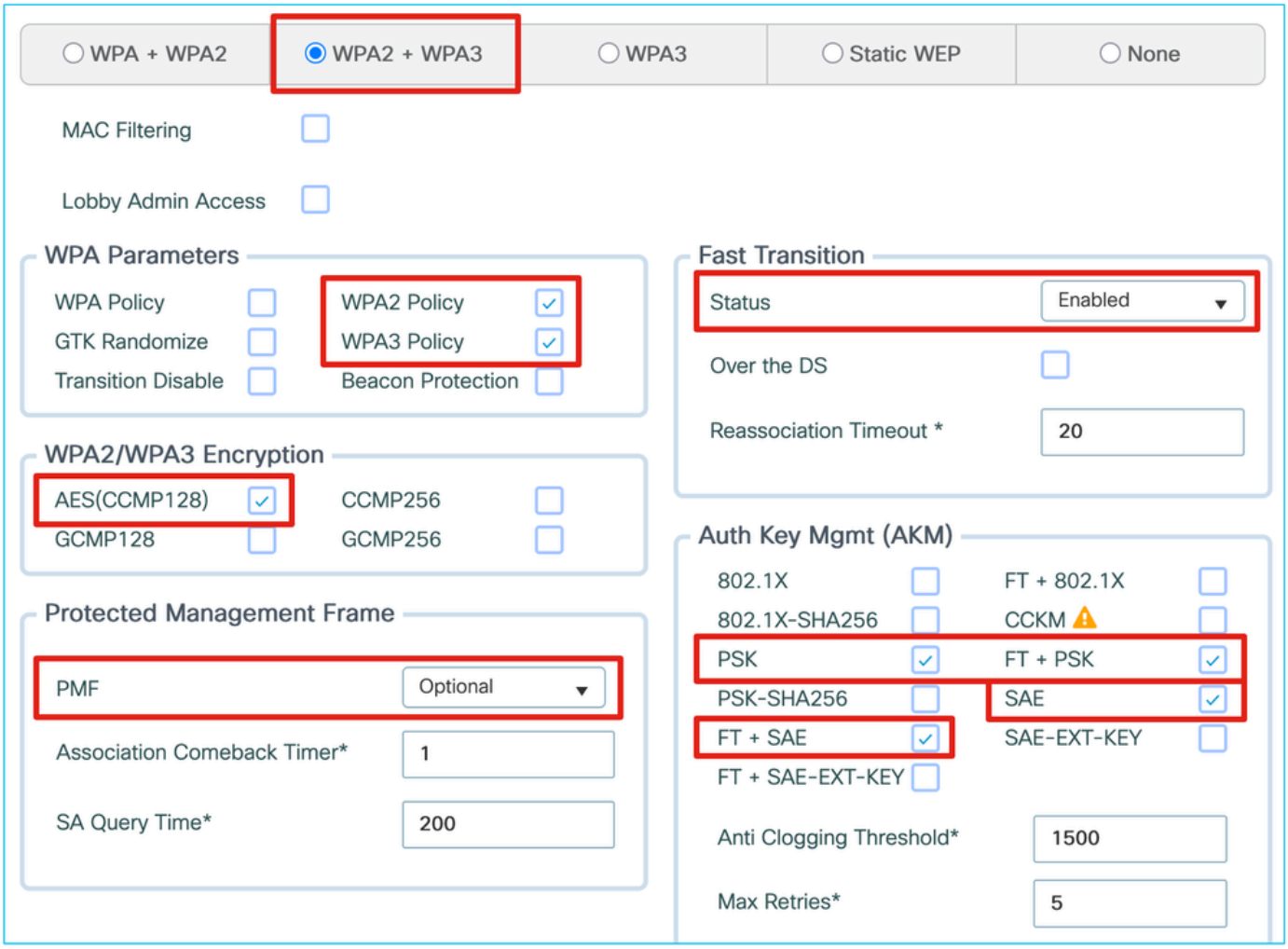
Nota: Se (FT +) SAE è abilitato sulla WLAN e un client Wi-Fi 7 tenta di associarlo a esso anziché (FT +) SAE-EXT-KEY, l'associazione viene rifiutata. Finché anche (FT +) SAE-EXT-KEY è abilitato, i client Wi-Fi 7 devono comunque usare quest'ultimo AKM e questo problema non deve verificarsi.

Un altro SSID WPA2 regolare, invece, può ancora ospitare i client legacy rimanenti.



Sebbene questa combinazione aumenti la quantità totale di SSID, consente di mantenere la massima compatibilità su un SSID, in cui è possibile anche disabilitare potenzialmente altre funzionalità avanzate che potrebbero influire sulla compatibilità e che potrebbero essere utili per molti scenari IoT, offrendo al contempo funzionalità e prestazioni massime per i dispositivi più recenti tramite l'altro SSID.
Un'altra opzione potrebbe essere ovviamente quella di non offrire il SSID Wi-Fi 7 e di mantenere solo un'opzione configurata per WPA2 PSK e WPA3 SAE. L'idea alla base potrebbe essere che i dispositivi IoT non possono comunque avere bisogno delle prestazioni di Wi-Fi 7.

Questo approccio potrebbe comunque supportare ancora 6 GHz per i client Wi-Fi 6E e Wi-Fi 7, che sarebbero in grado di collegarsi con prestazioni Wi-Fi 6E nel migliore dei casi.



In tutti questi scenari si consiglia di abilitare FT quando si utilizza SAE. Lo scambio di frame SAE è costoso in termini di risorse e più lungo dell'handshake a 4 vie WPA2 PSK.

Alcuni produttori di dispositivi come Apple prevedono di utilizzare SAE solo quando FT è abilitato e possono rifiutarsi di connettersi se non disponibile.

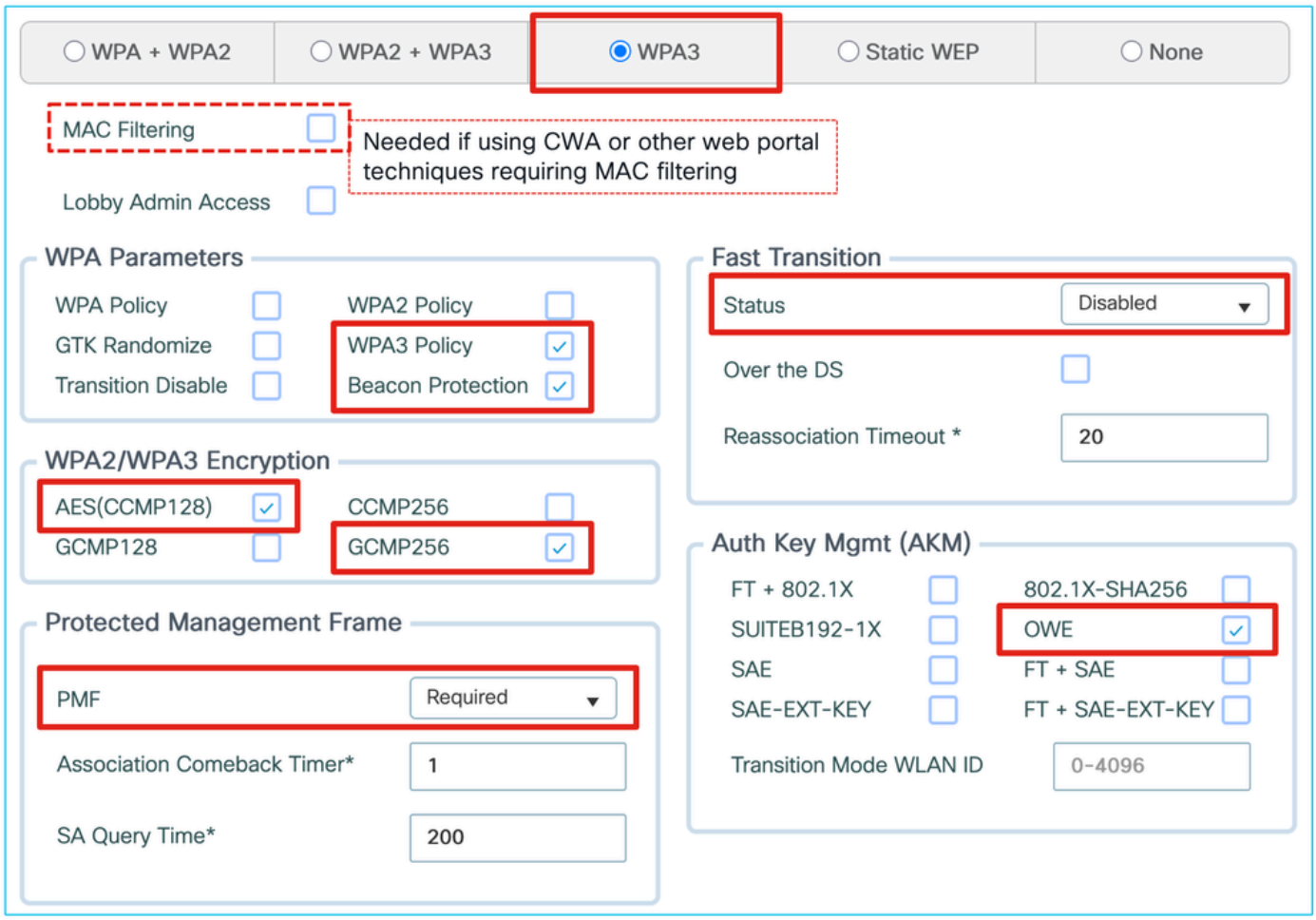
Reti aperte / migliorate aperte / OWE / guest

Le reti guest vengono fornite con molti gusti. In genere, non richiedono credenziali o passphrase 802.1X per la connessione e, probabilmente, implicano una pagina o un portale che può richiedere credenziali o un codice. Questo tipo di gestione viene in genere eseguita con un SSID aperto e con soluzioni di portale guest locali o esterne. Tuttavia, gli SSID con protezione aperta (senza crittografia) non sono consentiti su 6 GHz o per il supporto di Wi-Fi 7.

Un primo approccio molto conservativo sarebbe quello di dedicare le reti guest alla banda a 5 GHz e al Wi-Fi 6 nel migliore dei casi. In questo modo la banda a 6 GHz rimane riservata ai dispositivi aziendali, risolve il problema di complessità e offre la massima compatibilità, anche se non fino alle prestazioni Wi-Fi 6E/7.

Se volessimo fornire un servizio a 6 GHz agli ospiti, la raccomandazione sarebbe quella di creare un SSID separato con Enhanced Open / OWE (Opportunistic Wireless Encryption). Poteva offrire sia la cifratura AES(CCMP128), per la massima compatibilità fino ai client Wi-Fi 6E, sia i bit

GCMP256 per i client Wi-Fi 7.



Se da un lato Enhanced Open è un ottimo metodo di sicurezza che offre privacy mantenendo l'esperienza "aperta" (gli utenti finali non hanno bisogno di immettere credenziali o passphrase 802.1X), ancora oggi ha un supporto limitato tra gli endpoint. Alcuni client ancora non la supportano e, anche quando lo fanno, questa tecnica non è sempre gestita in modo fluido (il dispositivo può mostrare la connessione come non protetta, mentre in realtà è sicura, o può visualizzarla come passphrase protetta, anche se non è necessaria alcuna passphrase con OWE). Poiché si prevede che una rete guest funzioni su tutti i dispositivi guest non controllati, potrebbe essere troppo presto per fornire solo un Enhanced Open SSID e si consiglia di fornire entrambe le opzioni tramite SSID separati: uno aperto a 5 GHz e uno aperto a OWE a 5 e 6 GHz, entrambi con lo stesso portale in cattività, se necessario. La modalità Transizione non è supportata su Wi-Fi 6E, 6 GHz (anche se potrebbe essere consentita sul software) o Wi-Fi 7, quindi non è una soluzione consigliata. Tutte le tecniche di reindirizzamento del portale (autenticazione Web interna o esterna, autenticazione Web centrale e così via) sono ancora supportate in OWE.

WPA3 aggiuntivo e opzioni correlate

Mentre le opzioni WPA3 sono descritte e trattate in modo più approfondito nella guida all'installazione di WPA3, questa sezione fornisce alcuni consigli aggiuntivi per WPA3 relativi in modo specifico al supporto di 6 GHz e Wi-Fi 7.

Protezione beacon

Questa funzionalità consente di risolvere la vulnerabilità, in cui un utente malintenzionato può trasmettere i beacon anziché il punto di accesso legittimo, modificando alcuni campi per modificare la sicurezza o altre impostazioni dei client già associati. La protezione dei beacon è un elemento di informazione aggiuntivo nel beacon che funge da firma per il beacon stesso, per dimostrare che è stato inviato dal punto di accesso legittimo e che non è stato manomesso. Solo i client associati con una chiave di crittografia WPA3 possono verificare la legittimità del beacon. I client di prova non dispongono di alcun mezzo per verificarlo. L'elemento di informazioni aggiuntive nel beacon deve essere semplicemente ignorato dai client che non lo supportano (client non Wi-Fi 7) e in genere non rappresenta un problema di compatibilità (a meno che non si tratti di un driver client programmato in modo errato).

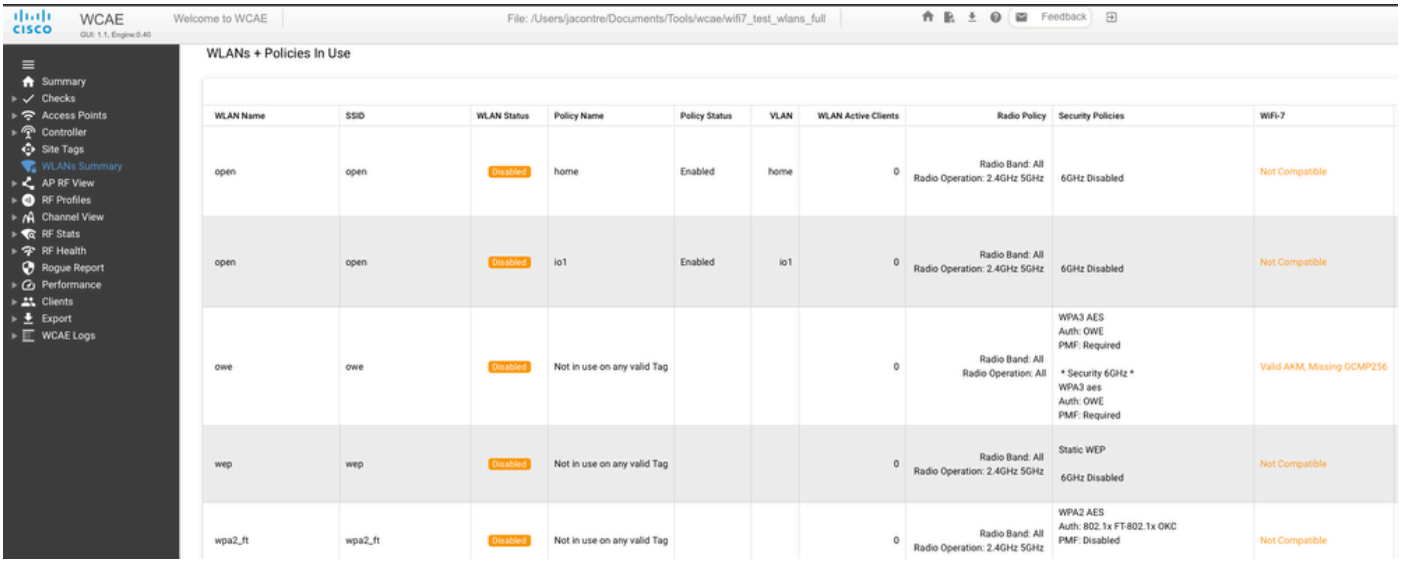
GCMP256

Fino alla certificazione Wi-Fi 7, la maggior parte dei client ha implementato la crittografia AES(CCMP128). CCMP256 e GCMP256 sono varianti molto specifiche relative a SUITE-B 802.1X AKM. Sebbene alcune prime generazioni di client Wi-Fi 7 sul mercato richiedano il supporto di Wi-Fi 7, è possibile che non implementino ancora la crittografia GCMP256, che può diventare un problema se i punti di accesso Wi-Fi 7 che applicano lo standard come previsto impediscono ai client di connettersi senza un supporto GCMP256 appropriato.

Risoluzione dei problemi e verifica

L'ultima versione di Wireless Configuration Analyzer Express (https://developer.cisco.com/docs/wireless-troubleshooting-tools/wireless-config-analyzer-express-gui/) dispone di un controllo di fattibilità Wi-Fi 7 che valuta la configurazione 9800 per tutti i requisiti Wi-Fi 7 sopra indicati.

Se si hanno ancora dubbi sul fatto che la configurazione sia predisposta per Wi-Fi 7, WCAE consente di sapere cosa è sbagliato.



Riferimenti

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).