Migration zu 6 GHz und Wi-Fi 7

Inhalt

Einleitung

Dieses Dokument beschreibt Design- und Konfigurationsrichtlinien zur Optimierung der Leistung von Wi-Fi 7 und zur optimalen Nutzung des 6-GHz-Spektrums.

Warum 6 GHz und Wi-Fi 7

6 GHz ist ein neues Frequenzband, das seit 2020 für den WLAN-Betrieb verfügbar ist und ursprünglich für die Wi-Fi 6E-Zertifizierung genutzt wurde. Auch wenn Wi-Fi 6E nach wie vor auf demselben 802.11ax-Standard beruht (zertifiziert nach Wi-Fi 6 für die 2,4/5 GHz-Bänder), kann es nur auf dem 6 GHz-Band betrieben werden, sofern bestimmte Anforderungen erfüllt werden.

Wi-Fi 7 entspricht der Zertifizierung des IEEE 802.11be-Standards und ist im Gegensatz zu Wi-Fi 6E, das nur auf 6 GHz beschränkt ist, für die Verwendung in allen drei Bändern definiert: 2,4, 5 und 6 GHz. Im Vergleich zu früheren Zertifizierungen bietet Wi-Fi 7 außerdem neue Funktionen.

6 GHz und/oder Wi-Fi 7 müssen spezifische Anforderungen erfüllen, was sich häufig in neuen Konfigurationen und RF-Designs niederschlägt, insbesondere im Vergleich zu den 2,4/5 GHz-Bändern und Wi-Fi 6. So verhindern z. B. die Verwendung von WEP-Sicherheit, dass 802.11-

Standards mit Ausnahme von 802.11a/b/g verwendet werden. Sicherheitsvoraussetzungen erfüllen, um die Einführung von sichereren Netzwerken voranzutreiben.

Auf der anderen Seite ermöglicht das neuere 6-GHz-Band in Verbindung mit modernen Zertifizierungen wie Wi-Fi 6E/7 eine bessere Nutzung von Frequenzen, bessere Leistung und neue Einsatzmöglichkeiten oder sogar eine problemlosere Implementierung bestehender Anwendungsfälle (z. B. Sprach-/Videokonferenzen).

Basisanforderungen für 6-GHz-Betrieb und Wi-Fi 7

Dies sind die Sicherheitsanforderungen, die in den Zertifizierungen für den Betrieb mit 6 GHz und Wi-Fi 7 festgeschrieben sind.

Anforderungen für das 6-GHz-Band

Das 6-GHz-Band kann nur WPA3 oder Enhanced Open WLANs zulassen, was eine der folgenden Sicherheitsoptionen bedeutet:

- WPA3-Enterprise mit 802.1X-Authentifizierung
- WPA3 Simultaneous Authentication of Equals (SAE) (alias WPA3-Personal) mit Passphrase. SAE-FT (SAE with Fast Transition) ist ein weiteres mögliches AKM und wird für die Verwendung empfohlen, da der SAE-Handshake nicht trivial ist und FT diesen längeren Austausch überspringen kann.
- Optimierte Offenheit durch Opportunistic Wireless Encryption (OWE)

Während gemäß den Spezifikationen von WPA3 v3.4 (Abschnitt 11.2) der Enhanced Open-Modus mit 6 GHz nicht unterstützt wird, wird dies von vielen Anbietern (einschließlich Cisco bis IOS® XE 17.18) noch nicht erzwungen. Aus diesem Grund ist es technisch möglich, z. B. eine Open SSID auf 5 GHz, eine entsprechende Enhanced Open SSID auf 5 und 6 GHz bei aktiviertem Transition Mode und all dem zu konfigurieren, ohne die Standardspezifikationen zu erfüllen. In einem solchen Szenario muss jedoch davon ausgegangen werden, dass wir eher eine Enhanced Open SSID ohne Übergangsmodus konfigurieren und nur auf 6 GHz verfügbar sind (Clients, die 6 GHz unterstützen, unterstützen normalerweise auch Enhanced Open), während wir unsere reguläre Open SSID auf 5 GHz halten, auch ohne Übergangsmodus.

Abgesehen von der Durchsetzung von 802.11w/Protected Management Frame (PMF) gibt es für WPA3-Enterprise keine neuen spezifischen Chiffren- oder Algorithmusanforderungen. Viele Anbieter, darunter Cisco, betrachten 802.1X-SHA256 oder "FT + 802.1X" (was tatsächlich 802.1X mit SHA256 und Fast Transition obendrauf ist) nur als WPA3-kompatibel und 802.1X (welches SHA1 verwendet) wird als Teil von WPA2 angesehen. 6 GHz nicht unterstützt.

Wi-Fi 7-Anforderungen

Mit der Wi-Fi 7-Zertifizierung des 802.11be-Standards hat die Wi-Fi Alliance die Sicherheitsanforderungen erhöht. Einige von ihnen ermöglichen die Verwendung der 802.11be-Datenraten und Protokollverbesserungen, während andere spezifisch für die Unterstützung von Multi-Link Operations (MLO) sind, sodass kompatible Geräte (Clients und/oder APs) mehrere

Frequenzbänder verwenden können, während die gleiche Zuordnung beibehalten wird.

Im Allgemeinen erfordert Wi-Fi 7 einen der folgenden Sicherheitstypen:

- WPA3-Enterprise mit AES(CCMP128) und 802.1X-SHA256 oder FT + 802.1X (die weiterhin SHA256 verwendet, auch wenn dies nicht explizit in ihrer Benennung angegeben ist). Dies stellt keine Änderung gegenüber den bisherigen WPA3-Sicherheitsvoraussetzungen für das 6-GHz-Band dar.
- WPA3-Personal mit GCMP256 und SAE-EXT-KEY und/oder FT + SAE-EXT-KEY (AKM 24 oder 25). Wi-Fi 6E erfordert WPA3 SAE und/oder FT + SAE nur mit regulärem AES (CCMP128) und keine zusätzlichen erweiterten Tastenbelegungen, daher ist dies eine neue Chiffre, die speziell für Wi-Fi 7 eingeführt wurde.
- Enhanced Open/OWE mit GCMP256. Während AES (CCMP128) immer noch auf derselben SSID konfiguriert werden kann, können Clients, die AES 128 verwenden, Wi-Fi 7 nicht unterstützen. Vor Wi-Fi 7 verwendeten die meisten Clients, die Enhanced Open unterstützen, nur AES 128. Dies ist eine neue, strengere Anforderung. Wie bei der 6-GHz-Unterstützung wird kein Übergangsmodus toleriert.

In allen diesen Fällen sind zur Unterstützung von Wi-Fi 7 im WLAN Protected Management Frames (PMF) und Beacon Protection erforderlich.

Wi-Fi 7 ist zum Zeitpunkt der Veröffentlichung dieses Dokuments noch relativ neu. Viele Anbieter haben diese Sicherheitsanforderungen jedoch nicht von Anfang an durchgesetzt, da die Technologie so früh wie möglich veröffentlicht wurde.

In letzter Zeit hat Cisco schrittweise die Konfigurationsoptionen durchgesetzt, um die Wi-Fi 7-Zertifizierung zu erfüllen. Hier sind die versionsspezifischen Verhaltensweisen:

17.18.1 und höher

In IOS XE 17.18 und höheren Versionen wird ein bestimmtes WLAN nur dann als Wi-Fi 7 aktiviert angekündigt, wenn das WLAN Sicherheitsparameter aufweist, die den Wi-Fi 7 Anforderungen entsprechen (Beacon Protection, PMF und das richtige AKM, wie zuvor beschrieben, je nach WLAN-Typ sowie Vorhandensein von GCMP256, um Wi-Fi 7 MLO zu erreichen, im Falle von OWE oder SAE-EXT). Das Vorhandensein von AES128 wird für die SSID toleriert, aber wenn es verwendet wird, wird es nur Wi-Fi 6E und nicht Wi-Fi 7 MLO liefern.

Ein Client kann eine Verbindung mit Wi-Fi 7 herstellen und Wi-Fi 7-Datenraten erzielen, unabhängig von der verwendeten Sicherheitsmethode (vorausgesetzt, diese wird weiterhin vom WLAN unterstützt). Der Client kann jedoch nur dann als MLO-fähig (auf einem oder mehreren Bändern) zuordnen, wenn er die strengen Anforderungen an die Wi-Fi 7-Sicherheit erfüllt oder andernfalls abgelehnt wird.

Versionen 17.15.3 und höher 17.15.x

In dieser Außenstelle werden alle WLANs als Wi-Fi 7-SSIDs übertragen, vorausgesetzt, Wi-Fi 7 ist global und unabhängig von den Sicherheitseinstellungen aktiviert.

Ein Client kann als Wi-Fi 7-fähig zugeordnet werden und Wi-Fi 7-Datenraten unabhängig von der verwendeten Sicherheitsmethode erzielen, sofern diese weiterhin vom WLAN unterstützt wird. Der Client kann jedoch nur als MLO-fähig (auf einem oder mehreren Bändern) assoziieren, wenn er die strengen Anforderungen an die Wi-Fi 7-Sicherheit erfüllt oder er abgelehnt wird.

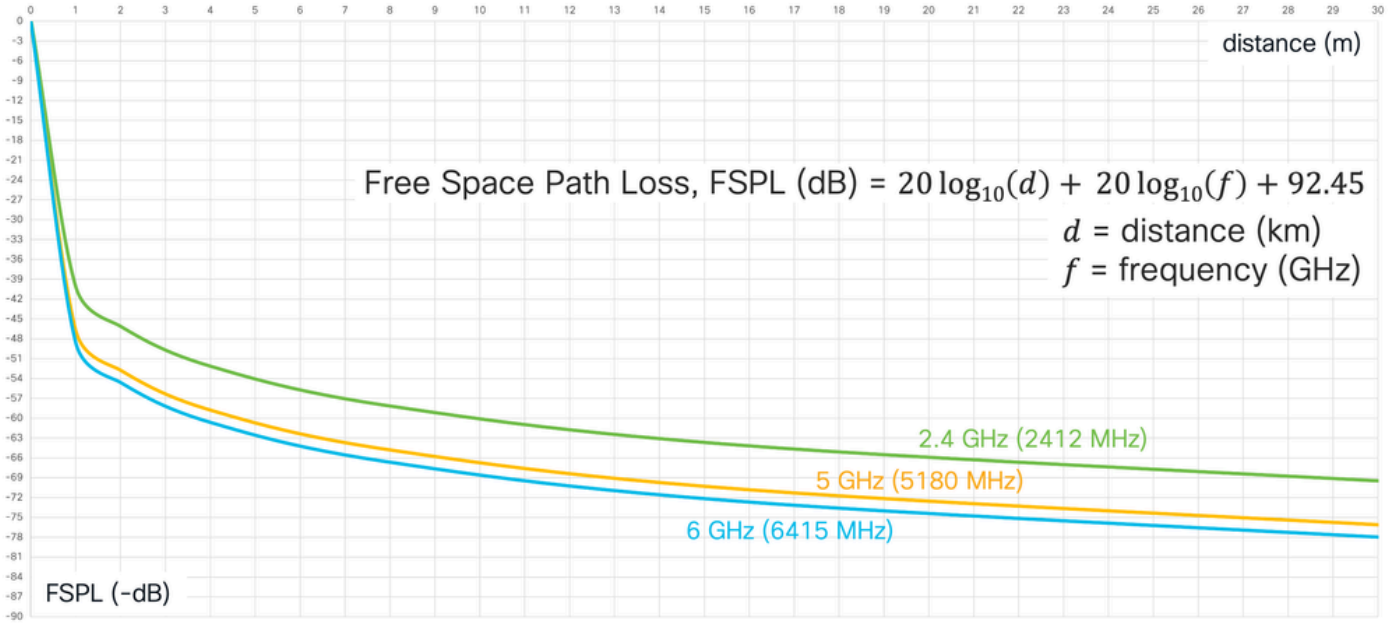
Dies kann zu Problemen führen, wenn ein früherer Wi-Fi 7-Client, der keine sichereren Chiffren wie GCMP256 unterstützen kann, versucht, eine Verbindung mit einem WLAN herzustellen, das als Wi-Fi 7 MLO-fähig ist und dessen Sicherheitseinstellungen nicht den Wi-Fi 7-Anforderungen entsprechen. In einer solchen Situation wird der Client aufgrund der ungültigen Sicherheitseinstellungen (die noch unter dem WLAN konfiguriert werden dürfen) abgelehnt.

Überlegungen zum Funkdesign für die 6-GHz-Abdeckung

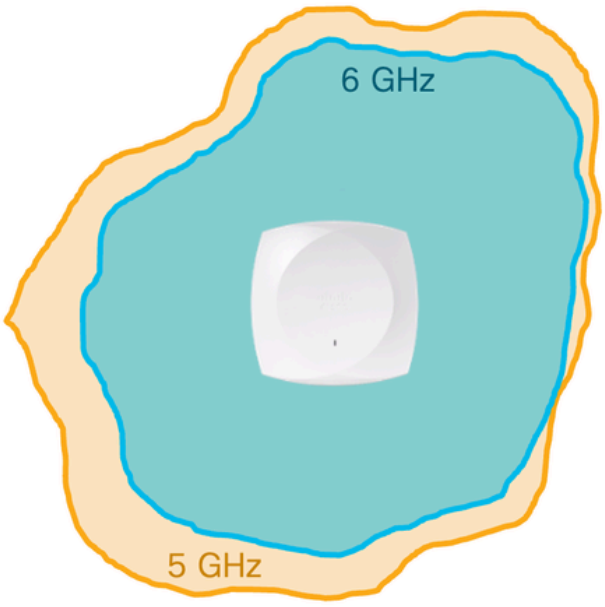
Ohne zu einem vollständigen Leitfaden für Standortuntersuchungen werden zu wollen, beschreibt dieser Abschnitt kurz einige Grundüberlegungen bei der Planung für eine 6-GHz-Abdeckung, insbesondere wenn es eine bereits vorhandene Installation für 2,4/5-GHz gibt, die wir zu Wi-Fi 6E oder 7 migrieren möchten.
Wie bei jeder neuen Wi-Fi-Bereitstellung, die wir auf 2,4 und/oder 5 GHz gewohnt waren, muss ein neues Wireless-Projekt auf 6 GHz auch eine entsprechende dedizierte 6 GHz-Standortuntersuchung umfassen.

Wenn Pre-Wi-Fi 6E/7 APs bereits für eine bestimmte 5 GHz-Abdeckung positioniert sind und benötigt werden, können wir in einigen Fällen davon ausgehen, dass wir sie durch Wi-Fi 6E/7-fähige APs ersetzen können und dennoch eine gute Abdeckung auch auf 6 GHz erhalten. Damit diese Theorie funktionieren kann, müssen unsere vorhandenen Access Points bereits die richtige 5-GHz-Abdeckung für die beabsichtigten Anforderungen bereitstellen (nur Daten, Sprache, bestimmte Anwendungen usw.), während sie bereits mindestens 3 bis 4 Übertragungsleistungspegel unter ihrem Höchstwert haben. APs haben in der Regel 7 bis 8 Leistungspegel, und jeder Leistungspegel teilt die Übertragungsleistung durch die Hälfte. Dies bedeutet, dass sich ein komfortabler Spot dann ergibt, wenn die Access Points das Medium ihres zulässigen Sendeleistungsbereichs verwenden.

Nach Berechnungen des freien Raumeinflusses werden 6-GHz-Signale um 2 dB mehr als 5 GHz-Signale gedämpft. Darüber hinaus können 6-GHz-Signale auch stärker von Hindernissen beeinflusst werden als ihre 5-GHz-Entsprechungen.



Wenn ein Cisco AP seine Sendeleistung um eine Ebene erhöht/verringert, erfolgt dies um einen "Sprung" von 3 dB. Ein Access Point, der von einem Leistungspegel von 4 mit einer Sendeleistung von beispielsweise 11 dBm auf einen Leistungspegel von 3 geht, erhöht seine Sendeleistung auf 14 dBm (11 dBm für den Leistungspegel von 4 und 14 dBm für den Leistungspegel von 3 sind nur ein generisches Beispiel, da verschiedene Modelle/Generationen von Access Points geringfügig unterschiedliche Sendeleistungswerte in dBm für den gleichen Leistungspegel haben könnten Nummer).



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.

Wenn beispielsweise ein Pre-Wi-Fi 6E/7 AP bereits eine gute Abdeckung bei 5 GHz auf Leistungsebene 4 bietet, könnte ein neuerer Wi-Fi 6E/7 AP mit ähnlichen 5 GHz Funkmustern diesen früheren AP ersetzen, ohne dass das bestehende 5 GHz Netzwerk erheblich beeinträchtigt würde.

Das 6-GHz-Funkmodul des neuen Wi-Fi 6E/7 AP könnte eine ähnliche 6-GHz-Abdeckung wie das 5-GHz-Funkmodul bieten, indem es nur eine Übertragungsleistung (also 3 dB) höher bereitstellt.

Wenn 5 GHz bereits korrekt mit dem 5-GHz-Funkmodul des AP abgedeckt ist, dessen maximale Leistung 3 bis 4 beträgt, könnte das entsprechende 6-GHz-Funkmodul daher für eine vergleichbare Abdeckung auf 2 bis 3 Leistungspegel unter seinem maximalen Wert eingestellt werden.

Wenn das 6-GHz-Funkmodul bereits eine korrekte Abdeckung bei 2-3 Leistungspegeln unterhalb seines Maximums bietet, kann es ausnahmsweise sogar ein paar Stufen höher liegen, um beispielsweise zeitweilig unerwartete Abdeckungslöcher zu umgehen (Ausfall eines benachbarten AP, unangekündigte Hindernisse, neue Funkanforderungen usw.).

Roaming-Verhalten zwischen APs vor Wi-Fi 6E/7 und Wi-Fi 6E/7

Die Implementierung von APs, die unterschiedliche Standards und/oder Frequenzbänder im gleichen Abdeckungsbereich unterstützen, ist seit jeher keine empfehlenswerte Vorgehensweise, insbesondere dann nicht, wenn diese unterschiedlichen Generationen von APs in einer "Salz-Pfeffer-Art" installiert werden (d. h. in derselben Zone miteinander vermischt werden).

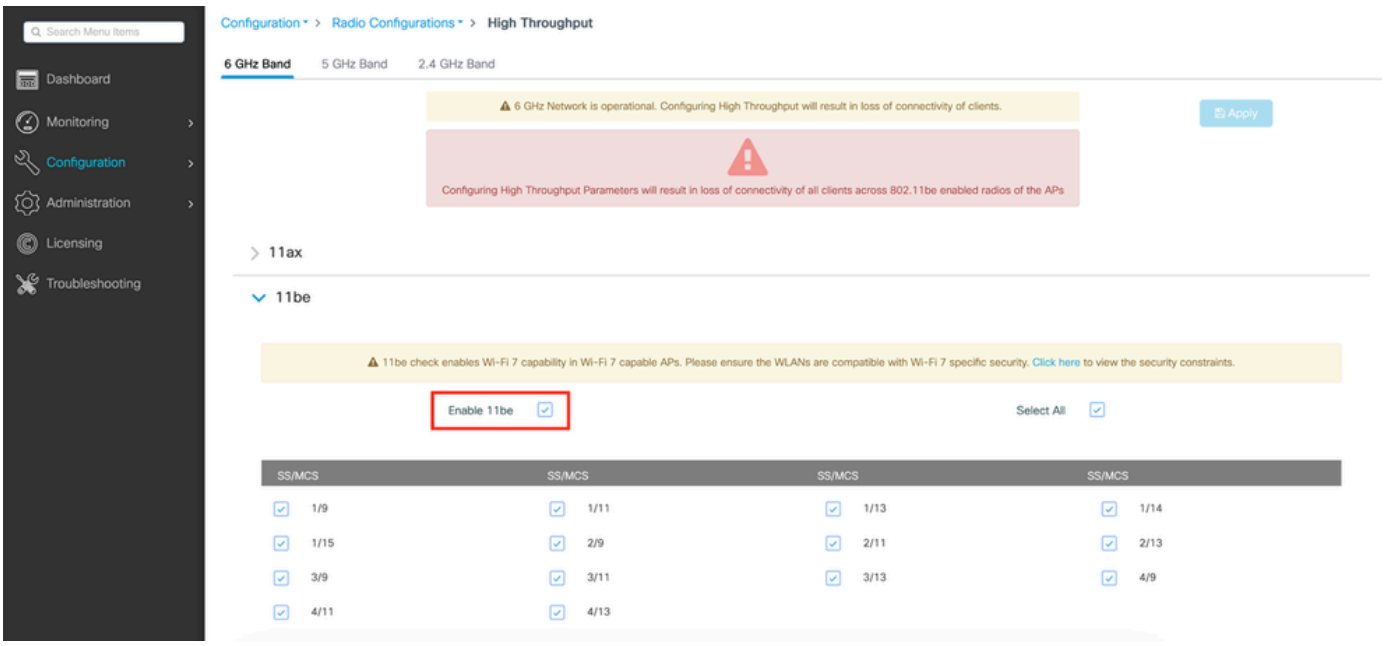
Während ein Wireless-Controller Vorgänge (z. B. dynamische Kanalzuweisung, Sendeleistungssteuerung, PMK-Cache-Verteilung usw.) von einer Gruppe verschiedener AP-Modelle aus verarbeiten könnte, können Clients, die zwischen verschiedenen Standards und sogar verschiedenen Frequenzbändern wechseln, dies nicht immer ordnungsgemäß verarbeiten, und sie könnten z. B. in Roaming-Probleme geraten.

Darüber hinaus unterstützen Wi-Fi 6E/7 APs aufgrund der neueren Standards GCMP256-Chiffren für WPA3. Dasselbe könnte jedoch nicht immer für einige Wi-Fi 6 APs und ältere Modelle gelten. Bei Passphrase/WPA3-Personal- und Enhanced Open/OWE-SSIDs, die die Konfiguration von AES-(CCMP128-) und GCMP256-Chiffren erfordern, unterstützen bestimmte Wi-Fi 6-Geräte (wie die Serien 9105, 9115 und 9120) GCMP256 nicht. und kann AES(CCMP128)-Chiffren nur für verknüpfende Clients anbieten, einschließlich Wi-Fi 6E/7-fähiger Clients. Wenn diese Wi-Fi 6E/7-Clients von/zu benachbarten Wi-Fi 6E/7-APs, die GCMP256 unterstützen, wechseln müssen, müssen sie eine ganz neue Verbindung durchlaufen, da die Neuverhandlung von Chiffren zwischen AES(CCMP128) und GCMP256 für transparentes Roaming nicht unterstützt wird. Darüber hinaus ist es im Allgemeinen nicht optimal, wenn einige APs neue Funktionen und andere APs im gleichen Bereich nicht dieselben Funktionen bieten: Es ermöglicht den Clients nicht, diese Funktionen sicher zu nutzen, während sie sich bewegen, und kann zu Stickyness oder Verbindungsunterbrechungen führen.
Obwohl dieses Szenario ein Eckfall sein muss, möchten wir dennoch bedenken, dass mit den im WLAN konfigurierten GCMP256-Chiffren das Roaming von Wi-Fi 6E/7-Clients zwischen 9105/9115/9120 APs und 9130/9124/916x/917x APs können nicht möglich sein, da letztere Serie unterstützt GCMP256 und erstere nicht.

Kanalbreiten von 40 MHz oder mehr auf 6 GHz können auch zu Anhaftungen für 6 GHz-fähige Clients führen, die sich weigern können, sich anderen Bändern erneut zuzuordnen. Dies muss ein weiterer Grund dafür sein, 6-GHz-fähige APs und nicht 6-GHz-fähige APs nicht im gleichen Roaming-Bereich zu mischen.

Globale Aktivierung von Wi-Fi 7

Bei der Installation oder dem Upgrade auf eine IOS XE-Version, die Wi-Fi 7 unterstützt, ist die Unterstützung für Wi-Fi 7 standardmäßig global deaktiviert.
Um sie zu aktivieren, müssen wir im Konfigurationsmenü für hohen Durchsatz jedes 2,4/5/6 GHz-Bands navigieren und das Kontrollkästchen markieren, um 11be zu aktivieren.



Eine weitere Möglichkeit besteht darin, diese drei Befehlszeilen über SSH/Konsole im Terminalkonfigurationsmodus auszuführen:

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

Wie im Warnhinweis erwähnt, führt die Änderung des Status der 802.11be-Unterstützung bei dem Versuch, diese Einstellungen zu ändern, zu einem kurzzeitigen Verbindungsverlust für alle Clients über Funkmodule von Wi-Fi 7 APs. Wenn Sie MLO ausführen möchten, d. h. Clients, die sich gleichzeitig mit mehreren Bändern verbinden, müssen Sie 11be auf allen Bändern aktivieren, mit denen der Client eine Verbindung herstellen soll. Es ist nicht notwendig, auf allen Bändern zu aktivieren, aber nur für die Leistung empfohlen.

Anwendungsfälle

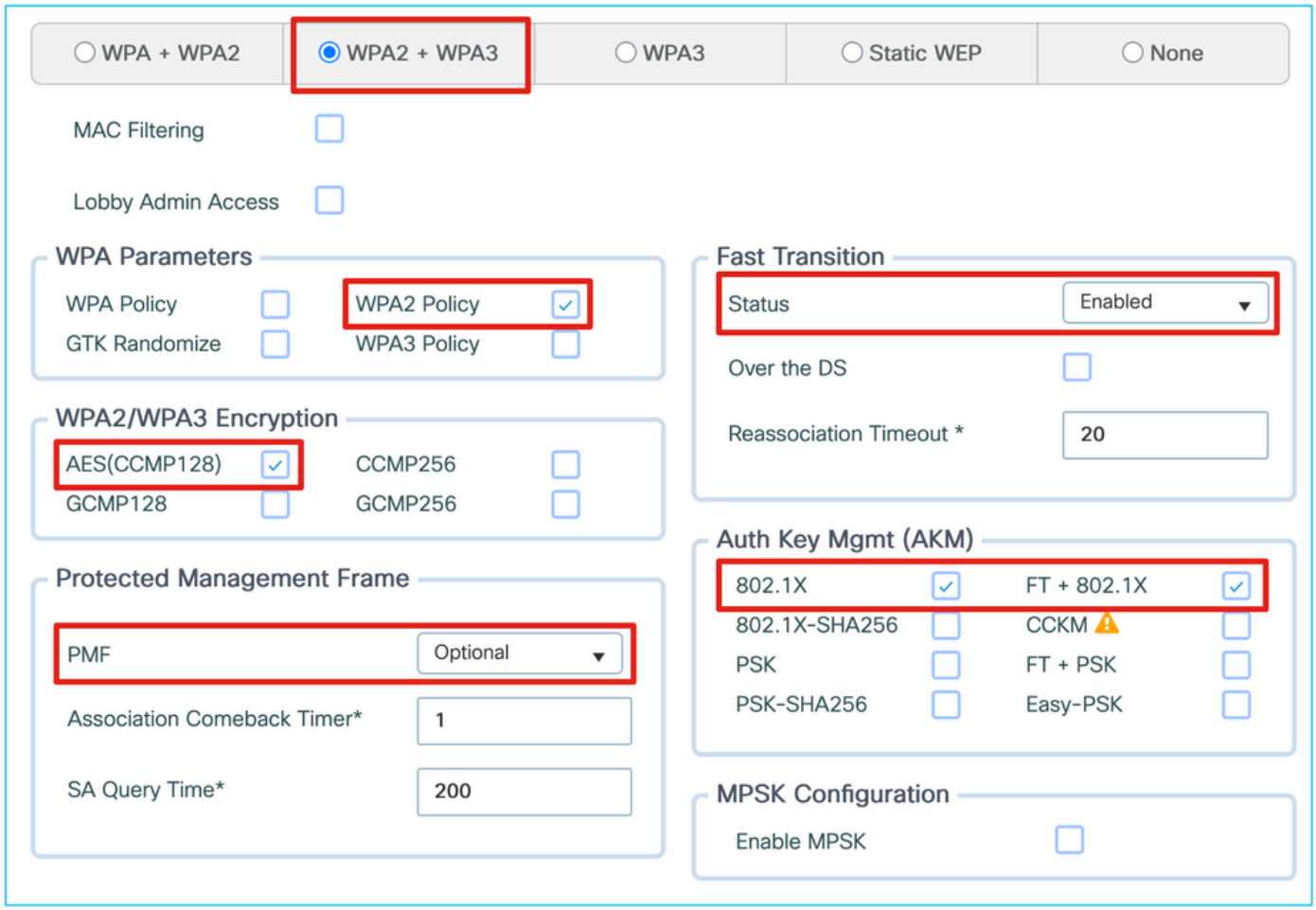
802.1X/WPA3-Enterprise-Netzwerke

WLANs der Enterprise-Klasse, die auf WPA2/3 mit 802.1X-Authentifizierung basieren, sind am einfachsten zu 6 GHz und/oder Wi-Fi 7 zu migrieren.

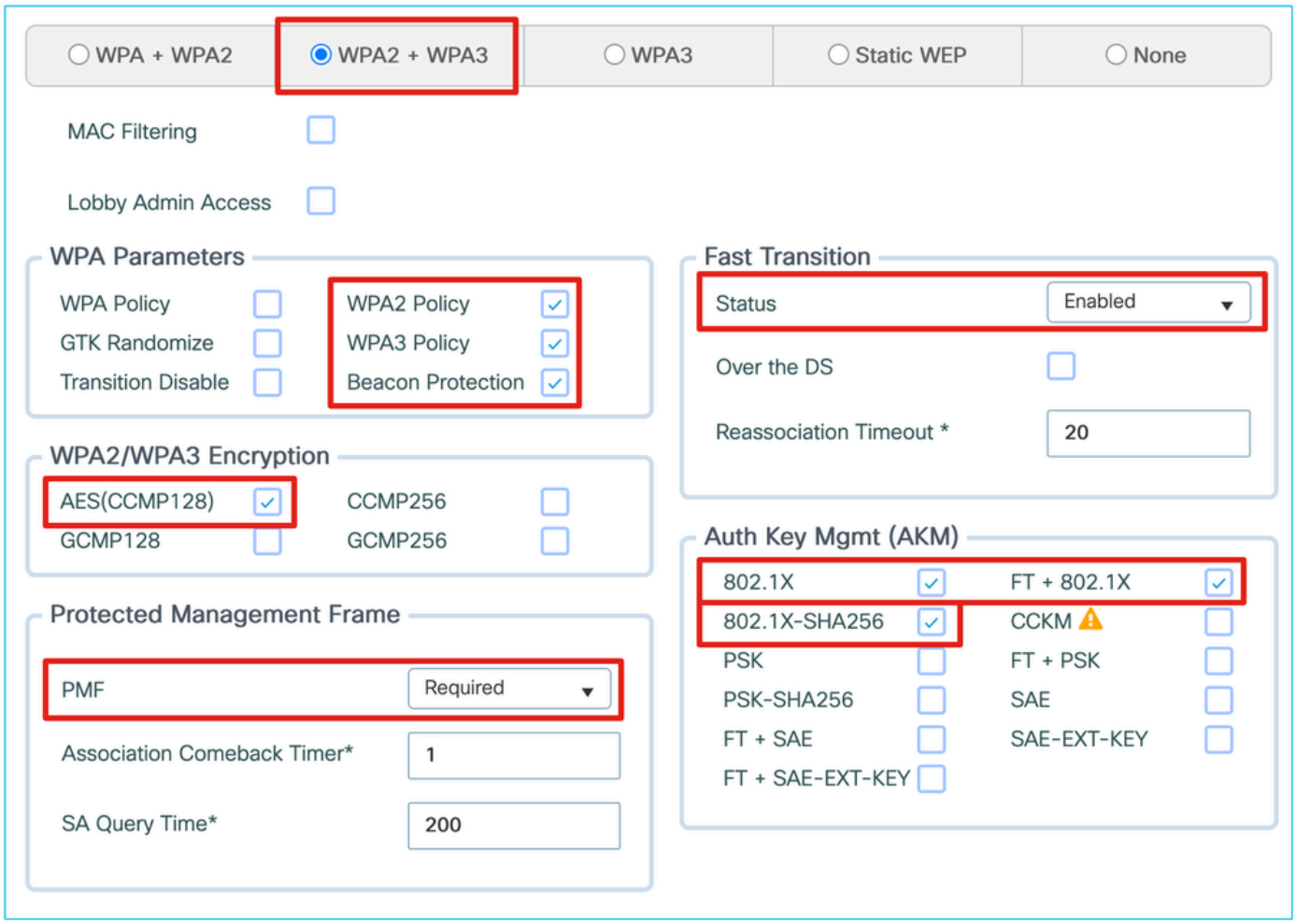
Die Aktivierung Ihrer 802.1X-SSID für 6 GHz erfordert lediglich die Aktivierung der PMF-Unterstützung (optional) sowie der 802.1X-SHA256- und/oder FT + 802.1X-AKMs, die beide WPA3-kompatibel sind.

WPA2 kann weiterhin mit dem Standard 802.1X (SHA1) im selben WLAN angeboten werden. Für die Wi-Fi 7-Unterstützung muss der Beacon-Schutz aktiviert und die PMF nicht optional, sondern nach Bedarf eingerichtet werden. WPA2 802.1X (SHA1) kann als Abwärtskompatibilitätsoption im WLAN beibehalten werden. Das bedeutet, dass alle Unternehmensgeräte unter einer einzigen SSID zusammengefasst werden können, vorausgesetzt, sie unterstützen 802.11w/PMF, was bei aktuellen Wireless-NICs für Laptops und andere mobile Endgeräte durchaus üblich ist.

Von einer typischen WPA2-SSID mit diesen L2-Sicherheitseinstellungen:



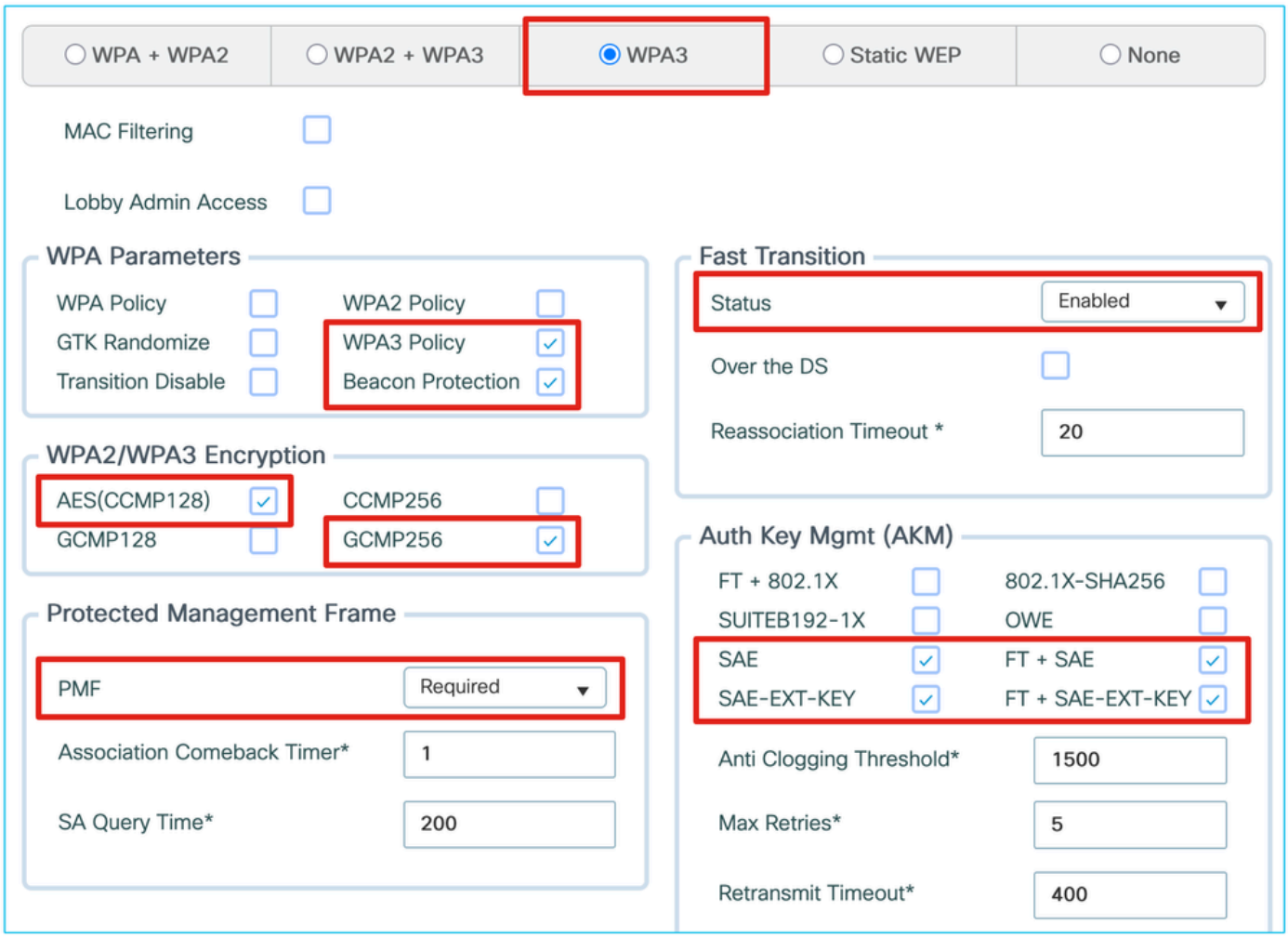
Wir können die Konfiguration für die Unterstützung von WPA3, 6 GHz und Wi-Fi 7 wie folgt migrieren:

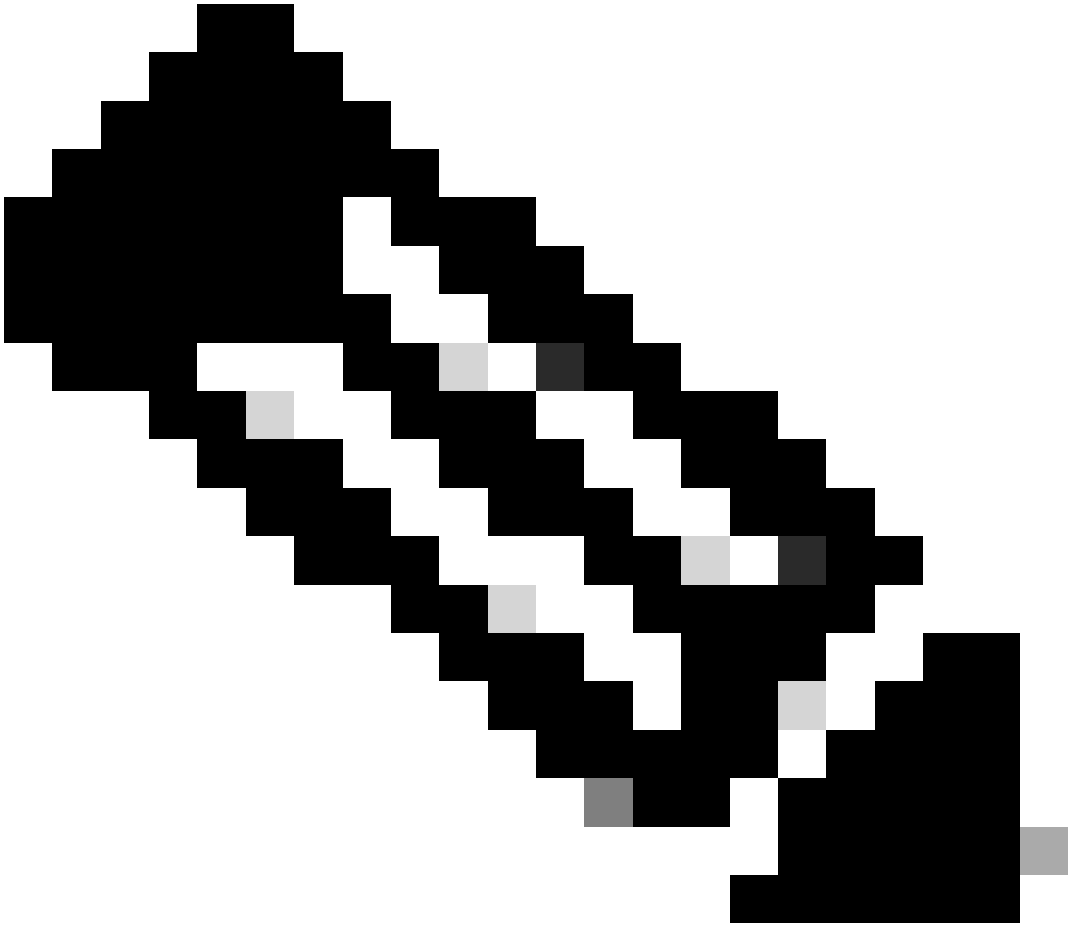


Passphrase/WPA3-Personal/IoT-Netzwerke

Die Aktivierung einer Passphrase-SSID für 6 GHz bis zur Wi-Fi 6E-Unterstützung ist einfach und erfordert SAE und/oder FT + SAE sowie ggf. weitere WPA2 PSK-AKMs. Für die Wi-Fi 7-Unterstützung muss die Zertifizierung jedoch alle WPA2 PSK-Optionen entfernen und SAE-EXT-KEY- und/oder FT + SAE-EXT-KEY-AKMs zusammen mit dem GCMP256-Chiffre hinzufügen. Es ist daher nicht möglich, ein WLAN mit Passphrase zu verwenden, das sowohl für ältere Clients maximale Kompatibilität als auch Wi-Fi 7-Leistung bietet.

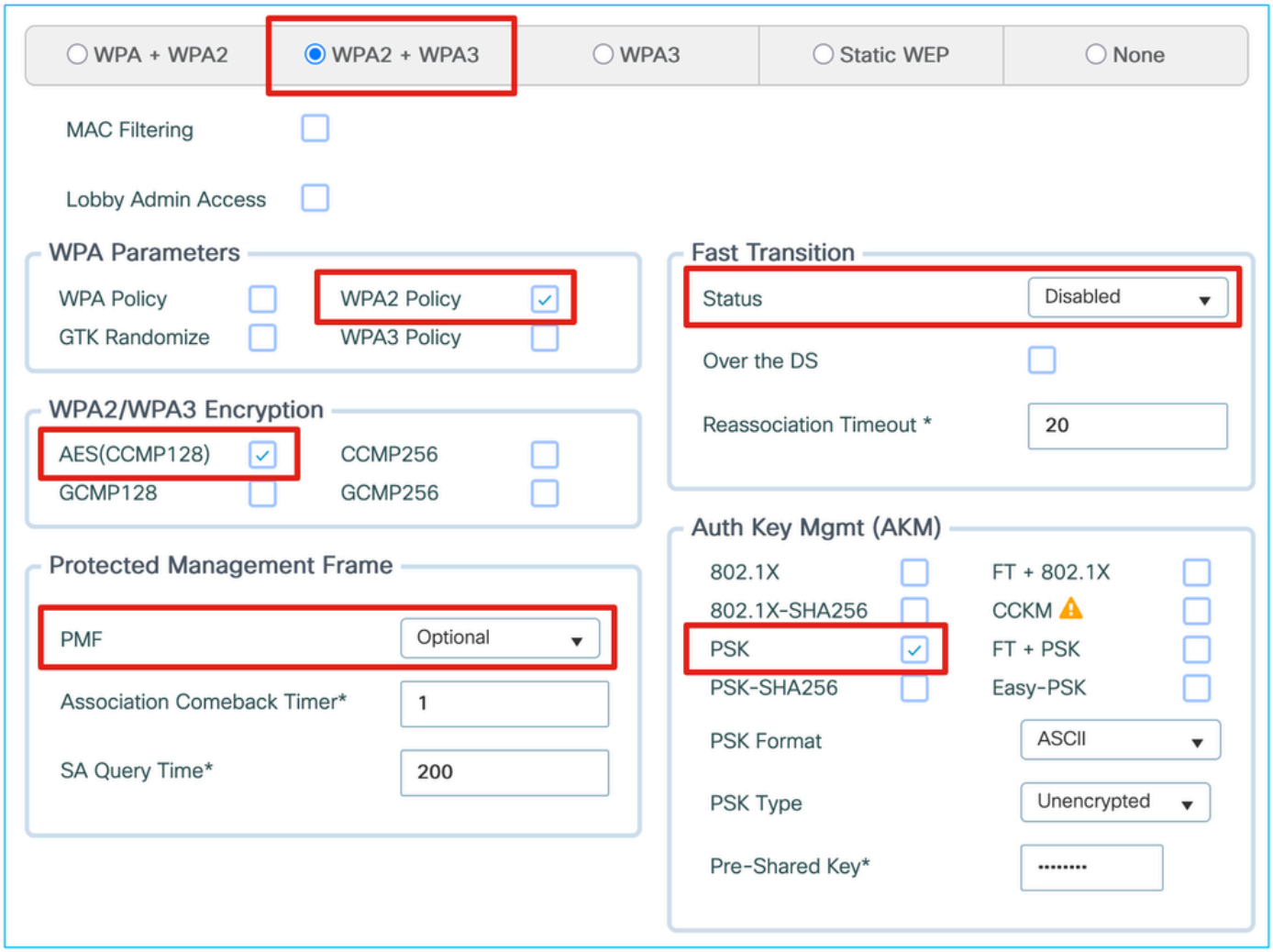
In solchen Fällen müssen wir eine dedizierte WPA3 Only-SSID mit SAE, FT + SAE, SAE-EXT-KEY und FT + SAE-EXT-KEY konfigurieren, die sowohl AES(CCMP128)- als auch GCMP256-Chiffren für neuere Wi-Fi 6E- und Wi-Fi 7-Clients bereitstellt.


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



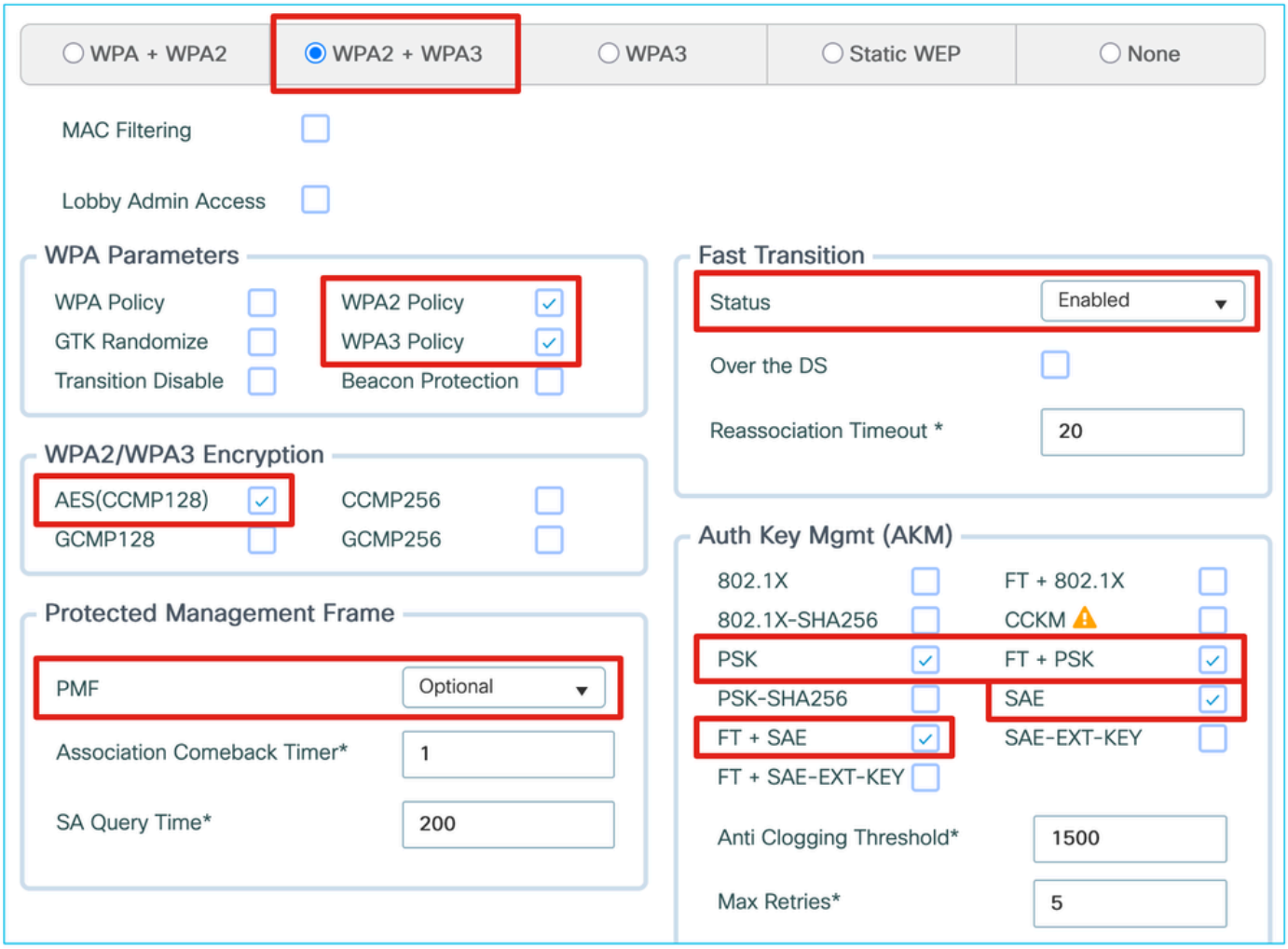
Anmerkung: Wenn (FT +) SAE im WLAN aktiviert ist und ein Wi-Fi 7-Client versucht, eine Verbindung mit ihm herzustellen, anstatt (FT +) SAE-EXT-KEY, wird er abgelehnt. Solange (FT +) SAE-EXT-KEY ebenfalls aktiviert ist, müssen Wi-Fi 7-Clients diesen AKM auf jeden Fall verwenden, und dieses Problem darf nicht auftreten.

Eine andere reguläre WPA2-SSID hingegen kann noch die verbleibenden Legacy-Clients unterstützen.



Diese Kombination erhöht zwar die Anzahl der SSIDs insgesamt, ermöglicht jedoch eine maximale Kompatibilität für eine SSID, wobei auch andere erweiterte Funktionen deaktiviert werden können, die die Kompatibilität beeinträchtigen könnten und die für viele IoT-Szenarien hilfreich sein könnten. Neueren Geräten werden über die andere SSID gleichzeitig maximale Funktionen und Leistungen geboten.
Eine weitere Option könnte natürlich sein, die Wi-Fi 7 SSID nicht anzubieten und nur eine einzige, die für WPA2 PSK und WPA3 SAE konfiguriert ist, beizubehalten. Die Idee dahinter könnte sein, dass IoT-Geräte ohnehin keine Wi-Fi 7-Leistung benötigen.

Dieser Ansatz würde trotzdem 6 GHz für Wi-Fi 6E und Wi-Fi 7 fähige Clients unterstützen, die bestenfalls mit Wi-Fi 6E Leistungen in Verbindung treten könnten.



In all diesen Szenarien wird dringend empfohlen, FT bei Verwendung von SAE zu aktivieren. Der SAE-Frame-Austausch ist ressourcenintensiv und länger als der 4-Wege-Handshake WPA2 PSK.

Einige Gerätehersteller wie Apple gehen davon aus, dass SAE nur verwendet wird, wenn FT aktiviert ist, und können sich weigern, eine Verbindung herzustellen, wenn sie nicht verfügbar ist.

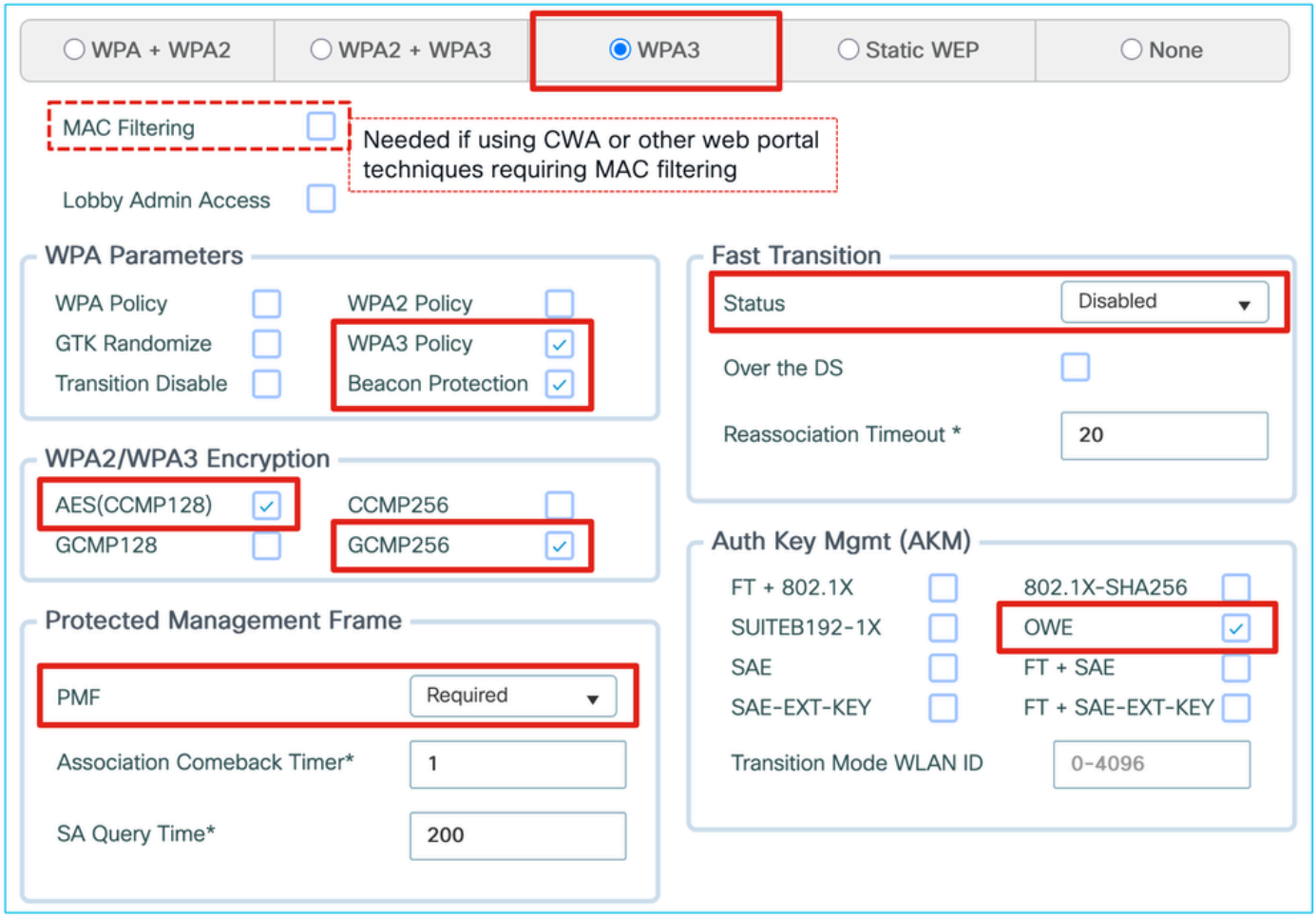
Offene/erweiterte offene/OWE/Gastnetzwerke

Gastnetzwerke bieten zahlreiche Vorteile. Normalerweise benötigen sie keine 802.1X-Anmeldeinformationen oder eine Passphrase für die Verbindung und implizieren möglicherweise eine Splash-Seite oder ein Portal, für die Anmeldeinformationen oder ein Code erforderlich sein können. Dies wird üblicherweise mit einer offenen SSID und einer lokalen oder externen Gastportal-Lösung umgesetzt. SSIDs mit offener Sicherheit (keine Verschlüsselung) sind jedoch für 6 GHz oder Wi-Fi 7 nicht zulässig.

Ein erster sehr konservativer Ansatz wäre, Gastnetzwerke bestenfalls dem 5-GHz-Band und Wi-Fi 6 zu widmen. Damit bleibt das 6 GHz-Band für Unternehmensgeräte reserviert, löst das Komplexitätsproblem und bringt maximale Kompatibilität, wenn auch nicht bis zu Wi-Fi 6E/7-Leistung.

Wenn wir den Gästen einen 6-GHz-Service bieten möchten, empfehlen wir die Erstellung einer separaten SSID mit Enhanced Open/OWE (Opportunistic Wireless Encryption). Es könnte sowohl

AES(CCMP128)-Chiffre bieten, für maximale Kompatibilität bis zu Wi-Fi 6E Clients, als auch GCMP256-Bits für Wi-Fi 7-fähige Clients.



Wenn Enhanced Open einerseits eine hervorragende Sicherheitsmethode ist, die Datenschutz bietet und gleichzeitig das "Open"-Erlebnis (Endbenutzer müssen keine 802.1X-Anmeldeinformationen oder Passphrase eingeben) beibehält, bietet es bis heute nur eingeschränkte Unterstützung unter den Endgeräten. Manche Clients unterstützen die Verbindung immer noch nicht, und selbst wenn sie dies tun, wird diese Technik nicht immer reibungslos gehandhabt (das Gerät kann die Verbindung als ungesichert anzeigen, während sie tatsächlich sicher ist, oder es kann sie als Passphrase geschützt anzeigen, auch wenn keine Passphrase mit OWE benötigt wird). Da erwartet wird, dass ein Gastnetzwerk auf allen nicht kontrollierten Gastgeräten funktioniert, kann es verfrüht sein, nur eine erweiterte offene SSID bereitzustellen. Es wird empfohlen, beide Optionen über separate SSIDs bereitzustellen: ein offenes 5-GHz-Portal und ein OWE-fähiges 5- und 6-GHz-Portal, sofern dies ebenfalls erforderlich ist. Der Übergangsmodus wird auf Wi-Fi 6E, 6 GHz (auch wenn dies mit Software möglich ist) oder Wi-Fi 7 nicht unterstützt. Daher wird davon abgeraten. Alle Techniken zur Portalumleitung (interne oder externe Webauthentifizierung, zentrale Webauthentifizierung usw.) werden von OWE weiterhin unterstützt.

Zusätzliche WPA3- und zugehörige Optionen

Obwohl die WPA3-Optionen am besten beschrieben und im WPA3-Bereitstellungsleitfaden

behandelt werden, enthält dieser Abschnitt einige zusätzliche Empfehlungen für WPA3, die sich speziell auf die Unterstützung von 6 GHz und Wi-Fi 7 beziehen.

Beacon-Schutz

Dies ist eine Funktion, die die Schwachstelle behebt, bei der ein böswilliger Angreifer Beacons anstelle des legitimen Access Points übertragen und gleichzeitig einige Felder ändern kann, um die Sicherheit oder andere Einstellungen bereits verbundener Clients zu ändern. Der Beacon-Schutz ist ein zusätzliches Informationselement im Beacon, das als Signatur für das Beacon selbst fungiert und nachweist, dass es vom legitimen Access Point gesendet wurde und nicht manipuliert wurde. Nur die zugehörigen Clients mit einem WPA3-Verschlüsselungsschlüssel können die Legitimität des Beacons überprüfen, die untersuchenden Clients haben keine Möglichkeit, dies zu überprüfen. Das zusätzliche Informationselement im Beacon muss einfach von Clients ignoriert werden, die es nicht unterstützen (Nicht-Wi-Fi 7 Clients) und stellt normalerweise kein Kompatibilitätsproblem dar (außer mit einem schlecht programmierten Client-Treiber).

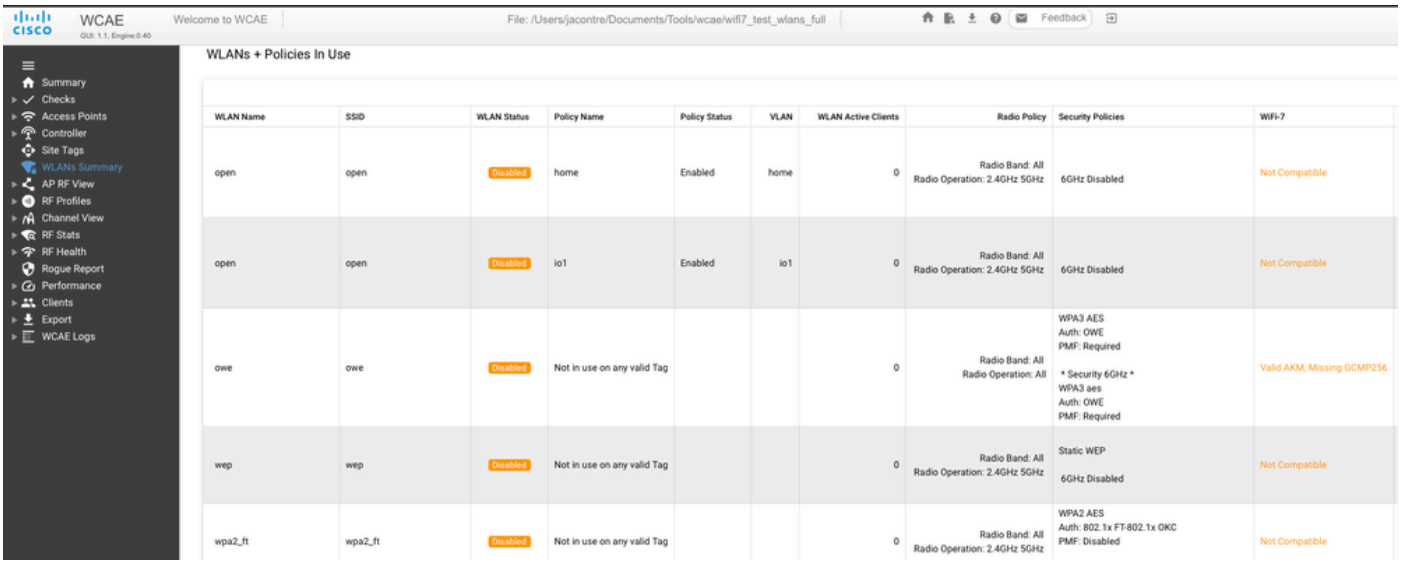
GMP 256

Bis zur Wi-Fi 7-Zertifizierung implementierten die meisten Clients AES (CCMP128)-Verschlüsselung. CCMP256 und GCMP256 sind sehr spezifische Varianten von SUITE-B 802.1X AKM. Obwohl einige der ersten Generationen von Wi-Fi 7 Clients auf dem Markt behaupten, Wi-Fi 7 zu unterstützen, implementieren sie möglicherweise immer noch keine GCMP256-Verschlüsselung, was zu einem Problem werden kann, wenn Wi-Fi 7 APs, die den Standard wie erwartet durchsetzen, verhindern, dass diese Clients eine Verbindung ohne ordnungsgemäße GCMP256-Unterstützung herstellen.

Fehlerbehebung und Verifizierung

Die neueste Version von Wireless Configuration Analyzer Express (https://developer.cisco.com/docs/wireless-troubleshooting-tools/wireless-config-analyzer-express-gui/) umfasst eine Überprüfung der Wi-Fi 7-Bereitschaft, mit der Ihre 9800-Konfiguration auf alle oben genannten Wi-Fi 7-Anforderungen hin ausgewertet wird.

Wenn Sie immer noch Zweifel haben, ob Ihre Konfiguration Wi-Fi 7-fähig ist, informieren Sie der WCAE darüber, was falsch ist.


WCAE
Welcome to WCAE
File: /Users/jacontre/Documents/Tools/wcae/wifi7_test_wlans_full
Feedback
Summary
Checks
Access Points
Controller
Site Tags
WLANs Summary
AP RF View
RF Profiles
Channel View
RF Stats
RF Health
Rogue Report
Performance
Clients
Export
WCAE Logs
WLANs + Policies In Use
WLAN Name | SSID | WLAN Status | Policy Name | Policy Status | VLAN | WLAN Active Clients | Radio Policy | Security Policies | WiFi-7
open | open | Disabled | home | Enabled | home | 0 | Radio Band: All Radio Operation: 2.4GHz 5GHz | 6GHz Disabled | Not Compatible
open | open | Disabled | io1 | Enabled | io1 | 0 | Radio Band: All Radio Operation: 2.4GHz 5GHz | 6GHz Disabled | Not Compatible
owe | owe | Disabled | Not in use on any valid Tag | | | 0 | Radio Band: All Radio Operation: All | WPA3 AES Auth: OWE PMF: Required * Security 6GHz * WPA3 aes Auth: OWE PMF: Required | Valid AKM, Missing GCMP256
wep | wep | Disabled | Not in use on any valid Tag | | | 0 | Radio Band: All Radio Operation: 2.4GHz 5GHz | Static WEP 6GHz Disabled | Not Compatible
wpa2_ft | wpa2_ft | Disabled | Not in use on any valid Tag | | | 0 | Radio Band: All Radio Operation: 2.4GHz 5GHz | WPA2 AES Auth: 802.1x FT-802.1x OKC PMF: Disabled | Not Compatible

Referenzen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.