Migreren naar 6 GHz en Wi-Fi 7

Inhoud

Inleiding

Dit document beschrijft ontwerp- en configuratierichtlijnen om de prestaties van Wi-Fi 7 te optimaliseren en het 6 GHz-spectrum volledig te benutten.

Waarom 6 GHz en Wi-Fi 7

6 GHz is een nieuwe band die in 2020 beschikbaar kwam voor WLAN-bewerkingen en aanvankelijk werd gebruikt door de Wi-Fi 6E-certificering. Hoewel Wi-Fi 6E nog steeds afhankelijk is van dezelfde 802.11ax-standaard (gecertificeerd onder Wi-Fi 6 voor de 2,4/5 GHz-banden), breidt deze zich uit om alleen op de 6 GHz-band te werken, mits aan specifieke vereisten wordt voldaan.

Wi-Fi 7 komt overeen met de certificering van de IEEE 802.11be-standaard en is, in tegenstelling tot Wi-Fi 6E dat alleen beperkt is tot 6 GHz, gedefinieerd voor gebruik in alle drie de banden: 2,4, 5 en 6 GHz. Wi-Fi 7 heeft ook nieuwe functies in vergelijking met eerdere certificeringen.

6 GHz en / of Wi-Fi 7 hebben specifieke vereisten die moeten worden ondersteund, wat zich vaak vertaalt in nieuwe configuraties en RF-ontwerpen, vooral in vergelijking met wat we tot de 2,4/5

GHz-banden en Wi-Fi 6 werden gebruikt. Net zoals het gebruik van WEP-beveiliging ons ervan weerhoudt om andere 802.11-standaarden dan 802.11a/b/g te gebruiken, worden nieuwere standaarden geleverd met hogere beveiligingsvereisten om de acceptatie van veiligere netwerken te stimuleren.

Aan de andere kant ontsluit de recentere 6 GHz-band, in combinatie met dergelijke moderne certificeringen zoals Wi-Fi 6E/7, schonere frequenties, betere prestaties en nieuwe toepassingen, of zelfs een meer "zorgeloze" implementatie van bestaande use cases (bijvoorbeeld spraak / video conferencing).

Basisvereisten voor 6 GHz-bewerkingen en Wi-Fi 7

Dit zijn de beveiligingseisen die zijn vastgelegd in de certificeringen voor 6 GHz- en Wi-Fi 7-bewerkingen.

Vereisten voor de 6 GHz-band

De 6 GHz-band kan alleen WPA3 of Enhanced Open WLAN's toestaan, wat betekent dat een van deze beveiligingsopties:

- WPA3-Enterprise met 802.1X-verificatie
- WPA3 Simultaneous Authentication of Equals (SAE) (ook bekend als WPA3-Personal) met wachtwoordgroep. SAE-FT (SAE met Fast Transition) is een andere mogelijke AKM en wordt eigenlijk aanbevolen voor gebruik omdat de SAE-handshake niet triviaal is en FT die langere uitwisseling kan overslaan.
- Verbeterde open verbinding met opportunistische draadloze codering (OWE)

Hoewel volgens de WPA3 v3.4-specificaties (sectie 11.2) de Enhanced Open-overgangsmodus niet wordt ondersteund met 6 GHz, wordt dat door veel leveranciers (waaronder Cisco tot IOS® XE 17.18) nog niet afgedwongen. Daarom is het technisch mogelijk om bijvoorbeeld een Open SSID op 5 GHz te configureren, een bijbehorende Enhanced Open SSID op 5 en 6 GHz, beide met Transition Mode ingeschakeld en dit alles zonder te voldoen aan de standaards specificaties. In een dergelijk scenario moet echter worden verwacht dat we eerder een Enhanced Open SSID configureren zonder overgangsmodus en alleen beschikbaar op 6 GHz (clients die 6 GHz ondersteunen, ondersteunen meestal ook Enhanced Open), terwijl onze reguliere Open SSID op 5 GHz blijft, ook zonder overgangsmodus.

Er zijn geen nieuwe specifieke coderingen of algoritmevereisten voor WPA3-Enterprise, met uitzondering van 802.11w/Protected Management Frame (PMF)-handhaving. Veel leveranciers, waaronder Cisco, beschouwen 802.1X-SHA256 of "FT + 802.1X" (dat eigenlijk 802.1X is met SHA256 en Fast Transition bovenaan) alleen als WPA3-compatibel en gewoon 802.1X (dat SHA1 gebruikt) wordt beschouwd als onderdeel van WPA2, daarom niet geschikt / ondersteund voor 6 GHz.

Vereisten voor Wi-Fi 7

Met de Wi-Fi 7-certificering van de 802.11be-standaard heeft de Wi-Fi Alliance de

beveiligingsvereisten verhoogd. Sommige van hen maken het mogelijk om de 802.11be-gegevenssnelheden en protocolverbeteringen te gebruiken, terwijl andere specifiek zijn voor het ondersteunen van Multi-Link Operations (MLO), waardoor compatibele apparaten (clients en / of AP's) meerdere frequentiebanden kunnen gebruiken met behoud van dezelfde associatie.

Over het algemeen vereist Wi-Fi 7 een van deze beveiligingstypen:

- WPA3-Enterprise met AES(CCMP128) en 802.1X-SHA256 of FT + 802.1X (waarbij nog steeds SHA256 wordt gebruikt, zelfs als dit niet expliciet in de naamgeving is). Dit is geen wijziging ten opzichte van de eerder bestaande WPA3-beveiligingsvereisten voor de 6 GHz-band.
- WPA3-Personal met GCMP256 en SAE-EXT-KEY en/of FT + SAE-EXT-KEY (AKM 24 of 25). Wi-Fi 6E verplicht WPA3 SAE en / of FT + SAE alleen met gewone AES (CCMP128) en geen extra uitgebreide sleutel gebruiken, dus dit is een nieuw cijfer speciaal geïntroduceerd voor Wi-Fi 7.
- Verbeterde Open / OWE met GCMP256. Hoewel AES(CCMP128) nog steeds op dezelfde SSID kan worden geconfigureerd, kunnen clients met AES 128 Wi-Fi 7 niet ondersteunen. Vóór Wi-Fi 7 gebruikten de meeste clients die Enhanced Open ondersteunden alleen AES 128, dus dit is een nieuwe sterkere vereiste. Wat betreft 6 GHz-ondersteuning, wordt geen overgangsmodus getolereerd.

In al deze gevallen zijn ook Protected Management Frames (PMF) en Beacon Protection vereist om Wi-Fi 7 op het WLAN te ondersteunen.

Omdat Wi-Fi 7 nog recent was op het moment van schrijven, met een zo vroeg mogelijke release, hebben veel leveranciers al deze beveiligingsvereisten niet vanaf het begin afgedwongen.

Meer recentelijk heeft Cisco de configuratieopties geleidelijk afgedwongen om te voldoen aan de Wi-Fi 7-certificering. Hier zijn de versie-specifieke gedragingen:

17.18.1 en later

IOS XE 17.18 en latere versie adverteert alleen een bepaald WLAN als Wi-Fi 7 ingeschakeld als het WLAN beveiligingsparameters heeft die overeenkomen met Wi-Fi 7-vereisten (bakenbescherming, PMF en de juiste AKM zoals eerder beschreven, afhankelijk van het WLAN-type en de aanwezigheid van GCMP256 om Wi-Fi 7 MLO te bereiken, in het geval van OWE of SAE-EXT). Aanwezigheid van AES128 wordt getolereerd op de SSID, maar bij gebruik levert het alleen Wi-Fi 6E en niet Wi-Fi 7 MLO.

Een client kan koppelen als Wi-Fi 7 en Wi-Fi 7-gegevenssnelheden bereiken, ongeacht de beveiligingsmethode die wordt gebruikt (op voorwaarde dat deze nog steeds wordt ondersteund door het WLAN). De klant kan echter alleen associëren als MLO-geschikt (op een of meer banden) als deze voldoet aan de strenge eisen voor Wi-Fi 7-beveiliging, of anders wordt afgewezen.

17.15.3 en hoger 17.15.x-versies

In deze tak worden alle WLAN's uitgezonden als Wi-Fi 7 SSID's, op voorwaarde dat Wi-Fi 7

wereldwijd is ingeschakeld en ongeacht de beveiligingsinstellingen.

Een client kan koppelen als Wi-Fi 7-compatibel en Wi-Fi 7-gegevenssnelheden bereiken, ongeacht de beveiligingsmethode die wordt gebruikt, op voorwaarde dat deze nog steeds wordt ondersteund door het WLAN. De klant kan echter alleen associëren als MLO-geschikt (op een of meer banden) als deze voldoet aan de strikte vereisten voor Wi-Fi 7-beveiliging, of anders wordt deze afgewezen.

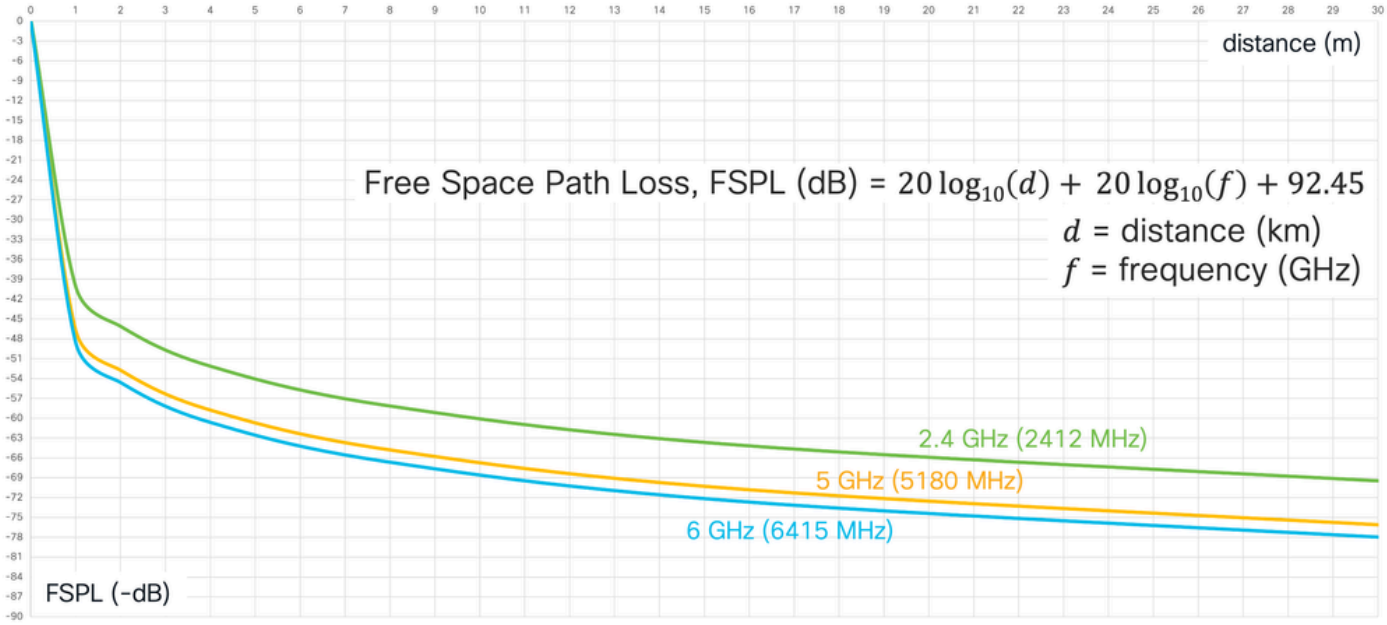
Dit kan mogelijk problemen veroorzaken, wanneer een vroege Wi-Fi 7-client die geen veiligere coderingen zoals GCMP256 kan ondersteunen, probeert te koppelen als Wi-Fi 7 MLO geschikt voor een WLAN, waarvan de beveiligingsinstellingen niet overeenkomen met de Wi-Fi 7-vereisten. In een dergelijke situatie wordt de client afgewezen vanwege de ongeldige beveiligingsinstellingen (die nog steeds mogen worden geconfigureerd onder het WLAN).

Overwegingen met betrekking tot radioontwerp voor 6 GHz-dekking

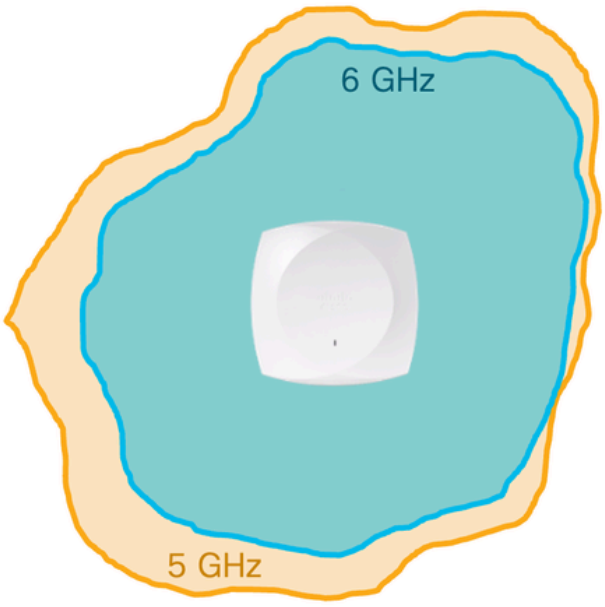
Zonder dat het de bedoeling is om een volledige prescriptieve gids voor enquêtes ter plaatse te worden, beschrijft dit gedeelte kort enkele basisoverwegingen bij het ontwerpen voor 6 GHz-dekking, vooral als er een reeds bestaande installatie voor 2,4/5 GHz is die we willen migreren naar Wi-Fi 6E of 7.
Zoals voor elke nieuwe Wi-Fi-implementatie die we gewend waren op 2,4 en / of 5 GHz, moet een nieuw draadloos project op 6 GHz ook een bijbehorende speciale 6 GHz-site-enquête bevatten.

Wanneer pre-Wi-Fi 6E/7 AP's al zijn gepositioneerd voor specifieke 5 GHz-dekking en -behoeften, kunnen we in sommige gevallen verwachten dat we ze kunnen vervangen door Wi-Fi 6E/7-compatibele AP's en nog steeds een goede dekking op 6 GHz krijgen ook. Om deze theorie te laten werken, moeten onze bestaande AP's al een juiste 5 GHz-dekking bieden voor de beoogde behoeften (alleen gegevens, spraak, specifieke toepassingen, enzovoort) terwijl ze al minstens 3-4 zendvermogensniveaus onder hun maximale limiet hebben. AP's hebben meestal 7 tot 8 energieniveaus en elk energieniveau verdeelt het zendvermogen met de helft. Dit betekent dat een comfortabele plek is wanneer AP's het medium van hun toegestane zendvermogensbereik gebruiken.

Volgens berekeningen van het verlies van vrije ruimte worden 6 GHz-signalen verzwakt door 2 dB meer dan 5 GHz-signalen. Bovendien kunnen 6 GHz-signalen ook meer worden beïnvloed door obstakels dan hun 5 GHz-equivalenten.



Wanneer een Cisco-toegangspunt het zendvermogen met één niveau verhoogt/verlaagt, gebeurt dit met een "sprong" van 3 dB. Een toegangspunt dat van een vermogensniveau van 4 gaat, met een zendvermogen van 11 dBm bijvoorbeeld, tot een vermogensniveau van 3, verhoogt het zendvermogen tot 14 dBm (11 dBm voor vermogensniveau 4 en 14 dBm voor vermogensniveau 3 zijn slechts een algemeen voorbeeld, omdat verschillende modellen/generaties toegangspunten enigszins verschillende zendvermogenswaarden in dBm kunnen hebben voor hetzelfde vermogensniveau).



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.

Als een pre-Wi-Fi 6E/7 AP al een goede dekking biedt op 5 GHz op energieniveau 4, bijvoorbeeld, kan een nieuwer Wi-Fi 6E/7 AP met vergelijkbare 5 GHz-radiopatronen dat voormalige AP vervangen zonder enige significante impact op het bestaande 5 GHz-netwerk.

Ook zou de 6 GHz-radio van de nieuwe Wi-Fi 6E / 7 AP een vergelijkbare 6 GHz-dekking kunnen bieden als de 5 GHz-radio door slechts één zendvermogensniveau (dus 3 dB) hoger te zijn.

Als 5 GHz al correct is afgedekt met de 5 GHz-radio van het toegangspunt bij 3-4 vermogensniveaus onder het maximum, kan de corresponderende 6 GHz-radio dus worden ingesteld op 2-3 vermogensniveaus onder het maximum voor vergelijkbare dekking.

Ook als de 6 GHz-radio al de juiste dekking biedt bij 2-3 vermogensniveaus lager dan het maximum, kan deze nog steeds uitzonderlijk een paar niveaus hoger gaan, bijvoorbeeld om te proberen rond tijdelijke onverwachte dekkingsgaten te werken (het falen van een naburige AP, onaangekondigde obstakels, nieuwe RF-behoeften enzovoort).

Roaminggedrag tussen pre-Wi-Fi 6E/7 en Wi-Fi 6E/7 AP's

Het gebruik van toegangspunten die verschillende standaarden en/of frequentiebanden in hetzelfde dekkingsgebied ondersteunen, is altijd niet aanbevolen, vooral niet als die verschillende generaties toegangspunten op een "zout-en-peper"-manier worden geïnstalleerd (die in dezelfde zone met elkaar wordt gemengd).

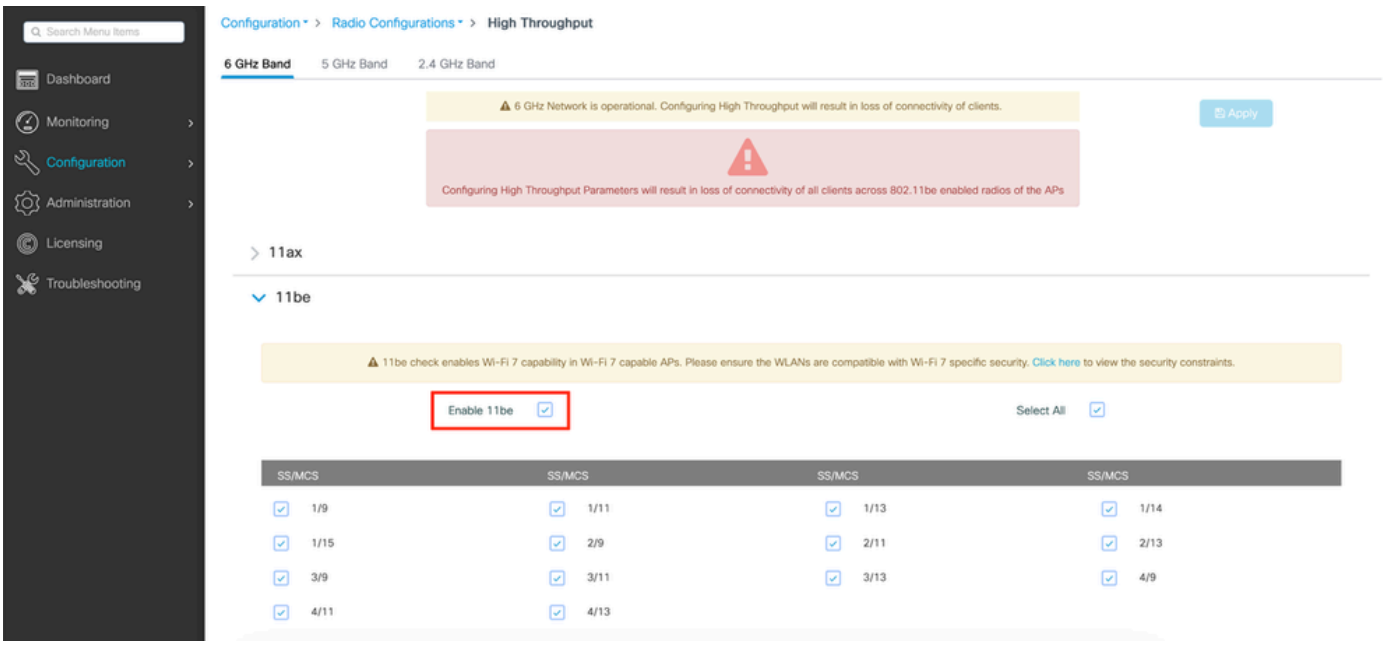
Hoewel een draadloze controller bewerkingen (bijvoorbeeld dynamische kanaaltoewijzing, transmissievermogensregeling, PMK-cachedistributie, enzovoort) van een groep van verschillende AP-modellen kan verwerken, kunnen clients die tussen verschillende standaarden en zelfs verschillende frequentiebanden bewegen, dat niet altijd goed afhandelen en kunnen ze waarschijnlijk bijvoorbeeld roamingproblemen tegenkomen.

Bovendien ondersteunen Wi-Fi 6E/7 AP's vanwege de nieuwere standaarden GCMP256-cijfers voor WPA3. Hetzelfde kan echter niet altijd waar zijn voor sommige Wi-Fi 6-toegangspunten en eerdere modellen. Voor wachtwoordgroep/WPA3-Personal en Enhanced Open/OWE SSID's, waarvoor de configuratie van zowel AES(CCMP128)- als GCMP256-coderingen vereist is, ondersteunen bepaalde Wi-Fi 6-coderingen (zoals de 9105-, 9115- en 9120-reeks) GCMP256 niet en kunnen deze alleen AES(CCMP128)-coderingen bieden aan gekoppelde clients, waaronder Wi-Fi 6E/7-compatibele clients. Als deze Wi-Fi 6E/7-clients van/naar naburige Wi-Fi 6E/7 AP's met GCMP256 moesten zwerven, zouden ze een gloednieuwe associatie moeten doorlopen, omdat het opnieuw onderhandelen van cijfers tussen AES(CCMP128) en GCMP256 niet wordt ondersteund voor transparante roaming. Bovendien is het over het algemeen niet optimaal om sommige toegangspunten nieuwe mogelijkheden te bieden en andere toegangspunten in hetzelfde gebied die niet dezelfde mogelijkheden bieden: het staat de klanten niet toe om deze mogelijkheden veilig te gebruiken tijdens het verplaatsen en kan leiden tot kleverigheid of verbroken verbindingen.
Hoewel dit scenario een hoekscenario moet vertegenwoordigen, willen we er toch rekening mee houden dat roaming van Wi-Fi 6E/7-clients tussen 9105/9115/9120 AP's en 9130/9124/916x/917x AP's niet mogelijk is met GCMP256-coderingen die zijn geconfigureerd in het kader van het WLAN, omdat deze laatste reeks GCMP256 ondersteunt en de eerste niet.

Kanaalbreedtes van 40 MHz of meer op 6 GHz kunnen ook plakkerigheid veroorzaken voor 6 GHz-compatibele clients, die kunnen weigeren opnieuw te koppelen aan andere banden. Dit moet nog een reden zijn om AP's die geschikt zijn voor 6 GHz en AP's die niet geschikt zijn voor 6 GHz niet in hetzelfde roaminggebied te combineren.

Wi-Fi 7 wereldwijd mogelijk maken

Bij het installeren of upgraden naar een IOS XE-versie die Wi-Fi 7 ondersteunt, is standaard ondersteuning voor Wi-Fi 7 wereldwijd uitgeschakeld.
Om het te activeren, moeten we navigeren onder het configuratiemenu High Throughput van elke 2,4/5/6 GHz-band en het selectievakje aanvinken om 11be in te schakelen.



Een andere optie zou ook kunnen zijn om deze drie opdrachtregels via SSH / console uit te voeren, in de terminalconfiguratiemodus:

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

Zoals vermeld in de waarschuwingsnotitie, resulteert het wijzigen van de status van 802.11be-ondersteuning bij het wijzigen van deze instellingen in een kort verlies van connectiviteit voor alle clients via radio's van Wi-Fi 7-toegangspunten. Als u MLO wilt doen, wat betekent dat clients verbinding maken met meerdere banden tegelijk, moet u 11be inschakelen op alle banden waarmee de client verbinding moet maken. Het is niet nodig om op alle banden in te schakelen, maar wordt alleen aanbevolen voor prestaties.

Use cases

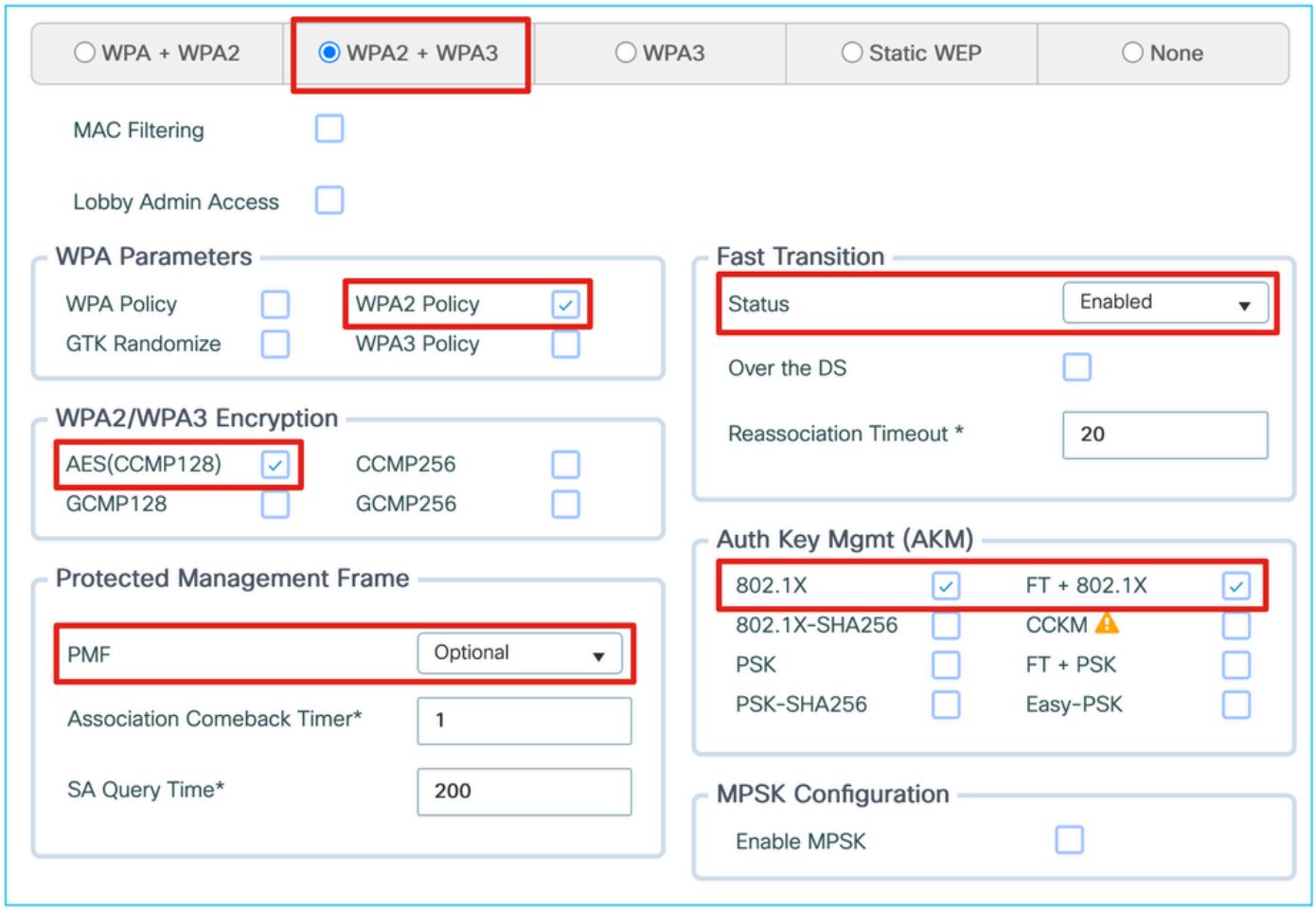
802.1X / WPA3-Enterprise-netwerken

Enterprise WLAN's op basis van WPA2/3 met 802.1X-verificatie zijn het eenvoudigst te migreren naar 6 GHz en/of Wi-Fi 7.

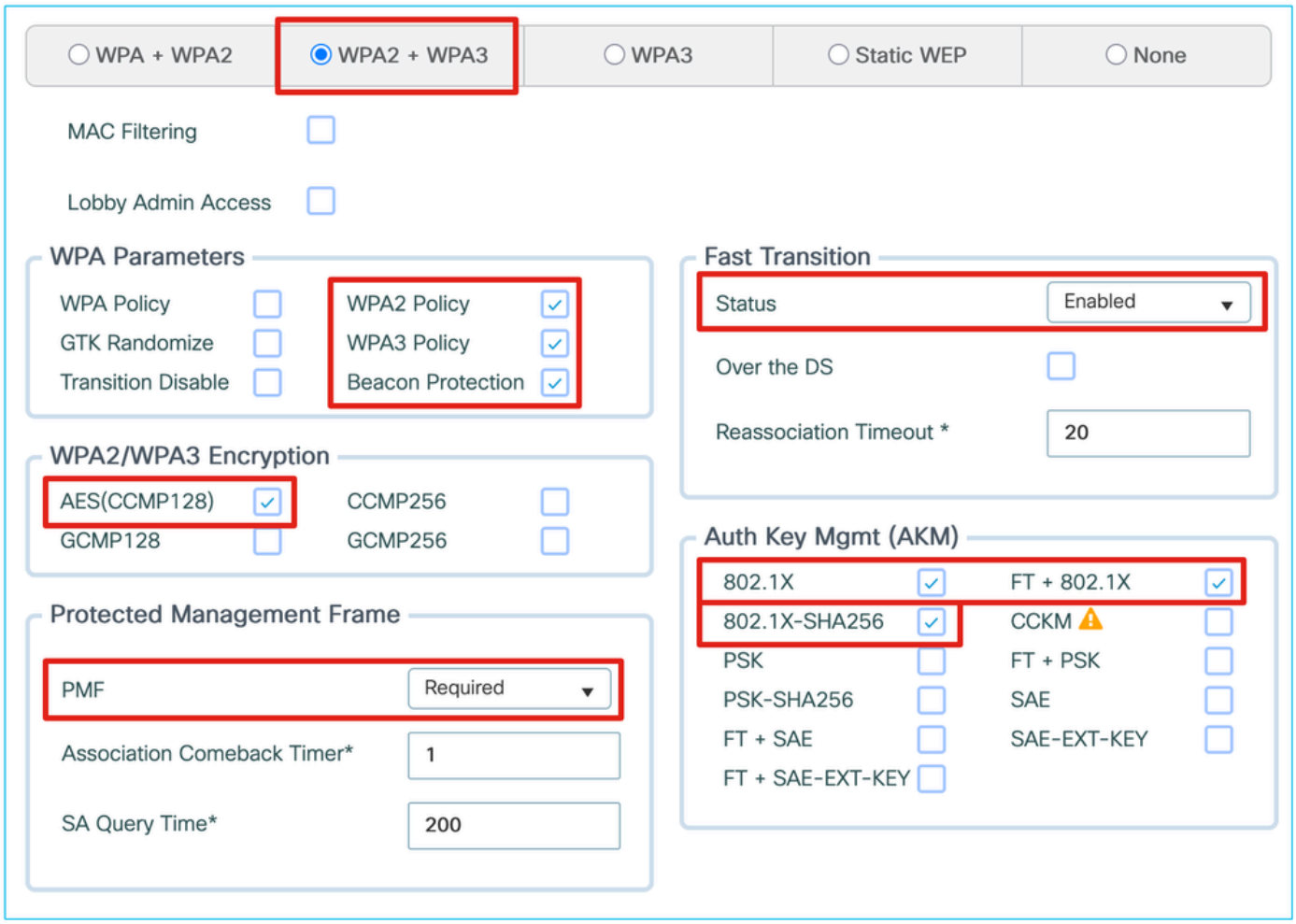
Voor het inschakelen van uw 802.1X SSID voor slechts 6 GHz is alleen PMF-ondersteuning nodig, zelfs als deze optioneel is, evenals 802.1X-SHA256 en/of FT + 802.1X AKM's, die beide WPA3-compatibel zijn.

We kunnen WPA2 met standaard 802.1X (SHA1) op hetzelfde WLAN blijven aanbieden. Ondersteuning voor Wi-Fi 7 vereist het inschakelen van Beacon Protection en het instellen van PMF zoals vereist in plaats van optioneel; WPA2 802.1X (SHA1) kan aanwezig blijven op het WLAN als een achterwaartse compatibiliteitsoptie. Dit betekent dat u al uw bedrijfsapparaten onder één SSID kunt plaatsen, op voorwaarde dat ze 802.11w/PMF ondersteunen, wat vrij gebruikelijk is op de huidige draadloze NIC's voor laptops en andere mobiele eindpunten.

Van een typische WPA2-SSID met deze L2-beveiligingsinstellingen:



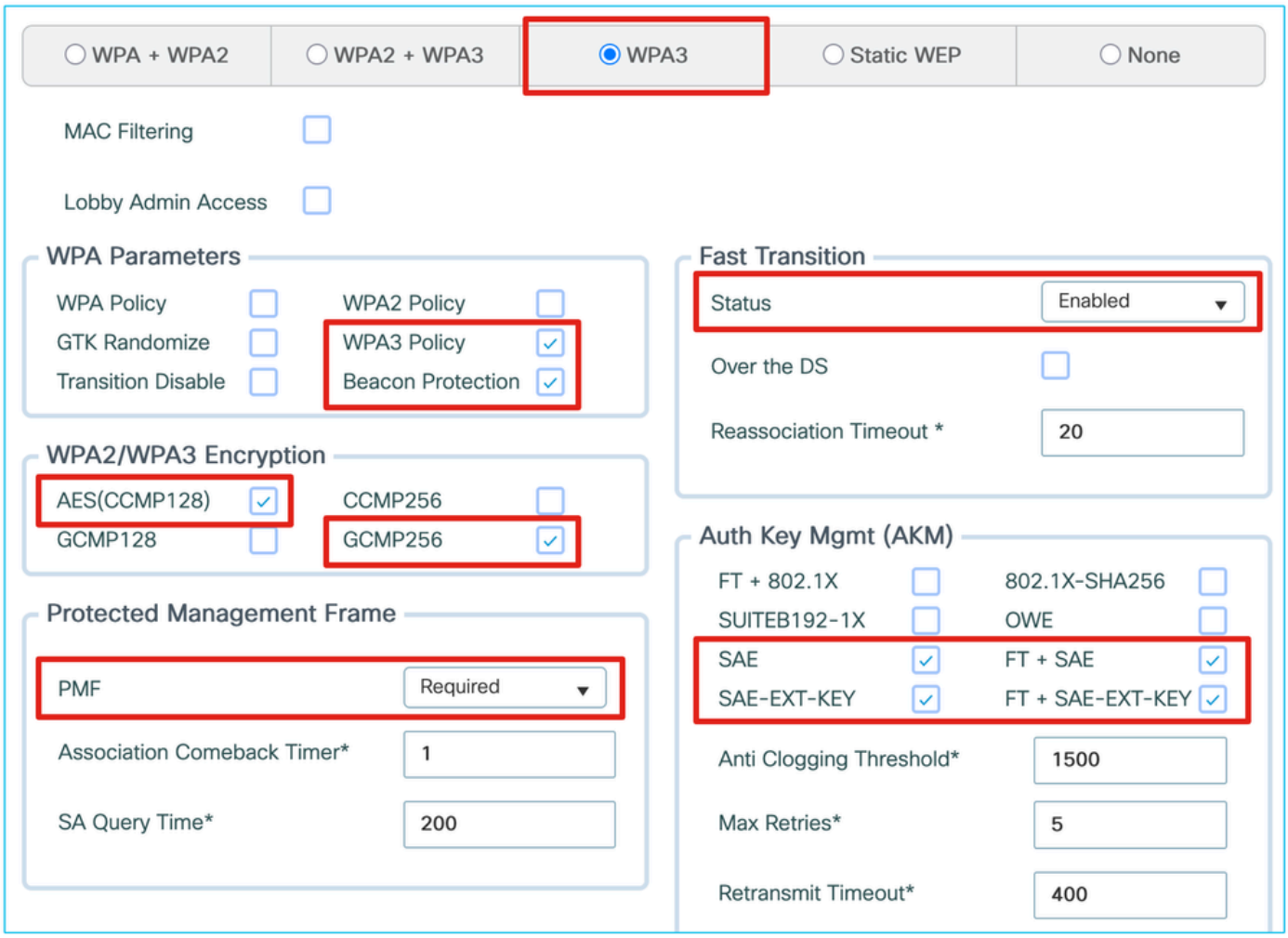
We kunnen de configuratie voor WPA3-, 6 GHz- en Wi-Fi 7-ondersteuning migreren zoals hier wordt weergegeven:

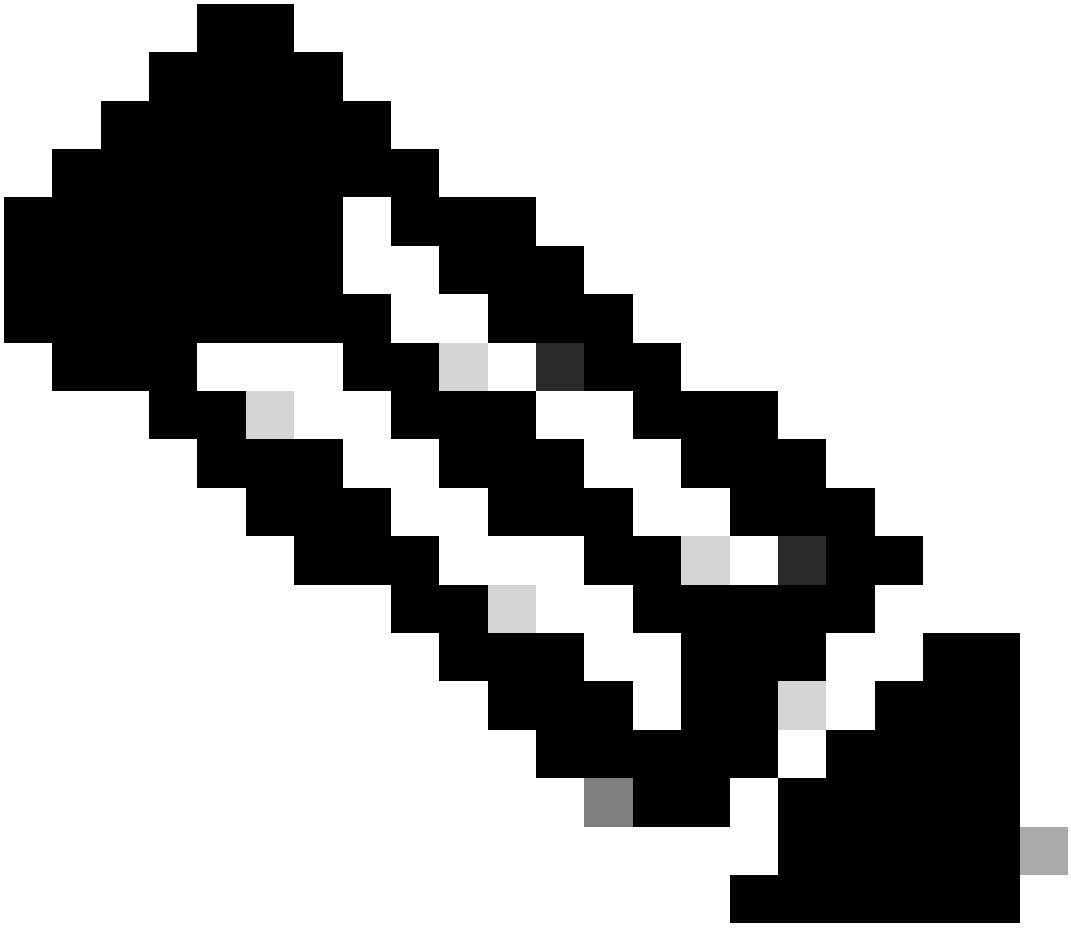


Wachtwoordgroep / WPA3-Personal / IoT-netwerken

Het inschakelen van een wachtwoordzin-SSID voor 6 GHz, tot Wi-Fi 6E-ondersteuning, is eenvoudig en vereist SAE en / of FT + SAE, samen met andere WPA2 PSK AKM's indien nodig. Voor Wi-Fi 7-ondersteuning vereist de certificering echter dat alle WPA2-PSK-opties worden verwijderd en dat SAE-EXT-KEY en/of FT + SAE-EXT-KEY AKM's worden toegevoegd, samen met GCMP256-codering. Het is daarom niet mogelijk om een op wachtwoordgroepen gebaseerd WLAN te hebben met zowel maximale compatibiliteit voor oudere clients als Wi-Fi 7-prestaties.

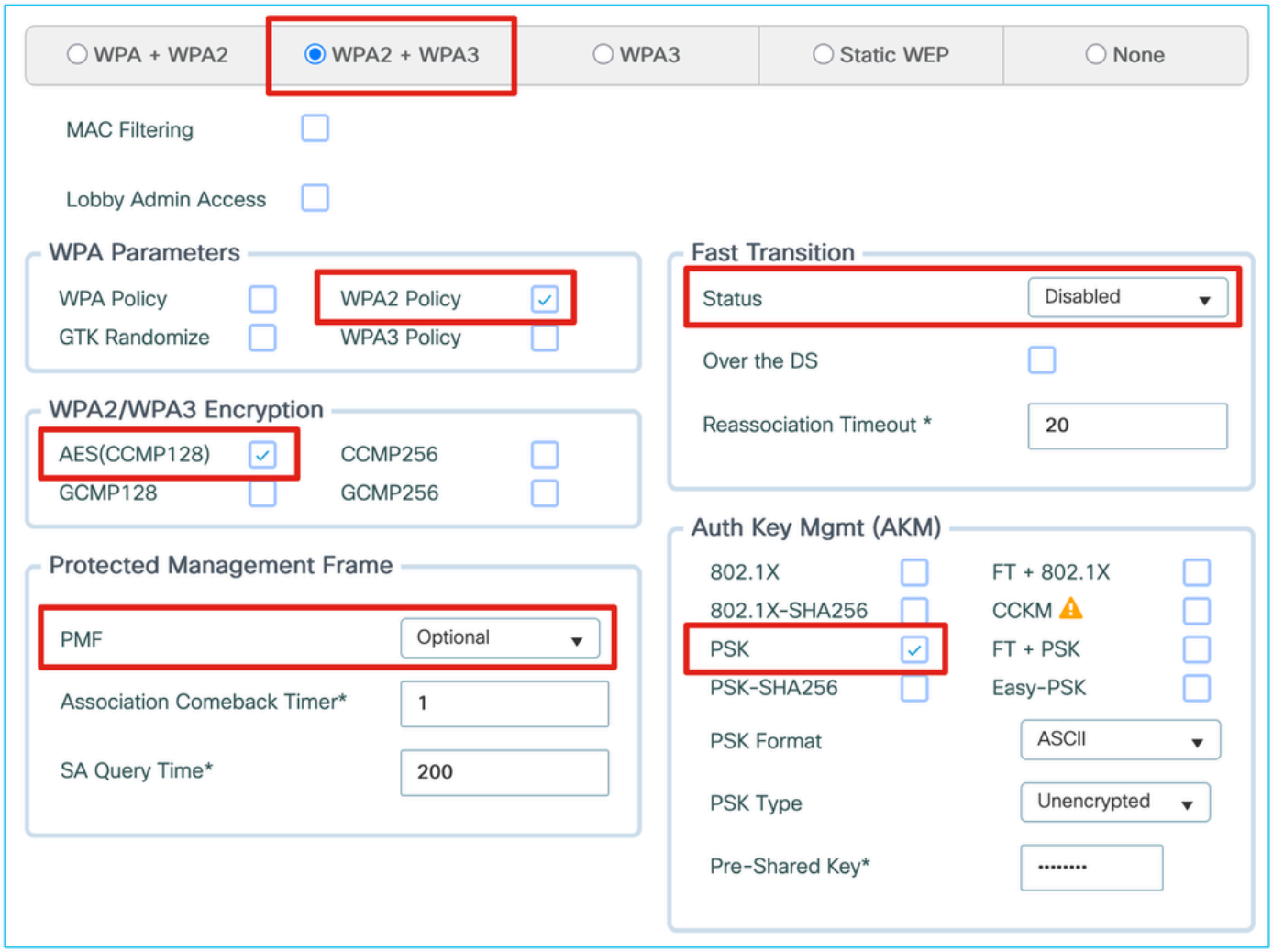
In dergelijke gevallen moeten we een speciale WPA3-SSID configureren met alleen SAE, FT + SAE, SAE-EXT-KEY en FT + SAE-EXT-KEY, die zowel AES(CCMP128)- als GCMP256-cijfers biedt, voor meer recente Wi-Fi 6E- en Wi-Fi 7-clients.


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



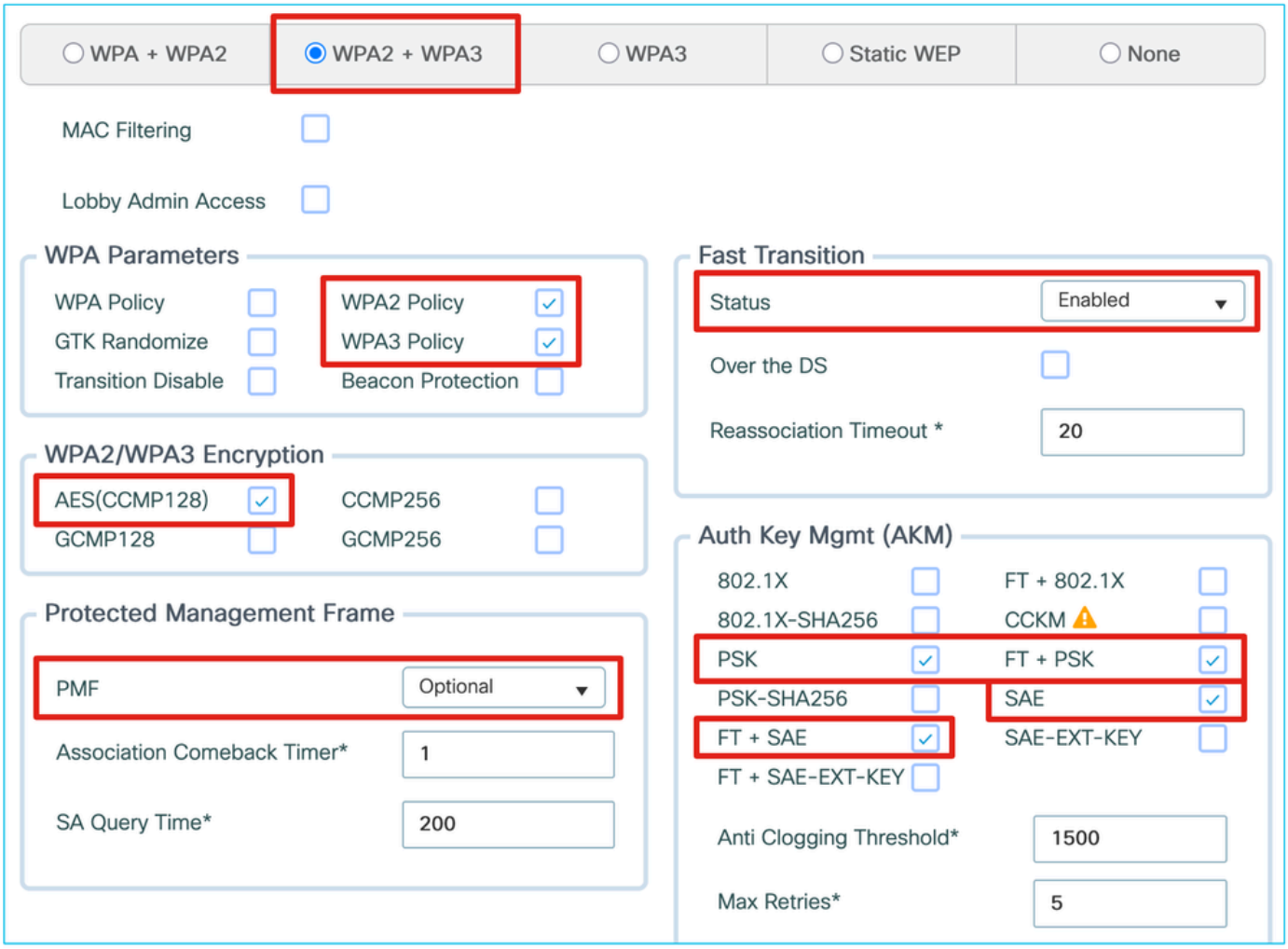
Opmerking: Als (FT +) SAE is ingeschakeld op het WLAN en een Wi-Fi 7-client probeert hieraan te koppelen in plaats van (FT +) SAE-EXT-KEY, wordt deze afgewezen. Zolang (FT +) SAE-EXT-KEY ook is ingeschakeld, moeten Wi-Fi 7-clients deze laatste AKM toch gebruiken en dit probleem mag zich niet voordoen.

Een andere standaard WPA2-SSID daarentegen kan nog steeds bestaande clients herbergen.



Hoewel deze combinatie de hoeveelheid totale SSID's verhoogt, kunnen we maximale compatibiliteit op één SSID behouden, waar we mogelijk ook andere geavanceerde functies kunnen uitschakelen die van invloed kunnen zijn op de compatibiliteit en die nuttig kunnen zijn voor veel IoT-scenario's, terwijl we maximale functies en prestaties bieden aan meer recente apparaten via de andere SSID.
Een andere optie zou natuurlijk ook kunnen zijn dat u de Wi-Fi 7 SSID niet aanbiedt en slechts één ervan geconfigureerd blijft voor WPA2 PSK en WPA3 SAE. Het idee erachter zou kunnen zijn dat IoT-apparaten sowieso geen Wi-Fi 7-prestaties nodig hebben.

Deze aanpak zou sowieso nog steeds 6 GHz ondersteunen voor Wi-Fi 6E en Wi-Fi 7-compatibele clients, die op zijn best verbinding zouden kunnen maken met Wi-Fi 6E-prestaties.



In al deze scenario's raden we sterk aan om FT in te schakelen bij het gebruik van SAE. De SAE-frameuitwisseling is kostbaar in termen van middelen en langer dan de WPA2 PSK 4-weg handshake.

Sommige fabrikanten van apparaten zoals Apple verwachten SAE alleen te gebruiken wanneer FT is ingeschakeld en kunnen weigeren verbinding te maken als deze niet beschikbaar is.

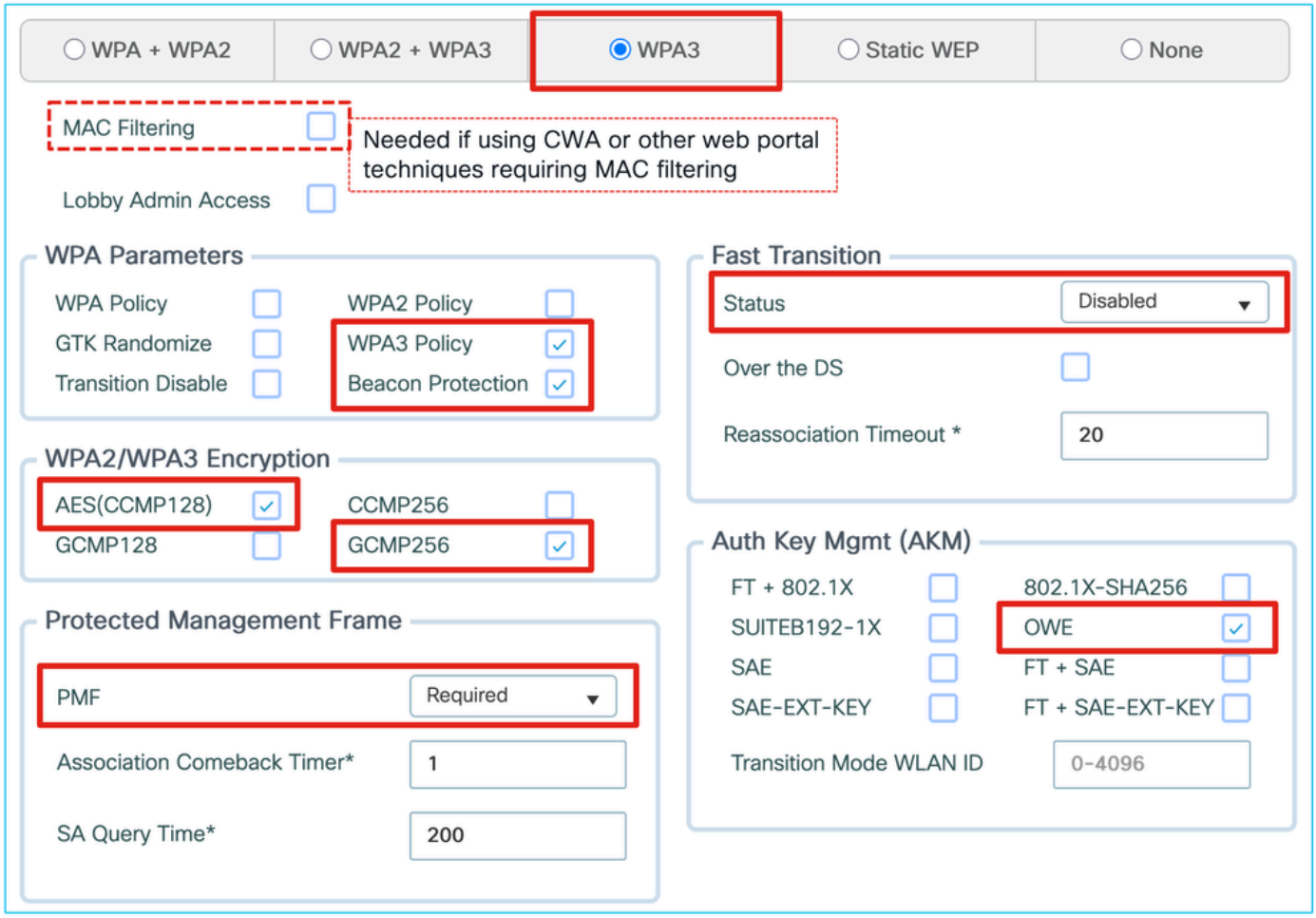
Open / Enhanced Open / OWE / gastnetwerken

Gastnetwerken komen met veel smaken. Meestal hebben ze geen 802.1X-referenties of wachtwoordzin nodig om verbinding te maken en mogelijk een splash-pagina of -portal te impliceren, waarvoor referenties of een code nodig kunnen zijn. Dit wordt traditioneel afgehandeld met een Open SSID en lokale of externe gastportaaloplossingen. SSID's met open beveiliging (geen codering) zijn echter niet toegestaan op 6 GHz of voor Wi-Fi 7-ondersteuning.

Een eerste zeer conservatieve benadering zou zijn om gastnetwerken op zijn best te wijden aan de 5 GHz-band en Wi-Fi 6. Dit laat de 6 GHz-band gereserveerd voor zakelijke apparaten, lost het complexiteitsprobleem op en zorgt voor maximale compatibiliteit, hoewel niet tot Wi-Fi 6E/7-prestaties.

Als we 6 GHz-service aan gasten willen bieden, zou de aanbeveling zijn om een afzonderlijke SSID te maken met Enhanced Open / OWE (Opportunistic Wireless Encryption). Het kan zowel

AES (CCMP128)-codering bieden, voor maximale compatibiliteit tot Wi-Fi 6E-clients, als GCMP256-bits voor Wi-Fi 7-compatibele clients.



Als aan de ene kant Enhanced Open een geweldige beveiligingsmethode is die privacy biedt en tegelijkertijd de "open" ervaring behoudt (eindgebruikers hoeven geen 802.1X-referenties of wachtwoordzin in te voeren), heeft deze tot op de dag van vandaag nog steeds beperkte ondersteuning tussen eindpunten. Sommige klanten ondersteunen het nog steeds niet en, zelfs als ze dat doen, wordt deze techniek niet altijd soepel afgehandeld (het apparaat kan de verbinding als onbeveiligd weergeven, terwijl deze eigenlijk veilig is, of het kan deze als wachtwoordbeveiligd weergeven, zelfs als er geen wachtwoordzin nodig is met OWE). Aangezien van een gastnetwerk wordt verwacht dat het op alle niet-gecontroleerde gastapparaten werkt, kan het te vroeg zijn om alleen een Enhanced Open SSID te leveren en wordt aanbevolen om beide opties via afzonderlijke SSID's te bieden: een open op 5 GHz en een OWE ingeschakeld op 5 en 6 GHz, beide met hetzelfde captive-portaal erachter als dit ook een vereiste is. De transitiemodus wordt niet ondersteund op Wi-Fi 6E, 6 GHz (hoewel het nog steeds kan worden toegestaan op software) of Wi-Fi 7, dus dat is geen aanbevolen oplossing. Alle portaalomleidingstechnieken (interne of externe webverificatie, centrale webverificatie, ...) worden nog steeds ondersteund door OWE.

Extra WPA3 en gerelateerde opties

Hoewel WPA3-opties het best kunnen worden beschreven en behandeld in de WPA3-

implementatiegids, behandelt dit gedeelte enkele aanvullende aanbevelingen voor WPA3 die specifiek betrekking hebben op 6 GHz- en Wi-Fi 7-ondersteuning.

Bakenbescherming

Dit is een functie die de kwetsbaarheid oplost, waarbij een kwaadwillende aanvaller bakens kan verzenden in plaats van het legitieme toegangspunt, terwijl sommige velden worden gewijzigd om de beveiliging of andere instellingen van reeds gekoppelde clients te wijzigen. Beacon-bescherming is een extra informatie-element in het baken dat als handtekening voor het baken zelf fungeert, om te bewijzen dat het door het legitieme toegangspunt is verzonden en dat er niet mee is geknoeid. Alleen gekoppelde clients met een WPA3-coderingssleutel kunnen de legitimiteit van het baken verifiëren, waardoor klanten geen middelen hebben om het te verifiëren. Het extra informatie-element in het baken moet eenvoudig worden genegeerd door clients die het niet ondersteunen (niet-Wi-Fi 7-clients) en het vertegenwoordigt normaal gesproken geen compatibiliteitsprobleem (tenzij met een slecht geprogrammeerd clientstuurprogramma).

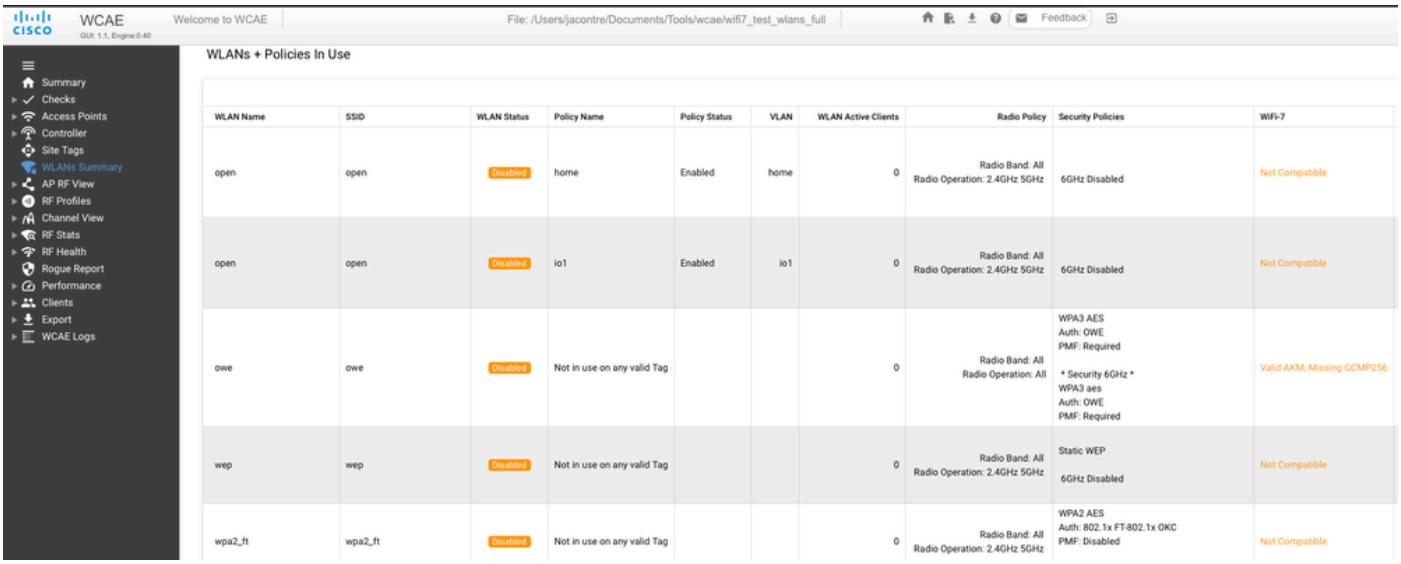
GCMP256

Tot de Wi-Fi 7-certificering, de meeste clients geïmplementeerd AES (CCMP128) encryptie. CCMP256 en GCMP256 zijn zeer specifieke varianten gerelateerd aan SUITE-B 802.1X AKM. Hoewel sommige eerste generaties van Wi-Fi 7-clients op de markt aanspraak maken op Wi-Fi 7-ondersteuning, implementeren ze mogelijk nog steeds geen GCMP256-codering, wat een probleem kan worden als Wi-Fi 7 AP's die de standaard afdwingen zoals verwacht voorkomen dat deze clients verbinding maken zonder de juiste GCMP256-ondersteuning.

Problemen oplossen en controleren

De nieuwste versie van Wireless Configuration Analyzer Express (https://developer.cisco.com/docs/wireless-troubleshooting-tools/wireless-config-analyzer-express-gui/) heeft een gereedheidscheck voor Wi-Fi 7 waarmee de 9800-configuratie wordt geëvalueerd voor alle hierboven genoemde Wi-Fi 7-vereisten.

Als u nog steeds twijfelt of uw configuratie klaar is voor Wi-Fi 7, laat de WCAE u weten wat er mis is.



Referenties

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.