6GHz 및 Wi-Fi로 마이그레이션 7

목차

소개

이 문서에서는 Wi-Fi 7의 성능을 최적화하고 6GHz 스펙트럼을 완전히 활용하기 위한 설계 및 구성 지침에 대해 설명합니다.

6GHz 및 Wi-Fi를 사용해야 하는 이유 7

6GHz는 2020년에 WLAN 운영에 사용할 수 있게 된 새로운 대역으로, Wi-Fi 6E 인증을 통해 초기에 악용되었습니다. Wi-Fi 6E는 여전히 동일한 802.11ax 표준(2.4/5GHz 대역용 Wi-Fi 6 인증)을 사용하지만, 특정 요구 사항이 충족될 경우 6GHz 대역에서만 작동하도록 확장됩니다.

Wi-Fi 7은 IEEE 802.11be 표준의 인증에 해당하며, 6GHz로만 제한되는 Wi-Fi 6E와 달리 세 가지 대역 모두에서 사용하도록 정의됩니다. 2.4, 5 및 6GHz Wi-Fi 7도 이전 인증 대비 새로운 기능을 제공합니다.

6GHz 및/또는 Wi-Fi 7은 지원해야 할 특정 요구 사항이 있습니다. 이는 특히 2.4/5GHz 대역 및 Wi-Fi 6까지 사용했던 것과 비교하여 새로운 구성과 RF 설계로 해석됩니다. 예를 들어, WEP 보안을 사용하면 802.11a/b/g가 아닌 802.11 표준을 사용할 수 없게 되는 것과 마찬가지로, 최신 표준은 더 안전한 네트워크 채택을 촉진하기 위해 더 높은 보안 필수 조건을 갖추게 됩니다.

반면, 최신 6GHz 대역은 Wi-Fi 6E/7과 같은 최신 인증과 결합되어 더 깨끗한 주파수, 더 나은 성능 및 새로운 사용 또는 기존 사용 사례(예: 음성/비디오 컨퍼런싱)의 "안심할 수 있는" 구현을 가능하게 합니다.

6GHz 작동 및 Wi-Fi 7에 대한 기본 요구 사항

다음은 6GHz 및 Wi-Fi 7 운영에 대한 인증서에 명시된 보안 요구 사항입니다.

6GHz 대역 요구 사항

6GHz 대역에서는 WPA3 또는 Enhanced Open WLAN만 허용할 수 있습니다. 이는 다음 보안 옵션 중 하나를 의미합니다.

- 802.1X 인증을 사용하는 WPA3-엔터프라이즈
- WPA3 SAE(Simultaneous Authentication of Equals)(예: WPA3-Personal) 및 비밀번호 사용 SAE-FT(Fast Transition을 사용하는 SAE)는 또 다른 가능한 AKM이며, SAE 핸드셰이크가 사소한 것이 아니며 FT는 더 긴 교환을 건너뛸 수 있으므로 실제로 사용하는 것이 좋습니다.
- Enhanced Open with Opportunational Wireless Encryption(OWE)

WPA3 v3.4 사양(섹션 11.2)에 따르면 Enhanced Open Transition 모드는 6GHz에서 지원되지 않지만, 많은 공급업체(최대 IOS® XE 17.18에 이르는 Cisco 포함)에서는 아직 이를 적용하지 않습니다. 따라서 기술적으로 5GHz의 Open SSID, 5GHz 및 6GHz의 해당 Enhanced Open SSID를 구성할 수 있으며, 둘 다 전환 모드가 활성화되어 있고 이 모든 것을 표준 사양을 준수하지 않고 구성할 수 있습니다. 그러나 이러한 시나리오에서는 전환 모드 없이 Enhanced Open SSID를 구성하고 6GHz에서만 사용할 수 있으며(일반적으로 6GHz를 지원하는 클라이언트는 Enhanced Open도 지원), 전환 모드 없이 5GHz에서 일반 Open SSID를 유지할 수 있어야 합니다.

802.11w/PMF(Protected Management Frame) 적용 외에 WPA3-Enterprise에 대한 새로운 특정 암호 또는 알고리즘 요구 사항은 없습니다. Cisco를 포함한 많은 공급업체는 802.1X-SHA256 또는 "FT + 802.1X"(실제로 SHA256 및 Fast Transition이 맨 위에 있는 802.1X)를 WPA3를 준수하고 일반 802.1X(SHA1 사용)를 WPA2의 일부로 간주하므로 6GHz에 대해 적합/지원되지 않습니다.

Wi-Fi 7 요건

802.11be 표준의 Wi-Fi 7 인증을 통해 Wi-Fi Alliance는 보안 요건을 강화했습니다. 그중 일부는 802.11be 데이터 전송률 및 프로토콜 개선을 사용할 수 있으며, 다른 일부는 MLO(Multi-Link Operations)를 지원하여 호환되는 장치(클라이언트 및/또는 AP)가 동일한 연결을 유지하면서 여러 주파수 대역을 사용할 수 있도록 합니다.

일반적으로 Wi-Fi 7에는 다음 보안 유형 중 하나가 필요합니다.

- AES(CCMP128) 및 802.1X-SHA256 또는 FT + 802.1X가 있는 WPA3-엔터프라이즈(명명 상 명시적이지 않더라도 여전히 SHA256을 사용함) 이는 6GHz 대역에 대한 기존 WPA3 보안 전제 조건과 비교할 때 변화를 나타내지 않습니다.
- GCMP256 및 SAE-EXT-KEY 및/또는 FT + SAE-EXT-KEY(AKM 24 또는 25)를 사용하는 WPA3-개인 Wi-Fi 6E는 일반 AES(CCMP128)와 함께 WPA3 SAE 및/또는 FT + SAE를 의무화했으며 추가 확장 키 사용이 없으므로 Wi-Fi 7에 특별히 도입된 새로운 암호입니다.

- GCMP256을 통한 Enhanced Open/WISE. 동일한 SSID에서 AES(CCMP128)를 구성할 수 있지만 AES 128을 사용하는 클라이언트는 Wi-Fi 7을 지원할 수 없습니다. Wi-Fi 7 이전에는 Enhanced Open을 지원하는 대부분의 클라이언트가 AES 128만 사용했으므로 이는 더욱 강력해진 새로운 요구 사항입니다. 6GHz 지원에서는 전환 모드가 허용되지 않습니다.

이 모든 경우 WLAN에서 Wi-Fi 7을 지원하려면 PMF(Protected Management Frame) 및 비컨 보호(Beacon Protection)도 필요합니다.

Wi-Fi 7은 이 문서를 작성할 당시에도 최신 버전이며, 가능한 한 일찍 릴리스되었으므로 많은 벤더가 처음부터 이러한 모든 보안 요구 사항을 시행하지 않았습니다.

최근에는 Cisco에서 Wi-Fi 7 인증을 준수하기 위해 구성 옵션을 점진적으로 적용하고 있습니다. 다음은 버전별 동작입니다.

17.18.1 이상

IOS XE 17.18 이상 버전에서는 WLAN에 Wi-Fi 7 요구 사항(WLAN 유형 및 Wi-Fi 7 MLO를 달성하기 위해 GCMP256의 존재 여부에 따라 앞에서 설명한 대로 WLAN 보호, PMF 및 올바른 AKM과 일치하는 보안 매개변수가 있는 경우 WLAN에 Wi-Fi 7이 활성화되었다고 광고만 합니다(SAE-EXT 또는 WISE의 경우). SSID에서는 AES128의 존재가 허용되지만, 사용 시 Wi-Fi 6E만 제공하고 Wi-Fi 7 MLO는 제공하지 않습니다.

클라이언트는 사용하는 보안 방법(WLAN에서 계속 지원하는 경우)에 관계없이 Wi-Fi 7로 연결하고 Wi-Fi 7 데이터 속도를 얻을 수 있습니다. 그러나 클라이언트가 Wi-Fi 7 보안에 대한 엄격한 요구 사항을 준수하거나 거부된 경우에만 MLO 지원(하나 이상의 밴드에서)으로 연결할 수 있습니다.

17.15.3 이상 17.15.x 버전

이 브랜치에서는 모든 WLAN이 Wi-Fi 7 SSID로 브로드캐스트됩니다. 단, Wi-Fi 7이 보안 설정과 상관없이 전역적으로 활성화되어 있어야 합니다.

클라이언트는 Wi-Fi 7 지원 클라이언트로 연결할 수 있으며 WLAN에서 계속 지원하는 경우 사용하는 보안 방법에 관계없이 Wi-Fi 7 데이터 속도를 달성할 수 있습니다. 그러나 클라이언트는 Wi-Fi 7 보안에 대한 엄격한 요구 사항을 준수하거나 거부된 경우에만 MLO 지원(하나 이상의 밴드에서)으로 연결할 수 있습니다.

GCMP256과 같이 일부 초기 Wi-Fi 7 클라이언트가 더 안전한 암호를 지원할 수 없는 경우, 보안 설정이 Wi-Fi 7 요구 사항과 일치하지 않는 WLAN에 Wi-Fi 7 MLO 지원 기능으로 연결하려고 하면 문제가 발생할 수 있습니다. 이러한 상황에서는 유효하지 않은 보안 설정(WLAN에서 구성할 수 있음)으로 인해 클라이언트가 거부됩니다.

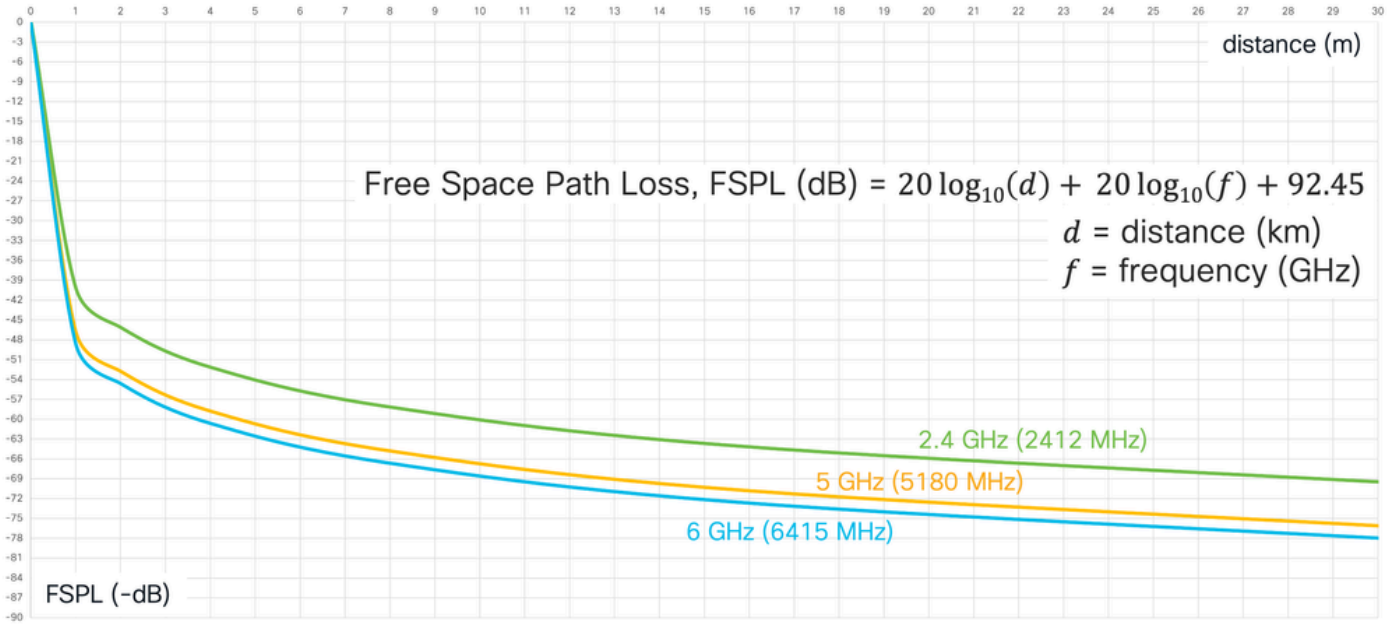
6GHz 커버리지에 대한 무선 설계 고려 사항

사이트 설문조사에 대한 완전한 규범적 가이드가 되기는 커녕, 이 섹션에서는 6GHz 커버리지를 설계할 때, 특히 Wi-Fi 6E 또는 7로 마이그레이션하려는 2.4/5GHz에 대한 기존 설치가 있는 경우 몇 가지 기본 고려 사항에 대해 간략하게 설명합니다.
2.4GHz 및/또는 5GHz에서 새로운 Wi-Fi 구축에 사용된 경우, 6GHz의 새로운 무선 프로젝트에는

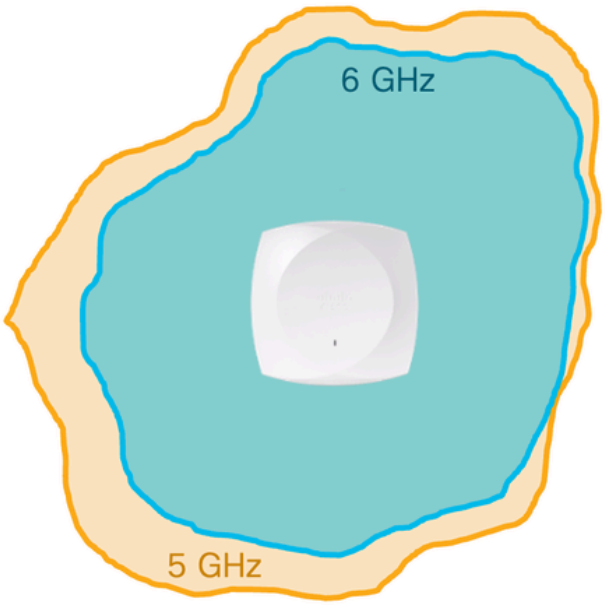
해당 전용 6GHz 사이트 설문조사도 포함되어야 합니다.

Wi-Fi 6E/7 이전 버전의 AP가 이미 특정 5GHz 범위 및 요구 사항에 맞게 배치된 경우, Wi-Fi 6E/7 지원 AP로 대체하고 여전히 6GHz에서도 양호한 커버리지를 확보할 수 있을 것으로 예상할 수 있습니다. 이러한 이론이 작동하려면 기존 AP가 최대 한도 내에서 3~4개 이상의 전송 전력 레벨을 이미 유지하면서 의도된 요구 사항(데이터 전용, 음성, 특정 애플리케이션 등)에 대해 올바른 5GHz 커버리지를 이미 제공해야 합니다. AP는 일반적으로 7~8개의 전력 레벨을 가지며 각 전력 레벨은 전송 전력을 절반으로 나눕니다. 이는 AP가 허용된 송신 전력 범위의 매체를 사용할 때 편안한 지점이 된다는 것을 의미합니다.

자유 공간 손실 계산에 따르면, 6GHz 신호는 5GHz 신호보다 2dB 이상 감쇠됩니다. 게다가 6GHz 신호는 5GHz에 해당하는 신호보다 장애물의 영향을 더 많이 받을 수 있습니다.



Cisco AP가 전송 전력을 한 단계 높이거나 낮출 때 3dB의 "점프"로 증가합니다. 예를 들어 전송 전력이 11dBm인 전력 레벨 4에서 3으로 가는 AP는 전송 전력을 14dBm으로 높입니다(전력 레벨 4의 경우 11dBm, 전력 레벨 3의 경우 14dBm은 일반적인 예이며, AP의 다른 모델/세대가 동일한 전력 레벨 번호의 경우 dBm에서 약간 다른 전송 전력 값을 가질 수 있으므로).



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.

예를 들어, Pre-Wi-Fi 6E/7 AP가 이미 전력 레벨 4에서 5GHz에서 커버리지가 우수한 경우, 유사한 5GHz 무선 패턴을 가진 최신 Wi-Fi 6E/7 AP가 기존 5GHz 네트워크에 큰 영향을 미치지 않고 이전 AP를 대체할 수 있습니다.

또한 새로운 Wi-Fi 6E/7 AP의 6GHz 무선 장치는 한 개의 송신 전력 레벨(3dB)만 높더라도 5GHz 무선 장치와 유사한 6GHz 커버리지를 제공할 수 있습니다.

5GHz가 AP의 5GHz 무선 장치에 최대 전력 레벨 3~4에서 올바르게 지원된 경우, 해당 6GHz 무선 장치는 최대 전력 레벨 2~3에서 동급의 지원 범위를 설정할 수 있습니다.

또한 6GHz 무선 장치가 이미 최대값보다 낮은 2~3개 전력 수준에서 올바른 커버리지를 제공하는 경우, 예외적으로 두 단계 높은 수준까지 이동할 수 있습니다. 예를 들어 일시적인 예기치 않은 커버리지 구멍(인접 AP의 고장, 예고 없이 발생한 장애, 새로운 RF 요구 사항 등)을 해결하기 위해 노력할 수 있습니다.

Wi-Fi 6E/7 이전 버전과 Wi-Fi 6E/7 이전 버전 AP 간의 로밍 동작

서로 다른 표준 및/또는 주파수 대역을 지원하는 AP를 동일한 커버리지 영역에 구축하는 것은 권장되지 않았습니다. 특히, 서로 다른 세대의 AP가 "소금 및 후추" 방식(동일한 영역에서 서로 혼합됨)으로 설치된 경우에는 권장되지 않았습니다.

무선 컨트롤러는 여러 AP 모델 그룹의 작업(예: 동적 채널 할당, 전송 전력 제어, PMK 캐시 배포 등)을 처리할 수 있지만, 서로 다른 표준과 서로 다른 주파수 대역 사이에서 이동하는 클라이언트는 이 작업을 항상 제대로 처리할 수 없으며 예를 들어 로밍 문제가 발생할 수 있습니다.

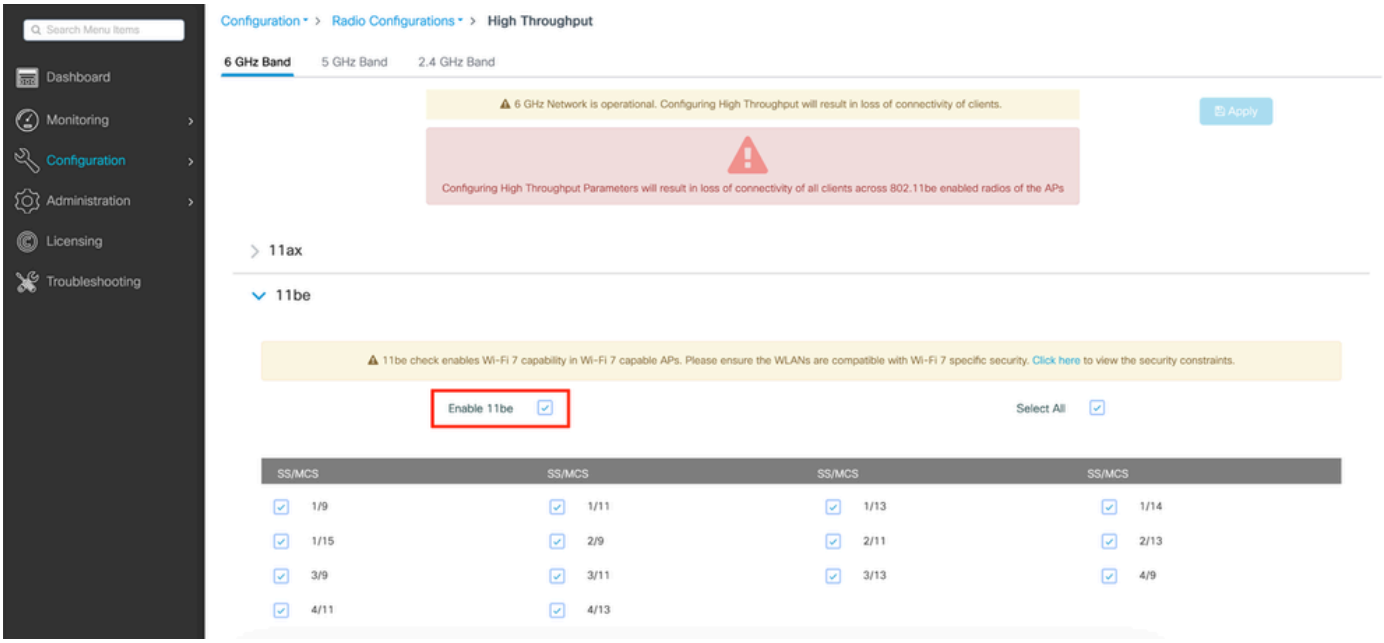
뿐만 아니라 최신 표준 때문에 Wi-Fi 6E/7 AP는 WPA3에 대해 GCMP256 암호를 지원합니다. 그러나 일부 Wi-Fi 6 AP 및 이전 모델에서는 항상 그렇지는 않습니다. AES(CCMP128) 및 GCMP256 암호를 모두 구성해야 하는 암호/WPA3-개인 및 향상된 개방형/WISE SSID의 경우 특정 Wi-Fi 6(예: 9105, 9115 및 9120 시리즈)은 GCMP256을 지원하지 않으며 Wi-Fi 6E/7 지원 클라이언트를 비롯한 연결 클라이언트에만 AES(CCMP128) 암호를 제공할 수 있습니다. 이러한 Wi-Fi 6E/7 클라이언트가 GCMP256을 지원하는 인접한 Wi-Fi 6E/7 AP에서/로 로밍해야 하는 경우 AES(CCMP128)와

GCMP256 간의 암호를 재협상하는 것이 투명 로밍에 지원되지 않으므로 새로운 연결을 거쳐야 합니다. 또한 일반적으로 일부 AP가 새로운 기능을 제공하고 다른 AP가 동일한 기능을 제공하지 않는 같은 영역의 경우 적합하지 않습니다. 클라이언트가 이동하는 동안 이러한 기능을 안전하게 사용할 수 없으며 고착성 또는 연결이 끊어질 수 있습니다.
이 시나리오는 매우 중요한 경우이지만, WLAN에 GCMP256 암호가 구성되어 있으면 9105/9115/9120 AP와 9130/9124/916x/917x AP 간에 Wi-Fi 6E/7 클라이언트의 로밍이 불가능하므로, 후자의 시리즈는 GCMP256을 지원하며 전자는 지원하지 않습니다.

6GHz에서 40MHz 이상의 채널 폭은 6GHz 지원 클라이언트에 고착성을 유발할 수 있으며, 이 클라이언트는 다른 대역과의 재연결을 거부할 수 있습니다. 이는 동일한 로밍 영역에서 6GHz 지원 AP와 6GHz가 아닌 지원 AP를 혼합하지 않는 또 다른 이유여야 합니다.

Wi-Fi 7을 전역적으로 활성화

Wi-Fi 7을 지원하는 IOS XE 버전으로 설치 또는 업그레이드할 경우 기본적으로 Wi-Fi 7에 대한 지원은 전역적으로 비활성화됩니다.
이를 활성화하려면 각 2.4/5/6GHz 대역의 High Throughput 컨피그레이션 메뉴 아래에서 11be를 활성화하는 확인란을 선택해야 합니다.



또 다른 옵션은 터미널 컨피그레이션 모드에서 SSH/콘솔을 통해 다음 3개의 명령행을 실행하는 것입니다.

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

경고 노트에서 언급한 것처럼, 이러한 설정을 수정하려고 할 때 802.11be 지원 상태를 변경하면 Wi-Fi 7 AP의 무선 전반에서 모든 클라이언트의 연결이 잠시 끊깁니다. 여러 밴드에 동시에 연결하는

클라이언트를 의미하는 MLO를 수행하려면 클라이언트가 연결할 모든 밴드에서 11be를 활성화해야 합니다. 모든 밴드에서 활성화할 필요는 없지만, 단순히 성능을 위해 권장됩니다.

활용 사례

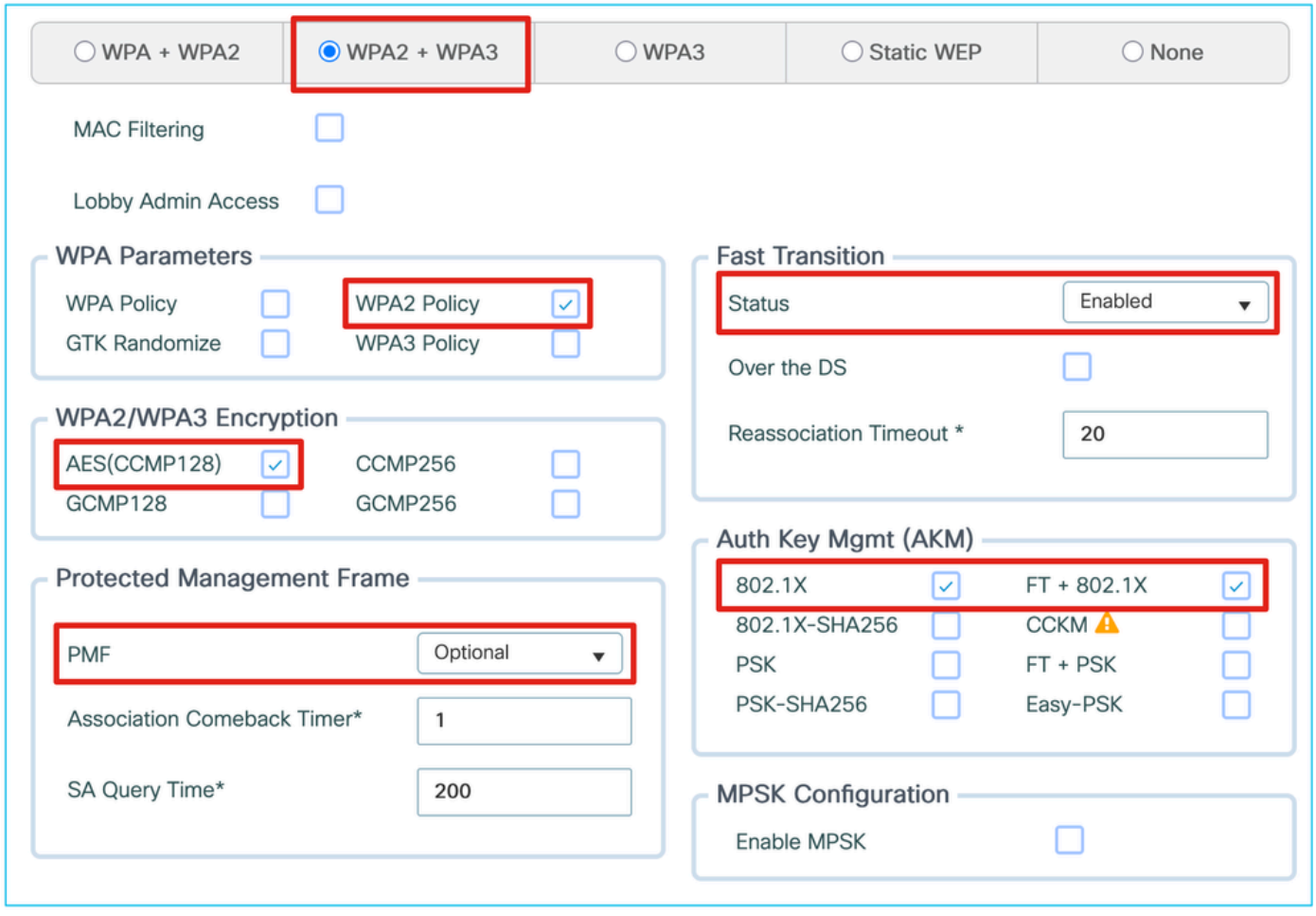
802.1X/WPA3-엔터프라이즈 네트워크

802.1X 인증을 사용하는 WPA2/3 기반 엔터프라이즈 WLAN은 6GHz 및/또는 Wi-Fi 7로 가장 쉽게 마이그레이션할 수 있습니다.

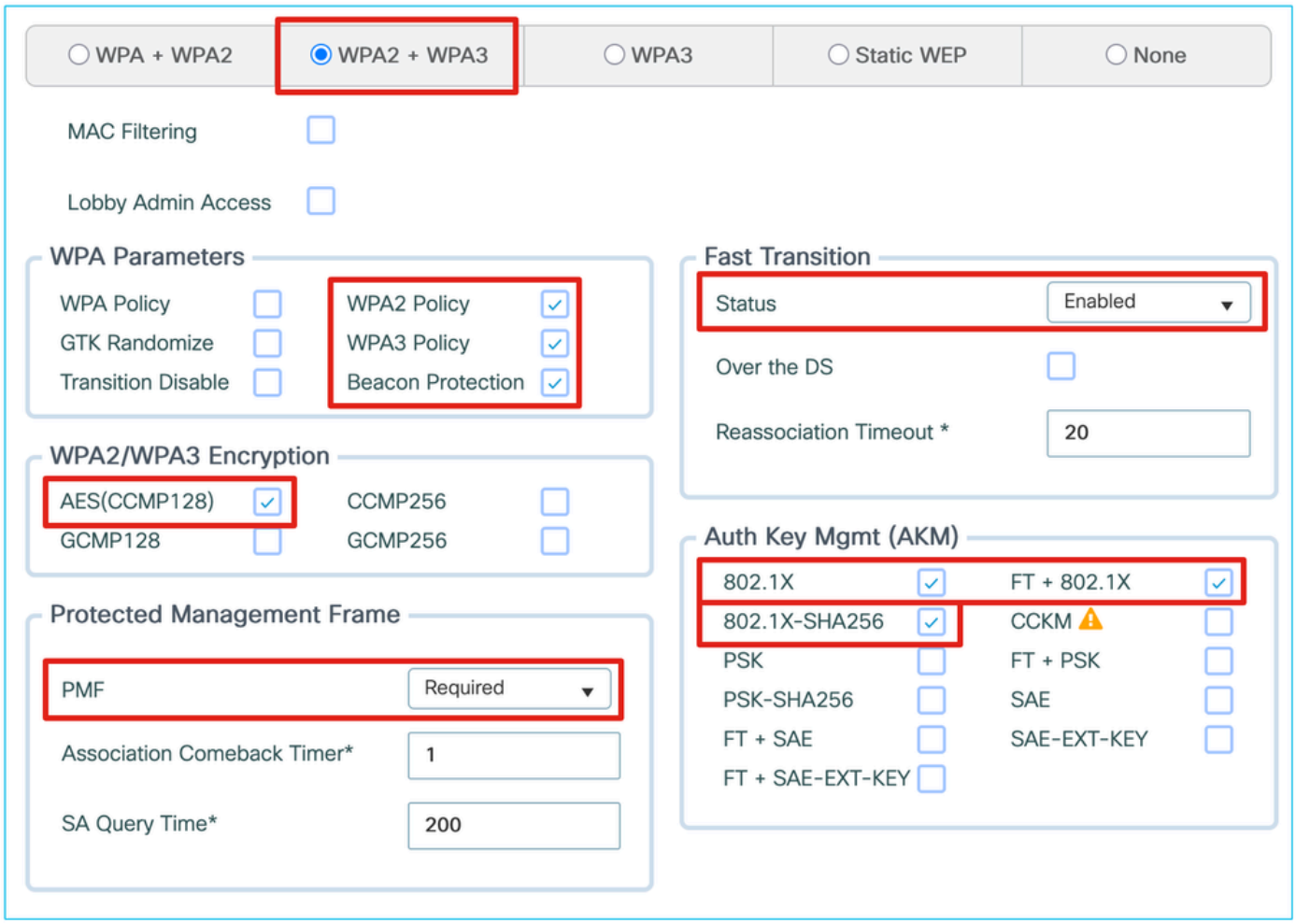
6GHz에 대해 802.1X SSID를 활성화하려면 PMF 지원만 활성화하면 됩니다(선택 사항). 또한 802.1X-SHA256 및/또는 FT + 802.1X AKM도 활성화해야 합니다. 둘 다 WPA3를 준수합니다.

동일한 WLAN에서 표준 802.1X(SHA1)를 사용하는 WPA2를 계속 제공할 수 있습니다. Wi-Fi 7 지원에는 비컨 보호(Beacon Protection)를 활성화하고 PMF를 선택 사항이 아닌 필수 사항으로 설정해야 합니다. WPA2 802.1X(SHA1)는 이전 버전과의 호환성 옵션으로 WLAN에 있을 수 있습니다. 즉, 모든 기업 장치가 802.11w/PMF를 지원하는 경우 단일 SSID로 연결할 수 있습니다. 이는 노트북 및 기타 모바일 엔드포인트용 최신 무선 NIC에서 매우 일반적입니다.

다음과 같은 L2 보안 설정을 사용하는 일반적인 WPA2 SSID에서



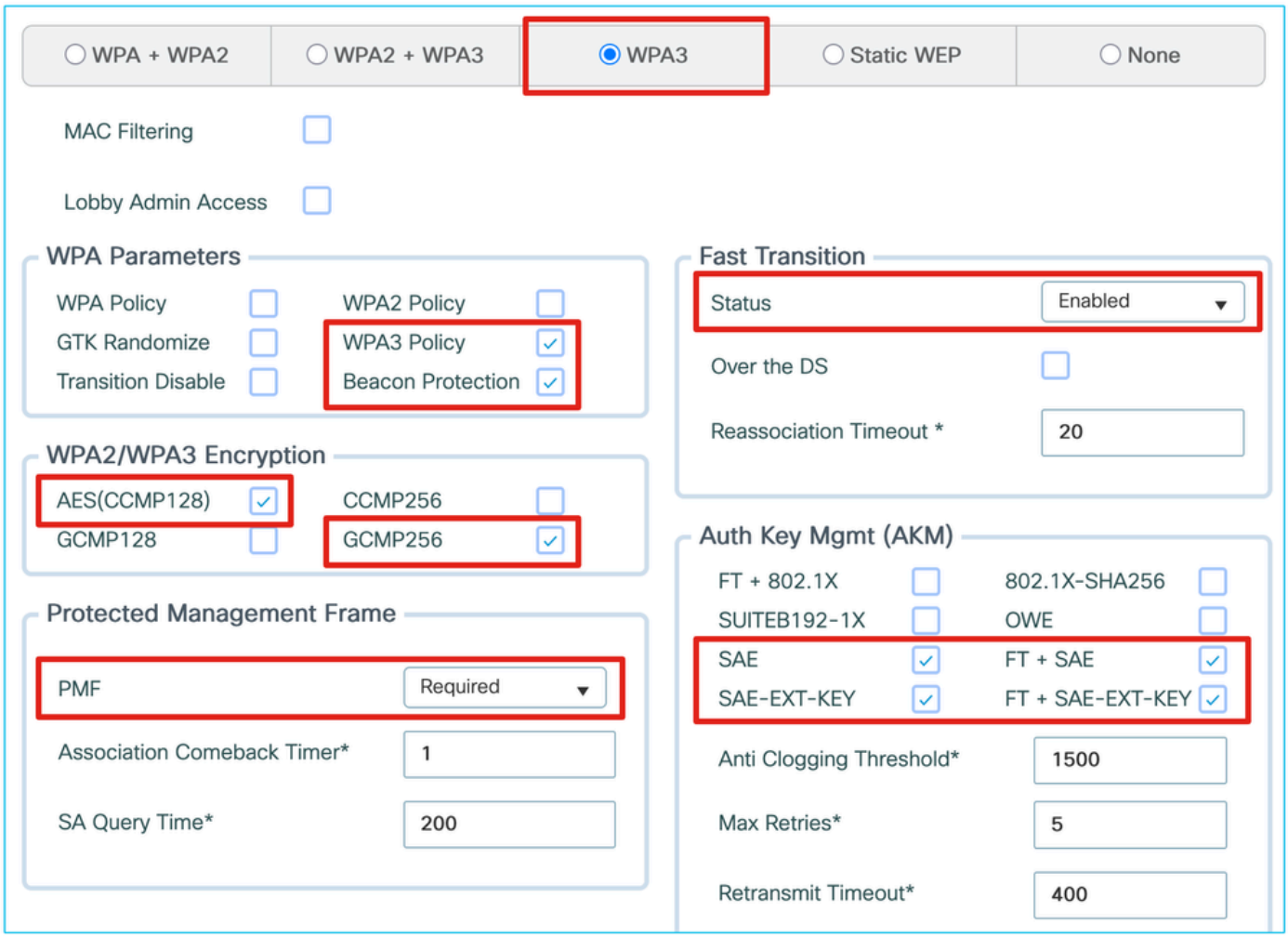
다음과 같이 WPA3, 6GHz 및 Wi-Fi 7 지원을 위한 컨피그레이션을 마이그레이션할 수 있습니다.

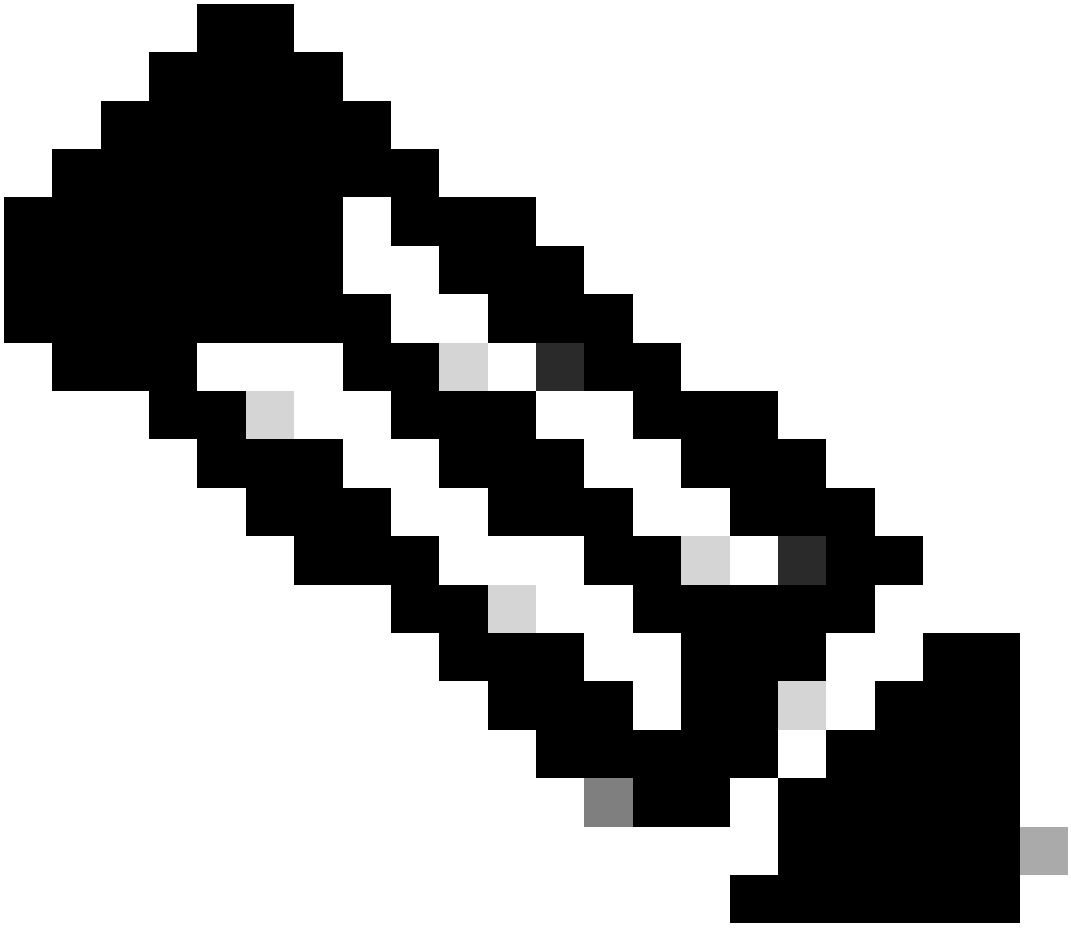


암호/WPA3-개인/IoT 네트워크

최대 Wi-Fi 6E를 지원하는 6GHz에 대해 패스프레이즈 SSID를 활성화하려면 SAE 및/또는 FT + SAE와 함께 필요한 경우 다른 WPA2 PSK AKM이 필요합니다. 그러나 Wi-Fi 7 지원의 경우 인증에서는 WPA2 PSK 옵션을 제거하고 GCMP256 암호와 함께 SAE-EXT-KEY 및/또는 FT + SAE-EXT-KEY AKM을 추가해야 합니다. 따라서 이전 클라이언트와 Wi-Fi 7 성능 모두에 대해 최대 호환성을 갖춘 암호 기반 WLAN을 보유할 수는 없습니다.

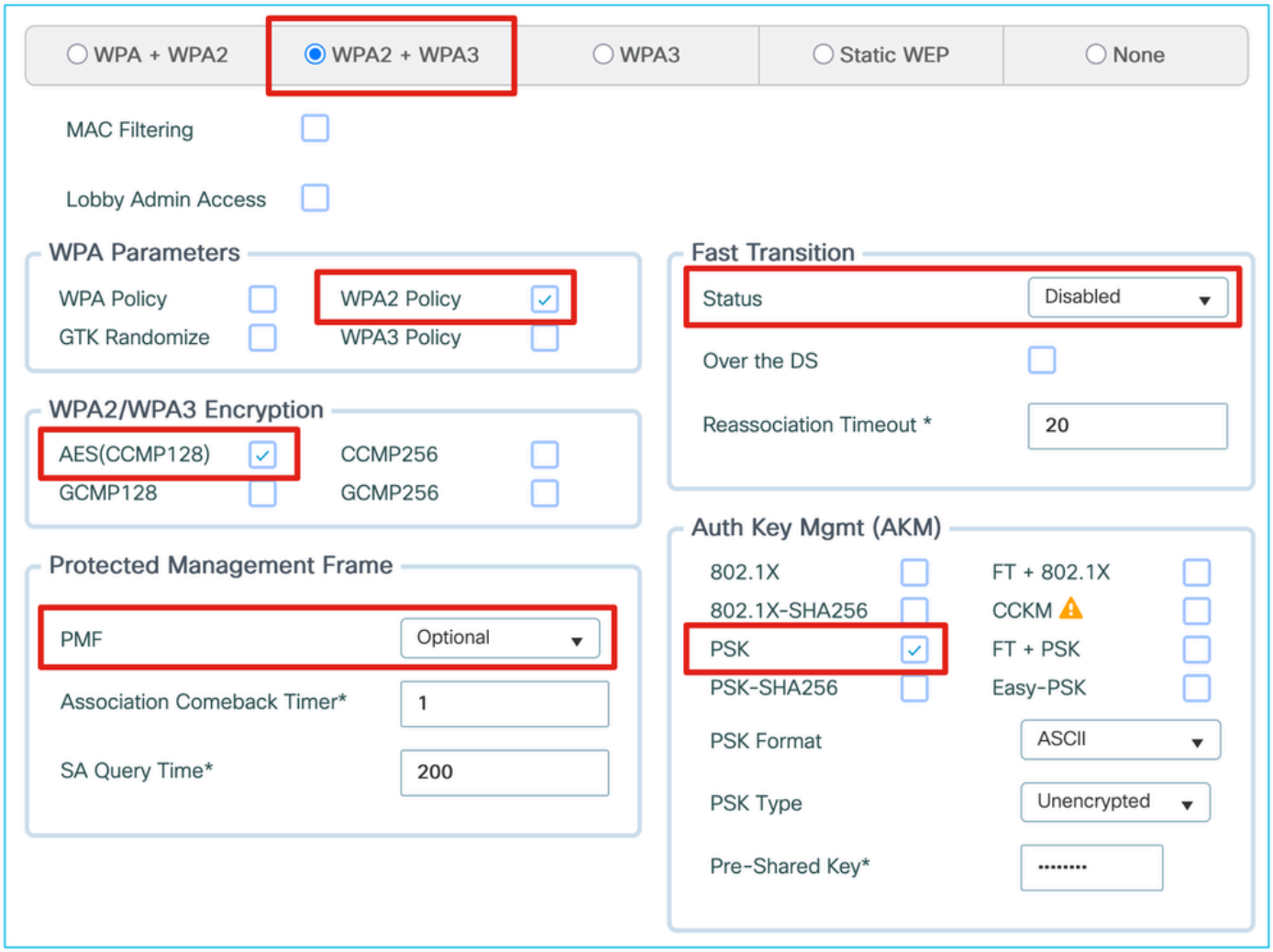
이러한 경우, 최신 Wi-Fi 6E 및 Wi-Fi 7 클라이언트에 대해 AES(CCMP128) 및 GCMP256 암호를 모두 제공하는 전용 WPA3 전용 SSID를 SAE, FT + SAE, SAE-EXT-KEY 및 FT + SAE-EXT-KEY로 구성해야 합니다.


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



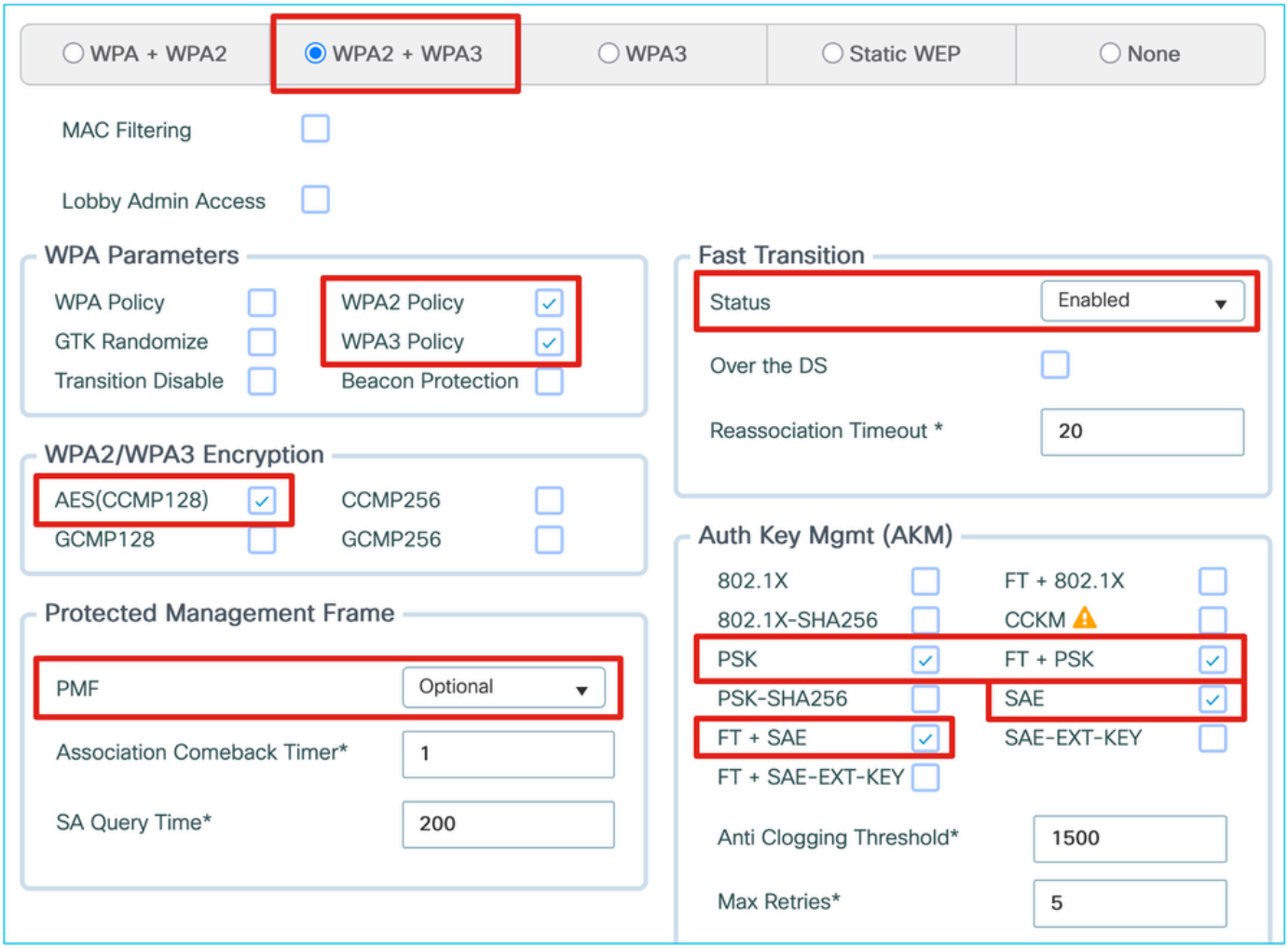
참고: WLAN에서 (FT +) SAE가 활성화되어 있고 Wi-Fi 7 클라이언트가 (FT +) SAE-EXT-KEY 대신 SAE와의 연결을 시도하면 거부됩니다. (FT +) SAE-EXT-KEY도 사용하도록 설정된 경우 Wi-Fi 7 클라이언트는 이 AKM을 나중에 사용해야 하며 이 문제가 발생하지 않아야 합니다.

반면 또 다른 일반 WPA2 SSID는 나머지 레거시 클라이언트를 계속 수용할 수 있습니다.



이 조합은 총 SSID의 양을 증가시키지만, 하나의 SSID에서 최대 호환성을 유지할 수 있습니다. 즉, 호환성에 영향을 줄 수 있고 많은 IoT 시나리오에 도움이 될 수 있는 다른 고급 기능을 잠재적으로 비활성화하는 동시에, 다른 SSID를 통해 최신 장치에 최대 기능과 성능을 제공할 수 있습니다. Wi-Fi 7 SSID를 제공하지 않고 WPA2 PSK 및 WPA3 SAE에 대해 구성된 단일 SSID만 유지하는 옵션이 하나 더 있습니다. IoT 장치는 Wi-Fi 7 성능이 필요하지 않을 수 있다는 것이 그 배경이 될 수 있습니다.

이 접근 방식은 Wi-Fi 6E 및 Wi-Fi 7 지원 클라이언트에 대해 여전히 6GHz를 지원하며, 이는 Wi-Fi 6E 성능에 기껏해야 연결할 수 있습니다.



이 모든 시나리오에서 SAE를 사용할 때는 FT를 활성화하는 것이 좋습니다. SAE 프레임 교환은 리소스 측면에서 비용이 많이 들고 WPA2 PSK 4방향 핸드셰이크보다 깁니다.

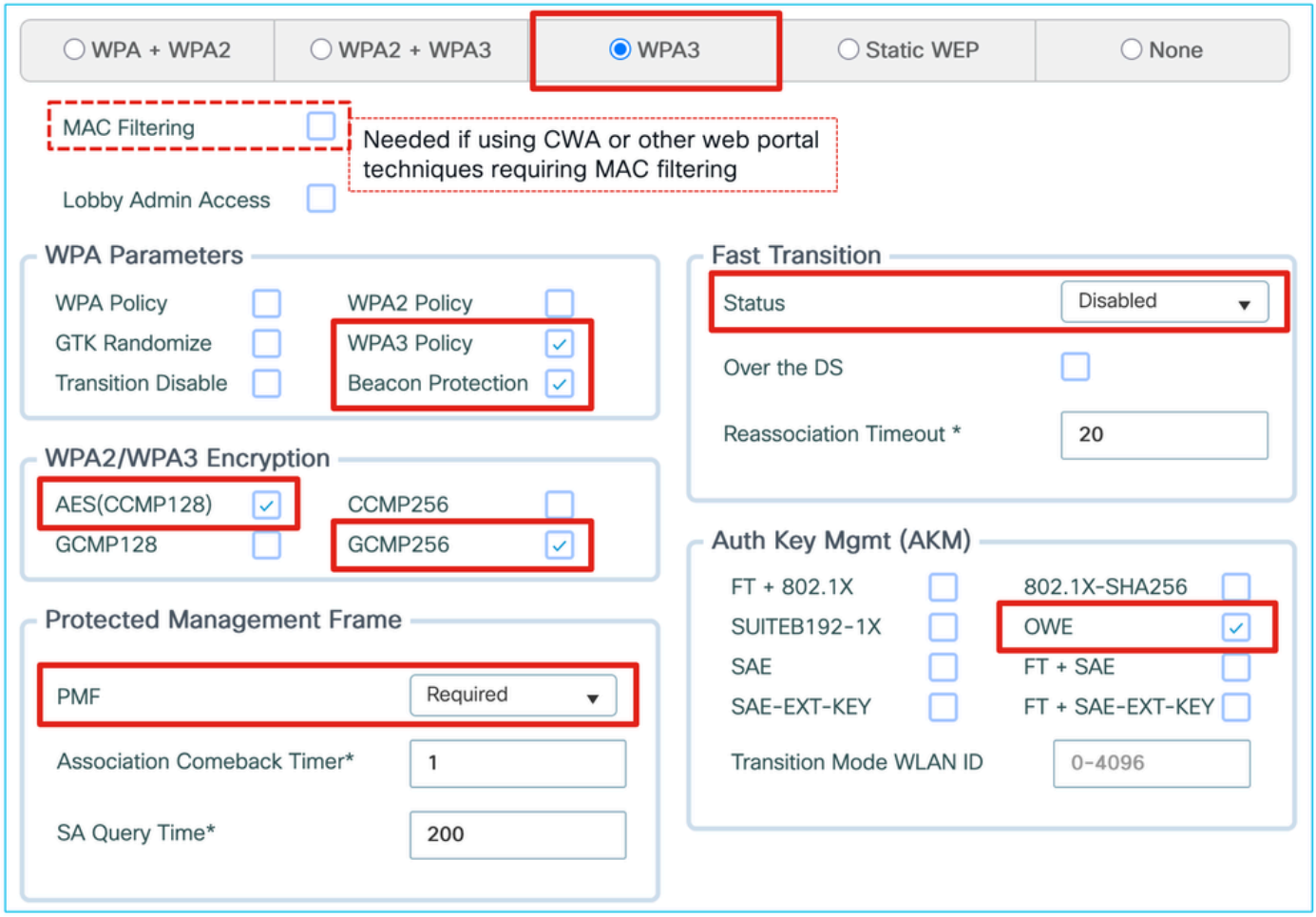
Apple과 같은 일부 디바이스 제조업체는 FT가 활성화된 경우에만 SAE를 사용할 것으로 예상하며, 사용 불가능한 경우 연결을 거부할 수 있습니다.

개방형/향상된 개방형/OWE/게스트 네트워크

게스트 네트워크는 다양한 방식으로 제공됩니다. 일반적으로 연결할 때 802.1X 자격 증명이나 암호가 필요하지 않으며, 자격 증명이나 코드가 필요할 수 있는 스플래시 페이지나 포털을 의미할 수도 있습니다. 이는 일반적으로 개방형 SSID 및 로컬 또는 외부 게스트 포털 솔루션으로 처리됩니다. 그러나 6GHz 또는 Wi-Fi 7 지원에서는 개방형 보안(암호화 없음)을 사용하는 SSID가 허용되지 않습니다.

매우 보수적인 첫 번째 접근 방식은 기껏해야 게스트 네트워크를 5GHz 대역 및 Wi-Fi 6에 할당하는 것입니다. 따라서 6GHz 대역은 기업 장치에 맞게 남겨두며, 최대 Wi-Fi 6E/7 성능은 아니지만 복잡성 문제를 해결하고 최대 호환성을 제공합니다.

게스트에게 6GHz 서비스를 제공하려면 Enhanced Open/OWE(Opportunistic Wireless Encryption)를 사용하여 별도의 SSID를 생성하는 것이 좋습니다. 최대 Wi-Fi 6E 클라이언트와의 호환성을 위해 AES(CCMP128) 암호를 모두 제공할 수 있을 뿐만 아니라 Wi-Fi 7 지원 클라이언트를 위한 GCMP256 비트를 제공할 수 있습니다.



Enhanced Open이 "개방형" 환경을 유지하면서 개인 정보를 제공하는 훌륭한 보안 방법이라면(최종 사용자가 802.1X 자격 증명 또는 암호를 입력할 필요가 없음), 현재까지도 엔드포인트 간에 지원이 제한되어 있습니다. 일부 클라이언트는 여전히 이를 지원하지 않으며, 심지어 지원하더라도 이 기술은 항상 원활하게 처리되지 않습니다(디바이스는 연결을 안전하지 않은 것으로 표시할 수 있지만 실제로 안전하거나, OWE와 함께 암호가 필요하지 않은 경우에도 암호로 보호되는 것으로 표시할 수 있음). 게스트 네트워크는 모든 게스트 비제어 디바이스에서 작동해야 하므로 Enhanced Open SSID만 제공하기에는 너무 이르며 별도의 SSID를 통해 두 옵션을 모두 제공하는 것이 좋습니다. 5GHz에서 열린 포털과 5GHz 및 6GHz에서 하나의 OWE를 활성화했으며 둘 다 종속 포털이 있어야 합니다. 전환 모드는 Wi-Fi 6E, 6GHz(소프트웨어에서 계속 허용될 수 있음) 또는 Wi-Fi 7에서는 지원되지 않으므로 이는 권장되는 솔루션이 아닙니다. 모든 포털 리디렉션 기술(웹 인증 내부 또는 외부, 중앙 웹 인증, ...)은 OWE를 통해 계속 지원됩니다.

추가 WPA3 및 관련 옵션

WPA3 옵션은 WPA3 구축 가이드에서 가장 잘 설명하고 다루지만, 이 섹션에서는 특히 6GHz 및 Wi-Fi 7 지원과 관련된 WPA3에 대한 몇 가지 추가 권장 사항을 다룹니다.

비컨 보호

이 기능은 취약성을 해결하는 기능으로, 악의적인 공격자가 합법적인 액세스 포인트 대신 비콘을 전송하는 한편 일부 필드를 수정하여 이미 연결된 클라이언트의 보안 또는 기타 설정을 변경할 수 있습니다. 비컨 보호는 비컨 자체의 시그니처 역할을 하는 비컨에 포함된 추가 정보 요소로, 합법적

인 액세스 포인트가 비컨을 보냈음을 입증하고 비컨이 변조되지 않았음을 입증합니다. WPA3 암호화 키를 가진 연결된 클라이언트만 비콘의 합법성을 확인할 수 있으며, 프로빙 클라이언트는 비콘을 확인할 방법이 없습니다. 비컨의 추가 정보 요소는 이를 지원하지 않는 클라이언트(비 Wi-Fi 7 클라이언트)에서 무시해야 하며, 일반적으로 호환성 문제를 나타내지 않습니다(제대로 프로그래밍되지 않은 클라이언트 드라이버가 없는 경우).

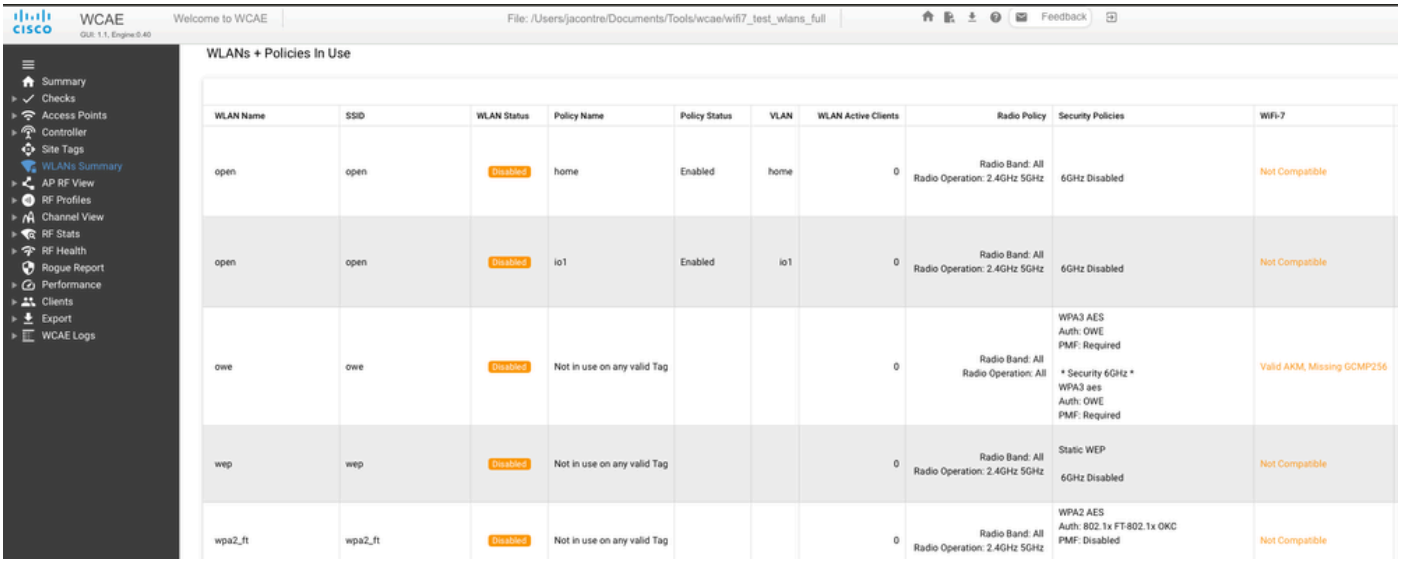
GCMP256

Wi-Fi 7 인증까지는 대부분의 클라이언트가 AES(CCMP128) 암호 암호화를 구현했습니다. CCMP256 및 GCMP256은 SUITE-B 802.1X AKM과 관련된 매우 구체적인 변종입니다. 시중에 나와 있는 일부 1세대 Wi-Fi 7 클라이언트는 Wi-Fi 7 지원을 주장하지만, 여전히 GCMP256 암호화를 구현하지 않을 수 있습니다. Wi-Fi 7 AP가 표준을 예상대로 시행하여 적절한 GCMP256 지원 없이 이러한 클라이언트가 연결되지 않을 경우 문제가 될 수 있습니다.

문제 해결 및 확인

Wireless Configuration Analyzer Express 최신 버전(https://developer.cisco.com/docs/wireless-troubleshooting-tools/wireless-config-analyzer-express-gui/)에는 위에서 언급한 모든 Wi-Fi 7 요구 사항에 대한 9800 컨피그레이션을 평가하는 Wi-Fi 7 준비도 검사가 있습니다.

컨피그레이션이 Wi-Fi 7을 사용할 준비가 되었는지 여전히 의심스러운 경우 WCAE를 통해 무엇이 잘못되었는지 알 수 있습니다.



참조

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.