

# Konfigurieren und Überprüfen des Wi-Fi 6E-Band-Betriebs und der Client-Links

## Inhalt

---

### [Einleitung](#)

### [Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

### [Hintergrundinformationen](#)

[Wi-Fi 6E-Sicherheit](#)

[Cisco Catalyst Wi-Fi 6E APs](#)

### [Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

### [Überprüfung](#)

[Beacon-Änderungen](#)

[Verifizierung](#)

[Multiple Basic Service Set Identifier \(BSSID\)](#)

[Konfigurieren des Multi-BSSID-Profiles \(GUI\)](#)

[Konfigurieren des Multi-BSSID-Profiles \(CLI\)](#)

[Konfigurieren von Multi-BSSID in der RF-Profiloberfläche \(GUI\)](#)

[Konfigurieren mehrerer BSSIDs im RF-Profil \(CLI\)](#)

[Erstellung mehrerer SSIDs](#)

[Verifizierung](#)

[AP-Erkennung durch Wireless-Clients](#)

[Out-of-Band](#)

[In-Band](#)

[FILES](#)

[Konfigurieren von FILS-Erkennungs-Frames im RF-Profil \(GUI\)](#)

[Konfigurieren von FILS-Erkennungs-Frames im RF-Profil \(CLI\)](#)

[Verifizierung](#)

[UPR](#)

[Konfigurieren der Broadcast-Testantwort in der RF-Profiloption \(GUI\)](#)

[Konfigurieren der Broadcast-Sondenantwort im RF-Profil \(CLI\)](#)

[Verifizierung](#)

[PSC](#)

[Bevorzugte Scan-Kanäle in der RF-Profil \(GUI\) konfigurieren](#)

[Bevorzugte Scan-Kanäle im RF-Profil \(CLI\) konfigurieren](#)

[Verifizierung](#)

[6-GHz-Client-Steuerung](#)

[Konfigurieren der 6-GHz-Client-Steuerung im globalen Konfigurationsmodus \(GUI\)](#)

[Konfigurieren der 6-GHz-Client-Steuerung im globalen Konfigurationsmodus \(CLI\)](#)

[Konfigurieren der 6-GHz-Client-Steuerung im WLAN \(GUI\)](#)

[Konfigurieren der 6-GHz-Client-Steuerung im WLAN \(CLI\)](#)

[Verifizierung](#)

# Einleitung

In diesem Dokument wird beschrieben, wie der Wi-Fi 6E-Bandbetrieb konfiguriert wird und was Sie auf verschiedenen Clients erwartet.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Wireless LAN Controller (WLC) 9800
- Cisco Access Points (APs), die Wi-Fi 6E unterstützen.
- IEEE-Standard 802.11ax
- Netzwerk-Tools: Wireshark

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- WLC 9800-CL mit Cisco IOS® XE 17.9.3
- APs: C9136, CW9162 und CW9166.
- Wi-Fi 6E-Clients:
  - Lenovo X1 Carbon Gen11 mit Intel AX211 Wi-Fi 6 und 6E Adapter mit Treiberversion 22.200.2(1).
  - Netgear A8000 Wi-Fi 6 und 6E Adapter mit Treiber v1(0.0.108)
  - Mobiltelefon Pixel 6a mit Android 13;
  - Handy Samsung S23 mit Android 13.
- Wireshark v4.0.6

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Hintergrundinformationen

Das Wichtigste ist, dass Wi-Fi 6E kein völlig neuer Standard ist, sondern eine Erweiterung. Als Basis dient Wi-Fi 6E als Erweiterung des Wireless-Standards Wi-Fi 6 (802.11ax) in das 6-GHz-Frequenzband.

Wi-Fi 6E basiert auf Wi-Fi 6, der neuesten Generation des Wi-Fi-Standards, aber nur Wi-Fi 6E-Geräte und -Anwendungen können im 6-GHz-Band betrieben werden.

Da das 6-GHz-Spektrum neu ist und nur Wi-Fi 6E-Geräte zulässt, weist es keine der alten Probleme auf, die die aktuellen Netzwerke verstopfen.

Es bietet mehr:

- **Kapazität:** In den USA, die von FCC definiert werden, gibt es ein zusätzliches Spektrum von 1200 MHz oder 59 neue Kanäle. Das neue 6-GHz-Band nutzt vierzehn 80-MHz- und sieben 160-MHz-Kanäle. In anderen Ländern können für WiFi 6E andere Frequenzen zugewiesen werden. Für aktuelle Informationen zur Einführung von [Wi-Fi 6E in Ländern, in denen Wi-Fi in 6 GHz \(Wi-Fi 6E\) aktiviert ist](#), lesen Sie bitte den Abschnitt Länder, in denen Wi-Fi 6E aktiviert ist.
- **Zuverlässigkeit:** Wi-Fi 6E bietet einen neuen Standard für Zuverlässigkeit und Vorhersehbarkeit von Verbindungen, der die Lücke zwischen drahtlosen und kabelgebundenen Verbindungen verkürzt. Geräte von Wi-Fi 1 (802.11b) bis Wi-Fi 6 (802.11ax) werden auf 6 GHz nicht unterstützt.
- **Sicherheit:** Wi-Fi Protected Access 3 (WPA3) ist eine zwingende Voraussetzung für das Wi-Fi 6E-Netzwerk und schützt das Netzwerk besser denn je. Da dieses Netzwerk nur für Wi-Fi 6-Produkte verwendet werden soll, gibt es keine veralteten Sicherheitsprobleme. WPA3 bietet neue Authentifizierungs- und Verschlüsselungsalgorithmen für Netzwerke und behebt Probleme, die WPA2 nicht behoben hat. Darüber hinaus implementiert es eine zusätzliche Schutzebene vor Deauthifizierungs- und Dissoziationsangriffen.

#### 6 GHz Band – Total Spectrum 1200 MHz



#### 5 GHz Band – Total Spectrum 500 MHz (180 MHz without DFS)



#### 2.4 GHz Band – Total Spectrum 80 MHz



Vergleich des 2,4-, 5- und 6-GHz-Wi-Fi-Spektrums und der Kanäle

Weitere Hintergrundinformationen zu Wi-Fi 6E finden Sie in unserem [Wi-Fi 6E: The Next Great Chapter im Wi-Fi Whitepaper](#) .

Es gibt verschiedene Management-Optionen und Änderungen in Wi-Fi 6E. Im Abschnitt "Überprüfung" dieses Dokuments finden Sie eine kurze Beschreibung einiger dieser Verbesserungen sowie eine Überprüfung der tatsächlichen Umgebung.

## Wi-Fi 6E-Sicherheit

Wi-Fi 6E erhöht die Sicherheit mit Wi-Fi Protected Access 3 (WPA3) und Opportunistic Wireless Encryption (OWE), und es gibt keine Abwärtskompatibilität mit Open- und WPA2-Sicherheit.

WPA3 und Enhanced Open Security sind jetzt für die Wi-Fi 6E-Zertifizierung obligatorisch, und für Wi-Fi 6E ist auch Protected Management Frame (PMF) sowohl auf dem Access Point als auch auf den Clients erforderlich.

Bei der Konfiguration einer 6-GHz-SSID müssen bestimmte Sicherheitsanforderungen erfüllt werden:

- WPA3 L2-Sicherheit mit OWE, SAE oder 802.1x-SHA256
- Geschützter Management-Frame aktiviert;
- Andere L2-Sicherheitsmethoden sind nicht zulässig, d. h., es ist kein gemischter Modus möglich.

Weitere Informationen zur WPA3-Implementierung in Cisco WLANs, einschließlich der Kompatibilitätmatrix für die Client-Sicherheit, finden Sie im [WPA3-Bereitstellungsfaden](#).

## Cisco Catalyst Wi-Fi 6E APs

Ideal for Small to Medium-sized deployments	Best In Class, Flexibility		Mission Critical, Performance
 <p><b>CW9162</b></p> <ul style="list-style-type: none"> <li>• 2x2 + 2x2 + 2x2</li> <li>• 2.5 Gbps mGig</li> <li>• Power Options: PoE, DC Power</li> <li>• IoT ready + Bluetooth 5.x</li> <li>• Partial iCAP</li> <li>• USB - 4.5 W</li> </ul> <p><small>Available with IOS-XE 17.9.2</small></p>	 <p><b>CW9164</b></p> <ul style="list-style-type: none"> <li>• 2x2, 4x4, 4x4</li> <li>• 2.5 Gbps mGig</li> <li>• Power Options: PoE, DC Power</li> <li>• IoT Ready + Bluetooth 5.x</li> <li>• Partial iCAP</li> <li>• USB- 4.5 W</li> </ul>	 <p><b>CW9166</b></p> <ul style="list-style-type: none"> <li>• 4x4 + 4x4 + 4x4 (XOR 5/6)</li> <li>• 5 Gbps mGig</li> <li>• Power Options: PoE, DC Power</li> <li>• IoT ready + Bluetooth 5.x</li> <li>• Environmental Sensor</li> <li>• Full Packet Capture (iCAP)</li> <li>• Zero-Wait DFS*</li> <li>• USB - 4.5W</li> </ul>	 <p><b>C9136</b></p> <ul style="list-style-type: none"> <li>• 4x4, 8x8, 4x4 (or) 4x4, 4x4+4x4, 4x4</li> <li>• Dual 5 Gbps mGig, active fail over</li> <li>• PoE Redundancy</li> <li>• IoT ready</li> <li>• Bluetooth 5.x</li> <li>• Environmental Sensor</li> <li>• Full Packet Capture (iCAP)</li> <li>• Zero-Wait DFS*</li> <li>• USB - 9W</li> </ul> <p><small>*Available in Future</small></p>
Full radio capability (6 GHz @ LPI) on single 30W PoE+			
Dedicated Radio for CleanAir Pro	Same Bracket, Industrial Design	AP Power Optimization	USB

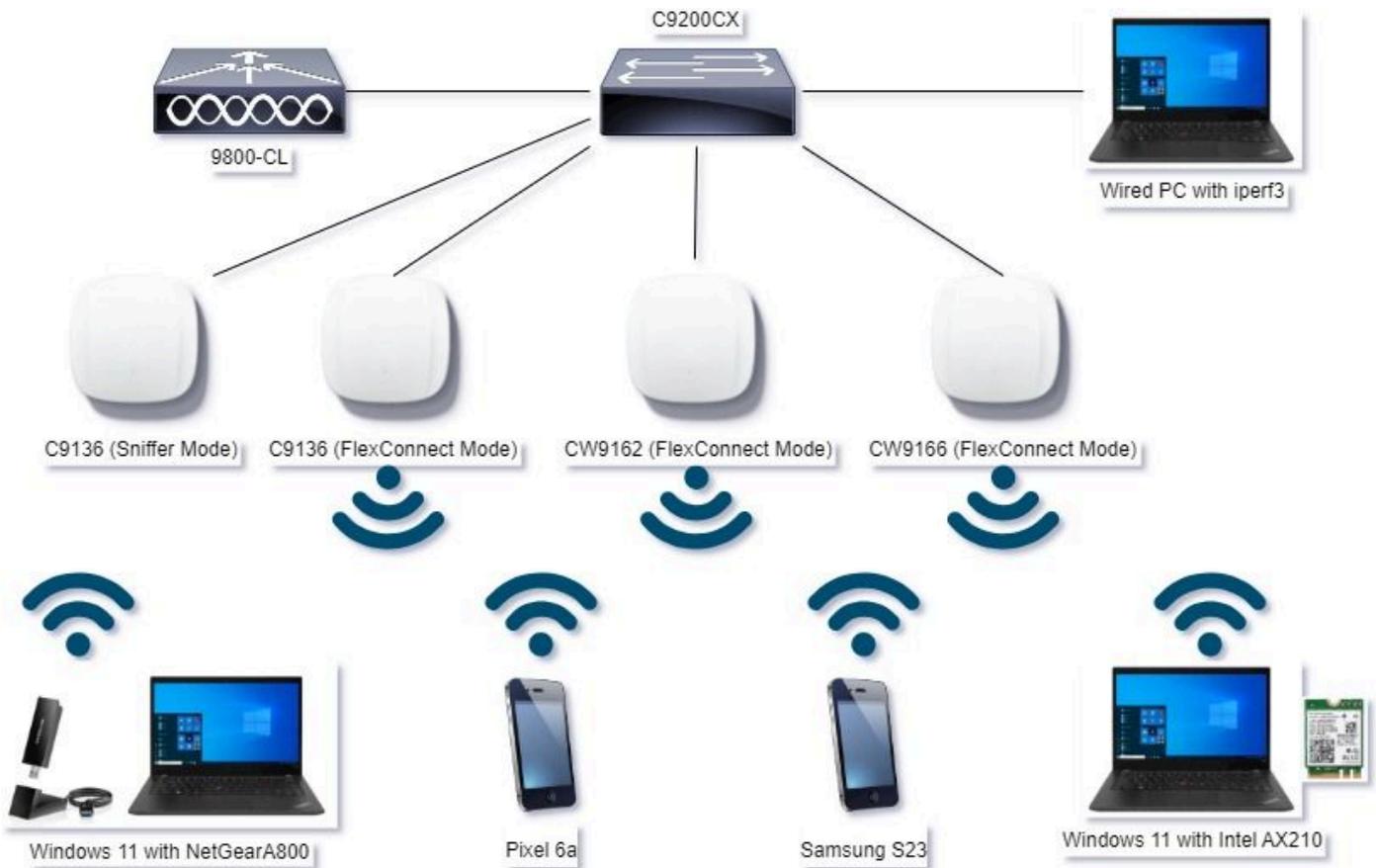
Wi-Fi 6E Access Points

## Konfigurieren

In diesem Abschnitt wird die grundlegende WLAN-Konfiguration beschrieben. Später im Dokument wird beschrieben, wie die einzelnen Wi-Fi 6E-Elemente konfiguriert werden und wie die

Konfiguration und das erwartete Verhalten überprüft werden.

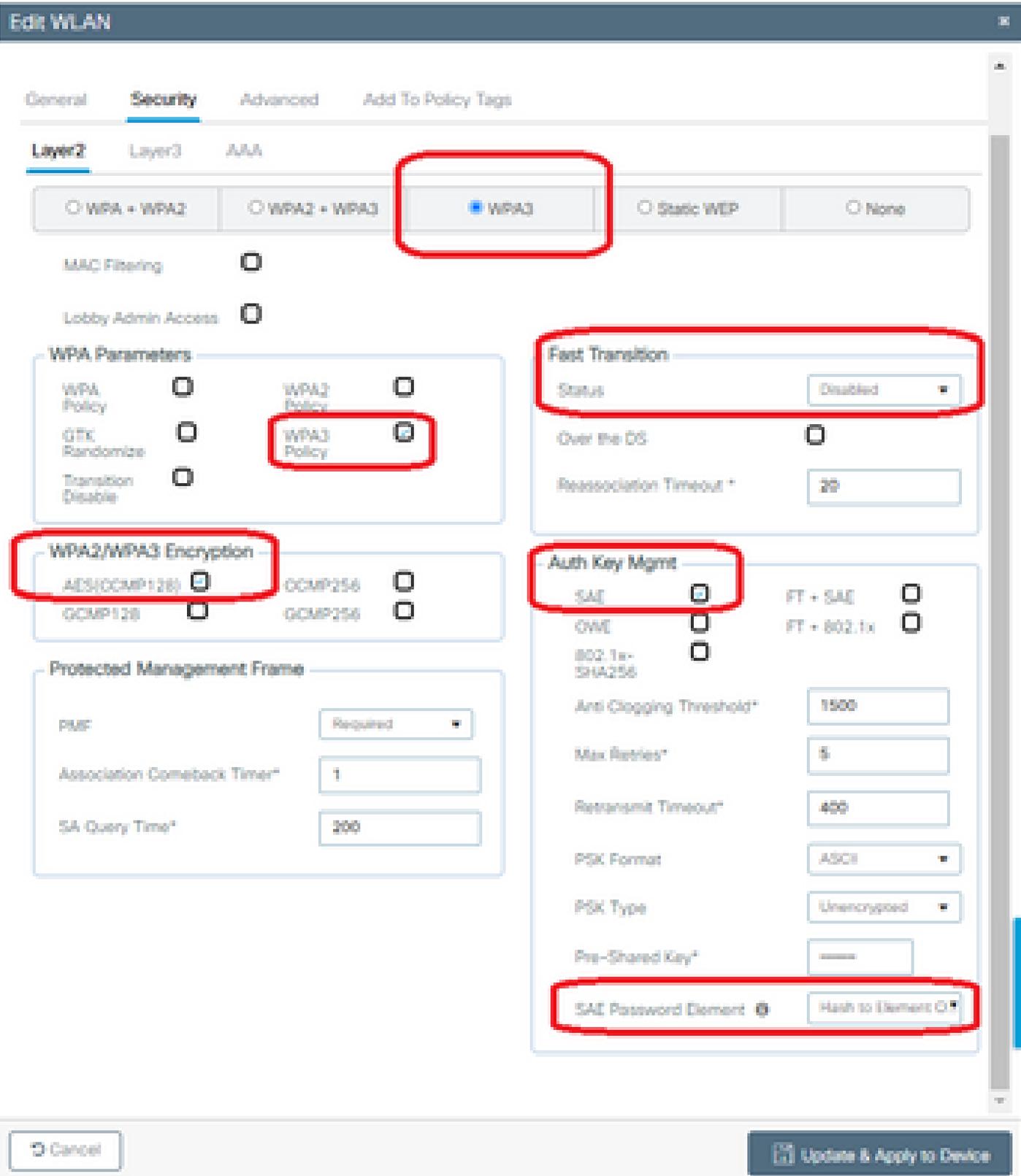
## Netzwerkdiagramm



Netzwerkdiagramm

## Konfigurationen

In diesem Dokument ist die anfängliche WLAN-basierte Sicherheitskonfiguration WPA3+AES+SAE mit H2E, wie hier gezeigt:



Die WLAN-Konfiguration und das Push an die APs erfolgen gemäß den Schritten im Abschnitt [How to Configure WLANs](#) from the Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS® XE Cupertino 17.9.x.

Das WLAN ist einem lokal geschalteten Richtlinienprofil mit Switching- und Authentifizierungsrichtlinie zugeordnet, wie hier gezeigt:

⚠ Disabling a Policy or configuring it in "Enabled" state, will result in loss of connectivity for clients associated with this Policy profile.

General Access Policies QOS and AVC Mobility Advanced

Name*	Policy4TiagoHome	WLAN Switching Policy	
Description	ProductionPolicy	Central Switching	<input type="checkbox"/> DISABLED
Status	<input checked="" type="checkbox"/> ENABLED	Central Authentication	<input type="checkbox"/> DISABLED
Passive Client	<input type="checkbox"/> DISABLED	Central DHCP	<input type="checkbox"/> DISABLED
IP MAC Binding	<input checked="" type="checkbox"/> ENABLED	Flex NAT/PAT	<input type="checkbox"/> DISABLED

## Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Der Verifizierungsbereich ist in neue Änderungen oder Funktionen und ggf. Beobachtungen nach Kundentyp unterteilt.

Für jede Funktion gibt es einen Abschnitt "Konfiguration und Verifizierung".

In diesen Tests und Verifizierungen wurden die Over-the-Air-Captures (OTAs) mit einem AP im Sniffer-Modus durchgeführt.

In diesem Artikel erfahren Sie, wie Sie einen Access Point im Sniffer-Modus einrichten: [APs Catalyst 91xx im Sniffer-Modus](#).

## Beacon-Änderungen

Beacons existieren weiterhin auf Wi-Fi 6E und werden standardmäßig alle 100 ms gesendet, sie unterscheiden sich jedoch geringfügig von den Wi-Fi 6-Beacons (2,4 GHz oder 5 GHz). In Wi-Fi 6 enthält das Beacon HT- und VHT-Informationselemente, in Wi-Fi 6E werden diese jedoch entfernt, und es gibt nur das HE-Informationselement.

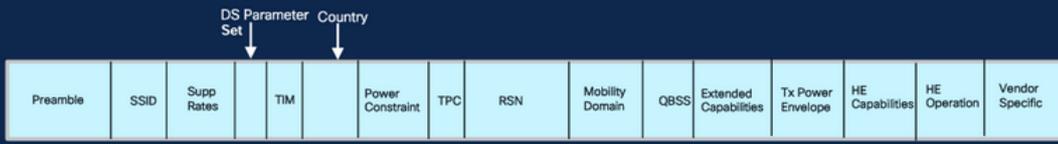
# Legacy HT/VHT Information Element Removed

## Wi-Fi 6 Beacon



## Comparison of Wi-Fi 6 and Wi-Fi 6E Beacon Frame

## Wi-Fi 6E Beacon



## Reduced Beacon Size

Vergleich von Wi-Fi 6 und Wi-Fi 6E Beacon Frames

## Verifizierung

Folgendes können wir in der OTA sehen:

```

> Frame 10: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits) on interface \Device\NPF_{04578985-2998-4456-8C33-C343166}
> Ethernet II, Src: Cisco_0d:7d:37 (08:0f:1d:dd:7d:37), Dst: Universa_b7:cf:06 (08:3a:88:b7:cf:06)
> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AirPeeek/OmniPeek encapsulated IEEE 802.11
< IEEE 802.11 radio information
  PHY type: 802.11a (OFDM) (5)
  Data rate: 12.0 Mb/s
  Channel: 64
  Signal strength (percentage): 67%
  Signal strength (dBm): -28 dBm
  Noise level (percentage): 67%
  Noise level (dBm): -95 dBm
  Signal/noise ratio (dB): 67 dB
  TSF timestamp: 63436667884472
  > [Duration: 292us]
  > IEEE 802.11 Beacon frame, Flags: .....C
  > IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  > Tagged parameters (362 bytes)
  > Tag: SSID parameter set: "wifi6e_test"
  > Tag: Supported Rates 6, 9, 12(8), 18, 24, 36, 48, 54, [Mbit/sec]
  > Tag: DS Parameter set: Current Channel: 64
  > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
  > Tag: Country Information: Country Code PT, Environment Global operating classes
  > Tag: Power Constraint: 3
  > Tag: TPC Report Transmit Power: 18, Link Margin: 0
  > Tag: RSN Information
  > Tag: QBSS Load Element 802.11e CCA Version
  > Tag: RH Enabled Capabilities (5 octets)
  > Tag: HT Capabilities (802.11n D1.10)
  > Tag: HT Information (802.11n D1.10)
  > Tag: Extended Capabilities (11 octets)
  > Tag: VHT Capabilities
  > Tag: VHT Operation
  > Tag: Tx Power Envelope
  > Tag: Reduced Neighbor Report
  > Ext Tag: HE Capabilities
  > Ext Tag: HE Operation
  > Ext Tag: Spatial Reuse Parameter Set
  > Ext Tag: MU ECCA Parameter Set
  > Tag: RSN extension (1 octet)
  > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
  > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (44)
  > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (11) (11)
  > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Client MFP Disabled
  > Tag: Vendor Specific: Cisco Systems, Inc: Aironet CCX version = 5
    
```

```

> Frame 5: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits) on interface \Device\NPF_{04578985-2998-4456-8C33-C343166}
> Ethernet II, Src: Cisco_0d:7d:37 (08:0f:1d:dd:7d:37), Dst: Universa_b7:cf:06 (08:3a:88:b7:cf:06)
> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AirPeeek/OmniPeek encapsulated IEEE 802.11
< IEEE 802.11 radio information
  PHY type: 802.11g (ERP) (6)
  Data rate: 6.0 Mb/s
  Channel: 5
  Signal strength (percentage): 60%
  Signal strength (dBm): -35 dBm
  Noise level (percentage): 60%
  Noise level (dBm): -95 dBm
  Signal/noise ratio (dB): 60 dB
  TSF timestamp: 62165356724611
  > [Duration: 420us]
  > IEEE 802.11 Beacon frame, Flags: .....C
  > IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  > Tagged parameters (256 bytes)
  > Tag: SSID parameter set: "wifi6e_test"
  > Tag: Supported Rates 6(8), 9, 12(8), 18, 24(8), 36, 48, 54, [Mbit/sec]
  > Tag: Traffic Indication Map (TIM): DTIM 2 of 3 bitmap
  > Tag: Country Information: country code na, Environment Global operating classes
  > Tag: Power Constraint: 6
  > Tag: TPC Report Transmit Power: 17, Link Margin: 0
  > Tag: RSN Information
  > Tag: QBSS Load Element 802.11e CCA Version
  > Tag: RH Enabled Capabilities (5 octets)
  > Tag: Extended Capabilities (11 octets)
  > Tag: Tx Power Envelope
  > Tag: Tx Power Envelope
  > Ext Tag: Multiple BSSID Configuration
  > Ext Tag: HE Capabilities
  > Ext Tag: HE Operation
  > Ext Tag: Spatial Reuse Parameter Set
  > Ext Tag: MU ECCA Parameter Set
  > Ext Tag: HE 6 GHz Band Capabilities
  > Tag: RSN extension (1 octet)
  > Tag: Vendor Specific: Atheros Communications, Inc.: Unknown
  > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
  > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (44)
  > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (11) (11)
  > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Client MFP Disabled
  > Tag: Vendor Specific: Cisco Systems, Inc: Aironet CCX version = 5
    
```



Hinweis: Der DS-Parametersatz ist ein optionales Feld und kann nicht in die Beacon-Frames aufgenommen werden.

---

## Multiple Basic Service Set Identifier (BSSID)

Multiple BSSID ist eine ursprünglich in 802.11v festgelegte Funktion. Es kombiniert mehrere SSID-Informationen in einem einzelnen Beacon-Frame, d. h., anstelle eines Beacons für jede SSID sendet es ein einzelnes Beacon, das verschiedene BSSIDs enthält.

Dies ist in Wi-Fi 6E vorgeschrieben, und das Hauptziel ist die Erhaltung der Funkzeit.

### Konfigurieren des Multi-BSSID-Profiles (GUI)

Schritt 1 - Wählen Sie Configuration > Tags & Profiles > Multi BSSID.

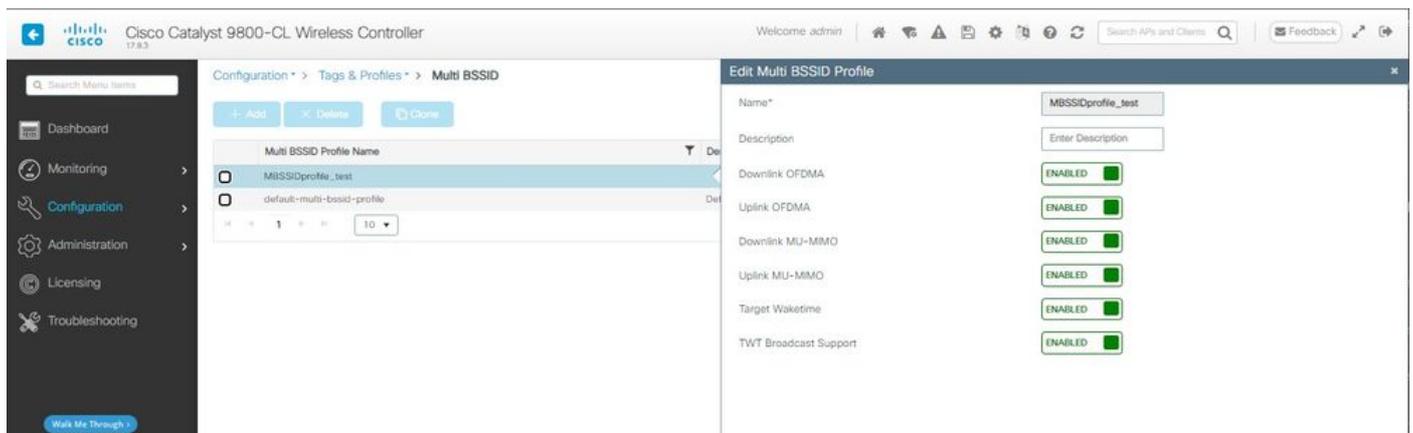
Schritt 2 - Klicken Sie auf Hinzufügen. Die Seite "Multi-BSSID-Profil hinzufügen" wird angezeigt.

Schritt 3 - Geben Sie den Namen und die Beschreibung des BSSID-Profiles ein.

Schritt 4 - Aktivieren Sie die folgenden 802.11ax-Parameter:

- Downlink von OFDMA
- Uplink OFDMA
- Downlink MU-MIMO
- Uplink-MU-MIMO
- Ziel-Waketime
- TWT-Broadcast-Unterstützung

Schritt 5 - Klicken Sie auf Auf Gerät anwenden.



## Konfigurieren des Multi-BSSID-Profiles (CLI)

```
Device# configure terminal
Device (config)# wireless profile multi-bssid multi-bssid-profile-name
Device (config-wireless-multi-bssid-profile)# dot11ax downlink-mumimo
```

## Konfigurieren von Multi-BSSID in der RF-Profiloberfläche (GUI)

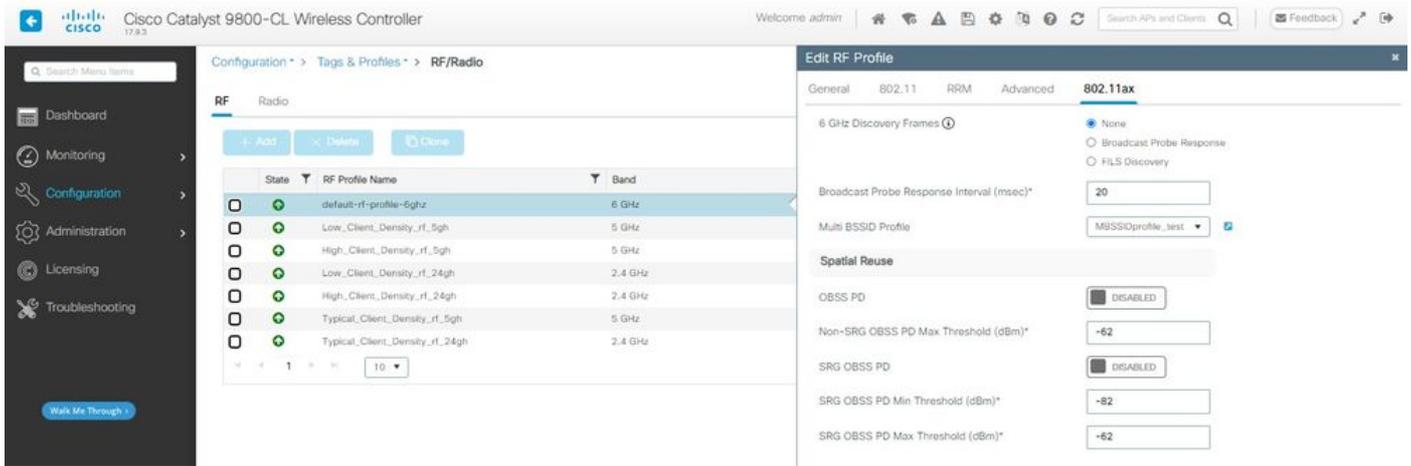
Schritt 1 - Wählen Sie Configuration > Tags & Profiles > RF/Radio.

Schritt 2 - Klicken Sie auf der Registerkarte RF auf Hinzufügen. Die Seite "RF-Profil hinzufügen" wird angezeigt.

Schritt 3: Wählen Sie die Registerkarte 802.11ax aus.

Schritt 4 - Wählen Sie im Feld Multi BSSID Profile (MultiBSSID-Profil) das Profil aus der Dropdown-Liste aus.

Schritt 5 - Klicken Sie auf Auf Gerät anwenden.

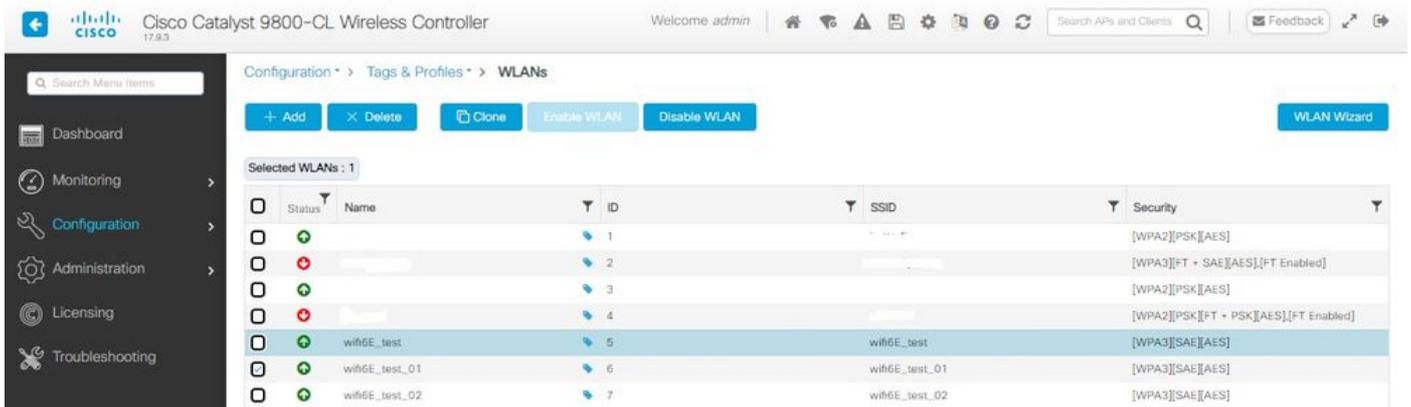


## Konfigurieren mehrerer BSSIDs im RF-Profil (CLI)

```
Device# configure terminal
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
Device(config-rf-profile)# dot11ax multi-bssid-profile multi-bssid-profile-name
```

## Erstellung mehrerer SSIDs

Um die MBSSID-Funktion zu überprüfen, müssen verschiedene SSIDs aktiviert und an die APs übertragen werden. Bei dieser Verifizierung werden drei SSIDs verwendet:



## Verifizierung

Führen Sie die folgenden Befehle aus, um zu überprüfen, ob die Konfiguration bereits vorhanden ist:

```
<#root>
```

```
WLC9800#
```

```
show ap rf-profile name default-rf-profile-6ghz detail | b 802.11ax
```

802.11ax  
 OBSS PD : Disabled  
 Non-SRG OBSS PD Maximum : -62 dBm  
 SRG OBSS PD : Disabled  
 SRG OBSS PD Minimum : -82 dBm  
 SRG OBSS PD Maximum : -62 dBm  
 Broadcast Probe Response : Disabled  
 FILS Discovery : Disabled  
 Multi-BSSID Profile Name :

MBSSIDprofile\_test

NDP mode : Auto  
 Guard Interval : 800ns  
 PSC Enforcement : Disabled

WLC9800#  
 WLC9800#

show wireless profile multi-bssid detailed MBSSIDprofile\_test

Multi bssid profile name :

MBSSIDprofile\_test

-----  
 Description :  
 802.11ax parameters  
 OFDMA Downlink : Enabled  
 OFDMA Uplink : Enabled  
 MU-MIMO Downlink : Enabled  
 MU-MIMO Uplink : Enabled  
 Target Waketime : Enabled  
 TWT broadcast support : Enabled

WLC9800#

Folgendes können Sie in den OTA-Aufnahmen bei Verwendung von Single BSSID sehen:

The screenshot shows a Wireshark capture of IEEE 802.11 Beacon frames. The interface is split into three panes: a packet list, a packet bytes, and a packet details pane. The packet details pane is expanded to show the 'Tagged parameters (256 bytes)' section of a selected beacon frame. This section contains several tags, including:

- Tag: SSID parameter set (0)
- Tag: Multiple BSSID configuration
- Tag: Supported Rates (6)
- Tag: Traffic Indication Map (TIM)
- Tag: Country Information
- Tag: TPC report transmit power
- Tag: QoS Load Element
- Tag: Extended Capabilities (5 octets)
- Tag: TX Power Envelope
- Tag: TX Power Envelope

The 'Tag: Multiple BSSID configuration' tag is highlighted with a red box in the image, indicating its significance in the context of the question.

Folgendes können Sie in den OTA-Aufnahmen sehen, wenn Sie mehrere BSSIDs verwenden:

The screenshot displays a Wireshark capture of 802.11 Beacon frames. The packet list pane shows a series of frames from source 00:00:00:00:00:00 to destination FF:FF:FF:FF:FF:FF. The details pane for one of these frames is expanded to show the IEEE 802.11 Wireless Management section. Key elements include:

- Tag: Multiple BSSID:** Indicates the presence of multiple BSSIDs.
  - Tag Number: Multiple BSSID (71)
  - Tag Length: 140
  - Max BSSID Indicator: 6
  - Subelement: Nontransmitted BSSID Profile (8)
  - Subelement ID: Nontransmitted BSSID Profile (8)
  - Length: 78
  - Nontransmitted Profile: 380211580077966609445574657345F3825580402004010100000fac04010000
  - Tag: Non Transmitted BSSID Capability
  - Tag: SSID parameter set: "wifi6e\_test\_01"
  - Tag: Multiple BSSID Index
  - Tag: RSN Information
  - Tag: RSN extension (1 octet)
  - Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (44)
  - Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (11) (11)
  - Subelement: Nontransmitted BSSID Profile (8)
  - Subelement ID: Nontransmitted BSSID Profile (8)
  - Length: 78
  - Nontransmitted Profile: 380211580077966609445574657345F3825580402004010100000fac04010000
  - Tag: Non Transmitted BSSID Capability
  - Tag: SSID parameter set: "wifi6e\_test\_02"
  - Tag: Multiple BSSID Index
  - Tag: RSN Information
  - Tag: RSN extension (1 octet)
  - Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (44)
  - Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (11) (11)
- Tag: SSID parameter set: "wifi6e\_test":** Shows the SSID for the active BSSID.
- Ext Tag: Multiple BSSID Configuration:**
  - Tag Number: Element ID Extension (255)
  - Ext Tag Length: 2
  - Ext Tag Number: Multiple BSSID Configuration (55)
  - BSSID Count: 3
  - Full Set Rx Periodicity: 1

## AP-Erkennung durch Wireless-Clients

Die Erkennung ist der Prozess, bei dem ein Client-Gerät beim Einschalten oder Betreten eines Gebäudes einen geeigneten Access Point für die Verbindung findet.

Die einfachste Methode zur Erkennung, die heutzutage von den meisten Client-Geräten verwendet wird, besteht darin, Kanäle nacheinander durch die Übertragung einer oder mehrerer Anfragen zu durchsuchen. Anschließend werden Antworten von Access Points im Bereich abgefragt, die Anfragen untersucht, um festzustellen, ob eine der SSIDs mit Profilen im Client übereinstimmt, und anschließend wird der nächste Kanal durchsucht.

Dies hat drei Nachteile:

- Es benötigt viel Zeit, was sich auf die Anwendungsleistung auswirken kann, während sich das Funkgerät nicht im eigenen Kanal befindet.
- Es erfordert viele Frames für die Abfrage und Antwort auf der Funkverbindung, wodurch die Effizienz der Funkübertragung verringert wird.
- Die Akkulaufzeit des Clients wird beeinflusst.

Die Zeit - in der Größenordnung von 20 ms pro Nicht-DFS-Kanal oder bis zu 100 ms auf DFS-Kanal - ist bereits ein Problem im 5 GHz-Band. Noch bedeutsamer wird es, wenn man bedenkt, dass ein Wi-Fi 6E-Client jeden der 59 möglichen 20-MHz-Kanäle im Band scannen muss, um alle verfügbaren Access Points zu erkennen.

Die alten Methoden, die passives Scannen und aktives Scannen, nicht auf 6 GHz skalieren. Bei 2,4 und 5 GHz wird die Methode "hunt-and-see" verwendet, um BSSIDs oder APs entweder durch passives Scannen oder aktives Scannen zu scannen:



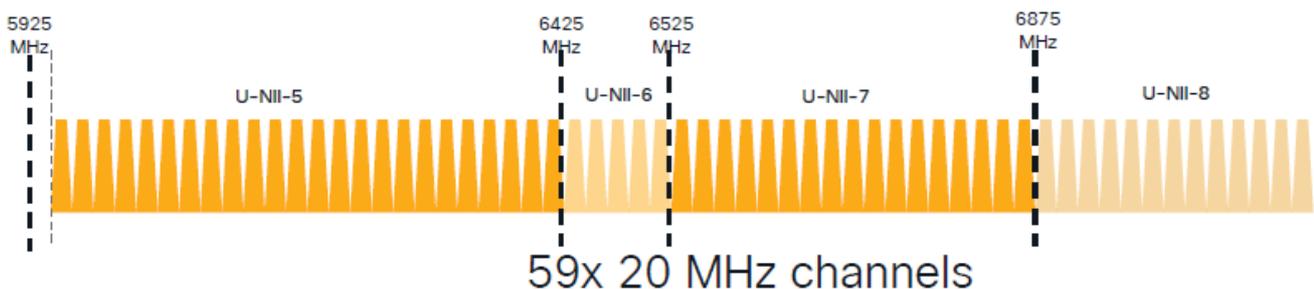
Bisher kommunizieren Wireless-Geräte mit Access Points in einem spezifischen Informationsaustausch. Client-Geräte verwenden einen aktiven "Hunt-and-Seek"-Ansatz, um nach APs in der Nähe zu suchen.

Dieser aktive Scanansatz umfasst das Senden von Testanforderungs-Frames entlang des Frequenzspektrums von 2,4 GHz und 5 GHz. Ein WAP würde mit einem Anfrage-Antwort-Frame antworten, der alle erforderlichen grundlegenden Service Set (BSS)-Informationen enthält, um eine Verbindung mit dem Netzwerk herzustellen.

Diese Informationen bestehen unter anderem aus SSID, BSSID, Kanalbreite und Sicherheitsinformationen.

Dieser aktive "Hunt-and-Seek"-Ansatz bei der Netzwerkkonnektivität ist nicht mehr erforderlich und wird im Wi-Fi 6E-Bereich im 6-GHz-Band sogar abgeschreckt, da es jetzt ineffizient ist, dieselben Anfragen über so viele Kanäle zu senden.

Wi-Fi-Clients können nur Prüfanforderungen auf 20-MHz-Kanälen senden, und auf 6-GHz-Kanälen gibt es bis zu 59 x 20 MHz, was bedeutet, dass der Client alle 59 Kanäle scannen muss, was ca. 6 Sekunden bedeutet, um alle 59 Kanäle passiv zu scannen:



Auf Wi-Fi 6E gibt es neue AP-Erkennungsmechanismen:

## Out of Band

### Reduced Neighbor Report

*Co-located Discovery*



## In Band

### Passive Scan:

Fast Link Setup (FILS) Discovery Frames  
Unsolicited Probe Response Frames

### Active Scan:

Preferred Scanning Channels (PSC)



Zum Zeitpunkt der Erstellung dieses Dokuments unterstützten die getesteten Windows-/Intel- und Android-Clients FILS und Broadcast-Anfragen, jedoch war dies bei Apple und einigen Android-Clients, die möglicherweise keine FILS oder Broadcast-Anfragen unterstützen, nicht der Fall. Aufgrund dieses Problems wird ein bevorzugter Scan-Kanal (PSC) als relevanter betrachtet. Da derzeit jedoch verschiedene Anbieter von Wireless-Clients nicht vollständig mit dem Wi-Fi 6-Scanning kompatibel sind, kann es nicht der ideale Ansatz sein, nur 6ghz wlan/ssid zu konfigurieren.



Hinweis: Wenn Sie wissen möchten, welchen Erkennungsmechanismus jeder Client unterstützt, müssen Sie sich an den Support des Wireless-Client-Anbieters wenden.

---

Basierend auf der Unterstützung von Wireless-Client-Anbietern ist es derzeit möglich, eine Out-of-Band-Erkennung durchzuführen, bei der 2,4/5 GHz für eine RNR/Reduced Neighbor Report-Option aktiviert ist, bei der Wireless-Clients eine 6-GHz-SSID auf einem Access Point entdecken können, indem sie auf das RNR-Informationselement hören, das in den 2,4/5-GHz-Beacons dieses Access Points enthalten ist.

Es ist sehr unwahrscheinlich, dass ein WLC und ein AP NUR ein 6-GHz-WLAN bereitstellen. Wahrscheinlich werden auch andere WLANs ausgestrahlt. In Anbetracht dessen empfiehlt die Kommission, diese Legacy-Bänder zu verwenden, um im RNR-Informationselement für Client-Geräte, die Inband-Erkennungsmechanismen nicht unterstützen, nur die 6-GHz-WLANs anzukündigen.

Letztlich entsteht kein zusätzlicher Konfigurationsaufwand, da die RNR eine Funktion ist, die

bereits von Wi-Fi 6E-Geräten unterstützt wird und daher von Wi-Fi 6E-Geräten unterstützt wird.

## Out-of-Band

Die Out-of-Band-Erkennung wird für die Kommunikation zwischen allen drei Frequenzbändern (2,4, 5 und 6 GHz) verwendet. Diese in 802.11v eingeführte Methode wird als Reduced Neighbor Reporting (RNR) bezeichnet.

Wenn ein Wi-Fi 6E-fähiger WAP ein Anfrage-Antwort-Frame sendet, enthält er (zusammen mit grundlegenden Service Set (BSS)-Informationen für das 2,4- oder 5-GHz-Band) RNR-Informationen über sein 6-GHz-Funkmodul.

Diese RNR-Daten stellen eine ausreichende Informationsmenge dar, damit das Client-Gerät zwischen 6-GHz- und 2,4- oder 5-GHz-Netzwerken wechseln kann.

Zusammenfassung: Clients verwenden nur RNR, um WLANs mit 6 GHz über Legacy-Bänder zu erkennen. 6 GHz wird nicht sofort gescannt.

Wenn wir den Datenverkehr auf 2,4 oder 5 GHz über Funk erfassen und die Testantworten beobachten.

Dies wird beispielsweise bei einer OTA-Erfassung einer Testantwort auf Kanal 1 (2,4 GHz) für eine SSID, die auf 2,4, 5 und 6 GHz ausgestrahlt wird, erwartet:

The image shows a Wireshark packet capture of a probe response (Frame 4867) containing a Reduced Neighbor Report (RNR). The report lists various BSSIDs and their associated channels. Red arrows highlight the TBT (Target BSS Type) and BSS Parameters fields within the report.

No.	Time	Source	Destination	Protocol	Length	Channel	Signal	Info
4867	2023-06-09 14:37:35.920264	0.000000 Cisco,11:00:00	Egress1_771: 002.11	415	1-29 dBm	Probe Response, Shw086, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Frame 4867: 415 bytes on wire (3320 bits), 415 bytes captured (3320 bits) on interface lbrsec0 (vif0) (DAS78905-2998-4456-0)
4868	2023-06-09 14:37:35.920264	0.000042 Cisco,11:00:00	Egress1_771: 002.11	415	1-29 dBm	Probe Response, Shw086, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Ethernet II, Src: Cisco_00:00:00:00:00:00, Dst: Universa_07:c7:c7:c7:c7:c7
4869	2023-06-09 14:37:35.920264	0.000019 Cisco,11:00:00	Egress1_771: 002.11	415	1-29 dBm	Probe Response, Shw086, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.1.121
4870	2023-06-09 14:37:35.920264	0.000700 Cisco,11:00:00	Egress1_771: 002.11	415	1-29 dBm	Probe Response, Shw086, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
4871	2023-06-09 14:37:35.920264	3.150219 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> AirPcap/Compucon encapsulated IEEE 802.11
4872	2023-06-09 14:37:35.920264	0.000167 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> IEEE 802.11 Probe Response, Flags: .....
4873	2023-06-09 14:37:35.920264	0.000038 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> IEEE 802.11 Neighbor Advertisement
4874	2023-06-09 14:37:35.920264	0.000152 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Fixed parameters (12 bytes)
4875	2023-06-09 14:37:35.920264	0.000161 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Tagged parameters (113 bytes)
4876	2023-06-09 14:37:35.920264	0.000275 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Tag: SSID parameter set: "WiFi6E_Test"
4877	2023-06-09 14:37:35.920264	0.000287 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Tag: Supported Rates 54, 6, 9, 12, 18, 24(0), 36, 48, [Mbit/sec]
4878	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Tag: DS Parameter set: Current Channel: 1
4879	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Tag: Country Information: Country Code FR, Environment global operating classes
4880	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Tag: TPC Report Transmit Power: 13, Link Margin: 0
4881	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Tag: ERP Information
4882	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Tag: RSN Information
4883	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Tag: QoS Load Element 802.11e cca version
4884	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Tag: HT Enabled Capabilities (9 octets)
4885	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Tag: HT Capabilities (802.11n D1.0)
4886	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Tag: Extended Capabilities (12 octets)
4887	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Tag: Reduced Neighbor Report
4888	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Tag Number: Reduced Neighbor Report (201)
4889	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Tag Length: 43
4890	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Neighbor AP Information
4891	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> BSSID: 000000000000
4892	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Short SSID: 000000000000
4893	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Channel Number: 5
4894	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Operating Class: 134
4895	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> TBT Information
4896	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Neighbor AP TBT Offset: 255
4897	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> BSS Parameters: Bw4
4898	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> PSD Subfield: 18.0 dBm/MHz
4899	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Neighbor AP TBT Offset: 255
4900	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> BSS Parameters: Bw4
4901	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> PSD Subfield: 18.0 dBm/MHz
4902	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> TBT Information
4903	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Neighbor AP TBT Offset: 255
4904	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> BSSID: 000000000000
4905	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> Short SSID: 000000000000
4906	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> BSS Parameters: Bw4
4907	2023-06-09 14:37:35.920264	0.000334 Cisco,11:00:00	Wistrom_071: 002.11	415	1-29 dBm	Probe Response, Shw087, Flw0, Flags=.....C, E1=100, SSID=WiFi6E_Test		> PSD Subfield: 18.0 dBm/MHz

Wie Sie sehen, meldet der RNR dieselbe SSID auf Kanal 5 mit 6 GHz und zwei anderen BSSIDs.

Dies gilt für dieselbe SSID, aber für eine Antwort mit Probe bei 5 GHz:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
1417	2023-06-09 14:37:10.724295	0.000000	Cisco_13:10:ef	hlstrom_871.. 802.11	404	64	-27 dBm	Probe Response, SNI=99, Fw=0, Flags=.....C, SSID="wlfi6_test"	
1420	2023-06-09 14:37:10.725614	0.001319	Cisco_13:10:ef	hlstrom_871.. 802.11	404	64	-27 dBm	Probe Response, SNI=99, Fw=0, Flags=.....C, SSID="wlfi6_test"	
124	2023-06-09 14:38:07.897585	17.171971	Cisco_13:10:ef	InteICor_021.. 802.11	404	64	-28 dBm	Probe Response, SNI=92, Fw=0, Flags=.....C, SSID="wlfi6_test"	
125	2023-06-09 14:38:08.063911	0.166326	Cisco_13:10:ef	InteICor_021.. 802.11	404	64	-27 dBm	Probe Response, SNI=93, Fw=0, Flags=.....C, SSID="wlfi6_test"	
126	2023-06-09 14:38:08.064436	0.000525	Cisco_13:10:ef	InteICor_021.. 802.11	404	64	-28 dBm	Probe Response, SNI=93, Fw=0, Flags=.....C, SSID="wlfi6_test"	
125	2023-06-09 14:38:08.064470	0.000434	Cisco_13:10:ef	InteICor_021.. 802.11	404	64	-28 dBm	Probe Response, SNI=93, Fw=0, Flags=.....C, SSID="wlfi6_test"	
125	2023-06-09 14:38:08.065420	0.000950	Cisco_13:10:ef	InteICor_021.. 802.11	404	64	-29 dBm	Probe Response, SNI=93, Fw=0, Flags=.....C, SSID="wlfi6_test"	
122	2023-06-09 14:38:10.720409	2.642069	Cisco_13:10:ef	hlstrom_871.. 802.11	404	64	-27 dBm	Probe Response, SNI=94, Fw=0, Flags=.....C, SSID="wlfi6_test"	
133	2023-06-09 14:38:10.720900	0.000481	Cisco_13:10:ef	hlstrom_871.. 802.11	404	64	-28 dBm	Probe Response, SNI=94, Fw=0, Flags=.....C, SSID="wlfi6_test"	
133	2023-06-09 14:38:10.729923	0.001018	Cisco_13:10:ef	hlstrom_871.. 802.11	404	64	-27 dBm	Probe Response, SNI=95, Fw=0, Flags=.....C, SSID="wlfi6_test"	
133	2023-06-09 14:38:10.730449	0.000521	Cisco_13:10:ef	hlstrom_871.. 802.11	404	64	-28 dBm	Probe Response, SNI=95, Fw=0, Flags=.....C, SSID="wlfi6_test"	
134	2023-06-09 14:38:10.732737	0.002288	Cisco_13:10:ef	hlstrom_871.. 802.11	404	64	-27 dBm	Probe Response, SNI=96, Fw=0, Flags=.....C, SSID="wlfi6_test"	

```

> Frame 5417: 404 bytes on wire (3272 bits), 404 bytes captured (3272 bits) on interface l0bvice\NPF_{04579965-2998-4456-B-
> Ethernet II, Src: Cisco_00:17:37_(00:17:37:00:17:37), Dst: Universa_03:cf:fe (00:3a:8b:07:cf:fe)
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.121
> User Datagram Protocol, Src Port: 5593, Dst Port: 5000
> Application/OSpec encapsulated IEEE 802.11
> 802.11 radio information
> IEEE 802.11 Probe Response, Flags: .....C
IEEE 802.11 Wireless Management
> Fixed parameters (42 bytes)
  Tagged parameters (382 bytes)
    > Tag: SSID parameter set: "wlfi6_test"
    > Tag: Supported Rates 6, 9, 12(0), 18, 24, 36, 48, 54, (Mbit/sec)
    > Tag: DS Parameter set: Current Channel: 64
    > Tag: Country Information: Country Code FI, Environment Global operating classes
    > Tag: Power Constraint: 3
    > Tag: TPC Report Transmit Power: 10, Link Margin: 0
    > Tag: RSN Information
    > Tag: QoS Load Element 802.11e CCA Version
    > Tag: M Enabled Capabilities (5 octets)
    > Tag: HT Capabilities (802.11n 01.10)
    > Tag: HT Information (802.11n 01.10)
    > Tag: Extended Capabilities (13 octets)
    > Tag: VHT Capabilities
    > Tag: VHT operation
    > Tag: TX Power Envelope
  > Tag: Reduced Neighbor Report
    Tag Number: Reduced Neighbor Report (20)
    Tag Length: 43
    > Neighbor AP Information
      .... .. -00 -> TBT Information Field: 0
      .... .. 0000 -> TBT Filtered Neighbor AP: 1
      .... .. 0000 -> TBT Information Count: 2
      0000 1000 -> TBT Information Length: Neighbor AP TBT offset subfield, the BSSID subfield, the SN
      OPERATING CLASS: 134
      Channel numbers: 6
    > TBT Information
      Neighbor AP TBT offset: 255
      BSSID: 3091071300ec
      Short SSID: #0d29d1c0
    > BSS Parameters: BSS4
      PSD Subfield: 10.0 dBm/MHz
    > TBT Information
      Neighbor AP TBT offset: 255
      BSSID: 3091071300ed
      Short SSID: #0d274d07
    > BSS Parameters: BSS4
      PSD Subfield: 10.0 dBm/MHz
    > TBT Information
      Neighbor AP TBT offset: 255
      BSSID: 3091071300ef
      Short SSID: #0a6ef625
    > BSS Parameters: BSS4
      PSD Subfield: 10.0 dBm/MHz
  
```

## In-Band

Die In-Band-Erkennung wird für die Kommunikation zwischen 6-GHz-Geräten verwendet. Es gibt drei Methoden für die In-Band-Erkennung:

- Fast Initial Link Setup (FILS) und Unsolicited Probe Response (UPR)-Frames sind zwei passive Methoden der In-Band-Erkennung. Es handelt sich um FILS oder UPR und nicht um beides. 6-GHz-Discovery-Frames werden nur benötigt, wenn nur das 6-GHz-Funkmodul betriebsbereit ist.
- Preferred Scanning Channels (PSC) sind eine aktive Methode zur In-Band-Erkennung. Wireless-Clients prüfen nur PSC-Kanäle; scannt Nicht-PSC, wenn es einen RNR erkennt.

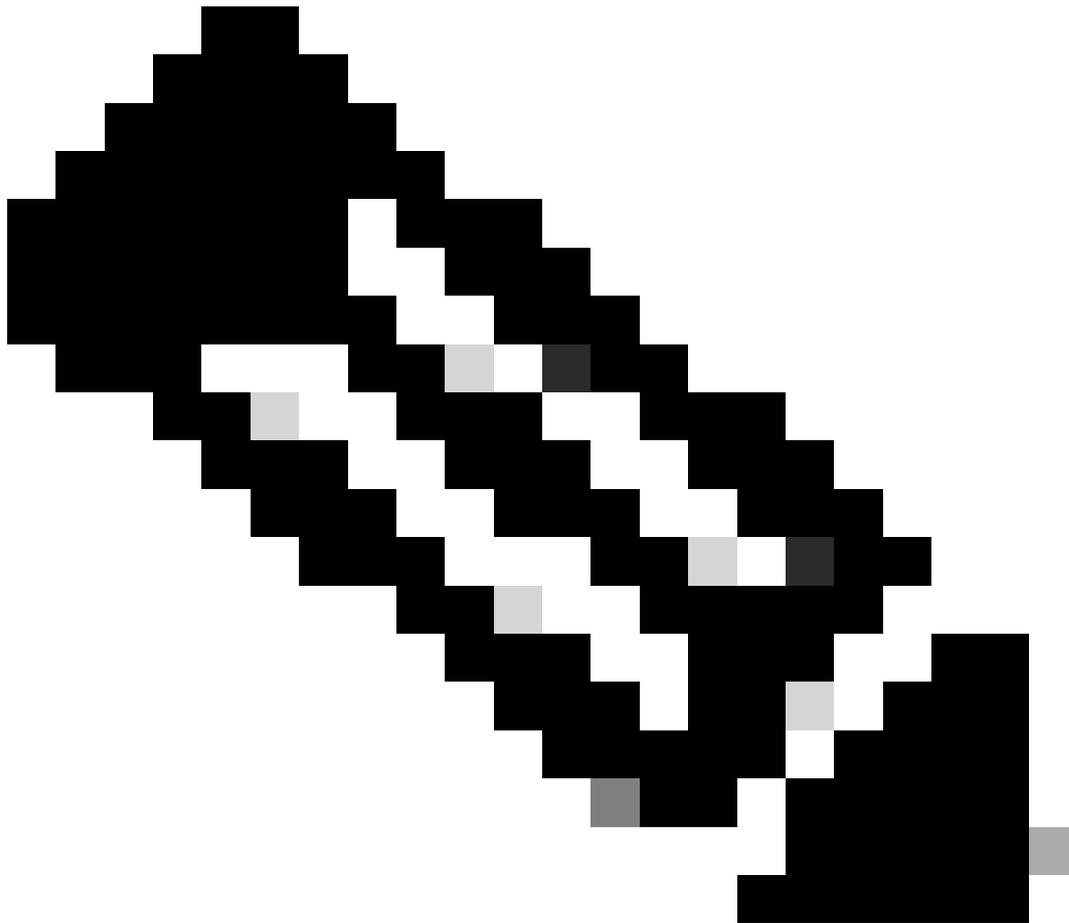
Beachten Sie, dass es sich hierbei um In-Band-Erkennungsmethoden handelt, d. h., dass dies nur für Wi-Fi 6E-Clients gilt, die sich mit Wireless-Netzwerken im 6-GHz-Band verbinden.

## FILES

FILS ist Teil des IEEE 802.11ai-Standards und unterstützt Verbesserungen bei der Erkennung, Authentifizierung und Zuordnung von Netzwerken und BSS sowie bei der Einrichtung von DHCP- und IP-Adressen.

FILS verwendet "Discovery-Ankündigungs-Frames", bei denen es sich im Wesentlichen um komprimierte Beacon-Frames handelt. In einem FILS-Frame werden nur wichtige Informationen gesendet: Short SSID, BSSID und Channel, damit der WAP über den anzuschließenden WAP entscheidet.

Wenn FILS konfiguriert ist, sendet der 6-GHz-WAP etwa alle 20 Millisekunden einen Ankündigungserkennungs-Frame, wodurch weniger Funkzeit verbraucht wird und der Overhead für die Anfragen reduziert wird.



Hinweis: 6-GHz-Ermittlungsrahmen werden nur benötigt, wenn nur das 6-GHz-Funkmodul betriebsbereit ist. Wenn andere Funkmodule (2,4/5 GHz) betriebsbereit sind, erkennen Clients eine 6-GHz-Präsenz von RNR IE.

---

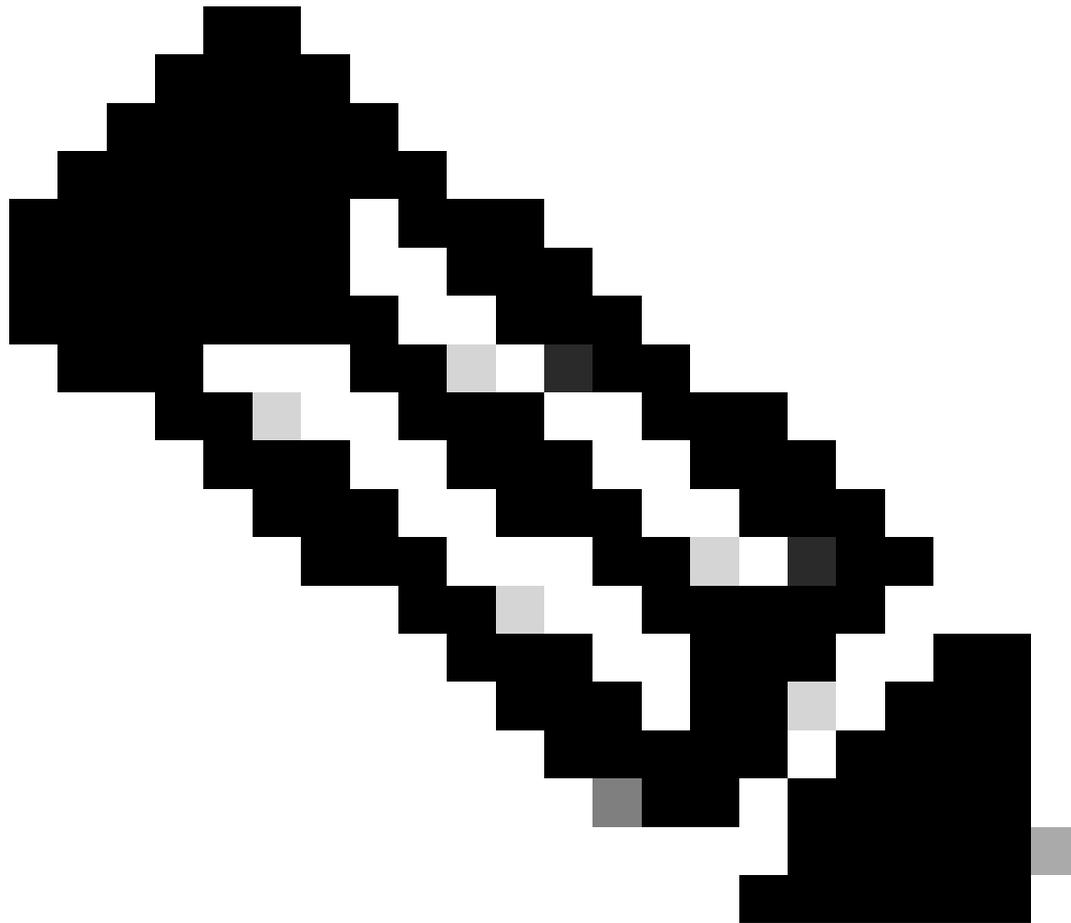
#### Konfigurieren von FILS-Erkennungs-Frames im RF-Profil (GUI)

Schritt 1 - Wählen Sie Configuration > Tags & Profiles > RF/Radio.

Schritt 2 - Klicken Sie auf der Registerkarte RF auf Hinzufügen. Die Seite "RF-Profil hinzufügen" wird angezeigt.

Schritt 3: Wählen Sie die Registerkarte 802.11ax aus.

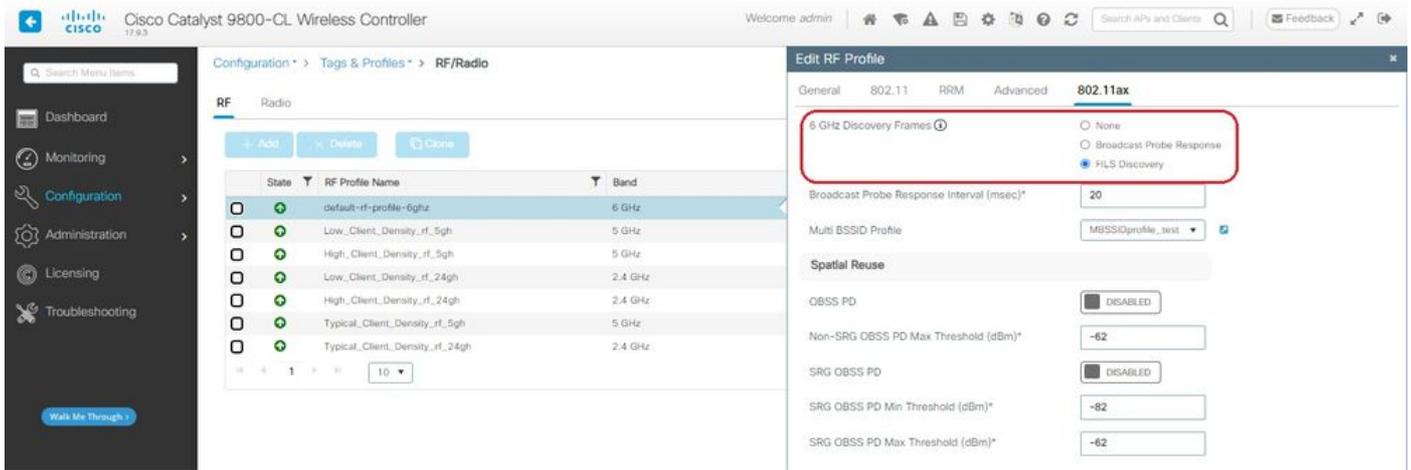
Schritt 4 - Klicken Sie im Abschnitt 6 GHz Discovery Frames auf die Option FILS Discovery.



Hinweis: Um die Übertragung von Erkennungs-FILS-Frames zu verhindern, wenn die Erkennungs-Frames im RF-Profil auf None gesetzt sind, müssen Sie FILS-Erkennungs-Frames deaktivieren, indem Sie entweder auf das 5-GHz- oder das 2,4-GHz-Band am Access Point wechseln oder die Option "Broadcast Probe Response" auswählen.

---

Schritt 5 - Klicken Sie auf Auf Gerät anwenden.



## Konfigurieren von FILS-Erkennungs-Frames im RF-Profil (CLI)

```
Device# configure terminal
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
Device(config-rf-profile)# dot11ax fils-discovery
```

## Verifizierung

Um zu überprüfen, ob die Konfiguration implementiert ist, führen Sie den Befehl show aus, wie hier gezeigt:

```
<#root>
```

```
WLC9800#
```

```
show ap rf-profile name default-rf-profile-6ghz detail | b 802.11ax
```

```
802.11ax
```

```
OBSS PD : Disabled
Non-SRG OBSS PD Maximum : -62 dBm
SRG OBSS PD : Disabled
SRG OBSS PD Minimum : -82 dBm
SRG OBSS PD Maximum : -62 dBm
Broadcast Probe Response : Disabled
```

```
FILS Discovery : Enabled
```

```
Multi-BSSID Profile Name :
```

```
MBSSIDprofile_test
```

```
NDP mode : Auto
Guard Interval : 800ns
PSC Enforcement : Disabled
```

Wir erwarten Folgendes, wenn wir den drahtlosen Datenverkehr über die Luft erfassen:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
5007	2023-06-09 14:59:17.112846	0.020885	Cisco_13:100:ec		Broadcast	002.11	115	5 -37 dBm	FILS Discovery, E5+100
5021	2023-06-09 14:59:17.152291	0.040845	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5024	2023-06-09 14:59:17.179789	0.026799	Cisco_13:100:ec		Broadcast	002.11	115	5 -37 dBm	FILS Discovery, E5+100
5027	2023-06-09 14:59:17.194300	0.020833	Cisco_13:100:ec		Broadcast	002.11	115	5 -37 dBm	FILS Discovery, E5+100
5031	2023-06-09 14:59:17.214796	0.020893	Cisco_13:100:ec		Broadcast	002.11	115	5 -37 dBm	FILS Discovery, E5+100
5046	2023-06-09 14:59:17.255787	0.040911	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5049	2023-06-09 14:59:17.276385	0.020850	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5054	2023-06-09 14:59:17.296779	0.020814	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5062	2023-06-09 14:59:17.317181	0.020802	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5071	2023-06-09 14:59:17.338075	0.040934	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5083	2023-06-09 14:59:17.378751	0.020900	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5095	2023-06-09 14:59:17.399121	0.020846	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5104	2023-06-09 14:59:17.419594	0.020873	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5118	2023-06-09 14:59:17.460812	0.040938	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5122	2023-06-09 14:59:17.480955	0.020823	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5124	2023-06-09 14:59:17.502561	0.021680	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5131	2023-06-09 14:59:17.522887	0.021676	Cisco_13:100:ec		Broadcast	002.11	115	5 -37 dBm	FILS Discovery, E5+100
5147	2023-06-09 14:59:17.562976	0.040939	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5150	2023-06-09 14:59:17.583235	0.020849	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5152	2023-06-09 14:59:17.604367	0.020842	Cisco_13:100:ec		Broadcast	002.11	115	5 -37 dBm	FILS Discovery, E5+100
5156	2023-06-09 14:59:17.624287	0.020820	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5172	2023-06-09 14:59:17.665387	0.041100	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5176	2023-06-09 14:59:17.685883	0.020896	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5179	2023-06-09 14:59:17.706338	0.020855	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5187	2023-06-09 14:59:17.727082	0.020864	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5202	2023-06-09 14:59:17.767771	0.040769	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5204	2023-06-09 14:59:17.788186	0.020815	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5208	2023-06-09 14:59:17.808734	0.020828	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5215	2023-06-09 14:59:17.829181	0.020874	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5218	2023-06-09 14:59:17.849351	0.041063	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5231	2023-06-09 14:59:17.890890	0.020839	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5236	2023-06-09 14:59:17.911149	0.020859	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5243	2023-06-09 14:59:17.931511	0.020866	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5256	2023-06-09 14:59:17.972562	0.040947	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5259	2023-06-09 14:59:17.993098	0.020868	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5262	2023-06-09 14:59:18.013608	0.020780	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5271	2023-06-09 14:59:18.034045	0.020837	Cisco_13:100:ec		Broadcast	002.11	115	5 -36 dBm	FILS Discovery, E5+100
5280	2023-06-09 14:59:18.075098	0.041005	Cisco_13:100:ec		Broadcast	002.11	115	5 -36 dBm	FILS Discovery, E5+100
5282	2023-06-09 14:59:18.095181	0.020891	Cisco_13:100:ec		Broadcast	002.11	115	5 -36 dBm	FILS Discovery, E5+100
5301	2023-06-09 14:59:18.116820	0.020869	Cisco_13:100:ec		Broadcast	002.11	115	5 -36 dBm	FILS Discovery, E5+100
5309	2023-06-09 14:59:18.136344	0.020824	Cisco_13:100:ec		Broadcast	002.11	115	5 -36 dBm	FILS Discovery, E5+100
5315	2023-06-09 14:59:18.177340	0.040966	Cisco_13:100:ec		Broadcast	002.11	115	5 -36 dBm	FILS Discovery, E5+100
5338	2023-06-09 14:59:18.197819	0.020899	Cisco_13:100:ec		Broadcast	002.11	115	5 -36 dBm	FILS Discovery, E5+100
5361	2023-06-09 14:59:18.218649	0.020830	Cisco_13:100:ec		Broadcast	002.11	115	5 -36 dBm	FILS Discovery, E5+100
5366	2023-06-09 14:59:18.238728	0.020871	Cisco_13:100:ec		Broadcast	002.11	115	5 -36 dBm	FILS Discovery, E5+100
5381	2023-06-09 14:59:18.279769	0.041040	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5394	2023-06-09 14:59:18.300285	0.020836	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5392	2023-06-09 14:59:18.320811	0.020840	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100
5399	2023-06-09 14:59:18.341213	0.020862	Cisco_13:100:ec		Broadcast	002.11	115	5 -36 dBm	FILS Discovery, E5+100
5417	2023-06-09 14:59:18.382372	0.041159	Cisco_13:100:ec		Broadcast	002.11	115	5 -36 dBm	FILS Discovery, E5+100
5430	2023-06-09 14:59:18.402851	0.020891	Cisco_13:100:ec		Broadcast	002.11	115	5 -36 dBm	FILS Discovery, E5+100
5432	2023-06-09 14:59:18.423192	0.020789	Cisco_13:100:ec		Broadcast	002.11	115	5 -36 dBm	FILS Discovery, E5+100
5430	2023-06-09 14:59:18.443617	0.020865	Cisco_13:100:ec		Broadcast	002.11	115	5 -36 dBm	FILS Discovery, E5+100
5448	2023-06-09 14:59:18.484693	0.040966	Cisco_13:100:ec		Broadcast	002.11	115	5 -36 dBm	FILS Discovery, E5+100
5451	2023-06-09 14:59:18.505086	0.020893	Cisco_13:100:ec		Broadcast	002.11	115	5 -36 dBm	FILS Discovery, E5+100
5457	2023-06-09 14:59:18.525880	0.020734	Cisco_13:100:ec		Broadcast	002.11	115	5 -38 dBm	FILS Discovery, E5+100

```

> Frame 5807: 115 bytes on wire (920 bits), 115 bytes captured (920 bits) on interface 10wdoc10p1_104578901-2990-486-8c3-c
> Ethernet II, Src: Cisco_Gi7/317 (08:00:0d:0e:76:137), Dst: Universa_b7:c7:06 (08:3a:18:1b:c7:06)
> Internet Protocol version 4, Src: 192.168.1.115, Dst: 192.168.1.121
> User Datagram Protocol, Src Port: 5555, Dst Port: 5500
> AirPeeq/Qualcomm encapsulated IEEE 802.11
> 802.11 radio information
> IEEE 802.11 Action, Flags: .....C
Type/Subtype: Action (8000)
> Frame Control field: 0x0000
> Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: Cisco_13:100:ec (18:19:1b:13:100:ec)
Source address: Cisco_13:100:ec (18:19:1b:13:100:ec)
BSS ID: Cisco_13:100:ec (18:19:1b:13:100:ec)
..... 0000 = Fragment Number: 0
819 1000 0001 ..... = Sequence number: 569
Frame check sequence: 0x00000000 [unverified]
[FCX Status: Unverified]
> IEEE 802.11 Wireless Management
> Uplink parameters
Category code: Public Action (4)
Public Action: FILS Discovery (002)
> Frame Control: 0x0000, Capability: Short SSID, Length
..... 0001 = SSID Length: 0x03
..... 01 ..... = Capability: Present
..... 00 ..... = Short SSID: Present
..... 00 ..... = AP-ESH: Not Present
..... 00 ..... = ANQ: Not Present
..... 00 ..... = Channel Center Frequency Segment 1: Not Present
..... 00 ..... = Primary Channel: Not Present
..... 00 ..... = RSN Info: Not Present
..... 00 ..... = Length: Present
..... 00 ..... = MD: Not Present
..... 00 ..... = Reserved: Not Present
Timestamp: 1800561928
Beacon Interval: 0.182000 [seconds]
Short SSID: 0x0d1c2b5
Length: 2
> Capability: 0x122c
..... 00 ..... = ESSI: 0x0
..... 00 ..... = PPKCH: 0x0
..... 00 ..... = BSS Operating Channel Width: 160MHz or 80MHz+80MHz / 20MHz or 20MHz+20MHz (8x3)
..... 0011 ..... = Maximum number of Spatial Streams: 2 spatial streams (8x3)
..... 00 ..... = Interference: 0x0
..... 00 ..... = Multiple BSSIDs: 0x0
..... 00 ..... = PHY ENQCH: 0x0
..... 00 ..... = FILS Minimum Rate: HE-MCS 0 (0x0)
> Tagged parameters (4 bytes)
> Tag: Tx Power Envelope
Tag Number: Tx Power Envelope (195)
Tag Length: 2
> Tx Par Info: 0x18
..... 0000 = Max Tx Par Count: 0
..... 00 ..... = Max Tx Par Unit Interpretation: Unknown (3)
..... 00 ..... = Reserved: 0
Local Max Tx Par Constraint: 20MHz: 18.0 dBm
    
```

Sie können beobachten, dass das Delta zwischen Frames die meisten Male ~20 ms beträgt, aber manchmal sehen Sie ~40 ms. Nach Überprüfung der Bildsequenz wurde festgestellt, dass der Sniffer AP die Aufnahme von FILS-Bildern sporadisch verpasste.

## UPR

Ein unsolicited Probe Response (UPR)-Frame enthält alle Informationen, die in einem Beacon gesendet werden, d. h., er überträgt mehrere BSSIDs und enthält alle Informationen, die für die Zuordnung benötigt werden.

Wenn der Access Point mit 6 GHz verwendet wird, sendet er alle 20 Millisekunden einen Frame mit voller Antwort auf die Anfrage, wodurch Sondenstürme vermieden werden.

Bei 6GHz gibt es neue Einschränkungen für die Überprüfung:

- Clients können keine Blindprobe durchführen, d. h. Broadcast-Zieladressen mit Platzhalter-SSID und BSSID sind nicht zulässig, da Broadcast-Anfragen und -Sonden mit Platzhalter-SSID einen Sondensturm verursachen und die Leistung beeinträchtigen.
- Die Clients müssen mindestens die Dauer des minimalen Testverzögerungsintervalls (~20 ms) abwarten.
- Antworten auf Fragen werden immer übertragen.

UPR wird auch als Broadcast Probe Response bezeichnet. Im nächsten Abschnitt wird die Aktivierung beschrieben.

Konfigurieren der Broadcast-Testantwort in der RF-Profiloption (GUI)

Schritt 1 - Wählen Sie Configuration > Tags & Profiles > RF/Radio.

Schritt 2 - Klicken Sie auf der Registerkarte RF auf Hinzufügen. Die Seite "RF-Profil hinzufügen"

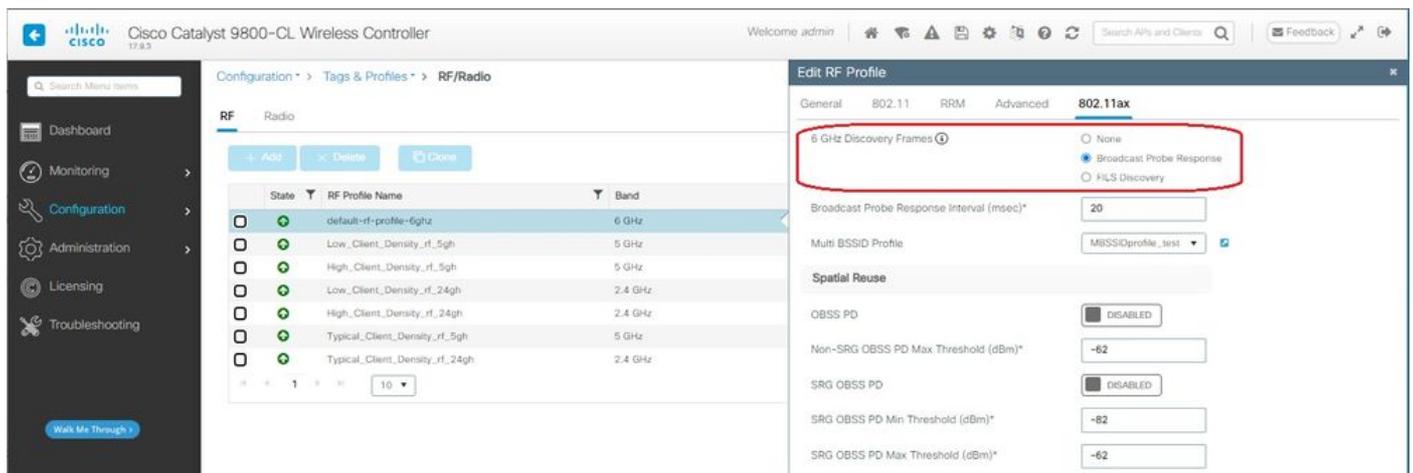
wird angezeigt.

Schritt 3: Wählen Sie die Registerkarte 802.11ax aus.

Schritt 4 - Klicken Sie im Abschnitt 6 GHz Discovery Frames auf die Option Broadcast Probe Response (Broadcast-Testantwort).

Schritt 5 - Geben Sie im Feld Broadcast Probe Response Interval (Intervall für Broadcast-Testantwort) das Intervall für die Broadcast-Testantwort in Millisekunden (ms) ein. Der Wertebereich liegt zwischen 5 ms und 25 ms. Der Standardwert ist 20 ms.

Schritt 6 - Klicken Sie auf Auf Gerät anwenden.



Konfigurieren der Broadcast-Sondenantwort im RF-Profil (CLI)

```
Device# configure terminal
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
Device(config-rf-profile)# dot11ax bcast-probe-response
Device(config-rf-profile)# dot11ax bcast-probe-response time-interval 20
```

Verifizierung

Um zu überprüfen, ob die Konfiguration implementiert ist, führen Sie den Befehl show aus, wie hier gezeigt:

```
<#root>
```

```
WLC9800#
```

```
show ap rf-profile name default-rf-profile-6ghz detail | b 802.11ax
```

```
802.11ax
```

```
OBSS PD : Disabled
```

```
Non-SRG OBSS PD Maximum : -62 dBm
```



6GHz band  
20 MHz Channel



PSC-Kanäle

Bevorzugte Scan-Kanäle in der RF-Profil (GUI) konfigurieren

Schritt 1 - Wählen Sie Configuration > Tags & Profiles > RF/Radio.

Schritt 2 - Klicken Sie auf der Registerkarte RF auf Hinzufügen. Die Seite "RF-Profil hinzufügen" wird angezeigt.

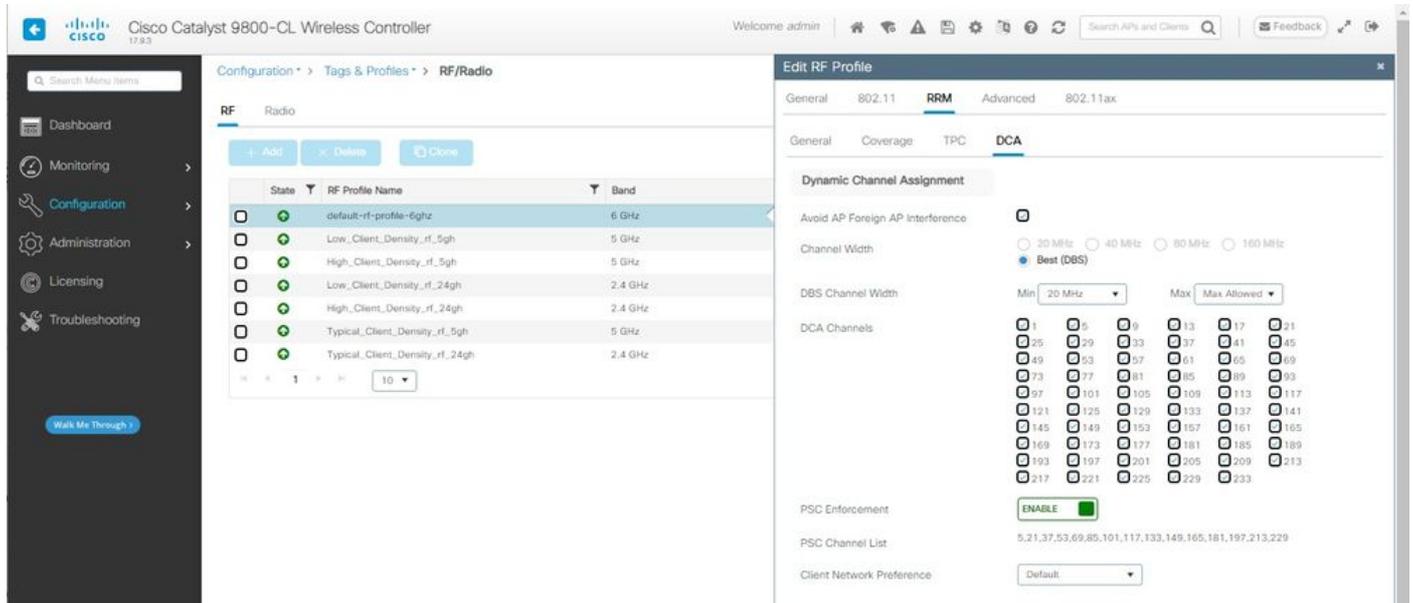
Schritt 3: Wählen Sie die Registerkarte "RRM".

Schritt 4 - Wählen Sie die Registerkarte DCA.

Schritt 5 - Wählen Sie im Abschnitt Dynamic Channel Assignment (Dynamische Kanalzuweisung) die erforderlichen Kanäle im Abschnitt DCA Channels (DCA-Kanäle) aus.

Schritt 6 - Klicken Sie im Feld "PSC Enforcement" (PSC-Durchsetzung) auf die Umschaltfläche, um die bevorzugte Scan-Channel-Durchsetzung für DCA zu aktivieren.

Schritt 7 - Klicken Sie auf Auf Gerät anwenden.



Bevorzugte Scan-Kanäle im RF-Profil (CLI) konfigurieren

```
Device# configure terminal
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
Device(config-rf-profile)# channel psc
```

## Verifizierung

Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die Konfiguration bereits vorhanden ist:

```
<#root>
```

```
WLC9800#
```

```
show ap rf-profile name default-rf-profile-6ghz detail | b DCA
```

```
DCA Channel List : 1,5,9,13,17,21,25,29,33,37,41,45,49,53,57,61,65,69,73,77,81,85,89,93,97,101,105,109,
Unused Channel List :
```

```
PSC Channel List : 5,21,37,53,69,85,101,117,133,149,165,181,197,213,229
```

```
DCA Bandwidth : best
```

```
DBS Min Channel Width : 20 MHz
```

```
DBS Max Channel Width : MAX ALLOWED
```

```
DCA Foreign AP Contribution : Enabled
```

```
[...]
```

```
PSC Enforcement : Enabled
```

Hier können wir Wi-Fi 6E-Clients beobachten, die Anfragen an PSC-Kanal 5 senden:

NetGear A8000

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal strength	Info
159	2023-06-09 15:10:48.797226	0.000000	netgear_48178...	Cisco_13108...	802.11	360	5	-47 dBm	Probe Request, Smb, Fw0, Flags=.....C, SSID="wifi6_test"
159	2023-06-09 15:10:48.799693	0.002467	netgear_48178...	Cisco_13108...	802.11	360	5	-47 dBm	Probe Request, Smb, Fw0, Flags=.....C, SSID="wifi6_test"
159	2023-06-09 15:10:48.799693	0.002467	netgear_48178...	Cisco_13108...	802.11	360	5	-47 dBm	Probe Request, Smb, Fw0, Flags=.....C, SSID="wifi6_test"
159	2023-06-09 15:10:49.009338	0.227768	netgear_48178...	Cisco_13108...	802.11	250	5	-47 dBm	Association Request, Smb, Fw0, Flags=.....C, SSID="wifi6_test"

```
> Frame 159580: 360 bytes on wire (2880 bits), 360 bytes captured (2880 bits) on interface \Device\NPF_{D4578965-2998-4A56-8C33-C343}
> Ethernet II, Src: Cisco_0017d37f (00:0f:1d:00:17:d37), Dst: Universa_07:cf:f06 (08:3a:8b:d7:cf:f06)
> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.123
> User Datagram Protocol, Src Port: 5555, Dst Port: 5800
> AloPcap/Omnipeak encapsulated IEEE 802.11
> 802.11 radio information
> IEEE 802.11 Probe Request, Flags: .....C
< Tagged parameters (276 bytes)
  < Tag: SSID parameter set: "wifi6_test"
    Tag Number: SSID parameter set (0)
    Tag Length: 11
    SSID: "wifi6_test"
  > Tag: Supported Rates 6(8), 9, 12(8), 18, 24(8), 36, 48, 54, [Mbit/sec]
  > Ext Tag: HE Capabilities
  > Tag: Vendor Specific: Microsoft Corp.: WPS
  > Tag: Vendor Specific: Wi-Fi Alliance: Multi Band operation - optimized connectivity experience
  < Tag: Extended Capabilities (10 octets)
    Tag Number: Extended Capabilities (227)
    Tag Length: 10
  > Extended Capabilities: 0x01 (octet 1)
  > Extended Capabilities: 0x00 (octet 2)
  > Extended Capabilities: 0x00 (octet 3)
  > Extended Capabilities: 0x00 (octet 4)
  > Extended Capabilities: 0x00 (octet 5)
  > Extended Capabilities: 0x00 (octet 6)
  > Extended Capabilities: 0x00 (octet 7)
  > Extended Capabilities: 0x000e (octets 8 & 9)
  < Extended Capabilities: 0x20 (octet 10)
  < .....0 = PLS Capable: False
  < .....0 = Extended Spectrum Management Capable: False
  < .....0 = Future Channel Capable: False
  < .....0 = Reserved: 0x0
  < .....0 = Reserved: 0x0
  < ..1..... = TWT Requester Support: True
  < ..0.... = TWT Responder Support: False
  < ..0.... = 20SS Narrow Bandwidth RU in UL OFDMA Tolerance Support: False
  < Ext Tag: HE Capabilities
  < Ext Tag: HE 6 GHz Band Capabilities
    Tag Number: Element ID Extension (255)
    Ext Tag Length: 2
    Ext Tag Number: HE 6 GHz Band Capabilities (59)
  > Capabilities Information: 0x6000
```

Pixel 6a

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info	
126.	2023-06-09 16:09:25.548710	11.144233	netgear_48170:95	BroadCast	002.11	166	5-4-40	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Frame 16581: 308 bytes on wire (2480 bits), 308 bytes captured (2480 bits) on interface 'Device\NPF_{04878965-2998-4456-8C33-C4316}	
126.	2023-06-09 16:09:25.549656	0.000085	netgear_48170:95	BroadCast	002.11	166	5-4-40	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Ethernet II, Src: Cisco:00:0C:29:1A:00:00, Dst: Univers:07:cf:c6 (00:18:8B:07:cf:c6)	
126.	2023-06-09 16:09:25.550449	0.000073	netgear_48170:95	BroadCast	002.11	166	5-4-40	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.15	
126.	2023-06-09 16:09:25.551120	0.000071	netgear_48170:95	BroadCast	002.11	166	5-4-40	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> User Datagram Protocol, Src Port: 5555, Dst Port: 5000	
126.	2023-06-09 16:09:25.551741	0.000061	netgear_48170:95	BroadCast	002.11	166	5-4-40	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> AirPreReq/OverPeek encapsulated IEEE 802.11	
126.	2023-06-09 16:09:25.552376	0.000065	netgear_48170:95	BroadCast	002.11	166	5-4-40	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> IEEE 802.11 Probe Request, Flags: .....C	
126.	2023-06-09 16:09:25.552987	0.000069	netgear_48170:95	BroadCast	002.11	166	5-4-40	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> IEEE 802.11 Wireless Management	
127.	2023-06-09 16:09:25.553217	2.745264	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tagged parameters (204 bytes)
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag: SSID parameter set: "billiard"
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag: SSID parameter set (8)
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag Length: 11
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag: Supported Rates (40), 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec]
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag: Extended Supported Rates: S04: 18, 24, 36, 48, 54, [Mbit/sec]
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag Number: Extended Supported Rates (50)
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag Length: 1
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag: Extended Supported Rates: S04: 18, 24, 36, 48, 54, [Mbit/sec]
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag: Extended Capabilities (11 octets)
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag: Interworking
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Ext Tag: FILS Request Parameters: Undecoded
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag Number: Element ID Extension (255)
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Ext Tag Length: 2
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Ext Tag Number: FILS Request Parameters (2)
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Ext Tag Data: 0x00
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> > Expert Info (Note/Undecoded): Dissector for IEEE 802.11 Extension Tag (FILS Request Parameters) code not implemented, Contact
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Ext Tag: HE Capabilities
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag: HE 6 Gz Band Capabilities
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag Number: Element ID Extension (255)
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Ext Tag Length: 2
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Capabilities Information: 0x0000
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag: HE 6 Gz Band Capabilities (59)
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Minimum MPOU Start Spacing: 8 uS (8uS)
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Maximum MPOU Length Exponent: 1 048 575 (8uS)
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Maximum MPOU Length: 11 454 (8uS)
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Reserved: 0x00
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> SM Power Save: SM Power Save Disabled (8uS)
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> HD Responder: Not supported
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Rx Antenna Pattern Consistency: Not supported
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tx Antenna Pattern Consistency: Not supported
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Reserved: 0x00
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Ext Tag: Short SSID
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag Number: Element ID Extension (255)
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Ext Tag Length: 4
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Ext Tag Number: Short SSID (58)
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Short SSID: 0x00000000
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag: Vendor Specific: Microsoft Corp.: WPS
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag: Vendor Specific: Wi-Fi Alliance: P2P
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag: Vendor Specific: Wi-Fi Alliance: Hotspot 2.0 Indication
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag: Vendor Specific: Microsoft Corp.: Unknown 8
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag: Vendor Specific: Broadcom
127.	2023-06-09 16:09:25.553217	0.000068	netgear_48170:95	BroadCast	002.11	168	5-51	00	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag: Vendor Specific: Wi-Fi Alliance: Multi Band Operation - Optimized Connectivity Experience

## Samsung S23

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
620.	2023-06-09 16:02:25.543089	0.000095	netgear_48170:95	BroadCast	002.11	166	5-4-40	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Frame 16584: 308 bytes on wire (2480 bits), 308 bytes captured (2480 bits) on interface 'Device\NPF_{04878965-2998-4456-8C33-C4316}
620.	2023-06-09 16:02:25.543382	0.000073	netgear_48170:95	BroadCast	002.11	166	5-4-40	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Ethernet II, Src: Cisco:00:0C:29:1A:00:00, Dst: Univers:07:cf:c6 (00:18:8B:07:cf:c6)
620.	2023-06-09 16:02:25.543676	0.000073	netgear_48170:95	BroadCast	002.11	166	5-4-40	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.15
620.	2023-06-09 16:02:25.543970	0.000073	netgear_48170:95	BroadCast	002.11	166	5-4-40	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
620.	2023-06-09 16:02:25.544264	0.000073	netgear_48170:95	BroadCast	002.11	166	5-4-40	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> AirPreReq/OverPeek encapsulated IEEE 802.11
620.	2023-06-09 16:02:25.544558	0.000073	netgear_48170:95	BroadCast	002.11	166	5-4-40	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> IEEE 802.11 Probe Request, Flags: .....C
620.	2023-06-09 16:02:25.544852	0.000073	netgear_48170:95	BroadCast	002.11	166	5-4-40	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> IEEE 802.11 Wireless Management
620.	2023-06-09 16:02:25.545146	0.000073	netgear_48170:95	BroadCast	002.11	166	5-4-40	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tagged parameters (204 bytes)
620.	2023-06-09 16:02:25.545440	0.000073	netgear_48170:95	BroadCast	002.11	166	5-4-40	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag: SSID parameter set: "billiard"
620.	2023-06-09 16:02:25.545734	0.000073	netgear_48170:95	BroadCast	002.11	166	5-4-40	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag: SSID parameter set (8)
620.	2023-06-09 16:02:25.546028	0.000073	netgear_48170:95	BroadCast	002.11	166	5-4-40	Probe Request, Src: 192.168.1.15, Dst: 192.168.1.15, SSID: "billiard"	> Tag Length: 11
620.	2023-06-09 16:02:25.546322	0.000073	netgear_48170:95	Broad					

bestehenden 2,4-GHz- und 5-GHz-Bändern eine geringere Netzwerküberlastung auf.

Wireless-Clients, die 6-GHz-fähig sind, können daher eine Verbindung zum 6-GHz-Funkmodul herstellen, um diese Vorteile zu nutzen.

In diesem Thema finden Sie Details zur 6-GHz-Client-Steuerung für APs, die das 6-GHz-Band unterstützen.

Die 6-GHz-Client-Steuerung erfolgt, wenn der Controller einen periodischen Client-Statistikbericht aus dem 2,4-GHz-Band oder dem 5-GHz-Band erhält.

Die Konfiguration der Client-Steuerung ist unter WLAN aktiviert und wird nur für Clients konfiguriert, die 6-GHz-fähig sind.

Wenn ein Client im Bericht 6-GHz-fähig ist, wird eine Client-Steuerung ausgelöst, und der Client wird auf das 6-GHz-Band gelenkt.

Mehr über Bandlenkung für Dual-Band Wi-Fi Access Points erfahren Sie im Dokument "Qualcomm Research Band-Steering for Dual-Band Wi-Fi Access Points".

#### Der Lenkungsmechanismus

Um die Steuerung eines Clients zu starten, trennt der WAP zunächst die Verbindung zum Client in einem bestimmten Band und blockiert dann die erneute Zuweisung des Clients in diesem Band für einen bestimmten Zeitraum.

Nach dem Trennen versucht der Client kurz, die Zuordnung zum Access Point für dieselbe SSID und das gleiche Band wie bei der letzten Zuordnung wiederherzustellen, bevor nach anderen Access Point- oder Bandoptionen gesucht wird.

Die meisten Wi-Fi-Clients scannen beide Bänder, indem sie Prüfanfragen senden und die Abwärtsstreckensignalstärke aus den Prüfanfragen schätzen, die auch die Bereitschaft des Access Points zur erneuten Zuordnung anzeigen.

Da dieses Scan- und Neuzuordnungsverhalten vollständig von der Clientimplementierung abhängt, können einige Clients schneller steuern als andere.

Es ist möglich, dass einige Clients nicht steuern und versuchen, erneut eine Verbindung mit dem ursprünglichen (blockierten) Band herzustellen, oder einfach die Verbindung mit dem Wi-Fi-Netzwerk trennen und nur dann eine neue Verbindung herstellen, wenn Pakete gesendet werden sollen.

#### Vorsicht bei der Lenkung

Es muss am Access Point darauf geachtet werden, dass solche lenkungsunfreundlichen Clients nicht am Access Point blockiert werden. In diesem Fall kann ein Benutzereingriff erforderlich sein, um die Wi-Fi-Verbindung wiederherzustellen.

Benutzereingriffe können genauso einfach sein wie das Ein- und Ausschalten des Wi-Fi-Netzwerks. Solche Benutzereingriffe sind eindeutig nicht wünschenswert. Daher liegt das Design

auf der konservativen Seite.

Wenn ein Client nicht gesteuert werden kann oder ein Lenkungsversuch fehlschlägt, lässt der WAP den Client dem ursprünglichen Band erneut zuordnen, anstatt zu riskieren, dass der Client für einen längeren Zeitraum vom WAP blockiert wird.

Da der Client nur im Leerlauf gesteuert wird, kommt es zu keiner Unterbrechung des Benutzerdatenverkehrs.

Konfigurieren der 6-GHz-Client-Steuerung im globalen Konfigurationsmodus (GUI)

Schritt 1 - Wählen Sie Configuration > Wireless > Advanced aus.

Schritt 2 - Klicken Sie auf die Registerkarte 6 GHz Client Steering (6-GHz-Client-Steuerung). Die Client-Steuerung ist per WLAN konfigurierbar.

Schritt 3 - Geben Sie im Feld Mindestanzahl Clients für den 6-GHz-Übergang einen Wert ein, um die Mindestanzahl Clients für die Client-Steuerung festzulegen. Der Standardwert ist drei Clients. Der Wertebereich liegt zwischen 0 und 200 Clients.

Schritt 4 - Geben Sie im Feld Mindestfenstergröße für den 6-GHz-Übergang einen Wert ein, um die Mindestfenstergröße der Client-Steuerung festzulegen. Der Standardwert ist drei Clients. Der Wertebereich liegt zwischen 0 und 200 Clients.

Schritt 5 - Geben Sie im Feld Maximale Auslastungsdifferenz für den 6 GHz-Übergang einen Wert ein, um die maximale Auslastungsdifferenz für die Steuerung festzulegen. Der Wertebereich liegt zwischen 0 % und 100 %. Der Standardwert ist 20.

Schritt 6 - Geben Sie im Feld 6 GHz Transition Minimum 2.4 GHz RSSI Threshold (Mindestwert für den 6-GHz-Übergang) einen Wert ein, um den Mindestwert für den Client-Lenkungs-RSSI-Schwellenwert von 2.4 GHz festzulegen.

Schritt 7 - Geben Sie im Feld 6 GHz Transition Minimum 5 GHz RSSI Threshold (RSSI-Mindestwert für 6 GHz Transition) einen Wert ein, um den Mindestwert für den Client-Steuerungs-RSSI-Schwellenwert von 5 GHz festzulegen.

Schritt 8 - Klicken Sie auf Anwenden.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The top navigation bar includes the Cisco logo, the device name 'Cisco Catalyst 9800-CL Wireless Controller', and the user 'Welcome admin'. The main content area is titled '6 GHz Client Steering' and contains five configuration fields:

Configuration Field	Value
6 GHz Transition Minimum Client Count*	3
6 GHz Transition Minimum Window Size*	3
6 GHz Transition Maximum Utilization Difference (%)*	20
6 GHz Transition Minimum 2.4 GHz RSSI Threshold (dBm)*	-60
6 GHz Transition Minimum 5 GHz RSSI Threshold (dBm)*	-65

An 'Apply' button is visible in the top right corner of the configuration area.

Konfigurieren der 6-GHz-Client-Steuerung im globalen Konfigurationsmodus (CLI)

```
Device# configure terminal
Device(config)# client-steering client-count 3
```

```

Device(config)# client-steering window-size 5
Device(config)# wireless client client-steering util-threshold 25
Device(config)# wireless client client-steering min-rssi-24ghz -70
Device(config)# wireless client client-steering min-rssi-5ghz -75

```

## Konfigurieren der 6-GHz-Client-Steuerung im WLAN (GUI)

Schritt 1 - Wählen Sie Configuration > Tags & Profiles > WLANs.

Schritt 2 - Klicken Sie auf Hinzufügen. Die Seite WLAN hinzufügen wird angezeigt.

Schritt 3 - Klicken Sie auf die Registerkarte Erweitert.

Schritt 4: Aktivieren Sie das Kontrollkästchen 6 GHz Client Steering (Client-Steuerung im WLAN).

Schritt 5 - Klicken Sie auf Auf Gerät anwenden.

The screenshot displays the Cisco Catalyst 9800-CL Wireless Controller GUI. On the left, a navigation sidebar includes Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main area shows the 'WLANs' configuration page with a table of WLANs. The 'wif6E\_test' WLAN is selected. On the right, the 'Edit WLAN' dialog is open, showing the 'Advanced' tab. The '6 GHz Client Steering' checkbox is checked and highlighted with a red rectangle. Other settings include Coverage Hole Detection, Aironet IE, P2P Blocking Action, Multicast Buffer, Media Stream Multicast-direct, 11ac MU-MIMO, WiFi to Cellular Steering, Fastlane+ (ASR), Deny LAA (RCM) clients, Max Client Connections, and Assisted Roaming (11k).

## Konfigurieren der 6-GHz-Client-Steuerung im WLAN (CLI)

```

Device# configure terminal
Device(config)# wlan wlan-name id ssid-name
Device(config-wlan)# client-steering

```

## Verifizierung

Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die Konfiguration bereits vorhanden ist:

<#root>

WLC9800#

show wireless client steering

#### Client Steering Configuration Information

Macro to micro transition threshold : -55 dBm  
Micro to Macro transition threshold : -65 dBm  
Micro-Macro transition minimum client count : 3  
Micro-Macro transition client balancing window : 3  
Probe suppression mode : Disabled  
Probe suppression transition aggressiveness : 3  
Probe suppression hysteresis : -6 dB  
6Ghz transition minimum client count : 3  
6Ghz transition minimum window size : 3  
6Ghz transition maximum channel util difference : 20%  
6Ghz transition minimum 2.4Ghz RSSI threshold : -60 dBm  
6Ghz transition minimum 5Ghz RSSI threshold : -65 dBm

#### WLAN Configuration Information

WLAN Profile Name      11k Neighbor Report      11v BSS Transition

-----  
5    wifi6E\_test            Enabled                    Enabled  
6    wifi6E\_test\_01        Enabled                    Enabled  
7    wifi6E\_test\_02        Enabled                    Enabled

WLC9800#

show wlan id 5 | i Client Steering

6Ghz Client Steering : Enabled

## Client-Verbindungen

In diesem Abschnitt wird der Prozess der OTA jedes Clients gezeigt, der sich mit dem WLAN verbindet.

Die Übung wurde unter folgenden Bedingungen durchgeführt:

- Clients und APs befanden sich ca. 1 m in Sichtlinie ohne Hindernisse.
- Alle APs, die WLAN mit einer Kanalbreite von 160 MHz und der Leistungsstufe 1 übertragen.
- Die Client-Geräte wurden auf demselben VLAN wie der iperf-Server geschaltet.
- Alle APs sind über eine 1-Gbit/s-Verbindung verbunden.

#### 6 GHz Radios

Total 6 GHz radios : 4

AP Name	Slot No	Base Radio MAC	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag	Channel Width	Channel	Power Level
AP9166_0E.6220	2	7411.b2d2.9740	✓	✓	W66E_TestPolicy	TiagoHomePTAPs	default-rf-tag	160 MHz	(69,65,73,77,81,85,89,93)*	*1/8 (19 dBm)
AP9162_53.CA50	2	3891.b713.80e0	✓	✓	W66E_TestPolicy	TiagoHomePTAPs	default-rf-tag	160 MHz	(5,1,9,13,17,21,25,29)*	*1/8 (17 dBm)
AP9136_5C.F524	3	00d1.1ddd.7d30	✓	✓	W66E_TestPolicy	TiagoHomePTAPs	default-rf-tag	160 MHz	(53,49,57,61,33,37,41,45)*	*1/8 (16 dBm)

Tests mit AP 9166

## NetGear A8000

### Client-Details in WLC:

<#root>

```
#show wireless client mac-address 9418.6548.7095 detail
```

```
Client MAC Address : 9418.6548.7095
[...]
Client IPv4 Address : 192.168.1.163
[...]
AP MAC Address : 7411.b2d2.9740
AP Name: AP9166_0E.6220
AP slot : 2
Client State : Associated
Policy Profile : Policy4TiagoHome
Flex Profile : TiagoHomeFlexProfile
Wireless LAN Id: 5
WLAN Profile Name: wifi6E_test
Wireless LAN Network Name (SSID): wifi6E_test
BSSID : 7411.b2d2.9747
Connected For : 1207 seconds

Protocol : 802.11ax - 6 GHz
```

```
Channel : 69
```

```
[...]
Current Rate : m11 ss2
Supported Rates : 54.0
[...]
```

```
Policy Type : WPA3
```

```
Encryption Cipher : CCMP (AES)
```

```
Authentication Key Management : SAE
```

```
AAA override passphrase : No
```

```
SAE PWE Method : Hash to Element(H2E)
```

```
[...]
```

```
Protected Management Frame - 802.11w : Yes
```

```
EAP Type : Not Applicable
[...]
[...]
FlexConnect Data Switching : Local
```

FlexConnect Dhcp Status : Local  
FlexConnect Authentication : Local  
Client Statistics:  
Number of Bytes Received from Client : 1026751751  
Number of Bytes Sent to Client : 106125429  
Number of Packets Received from Client : 793074  
Number of Packets Sent to Client : 184944  
Number of Policy Errors : 0

Radio Signal Strength Indicator : -44 dBm

Signal to Noise Ratio : 49 dB

[...]

Device Classification Information:

Device Type : Microsoft-Workstation

Device Name : CSCO-W-xxxxxxx

Protocol Map : 0x000029 (OUI, DHCP, HTTP)

Device OS : Windows NT 10.0; Win64; x64

Pixel 6a

Client-Details in WLC:

<#root>

#show wireless client mac-address 2495.2f72.8a66 detail

Client MAC Address : 2495.2f72.8a66  
[...]  
Client IPv4 Address : 192.168.1.162  
[...]  
AP MAC Address : 7411.b2d2.9740  
AP Name: AP9166\_OE.6220  
AP slot : 2  
Client State : Associated  
Policy Profile : Policy4TiagoHome  
Flex Profile : TiagoHomeFlexProfile  
Wireless LAN Id: 5  
WLAN Profile Name: wifi6E\_test  
Wireless LAN Network Name (SSID): wifi6E\_test  
BSSID : 7411.b2d2.9747  
Connected For : 329 seconds  
Protocol : 802.11ax - 6 GHz  
Channel : 69  
Client IIF-ID : 0xa000000a  
Association Id : 33  
Authentication Algorithm : Open System  
[...]  
Current Rate : 6.0  
Supported Rates : 61.0

[...]

Policy Type : WPA3

Encryption Cipher : CCMP (AES)

Authentication Key Management : SAE

AAA override passphrase : No

SAE PWE Method : Hash to Element(H2E)

[...]

Protected Management Frame - 802.11w : Yes

EAP Type : Not Applicable

[...]

Session Manager:

Point of Attachment : capwap\_90000025

IIF ID : 0x90000025

Authorized : TRUE

Session timeout : 86400

Common Session ID: 000000000000171BC51FF477

Acct Session ID : 0x00000000

Auth Method Status List

Method : SAE

Local Policies:

Service Template : wlan\_svc\_Policy4TiagoHome (priority 254)

VLAN : default

Absolute-Timer : 86400

Server Policies:

Resultant Policies:

VLAN Name : default

VLAN : 1

Absolute-Timer : 86400

[...]

FlexConnect Data Switching : Local

FlexConnect Dhcp Status : Local

FlexConnect Authentication : Local

Client Statistics:

Number of Bytes Received from Client : 603220312

Number of Bytes Sent to Client : 72111916

Number of Packets Received from Client : 461422

Number of Packets Sent to Client : 107888

Number of Policy Errors : 0

Radio Signal Strength Indicator : -45 dBm

Signal to Noise Ratio : 48 dB

[...]

Device Classification Information:

Device Type : Android-Google-Pixel

Device Name : Pixel-6a

Protocol Map : 0x000029 (OUI, DHCP, HTTP)

Device OS : X11; Linux x86\_64

## Samsung S23

### Client-Details in WLC:

<#root>

#show wireless client mac-address 0429.2ec9.e371 detail

Client MAC Address : 0429.2ec9.e371

[...]

Client IPv4 Address : 192.168.1.160

[...]

AP MAC Address : 7411.b2d2.9740

AP Name: AP9166\_0E.6220

AP slot : 2

Client State : Associated

Policy Profile : Policy4TiagoHome

Flex Profile : TiagoHomeFlexProfile

Wireless LAN Id: 5

WLAN Profile Name: wifi6E\_test

Wireless LAN Network Name (SSID): wifi6E\_test

BSSID : 7411.b2d2.9747

Connected For : 117 seconds

Protocol : 802.11ax - 6 GHz

Channel : 69

Client IIF-ID : 0xa0000002

Association Id : 33

Authentication Algorithm : Open System

[...]

Current Rate : 6.0

Supported Rates : 54.0

[...]

Policy Type : WPA3

Encryption Cipher : CCMP (AES)

Authentication Key Management : SAE

AAA override passphrase : No

SAE PWE Method : Hash to Element(H2E)

[...]

Protected Management Frame - 802.11w : Yes

EAP Type : Not Applicable

[...]

Session Manager:

Point of Attachment : capwap\_90000025

IIF ID : 0x90000025

Authorized : TRUE

Session timeout : 86400

Common Session ID: 0000000000001713C518E305

Acct Session ID : 0x00000000

Auth Method Status List

Method : SAE

Local Policies:

Service Template : wlan\_svc\_Policy4TiagoHome (priority 254)

VLAN : default

Absolute-Timer : 86400

Server Policies:

Resultant Policies:

VLAN Name : default

VLAN : 1

Absolute-Timer : 86400

[...]

FlexConnect Data Switching : Local

FlexConnect Dhcp Status : Local

FlexConnect Authentication : Local

Client Statistics:

Number of Bytes Received from Client : 550161686

Number of Bytes Sent to Client : 5751483

Number of Packets Received from Client : 417388

Number of Packets Sent to Client : 63427

Number of Policy Errors : 0

Radio Signal Strength Indicator : -52 dBm

Signal to Noise Ratio : 41 dB

[...]

Device Classification Information:

Device Type : Android-Device

Device Name : Galaxy-S23

Protocol Map : 0x000029 (OUI, DHCP, HTTP)

Intel AX211

## Client-Details in WLC:

<#root>

#show wireless client mac-address 286b.3598.580f detail

Client MAC Address : 286b.3598.580f  
[...]  
Client IPv4 Address : 192.168.1.159  
[...]  
AP MAC Address : 7411.b2d2.9740  
AP Name: AP9166\_0E.6220  
AP slot : 2  
Client State : Associated  
Policy Profile : Policy4TiagoHome  
Flex Profile : TiagoHomeFlexProfile  
Wireless LAN Id: 5  
WLAN Profile Name: wifi6E\_test  
Wireless LAN Network Name (SSID): wifi6E\_test  
BSSID : 7411.b2d2.9747  
Connected For : 145 seconds  
  
Protocol : 802.11ax - 6 GHz

Channel : 69

Client IIF-ID : 0xa0000001  
Association Id : 35  
Authentication Algorithm : Open System  
[...]  
Current Rate : 6.0  
Supported Rates : 54.0  
AAA QoS Rate Limit Parameters:  
QoS Average Data Rate Upstream : (kbps)  
QoS Realtime Average Data Rate Upstream : (kbps)  
QoS Burst Data Rate Upstream : (kbps)  
QoS Realtime Burst Data Rate Upstream : (kbps)  
QoS Average Data Rate Downstream : (kbps)  
QoS Realtime Average Data Rate Downstream : (kbps)  
QoS Burst Data Rate Downstream : (kbps)  
QoS Realtime Burst Data Rate Downstream : (kbps)  
[...]

Policy Type : WPA3

Encryption Cipher : CCMP (AES)

Authentication Key Management : SAE

AAA override passphrase : No

SAE PWE Method : Hash to Element(H2E)

[...]

Protected Management Frame - 802.11w : Yes

[...]

Session Manager:

Point of Attachment : capwap\_90000025

IIF ID : 0x90000025

Authorized : TRUE

Session timeout : 86400

Common Session ID: 000000000000171CC520478F

Acct Session ID : 0x00000000

Auth Method Status List

Method : SAE

Local Policies:

Service Template : wlan\_svc\_Policy4TiagoHome (priority 254)

VLAN : default

Absolute-Timer : 86400

Server Policies:

Resultant Policies:

VLAN Name : default

VLAN : 1

Absolute-Timer : 86400

[...]

FlexConnect Data Switching : Local

FlexConnect Dhcp Status : Local

FlexConnect Authentication : Local

Client Statistics:

Number of Bytes Received from Client : 335019921

Number of Bytes Sent to Client : 3315418

Number of Packets Received from Client : 250583

Number of Packets Sent to Client : 38960

Number of Policy Errors : 0

Radio Signal Strength Indicator : -54 dBm

Signal to Noise Ratio : 39 dB

[...]

Device Classification Information:

Device Type : LENOVO 21CCS43W0T

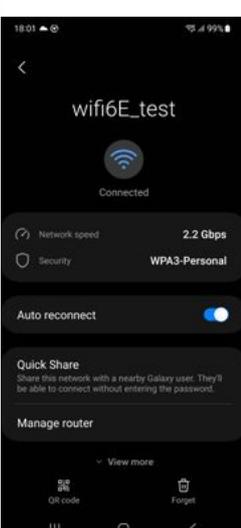
Device Name : CSCO-W-xxxxxxxx

Protocol Map : 0x000429 (OUI, DOT11, DHCP, HTTP)

Device OS : Windows 10

Hier können Sie die Netzwerkdetails sehen, die von jedem Client bereitgestellt werden:

NetzGearA8000	Pixel 6a	Samsung S23	Intel AX211
---------------	----------	-------------	-------------

<pre> Name: A8000_NETGEAR Description: NETGEAR A8000 WiFi 6 &amp; 6E Adapter Physical address (MAC): 94:18:65:48:70:95 Status: Operational Maximum transmission unit: 1500 Link speed (Receive/Transmit): 1201/1201 (Mbps) DHCP enabled: Yes DHCP servers: 192.168.1.254 DHCP lease obtained: Monday, June 19, 2023 6:20:11 PM DHCP lease expires: Tuesday, June 20, 2023 6:20:11 PM IPv4 address: 192.168.1.163/24 IPv6 address: 2001:8a0:fb91:1c00:f6e7:e29c:f0e1:63ea/64, 2001:8a0:fb91:1c00:299c:6c3b:b3c0:59b6/128 IPv4 default gateway: 192.168.1.254 IPv6 default gateway: fe80::5afc:20ff:fe9e:59af%16 DNS servers: 2001:8a0:fb91:1c00:1 (Unencrypted) 192.168.1.254 (Unencrypted) DNS domain name: Home DNS connection suffix: Home DNS search suffix list: Network name: wif6E_test </pre>			<pre> Name: Wi-Fi Description: Intel(R) Wi-Fi 6E AX211 160MHz Physical address (MAC): 28:6b:35:98:58:0f Status: Operational Maximum transmission unit: 1500 Link speed (Receive/Transmit): 2402/2402 (Mbps) DHCP enabled: Yes DHCP servers: 192.168.1.254 DHCP lease obtained: Monday, June 19, 2023 6:02:34 PM DHCP lease expires: Tuesday, June 20, 2023 6:02:34 PM IPv4 address: 192.168.1.159/24 IPv6 address: 2001:8a0:fb91:1c00:edb2:8d62:d379:c53b/64, 2001:8a0:fb91:1c00:ed62:d379:c53b/64 IPv4 default gateway: 192.168.1.254 IPv6 default gateway: fe80::5afc:20ff:fe9e:59af%8 DNS servers: 2001:8a0:fb91:1c00:1 (Unencrypted) 192.168.1.254 (Unencrypted) DNS domain name: Home DNS connection suffix: Home DNS search suffix list: Network name: wif6E_test </pre>
NetGearA8000-Client - Details	Pixel6a-Clientdetails	Details zum S23-Client	AX211-Client - Details

## Fehlerbehebung

Der Abschnitt zur Fehlerbehebung in diesem Dokument dient als allgemeine Anleitung zur Fehlerbehebung bei WLAN-Übertragungsproblemen, nicht bei clientspezifischen Problemen, die bei der Verwendung der in diesem Dokument beschriebenen Bandoperationen auftreten können.

Die Client-seitige Fehlerbehebung hängt stark vom Client-Betriebssystem ab. Windows ermöglicht es, nach Netzwerken zu suchen und festzustellen, ob die 6-GHz-BSSIDs vom Laptop gehört werden. Der Abschnitt über APs am gleichen Standort zeigt Ihnen, welche BSSIDs von denselben APs über den RNR-Bericht erfasst wurden.

```
C:\Windows\System32>netsh wlan show networks mode=Bssid
```

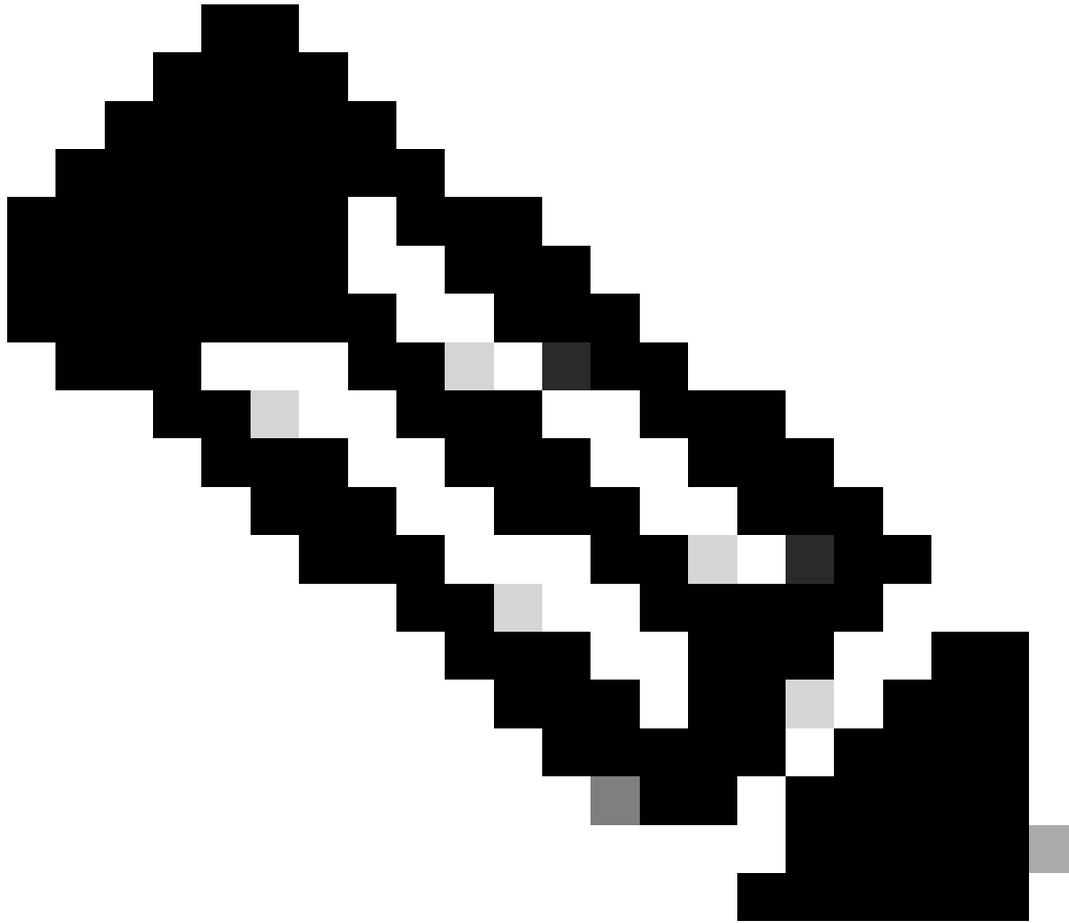
```
Interface name : A8000_NETGEAR
There are 4 networks currently visible.
(...)
```

```

SSID 3 : Darchis6
Network type           : Infrastructure
Authentication         : WPA3-Personal
Encryption             : CCMP
BSSID 1                : 10:a8:29:30:0d:07
Signal                 : 6%
Radio type             : 802.11ax
Band                   : 6 GHz
Channel                : 69
Hash-to-Element       : Supported
Bss Load:
  Connected Stations:   0
  Channel Utilization: 2 (0 %)
  Medium Available Capacity: 23437 (749984 us/s)
Colocated APs:        : 3
  BSSID: 10:a8:29:30:0d:01, Band: 2.4 GHz, Channel: 1
  BSSID: 10:a8:29:30:0d:0f, Band: 5 GHz, Channel: 36
  BSSID: 10:a8:29:30:0d:0e, Band: 5 GHz, Channel: 36
Basic rates (Mbps) : 6 12 24

```

Other rates (Mbps) : 9 18 36 48 54  
BSSID 2 : 10:a8:29:30:0d:0f  
Signal : 57%  
Radio type : 802.11ax  
Band : 5 GHz  
Channel : 36  
Hash-to-Element: : Supported  
Bss Load:  
Connected Stations: 0  
Channel Utilization: 9 (3 %)  
Medium Available Capacity: 23437 (749984 us/s)  
Colocated APs: : 1  
BSSID: 10:a8:29:30:0d:07, Band: 6 GHz , Channel: 69  
Basic rates (Mbps) : 6 12 24  
Other rates (Mbps) : 9 18 36 48 54  
BSSID 3 : 18:f9:35:4d:9d:67  
Signal : 79%  
Radio type : 802.11ax  
Band : 6 GHz  
Channel : 37  
Hash-to-Element: : Supported  
Bss Load:  
Connected Stations: 0  
Channel Utilization: 2 (0 %)  
Medium Available Capacity: 23437 (749984 us/s)  
Colocated APs: : 3  
BSSID: 18:f9:35:4d:9d:6f, Band: 5 GHz , Channel: 52  
BSSID: 18:f9:35:4d:9d:6e, Band: 5 GHz , Channel: 52  
BSSID: 18:f9:35:4d:9d:61, Band: 2.4 GHz, Channel: 11  
Basic rates (Mbps) : 6 12 24  
Other rates (Mbps) : 9 18 36 48 54



Hinweis: Siehe [Wichtige Informationen zu Debug-Befehlen](#), bevor Sie Befehle **debug** verwenden.

---

Es wird empfohlen, zur Behebung von Verbindungsproblemen mit Clients die folgenden Dokumente zu verwenden:

[Fehlerbehebung bei Verbindungsproblemen mit dem Catalyst 9800-Client:](#)

[Informationen zu Wireless-Debugs und zur Protokollierung auf Catalyst 9800 Wireless LAN-Controllern .](#)

Für die AP-Fehlerbehebung wird empfohlen, dieses Dokument zu verwenden:

[Fehlerbehebung bei COS-APs](#)

Informationen zur Berechnung und Validierung des Durchsatzes finden Sie in diesem Leitfaden:

[Leitfaden zur Prüfung und Validierung des Wireless-Durchsatzes nach 802.11ac.](#)

Obwohl es bei der Veröffentlichung von 11ac erstellt wurde, gelten die gleichen Berechnungen für 11ax.

Zugehörige Informationen

[Was ist Wi-Fi 6E?](#)

[Was ist Wi-Fi 6 im Vergleich zu Wi-Fi 6E?](#)

[Wi-Fi 6E - Informationen auf einen Blick](#)

[Wi-Fi 6E: Das nächste große Kapitel im Wi-Fi-Whitepaper](#)

[Cisco Live - Architektur eines Wireless-Netzwerks der nächsten Generation mit Catalyst Wi-Fi 6E Access Points](#)

[Länder, die Wi-Fi in 6 GHz ermöglichen \(Wi-Fi 6E\)](#)

[Software-Konfigurationsleitfaden für Cisco Catalyst Wireless Controller der Serie 9800 17.9.x](#)

[WPA3-Bereitstellungsleitfaden](#)

## 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.