

# Konfigurieren der SSIDs für 8821 Voice over Wireless auf den Catalyst Wireless Controllern 9800

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren einer SSID](#)

[Option A: Zentrales Switching](#)

[Netzwerkdiagramm](#)

[Tags und Profile](#)

[Befehlszeilenschnittstelle \(CLI\)](#)

[Option B: Lokales FlexConnect-Switching](#)

[Netzwerkdiagramm](#)

[Tags und Profile](#)

[Befehlszeilenschnittstelle \(CLI\)](#)

[Medienparameter konfigurieren](#)

[GUI-Konfiguration](#)

[Befehlszeilenschnittstelle \(CLI\)](#)

[Überprüfung](#)

[Fehlerbehebung](#)

## Einleitung

In diesem Dokument wird beschrieben, wie Sie einen 9800 Wireless LAN Controller (WLC) für eine Sprachbereitstellung mithilfe von Cisco 8821-Mobilteilen für Central Switching und FlexConnect Local Switching konfigurieren.

## Voraussetzungen

### Anforderungen

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

- Konfigurationsmodell für Catalyst Wireless 9800
- FlexConnect
- 802.11r
- Call Admission Control (CAC)

### Verwendete Komponenten

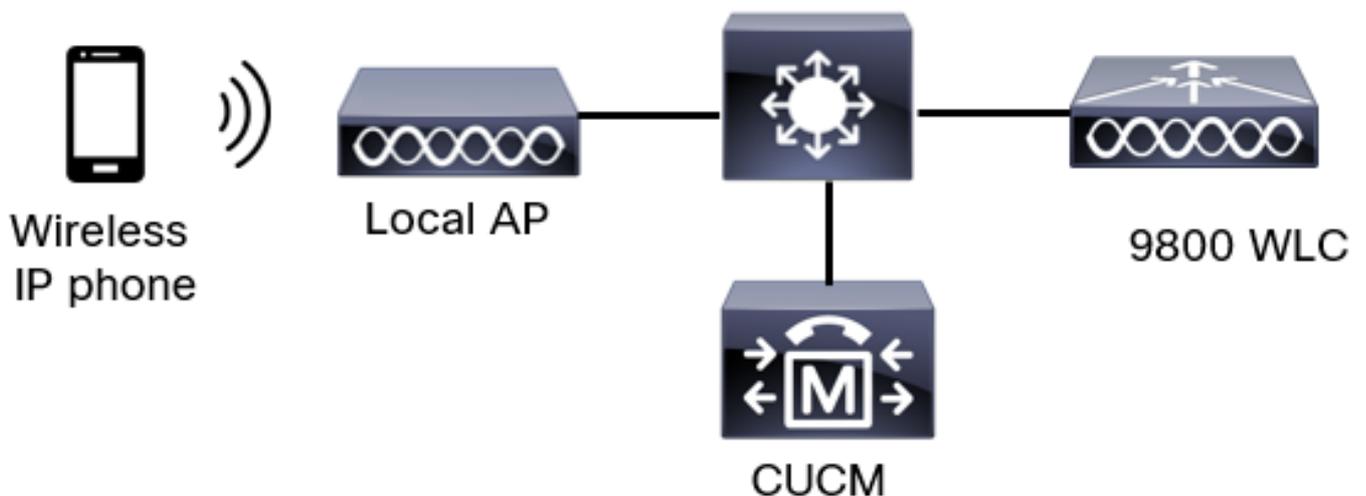
Die Informationen in diesem Dokument basieren auf einem 9800L v17.6.1.

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 potenziellen Auswirkungen eines Befehls verstehen.

## Konfigurieren einer SSID

### Option A: Zentrales Switching

#### Netzwerkdiagramm



#### Tags und Profile

In diesem Dokument wird die Konfiguration aller Tags und Profile mithilfe der **erweiterten Wireless-Einrichtung** vorgenommen, da alle Tags und Profile im gleichen Menü konfiguriert werden können.

Schritt 1: Navigieren Sie zu **Konfiguration > Wireless-Setup > Erweitert > Jetzt starten > WLAN-Profil**, und klicken Sie auf **+Hinzufügen**, um ein neues WLAN zu erstellen. Konfigurieren Sie die SSID, den Profilnamen, die WLAN-ID und den Status des WLAN. Navigieren Sie dann zu **Security > Layer 2**, und konfigurieren Sie die Einstellungen:

General **Security** Advanced**Layer2** Layer3 AAA

Layer 2 Security Mode

WPA + WPA2 ▼

MAC Filtering

Protected Management Frame

PMF

Disabled ▼

WPA Parameters

Lobby Admin Access

Fast Transition

Disabled ▼

Over the DS

Reassociation Timeout

20

MPSK Configuration

MPSK

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption

 AES(CCMP128) CCMP256 GCMP128 GCMP256

Auth Key Mgmt

 802.1x PSK Easy-PSK CCKM

- Easy-PSK
- CCKM
- FT + 802.1x
- FT + PSK
- 802.1x-SHA256
- PSK-SHA256

PSK Format ASCII ▾

PSK Type Unencrypted ▾

Pre-Shared Key\* .....|

Cancel

Apply to Device

### Sicherheitseinstellungen für Sprach-SSID Teil 3 Sicherheitseinstellungen für Sprach-SSID Teil 1

**Anmerkung:** Bei einer PSK-SSID muss FT nicht aktiviert werden, da der Handshake beim Roaming kurz ist. Bei der Konfiguration von 802.1X WPA Enterprise wird empfohlen, FT+802.1X als AKM zu aktivieren und die schnelle Umstellung zu aktivieren, jedoch "Over the DS" (Über die DS) als deaktiviert zu lassen. Sie können FT+PSK auch konfigurieren, aber in diesem Beispiel wird reguläres PSK verwendet, um der Einfachheit willen.

Schritt 2: Navigieren Sie zur Registerkarte **Erweitert**, und aktivieren Sie Aironet IE. Stellen Sie sicher, dass Load Balancing und die Bandauswahl deaktiviert sind:

Add WLAN
✕

---

General
Security
Advanced

Coverage Hole Detection <input checked="" type="checkbox"/>	Universal Admin <input type="checkbox"/>
<b>Aironet IE</b> <input checked="" type="checkbox"/>	OKC <input checked="" type="checkbox"/>
Advertise AP Name <input checked="" type="checkbox"/>	Load Balance <input type="checkbox"/>
P2P Blocking Action <span style="float: right;">Disabled ▾</span>	Band Select <input type="checkbox"/>
Multicast Buffer <span style="float: right;">DISABLED</span>	IP Source Guard <input type="checkbox"/>
Media Stream Multicast-direct <input type="checkbox"/>	WMM Policy <span style="float: right;">Allowed ▾</span>
11ac MU-MIMO <input checked="" type="checkbox"/>	mDNS Mode <span style="float: right;">Bridging ▾</span>
WiFi to Cellular Steering <input type="checkbox"/>	<span style="background-color: #ccc; padding: 5px 20px; font-weight: bold;">Off Channel Scanning Defer</span>

Cancel

Apply to Device

Stellen Sie auf derselben Seite sicher, dass die Off-Channel-Scan-Zurückstellung für die

Prioritäten 5, 6 und 7 aktiviert ist. Dadurch wird verhindert, dass der Access Point nach Erhalt eines Frames mit diesen UP-Prioritäten (im Wesentlichen ein Sprach-Frame) 100 ms von einem Kanal getrennt wird.

### Add WLAN

WiFi to Cellular Steering

Fastlane+ (ASR)

Deny LAA (RCM) clients

**Max Client Connections**

Per WLAN

Per AP Per WLAN

Per AP Radio Per WLAN

**11v BSS Transition Support**

**Off Channel Scanning Defer**

Defer Priority  0  1  2  
 3  4  5  
 6  7

Scan Defer Time

**Assisted Roaming (11k)**

Prediction Optimization

Neighbor List

Schritt 3: Wählen Sie **Richtlinienprofil** aus, und klicken Sie auf **Hinzufügen**:

The screenshot displays the configuration interface for Policy Profiles. On the left, a vertical list of items is shown under the heading "Tags & Profiles". The items are: WLAN Profile, Policy Profile (highlighted with a blue box), Policy Tag, AP Join Profile, Flex Profile, Site Tag, RF Profile, and RF Tag. Below this list is the "Apply" section, which includes "Tag APs". The "Start" button is at the top left, and the "Done" button is at the bottom left. On the right, a table lists the Policy Profile Name. The table has one row: "default-policy-profile". Above the table, there are buttons for "+ Add" (highlighted with a blue box) and "Delete". Below the table, there are navigation controls: a left arrow, a right arrow, a page number "1", and a dropdown menu showing "10 items per page".

Konfigurieren Sie den Namen des Richtlinienprofils, legen Sie den Status auf "Aktiviert" fest, und lassen Sie das Kontrollkästchen Central Switching, Authentication, DHCP und Zuordnung (nach 17.6 wird das Kontrollkästchen für die zentrale Zuordnung ausgeblendet) aktiviert:

## Add Policy Profile

⚠ 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\*

Description

Status  ENABLED

Passive Client  DISABLED

Encrypted Traffic Analytics  DISABLED

### CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

### WLAN Switching Policy

Central Switching  ENABLED

Central Authentication  ENABLED

Central DHCP  ENABLED

Flex NAT/PAT  DISABLED

Cancel

Apply to Device

Klicken Sie auf **Zugriffsrichtlinien**, und konfigurieren Sie das VLAN, dem der Wireless-Client bei der Verbindung mit der SSID **Voice** zugewiesen wird:

## Add Policy Profile

⚠ 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

RADIUS Profiling   
HTTP TLV Caching   
DHCP TLV Caching

### WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name

### VLAN

VLAN/VLAN Group

Multicast VLAN

### WLAN ACL

IPv4 ACL

IPv6 ACL

### URL Filters

Pre Auth

Post Auth

Seite mit Einstellungen für Richtlinien-Zugriffsrichtlinien

Klicken Sie auf **QoS und AVC**, und konfigurieren Sie den **Auto QoS**-Parameter als **Sprache**.  
Klicken Sie auf **Speichern** und auf **Gerät anwenden**.

## Add Policy Profile

General Access Policies **QoS and AVC** Mobility Advanced

Auto QoS

### SIP-CAC

Call Snooping

Send Disassociate

Send 486 Busy

### Flow Monitor IPv4

Egress

Ingress

### Flow Monitor IPv6

Egress

Ingress

Klicken Sie auf **Erweitert**, legen Sie das Sitzungs-Timeout auf 84000 fest, stellen Sie sicher, dass IPv4 DHCP erforderlich ist, und aktivieren Sie den ARP-Proxy.

### Edit Policy Profile

General Access Policies QOS and AVC Mobility **Advanced**

#### WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

#### DHCP

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

#### AAA Policy

Allow AAA Override

NAC State

Policy Name

Accounting List  ⓘ

#### WGB Parameters

Broadcast Tagging

WGB VLAN

#### Policy Proxy Settings

ARP Proxy

IPv6 Proxy

Fabric Profile

Link-Local Bridging

mDNS Service Policy  [Clear](#)

Hotspot Server

#### User Defined (Private) Network

Status

Drop Unicast

#### DNS Layer Security

DNS Layer Security Parameter Map  [Clear](#)

Flex DHCP Option for DNS

Flex DNS Traffic Redirect

#### WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

#### Air Time Fairness Policies

2.4 GHz Policy

5 GHz Policy

#### EoGRE Tunnel Profiles

Tunnel Profile

Seite "Policy Profile Advanced Settings"

Schritt 4: Wählen Sie **Policy Tag** aus, und klicken Sie auf **Hinzufügen**. Konfigurieren Sie den

Namen der Policy-Tag. Klicken Sie unter **WLAN-Richtlinienzuordnungen** auf **+Hinzufügen**. Wählen Sie das **WLAN-Profil** und das **Richtlinienprofil** aus den Dropdown-Menüs aus, und klicken Sie auf die Überprüfung der zu konfigurierenden Zuordnung. Klicken Sie anschließend auf **Speichern und auf Gerät anwenden**.

### Add Policy Tag ✕

Name\*

Description

▼ WLAN-POLICY Maps: 0

WLAN Profile  Policy Profile

◀ ◀ 0 ▶ ▶  items per page No items to display

#### Map WLAN and Policy

WLAN Profile\*

Policy Profile\*

➤ RLAN-POLICY Maps: 0

Schritt 5: Wählen Sie **Site Tag** aus, und klicken Sie auf **Hinzufügen**. Aktivieren Sie das **Kontrollkästchen Lokalen Standort aktivieren**, damit die Access Points im **lokalen Modus** betrieben werden können. Klicken Sie dann auf **Speichern und auf Gerät anwenden**:

### Add Site Tag ✕

Name\*

Description

AP Join Profile

Control Plane Name

Enable Local Site

Schritt 6: Wählen Sie **RF-Profil** aus und klicken Sie auf **Hinzufügen**. Konfigurieren Sie ein RF-Profil

pro Band.

**Add RF Profile** ✕

General 802.11 RRM Advanced

Name\*

Radio Band  ▼

Status ENABLE

Description

↶ Cancel Save & Apply to Device

**Add RF Profile** ✕

General 802.11 RRM Advanced

Name\*

Radio Band  ▼

Status ENABLE

Description

↶ Cancel Save & Apply to Device

Navigieren Sie zum Menü **802.11**. Deaktivieren Sie alle Raten unter 12 Mbit/s, legen Sie als obligatorische Rate 12 Mbit/s fest, und 18 Mbit/s und höher, je nach Unterstützung auf beiden Bändern.

Datenraten von 2,4 GHz:

General

802.11

RRM

Advanced

## Operational Rates

1 Mbps	Disabled
2 Mbps	Disabled
5.5 Mbps	Disabled
6 Mbps	Disabled
9 Mbps	Disabled
11 Mbps	Disabled
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Supported
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

## 802.11n MCS Rates

Enabled Data Rates:

```
[0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31]
```

Enable	MCS Index
<input checked="" type="checkbox"/>	0
<input checked="" type="checkbox"/>	1
<input checked="" type="checkbox"/>	2
<input checked="" type="checkbox"/>	3
<input checked="" type="checkbox"/>	4
<input checked="" type="checkbox"/>	5
<input checked="" type="checkbox"/>	6
<input checked="" type="checkbox"/>	7
<input checked="" type="checkbox"/>	8
<input checked="" type="checkbox"/>	9

◀ 1 2 3 4 ▶▶

10 items per page

1 - 10 of 32 items

Cancel

Save &amp; Apply to Device

Datenraten von 5 GHz:

General

802.11

RRM

Advanced

## Operational Rates

6 Mbps	Disabled ▼
9 Mbps	Disabled ▼
12 Mbps	Mandatory ▼
18 Mbps	Supported ▼
24 Mbps	Supported ▼
36 Mbps	Supported ▼
48 Mbps	Supported ▼
54 Mbps	Supported ▼

## 802.11n MCS Rates

Enabled Data Rates:

```
[0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31]
```

Enable	MCS Index ▼
<input checked="" type="checkbox"/>	0
<input checked="" type="checkbox"/>	1
<input checked="" type="checkbox"/>	2
<input checked="" type="checkbox"/>	3
<input checked="" type="checkbox"/>	4
<input checked="" type="checkbox"/>	5
<input checked="" type="checkbox"/>	6
<input checked="" type="checkbox"/>	7
<input checked="" type="checkbox"/>	8
<input checked="" type="checkbox"/>	9

◀ 1 2 3 4 ▶▶

10 ▼ items per page

1 - 10 of 32 items

Cancel

Save &amp; Apply to Device

Schritt 7: Wählen Sie **RF-Tag** aus, und klicken Sie auf **Hinzufügen**. Wählen Sie die in Schritt 5 dieses Abschnitts erstellten RF-Profilen aus. Klicken Sie anschließend auf **Speichern und auf Gerät anwenden**.

### Add RF Tag ✕

Name\*

Description

5 GHz Band RF Profile  ▼

2.4 GHz Band RF Profile  ▼

Schritt 8: Wählen Sie **Tag-APs aus**, wählen Sie die APs aus, und fügen Sie die zuvor erstellten Richtlinien-, Site- und RF-Tags hinzu. Klicken Sie anschließend auf **Speichern und auf Gerät anwenden**.

### Tag APs ✕

Tags

Policy  ▼

Site  ▼

RF  ▼

*Changing AP Tag(s) will cause associated AP(s) to reconnect*

### Befehlszeilenschnittstelle (CLI)

Führen Sie über die CLI die folgenden Befehle aus:

```
////////// WLAN Configuration
wlan Voice 1 Voice
```

```
ccx aironet-iesupport
no security ft adaptive
security wpa psk set-key ascii 0 Cisco123
no security wpa akm dot1x
security wpa akm psk
no shutdown
```

#### **//////// Policy Profile Configuration**

```
wireless profile policy PP1
autoqos mode voice
ipv4 arp-proxy
service-policy input platinum-up
service-policy output platinum
session-timeout 84000
vlan 1
no shutdown
```

#### **//////// Policy Tag Configuration**

```
wireless tag policy PT1
wlan Voice policy PP1
```

#### **//////// Site Tag Configuration**

```
wireless tag site ST1
local-site
```

#### **//////// 2.4 GHz RF Profile Configuration**

```
ap dot11 24ghz rf-profile Voice24GHz
rate RATE_11M disable
rate RATE_12M mandatory
rate RATE_1M disable
rate RATE_2M disable
rate RATE_5_5M disable
rate RATE_6M disable
rate RATE_9M disable
no shutdown
```

#### **//////// 5 GHz RF Profile Configuration**

```
ap dot11 5ghz rf-profile Voice5GHz
rate RATE_24M supported
rate RATE_6M disable
rate RATE_9M disable
no shutdown
```

#### **//////// RF Tag Configuration**

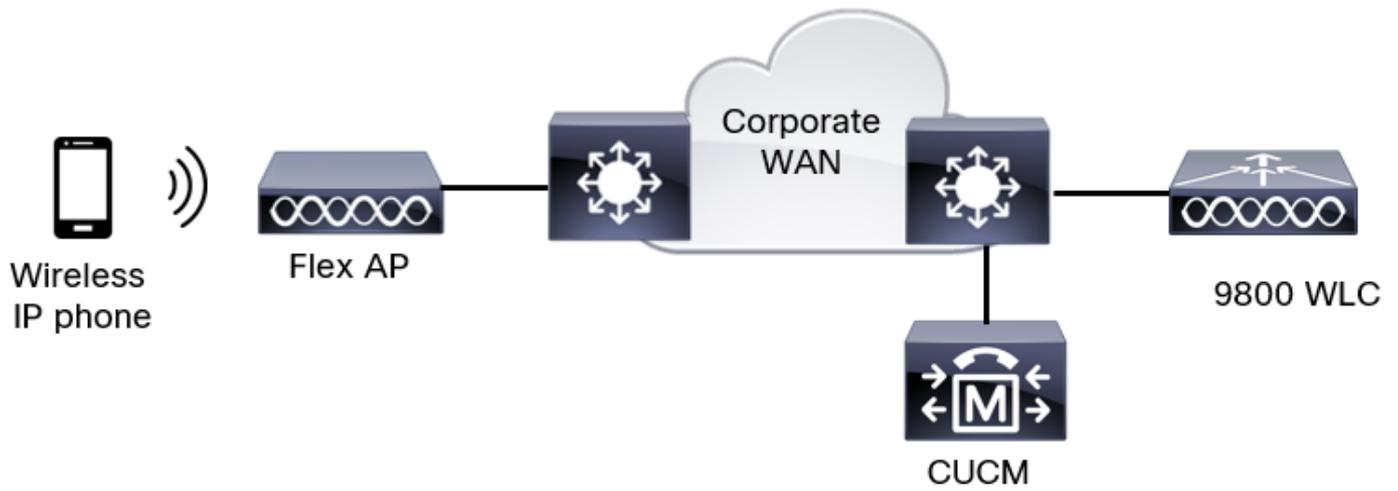
```
wireless tag rf RT1
24ghz-rf-policy Voice24GHz
5ghz-rf-policy Voice5GHz
```

#### **//////// AP Configuration**

```
ap a023.9f86.52c0
policy-tag PT1
rf-tag RT1
site-tag ST1
```

## **Option B: Lokales FlexConnect-Switching**

### **Netzwerkdiagramm**



## Tags und Profile

Schritt 1: Navigieren Sie zu **Konfiguration > Wireless-Setup > Erweitert > Jetzt starten > WLAN-Profil**, und klicken Sie auf **+Hinzufügen**, um ein neues WLAN zu erstellen. Konfigurieren Sie die SSID, den Profilnamen, die WLAN-ID und den Status des WLAN. Navigieren Sie dann zu **Security > Layer 2**, und konfigurieren Sie die Einstellungen:

Add WLAN
✕

---

General

Security

Advanced

Layer2

Layer3

AAA

Layer 2 Security Mode WPA + WPA2 ▼

MAC Filtering

Protected Management Frame

PMF Disabled ▼

WPA Parameters

Lobby Admin Access

Fast Transition Disabled ▼

Over the DS

Reassociation Timeout 20

MPSK Configuration

MPSK

WPA Policy	<input type="checkbox"/>
WPA2 Policy	<input checked="" type="checkbox"/>
GTK Randomize	<input type="checkbox"/>
OSEN Policy	<input type="checkbox"/>
WPA2 Encryption	<input checked="" type="checkbox"/> AES(CCMP128) <input type="checkbox"/> CCMP256 <input type="checkbox"/> GCMP128 <input type="checkbox"/> GCMP256
Auth Key Mgmt	<input type="checkbox"/> 802.1x <input checked="" type="checkbox"/> PSK <input type="checkbox"/> Easy-PSK <input type="checkbox"/> CCKM

## Sprach-SSID-Sicherheitseinstellungen Teil 2

	<input type="checkbox"/> Easy-PSK <input type="checkbox"/> CCKM <input type="checkbox"/> FT + 802.1x <input type="checkbox"/> FT + PSK <input type="checkbox"/> 802.1x-SHA256 <input type="checkbox"/> PSK-SHA256
PSK Format	ASCII
PSK Type	Unencrypted
Pre-Shared Key*	.....

Cancel

Apply to Device

## Sicherheitseinstellungen für Sprach-SSID Teil 3

**Anmerkung:** Bei einer PSK-SSID muss FT nicht aktiviert werden, da der Handshake beim Roaming kurz ist. Bei der Konfiguration von 802.1X WPA Enterprise wird empfohlen, FT+802.1X als AKM zu aktivieren und die schnelle Umstellung zu aktivieren, jedoch "Over the DS" (Über die DS) als deaktiviert zu lassen. Sie können FT+PSK auch konfigurieren, aber in diesem Beispiel wird reguläres PSK verwendet, um der Einfachheit willen.

Schritt 2: Navigieren Sie zur Registerkarte **Erweitert**, und aktivieren Sie Aironet IE. Stellen Sie sicher, dass Load Balancing und die Bandauswahl deaktiviert sind:

**Add WLAN** ✕

General   Security   **Advanced**

Coverage Hole Detection	<input checked="" type="checkbox"/>	Universal Admin	<input type="checkbox"/>
<b>Aironet IE</b>	<input checked="" type="checkbox"/>	OKC	<input checked="" type="checkbox"/>
Advertise AP Name	<input checked="" type="checkbox"/>	Load Balance	<input type="checkbox"/>
P2P Blocking Action	Disabled ▾	Band Select	<input type="checkbox"/>
Multicast Buffer	<input type="checkbox"/> DISABLED	IP Source Guard	<input type="checkbox"/>
Media Stream Multicast-direct	<input type="checkbox"/>	WMM Policy	Allowed ▾
11ac MU-MIMO	<input checked="" type="checkbox"/>	mDNS Mode	Bridging ▾
WiFi to Cellular Steering	<input type="checkbox"/>	<b>Off Channel Scanning Defer</b>	

Stellen Sie auf derselben Seite sicher, dass die Off-Channel-Scan-Zurückstellung für die Prioritäten 5, 6 und 7 aktiviert ist. Dadurch wird verhindert, dass der Access Point nach Erhalt eines Frames mit diesen UP-Prioritäten (im Wesentlichen ein Sprach-Frame) 100 ms von einem Kanal getrennt wird.

**Add WLAN** ✕

WiFi to Cellular Steering	<input type="checkbox"/>	<b>Off Channel Scanning Defer</b> Defer Priority <input type="checkbox"/> 0 <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input type="checkbox"/> 7 Scan Defer Time <input type="text" value="100"/>	
Fastlane+ (ASR)	<input checked="" type="checkbox"/>		
Deny LAA (RCM) clients	<input type="checkbox"/>		
<b>Max Client Connections</b>			
Per WLAN	<input type="text" value="0"/>	<b>Assisted Roaming (11k)</b>	
Per AP Per WLAN	<input type="text" value="0"/>	Prediction Optimization	<input type="checkbox"/>
Per AP Radio Per WLAN	<input type="text" value="200"/>	Neighbor List	<input checked="" type="checkbox"/>

Schritt 3: Wählen Sie **Richtlinienprofil** aus, und klicken Sie auf **Hinzufügen**:

The screenshot displays the configuration interface for wireless setup. On the left, a vertical flowchart starts with a 'Start' button and ends with a 'Done' button. The flowchart is divided into sections: 'Tags & Profiles' and 'Apply'. Under 'Tags & Profiles', there are several items: 'WLAN Profile', 'Policy Profile' (highlighted with a blue box), 'Policy Tag', 'AP Join Profile', 'Flex Profile', 'Site Tag', 'RF Profile', and 'RF Tag'. Each item has an information icon and a checkbox. Under 'Apply', there is 'Tag APs'. On the right, there is a '+ Add' button (highlighted with a blue box) and a 'Delete' button. Below these buttons is a table with the following content:

Policy Profile Name
<input type="checkbox"/> default-policy-profile

Below the table, there are navigation controls: a left arrow, a right arrow, a box containing '1', and a dropdown menu showing '10 items per page'.

Konfigurieren Sie den Namen des Richtlinienprofils, legen Sie den Status auf Aktiviert fest, deaktivieren Sie Central Switching und Central DHCP. Bei einer PSK-SSID kann die Authentifizierung auf "Lokal" verschoben werden, um dem Access Point die Funktion zur Überprüfung des PSK zu geben. Bei 802.1X soll der WLC in der Regel weiterhin die 802.1X-Authentifizierungen durchführen.

Add Policy Profile ✕

⚠ 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\*

Description

Status ENABLED

Passive Client  DISABLED

Encrypted Traffic Analytics  DISABLED

**CTS Policy**

Inline Tagging

SGACL Enforcement

Default SGT

**WLAN Switching Policy**

Central Switching  DISABLED

Central Authentication ENABLED

Central DHCP  DISABLED

Flex NAT/PAT  DISABLED

↶ Cancel

📄 Apply to Device

### Konfiguration des Flex Local Switching Policy-Profiles

Navigieren Sie zur Registerkarte **Zugriffsrichtlinien**, um das VLAN zuzuweisen, dem die Wireless-Clients standardmäßig zugewiesen sind, wenn sie eine Verbindung zu diesem WLAN herstellen. Sie können entweder einen VLAN-Namen aus dem Dropdown-Menü auswählen oder eine VLAN-ID manuell eingeben.

Klicken Sie auf **QoS und AVC**, und konfigurieren Sie den **Auto QoS**-Parameter als **Sprache**.  
Klicken Sie auf **Speichern und auf Gerät anwenden**.

## Add Policy Profile



General

Access Policies

**QoS and AVC**

Mobility

Advanced

Auto QoS

Voice



SIP-CAC

Call Snooping

Send Disassociate

Send 486 Busy

Flow Monitor IPv4

Egress

Search or Select



Ingress

Search or Select



Flow Monitor IPv6

Egress

Search or Select



Ingress

Search or Select



Cancel

Save & Apply to Device

Klicken Sie auf **Erweitert**, legen Sie das Sitzungs-Timeout auf 84000 fest, stellen Sie sicher, dass IPv4 DHCP erforderlich ist, und deaktivieren Sie den ARP-Proxy.

General

Access Policies

QOS and AVC

Mobility

**Advanced**

## WLAN Timeout

Session Timeout (sec) Idle Timeout (sec) Idle Threshold (bytes) Client Exclusion Timeout (sec)  Guest LAN Session Timeout 

## DHCP

IPv4 DHCP Required DHCP Server IP Address [Show more >>>](#)

## AAA Policy

Allow AAA Override NAC State Policy Name Accounting List  ⓘ

## WGB Parameters

Broadcast Tagging WGB VLAN 

## Policy Proxy Settings

ARP Proxy  DISABLEDIPv6 Proxy Fabric Profile  Link-Local Bridging mDNS Service Policy  [Clear](#)Hotspot Server 

## User Defined (Private) Network

Status Drop Unicast 

## DNS Layer Security

DNS Layer Security Parameter Map  [Clear](#)Flex DHCP Option for DNS  ENABLEDFlex DNS Traffic Redirect  IGNORE

## WLAN Flex Policy

VLAN Central Switching Split MAC ACL 

## Air Time Fairness Policies

2.4 GHz Policy 5 GHz Policy 

## EoGRE Tunnel Profiles

Tunnel Profile 

## Erweiterte Einstellungen des Flex-Richtlinienprofils

Schritt 4: Wählen Sie **Policy Tag** aus, und klicken Sie auf **Hinzufügen**. Konfigurieren Sie den Namen der Policy-Tag. Klicken Sie unter **WLAN-Richtlinienzuordnungen** auf **+Hinzufügen**. Wählen Sie das **WLAN-Profil** und das **Richtlinienprofil** aus den Dropdown-Menüs aus, und klicken Sie auf die Überprüfung, um die zu konfigurierende Zuordnung zu überprüfen. Klicken Sie anschließend

auf **Speichern** und auf **Gerät anwenden**.

### Add Policy Tag ✕

Name\*

Description

▼ WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
No items to display	

Map WLAN and Policy

WLAN Profile\*  Policy Profile\*

➤ RLAN-POLICY Maps: 0

Schritt 5: Klicken Sie auf **Flex Profile** und dann auf **Add**. Konfigurieren Sie den Namen des Flex-Profiles, die native VLAN-ID und aktivieren Sie das ARP-Caching:

## Edit Flex Profile

### General

Local Authentication

Policy ACL

VLAN

DNS Layer Security

Name*	FP2	Fallback Radio Shut	<input type="checkbox"/>
Description	Enter Description	Flex Resilient	<input type="checkbox"/>
Native VLAN ID	1	ARP Caching	<input checked="" type="checkbox"/>
HTTP Proxy Port	0	Efficient Image Upgrade	<input checked="" type="checkbox"/>
HTTP-Proxy IP Address	0.0.0.0	OfficeExtend AP	<input type="checkbox"/>
<b>CTS Policy</b>		Join Minimum Latency	<input type="checkbox"/>
Inline Tagging	<input type="checkbox"/>	IP Overlap	<input type="checkbox"/>
SGACL Enforcement	<input type="checkbox"/>	mDNS Flex Profile	Search or Select ▼
CTS Profile Name	default-sxp-profile ▼		

### Einstellungen für Flex-Profilrichtlinien

**Anmerkung:** Die native VLAN-ID bezieht sich auf das native VLAN, das im Switch-Port konfiguriert wurde. Die APs, die diesem Flex Profile zugeordnet sind, sind mit verbunden.

Schritt 6: Wählen Sie **Site Tag** aus, und klicken Sie auf **Hinzufügen**. Konfigurieren Sie den Namen der Site-Tag, deaktivieren Sie die Option **Lokalen Standort aktivieren**, und fügen Sie das Flex-Profil hinzu. Klicken Sie anschließend auf **Speichern und auf Gerät anwenden**.

### Add Site Tag

Name*	ST2
Description	Enter Description
AP Join Profile	default-ap-profile ▼
Flex Profile	FP2 ▼
Control Plane Name	default-control-plane ▼
Enable Local Site	<input type="checkbox"/>

**Anmerkung:** Da Lokalen Standort aktivieren deaktiviert ist, werden die dieser Site-Tag zugewiesenen APs automatisch als FlexConnect-APs konfiguriert.

Schritt 7: Wählen Sie **RF-Profil aus** und klicken Sie auf **Hinzufügen**. Konfigurieren Sie ein RF-Profil pro Band.

**Add RF Profile** ✕

**General** 802.11 RRM Advanced

Name\*

Radio Band  ▼

Status **ENABLE**

Description

↶ Cancel Save & Apply to Device

**Add RF Profile** ✕

**General** 802.11 RRM Advanced

Name\*

Radio Band  ▼

Status **ENABLE**

Description

↶ Cancel Save & Apply to Device

Navigieren Sie zum Menü **802.11**. Deaktivieren Sie alle Raten unter 12 Mbit/s, legen Sie als obligatorische Rate 12 Mbit/s und höher 18 Mbit/s und höher fest, je nach Unterstützung auf beiden Bändern.

Datenraten von 2,4 GHz:

General

802.11

RRM

Advanced

## Operational Rates

1 Mbps	Disabled
2 Mbps	Disabled
5.5 Mbps	Disabled
6 Mbps	Disabled
9 Mbps	Disabled
11 Mbps	Disabled
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Supported
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

## 802.11n MCS Rates

Enabled Data Rates:

```
[0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31]
```

Enable	MCS Index
<input checked="" type="checkbox"/>	0
<input checked="" type="checkbox"/>	1
<input checked="" type="checkbox"/>	2
<input checked="" type="checkbox"/>	3
<input checked="" type="checkbox"/>	4
<input checked="" type="checkbox"/>	5
<input checked="" type="checkbox"/>	6
<input checked="" type="checkbox"/>	7
<input checked="" type="checkbox"/>	8
<input checked="" type="checkbox"/>	9

◀ 1 2 3 4 ▶▶

10 items per page

1 - 10 of 32 items

Cancel

Save &amp; Apply to Device

Datenraten von 5 GHz:

General

802.11

RRM

Advanced

## Operational Rates

6 Mbps	Disabled
9 Mbps	Disabled
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Supported
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

## 802.11n MCS Rates

Enabled Data Rates:

```
[0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31]
```

Enable	MCS Index
<input checked="" type="checkbox"/>	0
<input checked="" type="checkbox"/>	1
<input checked="" type="checkbox"/>	2
<input checked="" type="checkbox"/>	3
<input checked="" type="checkbox"/>	4
<input checked="" type="checkbox"/>	5
<input checked="" type="checkbox"/>	6
<input checked="" type="checkbox"/>	7
<input checked="" type="checkbox"/>	8
<input checked="" type="checkbox"/>	9

10 items per page  
1 - 10 of 32 items

Cancel

Save &amp; Apply to Device

Schritt 8: Wählen Sie **RF-Tag** aus, und klicken Sie auf **Hinzufügen**. Konfigurieren Sie die in Schritt 6 erstellten RF-Profilen. In diesem Abschnitt beschrieben. Klicken Sie anschließend auf **Speichern** und auf **Gerät anwenden**.

### Add RF Tag ✕

Name\*

Description

5 GHz Band RF Profile

2.4 GHz Band RF Profile

Schritt 9: Wählen Sie **Tag-APs aus**, wählen Sie die APs aus, und fügen Sie die zuvor erstellten Richtlinien-, Site- und RF-Tags hinzu. Klicken Sie anschließend auf **Speichern und auf Gerät anwenden**.

### Tag APs ✕

Tags

Policy

Site

RF

*Changing AP Tag(s) will cause associated AP(s) to reconnect*

Der AP startet den CAPWAP-Tunnel neu und schließt sich dem 9800 WLC wieder an. Navigieren Sie zu **Configuration > Wireless > Access Points**, und überprüfen Sie, ob der AP-Modus **Flex** lautet:

AP Name	Total Slots	AP Model	Base Radio MAC	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag	Tag Source	Location	Country
AP2802I-21	2	AIR-AP2802I-B-K9	a023.9f86.52c0	Flex	Enabled	Registered	PT2	ST2	RT2	Static	default location	US

## Befehlszeilenschnittstelle (CLI)

Führen Sie über die CLI die folgenden Befehle aus:

### ////////// WLAN Configuration

```
wlan Voice 1 Voice
  ccx aironet-iesupport
no security ft adaptive
security wpa psk set-key ascii 0 Cisc0123
no security wpa akm dot1x
security wpa akm psk
no shutdown
```

### ////////// Policy Profile Configuration

```
wireless profile policy PP2
do wireless autoqos policy-profile PP2 mode voice
service-policy input platinum-up
service-policy output platinum
vlan 2672
no shutdown
```

### ////////// Policy Tag Configuration

```
wireless tag policy PT2
wlan Voice policy PP2
```

### ////////// Flex Profile Configuration

```
wireless profile flex FP2
arp-caching
vlan-name 1
native-vlan-id 1
```

### ////////// Site Tag Configuration

```
wireless tag site ST2
no local-site
flex-profile FP2
```

### ////////// 2.4 GHz RF Profile Configuration

```
ap dot11 24ghz rf-profile Voice24GHz
rate RATE_11M disable
rate RATE_12M mandatory
rate RATE_1M disable
rate RATE_2M disable
rate RATE_5_5M disable
rate RATE_6M disable
rate RATE_9M disable
no shutdown
```

### ////////// 5 GHz RF Profile Configuration

```
ap dot11 5ghz rf-profile Voice5GHz
rate RATE_24M supported
rate RATE_6M disable
rate RATE_9M disable
no shutdown
```

### ////////// RF Tag Configuration

```
wireless tag rf RT2
24ghz-rf-policy Voice24GHz
5ghz-rf-policy Voice5GHz
```

### ////////// AP Configuration

```
ap a023.9f86.52c0
```

policy-tag PT2

rf-tag RT2

site-tag ST2

# Medienparameter konfigurieren

## GUI-Konfiguration

Schritt 1: Navigieren Sie zu **Konfiguration > Funkkonfiguration > Netzwerk**. Deaktivieren Sie das 5-GHz- und das 2,4-GHz-Band, und klicken Sie auf **Anwenden**.

Achten Sie darauf, dass dies vorübergehend alle Ihre 5ghz WiFi-Netzwerke deaktivieren wird! Führen Sie dies nur aus, wenn Sie sich in einem Wartungsfenster befinden.

[Configuration](#) > [Radio Configurations](#) > [Network](#)

5 GHz Band

2.4 GHz Band

General

5 GHz Network Status

Beacon Interval\*

100

Fragmentation Threshold(bytes)\*

2346

DTPC Support

Schritt 2: Navigieren Sie zu **Konfiguration > Funkkonfiguration > Medienparameter**. Aktivieren Sie die Optionen Zugangskontrolle, Load Based Call Admission Control (CAC) und Traffic Stream Metrics (TSM) im 2,4-GHz- und 5-GHz-Band, und klicken Sie auf **Apply**:

## Voice

### Call Admission Control (CAC)

Admission Control (ACM)

Load Based CAC

Max RF Bandwidth (%)\*

75

Reserved Roaming Bandwidth (%)\*

6

Expedited Bandwidth

### SIP CAC and Bandwidth

SIP CAC Support

Schritt 3: Navigieren Sie zu **Konfiguration > Funkkonfigurationen > Parameter**. Konfigurieren Sie das EDCA-Profil als **optimierte Sprache** auf beiden Bändern, und klicken Sie auf **Apply**.

[Configuration](#) > [Radio Configurations](#) > [Parameters](#)

**5 GHz Band**

2.4 GHz Band

### EDCA Parameters

EDCA Profile

optimized-voice

### DFS (802.11h)

Schritt 4: Navigieren Sie zu **Konfiguration > Funkkonfiguration > Netzwerk**. Aktivieren Sie das 5-GHz- und das 2,4-GHz-Band, und klicken Sie auf **Übernehmen**.

## Befehlszeilenschnittstelle (CLI)

Führen Sie in der CLI folgende Befehle aus:

```
Andressi_9800(config)#ap dot11 24ghz shutdown
Andressi_9800(config)#ap dot11 5ghz shutdown
```

```
Andressi_9800(config)#dot11 24ghz cac voice acm
Andressi_9800(config)#dot11 24ghz tsm
```

```
Andressi_9800(config)#dot11 5ghz cac voice acm
Andressi_9800(config)#dot11 5ghz tsm
```

```
Andressi_9800(config)#ap dot11 24ghz edca-parameters optimized-voice
Andressi_9800(config)#ap dot11 5ghz edca-parameters optimized-voice
```

```
Andressi_9800(config)#no ap dot11 24ghz shutdown
Andressi_9800(config)#no ap dot11 5ghz shutdown
```

## Überprüfung

Mithilfe dieser Befehle können Sie die aktuelle Konfiguration überprüfen:

```
# show wlan { summary | id | name | all }
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

Führen Sie folgende Befehle aus, um die CAC-Statistiken und die Anrufsteuerungsmetriken zu überprüfen:

```
#show ap name AP2802I-21 dot11 5ghz voice stats
#show ap name <ap-name> dot11 5ghz call-control metrics
```

## Fehlerbehebung

### Bedingtes Debuggen und Radio Active Tracing

Die Radio Active (RA)-Ablaufverfolgung stellt Ablaufverfolgungen auf Debugebene für alle Prozesse bereit, die mit der angegebenen Bedingung interagieren (in diesem Fall Client MAC-Adresse). Führen Sie die folgenden Schritte aus, um bedingtes Debuggen zu aktivieren. Wir konzentrieren uns auf die Ausgabe, die der 9800 WLC während eines Anrufs bereitstellt.

Schritt 1: Stellen Sie sicher, dass keine Debugbedingungen aktiviert sind.

```
# clear platform condition all
```

Schritt 2: Aktivieren Sie die Debugbedingung für die MAC-Adresse des Wireless-Clients, die

überwacht werden soll. Mit diesem Befehl wird die angegebene MAC-Adresse für 30 Minuten (1800 Sekunden) überwacht. Optional können Sie diese Zeit auf bis zu 2085978494 Sekunden erhöhen.

```
# debug wireless mac <8821-MAC-address> {monitor-time <seconds>}
```

**Hinweis:** Um mehrere Clients gleichzeitig zu überwachen, führen Sie den Befehl `debug wireless mac <aaa.bbbb.cccc>` pro MAC-Adresse aus.

**Hinweis:** Die Ausgabe der Clientaktivität in der Terminalsitzung wird nicht angezeigt, da alles intern gepuffert wird, um später angezeigt zu werden.

Schritt 3: Stellen Sie einen Anruf vom Cisco IP-Telefon 8821 her.

Schritt 4: Beenden Sie das Debuggen, wenn der Anruf beendet ist oder das Problem reproduziert wird, bevor die Standard- oder konfigurierte Überwachungszeit aktiv ist.

```
# no debug wireless mac <8821-MAC-address>
```

Wenn die Überwachungszeit abgelaufen ist oder die Wireless-Debugging-Funktion beendet wurde, generiert der 9800 WLC eine lokale Datei mit dem Namen:

```
ra_trace_MAC_aaabbbccccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year_year.log
```

Schritt 5: Erfassen Sie die Datei der MAC-Adressenaktivität. Sie können die Datei `ra trace.log` auf einen externen Server kopieren oder die Ausgabe direkt auf dem Bildschirm anzeigen. Überprüfen Sie den Namen der RA Traces-Datei.

```
# dir bootflash: | inc ra_trace
```

Kopieren Sie die Datei auf einen externen Server:

```
# copy bootflash:ra_trace_MAC_aaabbbccccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year_year.log  
tftp://a.b.c.d/ra-FILENAME.txt
```

Inhalte anzeigen:

```
# more bootflash:ra_trace_MAC_aaabbbccccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year_year.log
```

Schritt 6: Entfernen Sie die Debugbedingungen.

```
# clear platform condition all
```

**Anmerkung:** Stellen Sie sicher, dass Sie die Debugbedingungen immer nach einer Fehlerbehebungssitzung entfernen.

Bei der Ausgabe der RA Trace (RA Trace) wird die Traffic Specification (TSPEC)-Aushandlung durchgeführt. Diese bestimmt, ob der 8821-Router den Datenverkehr mit der Benutzerpriorität 6

kennzeichnen darf und ob der Anruf eingerichtet werden kann oder nicht. Um die Verwendung von Warteschlange 6 auszuhandeln, sendet der 8821 und das Action Packet fordert eine Genehmigung an.

```
2019/08/25 18:53:54.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24
Got action frame from this client.
2019/08/25 18:53:54.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24
Received Action frame with code 0: ADDTS request
2019/08/25 18:53:54.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24
Got LBCAC Metrics IE:
2019/08/25 18:53:54.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24
ADD TS from mobile slot_id 1 direction = 3
up = 6, tid = 6, upsd = 1, medium_time = 653, TSRSIE: No
2019/08/25 18:53:54.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24
U-APSD Power save
```

Bei einer Paketerfassung:

```
▶ IEEE 802.11 Action, Flags: .....C
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters
    Category code: Management Notification (17)
    Action code: Setup request (0x0000)
    Dialog token: 0x2a
    Status code: Admission accepted (0x0000)
  ▼ Tagged parameters (84 bytes)
    ▼ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: TSPEC Element
      Tag Number: Vendor Specific (221)
      Tag length: 61
      OUI: 00:50:f2 (Microsoft Corp.)
      Vendor Specific OUI Type: 2
      Type: WMM/WME (0x02)
      WME Subtype: TSPEC Element (2)
      WME Version: 1
    ▼ TS Info: 0x0034ec
      .... .. 0 110. = TID: 6
      .... .. 11. .... = Direction: Bidirectional link (3)
      .... .. 1.. .... = PSB: U-APSD (1)
      .... .. 11 0... .. = UP: Voice (6)
      0000 0000 00... ..00 1... ..0 = Reserved: 0x000080
```

Der WLC bestimmt, ob genügend Bandbreite vorhanden ist, um den Anruf zuzuweisen, und sendet in diesem Fall einen Action Frame, der die TSPEC-Aushandlung akzeptiert:

```
2019/08/25 18:53:54.510 {wncd_x_R0-0}{1}: [auth-mgr] [18106]: (info): [0000.0000.0000:unknown]
Session info 0x559e2019/08/25 18:53:54.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info):
MAC: 0027.902a.ab24 LBCAC checks for tspec PASSED for ms slot_id 1 bw_req = 653, tot_available
MT for tspecs = 22031 tx_queue_req = 20, current tx queue util = 0
2019/08/25 18:53:54.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): Calls in progress
incremented to 1
2019/08/25 18:53:54.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): allocating voice bw
for client: maxBW = 23437, BW requested = 653, total voice bw alloc = 653
2019/08/25 18:53:54.511 {wncd_x_R0-0}{1}: [ewlc-qos-client] [18106]: (info): MAC: 0027.902a.ab24
Call Accepted for tspec client
```

```

2019/08/25 18:53:54.511 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (ERR): MAC: 0027.902a.ab24
TCLAS Set Not used for TCLAS of tid=6
2019/08/25 18:53:54.511 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): Recommended rate
6500kbps:MCS 0 is not operational for radio: 6
2019/08/25 18:53:54.511 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): Recommended rate
13000kbps:MCS 1 is not operational for radio: 6
2019/08/25 18:53:54.511 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): Recommended rate
26000kbps:MCS 3 is not operational for radio: 6
2019/08/25 18:53:54.511 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24
Sending Successful ADD TS resp to mobile slot_id 1
2019/08/25 18:53:54.511 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24
Build ADD TS slot:1, tid:6, user_priority:6, upsd_enable:1, dir:3,bandwidth:653, avail_bw:0,
inactive_timer:0, tsm_req_id:0
2019/08/25 18:53:54.511 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: a023.9f86.52c0
send qos ADD TS payload to AP

```

Bei einer Paketerfassung:

```

▶ IEEE 802.11 Action, Flags: .....C
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters
    Category code: Management Notification (17)
    Action code: Setup response (0x0001)
    Dialog token: 0x2a
    Status code: Admission accepted (0x0000)
  ▼ Tagged parameters (119 bytes)
    ▼ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: TSPEC Element
      Tag Number: Vendor Specific (221)
      Tag length: 61
      OUI: 00:50:f2 (Microsoft Corp.)
      Vendor Specific OUI Type: 2
      Type: WMM/WME (0x02)
      WME Subtype: TSPEC Element (2)
      WME Version: 1
      ▼ TS Info: 0x0034ec
        .... 0 110. = TID: 6
        .... .11. .... = Direction: Bidirectional link (3)
        .... .1.. .... = PSB: U-APSD (1)
        .... .11 0... .... = UP: Voice (6)
        0000 0000 00.. ..00 1... ..0 = Reserved: 0x000080

```

Anschließend wird der Anruf über SIP mit dem Anrufmanager eingerichtet, und der RTP-Datenverkehr wird weitergeleitet.

Time	Source	Destination	Transmitter address	Receiver address	Protocol	Info
16:11:41.860804	172.16.78.64	172.16.56.109	00:27:90:2a:ab:24	a0:23:9f:86:52:cf	SIP/SDP	Request: INVITE sip:181@172.16.56.109;user=phone
16:11:41.864384	172.16.56.109	172.16.78.64	a0:23:9f:86:52:cf	00:27:90:2a:ab:24	SIP	Status: 100 Trying
16:11:42.529759	172.16.56.109	172.16.78.64	a0:23:9f:86:52:cf	00:27:90:2a:ab:24	SIP	Status: 180 Ringing
16:11:47.581067	172.16.56.109	172.16.78.64	a0:23:9f:86:52:cf	00:27:90:2a:ab:24	SIP/SDP	Status: 200 OK
16:11:47.594494	172.16.78.64	172.16.56.109	00:27:90:2a:ab:24	a0:23:9f:86:52:cf	SIP	Request: ACK sip:181@172.16.56.109:5060;transport=tcp

RTP-Pakete:

16:11:47.700968	172.16.78.65	172.16.78.64	00:eb:d5:db:00:d6	a0:23:9f:86:52:cf	RTP
16:11:47.701470	172.16.78.65	172.16.78.64	a0:23:9f:86:52:cf	00:27:90:2a:ab:24	RTP
16:11:47.717783	172.16.78.65	172.16.78.64	00:eb:d5:db:00:d6	a0:23:9f:86:52:cf	RTP
16:11:47.718528	172.16.78.65	172.16.78.64	a0:23:9f:86:52:cf	00:27:90:2a:ab:24	RTP
16:11:47.730826	172.16.78.65	172.16.78.64	00:eb:d5:db:00:d6	a0:23:9f:86:52:cf	RTP
16:11:47.731395	172.16.78.65	172.16.78.64	a0:23:9f:86:52:cf	00:27:90:2a:ab:24	RTP
16:11:47.751602	172.16.78.65	172.16.78.64	00:eb:d5:db:00:d6	a0:23:9f:86:52:cf	RTP
16:11:47.752316	172.16.78.65	172.16.78.64	a0:23:9f:86:52:cf	00:27:90:2a:ab:24	RTP
16:11:47.766859	172.16.78.64	172.16.78.65	00:27:90:2a:ab:24	a0:23:9f:86:52:cf	RTP
16:11:47.776488	172.16.78.65	172.16.78.64	00:eb:d5:db:00:d6	a0:23:9f:86:52:cf	RTP

Anschließend informiert der 8821 den Anrufmanager, dass der Anruf beendet wird, und benachrichtigt den WLC, der nicht mehr die Warteschlange 6 verwendet, durch Senden eines weiteren Action Frame:

```

2019/08/25 18:54:08.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24
Got action frame from this client.
2019/08/25 18:54:08.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24
Received Action frame with code 2: DELTS request
2019/08/25 18:54:08.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24
DEL TS from mobile slot_id lup = 6, tid = 6, bw deleted = 653
2019/08/25 18:54:08.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24
Call Terminated for tspec client
2019/08/25 18:54:08.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24
Calls in progress - 1, Roam calls in progress - 0
2019/08/25 18:54:08.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24
Build DELETE TS slot:1 tid:6 up:6 upsd_enable:1 avail_bw: 0
2019/08/25 18:54:08.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: a023.9f86.52c0
send qos DELETE TS payload to AP

```

## SIP-Terminierung und Aktionsrahmen:

No.	Time	Source	Destination	Transmitter address	Receiver address	Protocol	Info
7260	16:11:54.400738	172.16.78.64	172.16.56.109	00:27:90:2a:ab:24	a0:23:9f:86:52:cf	SIP	Request: NOTIFY sip:100@172.16.56.109
7266	16:11:54.407572	172.16.56.109	172.16.78.64	a0:23:9f:86:52:cf	00:27:90:2a:ab:24	SIP	Status: 200 OK
7268	16:11:54.409575	172.16.78.64	172.16.56.109	00:27:90:2a:ab:24	a0:23:9f:86:52:cf	SIP	Request: BYE sip:181@172.16.56.109:5060;transport=tcp
7283	16:11:54.428215	172.16.56.109	172.16.78.64	a0:23:9f:86:52:cf	00:27:90:2a:ab:24	SIP	Status: 200 OK
7285	16:11:54.431823	172.16.78.64	172.16.56.109	00:27:90:2a:ab:24	a0:23:9f:86:52:cf	TCP	51254 → 5060 [ACK] Seq=14915 Ack=7435 Win=39736 Len=0 TSval=443233
7340	16:11:54.503030	Cisco_2a:ab:24	Cisco_86:52:cf	00:27:90:2a:ab:24	a0:23:9f:86:52:cf	802.11	Action, SN=3087, FN=0, Flags=...P....C

```

IEEE 802.11 Action, Flags: ...P....C
IEEE 802.11 wireless LAN
  Fixed parameters
    Category code: Management Notification (17)
    Action code: Teardown (0x0002)
    Dialog token: 0x00
    Status code: Admission accepted (0x0000)
  Tagged parameters (63 bytes)
    Tag: Vendor Specific: Microsoft Corp.: WMM/WME: TSPEC Element

```