

Configurazione di una WLAN per voce con Cisco 8821 su Catalyst 9800 WLC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurare un SSID](#)

[Opzione A. Switching centrale](#)

[Esempio di rete di switching centrale](#)

[Switching centrale: Tag e profili](#)

[Switching centrale: CLI \(Command Line Interface\)](#)

[Opzione B. Switching locale FlexConnect](#)

[Esempio di rete dello switching locale Flexconnect](#)

[Tag e profili di switching locale Flexconnect](#)

[Interfaccia CLI \(Command Line Interface\) di switching locale Flexconnect](#)

[Configura parametri multimediali](#)

[Configurazione GUI](#)

[CLI \(Command Line Interface\)](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare un controller WLC (Wireless LAN Controller) 9800 per un'implementazione vocale utilizzando i telefoni cellulari Cisco 8821 su switching centrale e switching locale FlexConnect.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Catalyst Wireless 9800 modello di configurazione
- FlexConnect
- 802.11r
- Controllo di ammissione di chiamata (CAC)

Componenti usati

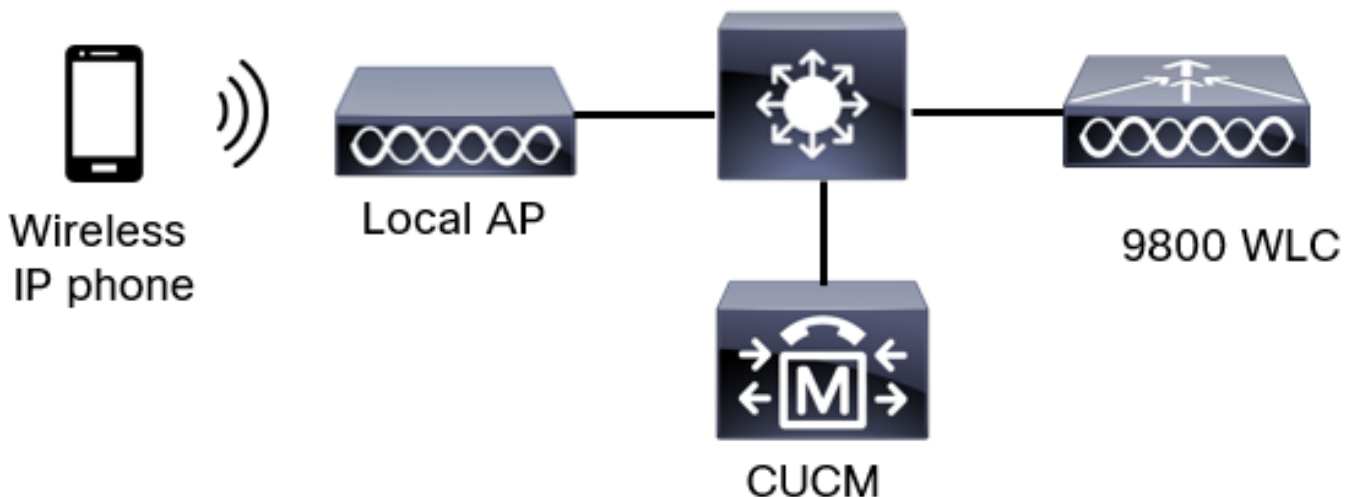
Il riferimento delle informazioni contenute in questo documento è 9800L v17.6.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurare un SSID

Opzione A. Switching centrale

Esempio di rete di switching centrale



Switching centrale: Tag e profili

In questo documento, la configurazione di tutti i tag e i profili viene effettuata con l'uso di **Advanced Wireless Setup**, in quanto tutti i tag e i profili possono essere configurati sullo stesso menu.

Passaggio 1. Selezionare **Configuration > Wireless Setup > Advanced > Start Now > WLAN Profile** (Configurazione > Configurazione wireless > Avanzate > Avvia ora > Profilo WLAN), quindi fare clic su **+Add** (Aggiungi) per creare una nuova WLAN. Configurare il SSID, il nome del profilo, l'ID della WLAN e lo stato della WLAN. Quindi, selezionare **Sicurezza > Layer 2** e configurare le impostazioni:

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 CCKMImpostazioni di sicurezza Voice SSID parte
2

- 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

Impostazioni di sicurezza Voice SSID parte 3 Impostazioni di protezione SSID voce parte 1

Nota: Con un SSID PSK non è necessario abilitare FT poiché l'handshake durante il roaming è breve. Quando si configura 802.1X WPA Enterprise, si consiglia di abilitare FT+802.1X come AKM e abilitare la transizione rapida, ma mantenere "Over the DS" come disabilitato. È anche possibile configurare FT+PSK, ma in questo esempio viene utilizzata la normale PSK per semplicità.

Passaggio 2. Passare alla scheda **Advanced** e abilitare Aironet IE. Assicurarsi che le funzioni Bilanciamento del carico e Selezione banda siano disabilitate:

Add WLAN ✕

General

Security

Advanced

Coverage Hole Detection <input checked="" type="checkbox"/>	Universal Admin <input type="checkbox"/>
Aironet IE <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 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"/>	Off Channel Scanning Defer

Cancel

Apply to Device

Nella stessa pagina, accertarsi che il rinvio della scansione del canale disattivato sia abilitato per

le priorità 5,6 e 7. Ciò impedisce all'access point di uscire dal canale per 100 ms dopo la ricezione di un frame con queste priorità UP (fondamentalmente un frame voce).

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

Passaggio 3. Selezionare **Policy Profile** e fare clic su **Add**:

The screenshot displays the 'Advanced' configuration page for wireless setup. On the left, a vertical navigation bar contains 'Start' at the top and 'Done' at the bottom. The main content area is divided into two sections: 'Tags & Profiles' and 'Apply'. Under 'Tags & Profiles', there are seven items: WLAN Profile, Policy Profile (highlighted with a blue box and a right-pointing arrow), Policy Tag, AP Join Profile, Flex Profile, Site Tag, RF Profile, and RF Tag. Each item has an information icon (i) on the left and a list icon (three horizontal lines) and a checkbox on the right. Under the 'Apply' section, there is one item: Tag APs, which also has an information icon and a list icon. On the right side, there is a '+ Add' button (highlighted with a blue box) and a 'Delete' button. Below these buttons is a list titled 'Policy Profile Name' with a dropdown arrow. The list contains one item: 'default-policy-profile'. At the bottom of the list, there are navigation controls: a left arrow, a page number '1', a right arrow, and a dropdown menu showing '10' items per page.

Configurare il nome del profilo dei criteri, impostare lo stato su Abilitato e mantenere abilitate le opzioni di switching centrale, autenticazione, DHCP e associazione (dopo la versione 17.6, la casella di controllo dell'associazione centrale scompare):

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

Fare clic su **Access Policies** (Criteri di accesso) e configurare la VLAN a cui verrà assegnato il client wireless quando ci si connette a SSID **Voice**:

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

Search or Select

VLAN

VLAN/VLAN Group

1

Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select

IPv6 ACL

Search or Select

URL Filters

Pre Auth

Search or Select

Post Auth

Search or Select

Cancel

Apply to Device

Pagina Impostazioni dei criteri di accesso al profilo dei criteri

Fare clic su **QoS e AVC** e configurare il parametro **Auto QoS** come **Voice**. Fare clic su **Salva e applica alla periferica**.

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

Fare clic su **Advanced** (Avanzate), impostare il timeout della sessione su 84000, verificare che IPv4 DHCP richiesto sia disabilitato e abilitare il proxy ARP.

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

Pagina Impostazioni avanzate profilo criteri

Passaggio 4. Selezionare **Tag criteri** e fare clic su **Aggiungi**. Configurare il nome del tag dei criteri.

In **Mappe WLAN-Policy** fare clic su **+Aggiungi**. Selezionare **Profilo WLAN** e **Profilo criterio** dai menu a discesa, quindi fare clic sul controllo della mappa da configurare. Quindi, fare clic su **Salva e applica al dispositivo**.

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
◀ 0 ▶ 10 items per page No items to display	

Map WLAN and Policy

WLAN Profile* Policy Profile*

➤ RLAN-POLICY Maps: 0

Passaggio 5. Selezionare **Site Tag** e fare clic su **Add**. Selezionare la casella **Attiva sito locale** per fare in modo che gli access point funzionino in **modalità locale**. Quindi, fare clic su **Save & Apply to Device (Salva e applica al dispositivo)**:

Add Site Tag ✕

Name*

Description

AP Join Profile

Control Plane Name

Enable Local Site

Passaggio 6. Selezionare **Profilo RF** e fare clic su **Aggiungi**. Configurare un profilo RF per banda.

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

Passare al menu **802.11**. Disabilitare tutte le velocità inferiori a 12 Mbps, impostare 12 Mbps come velocità obbligatoria e 18 Mbps e superiori come supportato su entrambe le bande.

Velocità di trasferimento dati a 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 & Apply to Device

Velocità di trasferimento dati a 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 & Apply to Device

Passaggio 7. Selezionare **RF Tag** e fare clic su **Add**. Selezionare i profili RF creati al punto 5 di questa sezione. Quindi, fare clic su **Salva e applica al dispositivo**.

Add RF Tag ✕

Name*

Description

5 GHz Band RF Profile ▼

2.4 GHz Band RF Profile ▼

Passaggio 8. Selezionare **Tag AP**, scegliere gli AP e aggiungere il tag Policy, Site e RF precedentemente creato. Quindi, fare clic su **Salva e applica al dispositivo**.

Tag APs ✕

Tags

Policy ▼

Site ▼

RF ▼

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

Switching centrale: CLI (Command Line Interface)

Dalla CLI, eseguire questi comandi:

```

////////// 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

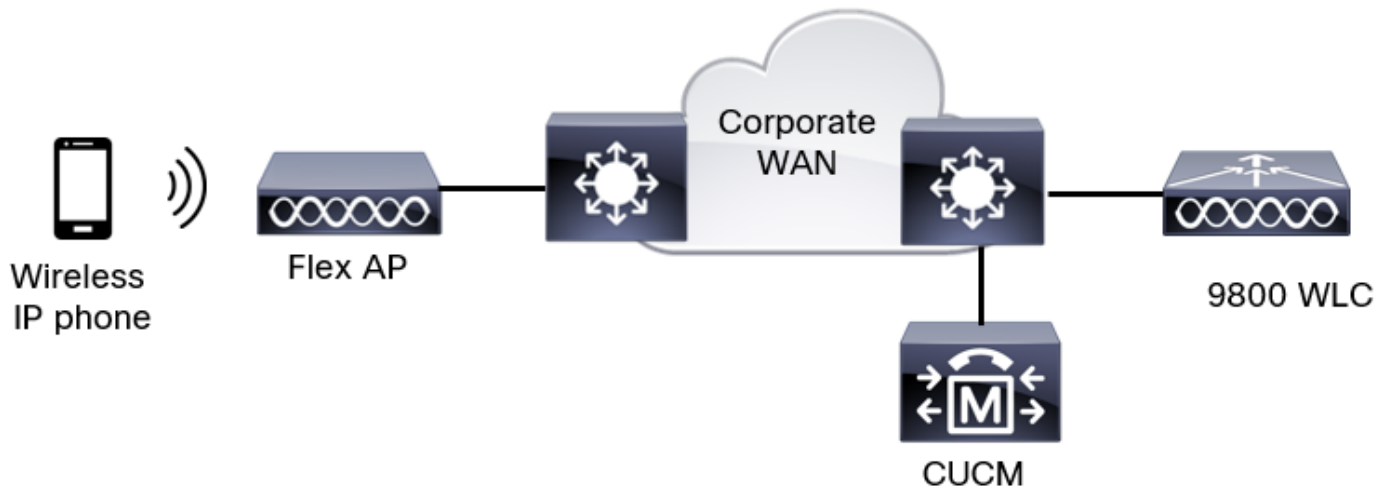
```
wireless tag rf RT1
24ghz-rf-policy Voice24GHz
5ghz-rf-policy Voice5GHz
```

//////// AP Configuration

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

Opzione B. Switching locale FlexConnect

Esempio di rete dello switching locale Flexconnect



Tag e profili di switching locale Flexconnect

Passaggio 1. Selezionare **Configuration > Wireless Setup > Advanced > Start Now > WLAN Profile** (Configurazione > Configurazione wireless > Avanzate > Avvia ora > Profilo WLAN), quindi fare clic su **+Add** (Aggiungi) per creare una nuova WLAN. Configurare il SSID, il nome del profilo, l'ID della WLAN e lo stato della WLAN. Quindi, selezionare **Sicurezza > Layer 2** e configurare le impostazioni:

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

Impostazioni di sicurezza Voice SSID parte 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	<div style="border: 1px solid blue; padding: 5px;"> <table> <tr> <td>PSK Format</td> <td>ASCII</td> </tr> <tr> <td>PSK Type</td> <td>Unencrypted</td> </tr> <tr> <td>Pre-Shared Key*</td> <td>.....</td> </tr> </table> </div>	PSK Format	ASCII	PSK Type	Unencrypted	Pre-Shared Key*
PSK Format	ASCII						
PSK Type	Unencrypted						
Pre-Shared Key*						

Cancel

Apply to Device

Impostazioni di sicurezza Voice SSID parte 3 Impostazioni di protezione SSID voce parte 1

Nota: Con un SSID PSK non è necessario abilitare FT poiché l'handshake durante il roaming è breve. Quando si configura 802.1X WPA Enterprise, si consiglia di abilitare FT+802.1X come AKM e abilitare la transizione rapida, ma mantenere "Over the DS" come disabilitato. È anche possibile configurare FT+PSK, ma in questo esempio viene utilizzata la normale PSK per semplicità.

Passaggio 2. Passare alla scheda **Advanced** e abilitare Aironet IE. Assicurarsi che le funzioni Bilanciamento del carico e Selezione banda siano disabilitate:

Add WLAN

General Security **Advanced**

Coverage Hole Detection	<input checked="" type="checkbox"/>	Universal Admin	<input type="checkbox"/>
Aironet IE	<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	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"/>	Off Channel Scanning Defer	

Cancel Apply to Device

Nella stessa pagina, accertarsi che il rinvio della scansione del canale disattivato sia abilitato per le priorità 5,6 e 7. Ciò impedisce all'access point di uscire dal canale per 100 ms dopo la ricezione di un frame con queste priorità UP (fondamentalmente un frame voce).

Add WLAN

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

Cancel Apply to Device

Passaggio 3. Selezionare **Policy Profile** e fare clic su **Add**:

The screenshot displays the 'Tags & Profiles' configuration page. On the left, a vertical navigation bar contains 'Start', 'Done', and several configuration items: WLAN Profile, Policy Profile (highlighted), Policy Tag, AP Join Profile, Flex Profile, Site Tag, RF Profile, RF Tag, and Tag APs. On the right, a panel titled 'Policy Profile Name' shows a list with one entry: 'default-policy-profile'. Above this list are '+ Add' and 'Delete' buttons, with '+ Add' highlighted. Below the list are navigation controls including a page number '1' and '10 items per page'.

Configurare il nome del profilo dei criteri, impostare lo stato su Abilitato, disabilitare la commutazione centrale e DHCP centrale. Per un SSID PSK, l'autenticazione potrebbe essere spostata in locale per assegnare al punto di accesso il ruolo di verifica della PSK. Nel caso di 802.1X, in genere si desidera che il WLC continui ad eseguire le autenticazioni 802.1X.

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

<p>Name* <input style="width: 100%;" type="text" value="PP2"/></p> <p>Description <input style="width: 100%;" type="text" value="Enter Description"/></p> <p>Status ENABLED <input checked="" type="checkbox"/></p> <p>Passive Client <input type="checkbox"/> DISABLED</p> <p>Encrypted Traffic Analytics <input type="checkbox"/> DISABLED</p>	<div style="background-color: #e8f5e9; padding: 5px; margin-bottom: 10px;">WLAN Switching Policy</div> <p>Central Switching <input type="checkbox"/> DISABLED</p> <p>Central Authentication ENABLED <input checked="" type="checkbox"/></p> <p>Central DHCP <input type="checkbox"/> DISABLED</p> <p>Flex NAT/PAT <input type="checkbox"/> DISABLED</p>
--	---

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

↶ Cancel

📄 Apply to Device

Configurazione profilo criteri di commutazione locale Flex

Passare alla scheda **Criteri di accesso** per assegnare la VLAN a cui sono assegnati i client wireless quando si connettono a questa WLAN per impostazione predefinita. È possibile selezionare un nome di VLAN dall'elenco a discesa o digitare manualmente un ID VLAN.

Fare clic su **QoS e AVC** e configurare il parametro **Auto QoS** come **Voice**. Fare clic su **Salva e applica alla periferica**.

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

Fare clic su **Advanced** (Avanzate), impostare il timeout della sessione su 84000, verificare che IPv4 DHCP richiesto sia disabilitato e disabilitare il proxy ARP.

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 [Cancel](#)[Update & Apply to Device](#)

Impostazioni avanzate del profilo criteri flessibilità

Passaggio 4. Selezionare **Tag criteri** e fare clic su **Aggiungi**. Configurare il nome del tag dei criteri. In **Mappe WLAN-Policy** fare clic su **+Aggiungi**. Selezionare il **Profilo WLAN** e il **Profilo criteri** dai menu a discesa, quindi fare clic sul controllo della mappa da configurare. Quindi, fare clic su **Salva e applica al dispositivo**.

Add Policy Tag

Name*

Description

WLAN-POLICY Maps: 0

WLAN Profile Policy Profile

◀ 0 ▶ 10 items per page No items to display

Map WLAN and Policy

WLAN Profile* Policy Profile*

RLAN-POLICY Maps: 0

Passaggio 5. Fare clic su **Flex Profile** e fare clic su **Add**. Configurare il nome del profilo Flex, l'ID VLAN nativo e abilitare la cache ARP:

Edit Flex Profile

General Local Authentication Policy ACL VLAN DNS Layer Security

Name*

Description

Native VLAN ID

HTTP Proxy Port

HTTP-Proxy IP Address

CTS Policy

Inline Tagging

SGACL Enforcement

CTS Profile Name

Fallback Radio Shut

Flex Resilient

ARP Caching

Efficient Image Upgrade

OfficeExtend AP

Join Minimum Latency

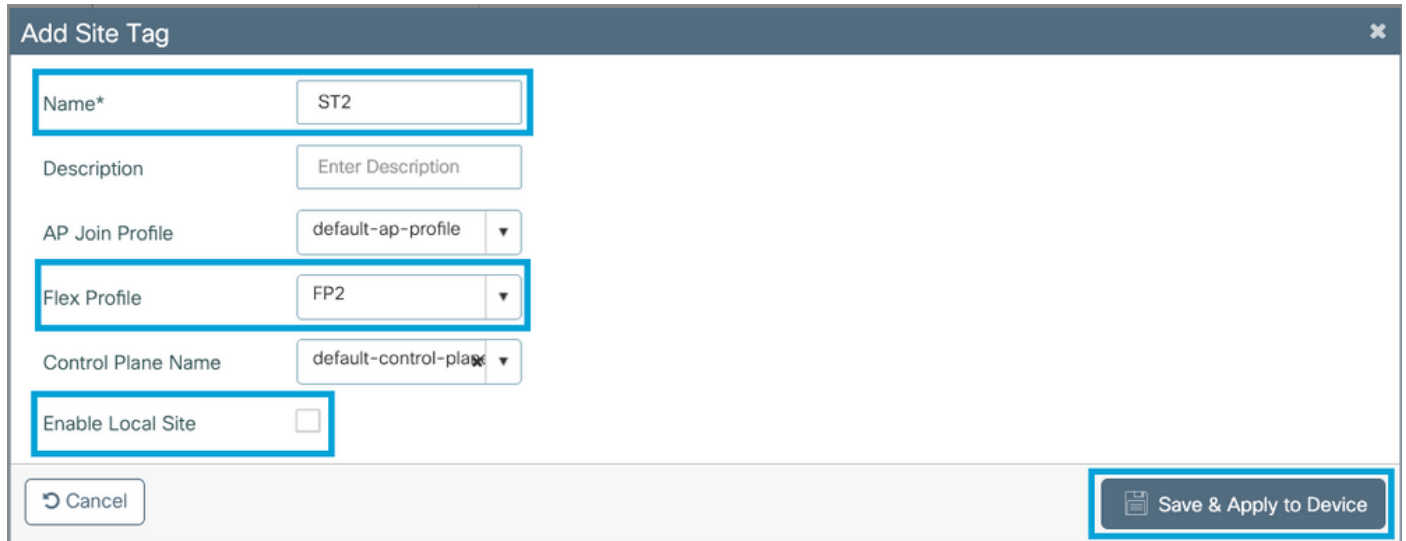
IP Overlap

mDNS Flex Profile

Impostazioni criteri profilo flessibile

Nota: L'ID della VLAN nativa si riferisce alla VLAN nativa configurata nella porta dello switch a cui sono connessi gli AP associati a questo profilo Flex.

Passaggio 6. Selezionare **Site Tag** e fare clic su **Aggiungi**. Configurare il nome del tag del sito, deselegionare l'opzione **Abilita sito locale** e aggiungere il profilo Flex. Quindi, fare clic su **Save & Apply to Device (Salva e applica al dispositivo)**.



Add Site Tag

Name*

Description

AP Join Profile

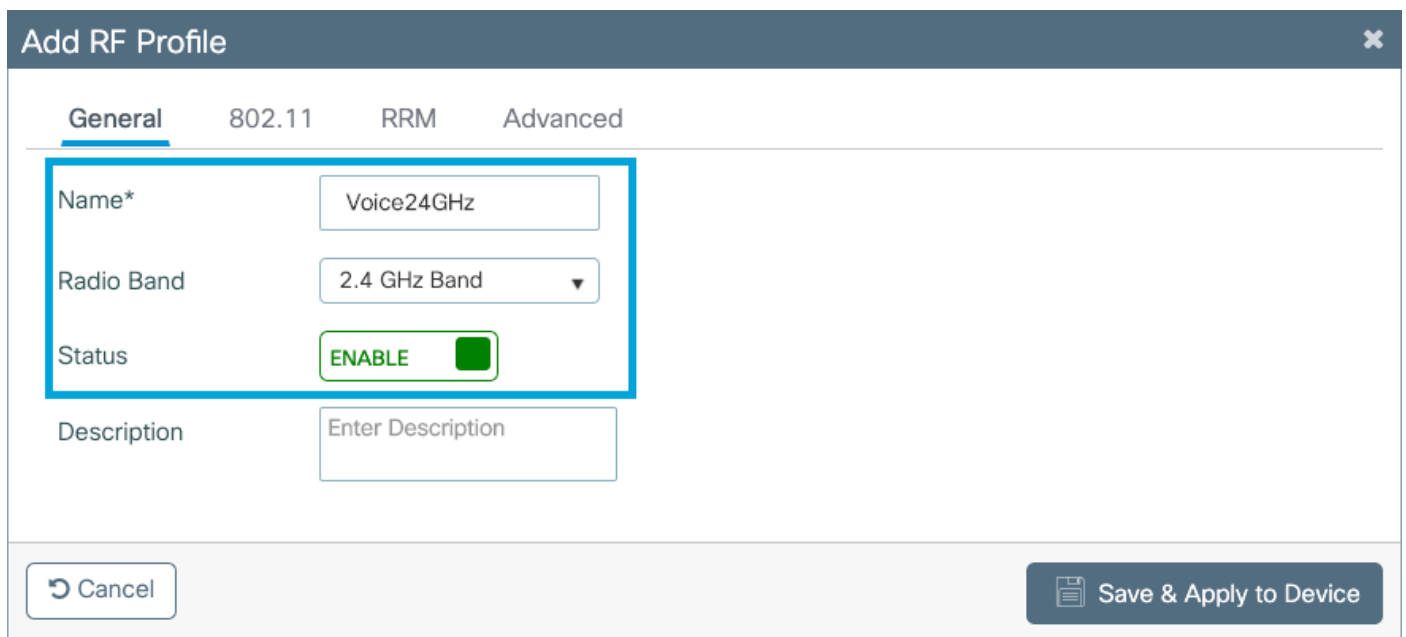
Flex Profile

Control Plane Name

Enable Local Site

Nota: Quando l'opzione Abilita sito locale è disabilitata, i punti di accesso assegnati a questo tag del sito verranno configurati automaticamente come punti di accesso FlexConnect.

Passaggio 7. Selezionare **Profilo RF** e fare clic su **Aggiungi**. Configurare un profilo RF per banda.



Add RF Profile

General 802.11 RRM Advanced

Name*

Radio Band

Status ENABLE

Description

Add RF Profile



General

802.11

RRM

Advanced

Name*	<input type="text" value="Voice5GHz"/>
Radio Band	<input type="text" value="5 GHz Band"/>
Status	<input checked="" type="checkbox"/> ENABLE
Description	<input type="text" value="Enter Description"/>

Cancel

Save & Apply to Device

Passare al menu **802.11**. Disabilitare tutte le velocità inferiori a 12 Mbps, impostare 12 Mbps come velocità obbligatoria e 18 Mbps e superiori come supportato su entrambe le bande.

Velocità di trasferimento dati a 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 & Apply to Device

Velocità di trasferimento dati a 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 & Apply to Device

Passaggio 8. Selezionare **RF Tag** e fare clic su **Add**. Configurare i profili RF creati nel passaggio 6. di questa sezione. Quindi, fare clic su **Salva e applica al dispositivo**.

Add RF Tag ✕

Name*

Description

5 GHz Band RF Profile

2.4 GHz Band RF Profile

Passaggio 9. Selezionare **Tag AP**, scegliere gli AP e aggiungere il tag Policy, Site e RF precedentemente creato. Quindi, fare clic su **Salva e applica al dispositivo**.

Tag APs ✕

Tags

Policy

Site

RF

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

L'access point riavvierà il proprio tunnel CAPWAP e si unirà al WLC 9800. Selezionare **Configurazione > Wireless > Access Point** e confermare che la modalità AP sia **Flex**:

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

Interfaccia CLI (Command Line Interface) di switching locale Flexconnect

Dalla CLI, eseguire questi comandi:

///////// 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 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
```

Configura parametri multimediali

Configurazione GUI

Passaggio 1. Passare a **Configurazione > Configurazione radio > Rete**. Disabilitare la banda a 5 GHz e a 2,4 GHz e fare clic su **Applica**.

Presta attenzione al fatto che questa operazione disabiliterà temporaneamente tutte le reti wifi da 5 ghz! Eseguire questa operazione solo quando si è in una finestra di manutenzione

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

Passaggio 2. Passare a **Configurazione > Configurazione radio > Parametri dei supporti**. **Abilitare il controllo dell'ammissione e il controllo dell'ammissione di chiamata basato sul carico (CAC) su entrambe le bande 2.4 GHz e 5 GHz**, quindi fare clic su **Applica**:

Voice

Call Admission Control (CAC)

Admission Control (ACM)	<input checked="" type="checkbox"/>
Load Based CAC	<input checked="" type="checkbox"/>

Max RF Bandwidth (%)*

Reserved Roaming Bandwidth (%)*

Expedited Bandwidth

SIP CAC and Bandwidth

SIP CAC Support

Passaggio 3. Passare a **Configurazione > Configurazioni radio > Parametri**. Configurare il profilo EDCA come **optimized-voice** su entrambe le bande, quindi fare clic su **Applica**.

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

5 GHz Band

2.4 GHz Band

EDCA Parameters

EDCA Profile

optimized-voice

DFS (802.11h)

Passaggio 4. Passare a **Configurazione > Configurazione radio > Rete**. Abilitare la banda a 5 GHz e a 2,4 GHz e fare clic su **Apply (Applica)**.

CLI (Command Line Interface)

Dalla CLI, eseguire i seguenti comandi:

```
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 5ghz cac voice acm

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
```

Verifica

Usare questi comandi per verificare la configurazione corrente:

```
# 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>
```

Per esaminare le statistiche CAC e le metriche di controllo delle chiamate, eseguire i seguenti comandi:

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

Risoluzione dei problemi

Debug condizionale e traccia Radioactive (RA)

La traccia Radio attiva (RA) fornisce le tracce dei livelli di debug per tutti i processi che interagiscono con la condizione specificata (in questo caso l'indirizzo MAC del client). Per abilitare il debug condizionale, attenersi alla seguente procedura. Ci concentriamo sull'output che il 9800 WLC fornisce durante una chiamata.

Passaggio 1. Accertarsi che non siano state abilitate condizioni di debug.

```
# clear platform condition all
```

Passaggio 2. Abilitare la condizione di debug per l'indirizzo MAC del client wireless che si desidera monitorare. Questo comando avvia il monitoraggio dell'indirizzo MAC fornito per 30 minuti (1800 secondi). È possibile aumentare questo tempo fino a 2085978494 secondi.


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

Nota: per monitorare più client alla volta, eseguire il comando `debug wireless mac <aaa.bbbb.ccc>` per indirizzo MAC.

Nota: l'output dell'attività del client nella sessione terminale non viene visualizzato, in quanto tutto viene memorizzato internamente nel buffer per essere visualizzato successivamente.

Passaggio 3. Effettuare una chiamata dal telefono IP Cisco 8821.

Passaggio 4. Interrompere i debug quando la chiamata viene completata o se il problema viene riprodotto prima che sia attivo il tempo di monitoraggio predefinito o configurato.

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

Una volta trascorso il tempo di monitoraggio o interrotto il debug wireless, il controller 9800 WLC genera un file locale con il nome:

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Passaggio 5. Raccogliere il file dell'attività dell'indirizzo MAC. È possibile copiare il file di log di traccia RAR in un server esterno o visualizzare l'output direttamente sullo schermo. Controllare il nome del file delle tracce RA

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

Copiare il file su un server esterno:

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

Visualizzare il contenuto:

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Passaggio 6. Rimuovere le condizioni di debug.

```
# clear platform condition all
```

Nota: accertarsi di rimuovere sempre le condizioni di debug dopo una sessione di risoluzione dei problemi.

Nell'output della traccia RA, viene eseguita la negoziazione TSPEC (Traffic Specification), che determina se è consentito contrassegnare il traffico dello switch 8821 con una priorità utente di 6 e se è possibile stabilire la chiamata. Per negoziare l'utilizzo della coda 6, lo switch 8821 invia e richiede l'autorizzazione tramite Action Packet.

```

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

```

In un'acquisizione pacchetto:

```

▶ 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

```

Il WLC determina se la larghezza di banda è sufficiente per allocare o meno la chiamata e, in tal caso, invia un frame di azione che accetta la negoziazione TSPEC:

```

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

```

In un'acquisizione pacchetto:

```

▶ 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

```

Quindi, la chiamata viene stabilita tramite SIP con il gestore delle chiamate e il traffico RTP viene inoltrato.

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

Pacchetti RTP:

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

Quindi, lo switch 8821 informa il gestore delle chiamate che la chiamata è terminata e avvisa il

WLC che non sta più utilizzando la coda 6 inviando un altro 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
```

Terminazione SIP e frame azione:

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