

在Catalyst 9800 WLC上使用Cisco 8821配置语音WLAN

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置SSID](#)

[方案 A：中央交换](#)

[中央交换网络图](#)

[集中交换：标记和配置文件](#)

[集中交换：命令行界面 \(CLI\)](#)

[方案 B：FlexConnect本地交换](#)

[FlexConnect本地交换网络图](#)

[FlexConnect本地交换标签和配置文件](#)

[FlexConnect本地交换命令行界面\(CLI\)](#)

[配置介质参数](#)

[GUI 配置](#)

[命令行界面 \(CLI\)](#)

[验证](#)

[故障排除](#)

简介

本文档介绍如何在中央交换和FlexConnect本地交换上使用Cisco 8821听筒配置9800无线LAN控制器(WLC)以进行语音部署。

先决条件

要求

Cisco 建议您了解以下主题：

- Catalyst无线9800配置型号
- FlexConnect
- 802.11r
- 呼叫准入控制 (CAC)

使用的组件

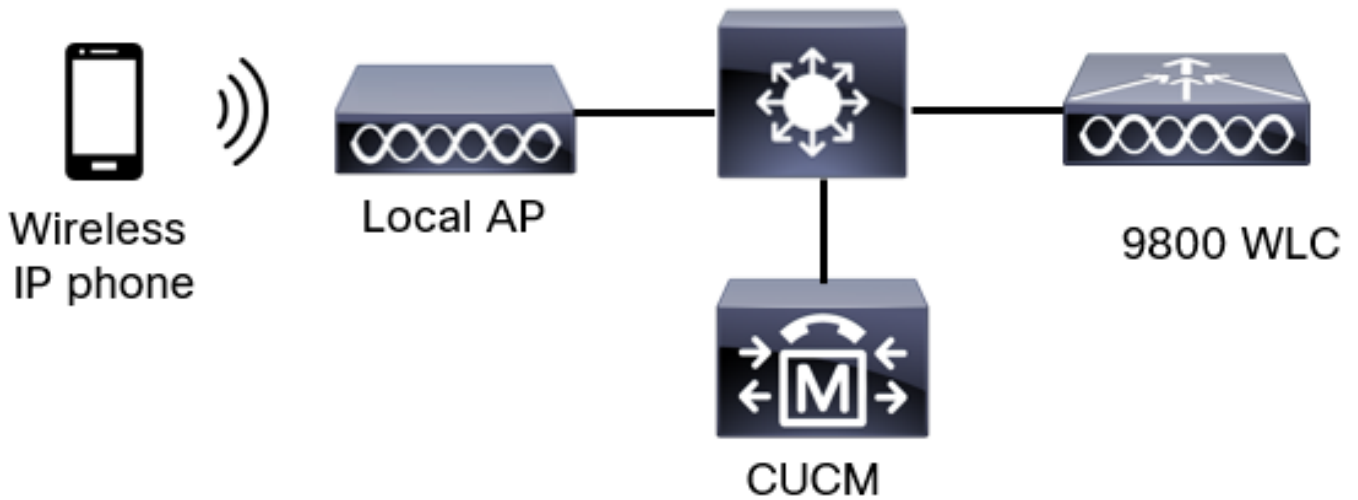
本文档中的信息基于9800L v17.6.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置SSID

方案 A：中央交换

中央交换网络图



集中交换：标记和配置文件

在本文档中，所有标记和配置文件的配置都使用高级无线设置完成，因为所有标记和配置文件都可以在同一菜单上配置。

步骤1. 导航至 **Configuration > Wireless Setup > Advanced > Start Now > WLAN Profile**，然后单击 +Add 以创建新的 WLAN。配置 SSID、配置文件名称、WLAN ID 和 WLAN 的状态。然后，导航至 **Security > Layer 2** 并配置设置：

The screenshot shows the 'Add WLAN' configuration page in a web interface. The 'Security' tab is selected, and the 'Layer 2' sub-tab is active. The 'Layer 2 Security Mode' is set to 'WPA + WPA2'. The 'MAC Filtering' checkbox is unchecked. The 'Protected Management Frame' section is collapsed. The 'PMF' dropdown is set to 'Disabled'. The 'WPA Parameters' section is collapsed. On the right side, 'Lobby Admin Access' is unchecked. The 'Fast Transition' dropdown is set to 'Disabled'. The 'Over the DS' checkbox is unchecked. The 'Reassociation Timeout' is set to '20'. The 'MPSK Configuration' section is collapsed, and 'MPSK' is unchecked.

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

语音SSID安全设置第2部分

	<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*

语音SSID安全设置第3部分 语音SSID安全设置第1部分

注意：使用PSK SSID时，无需启用FT，因为漫游期间的握手很短。配置802.1X WPA企业时，建议启用FT+802.1X作为AKM并启用快速过渡，但将“Over the DS”保持为禁用状态。您也可以配置FT+PSK，但为简单起见，本示例使用常规PSK。

步骤2.导航至“高级”选项卡并启用Aironet IE。确保已禁用负载平衡和频段选择：

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	

在同一页中，确保为优先级5、6和7启用了信道外扫描延迟。这可以防止AP在收到具有这些UP优先级的帧（基本上是语音帧）后100毫秒内信道外扫描。

Add WLAN ✕

WiFi to Cellular Steering	<input type="checkbox"/>	Off Channel Scanning Defer 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"/>		
Max Client Connections			
Per WLAN	<input type="text" value="0"/>	Assisted Roaming (11k)	
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"/>
11v BSS Transition Support			

步骤3.选择Policy Profile，然后单击Add:

The screenshot displays a configuration interface for wireless settings. On the left, a vertical timeline starts with a 'Start' button and ends with a 'Done' button. The main area is titled 'Tags & Profiles' and contains a list of items, each with an information icon, a name, a list icon, and a checkbox:

- WLAN Profile
- Policy Profile** (highlighted with a blue box)
- Policy Tag
- AP Join Profile
- Flex Profile
- Site Tag
- RF Profile
- RF Tag

Below this list is an 'Apply' section with a 'Tag APs' item. On the right side, there is a panel with a '+ Add' button (highlighted with a blue box) and a 'Delete' button. Below these buttons is a dropdown menu for 'Policy Profile Name' showing a list of items, with 'default-policy-profile' selected. Navigation controls (back, forward, page number '1', and items per page '10') are also visible.

配置策略配置文件名称，将状态设置为启用，并保持中心交换、身份验证、DHCP和关联（在17.6之后，中心关联复选框消失）已启用：

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*

PP1

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Flex NAT/PAT

DISABLED

Cancel

Apply to Device

单击**Access Policies**并配置无线客户端在连接到SSID Voice : 时将分配到的VLAN。

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

策略配置文件访问策略设置页面

单击QoS和AVC，并将Auto QoS参数配置为Voice。单击Save & Apply to Device。

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

单击“Advanced (高级)”，将会话超时设置为84000，确保禁用所需的IPv4 DHCP并启用ARP代理

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 ENABLED

Flex 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

策略配置文件高级设置页面

步骤4.选择Policy Tag并单击Add。配置策略标记名称。在“WLAN-Policy Maps”下，单击“+Add”。从下拉菜单中选择WLAN配置文件和策略配置文件，然后单击要配置的映射的检查。然后，单击保存

并应用到设备。

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

步骤5.选择“站点标记”并单击“添加”。选中启用本地站点框，使AP在本地模式下运行。然后，单击 Save & Apply to Device:

Add Site Tag ✕

Name*

Description

AP Join Profile

Control Plane Name

Enable Local Site

步骤6.选择RF配置文件并单击添加。按频段配置RF配置文件。

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

导航至**802.11**菜单。禁用所有低于12Mbps的速率，将12Mbps设置为强制速率，并根据两个频段的支持设置18 Mbps或更高速率。

2.4 GHz数据速率：

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

5 GHz数据速率：

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 & Apply to Device

步骤7.选择RF Tag(RF标签), 然后单击Add。选择在本节第5步中创建的RF配置文件。然后, 单击保存并应用到设备。

Add RF Tag ✕

Name*	<input type="text" value="RT1"/>
Description	<input type="text" value="Enter Description"/>
5 GHz Band RF Profile	<input type="text" value="Voice5GHz"/> ▼
2.4 GHz Band RF Profile	<input type="text" value="Voice24GHz"/> ▼

步骤8.选择Tag APs，选择AP并添加之前创建的策略、站点和RF标记。然后，单击保存并应用到设备。

Tag APs ✕

Tags

Policy	<input type="text" value="PT1"/> ▼
Site	<input type="text" value="ST1"/> ▼
RF	<input type="text" value="RT1"/> ▼

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

集中交换：命令行界面 (CLI)

从CLI运行以下命令：

```

////////// 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

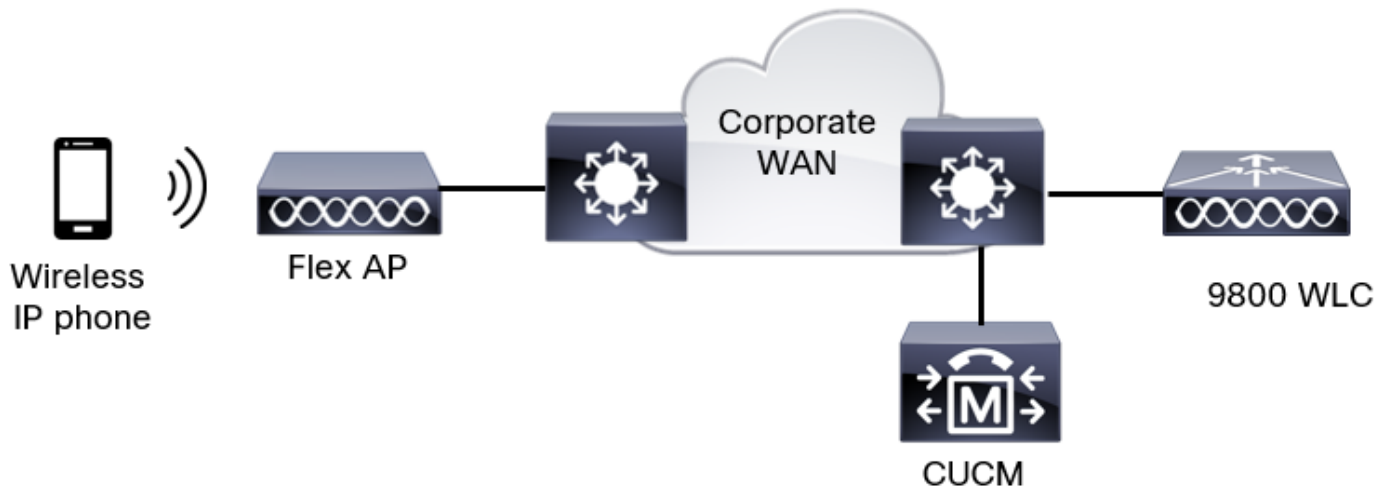
```
wireless tag rf RT1
24ghz-rf-policy Voice24GHz
5ghz-rf-policy Voice5GHz
```

//////// AP Configuration

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

方案 B : FlexConnect本地交换

FlexConnect本地交换网络图



FlexConnect本地交换标签和配置文件

步骤1. 导航至 **Configuration > Wireless Setup > Advanced > Start Now > WLAN Profile**，然后单击 **+Add** 以创建新的WLAN。配置SSID、配置文件名称、WLAN ID和WLAN的状态。然后，导航至 **Security > Layer 2** 并配置设置：

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

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

语音SSID安全设置第2部分

	<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*

语音SSID安全设置第3部分 语音SSID安全设置第1部分

注意：使用PSK SSID时，无需启用FT，因为漫游期间的握手很短。配置802.1X WPA企业时，建议启用FT+802.1X作为AKM并启用快速过渡，但将“Over the DS”保持为禁用状态。您也可以配置FT+PSK，但为简单起见，本示例使用常规PSK。

步骤2. 导航至“高级”选项卡并启用Aironet IE。确保已禁用负载平衡和频段选择：

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	<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"/>	Off Channel Scanning Defer	

在同一页中，确保为优先级5、6和7启用了信道外扫描延迟。这可以防止AP在收到具有这些UP优先级的帧（基本上是语音帧）后100毫秒内信道外扫描。

Add WLAN ✕

WiFi to Cellular Steering	<input type="checkbox"/>	Off Channel Scanning Defer 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"/>		
Max Client Connections			
Per WLAN	<input type="text" value="0"/>	Assisted Roaming (11k)	
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"/>
11v BSS Transition Support			

步骤3.选择Policy Profile，然后单击Add:

The screenshot displays a configuration interface for wireless settings. On the left, a vertical flow starts with a 'Start' button, followed by a section titled 'Tags & Profiles'. This section contains several items, each with an information icon (i), a name, and a status icon (checkbox or lock):

- WLAN Profile
- Policy Profile** (highlighted with a blue box)
- Policy Tag
- AP Join Profile
- Flex Profile
- Site Tag
- RF Profile
- RF Tag

Below this is an 'Apply' section with a 'Tag APs' item. The flow ends with a 'Done' button. On the right, a panel shows a '+ Add' button (highlighted with a blue box) and a 'Delete' button. Below these is a dropdown menu for 'Policy Profile Name' showing 'default-policy-profile'. At the bottom of this panel, there are navigation arrows, a page number '1', and a '10 items per page' selector.

配置策略配置文件名称，将状态设置为启用，禁用中央交换和中央DHCP。对于PSK SSID，身份验证可移至本地，以便让接入点承担检验PSK的角色。对于802.1X，通常希望WLC继续执行802.1X身份验证。

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

Flex Local交换策略配置文件配置

导航至**Access Policies**选项卡，以分配无线客户端在默认情况下连接到此WLAN时分配到的VLAN。您可以从下拉列表中选择一个VLAN名称，或手动键入VLAN ID。

单击**QoS和AVC**，并将Auto QoS参数配置为Voice。单击**Save & Apply to Device**。

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

单击“Advanced (高级)”，将会话超时设置为84000，确保禁用所需的IPv4 DHCP并禁用ARP代理。

Edit Policy Profile

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

WLAN Timeout

Session Timeout (sec)	<input type="text" value="84000"/>
Idle Timeout (sec)	<input type="text" value="300"/>
Idle Threshold (bytes)	<input type="text" value="0"/>
Client Exclusion Timeout (sec)	<input checked="" type="checkbox"/> <input type="text" value="60"/>
Guest LAN Session Timeout	<input type="checkbox"/>

DHCP

IPv4 DHCP Required	<input type="checkbox"/>
DHCP Server IP Address	<input type="text"/>

Show more >>>

AAA Policy

Allow AAA Override	<input type="checkbox"/>
NAC State	<input type="checkbox"/>
Policy Name	default-aaa-policy ✕ ▼
Accounting List	Search or Select ▼ ⓘ

WGB Parameters

Broadcast Tagging	<input type="checkbox"/>
WGB VLAN	<input type="checkbox"/>

Policy Proxy Settings

ARP Proxy	<input type="checkbox"/> DISABLED
IPv6 Proxy	None ▼

Fabric Profile

Fabric Profile	<input type="checkbox"/> Search or Select ▼
Link-Local Bridging	<input type="checkbox"/>
mDNS Service Policy	default-mdns-ser... ▼ Clear
Hotspot Server	Search or Select ▼

User Defined (Private) Network

Status	<input type="checkbox"/>
Drop Unicast	<input type="checkbox"/>

DNS Layer Security

DNS Layer Security Parameter Map	Not Configured ▼ Clear
Flex DHCP Option for DNS	ENABLED <input checked="" type="checkbox"/>
Flex DNS Traffic Redirect	<input type="checkbox"/> IGNORE

WLAN Flex Policy

VLAN Central Switching	<input type="checkbox"/>
Split MAC ACL	Search or Select ▼

Air Time Fairness Policies

2.4 GHz Policy	Search or Select ▼
5 GHz Policy	Search or Select ▼

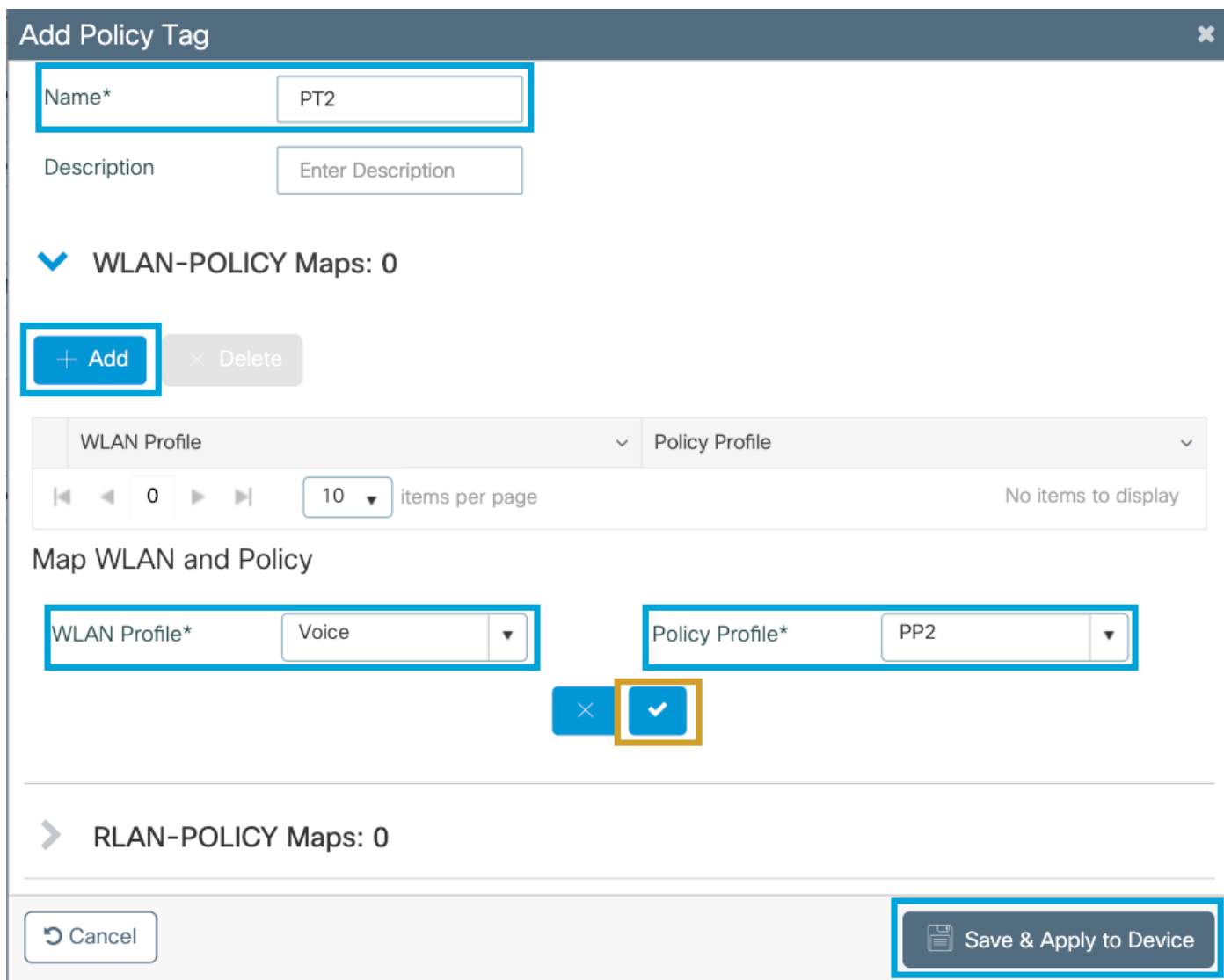
EoGRE Tunnel Profiles

Tunnel Profile	Search or Select ▼
----------------	--------------------

弹性策略配置文件的高级设置

步骤4.选择Policy Tag并单击Add。配置策略标记名称。在“WLAN-Policy Maps”下，单击“+Add”。从

下拉菜单中选择WLAN配置文件和策略配置文件，然后单击要配置的映射的检查。然后，单击保存并应用到设备。



Add Policy Tag

Name* PT2

Description Enter Description

WLAN-POLICY Maps: 0

+ Add Delete

WLAN Profile Policy Profile

0 10 items per page No items to display

Map WLAN and Policy

WLAN Profile* Voice Policy Profile* PP2

X ✓

RLAN-POLICY Maps: 0

Cancel Save & Apply to Device

步骤5.单击“Flex Profile”，然后单击“添加”。配置Flex Profile名称、本征VLAN ID和启用ARP缓存：

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"/>	
CTS Policy				
Inline Tagging	<input type="checkbox"/>	Join Minimum Latency	<input type="checkbox"/>	
SGACL Enforcement	<input type="checkbox"/>	IP Overlap	<input type="checkbox"/>	
CTS Profile Name	default-sxp-profile	mDNS Flex Profile	Search or Select	

Flex配置文件策略设置

注意：本征VLAN ID是指在交换机端口中配置的本征VLAN，与此Flex Profile关联的AP连接到该交换机端口。

步骤6.选择站点标记并单击添加。配置站点标记名称，取消选中启用本地站点选项并添加Flex配置文件。然后，单击保存并应用到设备。

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"/>

注意：禁用“启用本地站点”后，分配给此站点标记的AP将自动配置为FlexConnect AP。

步骤7.选择RF配置文件并单击添加。按频段配置RF配置文件。

Add RF Profile ✕

General 802.11 RRM Advanced

Name*	<input type="text" value="Voice24GHz"/>
Radio Band	<input type="text" value="2.4 GHz Band"/>
Status	<input checked="" type="checkbox"/> ENABLE
Description	<input type="text" value="Enter 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"/>

导航至**802.11**菜单。禁用所有低于12Mbps的速率，将12Mbps设置为强制速率，将两个频段支持的速率设置为18 Mbps及更高。

2.4 GHz数据速率：

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

5 GHz数据速率：

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 & Apply to Device

步骤8.选择RF Tag(RF标签)并单击Add (添加)。配置在本节第6步中创建的RF配置文件。然后,单击保存并应用到设备。

Add RF Tag ✕

Name*

Description

5 GHz Band RF Profile ▼

2.4 GHz Band RF Profile ▼

步骤9.选择Tag APs，选择AP并添加之前创建的策略、站点和RF标记。然后，单击保存并应用到设备。

Tag APs ✕

Tags

Policy ▼

Site ▼

RF ▼

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

AP将重新启动其CAPWAP隧道并重新加入9800 WLC。导航至Configuration > Wireless > Access Points，并确认AP模式为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

FlexConnect本地交换命令行界面(CLI)

从CLI运行以下命令：

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

配置介质参数

GUI 配置

步骤1.导航至**Configuration > Radio Configuration > Network**。禁用5 GHz和2.4 GHz频段，然后单击。

请注意，这将暂时禁用您的所有5ghz wifi网络！仅在您处于维护窗口时运行此命令

[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

步骤2.导航至**Configuration > Radio Configuration > Media Parameters**。在2.4 GHz和5 GHz频段上启用准入控制和基于负载的呼叫准入控制(CAC)，然后单击**应用**：

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

步骤3. 导航至 **Configuration > Radio Configurations > Parameters**。在两个频段上将EDCA配置文件配置为优化语音，然后单击“应用”。

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

5 GHz Band

2.4 GHz Band

EDCA Parameters

EDCA Profile

DFS (802.11h)

步骤4. 导航至 **Configuration > Radio Configuration > Network**。同时启用5 GHz和2.4 GHz频段，然后单击Apply。

命令行界面 (CLI)

从CLI运行以下命令：

```
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
```

验证

您可以使用以下命令验证当前配置：

```
# 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>
```

要查看CAC统计信息和呼叫控制度量，请运行以下命令：

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

故障排除

条件调试和无线电活动跟踪

Radio Active(RA)跟踪为与指定条件（本例中为客户端MAC地址）交互的所有进程提供调试级别跟踪。要启用条件调试，请执行以下步骤。我们重点介绍9800 WLC在呼叫期间提供的输出。

步骤1.确保未启用调试条件。

```
# clear platform condition all
```

步骤2.启用要监控的无线客户端MAC地址的调试条件。此命令开始监控提供的MAC地址30分钟（1800秒）。您可以选择将此时间增加到2085978494秒。

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

注意: 要一次监控多个客户端，请按mac地址运行debug wireless mac <aaaa.bbbb.cccc>命令。

注意:您看不到终端会话上客户端活动的输出，因为所有内容都在内部缓冲，以备以后查看。

步骤3.从8821 Cisco IP电话建立呼叫。

步骤4.当呼叫完成或问题在默认或配置的监控时间开启之前重现时停止调试。

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

监控时间过去或调试无线停止后，9800 WLC将生成名为：

```
ra_trace_MAC_aaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

步骤5.收集MAC地址活动的文件。您可以将ra trace .log复制到外部服务器或直接在屏幕上显示输出。检查RA跟踪文件的名称

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

将文件复制到外部服务器：

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

显示内容：

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

步骤6.删除调试条件。

```
# clear platform condition all
```

注意：确保在故障排除会话后始终删除调试条件。

在RA跟踪的输出中，会进行流量规范(TSPEC)协商，这将确定是否允许8821以用户优先级6标记其流量，以及是否可以建立呼叫。要协商队列6的使用，8821发送和操作数据包请求权限。

```
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
```

在数据包捕获中：

```
▶ 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
```

WLC确定是否有足够的带宽来分配呼叫，如果有，它会发送接受TSPEC协商的操作帧：

```
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
```

在数据包捕获中：


```

▶ 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

```

之后，通过SIP与呼叫管理器建立呼叫，并转发RTP流量。

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数据包：

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

然后，8821通知呼叫管理器呼叫已终止，并通过发送另一个操作帧通知不再使用队列6的WLC:

```

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终止和操作帧：

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 Status: 200 OK
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	Request: BYE sip:181@172.16.56.109:5060;transport=tcp 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 Status: 200 OK
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
  
```