

Configurer un WLAN pour la voix avec le 8821 sur le WLC Catalyst 9800

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer un SSID](#)

[Option a : Commutation centrale](#)

[Schéma du réseau de commutation central](#)

[Commutation centrale : balises et profils](#)

[Commutation centrale : interface de ligne de commande \(CLI\)](#)

[Option b : Commutation locale FlexConnect](#)

[Schéma du réseau de commutation locale Flexconnect](#)

[Balises et profils de commutation locale Flexconnect](#)

[Interface de ligne de commande \(CLI\) de commutation locale Flexconnect](#)

[Configuration des paramètres multimédias](#)

[Configuration de la GUI](#)

[Interface de ligne de commande \(CLI\)](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer un contrôleur LAN sans fil (WLC) 9800 pour un déploiement vocal à l'aide de combinés Cisco 8821.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Modèle de configuration Catalyst Wireless 9800
- FlexConnect
- 802.11r
- Contrôle d'admission des appels (CAC)

Composants utilisés

Les informations contenues dans ce document sont basées sur une version 9800L v17.6.1

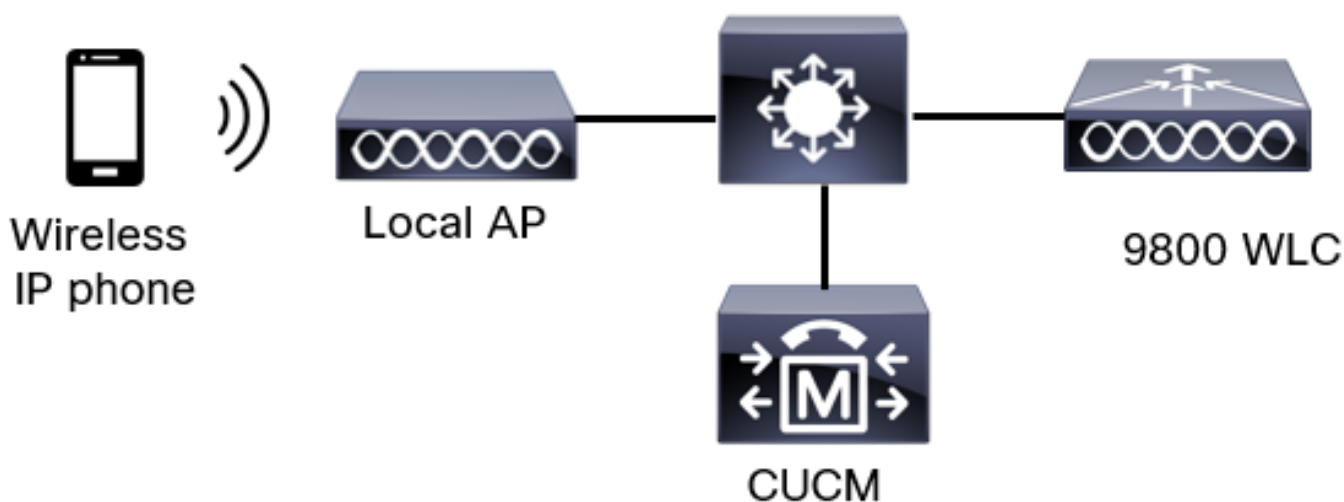
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Le document ne couvre pas SIP CAC car il n'est pas pris en charge sur le 9800 après la version 17.3.1

Configurer un SSID

Option a : Commutation centrale

Schéma du réseau de commutation central



Commutation centrale : balises et profils

Dans ce document, la configuration de toutes les balises et de tous les profils est effectuée avec l'utilisation de la Configuration sans fil avancée car toutes les balises et tous les profils peuvent être configurés sur le même menu.

Étape 1. Accédez à Configuration > Wireless Setup > Advanced > Start Now > WLAN Profile et cliquez sur +Add afin de créer un nouveau WLAN. Configurez le SSID, le nom de profil, l'ID WLAN et l'état du WLAN. Accédez ensuite à Security > Layer 2 et configurez les paramètres. Cet exemple utilise une clé prépartagée simple et ne nécessite donc pas la configuration de FT. Si vous configurez 802.1X, activez FT.

Add WLAN



General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode

MAC Filtering

Protected Management Frame

PMF

WPA Parameters

Lobby Admin Access

Fast Transition

Over the DS

Reassociation Timeout

MPSK Configuration

MPSK

Paramètres de sécurité SSID voix, partie 1

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption AES(CCMP128)

CCMP256

GCMP128

GCMP256

Auth Key Mgmt 802.1x

PSK

Easy-PSK

CCKM

Paramètres de sécurité SSID voix, partie 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

Paramètres de sécurité SSID voix, partie 3

 Remarque : avec un SSID PSK, il n'est pas nécessaire d'activer le protocole FTP, car la prise de contact pendant l'itinérance est courte. Lors de la configuration de 802.1X WPA Enterprise, il est conseillé d'activer FT+802.1X en tant qu'AKM et d'activer la transition rapide, mais de conserver le paramètre « Over the DS » comme désactivé. Vous pouvez également configurer FT+PSK, mais cet exemple utilise PSK normal pour simplifier.

Étape 2. Accédez à l'onglet Advanced et activez Aironet IE. Assurez-vous que l'équilibrage de charge et la sélection de bande sont désactivés :

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	

Sur la même page, assurez-vous que le report de l'analyse hors canal est activé pour les priorités 5, 6 et 7. Cela empêche le point d'accès de sortir du canal pendant 100 ms après la réception d'une trame avec ces priorités UP (essentiellement une trame vocale).

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"/>

Étape 3. Sélectionnez Profil de stratégie et cliquez sur Ajouter :

The screenshot displays a configuration page with a vertical flow from 'Start' to 'Done'. The main section is titled 'Tags & Profiles' and contains several 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. Below this is an 'Apply' section with 'Tag APs'. On the right side, there is a '+ Add' button (highlighted with a blue box) and a 'Delete' button. Below these is a list titled 'Policy Profile Name' with a dropdown arrow. The list contains one item: 'default-policy-profile' with an unchecked checkbox. Navigation controls show '1' items per page and '10 items per page'.

Configurez le nom du profil de stratégie, définissez l'état sur Activé et maintenez la commutation centrale, l'authentification, le protocole DHCP et l'association (après 17.6, la case à cocher d'association centrale disparaît) activés :

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

Cliquez sur Access Policies et configurez le VLAN auquel le client sans fil sera affecté lors de la connexion au 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

VLAN

VLAN/VLAN Group

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

Page Paramètres des stratégies d'accès aux profils de stratégie

Cliquez sur QoS et AVC, et configurez le paramètre Auto QoS en tant que Voice. Cliquez sur Enregistrer et appliquer au périphérique.

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

Cliquez sur Advanced, définissez le délai d'expiration de la session sur 84000, assurez-vous que DHCP IPv4 requis est désactivé et activez le proxy ARP.

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

Page Paramètres avancés du profil de stratégie

Étape 4. Sélectionnez Balise de stratégie et cliquez sur Ajouter. Configurez le nom de la balise de stratégie. Sous WLAN-Policy Maps, cliquez sur +Add. Sélectionnez WLAN Profile et Policy Profile

dans les menus déroulants, puis cliquez sur la vérification de la carte à configurer. Cliquez ensuite sur Enregistrer et appliquer au périphérique.

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

Étape 5. Sélectionnez Balise de site et cliquez sur Ajouter. Cochez la case Enable Local Site pour que les AP fonctionnent en mode local. Cliquez ensuite sur Enregistrer et appliquer au périphérique :

Add Site Tag

Name*

Description

AP Join Profile

Control Plane Name

Enable Local Site

Étape 6. Sélectionnez RF Profile et cliquez sur Add. Configurez un profil RF par bande.

Add RF Profile ✕

General 802.11 RRM Advanced

Name*

Radio Band

Status **ENABLE**

Description

↶ Cancel Save & Apply to Device

Accédez au menu 802.11. Désactivez tous les débits inférieurs à 12 Mbits/s, définissez 12 Mbits/s comme débit obligatoire et 18 Mbits/s et plus comme débit pris en charge sur les deux bandes.

Débits de données 2,4 GHz :

Add RF Profile



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

Navigation: 1 2 3 4

10 items per page

1 - 10 of 32 items

Cancel

Save & Apply to Device

Débits de données 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 & Apply to Device

Étape 7. Sélectionnez RF Tag et cliquez sur Add. Sélectionnez les profils RF créés à l'étape 5 de cette section. Cliquez ensuite sur Enregistrer et appliquer au périphérique.

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"/> ▼

Étape 8. Sélectionnez Tag APs, choisissez les AP et ajoutez la politique, le site et la balise RF précédemment créés. Cliquez ensuite sur Enregistrer et appliquer au périphérique.

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

Commutation centrale : interface de ligne de commande (CLI)

À partir de l'interface de ligne de commande, exécutez ces commandes :

<#root>

////////// 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

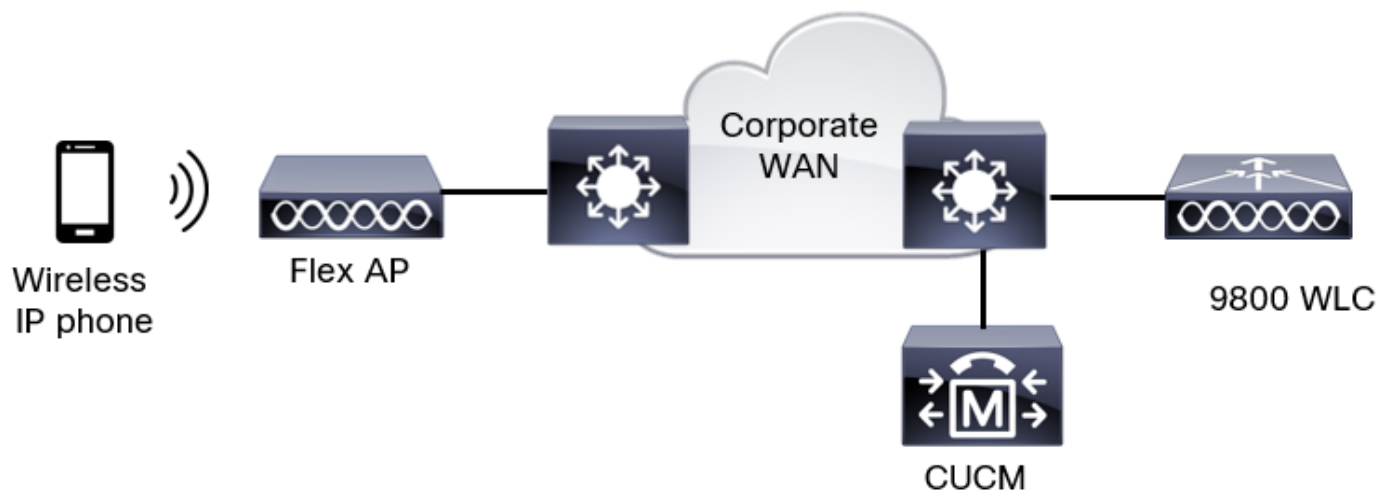
```
wireless tag rf RT1  
24ghz-rf-policy Voice24GHz  
5ghz-rf-policy Voice5GHz
```

////////// AP Configuration

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

Option b : Commutation locale FlexConnect

Schéma du réseau de commutation locale Flexconnect



Balises et profils de commutation locale Flexconnect

Étape 1. Accédez à Configuration > Wireless Setup > Advanced > Start Now > WLAN Profile et cliquez sur +Add afin de créer un nouveau WLAN. Configurez le SSID, le nom de profil, l'ID WLAN et l'état du WLAN. Accédez ensuite à Security > Layer 2 et configurez les paramètres :

Add WLAN



General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode

MAC Filtering

Protected Management Frame

PMF

WPA Parameters

Lobby Admin Access

Fast Transition

Over the DS

Reassociation Timeout

MPSK Configuration

MPSK

Paramètres de sécurité SSID voix, partie 1

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption AES(CCMP128)

CCMP256

GCMP128

GCMP256

Auth Key Mgmt 802.1x

PSK

Easy-PSK


CCKM

Paramètres de sécurité SSID voix, partie 2

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

PSK Format	ASCII
PSK Type	Unencrypted
Pre-Shared Key*

Paramètres de sécurité SSID voix, partie 3

 Remarque : avec un SSID PSK, il n'est pas nécessaire d'activer le protocole FTP, car la prise de contact pendant l'itinérance est courte. Lors de la configuration de 802.1X WPA Enterprise, il est conseillé d'activer FT+802.1X en tant qu'AKM et d'activer la transition rapide, mais de conserver le paramètre « Over the DS » comme désactivé. Vous pouvez également configurer FT+PSK, mais cet exemple utilise un PSK standard pour simplifier.

Étape 2. Accédez à l'onglet Advanced et activez Aironet IE. Assurez-vous que l'équilibrage de charge et la sélection de bande sont désactivés :

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	

Sur la même page, assurez-vous que le report de l'analyse hors canal est activé pour les priorités 5, 6 et 7. Cela empêche le point d'accès de sortir du canal pendant 100 ms après la réception d'une trame avec ces priorités UP (essentiellement une trame vocale).

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			

Étape 3. Sélectionnez Profil de stratégie et cliquez sur Ajouter :

The screenshot displays the 'Advanced' configuration page for wireless setup. On the left, a vertical navigation bar starts with a 'Start' button and ends with a 'Done' button. The main content area is divided into two sections: 'Tags & Profiles' and 'Apply'. Under 'Tags & Profiles', several configuration items are listed, each with an information icon, a name, and control icons (list, delete, and checkbox). The 'Policy Profile' item is highlighted with a blue box and a right-pointing arrow. Under 'Apply', there is a 'Tag APs' item. On the right side, there is a '+ Add' button (highlighted with a blue box) and a 'Delete' button. Below these buttons is a table with the header 'Policy Profile Name' and one row containing 'default-policy-profile'. Navigation controls show '1' items per page and '10 items per page'.

Configurez le nom du profil de stratégie, définissez l'état sur Activé, désactivez la commutation centrale et le DHCP central. Dans le cas d'un SSID PSK, l'authentification peut être déplacée sur local pour donner au point d'accès le rôle de vérifier le PSK. Dans le cas de la norme 802.1X, vous souhaitez généralement que le WLC continue à effectuer les authentifications 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

Name*	<input type="text" value="PP2"/>	WLAN Switching Policy	
Description	<input type="text" value="Enter Description"/>	Central Switching	<input type="checkbox"/> DISABLED
Status	<input checked="" type="checkbox"/> ENABLED	Central Authentication	<input checked="" type="checkbox"/> ENABLED
Passive Client	<input type="checkbox"/> DISABLED	Central DHCP	<input type="checkbox"/> DISABLED
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED	Flex NAT/PAT	<input type="checkbox"/> DISABLED
CTS Policy			
Inline Tagging	<input type="checkbox"/>		
SGACL Enforcement	<input type="checkbox"/>		
Default SGT	<input type="text" value="2-65519"/>		

Flex Configuration du profil de stratégie de commutation locale

Accédez à l'onglet Access Policies pour attribuer le VLAN auquel les clients sans fil sont affectés lorsqu'ils se connectent à ce WLAN par défaut. Vous pouvez sélectionner un nom de VLAN dans la liste déroulante ou saisir manuellement un ID de VLAN.

Cliquez sur QoS et AVC, et configurez le paramètre Auto QoS en tant que Voice. Cliquez sur Enregistrer et appliquer au périphérique.

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

Cliquez sur Advanced, définissez le délai d'expiration de la session sur 84000, assurez-vous que DHCP IPv4 requis est désactivé et désactivez le 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 DISABLED

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

[Cancel](#)

[Update & Apply to Device](#)

Paramètres avancés du profil de stratégie flexible

Étape 4. Sélectionnez Balise de stratégie et cliquez sur Ajouter. Configurez le nom de la balise de stratégie. Sous WLAN-Policy Maps, cliquez sur +Add. Sélectionnez WLAN Profile et Policy Profile

dans les menus déroulants, puis cliquez sur le bouton Check for the map to be configured. Cliquez ensuite sur Enregistrer et appliquer au périphérique.

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

Étape 5. Cliquez sur Flex Profile, puis sur Add. Configurez le nom du profil flexible, l'ID du VLAN natif et activez la mise en cache ARP :

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		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 ▾		

Paramètres de stratégie de profil flexible



Remarque : l'ID de VLAN natif fait référence au VLAN natif configuré dans le port de commutation auquel les AP, associés à ce profil flexible, sont connectés.

Étape 6. Sélectionnez Balise de site et cliquez sur Ajouter. Configurez le nom de la balise de site, décochez l'option Enable Local Site et ajoutez le profil paramétrable. Cliquez ensuite sur Enregistrer et appliquer au périphérique.

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"/>

Cancel

Save & Apply to Device



Remarque : lorsque l'option Activer le site local est désactivée, les points d'accès affectés à cette balise de site sont automatiquement configurés en tant que points d'accès FlexConnect.

Étape 7. Sélectionnez RF Profile et cliquez sur Add. Configurez un profil RF par bande.

Add RF Profile ✕

General 802.11 RRM Advanced

Name*

Radio Band

Status **ENABLE**

Description

Accédez au menu 802.11. Désactivez tous les débits inférieurs à 12 Mbits/s, définissez 12 Mbits/s comme débit obligatoire et 18 Mbits/s et plus comme débit pris en charge sur les deux bandes.

Débits de données 2,4 GHz :

Add RF Profile



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

10 items per page
1 - 10 of 32 items

Cancel

Save & Apply to Device

Débits de données 5 GHz :

Add RF Profile



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

Étape 8. Sélectionnez RF Tag et cliquez sur Add. Configurez les profils RF créés à l'étape 6 de cette section. Cliquez ensuite sur Enregistrer et appliquer au périphérique.

Add RF Tag ✕

Name*

Description

5 GHz Band RF Profile ▼

2.4 GHz Band RF Profile ▼

Étape 9. Sélectionnez Tag APs, choisissez les AP et ajoutez la politique, le site et la balise RF précédemment créés. Cliquez ensuite sur Enregistrer et appliquer au périphérique.

Tag APs ✕

Tags

Policy ▼

Site ▼

RF ▼

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

L'AP redémarrera son tunnel CAPWAP et rejoindra le WLC 9800. Accédez à Configuration > Wireless > Access Points et confirmez que le mode AP est 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

Interface de ligne de commande (CLI) de commutation locale Flexconnect

À partir de l'interface de ligne de commande, exécutez ces commandes :

```
<#root>
```

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

Configuration des paramètres multimédias

Configuration de la GUI

Étape 1. Accédez à Configuration > Radio Configuration > Network. Désactivez les bandes 5 GHz et 2,4 GHz, puis cliquez sur Appliquez.

Soyez attentif à ce que cela désactivera temporairement tous vos réseaux wifi 5 ghz ! Exécuter uniquement lorsque vous êtes dans une fenêtre de maintenance

5 GHz Band

2.4 GHz Band

General

5 GHz Network Status

Beacon Interval*

100

Fragmentation Threshold(bytes)*

2346

DTPC Support

Étape 2. Accédez à Configuration > Radio Configuration > Media Parameters. Activez le contrôle d'admission et le contrôle d'admission d'appel basé sur la charge (CAC) sur les bandes 2,4 GHz et 5 GHz, puis cliquez sur 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

Étape 3. Accédez à Configuration > Radio Configurations > Parameters. Configurez le profil EDCA en tant que voix optimisée sur les deux bandes, puis cliquez sur Apply.

Configuration > Radio Configurations > Parameters

5 GHz Band

2.4 GHz Band

EDCA Parameters

EDCA Profile

optimized-voice

DFS (802.11h)

Étape 4. Accédez à Configuration > Radio Configuration > Network. Activez les bandes 5 GHz et 2,4 GHz, puis cliquez sur Apply.

Interface de ligne de commande (CLI)

À partir de CLI, exécutez ces commandes :

```
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
```

Vérifier

Vous pouvez utiliser ces commandes pour vérifier la configuration actuelle:

```
# 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>
```

Pour consulter les statistiques CAC et les mesures de contrôle des appels, exécutez ces commandes :

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

Dépannage

Débogage conditionnel et traçage Radio Active

La trace Radio Active (RA) fournit des traces de niveau de débogage pour tous les processus qui interagissent avec la condition spécifiée (l'adresse MAC du client dans ce cas). Afin d'activer le débogage conditionnel, exécutez ces étapes. Nous nous concentrons sur le résultat que le WLC 9800 fournit pendant un appel.

Étape 1. Assurez-vous qu'aucune condition de débogage n'est activée.


```
# clear platform condition all
```

Étape 2. Activez la condition de débogage pour l'adresse MAC du client sans fil que vous souhaitez surveiller. Cette commande commence à surveiller l'adresse MAC fournie pendant 30 minutes (1 800 secondes). Vous pouvez aussi augmenter ce délai pour qu'il atteigne jusqu'à 2085978494 secondes.

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



Remarque : Afin de surveiller plusieurs clients à la fois, exécutez la <aaaa.bbbb.cccc>commande de débogage sans fil mac par adresse MAC.

 Remarque : Le résultat de l'activité du client ne s'affiche pas sur la session du terminal, car tout est mis en mémoire tampon interne pour être consulté plus tard.

Étape 3. Établir un appel à partir du téléphone IP Cisco 8821.

Étape 4. Arrêtez les débogages lorsque l'appel est terminé ou si le problème est reproduit avant que le temps de surveillance par défaut ou configuré ne soit écoulé.

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

Une fois que le temps de surveillance s'est écoulé ou que le débogage sans fil a été arrêté, le contrôleur WLC 9800 génère un fichier local du nom de :

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Étape 5. Recueillir le fichier de l'activité de l'adresse MAC. Il est possible de copier le fichier de suivi RA .log sur un serveur externe ou d'afficher le résultat directement à l'écran. Vérifiez le nom du fichier de suivi RA

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

Copiez le fichier sur un serveur externe :


```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.
```

Affichez-en le contenu :

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

Étape 6. Supprimez les conditions de débogage.

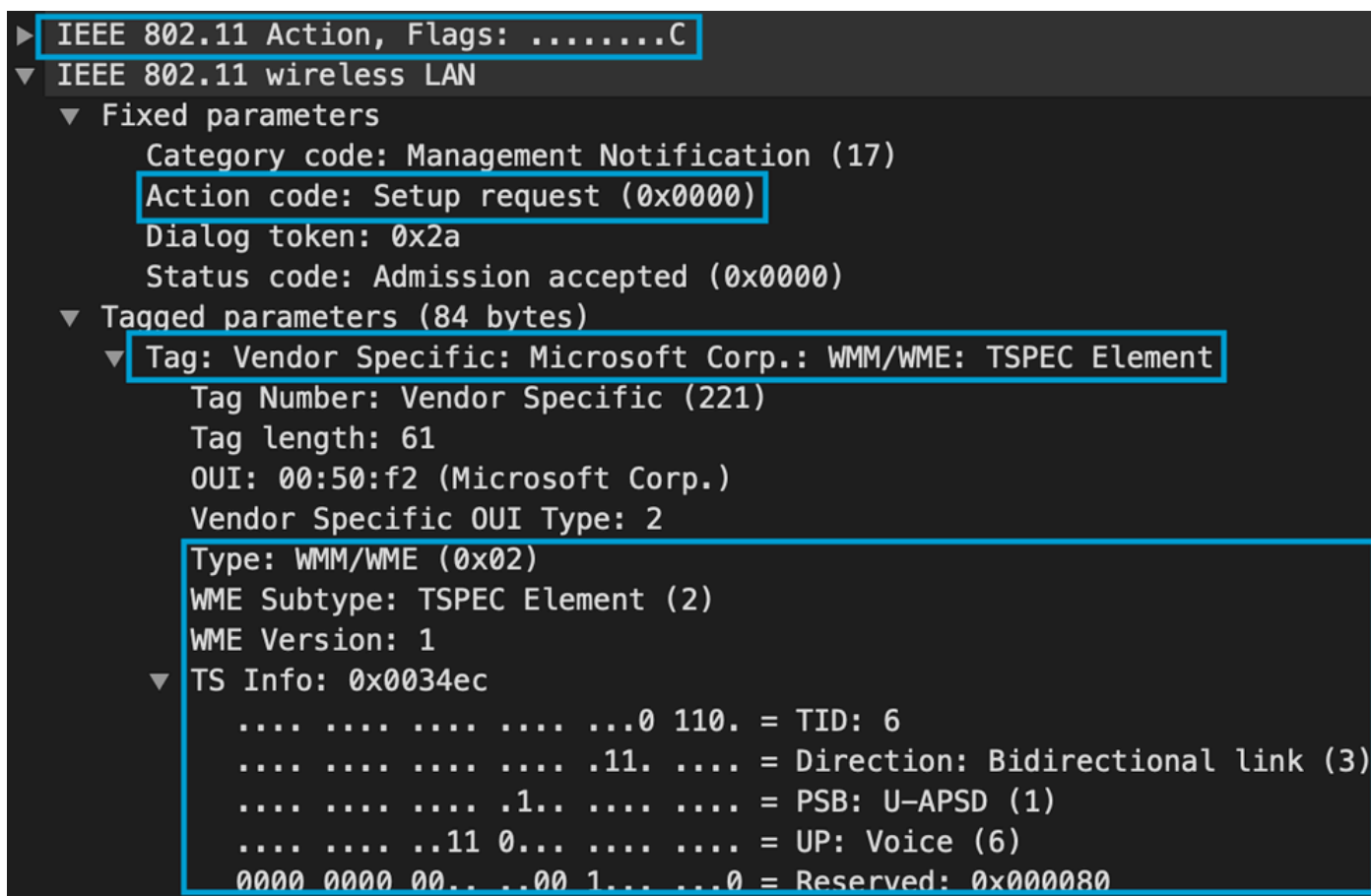
```
# clear platform condition all
```

 Remarque : assurez-vous de toujours supprimer les conditions de débogage après une session de dépannage.

Dans la sortie de la trace RA, la négociation de spécification de trafic (TSPEC) a lieu, cela déterminera si le 8821 est autorisé à marquer son trafic avec une priorité d'utilisateur de 6 et si l'appel peut être établi ou non. Pour négocier l'utilisation de la file d'attente 6, le 8821 envoie un paquet d'action demandant une autorisation.

```
2019/08/25 18:53:54.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24 Got act
2019/08/25 18:53:54.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24 Receive
2019/08/25 18:53:54.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24 Got LBC
2019/08/25 18:53:54.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24 ADD TS
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
```

Dans une capture de paquets :



```
▶ 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
```

Le WLC détermine s'il y a suffisamment de bande passante pour allouer l'appel ou non, et si c'est le cas, il envoie une trame d'action acceptant la négociation TSPEC :

```
2019/08/25 18:53:54.510 {wncd_x_R0-0}{1}: [auth-mgr] [18106]: (info): [0000.0000.0000:unknown] Session
2019/08/25 18:53:54.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): Calls in progress increment
```

```

2019/08/25 18:53:54.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): allocating voice bw for cli
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 Se
2019/08/25 18:53:54.511 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): Recommended rate 6500kbps:M
2019/08/25 18:53:54.511 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): Recommended rate 13000kbps:
2019/08/25 18:53:54.511 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): Recommended rate 26000kbps:
2019/08/25 18:53:54.511 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24 Sending
2019/08/25 18:53:54.511 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24 Build A
2019/08/25 18:53:54.511 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: a023.9f86.52c0 send qo

```

Dans une capture de paquets :

```

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

```

Ensuite, l'appel est établi via SIP avec le gestionnaire d'appels et le trafic RTP est transféré.

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

Paquets 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

Ensuite, le 8821 informe le gestionnaire d'appels que l'appel est terminé, et il notifie le WLC qui n'utilise plus la file d'attente 6 en envoyant une autre trame d'action :

```

2019/08/25 18:54:08.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24 Got act
2019/08/25 18:54:08.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24 Receive
2019/08/25 18:54:08.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24 DEL TS
2019/08/25 18:54:08.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24 Call Te
2019/08/25 18:54:08.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24 Calls i
2019/08/25 18:54:08.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: 0027.902a.ab24 Build D
2019/08/25 18:54:08.510 {wncd_x_R0-0}{1}: [ewlc-qos-voice] [18106]: (info): MAC: a023.9f86.52c0 send qo

```

Terminaison SIP et trame d'action :

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

```

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.