Exemple de configuration de QoS sur les contrôleurs d'accès convergents et les points d'accès légers

Contenu

Introduction

Ce document décrit comment configurer la QoS dans un réseau d'accès convergent Cisco avec des points d'accès légers (LAP) et avec le commutateur Cisco Catalyst 3850 ou le contrôleur LAN sans fil (WLC) Cisco 5760.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base sur la configuration des LAP et des contrôleurs d'accès convergents Cisco
- Savoir configurer le routage et la QoS de base dans un réseau filaire

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Commutateur Cisco Catalyst 3850 qui exécute Cisco IOS ? Logiciel XE version 3.2.2(SE)
- Contrôleur LAN sans fil Cisco 5760 qui exécute le logiciel Cisco IOS XE version 3.2.2(SE)
- Points d'accès légers de la gamme Cisco 3600

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. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

La QoS renvoie à la capacité du réseau à fournir un meilleur service ou un service particulier à un ensemble d'utilisateurs ou d'applications au détriment d'autres utilisateurs ou applications.

Grâce à la QoS, la bande passante peut être gérée plus efficacement sur les LAN, notamment les WLAN et les WAN. La QoS fournit un service réseau fiable et amélioré avec ces services :

- Prise en charge de la bande passante dédiée pour les utilisateurs et les applications essentiels.
- Contrôle la gigue et la latence requises par le trafic en temps réel.
- Gère et réduit la congestion du réseau.
- Forme le trafic réseau afin d'en lisser le flux.
- Définit les priorités du trafic réseau.

Par le passé, les réseaux WLAN servaient principalement à acheminer les applications de données à faible bande passante. Avec l'extension des WLAN vers des environnements verticaux (tels que la vente au détail, la finance et l'éducation) et d'entreprise, les WLAN sont désormais utilisés pour transporter des applications de données à bande passante élevée en conjonction avec des applications multimédias à durée limitée. Cette exigence a entraîné le besoin d'une QoS sans fil.

Le groupe de travail IEEE 802.11e du comité des normes IEEE 802.11 a complété la définition de norme, et Wi-Fi Alliance a créé la certification WMM (Wi-Fi Multimedia), mais l'adoption de la norme 802.11e reste limitée. La plupart des périphériques sont certifiés WMM, car la certification WMM est nécessaire pour les certifications 802.11n et 802.11ac. De nombreux périphériques sans fil n'attribuent pas différents niveaux de QoS aux paquets envoyés à la couche liaison de données, de sorte que ces périphériques envoient la majeure partie de leur trafic sans marquage QoS et sans hiérarchisation relative. Cependant, la plupart des téléphones IP VoWLAN (Voice

over Wireless LAN) 802.11 marquent et hiérarchisent leur trafic vocal. Ce document se concentre sur la configuration QoS pour les téléphones IP VoWLAN et sur les périphériques Wi-Fi compatibles vidéo qui marquent leur trafic voix.

> **Note**: La configuration QoS pour les périphériques qui n'effectuent pas de marquage interne n'entre pas dans le cadre de ce document.

La modification 802.11e définit huit niveaux de priorité utilisateur (UP), regroupés deux par deux en quatre niveaux de QoS (catégories d'accès) :

- Platinum/Voice (UP 7 et 6) : garantit une qualité de service élevée pour la voix sur le réseau sans fil.
- Gold/Video (UP 5 et 4) : prend en charge les applications vidéo de haute qualité.
- Silver/Best Effort (UP 3 et 0) : prend en charge la bande passante normale pour les clients. Voici la configuration par défaut .
- Bronze/Background (UP 2 et 1) : offre la bande passante la plus faible pour les services invités.

Platinum est couramment utilisé pour les clients VoIP et Gold pour les clients vidéo. Ce document fournit un exemple de configuration qui illustre comment configurer la QoS sur les contrôleurs et communiquer avec un réseau câblé configuré avec la QoS pour les clients VoWLAN et vidéo.

Améliorations du marquage des paquets QoS de couche 3

Les contrôleurs d'accès convergents Cisco prennent en charge le marquage DSCP (IP Differentiated Services Code Point) de couche 3 (L3) des paquets envoyés par les WLC et les LAP. Cette fonctionnalité améliore la façon dont les points d'accès (AP) utilisent ces informations de couche 3 afin de s'assurer que les paquets reçoivent la hiérarchisation correcte en direct du point d'accès au client sans fil.

Dans une architecture WLAN d'accès convergé qui utilise des commutateurs Catalyst 3850 comme contrôleurs sans fil, les points d'accès se connectent directement au commutateur. Dans une architecture WLAN d'accès convergé qui utilise des contrôleurs 5760, les données WLAN sont tunnellisées entre le point d'accès et le WLC via le protocole CAPWAP (Control and Provisioning of Wireless Access Points). Afin de maintenir la classification QoS d'origine dans ce tunnel, les paramètres QoS du paquet de données encapsulé doivent être correctement mappés aux champs de couche 2 (L2) (802.1p) et de couche 3 (IP DSCP) du paquet de tunnel externe.

Lorsque vous configurez la QoS pour VoWLAN et la vidéo, vous pouvez configurer une stratégie QoS spécifique aux clients sans fil et une stratégie spécifique à un WLAN, ou les deux. Vous pouvez également compléter la configuration par une configuration spécifique au port qui relie le point d'accès, en particulier avec les commutateurs Catalyst 3850. Cet exemple de configuration se concentre sur la configuration QoS pour le client sans fil, le WLAN et le port vers le point d'accès. Les principaux objectifs d'une configuration QoS pour les applications vidéo et VoWLAN sont les suivants :

- Reconnaître le trafic voix et vidéo (classification et marquage du trafic), en amont et en aval.
- Marquer le trafic voix et vidéo avec un niveau de priorité voix : 802.11e UP 6, 802.1p 5, DSCP 46 pour la voix.802.11e UP 5, DSCP 34 pour la vidéo.
- Allouer de la bande passante pour le trafic voix, la signalisation vocale et le trafic vidéo.

Configuration d'un réseau sans fil pour QoS avec MQC

Avant de configurer la QoS, vous devez configurer la fonction WCM (Wireless Controller Module) du commutateur Catalyst 3850 ou du WLC Cisco 5760 pour le fonctionnement de base et enregistrer les LAP sur le WCM. Ce document suppose que le WCM est configuré pour le fonctionnement de base et que les LAP sont enregistrés dans le WCM.

La solution d'accès convergé utilise l'interface de ligne de commande (CLI) MQC (Modular QoS). Référez-vous au Guide de configuration QoS, Cisco IOS XE version 3SE (commutateurs Catalyst 3850) pour plus d'informations sur l'utilisation de MQC dans la configuration QoS sur le commutateur Catalyst 3850.

La configuration de QoS avec MQC sur les contrôleurs d'accès convergents repose sur quatre éléments :

- **Les cartes-classes** sont utilisées afin de reconnaître le trafic d'intérêt. Les cartes de classe peuvent utiliser diverses techniques (telles que le marquage QoS existant, les listes d'accès ou les VLAN) afin d'identifier le trafic intéressant.
- **Les cartes de stratégie** sont utilisées afin de déterminer quels paramètres QoS doivent être appliqués au trafic concerné. Les cartes de stratégie appellent les cartes de classe et appliquent divers paramètres de QoS (tels que le marquage spécifique, les niveaux de priorité, l'allocation de bande passante, etc.) à chaque classe.
- **Les stratégies de service** sont utilisées afin d'appliquer des cartes de stratégie aux points stratégiques de votre réseau. Dans la solution d'accès convergé, les politiques de service peuvent être appliquées aux utilisateurs, aux SSID (Service Set Identifiers), aux radios AP et aux ports. Les stratégies de port, de SSID et de client peuvent être configurées par l'utilisateur. Les stratégies radio sont contrôlées par le module de contrôle sans fil. Les stratégies QoS sans fil pour le port, le SSID, le client et la radio sont appliquées dans la direction en aval lorsque le trafic circule du commutateur ou du contrôleur vers les clients sans fil.
- **Les tables-maps** sont utilisées pour examiner le marquage QoS entrant et pour décider des marquages QoS sortants. Les tables-maps sont positionnées dans les cartes-politiques appliquées aux SSID. Les cartes-tables peuvent être utilisées pour conserver (copier) ou modifier le marquage. Les tables-maps peuvent également être utilisées pour créer un mappage entre le marquage filaire et le marquage sans fil. Le marquage câblé utilise la qualité de service (QoS) DSCP (L3) ou 802.1p (QoS L2). Le marquage sans fil utilise la priorité utilisateur (UP). Les tables-maps sont couramment utilisées pour déterminer le marquage DSCP à utiliser pour chaque UP d'intérêt et le UP à utiliser pour chaque DSCP de valeur d'intérêt. Les tables-maps sont fondamentales pour la qualité de service d'accès convergé car il n'existe pas de traduction directe entre les valeurs DSCP et UP.

Cependant, les tables-maps DSCP à UP permettent également l'instruction *copy*. Dans ce cas, la solution d'accès convergé utilise la table de mappage AVVID (Architecture for Voice, Video and Integrated Data) de Cisco afin de déterminer la traduction DSCP vers UP ou UP vers DSCP :

Index des étiquettes	Champ Clé	Valeur entrante	DSCP externe	CoS	HAUT
0	N.A.	Non coché	0	0	0
1-10	DSCP	0-7	0-7	0	0
11-18	DSCP	8-15	8-15	1	2
19-26	DSCP	16-23	16-23	2	3
27-34	DSCP	24-31	24-31	3	4

35-46	DSCP	32-39	32-39	4	5
47-48	DSCP	40-47	40-47	5	6
49-63	DSCP	48-55	48-55	6	7
64	DSCP	56-63	56-63	7	7
65	CoS	0	0	0	0
66	CoS	1	8	1	2
67	CoS	2	16	2	3
68	CoS	3	24	3	4
69	CoS	4	32	4	5
70	CoS	5	40	5	6
71	CoS	6	48	6	7
72	CoS	7	56	7	7
73	HAUT	0	0	0	0
74	HAUT	1	8	1	1
75	HAUT	2	16	1	2
76	HAUT	3	24	2	3
77	HAUT	4	34	3	4
78	HAUT	5	34	4	5
79	HAUT	6	46	5	6
80	HAUT	7	46	7	7

Stratégies codées en dur par défaut

Les contrôleurs d'accès convergents lancent des profils de stratégie QoS codés en dur qui peuvent être appliqués aux WLAN. Ces profils appliquent les politiques métalliques (platine, or, etc.) qui sont familières aux administrateurs des contrôleurs Cisco Unified Wireless Networks (CUWN). Si votre objectif n'est pas de créer des stratégies qui attribuent une bande passante spécifique au trafic vocal, mais simplement de vous assurer que le trafic vocal reçoit le marquage QoS approprié, vous pouvez utiliser les stratégies codées en dur. Les politiques codées en dur peuvent être appliquées au WLAN et peuvent être différentes dans les directions amont et aval.

> **Remarques :**
>
> Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.
>
> L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Platine

La politique codée en dur pour la voix s'appelle le platine. Le nom ne peut pas être modifié.

Il s'agit de la politique en aval pour le niveau de QoS du platine :

```
Policy-map platinum
Class class-default
```

```
 set dscp dscp table plat-dscp2dscp
 set wlan user-priority dscp table plat-dscp2up
Table-map plat-dscp2dscp
   from 45 to 45
   from 46 to 46
   from 47 to 47
   default copy
Table-map plat-dscp2up
   from 34 to 4
   from 46 to 6
   default copy
```

Il s'agit de la stratégie en amont pour le niveau de QoS Platinum :

```
Policy-map platinum-up
   Class class-default
     set dscp wlan user-priority table plat-up2dscp

Table-map plat-up2dscp
   from 4 to 34
   from 5 to 34
   from 6 to 46
   from 7 to 8
   default copy
```

Or

La politique de la vidéo en dur est appelée gold. Le nom ne peut pas être modifié.

Il s'agit de la politique en aval pour le niveau de QoS or :

```
Policy Map gold
   Class class-default
     set dscp dscp table gold-dscp2dscp
     set wlan user-priority dscp table gold-dscp2u
Table Map gold-dscp2dscp
   from 45 to 34
   from 46 to 34
   from 47 to 34
   default copy

Table Map gold-dscp2up
   from 45 to 4
   from 46 to 4
   from 47 to 4
   default copy
```

Il s'agit de la politique en amont pour le niveau de QoS or :

```
Policy Map gold-up
   Class class-default
     set dscp wlan user-priority table gold-up2dscp

Table Map gold-up2dscp
   from 6 to 34
   from 7 to 34
   default copy
```

Argent

La politique codée en dur pour le meilleur effort est appelée argent. Le nom ne peut pas être modifié.

Il s'agit de la stratégie en aval pour le niveau QoS argenté :

```
Policy Map silver
   Class class-default
     set dscp dscp table silver-dscp2dscp
     set wlan user-priority dscp table silver-dscp2up

Table Map silver-dscp2dscp
   from 34 to 0
   from 45 to 0
   from 46 to 0
   from 47 to 0
   default copy
Table Map silver-dscp2up
   from 34 to 0
   from 45 to 0
   from 46 to 0
   from 47 to 0
   default copy
```

Il s'agit de la stratégie en amont pour le niveau QoS argenté :

```
Policy Map silver-up
   Class class-default
     set dscp wlan user-priority table silver-up2dscp
Table Map silver-up2dscp
   from 4 to 0
   from 5 to 0
   from 6 to 0
   from 7 to 0
   default copy
```

Bronze

La politique codée en dur pour le trafic en arrière-plan est appelée bronze. Le nom ne peut pas être modifié.

Il s'agit de la politique en aval pour le niveau de qualité de service en bronze :

```
Policy Map bronze
   Class class-default
     set dscp dscp table bronze-dscp2dscp
 set wlan user-priority dscp table bronze-dscp2up

Table Map bronze-dscp2dscp
   from 0 to 8
   from 34 to 8
   from 45 to 8
   from 46 to 8
   from 47 to 8
   default copy
```

```
Table Map bronze-dscp2up
   from 0 to 1
   from 34 to 1
   from 45 to 1
   from 46 to 1
   from 47 to 1
   default copy
```

Il s'agit de la stratégie en amont pour le niveau de qualité de service en bronze :

```
Policy Map bronze-up
   Class class-default
     set dscp wlan user-priority table bronze-up2dscp
Table Map bronze-up2dscp
   from 0 to 8
   from 1 to 8
   from 4 to 8
   from 5 to 8
   from 6 to 8
   from 7 to 8
   default copy
```

Une fois que vous avez décidé quelle table-map correspond le mieux au trafic cible pour un SSID donné, vous pouvez appliquer la stratégie correspondante à votre WLAN. Dans cet exemple, une stratégie est appliquée dans la direction en aval (sortie, du point d'accès au client sans fil), et une stratégie est appliquée dans la direction en amont (entrée, du client sans fil, via le point d'accès, au contrôleur) :

```
3850#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
3850(config)#wlan test1
3850(config-wlan)#service-policy output platinum
3850(config-wlan)#service-policy input platinum-up
3850(config-wlan)#end
3850#
```

Vérifiez la configuration WLAN afin de vérifier quelle stratégie a été appliquée à votre WLAN :

```
3850#show wlan name test1
WLAN Profile Name     : test1
===============================================
Identifier                                : 1
Network Name (SSID)                       : test1
Status                                    : Disabled
Broadcast SSID                            : Enabled
Maximum number of Associated Clients      : 0
AAA Policy Override                       : Disabled
Network Admission Control
 NAC-State                               : Disabled
Number of Active Clients                  : 0
Exclusionlist Timeout                     : 60
Session Timeout                           : 1800 seconds
CHD per WLAN                              : Enabled
Webauth DHCP exclusion                    : Disabled
Interface                                 : default
Interface Status                          : Up
Multicast Interface                       : Unconfigured
WLAN IPv4 ACL                             : unconfigured
WLAN IPv6 ACL                             : unconfigured
DHCP Server                               : Default
DHCP Address Assignment Required          : Disabled
```

```
DHCP Option 82                                  : Disabled
DHCP Option 82 Format                           : ap-mac
DHCP Option 82 Ascii Mode                       : Disabled
DHCP Option 82 Rid Mode                         : Disabled
QoS Service Policy - Input
 Policy Name                                   : platinum-up
 Policy State                                  : Validation Pending
QoS Service Policy - Output
 Policy Name                                   : platinum
 Policy State                                  : Validation Pending
QoS Client Service Policy
 Input  Policy Name                            : unknown
 Output Policy Name                            : unknown
WMM                                             : Allowed
Channel Scan Defer Priority:
 Priority (default)                            : 4
 Priority (default)                            : 5
 Priority (default)                            : 6
Scan Defer Time (msecs)                         : 100
Media Stream Multicast-direct                   : Disabled
CCX - AironetIe Support                         : Enabled
CCX - Gratuitous ProbeResponse (GPR)            : Disabled
CCX - Diagnostics Channel Capability            : Disabled
Dot11-Phone Mode (7920)                         : Invalid
Wired Protocol                                  : None
Peer-to-Peer Blocking Action                    : Disabled
Radio Policy                                    : All
DTIM period for 802.11a radio                   : 1
DTIM period for 802.11b radio                   : 1
Local EAP Authentication                        : Disabled
Mac Filter Authorization list name              : Disabled
Accounting list name                            : Disabled
802.1x authentication list name                 : Disabled
Security
   802.11 Authentication                        : Open System
   Static WEP Keys                              : Disabled
   802.1X                                       : Disabled
   Wi-Fi Protected Access (WPA/WPA2)            : Enabled
       WPA (SSN IE)                             : Disabled
       WPA2 (RSN IE)                            : Enabled
           TKIP Cipher                          : Disabled
           AES Cipher                           : Enabled
       Auth Key Management
           802.1x                               : Enabled
           PSK                                  : Disabled
           CCKM                                 : Disabled
   CKIP                                         : Disabled
   IP Security                                  : Disabled
   IP Security Passthru                         : Disabled
   L2TP                                         : Disabled
   Web Based Authentication                     : Disabled
   Conditional Web Redirect                     : Disabled
   Splash-Page Web Redirect                     : Disabled
   Auto Anchor                                  : Disabled
   Sticky Anchoring                             : Enabled
   Cranite Passthru                             : Disabled
   Fortress Passthru                            : Disabled
   PPTP                                         : Disabled
   Infrastructure MFP protection                : Enabled
   Client MFP                                   : Optional
   Webauth On-mac-filter Failure                : Disabled
   Webauth Authentication List Name             : Disabled
   Webauth Parameter Map                        : Disabled
   Tkip MIC Countermeasure Hold-down Timer      : 60
```

```
Call Snooping                                : Disabled
Passive Client                               : Disabled
Non Cisco WGB                                : Disabled
Band Select                                  : Disabled
Load Balancing                               : Disabled
IP Source Guard                              : Disabled
```

Configurer manuellement

Les stratégies codées en dur appliquent le marquage QoS par défaut, mais n'appliquent pas l'allocation de bande passante. Les stratégies codées en dur supposent également que votre trafic est déjà marqué. Dans un environnement complexe, vous pouvez utiliser une combinaison de stratégies afin de reconnaître et de marquer le trafic voix et vidéo de manière appropriée, de définir l'allocation de bande passante dans les directions aval et amont, et d'utiliser le contrôle d'admission des appels afin de limiter le nombre d'appels initiés à partir de la cellule sans fil.

> **Note**: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Étape 1 : Identification et marquage du trafic vocal

La première étape consiste à reconnaître le trafic voix et vidéo. Le trafic vocal peut être classé en deux catégories :

- Flux vocal, qui transporte la partie audio de la communication.
- Signalisation vocale, qui transporte les informations statistiques échangées entre les points d'extrémité vocaux.

Le flux vocal utilise généralement des ports de destination RTP (Real-time Transport Protocol) et UDP (User Datagram Protocol) dans la plage 16384 - 32767. Il s'agit de la plage ; les ports réels sont généralement plus étroits et dépendent de la mise en oeuvre.

Il existe plusieurs protocoles de signalisation vocale. Cet exemple de configuration utilise Jabber. Jabber utilise ces ports TCP pour la connexion et le répertoire :

- TCP 80 (HTTP)
- 143 (IMAP [Internet Message Access Protocol])
- 443 (HTTPS)
- 993 (IMAP) pour les services tels que Cisco Unified MeetingPlace ou Cisco WebEx pour les réunions et Cisco Unity ou Cisco Unity Connection pour les fonctions de messagerie vocale
- TCP 389/636 (serveur LDAP [Lightweight Directory Access Protocol] pour les recherches de contacts)
- FTP (1080)
- TFTP (UDP 69) pour le transfert de fichiers (tels que les fichiers de configuration) depuis des homologues ou depuis le serveur

Ces services peuvent ne pas nécessiter de hiérarchisation spécifique.

Jabber utilise le protocole SIP (Session Initiation Protocol) (UDP/TCP 5060 et 5061) pour la signalisation vocale.

Le trafic vidéo utilise différents ports et protocoles qui dépendent de votre mise en oeuvre. Cet exemple de configuration utilise une caméra Tandberg PrecisionHD 720p pour les vidéoconférences. La caméra Tandberg PrecisionHD 720p peut utiliser plusieurs codecs ; la bande passante consommée dépend du codec choisi :

- Les codecs C20, C40 et C60 utilisent H.323/SIP et peuvent consommer jusqu'à 6 Mbits/s en connexions point à point.
- Le codec C90 utilise ces mêmes protocoles et peut consommer jusqu'à 10 Mbits/s dans les communications multisites.

La mise en oeuvre Tandberg de H.323 utilise généralement le protocole UDP 970 pour la diffusion vidéo en continu, le protocole UDP 971 pour la signalisation vidéo, le protocole UDP 972 pour la diffusion audio en continu et le protocole UDP 973 pour la signalisation audio. Les caméras Tandberg utilisent également d'autres ports, tels que :

- UDP 161
- UDP 962 (Simple Network Management Protocol [SNMP])
- TCP 963 (netlog), TCP 964 (FTP)
- TCP 965 (Virtual Network Computing [VNC])
- UDP 974 (protocole d'annonce de session [SAP])

Ces ports supplémentaires peuvent ne pas nécessiter de hiérarchisation spécifique.

Une manière courante d'identifier le trafic consiste à créer des cartes de classe qui ciblent le trafic intéressant. Chaque class-map peut pointer vers une liste d'accès qui cible tout trafic qui utilise les ports voix et vidéo :

```
ip access-list extended JabberVOIP
permit udp any any range 16384 32767
ip access-list extended JabberSIGNALING
permit tcp any any range 5060 5061
permit udp any any range 5060 5061
ip access-list extended H323Videostream
permit udp any any eq 970
ip access-list extended H323Audiostream
permit udp any any eq 972
ip access-list extended H323VideoSignaling
permit udp any any eq 971
ip access-list extended H323AudioSignaling
permit udp any any eq 973
```

Vous pouvez ensuite créer une carte-classe pour chaque type de trafic ; chaque class-map pointe vers la liste d'accès appropriée :

```
class-map RTPaudio
match access-group name JabberVOIP
match access-group name H323Audiostream
class-map H323realtimevideo
match access-group name H323Videostream
class-map signaling
match access-group name JabberSIGNALING
match access-group name H323VideoSignaling
match access-group name H323AudioSignaling
```

Une fois que le trafic vocal et vidéo a été identifié par des cartes de classe, assurez-vous que le trafic est marqué correctement. Cela peut être fait au niveau du WLAN par le biais des tables-maps et peut également être fait par le biais des cartes-politiques du client.

Les tables-maps examinent le marquage QoS du trafic entrant et déterminent le marquage QoS sortant. Ainsi, les tables-maps sont utiles lorsque le trafic entrant a déjà un marquage QoS. Les tables-maps sont utilisées exclusivement au niveau SSID.

En revanche, les cartes-politiques peuvent cibler le trafic identifié par les cartes-classes et sont mieux adaptées au trafic potentiellement non étiqueté d'intérêt. Cet exemple de configuration suppose que le trafic du côté filaire a déjà été marqué correctement avant d'entrer dans le commutateur Catalyst 3850 ou le WLC Cisco 5760. Si ce n'est pas le cas, vous pouvez utiliser une carte de stratégie et l'appliquer au niveau SSID en tant que stratégie client. Étant donné que le trafic des clients sans fil n'a peut-être pas été marqué, vous devez marquer correctement le trafic voix et vidéo :

- La voix en temps réel doit être marquée avec DSCP 46 (Transmission accélérée [EF]).
- La vidéo doit être marquée DSCP 34 (Assecure Forwarding Class 41 [AF41]).
- La signalisation pour la voix et la vidéo doit être marquée DSCP 24 (valeur de service du sélecteur de classe 3 [CS3]).

Pour appliquer ces marquages, créez une carte-politique qui appelle chacune de ces classes et qui marque le trafic équivalent :

```
policy-map taggingPolicy
 class RTPaudio
 set dscp ef

 class H323realtimevideo
 set dscp af41

 class signaling
 set dscp cs3
```

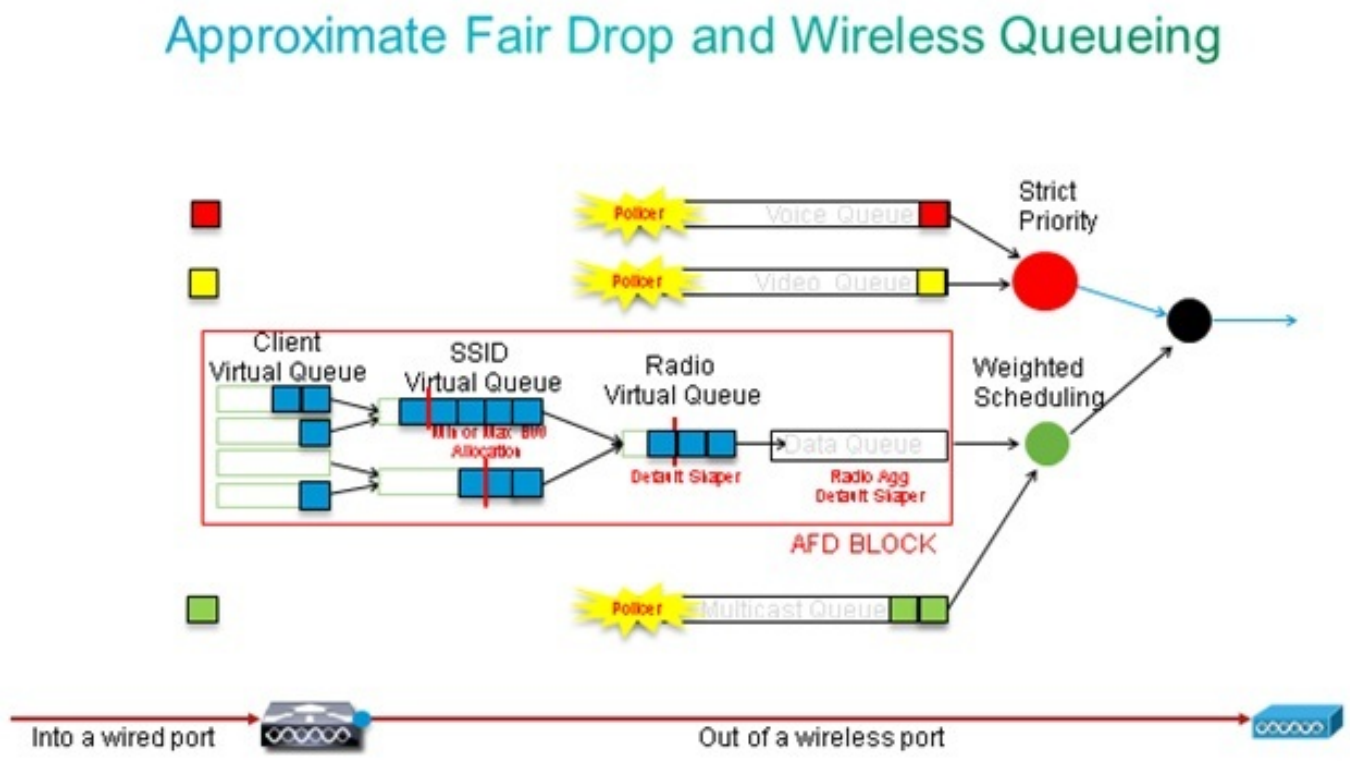
Étape 2 : Gestion de la bande passante et des priorités au niveau des ports

L'étape suivante consiste à déterminer une politique de QoS pour les ports qui vont et viennent vers les points d'accès. Cette étape s'applique principalement aux commutateurs Catalyst 3850. Si votre configuration est effectuée sur un contrôleur Cisco 5760, cette étape n'est pas obligatoire. Les ports Catalyst 3850 transportent le trafic voix et vidéo qui va aux clients et aux points d'accès sans fil ou qui en provient. La configuration QoS dans ce contexte correspond à deux exigences :

1. **Allouez la bande passante**. Vous pouvez décider de la quantité de bande passante allouée à chaque type de trafic. Cette allocation de bande passante peut également être effectuée au niveau du SSID. Définissez l'allocation de bande passante du port afin d'affiner la quantité de bande passante pouvant être reçue par chaque point d'accès qui dessert le SSID cible. Cette bande passante doit être définie pour tous les SSID sur l'AP cible. Cet exemple de configuration simplifiée suppose qu'il n'y a qu'un SSID et un AP, de sorte que l'allocation de bande passante de port pour la voix et la vidéo est identique à l'allocation de bande passante globale pour la voix et la vidéo au niveau SSID. Chaque type de trafic est affecté à 6 Mbits/s et est réglementé de sorte que cette bande passante allouée ne soit pas dépassée.

2. **Hiérarchiser le trafic**. Le port comporte quatre files d'attente. Les deux premières files d'attente sont hiérarchisées et réservées au trafic en temps réel, généralement voix et vidéo, respectivement. La quatrième file d'attente est réservée au trafic de multidiffusion non en temps réel et la troisième contient tout autre trafic. Avec la logique de file d'attente d'accès

convergé, le trafic de chaque client est affecté à une file d'attente virtuelle, où la QoS peut être configurée. Le résultat de la stratégie QoS du client est injecté dans la file d'attente virtuelle SSID, où QoS peut également être configuré. Comme plusieurs SSID peuvent exister sur une radio AP donnée, le résultat de chaque SSID présent sur une radio AP est injecté dans la file d'attente virtuelle de la radio AP, où le trafic est façonné en fonction de la capacité radio. Le trafic peut être retardé ou abandonné à l'une de ces étapes par le biais d'un mécanisme QoS appelé ASD (Approximate Fair Drop). Le résultat de cette stratégie est ensuite envoyé au port AP (appelé port sans fil), où la priorité est donnée aux deux premières files d'attente (jusqu'à une quantité configurable de bande passante), puis aux troisième et quatrième files d'attente comme décrit précédemment dans ce paragraphe.



Cet exemple de configuration place la voix dans la file d'attente de première priorité et la vidéo dans la file d'attente de deuxième priorité à l'aide de la commande **priority level**. Le reste du trafic est alloué au reste de la bande passante du port.

Notez que vous ne pouvez pas utiliser de cartes de classe qui ciblent le trafic en fonction des listes de contrôle d'accès (ACL). Les politiques appliquées au niveau du port peuvent cibler le trafic en fonction des cartes-classes, mais ces cartes-classes doivent cibler le trafic identifié par sa valeur QoS. Une fois que vous avez identifié le trafic en fonction des listes de contrôle d'accès et marqué correctement ce trafic au niveau du SSID client, il serait redondant d'effectuer une deuxième inspection approfondie de ce même trafic au niveau du port. Lorsque le trafic atteint le port qui va au point d'accès, il est déjà marqué correctement.

Dans cet exemple, vous réutilisez les class-maps générales créées pour la stratégie SSID et vous ciblez directement le trafic RTP voix et le trafic vidéo en temps réel :

```
Class-map allvoice
match dscp ef
Class-map videoandsignaling
Match dscp af41
match dscp cs3
```

Une fois que vous avez identifié le trafic d'intérêt, vous pouvez décider de la politique à appliquer. La stratégie par défaut (appelée parent_port) est appliquée automatiquement à chaque port lorsqu'un point d'accès est détecté. Vous ne devez pas modifier cette valeur par défaut, définie comme suit :

```
policy-map parent_port
class class-default
shape average 1000000000
service-policy port_child_policy
```

Comme la stratégie parent_port par défaut appelle la stratégie port_child_policy, une option est de modifier la stratégie port_child_policy. (Vous ne devez pas changer son nom). Cette stratégie enfant détermine le trafic à acheminer dans chaque file d'attente et la quantité de bande passante à allouer. La première file d'attente a la priorité la plus élevée, la deuxième file d'attente la priorité la plus élevée, etc. Ces deux files d'attente sont réservées au trafic en temps réel. La quatrième file d'attente est utilisée pour le trafic de multidiffusion non en temps réel. La troisième file d'attente contient tout autre trafic.

Dans cet exemple, vous décidez d'allouer le trafic vocal à la première file d'attente et le trafic vidéo à la deuxième file d'attente et d'allouer la bande passante à chaque file d'attente et à tout autre trafic :

```
Policy-map port_child_policy
Class allvoice
 Priority level 1
 police rate percent 10
 conform-action transmit
 exceed-action drop
class videoandsignaling
 priority level 2
 police rate percent 20
 conform-action transmit
 exceed-action drop
class non-client-nrt-class
 bandwidth remaining ratio 7
class class-default
 bandwidth remaining ratio 63
```

Dans cette stratégie, l'instruction de priorité associée aux classes 'voice' et 'videoandsigning' vous permet d'affecter ce trafic à la file d'attente de priorité appropriée. Notez cependant que les instructions de taux de police s'appliquent uniquement au trafic de multidiffusion et non de monodiffusion.

Vous n'avez pas besoin d'appliquer cette stratégie au niveau du port, car elle est appliquée automatiquement dès qu'un point d'accès est détecté.

Étape 3 : Bande passante et gestion des priorités au niveau SSID

L'étape suivante consiste à prendre en charge la stratégie QoS au niveau du SSID. Cette étape s'applique à la fois au commutateur Catalyst 3850 et au contrôleur 5760. Cette configuration suppose que le trafic voix et vidéo est identifié à l'aide de class-map et de listes d'accès et qu'il est étiqueté correctement. Cependant, un trafic entrant qui n'est pas ciblé par la liste d'accès peut ne pas afficher son marquage QoS. Dans ce cas, vous pouvez décider si ce trafic doit être marqué avec une valeur par défaut ou laissé sans étiquette. La même logique s'applique au trafic déjà marqué mais non ciblé par les class-maps. Utilisez l'instruction *de copie par défaut* dans une

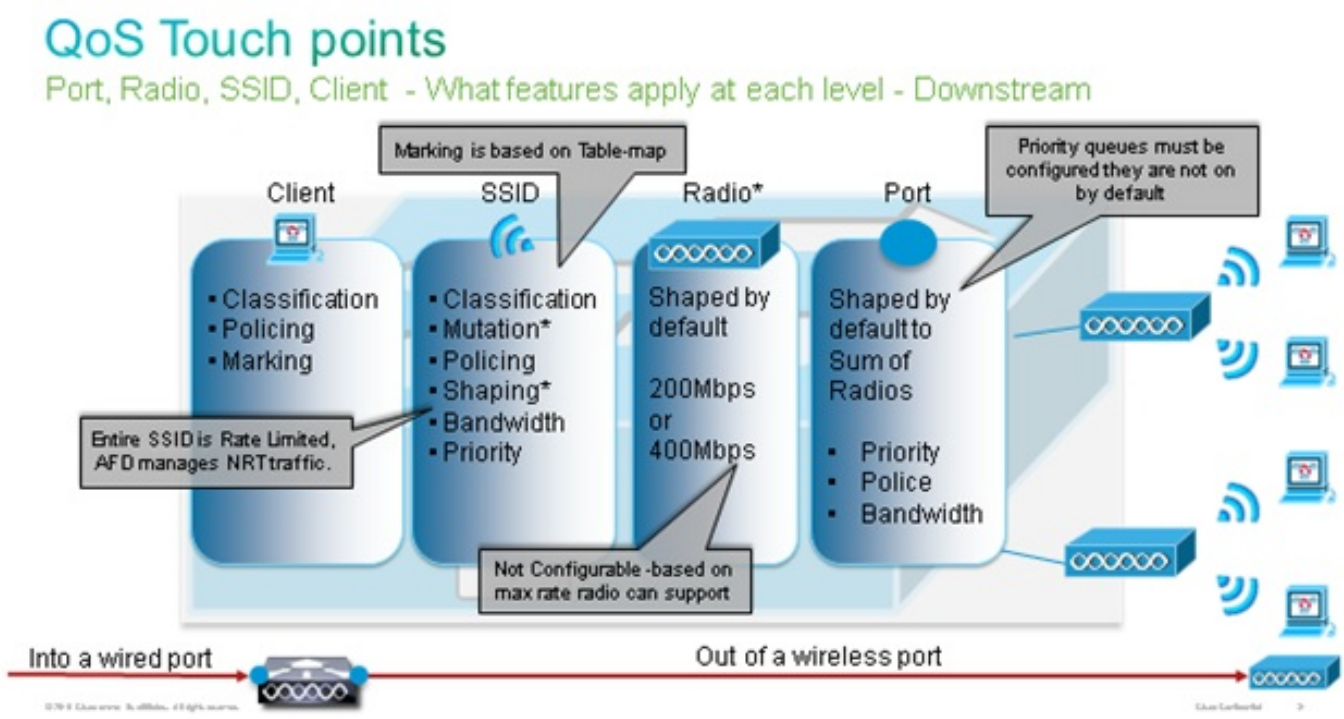
table-map afin de vous assurer que le trafic non marqué reste non marqué et que le trafic étiqueté conserve la balise et qu'il n'est pas noté.

Les tables-maps déterminent la valeur DSCP sortante, mais sont également utilisées pour créer une trame 802.11 afin de déterminer la valeur UP de la trame.

Dans cet exemple, le trafic entrant qui affiche le niveau de QoS voix (DSCP 46) conserve sa valeur DSCP, et la valeur est mappée au marquage 802.11 équivalent (UP 6). Le trafic entrant qui affiche le niveau de QoS vidéo (DSCP 34) conserve sa valeur DSCP et la valeur est mappée à la marque 802.11 équivalente (UP 5). De même, le trafic marqué DSCP 24 peut être une signalisation vocale ; la valeur DSCP doit être conservée et traduite en 802.11 UP 3 :

```
Table-map dscp2dscp
Default copy
Table-map dscp2up
Map from 46 to 6
Map from 24 to 3
Map from 34 to 5
Default copy
```

Le marquage peut également être effectué au niveau des ports câblés entrants. Cette figure montre les actions QoS pouvant être prises lors du transfert du trafic de la connexion filaire à la connexion sans fil :



Cet exemple de configuration se concentre sur l'aspect sans fil de la configuration QoS et marque le trafic au niveau du client sans fil. Une fois la partie de marquage terminée, vous devez allouer de la bande passante ; ici, 6 Mbits/s de bande passante sont alloués aux flux de trafic voix. (Bien qu'il s'agisse de l'allocation globale de bande passante pour la voix, chaque appel consommerait moins, par exemple 128 kbits/s.) Cette bande passante est allouée avec la commande **police** afin de réserver la bande passante et de supprimer le trafic en excès.

Le trafic vidéo est également alloué à 6 Mbits/s et réglementé. Cet exemple de configuration

suppose qu'il n'y a qu'un seul flux vidéo.

La partie signalisation du trafic vidéo et vocal doit également disposer d'une bande passante. Il existe deux stratégies possibles.

- Utilisez la commande **shape medium**, qui permet au trafic en excès d'être mis en mémoire tampon et envoyé ultérieurement. Cette logique n'est pas efficace pour le flux voix ou vidéo lui-même, car ces flux nécessitent un délai et une gigue constants ; cependant, il peut être efficace pour la signalisation, car la signalisation peut être légèrement retardée sans effet sur la qualité des appels. Dans la solution d'accès convergé, les commandes de forme n'acceptent pas ce qu'on appelle des configurations de compartiments, qui déterminent la quantité de trafic supérieure à la bande passante allouée pouvant être mise en mémoire tampon. Par conséquent, une deuxième commande, **queue-buffers ratio 0**, doit être ajoutée afin de spécifier que la taille du compartiment est 0. Si vous incluez la signalisation dans le reste du trafic et que vous utilisez les commandes shape, le trafic de signalisation peut être abandonné en cas de congestion élevée. Cela peut à son tour entraîner la suppression de l'appel, car l'une ou l'autre extrémité détermine que la communication n'a plus lieu.
- Pour éviter le risque d'abandon d'appels, vous pouvez inclure la signalisation dans l'une des files d'attente prioritaires. Cet exemple de configuration a précédemment défini les files d'attente prioritaires comme voix et vidéo et ajoute maintenant la signalisation à la file d'attente vidéo.

La stratégie utilise le contrôle d'admission des appels (CAC) pour le flux vocal. CAC cible le trafic sans fil et correspond à un UP spécifique (dans cet exemple de configuration, UP 6 et 7). CAC détermine ensuite la quantité maximale de bande passante que ce trafic doit utiliser. Dans une configuration où vous contrôlez le trafic vocal, CAC doit se voir attribuer un sous-ensemble de la quantité totale de bande passante allouée à la voix. Par exemple, si la voix est contrôlée à 6 Mbits/s, CAC ne peut pas dépasser 6 Mbits/s. CAC est configuré dans une carte-politique (appelée stratégie enfant) qui est intégrée dans la carte-politique principale en aval (appelée stratégie parent). CAC est introduit avec la commande **admettre cac wmm-tspec**, suivie des UP cibles et de la bande passante allouée au trafic ciblé.

Chaque appel ne consomme pas toute la bande passante allouée à la voix. Par exemple, chaque appel peut consommer 64 kbits/s dans chaque sens, ce qui donne une consommation de bande passante bidirectionnelle effective de 128 kbits/s. L'instruction de débit détermine la consommation de bande passante de chaque appel, tandis que l'instruction de police détermine la bande passante globale allouée au trafic vocal. Si tous les appels qui se produisent au sein de la cellule utilisent près de la bande passante maximale autorisée, tout nouvel appel initié à partir de la cellule et qui entraîne le dépassement de la bande passante maximale autorisée pour la voix sera refusé. Vous pouvez affiner ce processus en configurant CAC au niveau de la bande, comme expliqué à l'étape 4 : Limitation des appels avec CAC.

Par conséquent, vous devez configurer une stratégie enfant qui contient les instructions CAC et qui est intégrée dans la stratégie principale en aval. CAC n'est pas configuré dans la carte de stratégie en amont. CAC s'applique aux appels vocaux initiés à partir de la cellule, mais, comme il s'agit d'une réponse à ces appels, CAC est défini uniquement dans la carte de stratégie en aval. La carte-politique en amont sera différente. Vous ne pouvez pas utiliser les class-maps créés précédemment car ces class-maps ciblent le trafic basé sur une liste de contrôle d'accès. Le trafic injecté dans la stratégie SSID est déjà passé par la stratégie client, vous ne devez donc pas effectuer une inspection approfondie des paquets une deuxième fois. Au lieu de cela, ciblez le trafic avec un marquage QoS qui résulte de la stratégie du client.

Si vous décidez de ne pas laisser la signalisation dans la classe par défaut, vous devrez également établir une priorité pour la signalisation.

Dans cet exemple, la signalisation et la vidéo sont dans la même classe et une bande passante plus importante est allouée à cette classe afin de prendre en charge la partie signalisation ; 6 Mbits/s sont alloués au trafic vidéo (un flux point à point de la caméra Tandberg) et 1 Mbits/s à la signalisation pour tous les appels vocaux et le flux vidéo :

```
Class-map allvoice
match dscp ef
Class-map videoandsignaling
Match dscp af41
Match dscp cs3
```

La politique enfant en aval est la suivante :

```
Policy-map SSIDout_child_policy
class allvoice
priority level 1
police 6000000
admit cac wmm-tspec
rate 128
wlan-up 6 7
class videoandsignaling
priority level 2
police 1000000
```

La stratégie parent en aval est la suivante :

```
policy-map SSIDout
class class-default
set dscp dscp table dscp2dscp
set wlan user-priority dscp table dscp2up
shape average 30000000
queue-buffers ratio 0
service-policy SSIDout_child_policy
```

Le trafic en amont est le trafic qui provient de clients sans fil et qui est envoyé au WCM avant que le trafic ne soit envoyé à partir d'un port câblé ou à un autre SSID. Dans les deux cas, vous pouvez configurer des cartes-politiques qui définissent la bande passante allouée à chaque type de trafic. La stratégie sera probablement différente selon que le trafic est envoyé depuis un port câblé ou vers un autre SSID.

En amont, votre principale préoccupation est de décider de la priorité, pas de la bande passante. En d'autres termes, votre carte-politique en amont n'alloue pas de bande passante à chaque type de trafic. Comme le trafic se trouve déjà au point d'accès et a déjà franchi le cou de bouteille formé par l'espace sans fil bidirectionnel non simultané, votre objectif est d'amener ce trafic à la fonction de contrôleur du commutateur Catalyst 3850 ou du WLC Cisco 5760 pour un traitement ultérieur. Lorsque le trafic est collecté au niveau du point d'accès, vous pouvez décider si vous devez faire confiance au marquage QoS existant potentiel afin de hiérarchiser les flux de trafic envoyés au contrôleur. Dans cet exemple, les valeurs DSCP existantes peuvent être approuvées :

```
Policy-map SSIDin
Class class-default
set dscp dscp table dscp2dscp
```

Une fois vos stratégies créées, appliquez-les au WLAN. Dans cet exemple, tout périphérique qui

se connecte au WLAN doit prendre en charge WMM, donc WMM est requis.

```
wlan test1
wmm require
service-policy client input taggingPolicy
service-policy input SSIDin
service-policy output SSIDout
```

Étape 4 : Limitation des appels avec CAC

La dernière étape consiste à adapter le CAC à votre situation particulière. Dans la configuration CAC expliquée à l'étape 3 : Bande passante et gestion des priorités au niveau SSID, le point d'accès abandonne tout paquet vocal qui dépasse la bande passante allouée.

Afin d'éviter la bande passante maximale., vous devez également configurer le WCM afin de reconnaître les appels qui sont passés et les appels qui entraîneront un dépassement de la bande passante. Certains téléphones prennent en charge la spécification de trafic WMM (TSPEC) et informent l'infrastructure sans fil de la bande passante que l'appel projeté devrait consommer. Le WCM peut alors refuser l'appel avant qu'il ne soit placé.

Certains téléphones SIP ne prennent pas en charge TSPEC, mais le WCM et le point d'accès peuvent être configurés pour reconnaître les paquets d'initiation d'appel envoyés aux ports SIP et peuvent utiliser ces informations afin d'établir qu'un appel SIP est sur le point d'être passé. Comme le téléphone SIP ne spécifie pas la bande passante à utiliser par l'appel, l'administrateur doit déterminer la bande passante attendue, en fonction du codec, du temps d'échantillonnage, etc.

CAC calcule la bande passante consommée à chaque niveau de point d'accès. CAC peut être configuré pour utiliser uniquement la consommation de bande passante du client dans ses calculs (CAC statique) ou pour tenir compte des points d'accès et des périphériques voisins sur le même canal (CAC basé sur la charge). Cisco recommande d'utiliser un CAC statique pour les téléphones SIP et un CAC basé sur la charge pour les téléphones TSPEC.

Enfin, notez que CAC est activé par bande.

Dans cet exemple, les téléphones utilisent SIP plutôt que TSPEC pour leur lancement de session, chaque appel utilise 64 kbits/s pour chaque direction de flux, le CAC basé sur la charge est désactivé lorsque le CAC statique est activé et 75 % de la bande passante maximale de chaque point d'accès est alloué au trafic vocal :

```
ap dot11 5ghz shutdown
ap dot11 5ghz cac voice acm
no ap dot11 5ghz cac voice load-based
ap dot11 5ghz cac voice max-bandwidth 75
ap dot11 5ghz cac voice sip bandwidth 64
no ap dot11 5ghz shutdown
```

Vous pouvez répéter la même configuration pour la bande 2,4 GHz :

```
ap dot11 24ghz shutdown
ap dot11 24ghz cac voice acm
no ap dot11 24ghz cac voice load-based
ap dot11 24ghz cac voice max-bandwidth 75
```

```
ap dot11 24ghz cac voice sip bandwidth 64
no ap dot11 24ghz shutdown
```

Une fois CAC appliqué à chaque bande, vous devez également appliquer SIP CAC au niveau WLAN. Ce processus permet au point d'accès d'examiner les informations de couche 4 (L4) du trafic client sans fil afin d'identifier les requêtes envoyées à UDP 5060 qui indiquent des tentatives d'appel SIP. TSPEC fonctionne au niveau 802.11 et est détecté nativement par les points d'accès. Les téléphones SIP n'utilisent pas TSPEC, de sorte que le point d'accès doit effectuer une inspection plus approfondie des paquets afin d'identifier le trafic SIP. Comme vous ne voulez pas que le point d'accès effectue cette inspection sur tous les SSID, vous devez déterminer quels SSID attendent du trafic SIP. Vous pouvez ensuite activer la surveillance des appels sur ces SSID afin de rechercher des appels vocaux. Vous pouvez également déterminer l'action à effectuer si un appel SIP doit être rejeté - dissocier le client SIP ou envoyer un message SIP Occupé.

Dans cet exemple, la surveillance des appels est activée et un message de ligne occupée est envoyé si l'appel SIP doit être rejeté. Avec l'ajout de la stratégie QoS de l'étape 3 : Bande passante et gestion des priorités au niveau SSID, il s'agit de la configuration SSID pour l'exemple de WLAN :

```
wlan test1
wmm require
service-policy client input taggingPolicy
service-policy input SSIDin
service-policy output SSIDout
call-snoop
sip-cac send-486busy
```

Vérification

Utilisez ces commandes afin de confirmer que votre configuration QoS fonctionne correctement.

> **Remarques :**
>
> Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.
>
> L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

show class-map

Cette commande affiche les class-maps configurées sur la plate-forme :

```
3850#show class-map
 Class Map match-any H323realtimeaudio (id 6)
  Match access-group name H323Audiostream
Class Map match-any H323realtimevideo (id 7)
  Match access-group name H323Videostream
Class Map match-any allvideo (id 10)
  Match   dscp af41 (34)
```

```
Class Map match-any jabberaudiosignaling (id 11)
  Match access-group name JabberSIGNALING
Class Map match-any allvoice (id 12)
  Match   dscp ef (46)
Class Map match-any RTPaudio (id 19)
  Match access-group name JabberVOIP
  Match access-group name H323Audiostream
Class Map match-any class-default (id 0)
  Match any
Class Map match-any jabberRTPaudio (id 14)
  Match access-group name JabberVOIP
Class Map match-any non-client-nrt-class (id 1)
  Match non-client-nrt
Class Map match-any H323audiosignaling (id 17)
  Match access-group name H323AudioSignaling
Class Map match-any H323videosignaling (id 18)
  Match access-group name H323VideoSignaling
Class Map match-any signaling (id 20)
  Match access-group name JabberSIGNALING
  Match access-group name H323VideoSignaling
  Match access-group name H323AudioSignaling
```

show policy-map

Cette commande affiche les policy-maps configurés sur la plate-forme :

```
3850 #show policy-map
show policy-map
 Policy Map port_child_policy
   Class non-client-nrt-class
     bandwidth remaining ratio 7
   Class allvoice
     priority level 1
    police rate percent 10
      conform-action transmit
      exceed-action drop
   Class allvideo
     priority level 2
    police rate percent 20
      conform-action transmit
      exceed-action drop
   Class class-default
     bandwidth remaining ratio 63
 Policy Map SSIDin
   Class class-default
     set dscp dscp table dscp2dscp
 Policy Map SSIDout_child_policy
   Class allvoice
     priority level 1
    police cir 6000000 bc 187500
      conform-action transmit
      exceed-action drop
     admit cac wmm-tspec
       rate 6000 (kbps)
       wlan-up 6
   Class allvideo
     priority level 2
    police cir 6000000 bc 187500
      conform-action transmit
      exceed-action drop
     admit cac wmm-tspec
```

```
       rate 6000 (kbps)
       wlan-up 4 5
 Policy Map taggingPolicy
   Class RTPaudio
     set dscp ef
   Class H323realtimevideo
     set dscp af41
   Class signaling
     set dscp cs3
 Policy Map SSIDout
   Class class-default
     set dscp dscp table dscp2dscp
     set wlan user-priority dscp table dscp2up
     shape average 30000000 (bits/sec)
     queue-buffers ratio 0
     service-policy SSIDout_child_policy
 Policy Map parent_port
   Class class-default
     shape average 1000000000 (bits/sec) op
```

show wlan

Cette commande affiche la configuration WLAN et les paramètres de stratégie de service :

```
3850# show wlan name test1 | include Policy
AAA Policy Override                             : Disabled
QoS Service Policy - Input
 Policy Name                                    : SSIDin
 Policy State                                   : Validated
QoS Service Policy - Output
 Policy Name                                    : SSIDout
 Policy State                                   : Validated
QoS Client Service Policy
 Input  Policy Name                             : taggingPolicy
 Output Policy Name                             : taggingPolicy
Radio Policy                                    : All
```

show policy-map interface

Cette commande affiche le policy-map installé pour une interface spécifique :

```
3850#show policy-map interface wireless ssid name test1

Remote SSID test1 iifid: 0x01023F4000000033.0x00F2E98000000003.0x00C2EB000000001F
 Service-policy input: SSIDin
   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp dscp table dscp2dscp

Remote SSID test1 iifid: 0x01023F4000000033.0x00C8384000000004.0x00D0D08000000021

 Service-policy input: SSIDin

   Class-map: class-default (match-any)
     Match: any
```

```
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
      dscp dscp table dscp2dscp

SSID test1 iifid: 0x01023F4000000033.0x00F2E98000000003.0x00EC3E800000001E

 Service-policy input: SSIDin

   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp dscp table dscp2dscp

 Service-policy output: SSIDout

   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp dscp table dscp2dscp
       wlan user-priority dscp table dscp2up
     shape (average) cir 30000000, bc 120000, be 120000
     target shape rate 30000000
     queue-buffers ratio 0

     Service-policy : SSIDout_child_policy

       Class-map: allvoice (match-any)
         Match:  dscp ef (46)
           0 packets, 0 bytes
           30 second rate 0 bps
         Priority: Strict,

         Priority Level: 1
         police:
             cir 6000000 bps, bc 187500 bytes
           conformed 0 bytes; actions:
             transmit
           exceeded 0 bytes; actions:
             drop
           conformed 0000 bps, exceed 0000 bps
         cac wmm-tspec rate 6000 kbps

       Class-map: allvideo (match-any)
         Match:  dscp af41 (34)
           0 packets, 0 bytes
           30 second rate 0 bps
         Priority: Strict,

         Priority Level: 2
         police:
             cir 6000000 bps, bc 187500 bytes
           conformed 0 bytes; actions:
             transmit
           exceeded 0 bytes; actions:
             drop
           conformed 0000 bps, exceed 0000 bps
         cac wmm-tspec rate 6000 kbps

       Class-map: class-default (match-any)
```

```
        Match: any
          0 packets, 0 bytes
          30 second rate 0 bps

SSID test1 iifid: 0x01023F4000000033.0x00C8384000000004.0x00DB568000000020

 Service-policy input: SSIDin

   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp dscp table dscp2dscp

 Service-policy output: SSIDout

   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp dscp table dscp2dscp
       wlan user-priority dscp table dscp2up
     shape (average) cir 30000000, bc 120000, be 120000
     target shape rate 30000000
     queue-buffers ratio 0

     Service-policy : SSIDout_child_policy

       Class-map: allvoice (match-any)
         Match:  dscp ef (46)
           0 packets, 0 bytes
           30 second rate 0 bps
         Priority: Strict,

         Priority Level: 1
         police:
             cir 6000000 bps, bc 187500 bytes
           conformed 0 bytes; actions:
             transmit
           exceeded 0 bytes; actions:
             drop
           conformed 0000 bps, exceed 0000 bps
         cac wmm-tspec rate 6000 kbps

       Class-map: allvideo (match-any)
         Match:  dscp af41 (34)
           0 packets, 0 bytes
           30 second rate 0 bps
         Priority: Strict,

         Priority Level: 2
         police:
             cir 6000000 bps, bc 187500 bytes
           conformed 0 bytes; actions:
             transmit
           exceeded 0 bytes; actions:
             drop
           conformed 0000 bps, exceed 0000 bps
         cac wmm-tspec rate 6000 kbps

       Class-map: class-default (match-any)
         Match: any
```

```
          0 packets, 0 bytes
          30 second rate 0 bps

3850#show policy-map interface wireless client
Client 8853.2EDC.68EC iifid:
0x01023F4000000033.0x00F2E98000000003.0x00EC3E800000001E.0x00E0D04000000022

 Service-policy input: taggingPolicy

   Class-map: RTPaudio (match-any)
     Match: access-group name JabberVOIP
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: access-group name H323Audiostream
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp ef

   Class-map: H323realtimevideo (match-any)
     Match: access-group name H323Videostream
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp af41

   Class-map: signaling (match-any)
     Match: access-group name JabberSIGNALING
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: access-group name H323VideoSignaling
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: access-group name H323AudioSignaling
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp cs3
   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps

 Service-policy output: taggingPolicy

   Class-map: RTPaudio (match-any)
     Match: access-group name JabberVOIP
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: access-group name H323Audiostream
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp ef

   Class-map: H323realtimevideo (match-any)
     Match: access-group name H323Videostream
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp af41

   Class-map: signaling (match-any)
     Match: access-group name JabberSIGNALING
```

```
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: access-group name H323VideoSignaling
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: access-group name H323AudioSignaling
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
      dscp cs3
  Class-map: class-default (match-any)
    Match: any
      0 packets, 0 bytes
      30 second rate 0 bps
```

show platform qos policies

Cette commande affiche les stratégies QoS installées pour les ports, les radios AP, les SSID et les clients. Notez que vous pouvez vérifier, mais ne pouvez pas modifier, les stratégies radio :

```
3850#show platform qos policies PORT
Loc Interface          IIF-ID             Dir Policy           State
--- ------------------ ------------------ --- ---------------- ---------------
L:0 Gi1/0/20           0x01023f4000000033 OUT defportangn      INSTALLED IN HW
L:0 Gi1/0/20           0x01023f4000000033 OUT port_child_policyINSTALLED IN HW

3850#show platform qos policies RADIO
Loc Interface          IIF-ID             Dir Policy           State
--- ------------------ ------------------ --- ---------------------------------
L:0 R56356842871193604 0x00c8384000000004 OUT def-11an         INSTALLED IN HW
L:0 R68373680329064451 0x00f2e98000000003 OUT def-11gn         INSTALLED IN HW
3850#show platform qos policies SSID
Loc Interface          IIF-ID             Dir Policy           State
--- ------------------ ------------------ --- ------------------------------
L:0 S70706569125298203 0x00fb33400000001b OUT SSIDout_child_policyINSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 OUT SSIDout_child_policyINSTALLED IN HW
L:0 S70706569125298203 0x00fb33400000001b OUT SSIDout          INSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 OUT SSIDout          INSTALLED IN HW
L:0 S70706569125298203 0x00fb33400000001b IN  SSIDin           INSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 IN  SSIDin           INSTALLED IN HW

3850#show platform qos policies CLIENT
Loc Interface          IIF-ID             Dir Policy           State
--- ------------------ ------------------ --- ---------------- ---------------
L:0 8853.2edc.68ec     0x00e0d04000000022 IN  taggingPolicy    NOT INSTALLED IN HW
L:0 8853.2edc.68ec     0x00e0d04000000022 OUT taggingPolicy    NOT INSTALLED IN HW
```

show wireless client mac-address <mac> service-policy

Cette commande affiche les policy-maps appliqués au niveau du client :

```
3850#show wireless client mac-address 8853.2EDC.68EC service-policy output
Wireless Client QoS Service Policy
Policy Name  : taggingPolicy
Policy State : Installed
3850#sh wireless client mac-address 8853.2EDC.68EC service-policy in
3850#sh wireless client mac-address 8853.2EDC.68EC service-policy input
Wireless Client QoS Service Policy
```

```
Policy Name  : taggingPolicy
Policy State : Installed
```

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.