QoS sur les contrôleurs convergés d'Access et l'exemple léger de configuration aps

Contenu

Introduction

Ce document décrit comment configurer QoS dans un réseau d'accès convergé par Cisco avec le Point d'accès léger (recouvrements) et avec le commutateur de Cisco Catalyst 3850 ou le contrôleur LAN Sans fil de Cisco 5760 (WLC).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance de base de la façon configurer des recouvrements et le Cisco ont convergé des contrôleurs d'accès
- La connaissance de la façon configurer le routage de base et le QoS dans un réseau câblé

Composants utilisés

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

- Commutateur de Cisco Catalyst 3850 qui exécute le Cisco IOS? Version logicielle XE 3.2.2(SE)
- Contrôleur LAN de radio de Cisco 5760 qui exécute la version de Logiciel Cisco IOS XE version 2 3.2.2(SE)
- Point d'accès léger de gamme Cisco 3600

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

QoS se réfère à la capacité du réseau de fournir un meilleur ou spécial service à un ensemble d'utilisateurs ou des applications au détriment d'autres utilisateurs ou applications.

Avec QoS, la bande passante peut être gérée plus efficacement à travers des réseaux locaux, qui inclut les réseaux locaux Sans fil (WLAN) et les WAN. QoS fournit au service réseau amélioré et digne de confiance ces services :

- Bande passante dédiée de supports pour les utilisateurs essentiels et les applications.
- Contrôle le jitter et la latence qui est exigée par le trafic en temps réel.
- Gère et réduit l'encombrement de réseau.
- Forme le trafic réseau afin de lisser l'écoulement du trafic.
- Fixe des priorités du trafic réseau.

Dans le passé, des WLAN ont été principalement utilisés pour transporter la faible bande passante, le trafic d'application de données. Avec l'extension des WLAN dans la verticale (telle que le détail, les finances, et la formation) et les environnements d'entreprise, des WLAN sont maintenant utilisés pour transporter des applications de données de bande passante élevée en même temps que sensible au temps, des applications multimédias. Cette condition requise a mené à la nécessité pour QoS Sans fil.

Le groupe de travail d'IEEE 802.11e au sein du comité de normalisation d'IEEE 802.11 s'est terminé la définition standard, et le Wi-Fi Alliance a créé la certification du Wi-Fi Multimedia (WMM), mais l'adoption de la norme 802.11e est encore limitée. La plupart des périphériques WMM-sont certifiés, parce que la certification WMM est nécessaire pour la certification 802.11n et

802.11ac. Beaucoup de périphériques sans fil n'assignent pas différents niveaux de QoS aux paquets envoyés à la couche liaison de données, ainsi ces périphériques envoient la majeure partie de leur trafic sans le marquage de QoS et aucune hiérarchisation relative. Cependant, la plupart des Téléphones IP de Voix sur réseau local sans fil (VoWLAN) de 802.11 marquent et donnent la priorité à leur trafic vocal. Ce document se concentre sur la configuration QoS pour des Téléphones IP VoWLAN et sur les périphériques vidéo-capables de Wi-Fi qui marquent leur trafic vocal.

> Remarque: La configuration QoS pour les périphériques qui n'exécutent pas le marquage interne est hors de portée de ce document.

L'amendement 802.11e définit huit niveaux de priorité utilisateur (), groupés deux par deux dans quatre niveaux de QoS (catégories d'accès) :

- Platine/Voix (VERS LE HAUT de 7 et 6) - assure une haute qualité de service pour la Voix au-dessus de la radio.
- Or/vidéo (VERS LE HAUT de 5 et 4) - applications vidéo de haute qualité de supports.
- Argent/bande passante normale supports de meilleur effort (VERS LE HAUT de 3 et de 0) - pour des clients. C'est la valeur par défaut.
- Bronze/fond (VERS LE HAUT de 2 et 1) - fournit la plus basse bande passante pour des services d'invité.

Le platine est utilisé généralement pour les clients et l'or VoIP pour les clients visuels. Ce document fournit un exemple de configuration qui montre comment configurer QoS sur des contrôleurs et communiquer avec un réseau câblé qui est configuré avec QoS pour le VoWLAN et les clients visuels.

Améliorations du Marquage des paquets QoS L3

Cisco a convergé le marquage de Differentiated Services Code Point IP de la couche 3 de support de contrôleurs d'accès (L3) (DSCP) des paquets envoyés par WLCs et recouvrements. Cette caractéristique améliore comment les Points d'accès (aps) emploient ces informations L3 afin de s'assurer que les paquets reçoivent le correct au-dessus du - aèrent la hiérarchisation d'AP au client sans fil.

En architecture convergée de l'accès WLAN qui utilise des Commutateurs du Catalyst 3850 comme contrôleurs sans-fil, les aps se connectent directement au commutateur. En architecture convergée de l'accès WLAN qui utilise 5760 contrôleurs, des données WLAN sont percées un tunnel entre AP et le WLC par l'intermédiaire du contrôle et le ravitaillement du protocole des points d'accès sans fil (CAPWAP). Afin de mettre à jour la classification QoS d'origine à travers ce tunnel, les configurations de QoS du paquet de données encapsulé doivent être convenablement tracées à la couche 2 (L2) (802.1p) et aux champs L3 (IP DSCP) du paquet externe de tunnel.

Quand vous configurez QoS pour le VoWLAN et le vidéo, vous pouvez configurer une particularité de stratégie QoS pour des clients sans fil et une particularité de stratégie à un WLAN, ou chacun des deux. Vous pouvez également compléter l'installation avec une particularité de configuration au port qui joint AP, particulièrement avec des Commutateurs du Catalyst 3850. Cet exemple de configuration se concentre sur la configuration QoS pour le client sans fil, le WLAN, et le port à AP. Les buts principaux d'une configuration QoS pour le VoWLAN et les applications vidéo sont :

- Identifiez le trafic de Voix et de vidéo (Classification du trafic et marquage), chacun des deux en amont et en aval.
- Marquez le trafic de Voix et de vidéo avec un niveau de priorité de Voix : 802.11e VERS LE HAUT de 6, 802.1p 5, DSCP 46 pour la Voix.802.11e LÈVENT 5, le DSCP 34 pour le vidéo.
- Allouez la bande passante pour le trafic vocal, la signalisation de Voix, et le trafic visuel.

Configurez le réseau sans fil pour QoS avec MQC

Avant que vous configuriez QoS, vous devez configurer la fonction du module de contrôleur sans-fil (WCM) du commutateur ou de Cisco du Catalyst 3850 5760 WLC pour le fonctionnement de base et enregistrer les recouvrements au WCM. Ce document suppose que le WCM est configuré pour le fonctionnement de base et que les recouvrements sont enregistrés au WCM.

Les solutions d'accès convergées utilisent l'interface de ligne de commande modulaire de QoS (MQC) (CLI). Référez-vous au guide de configuration QoS, la release 3SE (Commutateurs de Cisco IOS XE de Catalyst 3850) pour des informations supplémentaires sur l'utilisation de MQC en configuration QoS sur le commutateur du Catalyst 3850.

La configuration de QoS avec MQC sur les contrôleurs convergés d'accès se fonde sur quatre éléments :

- **Des class-map** sont utilisés afin d'identifier le trafic d'intérêt. Les class-map peuvent employer de diverses techniques (telles que le marquage, les Listes d'accès, ou les VLAN existants de QoS) afin d'identifier le trafic d'intérêt.
- **Des policy-map** sont utilisés afin de déterminer quelles configurations de QoS devraient être appliquées au trafic d'intérêt. Les policy-map appellent des class-map et appliquent de diverses configurations de QoS (telles que le marquage, les niveaux de priorité, l'allocation spécifiques de bande passante, et ainsi de suite) à chaque classe.
- **des Service-stratégies** sont utilisées afin d'appliquer des policy-map aux points stratégiques de votre réseau. Dans les solutions d'accès convergées, des service-stratégies peuvent être appliquées aux utilisateurs, aux identifiants d'ensemble de services (SSID), aux radios AP, et aux ports. Le port, le SSID, et les stratégies de client peuvent être configurés par l'utilisateur. Des stratégies par radio sont contrôlées par la module de commande Sans fil. Des stratégies QoS Sans fil pour le port, le SSID, le client, et la radio sont appliquées dans la direction en aval quand le trafic circule du commutateur ou du contrôleur aux clients sans fil.
- **Des table-map** sont utilisés afin d'examiner le marquage entrant de QoS et décider les marquages sortants de QoS. Des table-map sont placés dans les policy-map appliqués au SSID. Des table-map peuvent être utilisés afin de garder (copie) ou changer le marquage. Des table-map peuvent également être utilisés afin de créer un mappage entre le marquage de câble et Sans fil. Le marquage de câble utilise le DSCP (L3 QoS) ou le 802.1p (L2 QoS). Le marquage Sans fil utilise la priorité utilisateur (). Les table-map sont utilisés généralement pour déterminer quel repérage de DSCP devrait être utilisé pour chacun d'intérêt et ce qui devrait être utilisé pour chaque valeur DSCP d'intérêt. Les table-map sont fondamentaux à l'accès convergé QoS parce qu'il n'y a aucune traduction directe entre le DSCP et les valeurs HAUTES.

Cependant, le DSCP aux table-map HAUTS permettent également l'instruction de *copie*. Dans ce cas, les solutions d'accès convergées emploient l'architecture Cisco pour la Voix, le vidéo, et la table de mappage intégrée des données (AVVID) afin de déterminer le DSCP à HAUT ou jusqu'à la traduction de DSCP :

Index d'étiquette	Zone de tri	Valeur entrante	DSCP externe	Cos	VERS LE HAUT DE
0	N.A.	Non vérifié	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	VERS LE HAUT DE	0	0	0	0
74	VERS LE HAUT DE	1	8	1	1
75	VERS LE HAUT DE	2	16	1	2
76	VERS LE HAUT DE	3	24	2	3
77	VERS LE HAUT DE	4	34	3	4
78	VERS LE HAUT DE	5	34	4	5
79	VERS LE HAUT DE	6	46	5	6
80	VERS LE HAUT DE	7	46	7	7

Stratégies codées en dur par par défaut

Les contrôleurs convergés d'accès embarquent les profils codés en dur de stratégie QoS qui peuvent être appliqués aux WLAN. Ces profils appliquent les stratégies en métal (platine, or, et ainsi de suite) qui sont bien connues aux administrateurs des contrôleurs des réseaux sans fil unifié Cisco (CUWN). Si votre objectif n'est pas de créer les stratégies qui assignent la bande passante spécifique au trafic vocal mais de s'assurer simplement que le trafic vocal reçoit le marquage approprié de QoS, vous pouvez utiliser les stratégies codées en dur. Les stratégies codées en dur peuvent être appliquées au WLAN et peuvent être différentes dans l'en amont et les directions en aval.

Remarques :

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

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Platine

La stratégie codée en dur pour la Voix s'appelle le platine. Le nom ne peut pas être changé.

C'est la stratégie en aval pour le niveau de QoS de 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
```

C'est la stratégie en amont pour le niveau de QoS de platine :

```
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 stratégie codée en dur pour le vidéo s'appelle l'or. Le nom ne peut pas être changé.

C'est la stratégie en aval pour le niveau de QoS d'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
```

C'est la stratégie en amont pour le niveau de QoS d'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 stratégie codée en dur pour le meilleur effort s'appelle argentée. Le nom ne peut pas être changé.

C'est la stratégie en aval pour le niveau argenté de QoS :

```
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
```

C'est la stratégie en amont pour le niveau argenté de QoS :

```
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 stratégie codée en dur pour le trafic de fond s'appelle en bronze. Le nom ne peut pas être changé.

C'est la stratégie en aval pour le niveau en bronze de QoS :

```
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
```

C'est la stratégie en amont pour le niveau en bronze de QoS :

```
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 quel table-map meilleur apparie le trafic de cible pour un SSID donné, vous pouvez s'appliquer la stratégie assortie à votre WLAN. Dans cet exemple, une stratégie est appliquée dans la direction en aval (sortie, d'AP au client sans fil), et une stratégie est appliquée sur la direction en amont (entrée, du client sans fil, par AP, 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
```

Configurez manuellement

Les stratégies codées en dur appliquent le marquage par défaut de QoS 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 vouloir employer une combinaison des stratégies afin d'identifier et marquer le trafic de Voix et de vidéo convenablement, pour placer l'allocation de bande passante dans les directions en aval et en amont, et pour utiliser le contrôle d'admission d'appel afin de limiter le nombre d'appels initiés de la cellule Sans fil.

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

Étape 1 : Identification et marquage du trafic vocal

La première étape est d'identifier le trafic de Voix et de vidéo. Le trafic vocal peut être classifié dans deux catégories :

- Flux voix, qui assume la partie sonore de la transmission.
- Exprimez la signalisation, qui diffuse les informations statistiques permutées entre les points finaux de Voix.

Le flux voix utilise généralement des destinations port de Protocole RTP (Real-Time Transport Protocol) et de Protocole UDP (User Datagram Protocol) de l'ordre de 16384 - 32767. C'est la plage ; les ports réels sont habituellement plus étroits et dépendent de l'implémentation.

Il y a plusieurs protocoles de signalisation de Voix. Ce Jabber d'utilisations d'exemple de configuration. Le Jabber utilise ces ports TCP pour la connexion et le répertoire :

- TCP 80 (HTTP)
- 143 (Internet Message Access Protocol [IMAP])
- 443 (HTTPS)
- 993 (IMAP) pour des services tels que le Cisco Unified MeetingPlace ou le Cisco WebEx pour les téléconférences et le Cisco Unity ou le Cisco Unity Connection pour des caractéristiques de messagerie vocale
- TCP 389/636 (serveur de protocole LDAP [LDAP] pour des recherches de contact)
- FTP (1080)
- TFTP (UDP 69) pour le transfert de fichiers (tel que des fichiers de configuration) des pairs ou

du serveur

Ces services peuvent ne pas avoir besoin d'une hiérarchisation spécifique.

Le Jabber utilise le Protocole SIP (Session Initiation Protocol) (UDP/TCP 5060 et 5061) pour la signalisation de Voix.

Le trafic visuel utilise les différents ports et les protocoles qui dépendent de votre implémentation. Cet exemple de configuration utilise une caméra de Tandberg PrecisionHD 720p pour des conférences vidéo. La caméra de Tandberg PrecisionHD 720p peut utiliser plusieurs codecs ; la bande passante consommée dépend des codecs choisis :

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

L'implémentation de Tandberg de utilise H.323 typique l'UDP 970 pour le streaming vidéo, l'UDP 971 pour la signalisation visuelle, l'UDP 972 pour le streaming audio, et l'UDP 973 pour la signalisation sonore. Les caméras de Tandberg utilisent également d'autres ports, comme :

- UDP 161
- UDP 962 (protocole SNMP [SNMP])
- TCP 963 (netlog), TCP 964 (FTP)
- TCP 965 (calculer de réseau virtuel [VNC])
- UDP 974 (annonce Protocol [SAP] de session)

Ces ports supplémentaires peuvent ne pas avoir besoin d'une hiérarchisation spécifique.

Une manière courante d'identifier le trafic est de créer les class-map qui visent le trafic d'intérêt. Chaque class-map peut indiquer une liste d'accès qui vise n'importe quel trafic qui utilise la Voix et les ports vidéos :

```
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 alors créer un class-map pour chaque type de trafic ; chaque class-map indique 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 du trafic vocal et de vidéo ont été identifiés par des class-map, assurez-vous que le trafic est marqué correctement. Ceci peut être fait au niveau WLAN par les table-map et peut également être fait par des policy-map de client.

Les table-map examinent le marquage de QoS du trafic entrant et déterminent ce qu'être le marquage sortant de QoS devrait. Ainsi, les table-map sont utiles quand le trafic entrant a déjà le marquage de QoS. Des table-map sont utilisés exclusivement au niveau SSID.

En revanche, les policy-map peuvent viser le trafic identifié par des class-map et mieux sont adaptés au trafic potentiellement non-marqué d'intérêt. Cet exemple de configuration suppose que le trafic du côté de câble déjà a été marqué correctement avant qu'il entre dans le commutateur du Catalyst 3850 ou le Cisco 5760 WLC. Si ce n'est pas le cas, vous pouvez utiliser un policy-map et l'appliquer au niveau SSID comme stratégie de client. Puisque le trafic des clients sans fil ne peut avoir été marqué, vous devez marquer le trafic de Voix et de vidéo correctement :

- La Voix en temps réel devrait être identifiée par le DSCP 46 (expédition expédié [E-F]).
- Le vidéo devrait être le DSCP marqué 34 (classe assurément 41 [AF41] d'expédition).
- La signalisation pour la Voix et le vidéo devrait être le DSCP marqué 24 (valeur 3 [CS3] de service de sélecteur de classe).

Pour appliquer ces marquages, créez un policy-map 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
```

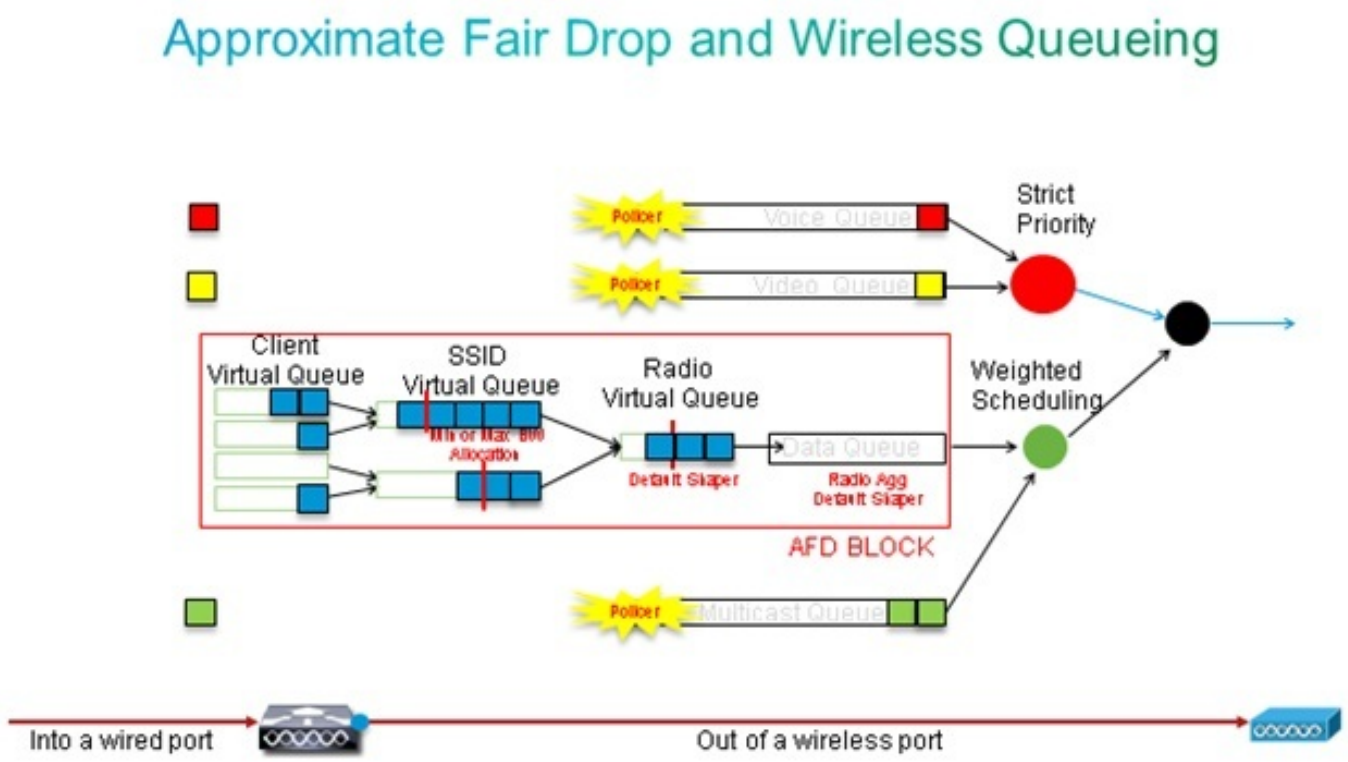
Étape 2 : Gestion de bande passante et prioritaire au niveau de port

L'étape suivante est de déterminer une stratégie QoS pour les ports qui sont livré et vont aux aps. Cette étape applique principalement aux Commutateurs du Catalyst 3850. Si votre configuration est faite sur un contrôleur de Cisco 5760, cette étape n'est pas obligatoire. Les ports du Catalyst 3850 portent le trafic de Voix et de vidéo qui va à ou provient des clients sans fil et des aps. La configuration QoS dans ce contexte apparie deux conditions requises :

1. **Allouez la bande passante**. Vous pouvez vouloir décider combien de bande passante est allouée pour chaque type de trafic. Cette allocation de bande passante peut également être faite au niveau SSID. Placez l'allocation de bande passante de port afin d'affiner combien de bande passante peut être reçue par chaque AP qui sert la cible SSID. Cette bande passante doit être placée pour tout le SSID sur la cible AP. Cet exemple simplifié de configuration suppose qu'il y a seulement un SSID et un AP, ainsi l'allocation de bande passante de port pour la Voix et le vidéo est identique que l'allocation globale de bande passante pour la Voix et le vidéo au niveau SSID. Chaque type de trafic est alloué 6 Mbits/s et est maintenu l'ordre de sorte que cette bande passante allouée ne soit pas dépassée.

2. **Donnez la priorité au trafic**. Le port a quatre files d'attente. Les deux premières files d'attente sont données la priorité et réservées pour le trafic en temps réel - typiquement Voix et vidéo,

respectivement. La quatrième file d'attente est réservée pour le trafic de multidiffusion de temps machine, et la troisième file d'attente contient tout autre trafic. Avec la logique convergée de Mise en file d'attente d'accès, le trafic pour chaque client est assigné à une file d'attente virtuelle, où QoS peut être configuré. Le résultat de la stratégie QoS de client est injecté dans la file d'attente virtuelle SSID, où QoS peut également être configuré. Puisque plusieurs le SSID peut exister sur une radio donnée AP, le résultat de chaque SSID qui est présent sur une radio AP est injecté dans la file d'attente virtuelle par radio AP, où le trafic est formé a basé sur la capacité par radio. Le trafic peut être retardé ou abandonné à l'un de ces étapes au moyen d'un mécanisme de QoS appelé la baisse d'Approximate Fair (AFD). Le résultat de cette stratégie est alors envoyé au port AP (appelé le port Sans fil), où la priorité est accordée aux deux premières files d'attente (jusqu'à une quantité de bande passante configurable), et puis aux troisième et quatrièmes files d'attente comme décrit plus tôt dans ce paragraphe.



Cette Voix d'endroits d'exemple de configuration dans la première file d'attente prioritaire et vidéo dans la deuxième file d'attente prioritaire par l'utilisation de la commande de **niveau de priorité**. Le reste du trafic est alloué le reste de la bande passante de port.

Notez que vous ne pouvez pas utiliser les class-map que le trafic de cible a basés sur le Listes de contrôle d'accès (ACL). Les stratégies appliquées au niveau de port peuvent viser le trafic basé sur des class-map, mais ces class-map devraient viser le trafic identifié par sa valeur de QoS. Une fois que vous avez identifié le trafic basé sur ACLs et marqué ce trafic correctement au niveau du client SSID, il serait redondant d'exécuter une deuxième inspection profonde de ce même trafic au niveau de port. Quand le trafic atteint le port qui va à AP, il est déjà marqué correctement.

Dans cet exemple, vous réutilisez les class-map généraux créés pour la stratégie SSID et visez directement le trafic de RTP de Voix et le trafic en temps réel de vidéo :

```
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 quelle stratégie à appliquer. La stratégie par défaut (appelée le parent_port) est appliquée automatiquement à chaque port quand AP est détecté. Vous ne devriez pas changer ce par défaut, en tant que lequel est placé :

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

Puisque la stratégie par défaut de parent_port appelle le port_child_policy, une option est d'éditer le port_child_policy. (Vous ne devriez pas changer son nom). Cette stratégie enfant détermine quel trafic devrait entrer dans chaque file d'attente et combien de bande passante devrait être allouée. La première file d'attente a le plus prioritaire, la deuxième file d'attente a le deuxième plus prioritaire, et ainsi de suite. Ces deux files d'attente sont réservées pour le trafic en temps réel. La quatrième file d'attente est utilisée pour le trafic de multidiffusion de temps machine. La troisième file d'attente contient tout autre trafic.

Dans cet exemple, vous décidez d'allouer le trafic vocal au premier trafic de file d'attente et de 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, la déclaration de priorité associée à la « Voix » et aux classes « videoandsignaling » te permet pour assigner ce trafic à la file d'attente prioritaire appropriée. Avis, cependant, que les déclarations de pour cent de la police rate s'appliquent seulement à la Multidiffusion, pas unicast, le trafic.

Vous n'avez pas besoin d'appliquer cette stratégie au niveau de port parce qu'il est appliqué automatiquement dès qu'AP sera détecté.

Étape 3 : Gestion de bande passante et prioritaire au niveau SSID

L'étape suivante est de prendre soin de la stratégie QoS au niveau SSID. Cette étape applique au commutateur du Catalyst 3850 et au contrôleur 5760. Cette configuration suppose que le trafic de Voix et de vidéo est identifié par l'utilisation du class-map et des Listes d'accès et est étiqueté correctement. Cependant, du trafic entrant qui n'est pas visé par la liste d'accès peut ne pas afficher son marquage de QoS. Dans ce cas, vous pouvez décider si ce trafic est identifié par une valeur par défaut ou laissé non-marqué. La même logique va pour le trafic déjà marqué mais non visé par les class-map. Employez la déclaration *par défaut de copie* dans un table-map afin de

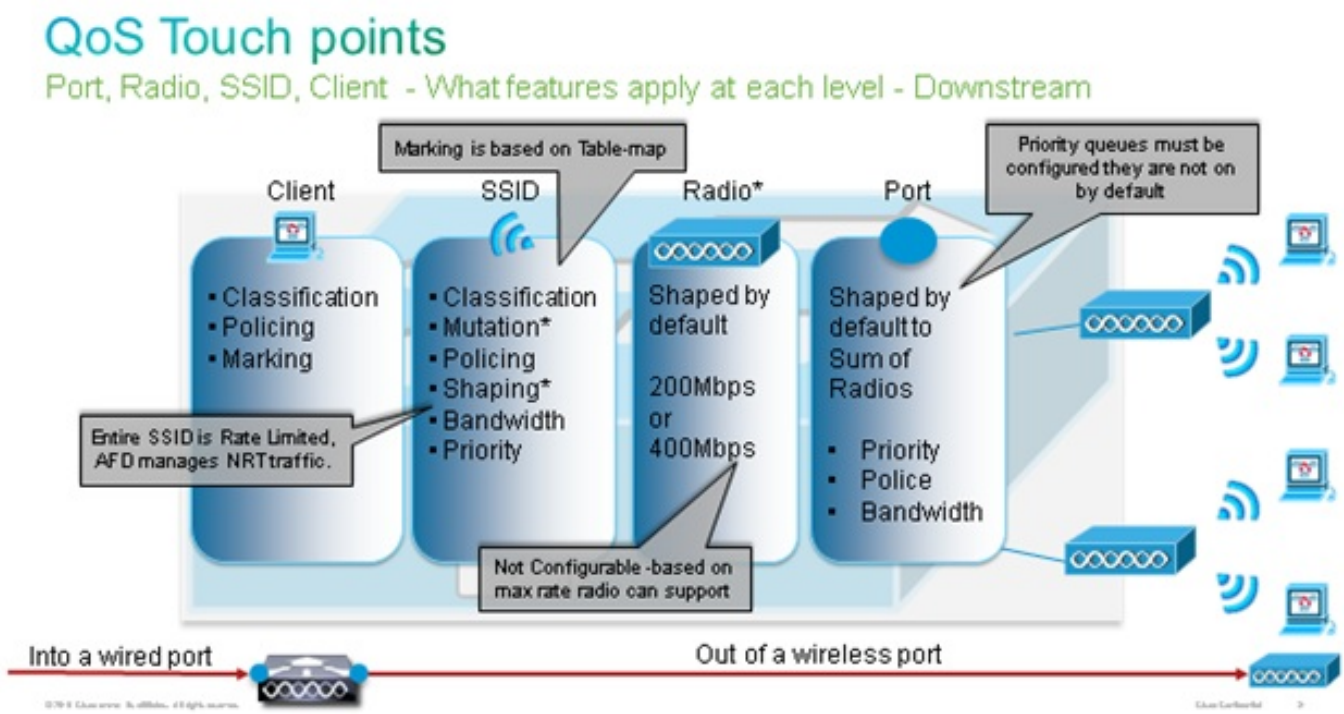
s'assurer que le trafic non marqué est laissé non marqué et que le trafic étiqueté garde la balise et il non remarqué.

Les table-map décident la valeur DSCP sortante mais sont également utilisés pour créer une trame de 802.11 pour décider la trame VERS LE HAUT de la valeur.

Dans cet exemple, le trafic entrant qui affiche niveau de QoS de Voix (DSCP 46) met à jour sa valeur DSCP, et la valeur est tracé au repérage équivalent de 802.11 (VERS LE HAUT de 6). Le trafic entrant qui affiche le niveau visuel de QoS (DSCP 34) met à jour sa valeur DSCP, et la valeur est tracé au repérage équivalent de 802.11 (VERS LE HAUT de 5). De même, le DSCP marqué par trafic 24 peut être signalisation de Voix ; la valeur DSCP devrait être mise à jour et traduite dans le 802.11 VERS LE HAUT de 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 a pu également être fait au niveau de câble entrant de port. Cette figure affiche ce que des actions de QoS peuvent être prises comme transits du trafic de câble à la radio :



Les foyers de cet exemple de configuration sur l'aspect Sans fil de la configuration QoS et des marques trafiquent au niveau de client sans fil. Une fois que la partie de marquage a été terminée, vous devez allouer la bande passante ; ici, 6 Mbits/s de bande passante est alloués aux écoulements du trafic vocal. (Tandis que c'est l'allocation globale de bande passante pour la Voix, chaque appel consommerait moins - par exemple, 128 Kbps.) Cette bande passante est allouée avec l'ordre de **police** afin de réserver la bande passante et relâcher le trafic supérieur.

Le trafic visuel est également alloué 6 Mbits/s et maintenu l'ordre. Cet exemple de configuration suppose qu'il y a seulement un écoulement visuel.

La partie de signalisation du vidéo et du trafic vocal doit également être bande passante allouée. Il y a deux stratégies possibles.

- Utilisez la commande de **shape average**, qui permet au trafic supérieur pour être mise en mémoire tampon et envoyée plus tard. Cette logique n'est pas efficace pour l'écoulement de Voix ou de vidéo lui-même parce que ces écoulements exigent à retard et instabilité cohérent ; cependant, il peut être efficace pour signaler parce que la signalisation peut être légèrement retardée sans effet sur la qualité des communications. Dans les solutions d'accès convergées, les commandes de forme ne reçoivent pas ce qui s'appelle les « configurations de positions, » qui déterminent combien de trafic au-dessus de la bande passante allouée peut être mis en mémoire tampon. Par conséquent, une deuxième commande, le **rapport 0 de file d'attente-mémoires tampons**, doit être ajoutée afin de spécifier que la taille de position est 0. Si vous incluez la signalisation dans le reste du trafic et utilisez des commandes de forme, le trafic de signalisation pourrait être abandonné en période de l'encombrement élevé. Ceci pourrait, consécutivement, causer l'appel d'être relâché parce que l'un ou l'autre d'extrémité détermine que la transmission ne se produit plus.
- Pour éviter le risque d'appels abandonnés, vous pouvez inclure la signalisation dans une des files d'attente prioritaire. Cet exemple de configuration a précédemment défini les files d'attente prioritaire comme Voix et vidéo et ajoute maintenant la signalisation à la file d'attente visuelle.

Les utilisations de stratégie appellent le contrôle d'admission (CAC) pour le flux voix. Le trafic Sans fil de cibles CAC et apparie une particularité (dans cet exemple de configuration, VERS LE HAUT de 6 et de 7). Le CAC détermine alors la bande passante maximale que ce trafic devrait l'utiliser. Dans une configuration où vous maintenez l'ordre le trafic vocal, le CAC devrait être alloué un sous-ensemble de la quantité de bande passante globale allouée pour la Voix. Par exemple, si la Voix est maintenue l'ordre à 6 Mbits/s, le CAC ne peut pas dépasser 6 Mbits/s. Le CAC est configuré dans un policy-map (appelé une stratégie enfant) qui est intégré dans le policy-map en aval principal (appelé la stratégie de parent). Le CAC est introduit avec la commande de **wmm-tspec de cac d'admission**, suivie de la cible se lève et la bande passante allouée au trafic visé.

Chaque appel ne consomme pas toute la bande passante allouée pour exprimer. Par exemple, chaque appel peut consommer des 64 Kbits/s chaque manière, qui a comme conséquence 128 Kbps de consommation de bande passante bidirectionnelle efficace. L'instruction de débit détermine chaque consommation de bande passante d'appel, alors que la déclaration de réglementation détermine la bande passante globale allouée au trafic vocal. Si tous les appels qui se produisent dans l'utilisation de cellules près de la bande passante de maximum autorisé, n'importe quel nouvel appel qui est initié de la cellule et qui fait dépasser la bande passante consommée la bande passante maximum permise pour la Voix seront refusés. Vous pouvez régler avec précision ce processus par la configuration du CAC au niveau de bande, comme expliqué dans l'étape 4 : Limite d'appel avec le CAC.

Par conséquent, vous devez configurer une stratégie enfant qui contient les instructions CAC et qui est intégrée dans la stratégie en aval principale. Le CAC n'est pas configuré dans le policy-map en amont. Le CAC s'applique aux communications voix initiées à partir de la cellule, mais, parce que c'est une réponse à ces appels, le CAC est placé seulement dans le policy-map en aval. Le policy-map en amont sera différent. Vous ne pouvez pas utiliser les class-map créés précédemment parce que le trafic de cible de ces class-map basé sur un ACL. Le trafic injecté dans la stratégie SSID est déjà passé par la stratégie de client, ainsi vous ne devriez pas exécuter l'inspection profonde sur les paquets une deuxième fois. Au lieu de cela, le trafic de cible avec un marquage de QoS ce résulte de la stratégie de client.

Si vous décidez de ne pas laisser la signalisation dans la classe par défaut, vous devrez également donner la priorité à la signalisation.

Dans cet exemple, la signalisation et le vidéo sont dans la même classe, et plus de bande passante est allouée à cette classe afin de faciliter la partie de signalisation ; 6 Mbits/s sont alloués pour le trafic visuel (un écoulement point par point de caméra de Tandberg), et le Mbits/s 1 est alloué à la signalisation pour toutes les communications voix et l'écoulement visuel :

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

La stratégie enfant en aval est :

```
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 en aval de parent est :

```
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 des clients sans fil et est envoyé au WCM avant que le trafic soit envoyé hors d'un port de câble ou soit envoyé à un autre SSID. Dans des les deux cas, vous pouvez configurer les policy-map qui définissent la bande passante allouée à chaque type de trafic. La stratégie différera probablement basé en fonction si le trafic est envoyé hors d'un port de câble ou à un autre SSID.

Dans la direction en amont, votre principale préoccupation est de décider la priorité, pas la bande passante. En d'autres termes, votre policy-map en amont n'alloue pas la bande passante à chaque type de trafic. Puisque le trafic est déjà à AP et a déjà croisé le goulot d'étranglement constitué par l'espace Sans fil bidirectionnel-alterné, votre but est d'apporter ce trafic à la fonction de contrôleur du commutateur du Catalyst 3850 ou du Cisco 5760 WLC pour une transformation plus ultérieure. Quand le trafic est collecté au niveau AP, vous pouvez décider si vous faites confiance au marquage existant potentiel de QoS afin de donner la priorité à la circulation envoyée au contrôleur. Dans cet exemple, les valeurs DSCP existantes mettent en boîte sont de confiance :

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

Une fois que vos stratégies sont créées, appliquez les policy-map au WLAN. Dans cet exemple, on s'attend à ce que n'importe quel périphérique qui se connecte au WLAN prenne en charge WMM, ainsi WMM est exigé.

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

Étape 4 : Limite d'appel avec le CAC

La dernière étape est de concevoir en fonction le CAC votre situation spécifique. Dans la configuration CAC expliquée dans l'étape 3 : La Gestion de bande passante et prioritaire au niveau SSID, AP relâche n'importe quel paquet vocal qui dépasse la bande passante allouée.

Afin d'éviter le maximum de bande passante., vous devez également configurer le WCM afin d'identifier les appels qui sont placés et les appels qui causeront la bande passante d'être dépassée. La spécification du trafic du support WMM de quelques téléphones (TSPEC) et informent l'infrastructure Sans fil de la bande passante qu'on s'attend à ce que l'appel projeté consomme. Le WCM peut alors refuser l'appel avant qu'il soit placé.

Quelques téléphones SIP ne prennent en charge pas TSPEC, mais le WCM et l'AP peuvent être placés pour identifier des paquets d'initiation d'appel envoyés POUR SIROTER des ports et peuvent employer ces informations afin d'établir qu'un appel de SIP est sur le point d'être placé. Puisque le téléphone SIP ne spécifie pas la bande passante qui doit être consommée par l'appel, l'administrateur doit déterminer la bande passante prévue, basée sur les codecs, le temps d'échantillonnage, et ainsi de suite.

Le CAC calcule la bande passante consommée à chaque niveau AP. Le CAC peut être placé pour utiliser seulement la consommation de bande passante de client dans ses calculs (CAC statique) ou pour considérer également des aps voisins et des périphériques sur le même canal (CAC chargement chargement). Cisco recommande que vous utilisiez le CAC statique pour des téléphones SIP et le CAC chargement chargement pour des téléphones TSPEC.

En conclusion, notez que le CAC est lancé sur a par base de bande.

Dans cet exemple, le SIP d'utilisation de téléphones plutôt que TSPEC pour leur initiation de session, chaque appel utilise des 64 Kbits/s pour chaque direction de flot, le CAC chargement chargement est désactivé quand le CAC statique est activé, et 75% de chaque bande passante AP maximum 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 gigahertz :

```
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 que le CAC est appliqué pour chaque bande, vous devez également appliquer le SIP CAC au niveau WLAN. Ce processus permet à AP d'examiner les informations de la couche 4 (L4) du trafic de client sans fil afin d'identifier les requêtes envoyées à l'UDP 5060 qui indiquent

des tentatives d'appel de SIP. TSPEC fonctionne au niveau de 802.11 et est détecté à la façon des indigènes par des aps. Les téléphones SIP n'utilisent pas TSPEC, ainsi AP doit exécuter une inspection plus profonde de paquet afin d'identifier le trafic de SIP. Puisque vous ne voulez pas qu'AP exécute cette inspection sur tout le SSID, vous devez déterminer quel SSID s'attendent au trafic de SIP. Vous pouvez alors activer l'appel pillant sur des ces SSID afin de rechercher des communications voix. Vous pouvez également déterminer quelle action d'exécuter si un appel de SIP doit être rejeté - dissociez le client de SIP ou envoyez un message occupé de SIP.

Dans cet exemple, piller d'appel est activé, et un message occupé est envoyé si l'appel de SIP doit être rejeté. En plus de la stratégie QoS de l'étape 3 : La Gestion de bande passante et prioritaire au niveau SSID, ceci est la configuration SSID pour l'exemple WLAN :

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

Vérifiez

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

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

show class-map

Cette commande affiche les class-map configurés 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-map 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 les paramètres de configuration et de service-stratégie WLAN :

```
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
```

stratégies de show platform qos

Cette commande affiche les stratégies QoS installées pour des ports, des radios AP, le SSID, et des clients. Notez que vous pouvez vérifier, mais ne pouvez pas changer, les stratégies par 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
```

affichez la service-stratégie de <mac> de mac-address de client sans fil

Cette commande affiche les policy-map appliqués au niveau de 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
```

Dépannez

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