

QoS en los reguladores convergidos del acceso y el ejemplo de configuración ligero AP

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Mejoras de la Marcación de paquetes QoS L3](#)

[Red inalámbrica de la configuración para QoS con el MQC](#)

[Directivas puestas en hard-code valor por defecto](#)

[Platino](#)

[Oro](#)

[Plata](#)

[Bronce](#)

[Configuración manualmente](#)

[Paso 1: Identificación y marca del tráfico de voz](#)

[Paso 2: Administración del ancho de banda y de la prioridad en el nivel del puerto](#)

[Paso 3: Administración del ancho de banda y de la prioridad en el nivel SSID](#)

[Paso 4: Limitación de la llamada con el CAC](#)

[Verificación](#)

[muestre el clase-mapa](#)

[muestre el directiva-mapa](#)

[muestre wlan](#)

[show policy-map interface](#)

[muestre las directivas de los qos de la plataforma](#)

[muestre la servicio-directiva del <mac> del MAC address del cliente de red inalámbrica](#)

[Troubleshooting](#)

Introducción

Este documento describe cómo configurar QoS en Cisco convergió red de acceso con los Puntos de acceso ligeros (revestimientos) y con el Cisco Catalyst 3850 Switch o el regulador del Wireless LAN de Cisco 5760 (WLC).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- El conocimiento básico de cómo configurar los revestimientos y Cisco convergieron los reguladores del acceso
- Conocimiento de cómo configurar la encaminamiento básica y QoS en una red alámbrica

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ¿Cisco Catalyst 3850 Switch que funciona con el Cisco IOS? Versión de software XE 3.2.2(SE)
- Regulador del Wireless LAN de Cisco 5760 que funciona con la versión del Software Cisco IOS XE 3.2.2(SE)
- Puntos de acceso ligeros de las Cisco 3600 Series

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

QoS refiere a la capacidad de la red de proporcionar mejor o al servicio especial a un conjunto de los usuarios o a las aplicaciones al detrimento de otros usuarios o aplicaciones.

Con QoS, el ancho de banda se puede manejar más eficientemente a través de los LAN, que incluye la Tecnología inalámbrica LAN (WLAN) y WAN. QoS proporciona servicio aumentado y de red confiable con estos servicios:

- Ancho de banda dedicado de los soportes para los usuarios críticos y las aplicaciones.
- Controla el jitter y el tiempo de espera que es requerido por el tráfico en tiempo real.
- Maneja y minimiza la congestión de red.
- Forma el tráfico de la red para alisar el flujo de tráfico.
- Establece las prioridades del tráfico de la red.

En el pasado, los WLAN fueron utilizados principalmente para transportar el ancho de banda baja, tráfico de la aplicación de datos. Con la extensión de los WLAN en la vertical (tal como venta al por menor, finanzas, y educación) y los entornos para empresas, los WLAN ahora se utilizan para transportar las aplicaciones de datos del ancho de banda alto conjuntamente con el time sensible, las aplicaciones multimedia. Este requisito llevado a la necesidad para QoS inalámbrico.

El Grupo de trabajo de IEEE 802.11e dentro del comité regulatorio del IEEE 802.11 ha completado la definición estándar, y el Wi-Fi Alliance ha creado la certificación de las multimedias del Wi-Fi (WMM), pero la adopción del estándar 802.11e todavía se limita. WMM-se certifican la mayoría de los dispositivos, porque la certificación WMM es necesaria para la certificación 802.11n y 802.11ac. Muchos dispositivos de red inalámbrica no asignan diversos niveles de QoS

a los paquetes enviados a la capa del link de datos, así que esos dispositivos envían la mayor parte de su tráfico sin la marca de QoS y ninguna priorización relativa. Sin embargo, la mayoría de los Teléfonos IP del Voice over wireless LAN (VoWLAN) del 802.11 marcan y dan prioridad a su tráfico de voz. Este documento se centra en la configuración de QoS para los Teléfonos IP de VoWLAN y en los dispositivos vídeo-capaces del Wi-fi que marcan su tráfico de voz.

Nota: La configuración de QoS para los dispositivos que no realizan la marca interna está fuera del ámbito de este documento.

La enmienda 802.11e define ocho niveles de la prioridad de usuario (PARA ARRIBA), agrupados dos por dos en cuatro niveles de QoS (categorías del acceso):

- Platino/Voz (ENCIMA de 7 y 6) - asegura un de alta calidad del servicio para la Voz sobre la Tecnología inalámbrica.
- Oro/vídeo (ENCIMA de 5 y 4) - aplicación de video de alta calidad de los soportes.
- Ancho de banda normal de plata/mejor de esfuerzo (ENCIMA de 3 y de 0) - de los soportes para los clientes. Ésta es la configuración predeterminada.
- Bronce/fondo (ENCIMA de 2 y 1) - proporciona el ancho de banda más bajo para los servicios del invitado.

El platino es de uso general para los clientes y el oro VoIP para los clientes video. Este documento proporciona un ejemplo de configuración que ilustre cómo configurar QoS en los reguladores y comunicar con una red alámbrica que se configure con QoS para VoWLAN y los clientes video.

Mejoras de la Marcación de paquetes QoS L3

Cisco convergió marcado del Differentiated Services Code Point IP de la capa 3 del soporte de los reguladores del acceso (L3) (DSCP) de los paquetes enviados por el WLCs y los revestimientos. Esta característica aumenta cómo el uso del (APS) de los Puntos de acceso esta información L3 para asegurarse de que los paquetes reciben el correcto sobre - ventila el priorización del AP al cliente de red inalámbrica.

En una arquitectura de WLAN convergida del acceso que utilice los Catalyst 3850 Switch como reguladores inalámbricos, los AP conectan directamente con el Switch. En una arquitectura de WLAN convergida del acceso que utilice 5760 reguladores, los datos WLAN son tunneled entre el AP y el WLC vía el control y el aprovisionamiento del protocolo de los untos de acceso de red inalámbrica (CAPWAP). Para mantener la clasificación de QoS original a través de este túnel, las configuraciones de QoS del paquete de datos encapsulados se deben asociar apropiadamente a la capa 2 (L2) (802.1p) y (IP DSCP) a los campos L3 del paquete del túnel externo.

Cuando usted configura QoS para VoWLAN y el vídeo, usted puede configurar política de calidad de servicio (QoS) un específico para los clientes de red inalámbrica y un específico de la directiva a una red inalámbrica (WLAN), o ambos. Usted puede también complementar la configuración con un específico de la configuración al puerto que conecta el AP, especialmente con los Catalyst 3850 Switch. Este ejemplo de configuración se centra en la configuración de QoS para el cliente de red inalámbrica, la red inalámbrica (WLAN), y el puerto al AP. Los objetivos primarios de una configuración de QoS para VoWLAN y los aplicación de video son:

- Reconozca la Voz y el tráfico de video (Clasificación de tráfico y marca), ambos en sentido

ascendente y descendentes.

- Marque la Voz y el tráfico de video con un nivel de prioridad de voz: 802.11e ENCIMA de 6, 802.1p 5, DSCP 46 para la Voz.802.11e SUBEN 5, DSCP 34 para el vídeo.
- Afecte un aparato el ancho de banda para el tráfico de voz, la señalización de voz, y el tráfico de video.

Configure la red inalámbrica para QoS con el MQC

Antes de que usted configure QoS, usted debe configurar la función inalámbrica del módulo del regulador (WCM) del WLC del Catalyst 3850 Switch o de Cisco 5760 para la operación básica y registrar los revestimientos al WCM. Este documento asume que el WCM está configurado para la operación básica y que los revestimientos están registrados al WCM.

La solución de acceso convergida utiliza el comando `line interface(cli)` de la Calidad del servicio (QoS) modular (MQC). Refiera a la [guía de configuración de QoS, la versión 3SE \(Catalyst 3850 Switch\) del Cisco IOS XE](#) para más información sobre el uso del MQC en configuración de QoS en el Catalyst 3850 Switch.

La configuración de QoS con el MQC en los reguladores convergidos del acceso confía en cuatro elementos:

- **Class-maps** se utilizan para reconocer el tráfico del interés. Class-maps puede utilizar las diversas técnicas (tales como marca, listas de acceso, o VLA N existentes de QoS) para identificar el tráfico del interés.
- **Las correspondencias de políticas** se utilizan para determinar qué configuraciones de QoS se deben aplicar al tráfico del interés. Las correspondencias de políticas llaman class-maps y aplican las diversas configuraciones de QoS (tales como marca, niveles de prioridad, asignación de ancho de banda específicos, y así sucesivamente) a cada clase.
- **Las políticas de servicio** se utilizan para aplicar las correspondencias de políticas a las puntas estratégicas de su red. En la solución de acceso convergida, las políticas de servicio se pueden aplicar a los usuarios, a los identificadores del conjunto de servicio (SSID), a los radios AP, y a los puertos. El puerto, el SSID, y las políticas de cliente se pueden configurar por el usuario. Las directivas de radio son controladas por el módulo de control inalámbrico. Las directivas inalámbricas de QoS para el puerto, el SSID, el cliente, y la radio se aplican en la dirección descendente cuando el tráfico está fluyendo del Switch o del regulador a los clientes de red inalámbrica.
- **las Tabla-correspondencias** se utilizan para examinar la marca entrante de QoS y decidir a las marcas salientes de QoS. las Tabla-correspondencias se colocan en las correspondencias de políticas aplicadas a los SSID. las Tabla-correspondencias se pueden utilizar para guardar (copia) o cambiar la marca. las Tabla-correspondencias se pueden también utilizar para crear una asignación entre la marca atada con alambre y inalámbrica. La marca atada con alambre utiliza DSCP (L3 QoS) o 802.1p (L2 QoS). La marca inalámbrica utiliza la prioridad de usuario (PARA ARRIBA). las Tabla-correspondencias son de uso general determinar qué marca DSCP se debe consumir para cada uno de interés y qué se debe consumir para cada valor DSCP del interés. las Tabla-correspondencias son fundamentales al acceso convergido QoS porque no hay traducción directa entre el DSCP y los valores ASCENDENTES.

Sin embargo, el DSCP a las tabla-correspondencias ASCENDENTES también permite la instrucción de la *copia*. En ese caso, la solución de acceso convergida utiliza la arquitectura Cisco

para la Voz, el vídeo, y la tabla de correspondencia integrada de los datos (AVVID) para determinar el DSCP a ASCENDENTE o hasta la traducción DSCP:

Índice de la escritura de la etiqueta	Campo clave	Valor entrante	DSCP externo	CoS	EN FUNCIONAMIENTO
0	N.A.	No marcado	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	EN FUNCIONAMIENTO	0	0	0	0
74	EN FUNCIONAMIENTO	1	8	1	1
75	EN FUNCIONAMIENTO	2	16	1	2
76	EN FUNCIONAMIENTO	3	24	2	3
77	EN FUNCIONAMIENTO	4	34	3	4
78	EN FUNCIONAMIENTO	5	34	4	5
79	EN FUNCIONAMIENTO	6	46	5	6
80	EN FUNCIONAMIENTO	7	46	7	7

Directivas puestas en hard-code valor por defecto

Los reguladores convergidos del acceso embarcan política de calidad de servicio (QoS) los perfiles puestos en hard-code que se pueden aplicar a los WLAN. Estos perfiles aplican las directivas del metal (platino, oro, y así sucesivamente) que son familiares a los administradores de los reguladores de las redes del Cisco Unified Wireless (CUWN). Si su objetivo no es crear las directivas que asignan el ancho de banda específico al tráfico de voz pero asegurarse simplemente de que el tráfico de voz recibe la marca apropiada de QoS, usted puede utilizar las directivas puestas en hard-code. Las directivas puestas en hard-code se pueden aplicar a la red inalámbrica (WLAN) y pueden ser diferentes en la conexión en sentido ascendente y las

direcciones descendentes.

Notas:

Use la [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos usados en esta sección.

[La herramienta del Output Interpreter](#) ([clientes registrados solamente](#)) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

Platino

La directiva puesta en hard-code para la Voz se llama platino. El nombre no puede ser cambiado.

Ésta es la directiva rio abajo para el nivel de QoS del platino:

```
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
```

Ésta es la directiva por aguas arriba para el nivel de QoS del platino:

```
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
```

Oro

La directiva puesta en hard-code para el vídeo se llama oro. El nombre no puede ser cambiado.

Ésta es la directiva rio abajo para el nivel de QoS del oro:

```
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
```

Ésta es la directiva por aguas arriba para el nivel de QoS del oro:

```
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
```

Plata

La directiva puesta en hard-code para mejor esfuerzo se llama de plata. El nombre no puede ser cambiado.

Ésta es la directiva rio abajo para el nivel de plata 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
```

Ésta es la directiva por aguas arriba para el nivel de plata 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
```

Bronce

La directiva puesta en hard-code para el tráfico de fondo se llama de bronce. El nombre no puede

ser cambiado.

Ésta es la directiva rio abajo para el nivel de bronce 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
```

Ésta es la directiva por aguas arriba para el nivel de bronce 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
```

Una vez que usted ha decidido qué mejor del tabla-mapa hace juego el tráfico de la blanco para un SSID dado, usted puede aplicar la directiva que corresponde con a su red inalámbrica (WLAN). En este ejemplo, una directiva se aplica en la dirección descendente (salida, del AP al cliente de red inalámbrica), y una directiva se aplica en la dirección ascendente (entrada, del cliente de red inalámbrica, con el AP, al regulador):

```
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#
```

Marque la configuración de la red inalámbrica (WLAN) para verificar qué directiva fue aplicada a su red inalámbrica (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

Configuración manualmente

Las directivas puestas en hard-code aplican la marca predeterminada de QoS pero no aplican la asignación de ancho de banda. Las directivas puestas en hard-code también asumen que su tráfico es ya marcado. En un entorno complejo, usted puede querer utilizar una combinación de directivas para reconocer y marcar la Voz y el tráfico de video apropiadamente, para fijar la asignación de ancho de banda en el río abajo y las direcciones ascendentes, y para utilizar el control de admisión de llamadas para limitar el número de llamadas iniciadas de la célula inalámbrica.

Nota: Use la [Command Lookup Tool \(clientes registrados solamente\)](#) para obtener más información sobre los comandos usados en esta sección.

Paso 1: Identificación y marca del tráfico de voz

El primer paso es reconocer la Voz y el tráfico de video. El tráfico de voz se puede clasificar en dos categorías:

- Flujo de la voz, que lleva a la parte de audio la comunicación.
- La señalización de voz, que lleva la información estadística intercambiado entre los puntos finales de la Voz.

El flujo de la voz utiliza comúnmente los puertos destino del Real-Time Transport Protocol (RTP) y del User Datagram Protocol (UDP) en el rango de 16384 - 32767. Éste es el rango; los puertos reales son generalmente más estrechos y dependen de la implementación.

Hay varios protocolos de señalización de voz. Este ejemplo de configuración utiliza el Jabber. El Jabber utiliza estos puertos TCP para la conexión y el directorio:

- TCP 80 (HTTP)
- 143 ([IMAP] del Protocolo de acceso a mensajes de Internet)

- 443 (HTTPS)
- 993 (IMAP) para los servicios tales como Cisco Unified MeetingPlace o WebEx de Cisco para las reuniones y Cisco Unity o Cisco Unity Connection para las características del voicemail
- TCP 389/636 (servidor del [LDAP] del protocolo lightweight directory access para las búsquedas del contacto)
- FTP (1080)
- TFTP (UDP 69) para la transferencia de archivos (tal como archivos de configuración) de los pares o del servidor

Estos servicios pueden no necesitar un priorización específico.

El Jabber utiliza el Session Initiation Protocol (SIP) (UDP/TCP 5060 y 5061) para la señalización de voz.

El tráfico de video utiliza diversos puertos y protocolos que dependan de su implementación. Este ejemplo de configuración utiliza una cámara de Tandberg PrecisionHD 720p para los Video conferencia. La cámara de Tandberg PrecisionHD 720p puede utilizar vario codecs; el ancho de banda consumido depende del codificador-decodificador elegido:

- C20, el uso H.323/SIP del codecs C40, y C60 y puede consumir hasta el 6 Mbps en las conexiones Point-to-Point.
- El codificador-decodificador C90 utiliza estos mismos protocolos y puede consumir hasta el 10 Mbps en las comunicaciones del multi-sitio.

La implementación de Tandberg de H.323 utiliza típicamente UDP 970 para el vídeo de flujo continuo, UDP 971 para la señalización video, UDP 972 para fluir el audio, y UDP 973 para la señalización audio. Las cámaras de Tandberg también utilizan otros puertos, por ejemplo:

- UDP 161
- UDP 962 (protocolo administración de red simple [SNMP])
- TCP 963 (netlog), (FTP) TCP 964
- TCP 965 ([VNC] del Virtual Network Computing)
- UDP 974 ([SAP] del protocolo del anuncio de sesión)

Estos puertos adicionales pueden no necesitar un priorización específico.

Una manera común de identificar el tráfico es crear class-maps que apunta el tráfico del interés. Cada clase-mapa puede señalar a una lista de acceso que apunte cualquier tráfico que utilice la Voz y los puerto de video:

```
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
```

Usted puede entonces crear un clase-mapa para cada tipo de tráfico; cada clase-mapa señala a la lista de acceso relevante:

```

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

```

Una vez que el tráfico de voz y el tráfico de video se han identificado con class-maps, asegúrese de que el tráfico esté marcado correctamente. Esto se puede hacer en la red inalámbrica (WLAN) llana a través de las tabla-correspondencias y se puede también hacer a través de las correspondencias de políticas del cliente.

las Tabla-correspondencias examinan la marca de QoS del tráfico entrante y determinan lo que debe ser la marca saliente de QoS. Así, las Tabla-correspondencias son útiles cuando el tráfico entrante tiene ya marca de QoS. las Tabla-correspondencias se utilizan exclusivamente en el nivel SSID.

Por el contrario, las correspondencias de políticas pueden apuntar el tráfico identificado por class-maps y se adaptan mejor potencialmente al tráfico sin Tags del interés. Este ejemplo de configuración asume que el tráfico de la cara tela se ha marcado ya correctamente antes de que ingrese el Catalyst 3850 Switch o el WLC de Cisco 5760. En caso contrario, usted puede utilizar un directiva-mapa y aplicarlo en el nivel SSID como política de cliente. Porque el tráfico de los clientes de red inalámbrica no pudo haber sido marcado, usted necesita marcar la Voz y el tráfico de video correctamente:

- La voz en tiempo real se debe marcar con DSCP 46 ([EF] del Expedited Forwarding).
- El vídeo debe ser DSCP 34 marcado (clase de reenvío confiada 41 [AF41]).
- La señalización para la Voz y el vídeo debe ser DSCP marcado 24 (el valor 3 [CS3] del servicio del Selector de clase).

Para aplicar estas marcas, cree un directiva-mapa que llame cada uno de estas clases y que marque el tráfico equivalente:

```

policy-map taggingPolicy
class RTPaudio
set dscp ef

class H323realtimevideo
set dscp af41

class signaling
set dscp cs3

```

Paso 2: Administración del ancho de banda y de la prioridad en el nivel del puerto

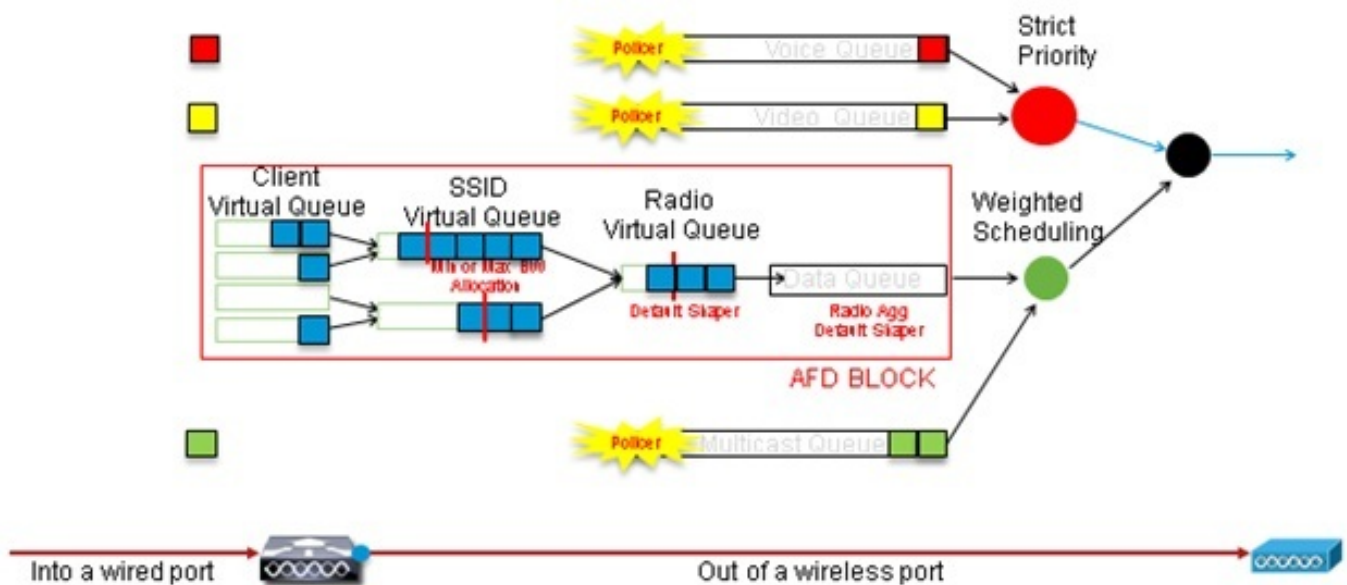
El siguiente paso es determinar a política de calidad de servicio (QoS) para los puertos que vienen y van a los AP. Este paso se aplica sobre todo a los Catalyst 3850 Switch. Si su configuración se hace en un regulador de Cisco 5760, este paso no es obligatorio. Los puertos del Catalyst 3850 llevan la Voz y el tráfico de video que va a o viene de los clientes de red inalámbrica y de los AP. La configuración de QoS en este contexto hace juego dos requisitos:

1. **Afecte un aparato el ancho de banda.** Usted puede querer decidir cuánto ancho de banda se afecta un aparato para cada tipo de tráfico. Esta asignación de ancho de banda se puede

también hacer en el nivel SSID. Fije la asignación de ancho de banda del puerto para refinar cuánto ancho de banda se puede recibir por cada AP que sirva la blanco SSID. Este ancho de banda tiene que ser fijado para todos los SSID en la blanco AP. Este ejemplo de la configuración simplificada asume que hay solamente un SSID y un AP, así que la asignación de ancho de banda del puerto para la Voz y el vídeo es lo mismo que la asignación de ancho de banda global para la Voz y el vídeo en el nivel SSID. Cada tipo de tráfico es 6 Mbps afectado un aparato y se limpia para no exceder este ancho de banda afectado un aparato.

2. **Dé prioridad al tráfico.** El puerto tiene cuatro colas de administración del tráfico. Las primeras dos colas de administración del tráfico se dan prioridad y se reservan para el tráfico en tiempo real - típicamente Voz y vídeo, respectivamente. La cuarta cola es reservada para el tráfico Multicast no en tiempo real, y la tercera cola contiene el resto del tráfico. Con la lógica convergida de los Datos en espera del acceso, el tráfico para cada cliente se asigna a una cola virtual, donde QoS puede ser configurado. El resultado del cliente política de calidad de servicio (QoS) se inyecta en la cola virtual SSID, donde QoS puede también ser configurado. Puesto que varios SSID pueden existir en una radio AP dada, el resultado de cada SSID que esté presente en una radio AP se inyecta en la cola virtual de la radio AP, donde se forma el tráfico basó en la capacidad de radio. El tráfico se puede retrasar o caer en ninguno de estos etapas por medio de un mecanismo de Calidad de servicio (QoS) llamado descenso de Approximate Fair (AFD). El resultado de esta directiva entonces se envía al puerto AP (llamado el puerto inalámbrico), donde la prioridad se da a las primeras dos colas de administración del tráfico (hasta una cantidad configurable de ancho de banda), y entonces a las terceras y cuartas colas de administración del tráfico según lo descrito anterior en este párrafo.

Approximate Fair Drop and Wireless Queueing



Este ejemplo de configuración pone la Voz en la cola de primera prioridad y el vídeo en el segundo priority queue con el uso del comando del nivel de prioridad. El resto del tráfico se afecta un aparato el resto del ancho de banda del puerto.

Note que usted no puede utilizar class-maps que el tráfico de la blanco basó en el Listas de control de acceso (ACL). Las directivas aplicadas en el nivel del puerto pueden apuntar el tráfico basado en class-maps, pero este class-maps debe apuntar el tráfico identificado por su valor de QoS. Una vez que usted ha identificado el tráfico basado en los ACL y marcado este tráfico correctamente en el nivel del cliente SSID, sería redundante realizar un segundo examen profundo de ese mismo tráfico en el nivel del puerto. Cuando el tráfico alcanza el puerto que va al AP, se marca ya correctamente.

En este ejemplo, usted reutiliza el class-maps general creado para la directiva SSID y apunta directamente el tráfico de la Voz RTP y el tráfico en tiempo real del vídeo:

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

Una vez que usted ha identificado el tráfico del interés, usted puede decidir qué directiva a aplicarse. La política predeterminada (llamada parent_port) se aplica automáticamente en cada puerto cuando se detecta un AP. Usted no debe cambiar este valor por defecto, como el cual se fija:

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

Porque la directiva predeterminada del parent_port llama el port_child_policy, una opción es editar el port_child_policy. (Usted no debe cambiar su nombre). Esta política hija determina qué tráfico debe entrar en cada cola y cuánto ancho de banda debe ser afectado un aparato. La primera cola tiene la prioridad más alta, la segunda cola tiene la segunda prioridad más alta, y así sucesivamente. Estas dos colas de administración del tráfico son reservadas para el tráfico en tiempo real. La cuarta cola se utiliza para el tráfico Multicast no en tiempo real. La tercera cola contiene el resto del tráfico.

En este ejemplo, usted decide afectar un aparato el tráfico de voz a la primera cola y el tráfico de video a la segunda cola y afectar un aparato el ancho de banda a cada cola y al resto del tráfico:

```
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
```

En esta directiva, la sentencia de prioridad asociada a la “Voz” y a las clases “videoandsignaling” permite que usted asigne ese tráfico al priority queue relevante. El aviso, sin embargo, que la policía valora las declaraciones del por ciento se aplica solamente al Multicast, no unicast, tráfico.

Usted no necesita aplicar esta directiva en el nivel del puerto porque se aplica automáticamente tan pronto como se detecte un AP.

Paso 3: Administración del ancho de banda y de la prioridad en el nivel SSID

El siguiente paso es tomar el cuidado del política de calidad de servicio (QoS) en el nivel SSID. Este paso se aplica al Catalyst 3850 Switch y al regulador 5760. Esta configuración asume que la Voz y el tráfico de video está identificada con el uso del clase-mapa y de las listas de acceso y marcada con etiqueta correctamente. Sin embargo, un cierto tráfico entrante que no es apuntado por la lista de acceso puede no visualizar su marca de QoS. En ese caso, usted puede decidir si este tráfico se marca con un valor predeterminado o se fue untagged. La misma lógica va para el tráfico marcado pero no apuntado ya por el class-maps. Utilice la declaración de la *copia predeterminada* en un tabla-mapa para asegurarse de que el tráfico no marcado está dejado no marcado y de que el tráfico con Tag guarda la etiqueta y él no comentado.

las Tabla-correspondencias deciden al valor saliente DSCP pero también se utilizan para crear una trama del 802.11 para decidir a la trama ENCIMA del valor.

En este ejemplo, el tráfico entrante que visualiza el nivel de QoS de la Voz (DSCP 46) mantiene su valor DSCP, y el valor se asocia al marcado equivalente del 802.11 (ENCIMA de 6). El tráfico entrante que visualiza el nivel video de QoS (DSCP 34) mantiene su valor DSCP, y el valor se asocia al marcado equivalente del 802.11 (ENCIMA de 5). Semejantemente, trafique DSCP marcado 24 puede ser señalización de voz; el valor DSCP se debe mantener y traducir al 802.11 ENCIMA de 3:

```
Table-map dscp2dscp
```

```
Default copy
```

```
Table-map dscp2up
```

```
Map from 46 to 6
```

```
Map from 24 to 3
```

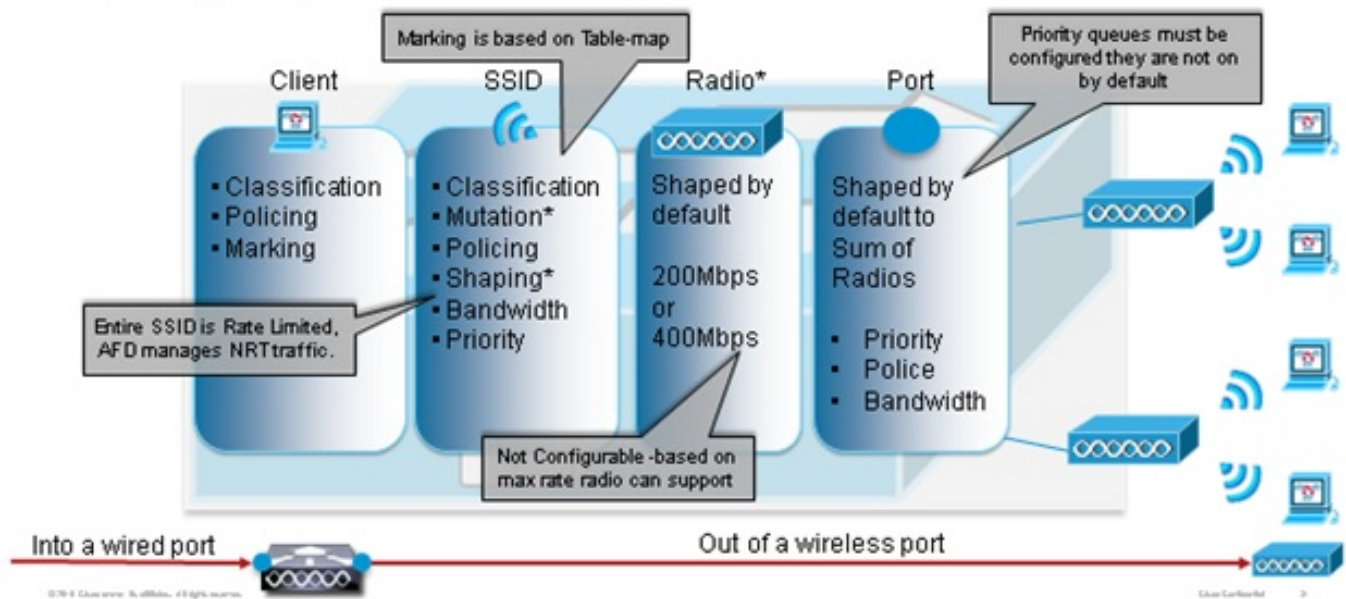
```
Map from 34 to 5
```

```
Default copy
```

La marca se podía también hacer en el nivel atado con alambre entrante del puerto. Esta figura muestra que lo que se pueden tomar las acciones de QoS como tráfico transita de atado con alambre a la Tecnología inalámbrica:

QoS Touch points

Port, Radio, SSID, Client - What features apply at each level - Downstream



Este ejemplo de configuración se centra en el aspecto inalámbrico de la configuración de QoS y las marcas trafican en el nivel del cliente de red inalámbrica. Una vez que se ha completado la porción de la marca, usted necesita afectar un aparato el ancho de banda; aquí, el 6 Mbps del ancho de banda se afecta un aparato a los flujos del tráfico de voz. (Mientras que ésta es la asignación del ancho de banda general para la Voz, cada llamada consumiría menos - por ejemplo, el kbps 128.) Este ancho de banda se afecta un aparato con el **comando police** para reservar el ancho de banda y caer el tráfico superior.

El tráfico de video es 6 Mbps también afectado un aparato y limpiado. Este ejemplo de configuración asume que hay solamente un flujo video.

La parte de señalización el vídeo y el tráfico de voz también necesita ser ancho de banda afectado un aparato. Hay dos estrategias posibles.

- Utilice el comando **medio de la dimensión de una variable**, que permite que envíen el tráfico superior sea mitigado y más adelante. Esta lógica no es eficiente para el flujo sí mismo de la Voz o del vídeo porque esos flujos requieren la fluctuación y retraso constante; sin embargo, puede ser eficiente para señalar porque la señalización se puede retrasar levemente sin un efecto sobre la calidad de la llamada. En la solución de acceso convergida, los comandos shape no validan qué se llama las "configuraciones de los compartimentos," que determinan cuánto tráfico superior al ancho de banda afectado un aparato puede ser mitigado. Por lo tanto, un comando second, la **relación de transformación 0 de los búferes de cola**, debe ser agregado para especificar que el tamaño del compartimento es 0. Si usted incluye la señalización en el resto del tráfico y utiliza los comandos shape, la señalización de tráfico se pudo caer en tiempos del alto nivel de congestión. Esto pudo, a su vez, hacer la llamada ser caído porque cualquier extremo determina que está ocurriendo la comunicación no más.
- Para evitar el riesgo de llamadas interrumpidas, usted puede incluir la señalización en una de las colas de administración del tráfico de prioridad. Este ejemplo de configuración definió previamente las colas de administración del tráfico de prioridad como Voz y vídeo y ahora

agrega la señalización a la cola video.

La directiva utiliza el control de admisión de llamadas (CAC) para el flujo de la voz. El CAC apunta el tráfico de red inalámbrica y hace juego un específico PARA ARRIBA (en este ejemplo de configuración, ENCIMA de 6 y de 7). El CAC entonces determina la cantidad máxima de ancho de banda que este tráfico debe utilizar. En una configuración donde usted limpia el tráfico de voz, el CAC se debe afectar un aparato un subconjunto de la cantidad total de ancho de banda afectada un aparato para la Voz. Por ejemplo, si la Voz se limpia al 6 Mbps, el CAC no puede exceder el 6 Mbps. El CAC se configura en un directiva-mapa (llamado una política hija) que sea integrado en el directiva-mapa rio abajo de la tubería (llamado la política controlante). El CAC se introduce con el comando del **wmm-tspec del cac de la admisión**, seguido por la blanco sube y el ancho de banda afectado un aparato al tráfico apuntado.

Cada llamada no consume todo el ancho de banda afectado un aparato para expresar. Por ejemplo, cada llamada puede consumir 64 kbps cada manera, que da lugar al kbps 128 del consumo de ancho de banda bidireccional eficaz. La instrucción de la tarifa determina cada consumo de ancho de banda de la llamada, mientras que la declaración de política determina el ancho de banda general afectado un aparato al tráfico de voz. Si todas las llamadas que ocurren dentro del uso de la célula cerca del Ancho de banda máximo permitido, cualquier nueva llamada que se inicie dentro de la célula y que haga el ancho de banda consumido exceder el ancho de banda máximo permitido para la Voz son negadas. Usted puede ajustar este proceso con la configuración del CAC en el nivel de banda, como se explica en el [paso 4: Limitación de la llamada con el CAC](#).

Por lo tanto, usted necesita configurar una política hija que contenga las instrucciones CAC y que sea integrada en la directiva rio abajo de la tubería. El CAC no se configura en el directiva-mapa por aguas arriba. El CAC se aplica a las llamadas de voz iniciadas de la célula, pero, porque es una respuesta a esas llamadas, el CAC se fija solamente en el directiva-mapa rio abajo. El directiva-mapa por aguas arriba será diferente. Usted no puede utilizar el class-maps creado previamente porque este tráfico class-maps de la blanco basado en un ACL. El tráfico inyectado en la directiva SSID pasó ya con la política de cliente, así que usted no debe realizar el examen profundo en los paquetes al por segunda vez. En lugar, el tráfico de la blanco con una marca de QoS esa resulta de la política de cliente.

Si usted decide no dejar la señalización en la clase predeterminada, usted también necesitará dar prioridad a la señalización.

En este ejemplo, la señalización y el vídeo están en la misma clase, y más ancho de banda se afecta un aparato a esa clase para acomodar la parte de señalización; El 6 Mbps se afecta un aparato para el tráfico de video (un flujo de punto a punto de la cámara de Tandberg), y el 1 Mbps se afecta un aparato a la señalización para todas las llamadas de voz y el flujo video:

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

La política hija rio abajo es:

```
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 política controlante rio abajo es:

```
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
```

El tráfico por aguas arriba es el tráfico que viene de los clientes de red inalámbrica y se envía al WCM antes de que el tráfico se envíe fuera de un puerto atado con alambre o se envíe a otro SSID. En ambos casos, usted puede configurar las correspondencias de políticas que definen el ancho de banda afectado un aparato a cada tipo de tráfico. La directiva diferenciará probablemente basado encendido si el tráfico está enviado fuera de un puerto atado con alambre o a otro SSID.

En la dirección ascendente, su problema principal es decidir a la prioridad, no el ancho de banda. Es decir su directiva-mapa por aguas arriba no afecta un aparato el ancho de banda a cada tipo de tráfico. Porque el tráfico está ya en el AP y ha cruzado ya el embotellamiento formado por el espacio inalámbrico semidúplex, su meta es traer este tráfico a la función del controlador del Catalyst 3850 Switch o el WLC de Cisco 5760 para el procesamiento adicional. Cuando el tráfico se recoge en el nivel AP, usted puede decidir si usted confía en la marca existente potencial de QoS para dar prioridad a los flujos de tráfico enviados al regulador. En este ejemplo, los valores existentes DSCP pueden ser confiados en:

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

Una vez que se crean sus directivas, aplique las correspondencias de políticas a la red inalámbrica (WLAN). En este ejemplo, se espera que se requiere cualquier dispositivo que conecte con la red inalámbrica (WLAN) soporte WMM, así que WMM.

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

Paso 4: Limitación de la llamada con el CAC

El paso más reciente es adaptar el CAC a su situación específica. En la configuración CAC explicada en el [paso 3: La Administración del ancho de banda y de la prioridad en el nivel SSID](#), el AP cae cualquier paquetes de voz que exceda el ancho de banda afectado un aparato.

Para evitar el máximo del ancho de banda., usted también necesita configurar el WCM para reconocer las llamadas se ponen que y las llamadas que harán el ancho de banda ser excedidas. Algunos teléfonos soportan la especificación del tráfico WMM (TSPEC) e informan a la infraestructura de red inalámbrica el ancho de banda que se espera que la llamada proyectada consuma. El WCM puede entonces rechazar la llamada antes de que se coloque.

Algunos teléfonos del SORBO no soportan TSPEC, pero el WCM y el AP se pueden fijar para reconocer los paquetes de la iniciación de llamada enviados PARA SORBER los puertos y

pueden utilizar esta información para establecer que una llamada del SORBO está a punto de ser colocada. Porque el teléfono SIP no especifica el ancho de banda que debe ser consumido por la llamada, el administrador debe determinar el ancho de banda previsto, sobre la base del codificador-decodificador, el tiempo del muestreo, etc.

El CAC calcula el ancho de banda consumido en cada nivel AP. El CAC se puede fijar para utilizar solamente el consumo de ancho de banda del cliente en sus cálculos (CAC estático) o también para considerar los AP vecinos y los dispositivos en el mismo canal (CAC carga-basado). Cisco recomienda que usted utiliza el CAC estático para los teléfonos del SORBO y el CAC carga-basado para los teléfonos TSPEC.

Finalmente, observe que el CAC está activado en a por la base de la banda.

En este ejemplo, el SORBO del uso de los teléfonos bastante que TSPEC para su inicio de sesión, cada llamada utiliza 64 kbps para cada dirección de la secuencia, se inhabilita el CAC carga-basado cuando se habilita el CAC estático, y el 75% de cada ancho de banda AP máximo se afecta un aparato al tráfico de voz:

```
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
```

Usted puede relanzar la misma configuración para la banda 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
```

Una vez que el CAC es aplicado para cada banda, usted también necesita aplicar el SORBO CAC en el nivel de la red inalámbrica (WLAN). Este proceso permite al AP para examinar la información de la capa 4 (L4) del tráfico del cliente de red inalámbrica para identificar las interrogaciones enviadas al UDP 5060 que indican los intentos de llamada del SORBO. TSPEC actúa en el nivel del 802.11 y es detectado nativo por los AP. Los teléfonos del SORBO no utilizan TSPEC, así que el AP tiene que realizar una inspección de paquetes más profunda para identificar el tráfico del SORBO. Porque usted no quisiera que el AP realizara este examen en todos los SSID, usted necesita determinar qué SSID cuentan con el tráfico SIP. Usted puede entonces permitir al snooping de la llamada en esos SSID para buscar las llamadas de voz. Usted puede también determinar qué acción a realizarse si una llamada SIP tiene que ser rechazada - desasocie al cliente SIP o envíe un mensaje ocupado SIP.

En este ejemplo, se habilita el snooping de la llamada, y se envía un mensaje ocupado si la llamada SIP tiene que ser rechazada. Con la adición del política de calidad de servicio (QoS) del [paso 3: La Administración del ancho de banda y de la prioridad en el nivel SSID](#), esto es la configuración SSID para la red inalámbrica (WLAN) del ejemplo:

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

Verificación

Utilice estos comandos para confirmar que su configuración de QoS trabaja correctamente.

Notas:

Use la [Command Lookup Tool \(clientes registrados solamente\)](#) para obtener más información sobre los comandos usados en esta sección.

[La herramienta del Output Interpreter \(clientes registrados solamente\)](#) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

muestre el clase-mapa

Este comando visualiza el class-maps configurado en la plataforma:

```
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
```

muestre el directiva-mapa

Este comando visualiza las correspondencias de políticas configuradas en la plataforma:

```
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

```

muestre wlan

Este comando visualiza los parámetros de la configuración y de la servicio-directiva de la red inalámbrica (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

Este comando visualiza el directiva-mapa instalado para una interfaz específica:

```
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

```

muestre las directivas de los qos de la plataforma

Este comando visualiza las directivas de QoS instaladas para los puertos, las radios AP, los SSID, y los clientes. Note que usted puede verificar, pero no puede cambiar, las directivas de radio:

3850#show platform qos policies PORT

Loc	Interface	IIF-ID	Dir	Policy	State
L:0	Gil/0/20	0x01023f4000000033	OUT	defportangn	INSTALLED IN HW
L:0	Gil/0/20	0x01023f4000000033	OUT	port_child_policy	INSTALLED IN HW

3850#show platform qos policies RADIO

Loc	Interface	IIF-ID	Dir	Policy	State
L:0	R56356842871193604	0x00c8384000000004	OUT	def-1lan	INSTALLED IN HW
L:0	R68373680329064451	0x00f2e98000000003	OUT	def-1lgn	INSTALLED IN HW

3850#show platform qos policies SSID

Loc	Interface	IIF-ID	Dir	Policy	State
L:0	S70706569125298203	0x00fb33400000001b	OUT	SSIDout_child_policy	INSTALLED IN HW
L:0	S69318160817324057	0x00f6448000000019	OUT	SSIDout_child_policy	INSTALLED 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

muestre la servicio-directiva del <mac> del MAC address del cliente de red inalámbrica

Este comando visualiza las correspondencias de políticas aplicadas en el nivel del cliente:

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

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.