Ejemplo de Configuración de QoS en Controladores de Acceso Convergentes y AP Ligeros

Contenido

Introducción

Este documento describe cómo configurar QoS en una red de acceso convergente de Cisco con Lightweight Access Points (LAP) y con el switch Cisco Catalyst 3850 o el controlador Cisco 5760 Wireless LAN Controller (WLC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos sobre cómo configurar los LAP y los controladores de acceso convergentes de Cisco
- Conocimiento de cómo configurar el ruteo básico y la QoS en una red por cable

Componentes Utilizados

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

- ¿El switch Cisco Catalyst 3850 que ejecuta Cisco IOS? Versión de software XE 3.2.2(SE)
- Controlador de LAN inalámbrica Cisco 5760 que ejecuta Cisco IOS XE Software Release 3.2.2(SE)
- Puntos de acceso ligeros Cisco serie 3600

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

QoS se refiere a la capacidad de la red para proporcionar un servicio mejor o especial a un conjunto de usuarios o aplicaciones en detrimento de otros usuarios o aplicaciones.

Con QoS, el ancho de banda se puede gestionar de forma más eficaz en las LAN, lo que incluye LAN inalámbricas (WLAN) y WAN. QoS proporciona un servicio de red mejorado y fiable con estos servicios:

- Admite ancho de banda dedicado para aplicaciones y usuarios críticos.
- Controla la fluctuación y la latencia que requiere el tráfico en tiempo real.
- Administra y minimiza la congestión de la red.
- Configura el tráfico de red para suavizar el flujo del tráfico.
- Establece las prioridades de tráfico de red.

En el pasado, las WLAN se utilizaban principalmente para transportar tráfico de aplicaciones de datos de ancho de banda bajo. Con la expansión de las WLAN en entornos verticales (como el comercio minorista, las finanzas y la educación) y empresariales, las WLAN se utilizan ahora para transportar aplicaciones de datos de gran ancho de banda junto con aplicaciones multimedia urgentes. Este requisito condujo a la necesidad de QoS inalámbrica.

El grupo de trabajo IEEE 802.11e dentro del comité de estándares IEEE 802.11 ha completado la definición estándar, y Wi-Fi Alliance ha creado la certificación Wi-Fi Multimedia (WMM), pero la adopción del estándar 802.11e sigue siendo limitada. La mayoría de los dispositivos cuentan con la certificación WMM, ya que la certificación WMM es necesaria para las certificaciones 802.11n y 802.11ac. Muchos dispositivos inalámbricos no asignan diferentes niveles de QoS a los paquetes enviados a la capa de enlace de datos, por lo que estos dispositivos envían la mayor parte de su tráfico sin marcación de QoS ni asignación de prioridad relativa. Sin embargo, la mayoría de los

teléfonos IP de voz sobre LAN inalámbrica (VoWLAN) 802.11 marcan y priorizan el tráfico de voz. Este documento se centra en la configuración de QoS para teléfonos IP VoWLAN y en dispositivos wi-fi compatibles con vídeo que marcan su tráfico de voz.

> **Nota:** La configuración de QoS para dispositivos que no realizan marcación interna está fuera del alcance de este documento.

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

- Platinum/Voice (UP 7 y 6): garantiza una alta calidad de servicio para voz sobre tecnología inalámbrica.
- Gold/Video (UP 5 y 4): admite aplicaciones de vídeo de alta calidad.
- Silver/Best Effort (UP 3 y 0): admite ancho de banda normal para los clientes. Esta es la configuración predeterminada.
- Bronze/Background (UP 2 y 1): proporciona el ancho de banda más bajo para los servicios de invitados.

Platinum se utiliza habitualmente para clientes VoIP y Gold para clientes de vídeo. Este documento proporciona un ejemplo de configuración que ilustra cómo configurar QoS en los controladores y comunicarse con una red por cable configurada con QoS para los clientes de vídeo y VoWLAN.

Mejoras en la Marcación de Paquetes QoS L3

Los controladores de acceso convergente de Cisco admiten la marcación de punto de código de servicios diferenciados (DSCP) IP de capa 3 (L3) de los paquetes enviados por WLC y LAP. Esta función mejora el modo en que los puntos de acceso (AP) utilizan esta información de L3 para garantizar que los paquetes reciban la prioridad sobre el aire correcta del AP al cliente inalámbrico.

En una arquitectura WLAN de acceso convergente que utiliza switches Catalyst 3850 como controladores inalámbricos, los AP se conectan directamente al switch. En una arquitectura WLAN de acceso convergente que utiliza controladores 5760, los datos de WLAN se tunelizan entre el AP y el WLC a través del protocolo de control y aprovisionamiento de puntos de acceso inalámbricos (CAPWAP). Para mantener la clasificación de QoS original a través de este túnel, la configuración de QoS del paquete de datos encapsulado se debe asignar apropiadamente a los campos de Capa 2 (L2) (802.1p) y L3 (IP DSCP) del paquete de túnel externo.

Al configurar QoS para VoWLAN y vídeo, puede configurar una política de QoS específica para clientes inalámbricos y una política específica para una WLAN, o ambas. También puede complementar la configuración con una configuración específica del puerto que enlaza el AP, especialmente con los switches Catalyst 3850. Este ejemplo de configuración se centra en la configuración de QoS para el cliente inalámbrico, la WLAN y el puerto al AP. Los objetivos principales de una configuración de QoS para aplicaciones de vídeo y VoWLAN son:

- Reconocer el tráfico de voz y vídeo (clasificación y marcación del tráfico), tanto ascendente como descendente.
- Marcar el tráfico de voz y vídeo con un nivel de prioridad de voz: 802.11e UP 6, 802.1p 5, DSCP 46 para voz.802.11e UP 5, DSCP 34 para vídeo.

- Asigne ancho de banda para tráfico de voz, señalización de voz y tráfico de vídeo.

Configuración de la red inalámbrica para QoS con MQC

Antes de configurar QoS, debe configurar la función Wireless Controller Module (WCM) del switch Catalyst 3850 o del WLC Cisco 5760 para el funcionamiento básico y registrar los LAP en el WCM. Este documento asume que el WCM está configurado para el funcionamiento básico y que los LAPs están registrados en el WCM.

La solución de acceso convergente utiliza la interfaz de línea de comandos (CLI) de QoS modular (MQC). Consulte Guía de Configuración de QoS, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) para obtener información adicional sobre el uso de MQC en la configuración de QoS en el switch Catalyst 3850.

La configuración de QoS con MQC en los controladores de acceso convergentes se basa en cuatro elementos:

- **Los mapas de clase** se utilizan para reconocer el tráfico de interés. Los mapas de clase pueden utilizar diversas técnicas (como el marcado de QoS existente, listas de acceso o VLAN) para identificar el tráfico de interés.
- **Los mapas de políticas** se utilizan para determinar qué configuración de QoS se debe aplicar al tráfico de interés. Los mapas de políticas asignan las clases y aplican diversas configuraciones de QoS (como marcado específico, niveles de prioridad, asignación de ancho de banda, etc.) a cada clase.
- **Las políticas de servicio** se utilizan para aplicar mapas de políticas a puntos estratégicos de su red. En la solución de acceso convergente, las políticas de servicio se pueden aplicar a los usuarios, los identificadores de conjunto de servicios (SSID), las radios AP y los puertos. El usuario puede configurar las políticas de puerto, SSID y cliente. Las políticas de radio se controlan mediante el módulo de control inalámbrico. Las políticas de QoS inalámbrica para puerto, SSID, cliente y radio se aplican en la dirección descendente cuando el tráfico fluye del switch o controlador a los clientes inalámbricos.
- **Los mapas de tabla** se utilizan para examinar la marcación de QoS entrante y para decidir las marcas de QoS saliente. Los mapas de tabla se colocan en mapas de políticas aplicados a los SSID. Los mapas de tabla se pueden utilizar para guardar (copiar) o cambiar el marcado. Los mapas de tabla también se pueden utilizar para crear un mapping entre el marcado por cable e inalámbrico. La marcación por cable utiliza DSCP (QoS L3) u 802.1p (QoS L2). El marcado inalámbrico utiliza la prioridad de usuario (UP). Los mapas de tabla se utilizan comúnmente para determinar qué marcado DSCP debe utilizarse para cada UP de interés y qué UP debe utilizarse para cada valor DSCP de interés. Los mapas de tabla son fundamentales para la QoS de acceso convergente porque no hay traducción directa entre los valores DSCP y UP.

Sin embargo, los mapas de tabla DSCP a UP también permiten la instrucción *copy*. En ese caso, la solución de acceso convergente utiliza la tabla de asignación de la arquitectura de Cisco para voz, vídeo y datos integrados (AVVID) para determinar el DSCP a la traducción UP o UP a DSCP:

Índice de etiquetas	Campo Clave	Valor entrante	DSCP externo	CoS	EN FUNCIONAMIENTO
0	N.A.	No activado	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

Políticas predeterminadas codificadas por hardware

Los controladores de acceso convergente embarcan perfiles de política de QoS codificados que se pueden aplicar a las WLAN. Estos perfiles aplican las políticas de metal (platino, oro, etc.) que conocen los administradores de los controladores de redes inalámbricas unificadas de Cisco (CUWN). Si su objetivo no es crear políticas que asignen ancho de banda específico al tráfico de voz, sino simplemente asegurarse de que el tráfico de voz reciba la marca de QoS adecuada, puede utilizar las políticas codificadas. Las políticas codificadas pueden aplicarse a la WLAN y pueden ser diferentes en las direcciones ascendente y descendente.

Notas:

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

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

Platino

La política codificada para voz se denomina platinum. No se puede cambiar el nombre.

Esta es la política de flujo descendente para el nivel QoS de 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
```

Esta es la política ascendente para el nivel QoS de Platinum:

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

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

Gold

La política codificada para vídeo se denomina gold. No se puede cambiar el nombre.

Esta es la política de flujo descendente para el nivel de QoS Gold:

```
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
```

Esta es la política ascendente para el nivel de QoS Gold:

```
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 política codificada para el mejor esfuerzo se llama plata. No se puede cambiar el nombre.

Esta es la política de flujo descendente para el nivel de QoS plateado:

```
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
```

Esta es la política ascendente para el nivel de QoS plateado:

```
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 política codificada para el tráfico en segundo plano se denomina bronce. No se puede cambiar el nombre.

Esta es la política de flujo descendente para el nivel de QoS de bronce:

```
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
```

Esta es la política ascendente para el nivel de QoS de bronce:

```
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 haya decidido qué mapa de tabla coincide mejor con el tráfico de destino para un SSID determinado, puede aplicar la política correspondiente a su WLAN. En este ejemplo, una política se aplica en la dirección descendente (salida del AP al cliente inalámbrico) y una política se aplica en la dirección ascendente (entrada, desde el cliente inalámbrico, a través del AP, al controlador):

```
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#
```

Verifique la configuración de WLAN para verificar qué política se aplicó a su 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 manual

Las políticas codificadas aplican la marcación de QoS predeterminada pero no aplican la asignación de ancho de banda. Las políticas codificadas también asumen que su tráfico ya está marcado. En un entorno complejo, es posible que desee utilizar una combinación de políticas para reconocer y marcar el tráfico de voz y vídeo de forma adecuada, establecer la asignación de ancho de banda en las direcciones descendente y ascendente y utilizar el control de admisión de llamadas para limitar el número de llamadas iniciadas desde la celda 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 Marcado del Tráfico de Voz

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

- Flujo de voz, que transporta la parte de audio de la comunicación.
- Señalización de voz, que transporta información estadística intercambiada entre terminales de voz.

El flujo de voz suele utilizar puertos de destino de protocolo de transporte en tiempo real (RTP) y protocolo de datagramas de usuario (UDP) en el intervalo de 16384 a 32767. Este es el rango; los puertos reales suelen ser más estrechos y dependen de la implementación.

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

- TCP 80 (HTTP)
- 143 (protocolo de acceso a mensajes de Internet [IMAP])
- 443 (HTTPS)
- 993 (IMAP) para servicios como Cisco Unified MeetingPlace o Cisco WebEx para reuniones y Cisco Unity o Cisco Unity Connection para funciones de correo de voz
- TCP 389/636 (servidor LDAP [protocolo ligero de acceso a directorios] para búsquedas de contactos)

- FTP (1080)
- TFTP (UDP 69) para la transferencia de archivos (como archivos de configuración) desde pares o desde el servidor

Es posible que estos servicios no necesiten una priorización específica.

Jabber utiliza el protocolo de inicio de sesión (SIP) (UDP/TCP 5060 y 5061) para la señalización de voz.

El tráfico de vídeo utiliza diferentes puertos y protocolos que dependen de su implementación. Este ejemplo de configuración utiliza una cámara Tandberg PrecisionHD 720p para videoconferencias. La cámara Tandberg PrecisionHD 720p puede utilizar varios códecs; el ancho de banda consumido depende del códec elegido:

- Los códecs C20, C40 y C60 utilizan H.323/SIP y pueden consumir hasta 6 Mbps en conexiones punto a punto.
- El códec C90 utiliza estos mismos protocolos y puede consumir hasta 10 Mbps en comunicaciones multisitio.

La implementación Tandberg de H.323 generalmente utiliza UDP 970 para transmisión de video, UDP 971 para señalización de video, UDP 972 para transmisión de audio y UDP 973 para señalización de audio. Las cámaras Tandberg también utilizan otros puertos, como:

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

Es posible que estos puertos adicionales no necesiten una priorización específica.

Una manera común de identificar el tráfico es crear mapas de clase que apunten al tráfico de interés. Cada class-map puede apuntar a una lista de acceso dirigida a cualquier tráfico que utilice los puertos de voz y vídeo:

```
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
```

A continuación, puede crear un mapa de clase para cada tipo de tráfico; cada class-map 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 se haya identificado el tráfico de voz y de vídeo a través de los class-maps, asegúrese de que el tráfico esté marcado correctamente. Esto se puede hacer a nivel de WLAN a través de los mapas de tabla y también se puede hacer a través de los mapas de políticas del cliente.

Los mapas de tabla examinan el marcado de QoS del tráfico entrante y determinan cuál debe ser el marcado de QoS saliente. Por lo tanto, los mapas de tabla son útiles cuando el tráfico entrante ya tiene marcado QoS. Los mapas de tabla se utilizan exclusivamente en el nivel SSID.

Por el contrario, los mapas de políticas pueden dirigirse al tráfico identificado por los mapas de clase y están mejor adaptados al tráfico potencialmente no etiquetado de interés. Este ejemplo de configuración asume que el tráfico del lado cableado ya se ha marcado correctamente antes de ingresar al switch Catalyst 3850 o al WLC Cisco 5760. Si no es así, puede utilizar un policy-map y aplicarlo en el nivel SSID como política de cliente. Dado que es posible que el tráfico de los clientes inalámbricos no se haya marcado, es necesario marcar correctamente el tráfico de voz y vídeo:

- La voz en tiempo real se debe marcar con DSCP 46 (Reenvío acelerado [EF]).
- El vídeo se debe marcar DSCP 34 (clase de reenvío garantizado 41 [AF41]).
- La señalización de voz y vídeo debe marcarse como DSCP 24 (Class Selector Service value 3 [CS3]).

Para aplicar estas marcas, cree un policy-map que llame a cada una 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
```

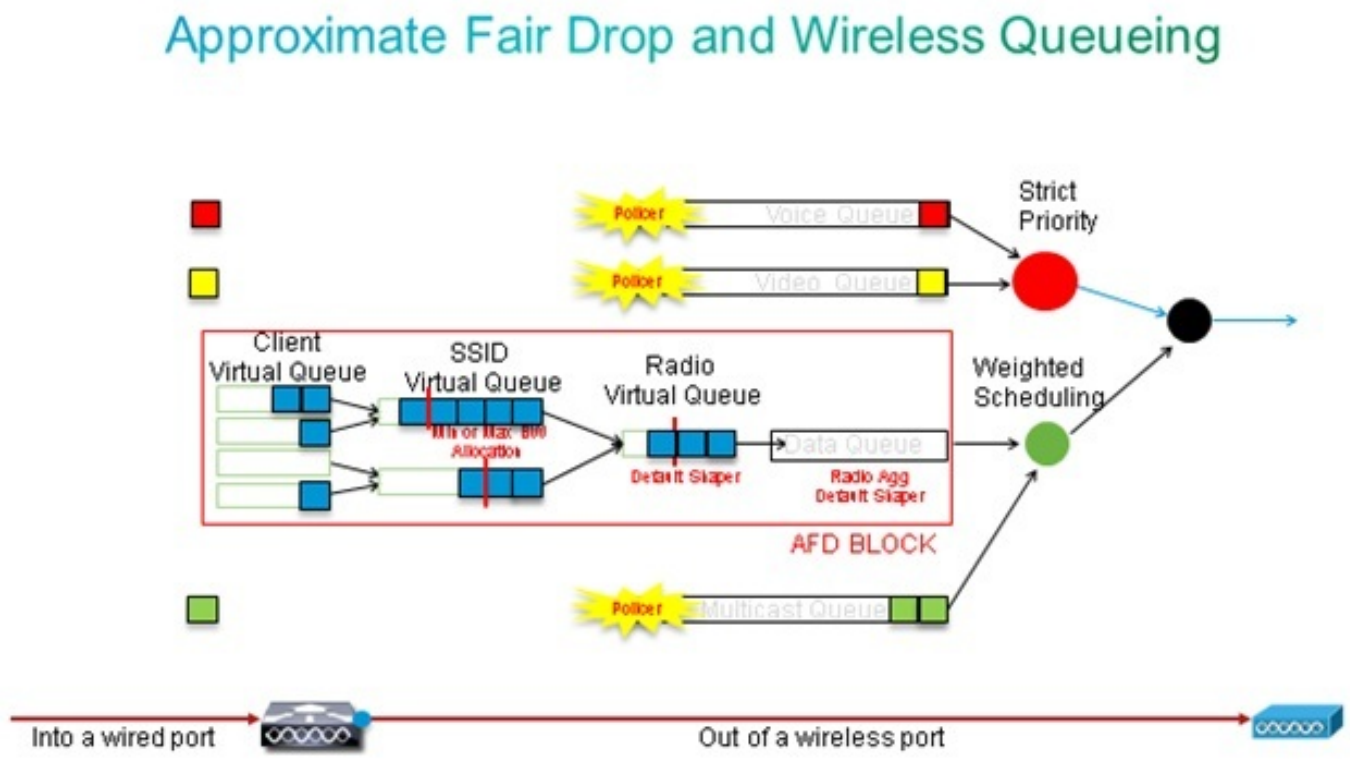
Paso 2: Administración de prioridad y ancho de banda en el nivel de puerto

El siguiente paso es determinar una política de QoS para los puertos que vienen y van a los AP. Este paso se aplica principalmente a los switches Catalyst 3850. Si su configuración se realiza en un controlador Cisco 5760, este paso no es obligatorio. Los puertos Catalyst 3850 transportan tráfico de voz y vídeo que llega o llega de clientes inalámbricos y AP. La configuración de QoS en este contexto coincide con dos requisitos:

1. **Asigne ancho de banda**. Puede decidir cuánta ancho de banda se asigna para cada tipo de tráfico. Esta asignación de ancho de banda también se puede realizar en el nivel SSID. Configure la asignación de ancho de banda del puerto para refinar cuánto ancho de banda puede recibir cada AP que atiende el SSID de destino. Este ancho de banda debe configurarse para todos los SSID en el AP de destino. Este ejemplo de configuración

simplificado supone que hay solamente un SSID y un AP, por lo que la asignación de ancho de banda del puerto para voz y vídeo es la misma que la asignación de ancho de banda global para voz y vídeo en el nivel SSID. A cada tipo de tráfico se le asignan 6 Mbps y se controla para que no se exceda este ancho de banda asignado.

2. **Dar prioridad al tráfico**. El puerto tiene cuatro colas. Las dos primeras colas tienen prioridad y se reservan para el tráfico en tiempo real, normalmente de voz y vídeo, respectivamente. La cuarta cola está reservada para el tráfico multicast en tiempo no real y la tercera contiene el resto del tráfico. Con la lógica de cola de acceso convergente, el tráfico de cada cliente se asigna a una cola virtual, donde se puede configurar QoS. El resultado de la política de QoS del cliente se inyecta en la cola virtual SSID, donde también se puede configurar QoS. Dado que varios SSID pueden existir en una radio AP dada, el resultado de cada SSID que está presente en una radio AP se inyecta en la cola virtual de radio AP, donde el tráfico se modela según la capacidad de radio. El tráfico se puede retrasar o descartar en cualquiera de estas etapas mediante el uso de un mecanismo de QoS denominado Aproximate Fair Drop (AFD). El resultado de esta política se envía luego al puerto AP (llamado puerto inalámbrico), donde se da prioridad a las dos primeras colas (hasta una cantidad configurable de ancho de banda), y luego a las colas tercera y cuarta como se describe anteriormente en este párrafo.



Este ejemplo de configuración coloca la voz en la primera cola prioritaria y el vídeo en la segunda cola de prioridad mediante el uso del comando **priority level**. El resto del tráfico se asigna al resto del ancho de banda del puerto.

Observe que no puede utilizar mapas de clase que dirijan el tráfico basado en listas de control de acceso (ACL). Las políticas aplicadas en el nivel de puerto pueden dirigir el tráfico basado en class-maps, pero estos class-maps deben apuntar al tráfico identificado por su valor de QoS. Una vez que haya identificado el tráfico basado en las ACL y marcado este tráfico correctamente en el nivel de SSID del cliente, sería redundante realizar una segunda inspección profunda del mismo tráfico en el nivel del puerto. Cuando el tráfico alcanza el puerto que va al AP, ya se marca

correctamente.

En este ejemplo, reutiliza los class-maps generales creados para la política SSID y dirige directamente el tráfico RTP de voz y el tráfico de vídeo en tiempo real:

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

Una vez identificado el tráfico de interés, puede decidir qué política aplicar. La política predeterminada (denominada parent_port) se aplica automáticamente en cada puerto cuando se detecta un AP. No debe cambiar este valor predeterminado, que se establece como:

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

Debido a que la política predeterminada parent_port llama a port_child_policy, una opción es editar la política_secundaria_de_puerto. (No debe cambiar su nombre). Esta política secundaria determina qué tráfico debe ir en cada cola y cuánto ancho de banda debe asignarse. La primera cola tiene la prioridad más alta, la segunda cola tiene la segunda prioridad más alta, y así sucesivamente. Estas dos colas están reservadas para el tráfico en tiempo real. La cuarta cola se utiliza para el tráfico multicast en tiempo no real. La tercera cola contiene el resto del tráfico.

En este ejemplo, decide asignar el tráfico de voz a la primera cola y el tráfico de vídeo a la segunda cola y asignar 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 política, la instrucción priority asociada a las clases 'voice' y 'video and signaling' permite asignar ese tráfico a la cola de prioridad pertinente. Observe, sin embargo, que las sentencias police rate percent se aplican solamente al tráfico multicast, no unicast.

No necesita aplicar esta política en el nivel del puerto porque se aplica automáticamente en cuanto se detecta un AP.

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

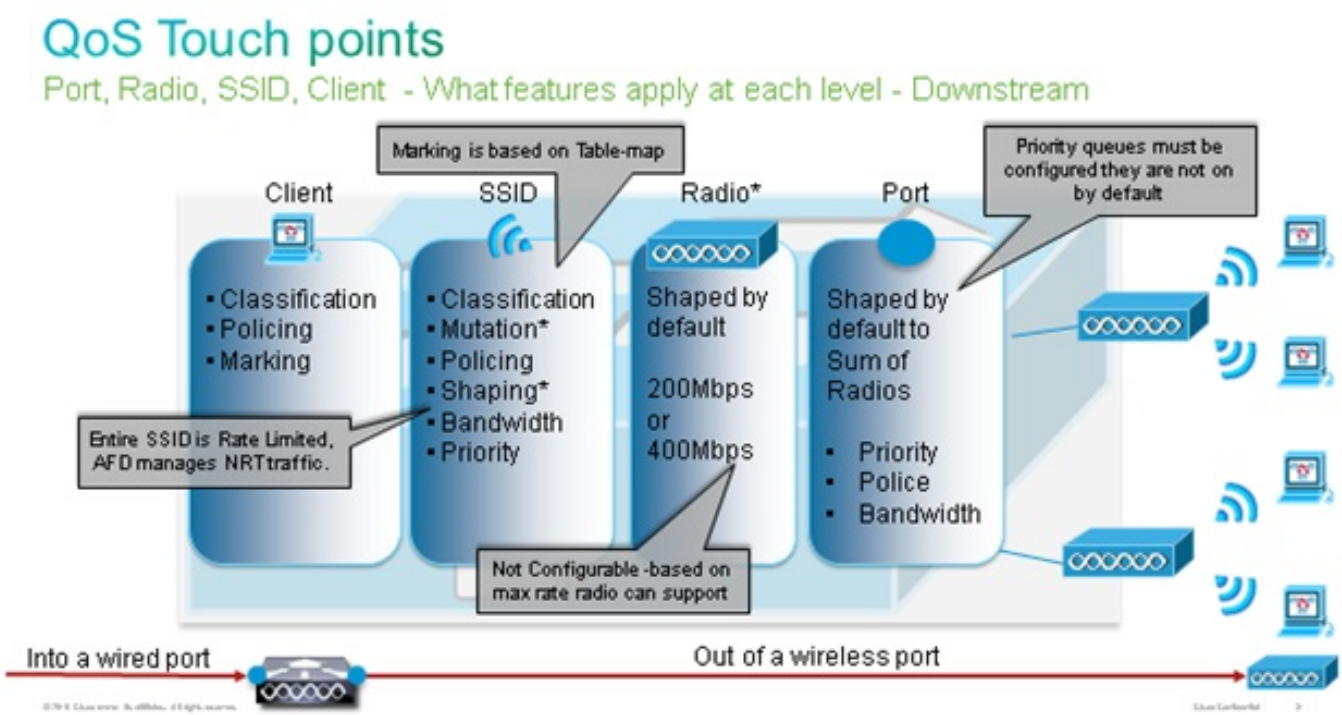
El siguiente paso es ocuparse de la política de QoS en el nivel SSID. Este paso se aplica tanto al switch Catalyst 3850 como al controlador 5760. Esta configuración asume que el tráfico de voz y vídeo se identifica mediante el uso de class-map y listas de acceso y se etiqueta correctamente. Sin embargo, es posible que el tráfico entrante que no está dirigido por la lista de acceso no muestre su marcado de QoS. En ese caso, puede decidir si este tráfico se debe marcar con un valor predeterminado o si se debe dejar sin etiquetar. La misma lógica se aplica al tráfico ya marcado pero no dirigido por los class-maps. Utilice la instrucción *copy predeterminada* en un table-map para asegurarse de que el tráfico no marcado se deje sin marcar y que el tráfico etiquetado mantenga la etiqueta y no se remarque.

Los mapas de tabla deciden el valor DSCP saliente pero también se utilizan para crear una trama 802.11 para decidir el valor UP de trama.

En este ejemplo, el tráfico entrante que muestra el nivel de QoS de voz (DSCP 46) mantiene su valor DSCP y el valor se asigna al marcado 802.11 equivalente (UP 6). El tráfico entrante que muestra el nivel de QoS de vídeo (DSCP 34) mantiene su valor DSCP y el valor se asigna al marcado 802.11 equivalente (UP 5). Del mismo modo, el tráfico marcado con DSCP 24 puede ser la señalización de voz; el valor DSCP debe mantenerse y traducirse al 802.11 UP 3:

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

El marcado también se puede realizar en el nivel de puerto por cable entrante. Esta figura muestra las acciones de QoS que se pueden realizar a medida que el tráfico pasa de una red por cable a una red inalámbrica:



Este ejemplo de configuración se centra en el aspecto inalámbrico de la configuración de QoS y

marca el tráfico en el nivel de cliente inalámbrico. Una vez completada la parte de marcado, debe asignar ancho de banda; aquí, se asignan 6 Mbps de ancho de banda a los flujos de tráfico de voz. (Aunque esta es la asignación de ancho de banda general para voz, cada llamada consumiría menos, por ejemplo, 128 kbps.) Este ancho de banda se asigna con el comando **police** para reservar el ancho de banda y descartar el tráfico en exceso.

El tráfico de vídeo también se asigna a 6 Mbps y se controla. Este ejemplo de configuración asume que hay sólo un flujo de vídeo.

La parte de señalización del tráfico de voz y vídeo también debe asignarse al ancho de banda. Hay dos estrategias posibles.

- Utilice el comando **shape promedio**, que permite almacenar en búfer el tráfico en exceso y enviarlo más tarde. Esta lógica no es eficiente para el flujo de voz o vídeo en sí mismo porque estos flujos requieren un retraso y fluctuación consistentes; sin embargo, puede ser eficiente para la señalización porque la señalización puede retrasarse ligeramente sin afectar a la calidad de la llamada. En la solución de acceso convergente, los comandos shape no aceptan lo que se denomina "configuraciones de bloques", que determinan cuánto tráfico que excede el ancho de banda asignado se puede almacenar en búfer. Por lo tanto, se debe agregar un segundo comando, **queue-buffers ratio 0**, para especificar que el tamaño de la cubeta sea 0. Si se incluye la señalización en el resto del tráfico y se utilizan comandos shape, el tráfico de señalización podría perderse en momentos de alta congestión. Esto, a su vez, podría hacer que la llamada se pierda porque cualquiera de los extremos determina que la comunicación ya no se está produciendo.
- Para evitar el riesgo de llamadas perdidas, puede incluir la señalización en una de las colas de prioridad. Este ejemplo de configuración definió previamente las colas de prioridad como voz y vídeo y ahora agrega señalización a la cola de vídeo.

La política utiliza el control de admisión de llamadas (CAC) para el flujo de voz. CAC se dirige al tráfico inalámbrico y coincide con una UP específica (en este ejemplo de configuración, UP 6 y 7). A continuación, CAC determina la cantidad máxima de ancho de banda que debe utilizar este tráfico. En una configuración en la que se controla el tráfico de voz, a CAC se le debe asignar un subconjunto de la cantidad total de ancho de banda asignado para voz. Por ejemplo, si la voz se controla a 6 Mbps, CAC no puede exceder los 6 Mbps. CAC se configura en un policy-map (denominado política secundaria) que se integra en el policy map descendente principal (denominado política primaria). CAC se introduce con el comando **allow cac wmm-tspec**, seguido por los UPs de destino y el ancho de banda asignado al tráfico de destino.

Cada llamada no consume todo el ancho de banda asignado a la voz. Por ejemplo, cada llamada puede consumir 64 kbps cada forma, lo que da como resultado 128 kbps de consumo de ancho de banda bidireccional efectivo. La instrucción de velocidad determina cada consumo de ancho de banda de llamada, mientras que la instrucción police determina el ancho de banda total asignado al tráfico de voz. Si todas las llamadas que se producen dentro de la celda utilizan un ancho de banda cercano al máximo permitido, se denegará cualquier llamada nueva que se inicie desde dentro de la celda y que haga que el ancho de banda consumido exceda el ancho de banda máximo permitido para la voz. Puede ajustar con precisión este proceso mediante la configuración de CAC en el nivel de banda, como se explica en el Paso 4: Limitación de llamada con CAC.

Por lo tanto, debe configurar una política secundaria que contenga las instrucciones CAC y que se integre en la política de flujo descendente principal. CAC no está configurado en el policy-map ascendente. CAC se aplica a las llamadas de voz iniciadas desde la celda, pero, como es una

respuesta a esas llamadas, CAC se configura solamente en el policy-map descendente. El policy-map ascendente será diferente. No puede utilizar los class-maps creados previamente porque estos class-maps tienen el tráfico de destino basado en una ACL. El tráfico inyectado en la política SSID ya pasó por la política del cliente, por lo que no debería realizar una inspección profunda en los paquetes por segunda vez. En su lugar, dirija el tráfico con una marca de QoS que resulta de la política del cliente.

Si decide no dejar la señalización en la clase predeterminada, también deberá priorizar la señalización.

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

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

La política secundaria de flujo descendente 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 primaria descendente 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 ascendente es el tráfico que proviene de los clientes inalámbricos y se envía al WCM antes de que el tráfico se envíe desde un puerto cableado o se envíe a otro SSID. En ambos casos, puede configurar mapas de políticas que definen el ancho de banda asignado a cada tipo de tráfico. La política probablemente difiera en función de si el tráfico se envía desde un puerto cableado o a otro SSID.

En la dirección ascendente, su principal preocupación es decidir la prioridad, no el ancho de banda. En otras palabras, su policy-map ascendente no asigna ancho de banda a cada tipo de tráfico. Debido a que el tráfico ya está en el AP y ya ha cruzado el cuello de botella formado por el espacio inalámbrico semidúplex, su objetivo es llevar este tráfico a la función de controlador del switch Catalyst 3850 o el WLC Cisco 5760 para un procesamiento adicional. Cuando el tráfico se recopila en el nivel AP, puede decidir si debe confiar en el marcado QoS existente potencial para

dar prioridad a los flujos de tráfico enviados al controlador. En este ejemplo, se puede confiar en los valores DSCP existentes:

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

Una vez creadas las políticas, aplique los mapas de políticas a la WLAN. En este ejemplo, se espera que cualquier dispositivo que se conecte a la WLAN admita WMM, por lo que se requiere WMM.

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

Paso 4: Limitación de llamadas con CAC

El último paso es adaptar el CAC a su situación específica. En la configuración de CAC explicada en el Paso 3: Administración de Prioridad y Ancho de Banda en el Nivel SSID, el AP descarta cualquier paquete de voz que exceda el ancho de banda asignado.

Para evitar el máximo de ancho de banda., también necesita configurar el WCM para reconocer las llamadas que se realizan y las que causarán que se exceda el ancho de banda. Algunos teléfonos admiten la especificación de tráfico WMM (TSPEC) e informan a la infraestructura inalámbrica del ancho de banda que se espera consuma la llamada proyectada. A continuación, WCM puede rechazar la llamada antes de que se realice.

Algunos teléfonos SIP no admiten TSPEC, pero el WCM y el AP pueden configurarse para reconocer los paquetes de inicio de llamada enviados a los puertos SIP y pueden utilizar esta información para establecer que se va a realizar una llamada SIP. Dado que el teléfono SIP no especifica el ancho de banda que debe consumir la llamada, el administrador debe determinar el ancho de banda esperado, en función del códec, el tiempo de muestreo, etc.

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

Por último, tenga en cuenta que CAC se activa por banda.

En este ejemplo, los teléfonos utilizan SIP en lugar de TSPEC para el inicio de la sesión, cada llamada utiliza 64 kbps para cada dirección de flujo, CAC basado en carga se inhabilita cuando CAC estático se habilita, y el 75% de cada ancho de banda de AP máximo se asigna 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
```

Puede repetir la misma configuración para la banda de 2,4 GHz:

```
ap dot11 24ghz shutdown
ap dot11 24ghz cac voice acm
no ap dot11 24ghz cac voice load-based
ap dot11 24ghz cac voice max-bandwidth 75
ap dot11 24ghz cac voice sip bandwidth 64
no ap dot11 24ghz shutdown
```

Una vez que CAC se aplica a cada banda, también debe aplicar SIP CAC en el nivel WLAN. Este proceso permite al AP examinar la información de capa 4 (L4) del tráfico del cliente inalámbrico para identificar las consultas enviadas a UDP 5060 que indican los intentos de llamada SIP. TSPEC funciona en el nivel 802.11 y es detectado nativamente por los AP. Los teléfonos SIP no utilizan TSPEC, por lo que el AP debe realizar una inspección de paquetes más profunda para identificar el tráfico SIP. Debido a que no desea que el AP realice esta inspección en todos los SSID, debe determinar qué SSID esperan tráfico SIP. A continuación, puede activar la detección de llamadas en esos SSID para buscar llamadas de voz. También puede determinar qué acción realizar si hay que rechazar una llamada SIP: anule la asociación del cliente SIP o envíe un mensaje de ocupado de SIP.

En este ejemplo, se habilita la indagación de llamadas y se envía un mensaje de ocupado si se tiene que rechazar la llamada SIP. Con la adición de la política de QoS del Paso 3: Administración de Prioridad y Ancho de Banda en el Nivel SSID, ésta es la configuración SSID para el ejemplo de WLAN:

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

Verificación

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

> **Notas:**
>
> Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.
>
> La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

show class-map

Este comando muestra los class-maps configurados 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
```

show policy-map

Este comando muestra los policy-maps configurados 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
```

show wlan

Este comando muestra la configuración de WLAN y los parámetros de política de servicio:

```
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 muestra el policy-map 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
```

show platform qos policies

Este comando muestra las políticas de QoS instaladas para los puertos, las radios AP, los SSID y los clientes. Observe que puede verificar, pero no puede cambiar, las políticas de radio:

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

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

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

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

Este comando muestra los policy-maps aplicados en el nivel de 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
```

Troubleshoot

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