Exemplo de configuração de QoS em controladores de acesso convergente e APs leves

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[Melhorias na marcação de pacotes de QoS L3](#)
[Configurar rede sem fio para QoS com MQC](#)
[Políticas padrão codificadas](#)
[Platinum](#)
[Gold](#)
[Prata](#)
[Bronze](#)
[Configurar manualmente](#)
[Passo 1: Identificação e marcação do tráfego de voz](#)
[Passo 2: Gerenciamento de largura de banda e prioridade no nível da porta](#)
[Passo 3: Gerenciamento de prioridade e largura de banda no nível de SSID](#)
[Passo 4: Limitação de chamada com CAC](#)
[Verificar](#)
[show class-map](#)
[show policy-map](#)
[show wlan](#)
[show policy-map interface](#)
[show platform qos policies](#)
[show wireless client mac-address <mac> service-policy](#)
[Troubleshoot](#)

Introduction

Este documento descreve como configurar a QoS em uma rede de acesso convergente da Cisco com Pontos de Acesso Lightweight (LAPs) e com o switch Cisco Catalyst 3850 ou o controlador de LAN sem fio (WLC) Cisco 5760.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico de como configurar LAPs e controladores de acesso convergente da Cisco
- Conhecimento de como configurar o roteamento básico e a QoS em uma rede com fio

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Switch Cisco Catalyst 3850 que executa o Cisco IOS? Software XE versão 3.2.2(SE)
- Controlador de LAN sem fio Cisco 5760 que executa o software Cisco IOS XE versão 3.2.2(SE)
- Pontos de acesso Lightweight Cisco 3600 Series

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.

Informações de Apoio

QoS refere-se à capacidade da rede de fornecer serviços melhores ou especiais a um conjunto de usuários ou aplicativos em detrimento de outros usuários ou aplicativos.

Com a QoS, a largura de banda pode ser gerenciada de forma mais eficiente através das LANs, o que inclui LANs sem fio (WLANs) e WANs. A QoS oferece serviço de rede aprimorado e confiável com estes serviços:

- Suporta largura de banda dedicada para usuários e aplicativos críticos.
- Controla o jitter e a latência exigidos pelo tráfego em tempo real.
- Gerencia e minimiza o congestionamento da rede.
- Modela o tráfego de rede para suavizar o fluxo de tráfego.
- Define as prioridades do tráfego de rede.

Antigamente, as WLANs eram usadas principalmente para transportar tráfego de aplicações de dados de baixa largura de banda. Com a expansão das WLANs em ambientes verticais (como varejo, finanças e educação) e empresariais, as WLANs agora são usadas para transportar aplicativos de dados de alta largura de banda em conjunto com aplicativos multimídia sensíveis ao tempo. Esse requisito levou à necessidade de QoS sem fio.

O grupo de trabalho IEEE 802.11e no comitê de padrões IEEE 802.11 concluiu a definição padrão e a Wi-Fi Alliance criou a certificação Wi-Fi Multimedia (WMM), mas a adoção do padrão 802.11e ainda é limitada. A maioria dos dispositivos tem certificação WMM, pois a certificação WMM é necessária para as certificações 802.11n e 802.11ac. Muitos dispositivos sem fio não atribuem níveis de QoS diferentes aos pacotes enviados à camada de enlace de dados, de modo que esses dispositivos enviam a maior parte de seu tráfego sem marcação de QoS e sem priorização relativa. No entanto, a maioria dos telefones IP de voz sobre LAN sem fio (VoWLAN) 802.11 marcam e priorizam o tráfego de voz. Este documento concentra-se na configuração de QoS para

telefones IP VoWLAN e em dispositivos wi-fi com capacidade de vídeo que marcam seu tráfego de voz.

> **Note**: A configuração de QoS para dispositivos que não executam marcação interna está fora do escopo deste documento.

A emenda 802.11e define oito níveis de prioridade de usuário (UP), agrupados dois por dois em quatro níveis de QoS (categorias de acesso):

- Platinum/Voice (UP 7 e 6) - Garante uma alta qualidade de serviço para voz sobre conexão sem fio.
- Gold/Video (ATÉ 5 e 4) - Suporta aplicativos de vídeo de alta qualidade.
- Prata/melhor esforço (UP 3 e 0) - Suporta largura de banda normal para clientes. Essa é a configuração padrão.
- Bronze/plano de fundo (UP 2 e 1) - Fornece a menor largura de banda para serviços para convidados.

O Platinum é comumente usado para clientes VoIP e Gold para clientes de vídeo. Este documento fornece um exemplo de configuração que ilustra como configurar a QoS em controladores e se comunicar com uma rede com fio configurada com QoS para VoWLAN e clientes de vídeo.

Melhorias na marcação de pacotes de QoS L3

Os controladores de acesso convergido da Cisco suportam a marcação de Ponto de Código de Serviços Diferenciados (DSCP - Differentiated Services Code Point) de Camada 3 (L3 - Layer 3) de pacotes enviados por WLCs e LAPs. Esse recurso melhora o modo como os access points (APs) usam essas informações L3 para garantir que os pacotes recebam a priorização aérea correta do AP para o cliente sem fio.

Em uma arquitetura WLAN de acesso convergido que usa switches Catalyst 3850 como controladores sem fio, os APs se conectam diretamente ao switch. Em uma arquitetura de WLAN de acesso convergido que usa controladores 5760, os dados da WLAN são encapsulados entre o AP e a WLC através do protocolo de Controle e Provisionamento de Pontos de Acesso Sem Fio (CAPWAP - Wireless Access Points). Para manter a classificação de QoS original neste túnel, as configurações de QoS do pacote de dados encapsulado devem ser mapeadas adequadamente para os campos Camada 2 (L2) (802.1p) e L3 (IP DSCP) do pacote de túnel externo.

Ao configurar a QoS para VoWLAN e vídeo, você pode configurar uma política de QoS específica para clientes sem fio e uma política específica para uma WLAN, ou ambas. Você também pode complementar a configuração com uma configuração específica para a porta que conecta o AP, especialmente com os switches Catalyst 3850. Este exemplo de configuração concentra-se na configuração de QoS para o cliente sem fio, a WLAN e a porta para o AP. Os principais objetivos de uma configuração de QoS para VoWLAN e aplicativos de vídeo são:

- Reconhecer o tráfego de voz e vídeo (classificação e marcação de tráfego), tanto upstream como downstream.
- Marque o tráfego de voz e vídeo com um nível de prioridade de voz: 802.11e UP 6, 802.1p 5, DSCP 46 para voz.802.11e UP 5, DSCP 34 para vídeo.
- Alocar largura de banda para tráfego de voz, sinalização de voz e tráfego de vídeo.

Configurar rede sem fio para QoS com MQC

Antes de configurar a QoS, você deve configurar a função do Wireless Controller Module (WCM) do switch Catalyst 3850 ou Cisco 5760 WLC para operação básica e registrar os LAPs no WCM. Este documento pressupõe que o WCM está configurado para a operação básica e que os LAPs estão registrados no WCM.

A solução de acesso convergido usa a interface de linha de comando (CLI) de QoS modular (MQC). Consulte o Guia de Configuração de QoS, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) para obter informações adicionais sobre o uso de MQC na configuração de QoS no switch Catalyst 3850.

A configuração de QoS com MQC em controladores de acesso convergente depende de quatro elementos:

- **Mapas de classe** são usados para reconhecer o tráfego de interesse. Os mapas de classe podem usar várias técnicas (como marcação QoS existente, listas de acesso ou VLANs) para identificar o tráfego de interesse.
- **Os mapas de política** são usados para determinar quais configurações de QoS devem ser aplicadas ao tráfego de interesse. Os mapas de política chamam os mapas de classes e aplicam várias configurações de QoS (como marcação específica, níveis de prioridade, alocação de largura de banda, etc.) a cada classe.
- **Políticas de serviço** são usadas para aplicar mapas de políticas a pontos estratégicos de sua rede. Na solução de acesso convergido, as políticas de serviço podem ser aplicadas a usuários, identificadores de conjunto de serviços (SSIDs), rádios de AP e portas. As políticas de porta, SSID e cliente podem ser configuradas pelo usuário. As políticas de rádio são controladas pelo módulo de controle sem fio. As políticas de QoS sem fio para porta, SSID, cliente e rádio são aplicadas na direção de downstream quando o tráfego está fluindo do switch ou controlador para clientes sem fio.
- **Os mapas de tabela** são usados para examinar a marcação de QoS de entrada e para decidir as marcas de QoS de saída. Os mapas de tabelas são posicionados em mapas de políticas aplicados aos SSIDs. Os mapas de tabelas podem ser usados para manter (copiar) ou alterar a marcação. Os mapas de tabelas também podem ser usados para criar um mapeamento entre a marcação com e sem fio. A marcação com fio usa DSCP (L3 QoS) ou 802.1p (L2 QoS). A marcação sem fio usa UP (User Priority, Prioridade de usuário). Os mapas de tabela são comumente usados para determinar qual marcação DSCP deve ser usada para cada UP de interesse e qual UP deve ser usado para cada valor DSCP de interesse. Os mapas de tabela são fundamentais para a QoS de acesso convergido porque não há tradução direta entre os valores DSCP e UP.

No entanto, os mapas de tabela DSCP para UP também permitem a instrução *copy*. Nesse caso, a solução de acesso convergido usa a tabela de mapeamento da Cisco Architecture for Voice, Video, and Integrated Data (AVVID) para determinar a tradução de DSCP para UP ou UP para DSCP:

Índice de etiquetas	Campo chave	Valor recebido	DSCP externo	CoS	PARA CIMA
0	N.D.	Não verificado	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	PARA CIMA	0	0	0	0
74	PARA CIMA	1	8	1	1
75	PARA CIMA	2	16	1	2
76	PARA CIMA	3	24	2	3
77	PARA CIMA	4	34	3	4
78	PARA CIMA	5	34	4	5
79	PARA CIMA	6	46	5	6
80	PARA CIMA	7	46	7	7

Políticas padrão codificadas

Os controladores de acesso convergente embarcam em perfis de política de QoS codificada que podem ser aplicados às WLANs. Esses perfis aplicam as políticas de metal (platina, ouro e assim por diante) familiares aos administradores dos controladores Cisco Unified Wireless Networks (CUWN). Se seu objetivo não é criar políticas que atribuam largura de banda específica ao tráfego de voz, mas simplesmente garantir que o tráfego de voz receba a marcação de QoS apropriada, você pode usar as políticas codificadas. As políticas codificadas podem ser aplicadas à WLAN e podem ser diferentes nas direções upstream e downstream.

> **Notas:**
>
> Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.
>
> A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

Platinum

A política de voz codificada é chamada platina. O nome não pode ser alterado.

Esta é a política de downstream para o nível de QoS platina:

```
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 é a política de upstream para o nível de QoS Platinum:

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

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

Gold

A política de vídeo codificada é chamada de ouro. O nome não pode ser alterado.

Esta é a política de downstream para o nível de QoS ouro:

```
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 é a política de upstream para o nível de QoS ouro:

```
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
```

Prata

A política programada para o melhor esforço chama-se prata. O nome não pode ser alterado.

Esta é a política de downstream para o nível de QoS prata:

```
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 é a política de upstream para o nível de QoS prata:

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

Bronze

A política codificada para o tráfego em segundo plano é chamada de bronze. O nome não pode ser alterado.

Esta é a política de downstream para o nível de QoS de bronze:

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

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

Table Map bronze-dscp2up
```

```
   from 0 to 1
   from 34 to 1
   from 45 to 1
   from 46 to 1
   from 47 to 1
   default copy
```

Esta é a política de upstream para o nível de QoS de bronze:

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

Depois de decidir qual mapa de tabela melhor corresponde ao tráfego de destino de um SSID específico, você pode aplicar a política correspondente à sua WLAN. Neste exemplo, uma política é aplicada na direção de downstream (saída, do AP para o cliente sem fio) e uma política é aplicada na direção de upstream (entrada, do cliente sem fio, através do AP, para o 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 a configuração da WLAN para verificar qual política foi aplicada à sua 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
```

Configurar manualmente

As políticas codificadas aplicam a marcação de QoS padrão, mas não aplicam a alocação de largura de banda. As políticas codificadas também assumem que o tráfego já está marcado. Em um ambiente complexo, você pode usar uma combinação de políticas para reconhecer e marcar o tráfego de voz e vídeo adequadamente, para definir a alocação de largura de banda nas direções downstream e upstream e para usar o controle de admissão de chamadas a fim limitar o número de chamadas iniciadas a partir da célula sem fio.

> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Passo 1: Identificação e marcação do tráfego de voz

A primeira etapa é reconhecer o tráfego de voz e vídeo. O tráfego de voz pode ser classificado em duas categorias:

- Fluxo de voz, que transporta a parte de áudio da comunicação.
- Sinalização de voz, que transporta informações estatísticas trocadas entre terminais de voz.

O fluxo de voz geralmente usa as portas de destino do Protocolo de Transporte em Tempo Real (RTP - Real-Time Transport Protocol) e do Protocolo de Datagrama do Usuário (UDP - User Datagram Protocol) no intervalo de 16384 a 32767. Este é o intervalo. as portas reais são geralmente mais estreitas e dependem da implementação.

Há vários protocolos de sinalização de voz. Este exemplo de configuração usa Jabber. O Jabber usa estas portas TCP para conexão e diretório:

- TCP 80 (HTTP)
- 143 (Internet Message Access Protocol [IMAP])
- 443 (HTTPS)
- 993 (IMAP) para serviços como o Cisco Unified MeetingPlace ou Cisco WebEx para reuniões e o Cisco Unity ou Cisco Unity Connection para recursos de correio de voz
- Servidor TCP 389/636 (Lightweight Diretory Access Protocol [LDAP] para pesquisas de contatos)
- FTP (1080)
- TFTP (UDP 69) para transferência de arquivos (como arquivos de configuração) de pares ou do servidor

Esses serviços podem não precisar de uma priorização específica.

O Jabber usa o Session Initiation Protocol (SIP) (UDP/TCP 5060 e 5061) para sinalização de voz.

O tráfego de vídeo usa diferentes portas e protocolos que dependem de sua implementação. Este exemplo de configuração usa uma câmera Tandberg PrecisionHD 720p para videoconferências. A câmera Tandberg PrecisionHD 720p pode usar vários codecs; a largura de banda consumida

depende do codec escolhido:

- Os codecs C20, C40 e C60 usam H.323/SIP e podem consumir até 6 Mbps em conexões ponto-a-ponto.
- O codec C90 usa esses mesmos protocolos e pode consumir até 10 Mbps em comunicações em vários locais.

A implementação Tandberg do H.323 geralmente usa o UDP 970 para transmissão de vídeo, o UDP 971 para sinalização de vídeo, o UDP 972 para transmissão de áudio e o UDP 973 para sinalização de áudio. As câmeras Tandberg também usam outras portas, como:

- UDP 161
- UDP 962 (Simple Network Management Protocol [SNMP])
- TCP 963 (netlog), TCP 964 (FTP)
- TCP 965 (Virtual Network Computing [VNC])
- UDP 974 (Session Announement Protocol [SAP])

Essas portas adicionais podem não precisar de uma priorização específica.

Uma maneira comum de identificar o tráfego é criar mapas de classe que direcionem o tráfego de interesse. Cada mapa de classe pode apontar para uma lista de acesso direcionada a qualquer tráfego que use as portas de voz e 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
```

Você pode criar um mapa de classe para cada tipo de tráfego; cada mapa de classe aponta para a lista de acesso 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
```

Depois que o tráfego de voz e vídeo tiver sido identificado por meio de mapas de classe, certifique-se de que o tráfego esteja marcado corretamente. Isso pode ser feito no nível da WLAN por meio de mapas de tabela e também pode ser feito por meio de mapas de políticas de clientes.

Os mapas de tabela examinam a marcação de QoS do tráfego de entrada e determinam o que deve ser a marcação de QoS de saída. Assim, os mapas de tabela são úteis quando o tráfego de entrada já tem marcação de QoS. Os mapas de tabela são usados exclusivamente no nível de

SSID.

Em contrapartida, os mapas de políticas podem direcionar o tráfego identificado por mapas de classe e são mais bem adaptados ao tráfego de interesse potencialmente não marcado. Este exemplo de configuração pressupõe que o tráfego do lado com fio já foi marcado corretamente antes de entrar no switch Catalyst 3850 ou no Cisco 5760 WLC. Se esse não for o caso, você pode usar um mapa de política e aplicá-lo no nível SSID como uma política de cliente. Como o tráfego de clientes sem fio pode não ter sido marcado, você precisa marcar o tráfego de voz e vídeo corretamente:

- A voz em tempo real deve ser marcada com DSCP 46 (Encaminhamento expresso [EF]).
- O vídeo deve estar marcado como DSCP 34 (Assured Forwarding Class 41 [AF41]).
- A sinalização de voz e vídeo deve ser marcada como DSCP 24 (Class Seletor Service value 3 [CS3]).

Para aplicar essas marcas, crie um mapa de políticas que chame cada uma dessas classes e marque o tráfego equivalente:

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

 class H323realtimevideo
 set dscp af41

 class signaling
 set dscp cs3
```

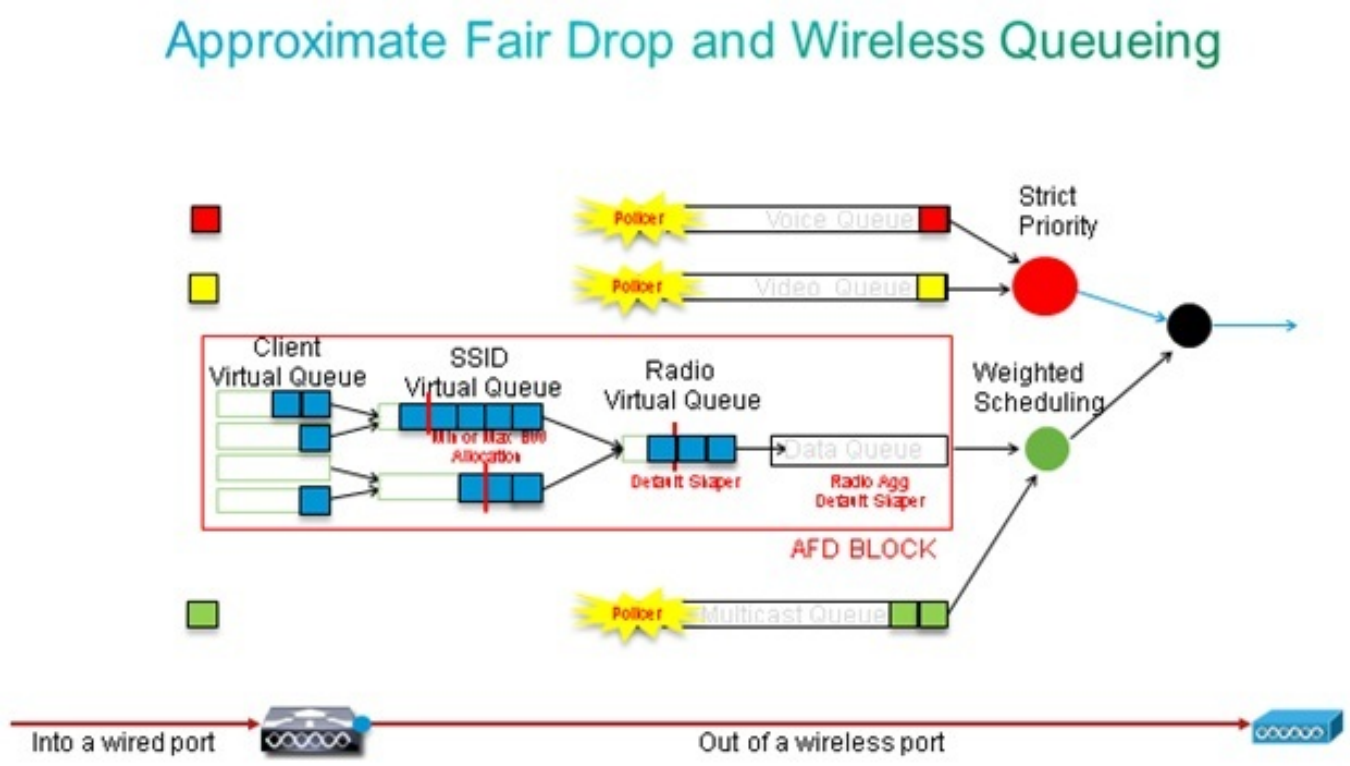
Passo 2: Gerenciamento de largura de banda e prioridade no nível da porta

A próxima etapa é determinar uma política de QoS para as portas que chegam e vão para os APs. Esta etapa se aplica principalmente aos switches Catalyst 3850. Se sua configuração for feita em um controlador Cisco 5760, esta etapa não é obrigatória. As portas Catalyst 3850 transportam tráfego de voz e vídeo que vai para ou vem de clientes e APs sem fio. A configuração de QoS neste contexto corresponde a dois requisitos:

1. Alocar largura de banda. Você pode decidir a quantidade de largura de banda alocada para cada tipo de tráfego. Essa alocação de largura de banda também pode ser feita no nível SSID. Defina a alocação de largura de banda da porta para refinar a quantidade de largura de banda que pode ser recebida por cada AP que atende ao SSID de destino. Essa largura de banda deve ser definida para todos os SSIDs no AP de destino. Este exemplo de configuração simplificado pressupõe que há apenas um SSID e um AP, de modo que a alocação de largura de banda de porta para voz e vídeo é a mesma alocação de largura de banda global para voz e vídeo no nível de SSID. Cada tipo de tráfego é alocado a 6 Mbps e é policiado de modo que essa largura de banda alocada não seja excedida.

2. Priorize o tráfego. A porta tem quatro filas. As duas primeiras filas são priorizadas e reservadas para tráfego em tempo real - geralmente voz e vídeo, respectivamente. A quarta fila é reservada para tráfego multicast não em tempo real e a terceira fila contém todo o tráfego restante. Com a lógica de enfileiramento de acesso convergente, o tráfego de cada cliente é atribuído a uma fila virtual, onde a QoS pode ser configurada. O resultado da política de QoS do cliente é injetado na fila virtual SSID, onde a QoS também pode ser

configurada. Como vários SSIDs podem existir em um determinado rádio AP, o resultado de cada SSID presente em um rádio AP é injetado na fila virtual de rádio do AP, onde o tráfego é modelado com base na capacidade de rádio. O tráfego pode ser atrasado ou descartado em qualquer um desses estágios pelo uso de um mecanismo de QoS chamado AFD (Aproximate Fair Drop, queda justa aproximada). O resultado dessa política é então enviado à porta do AP (chamada de porta sem fio), onde a prioridade é dada às duas primeiras filas (até uma quantidade configurável de largura de banda) e, em seguida, às terceira e quarta filas, conforme descrito anteriormente neste parágrafo.



Este exemplo de configuração coloca voz na primeira fila de prioridade e vídeo na segunda fila de prioridade por meio do uso do comando **priority level**. O restante do tráfego é alocado para o restante da largura de banda da porta.

Observe que você não pode usar mapas de classe que direcionam o tráfego com base nas listas de controle de acesso (ACLs). As políticas aplicadas no nível da porta podem direcionar o tráfego com base em mapas de classe, mas esses mapas de classe devem direcionar o tráfego identificado por seu valor de QoS. Depois de identificar o tráfego com base nas ACLs e marcar esse tráfego corretamente no nível de SSID do cliente, seria redundante executar uma segunda inspeção profunda desse mesmo tráfego no nível da porta. Quando o tráfego chega à porta que vai para o AP, ele já está marcado corretamente.

Neste exemplo, você reutiliza os mapas de classe gerais criados para a política de SSID e direciona diretamente o tráfego de RTP de voz e o tráfego de vídeo em tempo real:

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

Depois de identificar o tráfego de interesse, você pode decidir qual política aplicar. A política padrão (chamada parent_port) é aplicada automaticamente em cada porta quando um AP é

detectado. Você não deve alterar esse padrão, que é definido como:

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

Como a política pai_port padrão chama port_child_policy, uma opção é editar port_child_policy. (Você não deve alterar seu nome). Essa política filha determina qual tráfego deve ser enviado em cada fila e quanta largura de banda deve ser alocada. A primeira fila tem a prioridade mais alta, a segunda fila tem a segunda prioridade mais alta e assim por diante. Essas duas filas são reservadas para tráfego em tempo real. A quarta fila é usada para tráfego multicast não em tempo real. A terceira fila contém todo o tráfego restante.

Neste exemplo, você decide alocar tráfego de voz para a primeira fila e tráfego de vídeo para a segunda fila e alocar largura de banda para cada fila e para todos os outros tráfegos:

```
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
```

Nesta política, a instrução de prioridade associada às classes 'voz' e 'sinalização de vídeo' permite atribuir esse tráfego à fila de prioridade relevante. Observe, no entanto, que as instruções de porcentagem da taxa policial se aplicam apenas ao tráfego multicast, não unicast.

Você não precisa aplicar essa política no nível da porta porque ela é aplicada automaticamente assim que um AP é detectado.

Passo 3: Gerenciamento de prioridade e largura de banda no nível de SSID

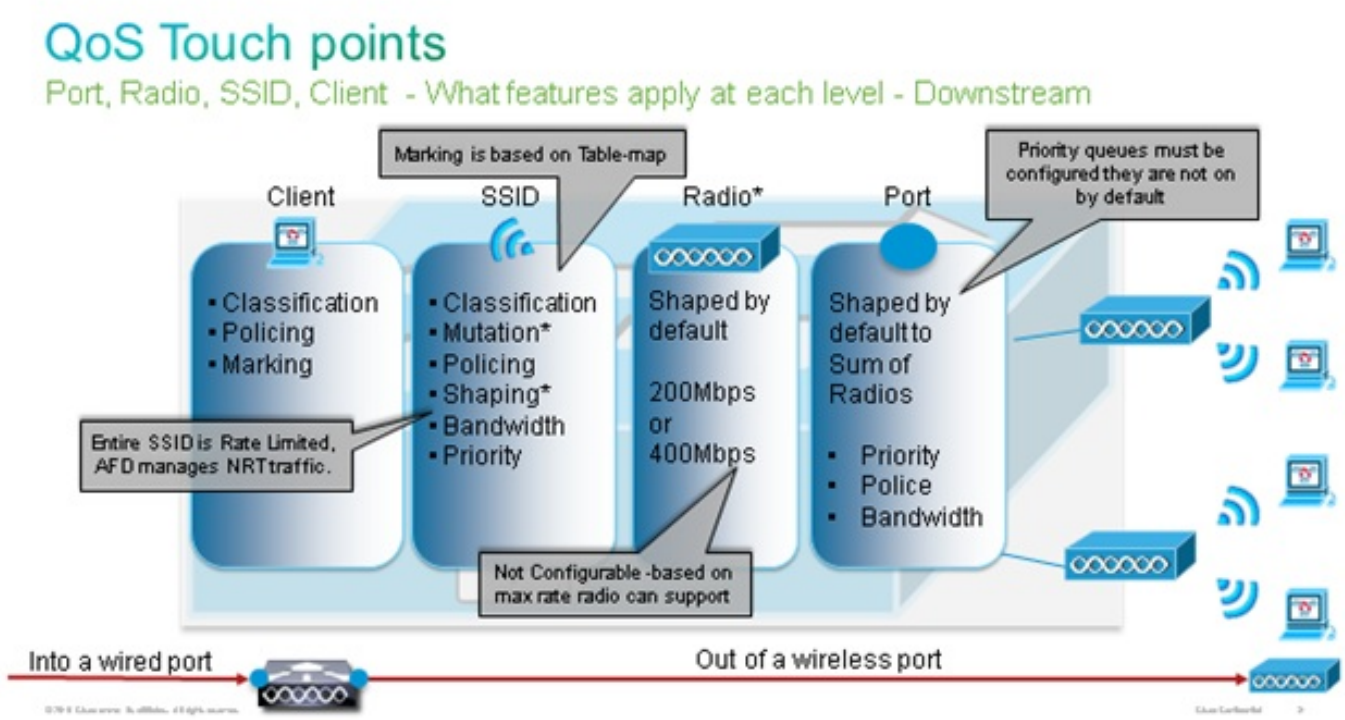
A próxima etapa é cuidar da política de QoS no nível de SSID. Esta etapa se aplica ao switch Catalyst 3850 e ao controlador 5760. Essa configuração pressupõe que o tráfego de voz e vídeo é identificado por meio do uso de class-map e access-lists e está marcado corretamente. No entanto, alguns tráfegos de entrada não direcionados pela lista de acesso podem não exibir sua marcação de QoS. Nesse caso, você pode decidir se esse tráfego deve ser marcado com um valor padrão ou não marcado. A mesma lógica se aplica ao tráfego já marcado, mas não direcionado pelos mapas de classe. Use a instrução *copy padrão* em um mapa de tabela para garantir que o tráfego não marcado seja deixado sem marca e que o tráfego marcado mantenha a marca e não seja remarcado.

Os mapas de tabela decidem o valor DSCP de saída, mas também são usados para criar um quadro 802.11 para decidir o valor UP do quadro.

Neste exemplo, o tráfego de entrada que exibe o nível de QoS de voz (DSCP 46) mantém seu valor de DSCP e o valor é mapeado para a marcação equivalente 802.11 (UP 6). O tráfego de entrada que exibe o nível de QoS de vídeo (DSCP 34) mantém seu valor de DSCP e o valor é mapeado para a marcação equivalente 802.11 (UP 5). Da mesma forma, o tráfego marcado como DSCP 24 pode ser sinalização de voz; o valor de DSCP deve ser mantido e convertido no 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
```

A marcação também pode ser feita no nível da porta com fio de entrada. Esta figura mostra quais ações de QoS podem ser tomadas à medida que o tráfego transita da rede com fio para a rede sem fio:



Este exemplo de configuração concentra-se no aspecto sem fio da configuração de QoS e marca o tráfego no nível do cliente sem fio. Depois que a parte de marcação for concluída, será necessário alocar largura de banda; aqui, 6 Mbps de largura de banda são alocados para fluxos de tráfego de voz. (Embora essa seja a alocação de largura de banda geral para voz, cada chamada consumiria menos - por exemplo, 128 kbps.) Essa largura de banda é alocada com o comando **police** para reservar a largura de banda e descartar o tráfego em excesso.

O tráfego de vídeo também é alocado para 6 Mbps e policiado. Este exemplo de configuração pressupõe que há apenas um fluxo de vídeo.

A parte de sinalização do tráfego de vídeo e voz também precisa ter largura de banda alocada. Há duas estratégias possíveis.

- Use o comando **shape medium**, que permite que o tráfego em excesso seja colocado em buffer e enviado posteriormente. Essa lógica não é eficiente para o fluxo de voz ou vídeo em si, pois esses fluxos exigem retardo e jitter consistentes; no entanto, ela pode ser eficiente para sinalização porque a sinalização pode ser ligeiramente adiada sem afetar a qualidade da chamada. Na solução de acesso convergido, os comandos shape não aceitam o que é chamado de "configurações de buckets", que determinam quanto tráfego além da largura de banda alocada pode ser colocado em buffer. Portanto, um segundo comando, **queue-buffers ratio 0**, deve ser adicionado para especificar que o tamanho do bucket é 0. Se você incluir a sinalização no restante do tráfego e usar comandos shape, o tráfego de sinalização poderá ser descartado em tempos de alto congestionamento. Isso pode, por sua vez, fazer com que a chamada seja descartada, pois uma das extremidades determina que a comunicação não está mais ocorrendo.
- Para evitar o risco de chamadas perdidas, você pode incluir a sinalização em uma das filas de prioridade. Este exemplo de configuração definiu previamente as filas de prioridade como voz e vídeo e agora adiciona sinalização à fila de vídeo.

A política usa o CAC (controle de admissão de chamada) para o fluxo de voz. O CAC destina-se ao tráfego sem fio e corresponde a um UP específico (neste exemplo de configuração, UP 6 e 7). Em seguida, o CAC determina a quantidade máxima de largura de banda que esse tráfego deve usar. Em uma configuração em que você policia o tráfego de voz, CAC deve receber um subconjunto da quantidade total de largura de banda alocada para voz. Por exemplo, se a voz for policiada para 6 Mbps, o CAC não poderá exceder 6 Mbps. O CAC é configurado em um mapa de políticas (chamado de política filho) que é integrado no mapa de políticas downstream principal (chamado de política pai). O CAC é introduzido com o comando **admac wmm-tspec**, seguido pelos UPs de destino e pela largura de banda alocada para o tráfego de destino.

Cada chamada não consome toda a largura de banda alocada para voz. Por exemplo, cada chamada pode consumir 64 kbps de cada maneira, o que resulta em 128 kbps de consumo efetivo de largura de banda bidirecional. A taxa de instrução determina cada consumo de largura de banda de chamada, enquanto a instrução policial determina a largura de banda geral alocada para o tráfego de voz. Se todas as chamadas que ocorrerem dentro da célula usarem uma largura de banda próxima à máxima permitida, qualquer nova chamada que seja iniciada dentro da célula e que faça com que a largura de banda consumida exceda a largura de banda máxima permitida para voz será negada. Você pode ajustar esse processo através da configuração do CAC no nível da banda, como explicado na Etapa 4: Limitação de chamadas com CAC.

Portanto, você precisa configurar uma política filho que contenha as instruções CAC e que esteja integrada à política de downstream principal. CAC não está configurado no mapa de política de upstream. O CAC se aplica a chamadas de voz iniciadas a partir da célula, mas, como é uma resposta a essas chamadas, o CAC é definido somente no mapa de política de downstream. O mapa de política de upstream será diferente. Você não pode usar os mapas de classe criados anteriormente porque esses mapas de classe direcionam o tráfego com base em uma ACL. O tráfego injetado na política de SSID já passou pela política do cliente, portanto, você não deve realizar uma inspeção profunda nos pacotes uma segunda vez. Em vez disso, direcione o tráfego com uma marcação de QoS que resulta da política do cliente.

Se decidir não deixar a sinalização na classe padrão, você também precisará priorizar a sinalização.

Neste exemplo, a sinalização e o vídeo estão na mesma classe, e mais largura de banda é alocada para essa classe para acomodar a parte de sinalização; 6 Mbps são alocados para tráfego de vídeo (um fluxo ponto-a-ponto da câmera Tandberg), e 1 Mbps é alocado para

sinalização para todas as chamadas de voz e fluxo de vídeo:

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

A política filha de downstream é:

```
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
```

A política pai de downstream é:

```
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
```

O tráfego upstream é o tráfego que vem de clientes sem fio e é enviado para o WCM antes do tráfego ser enviado de uma porta com fio ou é enviado para outro SSID. Em ambos os casos, você pode configurar mapas de política que definem a largura de banda alocada para cada tipo de tráfego. A política provavelmente será diferente se o tráfego for enviado de uma porta com fio ou para outro SSID.

Na direção upstream, sua principal preocupação é decidir a prioridade, não a largura de banda. Em outras palavras, seu mapa de política de upstream não aloca largura de banda para cada tipo de tráfego. Como o tráfego já está no AP e já atravessou o gargalo formado pelo espaço sem fio half-duplex, seu objetivo é levar esse tráfego para a função de controlador do switch Catalyst 3850 ou Cisco 5760 WLC para processamento adicional. Quando o tráfego é coletado no nível de AP, você pode decidir se deve confiar na marcação de QoS existente em potencial para priorizar os fluxos de tráfego enviados ao controlador. Neste exemplo, os valores de DSCP existentes podem ser confiáveis:

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

Depois que suas políticas forem criadas, aplique os mapas de políticas à WLAN. Neste exemplo, espera-se que qualquer dispositivo que se conecte à WLAN ofereça suporte à WMM, portanto a WMM é necessária.

```
wlan test1
wmm require
```

```
service-policy client input taggingPolicy
service-policy input SSIDin
service-policy output SSIDout
```

Passo 4: Limitação de chamada com CAC

A última etapa é adaptar o CAC à sua situação específica. Na configuração do CAC explicada na Etapa 3: Gerenciamento de largura de banda e prioridade no nível SSID, o AP descarta qualquer pacote de voz que exceda a largura de banda alocada.

Para evitar o máximo de largura de banda., você também precisa configurar o WCM para reconhecer as chamadas feitas e as chamadas que farão com que a largura de banda seja excedida. Alguns telefones suportam a TSPEC (WMM Traffic Specification, Especificação de tráfego WMM) e informam a infraestrutura sem fio sobre a largura de banda que a chamada projetada deve consumir. O WCM pode então recusar a chamada antes de ela ser feita.

Alguns telefones SIP não suportam TSPEC, mas o WCM e o AP podem ser configurados para reconhecer os pacotes de iniciação de chamadas enviados às portas SIP e podem usar essas informações para estabelecer que uma chamada SIP está prestes a ser feita. Como o telefone SIP não especifica a largura de banda a ser consumida pela chamada, o administrador deve determinar a largura de banda esperada, com base no codec, no tempo de amostragem e assim por diante.

A CAC calcula a largura de banda consumida em cada nível de AP. O CAC pode ser definido para usar somente o consumo de largura de banda do cliente em seus cálculos (CAC estático) ou também para considerar APs e dispositivos vizinhos no mesmo canal (CAC baseado em carga). A Cisco recomenda que você use CAC estático para telefones SIP e CAC baseado em carga para telefones TSPEC.

Finalmente, observe que o CAC é ativado por banda.

Neste exemplo, os telefones usam SIP em vez de TSPEC para sua iniciação de sessão, cada chamada usa 64 kbps para cada direção de fluxo, o CAC baseado em carga é desabilitado quando o CAC estático é habilitado e 75% de cada largura de banda de AP máxima é alocado para o tráfego 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
```

Você pode repetir a mesma configuração para a 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
```

Depois que o CAC for aplicado a cada banda, você também precisará aplicar o CAC SIP no nível da WLAN. Esse processo permite que o AP examine as informações da camada 4 (L4) do tráfego do cliente sem fio para identificar consultas enviadas ao UDP 5060 que indicam tentativas de

chamada SIP. O TSPEC opera no nível 802.11 e é detectado nativamente por APs. Os telefones SIP não usam TSPEC, portanto, o AP precisa executar uma inspeção de pacote mais profunda para identificar o tráfego SIP. Como você não deseja que o AP execute essa inspeção em todos os SSIDs, você precisa determinar quais SSIDs esperam tráfego SIP. Você pode ativar o rastreamento de chamadas nesses SSIDs para procurar chamadas de voz. Você também pode determinar qual ação executar se uma chamada SIP tiver que ser rejeitada - desassociar o cliente SIP ou enviar uma mensagem SIP ocupada.

Neste exemplo, o rastreamento de chamadas está ativado e uma mensagem de ocupado é enviada se a chamada SIP tiver que ser rejeitada. Com a adição da política de QoS da Etapa 3: Gerenciamento de largura de banda e prioridade no nível SSID, esta é a configuração do SSID para o exemplo 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
```

Verificar

Use estes comandos para confirmar se sua configuração de QoS funciona corretamente.

> **Notas:**
>
> Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.
>
> A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

show class-map

Este comando exibe os mapas de classe configurados na 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 exibe os mapas de políticas configurados na 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 exibe a configuração da WLAN e os parâmetros da política de serviço:

```
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

Esse comando exibe o mapa de políticas instalado para uma interface 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

Esse comando exibe as políticas de QoS instaladas para portas, rádios AP, SSIDs e clientes. Observe que você pode verificar, mas não pode alterar, as políticas de rádio:

```
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 exibe os mapas de política aplicados no nível do 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

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.