QoS em controladores convirgidos do acesso e no exemplo de configuração de pouco peso AP

Índice

Introdução

Este documento descreve como configurar QoS em Cisco convirgiu rede de acesso com Lightweight Access Points (regaços) e com o Cisco Catalyst 3850 Switch ou o controlador do Wireless LAN de Cisco 5760 (WLC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- O conhecimento básico de como configurar regaços e Cisco convirgiram controladores do acesso
- Conhecimento de como configurar o roteamento básico e o QoS em uma rede ligada com fio

Componentes Utilizados

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

- Cisco Catalyst 3850 Switch que executa o Cisco IOS? Software release XE 3.2.2(SE)
- Controlador do Wireless LAN de Cisco 5760 que executa a liberação do Software Cisco IOS XE 3.2.2(SE)
- Lightweight Access Points do Cisco 3600 Series

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

QoS refere a capacidade da rede para fornecer melhor ou o serviço especial a um grupo de usuários ou os aplicativos ao detrimento de outros usuários ou aplicativos.

Com QoS, a largura de banda pode ser controlada mais eficientemente através dos LAN, que inclui o Sem fio LAN (WLAN) e WAN. QoS fornece serviço aumentada e de rede confiável com estes serviços:

- Largura de banda dedicada dos apoios para usuários críticos e aplicativos.
- Controla o tremor e a latência que é exigida pelo tráfego de tempo real.
- Controla e minimiza o congestionamento de rede.
- Dá forma ao tráfego de rede a fim alisar o fluxo do tráfego.
- Ajusta prioridades do tráfego de rede.

No passado, os WLAN foram usados principalmente para transportar a largura de banda baixa, tráfego do aplicativo de dados. Com a expansão dos WLAN no vertical (tal como o retalho, a finança, e a educação) e nos ambientes de empreendimento, os WLAN são usados agora para transportar aplicativos de dados da largura de banda elevada conjuntamente com o sensível ao tempo, aplicativos multimídia. Esta exigência conduzida à necessidade para QoS wireless.

O grupo em funcionamento da IEEE 802.11e dentro do comitê de padrões do IEEE 802.11 terminou a definição padrão, e o Wi-fi Alliance criou a certificação dos multimédios do Wi-fi (WMM), mas a adoção do padrão 802.11e é limitada ainda. A maioria de dispositivos WMM-são certificados, porque a certificação WMM é precisada para a certificação 802.11n e 802.11ac. Muitos dispositivos Wireless não atribuem níveis diferentes de QoS aos pacotes enviados à camada de link de dados, assim que aqueles dispositivos enviam a maioria de seu tráfego sem a marcação de QoS e nenhuma prioridade relativa. Contudo, a maioria de Telefones IP do Voz sobre LAN sem fio (VoWLAN) do 802.11 marcam e dão a prioridade a seu tráfego de voz. Este

documento focaliza na configuração de QoS para Telefones IP de VoWLAN e nos dispositivos vídeo-capazes do Wi-fi que marcam seu tráfego de voz.

> Nota: A configuração de QoS para os dispositivos que não executam a marcação interna é fora do âmbito deste documento.

A alteração 802.11e define oito níveis da prioridade de usuário (ACIMA), agrupados dois por dois em quatro níveis de QoS (categorias do acesso):

- Platina/Voz (ACIMA de 7 e de 6) - assegura um de alta qualidade do serviço para a Voz sobre o Sem fio.
- Aplicativos de vídeo de alta qualidade dos apoios do ouro/vídeo (ACIMA de 5 e de 4) -.
- Largura de banda normal de prata/melhor do esforço (ACIMA de 3 e de 0) - dos apoios para clientes. Esta é a configuração padrão.
- Bronze/fundo (ACIMA de 2 e de 1) - fornece a mais baixa largura de banda para serviços do convidado.

A platina é de uso geral para clientes e ouro de VoIP para os clientes video. Este documento fornece um exemplo de configuração que ilustre como configurar QoS em controladores e se comunicar com uma rede ligada com fio que seja configurada com o QoS para VoWLAN e os clientes video.

Realces da Marcação de pacotes QoS L3

Cisco convirgiu marcação do Differentiated Services Code Point IP da camada 3 do apoio dos controladores do acesso (L3) (DSCP) dos pacotes enviados por WLC e por regaços. Esta característica aumenta como os Access point (AP) usam esta informação L3 a fim se assegurar de que os pacotes recebam o correto sobre - arejam a prioridade do AP ao cliente Wireless.

Em uma arquitetura de WLAN convirgida do acesso que use Catalyst 3850 Switch como controladores wireless, os AP conectam diretamente ao interruptor. Em uma arquitetura de WLAN convirgida do acesso que use 5760 controladores, os dados WLAN são escavados um túnel entre o AP e o WLC através do controle e o abastecimento do protocolo dos pontos de acesso Wireless (CAPWAP). A fim manter a classificação de QoS original através deste túnel, os ajustes de QoS do pacote de dados encapsulados devem apropriadamente ser traçados à camada 2 (L2) (802.1p) e (IP DSCP) aos campos L3 do pacote de túnel exterior.

Quando você configura QoS para VoWLAN e vídeo, você pode configurar um específico da política de QoS para clientes Wireless e um específico da política a um WLAN, ou ambos. Você pode igualmente complementar a instalação com um específico da configuração à porta que liga o AP, especialmente com Catalyst 3850 Switch. Este exemplo de configuração centra-se sobre a configuração de QoS para o cliente Wireless, o WLAN, e a porta ao AP. Os objetivos principais de uma configuração de QoS para VoWLAN e aplicativos de vídeo são:

- Reconheça a Voz e o tráfego de vídeo (Classificação de tráfego e marcação), ambos fluxo acima e fluxo abaixo.
- Marque a Voz e o tráfego de vídeo com um nível de prioridade de voz: 802.11e ACIMA de 6, 802.1p 5, DSCP 46 para a Voz.802.11e LEVANTAM 5, DSCP 34 para o vídeo.
- Atribua a largura de banda para o tráfego de voz, a sinalização de voz, e o tráfego de vídeo.

Configurar a rede Wireless para QoS com MQC

Antes que você configure QoS, você deve configurar a função wireless do módulo do controlador (WCM) do Catalyst 3850 Switch ou de Cisco 5760 WLC para a operação básica e registrar os regaços ao WCM. Este documento supõe que o WCM está configurado para a operação básica e que os regaços estão registrados ao WCM.

A solução de acesso convirgida usa o comando line interface(cli) do QoS modular (MQC). Refira o guia de configuração de QoS, a liberação 3SE do Cisco IOS XE (Catalyst 3850 Switch) para obter informações adicionais sobre do uso do MQC na configuração de QoS no Catalyst 3850 Switch.

A configuração de QoS com o MQC em controladores convirgidos do acesso confia em quatro elementos:

- **Os mapas de classe** são usados a fim reconhecer o tráfego do interesse. Os mapas de classe podem usar várias técnicas (tais como a marcação, listas de acesso, ou VLAN existentes de QoS) a fim identificar o tráfego do interesse.
- **os Política-mapas** são usados a fim determinar que ajustes de QoS devem ser aplicados ao tráfego do interesse. os Política-mapas chamam mapas de classe e aplicam vários ajustes de QoS (tais como a marcação, níveis da prioridade, a alocação de largura de banda específicos, e assim por diante) a cada classe.
- **As políticas de serviços** são usadas a fim aplicar política-mapas aos pontos estratégicos de sua rede. Na solução de acesso convirgida, as políticas de serviços podem ser aplicadas aos usuários, aos service set identifier (SSID), aos rádios AP, e às portas. A porta, o SSID, e as políticas de cliente podem ser configurados pelo usuário. As políticas de rádio são controladas pelo módulo de controle wireless. As políticas de QoS wireless para a porta, o SSID, o cliente, e o rádio são aplicadas na direção fluxo abaixo quando o tráfego está fluindo do interruptor ou do controlador aos clientes Wireless.
- **os Tabela-mapas** são usados a fim examinar a marcação entrante de QoS e decidir marcações que parte de QoS. os Tabela-mapas são posicionados nos política-mapas aplicados aos SSID. os Tabela-mapas podem ser usados a fim manter (cópia) ou mudar a marcação. os Tabela-mapas podem igualmente ser usados a fim criar um mapeamento entre a marcação prendida e wireless. A marcação prendida usa DSCP (L3 QoS) ou 802.1p (L2 QoS). A marcação wireless usa a prioridade de usuário (ACIMA). os Tabela-mapas são de uso geral determinar que marcação DSCP deve ser usada para cada um ACIMA do interesse e o que ACIMA deve ser usado para cada valor DSCP do interesse. os Tabela-mapas são fundamentais ao acesso convirgido QoS porque não há nenhuma tradução direta entre o DSCP e valores ASCENDENTES.

Contudo, o DSCP aos tabela-mapas ASCENDENTES igualmente permite a instrução da *cópia*. Nesse caso, a solução de acesso convirgida usa a arquitetura Cisco para a Voz, o vídeo, e a tabela de mapeamento integrada dos dados (AVVID) a fim determinar o DSCP a ASCENDENTE ou até a tradução DSCP:

Deslocamento predeterminado da etiqueta	Campo chave	Valor entrante	DSCP exterior	CoS	PARA CIMA
0	N.A.	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 codificadas padrão

Os controladores convirgidos do acesso embarcam os perfis codificados da política de QoS que podem ser aplicados aos WLAN. Estes perfis aplicam as políticas do metal (platina, ouro, e assim por diante) que são familiares aos administradores de controladores das redes de Cisco Unified Wireless (CUWN). Se seu objetivo não é criar as políticas que atribuem a largura de banda específica ao tráfego de voz mas se assegurar de simplesmente que o tráfego de voz receba a marcação apropriada de QoS, você pode usar as políticas codificadas. As políticas codificadas podem ser aplicadas ao WLAN e podem ser diferentes no ascendente e nas direções fluxo abaixo.

Notas:

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

A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

Platinum

A política codificada para a Voz é chamada platina. O nome não pode ser mudado.

Esta é a política a jusante para o nível de QoS da 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 ascendente para o nível de QoS da platina:

```
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
```

Ouro

A política codificada para o vídeo é chamada ouro. O nome não pode ser mudado.

Esta é a política a jusante para o nível de QoS do 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 ascendente para o nível de QoS do 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 codificada para o melhor esforço é chamada de prata. O nome não pode ser mudado.

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

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

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

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

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

Bronze

A política codificada para o tráfego de background é chamada de bronze. O nome não pode ser mudado.

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

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

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

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

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

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

Uma vez que você decidiu que tabela-mapa melhor combina o tráfego do alvo para um SSID dado, você pode aplicar a política de harmonização a seu WLAN. Neste exemplo, uma política é aplicada na direção fluxo abaixo (saída, do AP ao cliente Wireless), e uma política é aplicada na direção de upstream (entrada, do cliente Wireless, com o AP, ao 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 WLAN a fim verificar que política foi aplicada a seu 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 do padrão mas não aplicam a alocação de largura de banda. As políticas codificadas igualmente supõem que seu tráfego está marcado já. Em um ambiente complexo, você pode querer usar uma combinação de políticas a fim reconhecer apropriadamente e marcar a Voz e o tráfego de vídeo, para ajustar a alocação de largura de banda no a jusante e nas direções de upstream, e para usar o controle de admissão da chamada a fim limitar o número de atendimentos iniciados da pilha wireless.

> Nota: 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 a Voz e o tráfego de vídeo. O tráfego de voz pode ser classificado em duas categorias:

- Fluxo de voz, que leva o áudio parte da comunicação.
- A sinalização de voz, que leva a informação estatística trocou entre valores-limite da Voz.

O fluxo de voz usa geralmente portas do destino do Real-Time Transport Protocol (RTP) e do User Datagram Protocol (UDP) na escala de 16384 - 32767. Esta é a escala; as portas reais são geralmente mais estreitas e dependem da aplicação.

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

- TCP 80 (HTTP)
- 143 ([IMAP] do protocolo de acesso de mensagens de Internet)
- 443 (HTTPS)
- 993 (IMAP) para serviços tais como o Cisco Unified MeetingPlace ou o WebEx de Cisco para reuniões e Cisco Unity ou Cisco Unity Connection para características do correio de voz
- TCP 389/636 (server do [LDAP] do protocolo lightweight directory access para buscas do contato)
- FTP (1080)
- TFTP (UDP 69) para transferência de arquivo (tal como arquivos de configuração) dos pares ou do server

Estes serviços não podem precisar uma prioridade específica.

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

O tráfego de vídeo usa as portas e protocolo diferentes que dependem de sua aplicação. Este exemplo de configuração usa uma câmera de Tandberg PrecisionHD 720p para videoconferências. A câmera de Tandberg PrecisionHD 720p pode usar diversos codecs; a

largura de banda consumida depende do codec escolhido:

- Os codecs C20, C40, e C60 usam o H.323/SIP e podem consumir até o 6 Mbps nas conexões Point-to-Point.
- O codec C90 usa estes mesmos protocolos e pode consumir até o 10 Mbps em comunicações do multi-local.

A aplicação de Tandberg de H.323 usa tipicamente UDP 970 para a vídeo fluente, UDP 971 para a sinalização video, UDP 972 para fluir o áudio, e UDP 973 para a sinalização audio. As câmeras de Tandberg igualmente usam outras portas, como:

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

Estas portas adicionais não podem precisar uma prioridade específica.

Uma forma comum identificar o tráfego é criar os mapas de classe que visam o tráfego do interesse. Cada mapa de classe pode apontar a uma lista de acesso que vise todo o tráfego que usar a Voz e as portas de 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 então criar um mapa de classe para cada tipo de tráfego; cada mapa de classe aponta à 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
```

Uma vez que o tráfego de voz e o tráfego de vídeo foram identificados através dos mapas de classe, assegure-se de que o tráfego esteja marcado corretamente. Isto pode ser feito a nível WLAN através dos tabela-mapas e pode igualmente ser feito através dos política-mapas do cliente.

os Tabela-mapas examinam a marcação de QoS do tráfego de entrada e determinam o que a marcação que parte de QoS deve ser. Assim, os Tabela-mapas são úteis quando o tráfego de entrada já tem a marcação de QoS. os Tabela-mapas são usados exclusivamente a nível SSID.

Pelo contraste, os política-mapas podem visar o tráfego identificado por mapas de classe e são adaptados melhor potencialmente ao tráfego sem etiqueta do interesse. Este exemplo de configuração supõe que o tráfego da face da tela esteve marcado já corretamente antes que entre no Catalyst 3850 Switch ou no Cisco 5760 WLC. Se tal não for o caso, você pode usar um mapa de política e aplicá-lo a nível SSID como uma política de cliente. Porque o tráfego dos clientes Wireless não pode ter sido marcado, você precisa de marcar corretamente a Voz e o tráfego de vídeo:

- A voz em tempo real deve ser identificada por meio de DSCP 46 ([EF] do Expedited Forwarding).
- O vídeo deve ser DSCP 34 marcado (classe de encaminhamento assegurada 41 [AF41]).
- Sinalizar para a Voz e o vídeo deve ser DSCP marcado 24 (valor 3 [CS3] do serviço do seletor de classe).

Para aplicar estas marcações, crie um mapa de política que chamam cada um destas classes e que marca o tráfego equivalente:

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

 class H323realtimevideo
 set dscp af41

 class signaling
 set dscp cs3
```

Passo 2: Gerenciamento da largura de banda e da prioridade a nível da porta

A próxima etapa é determinar uma política de QoS para as portas que vêm e vão aos AP. Esta etapa aplica-se primeiramente aos Catalyst 3850 Switch. Se sua configuração é feita em um controlador de Cisco 5760, esta etapa não é imperativa. As portas do catalizador 3850 levam a Voz e o tráfego de vídeo que vai a ou vem dos clientes Wireless e dos AP. A configuração de QoS neste contexto combina duas exigências:

1. **Atribua a largura de banda**. Você pode querer decidir quanto largura de banda é atribuída para cada tipo de tráfego. Esta alocação de largura de banda pode igualmente ser feita a nível SSID. Ajuste a alocação de largura de banda da porta a fim refinar quanto largura de banda pode ser recebida por cada AP que serve o alvo SSID. Esta largura de banda tem que ser ajustada para todos os SSID no alvo AP. Este exemplo da configuração simplificada supõe que há somente um SSID e um AP, assim que a alocação de largura de banda da porta para a Voz e o vídeo é a mesma que a alocação de largura de banda global para a Voz e o vídeo a nível SSID. Cada tipo de tráfego é 6 Mbps atribuído e é policiado de modo que esta largura de banda atribuída não seja excedida.

2. **Dê a prioridade ao tráfego**. A porta tem quatro filas. As primeiras duas filas são dadas a prioridade e reservadas para o tráfego de tempo real - tipicamente Voz e vídeo, respectivamente. A quarta fila é reservada para o tráfego multicast do tempo não real, e a terceira fila contém todo tráfego restante. Com lógica convirgida do Enfileiramento do acesso, o tráfego para cada cliente é atribuído a uma fila virtual, onde QoS possa ser configurado. O resultado da política de QoS do cliente é injetado na fila virtual SSID, onde QoS pode igualmente ser configurado. Desde que diversos SSID podem existir em um rádio

AP dado, o resultado de cada SSID que esta presente em um rádio AP é injetado na fila virtual do rádio AP, onde o tráfego é dado forma baseou na capacidade de rádio. O tráfego pode ser atrasado ou deixado cair em qualqueras um fases por meio de um mecanismo de QoS chamado a gota de Aproximado Justo (AFD). O resultado desta política é enviado então à porta AP (chamada a porta wireless), onde a prioridade é dada às primeiras duas filas (até uma quantidade configurável de largura de banda), e então às terceiras e quartas filas como descrito mais cedo neste parágrafo.

Este exemplo de configuração coloca a Voz na fila de prioridade principal e o vídeo na segunda fila de prioridade com o uso do comando do **nível da prioridade**. O resto do tráfego é atribuído o resto da largura de banda da porta.

Observe que você não pode usar os mapas de classe que o tráfego do alvo baseou no Access Control Lists (ACLs). As políticas aplicadas a nível da porta podem visar o tráfego baseado em mapas de classe, mas estes mapas de classe devem visar o tráfego identificado por seu valor do QoS. Uma vez que você identificou o tráfego baseado em ACL e marcado este tráfego corretamente a nível do cliente SSID, seria redundante executar uma segunda inspeção profunda desse mesmo tráfego a nível da porta. Quando o tráfego alcança a porta que vai ao AP, é marcado já corretamente.

Neste exemplo, você reutiliza os mapas de classe gerais criados para a política SSID e visa diretamente o tráfego da Voz RTP e o tráfego de tempo real do vídeo:

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

Uma vez que você identificou o tráfego do interesse, você pode decidir que política a se aplicar. A política padrão (chamada parent_port) está aplicada automaticamente em cada porta quando um AP é detectado. Você não deve mudar este padrão, que é ajustado como:

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

Porque a política do parent_port do padrão chama o port_child_policy, uma opção é editar o port_child_policy. (Você não deve mudar seu nome). Esta política infantil determina que tráfego deve ir em cada fila e quanto largura de banda deve ser atribuída. A primeira fila tem a prioridade mais alta, a segunda fila tem a segunda prioridade mais alta, e assim por diante. Estas duas filas são reservadas para o tráfego de tempo real. A quarta fila é usada para o tráfego multicast do tempo não real. A terceira fila contém todo tráfego restante.

Neste exemplo, você decide atribuir o tráfego de voz à primeira fila e o tráfego de vídeo à segunda fila e atribuir a largura de banda a cada fila e a todo tráfego restante:

```
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 à “Voz” e às classes “videoandsignaling” permite que você atribua esse tráfego à fila de prioridade relevante. A observação, contudo, que a polícia avalia indicações dos por cento aplica-se somente ao Multicast, não unicast, tráfego.

Você não precisa de aplicar esta política a nível da porta porque está aplicado automaticamente assim que um AP for detectado.

Passo 3: Gerenciamento da largura de banda e da prioridade a nível SSID

A próxima etapa é tomar da política de QoS a nível SSID. Esta etapa aplica-se ao Catalyst 3850 Switch e ao controlador 5760. Esta configuração supõe que a Voz e o tráfego de vídeo estão identificados com o uso do mapa de classe e das listas de acesso e etiquetados corretamente. Contudo, algum tráfego de entrada que não é visado pela lista de acesso não pode indicar sua marcação de QoS. Nesse caso, você pode decidir se este tráfego for identificado por meio de um valor padrão ou um sem etiqueta esquerdo. A mesma lógica vai para o tráfego já marcado mas não visado pelos mapas de classe. Use a indicação da *cópia padrão em um tabela*-mapa a fim assegurar-se de que o tráfego não marcado esteja deixado não marcado e que o tráfego rotulado mantém a etiqueta e ele não observado.

os Tabela-mapas decidem o valor que parte DSCP mas são usados igualmente para criar um quadro do 802.11 para decidir o valor ASCENDENTE do quadro.

Neste exemplo, o tráfego de entrada que indica o nível de QoS da Voz (DSCP 46) mantém seu valor DSCP, e o valor é traçado à marcação equivalente do 802.11 (ACIMA de 6). O tráfego de entrada que indica o nível video de QoS (DSCP 34) mantém seu valor DSCP, e o valor é traçado à marcação equivalente do 802.11 (ACIMA de 5). Similarmente, o DSCP marcado tráfego 24 pode ser sinalização de voz; o valor DSCP deve ser mantido e traduzido no 802.11 ACIMA de 3:

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

A marcação podia igualmente ser feita a nível prendido entrante da porta. Esta figura mostra o que as ações QoS podem ser tomadas como trânsitos do tráfego do prendido ao Sem fio:

Este exemplo de configuração centra-se sobre o aspecto wireless da configuração de QoS e as marcas traficam a nível do cliente Wireless. Uma vez que a parcela da marcação foi terminada, você precisa de atribuir a largura de banda; aqui, o 6 Mbps da largura de banda é atribuído aos fluxos de tráfego de voz. (Quando esta for a atribuição da largura de banda total para a Voz, cada atendimento consumiria menos - por exemplo, os kbps 128.) Esta largura de banda é atribuída com o comando police a fim reservar a largura de banda e deixar cair o tráfego superior.

O tráfego de vídeo é 6 Mbps igualmente atribuído e policiado. Este exemplo de configuração supõe que há somente um fluxo video.

A sinalização parte de do vídeo e do tráfego de voz igualmente precisa de ser largura de banda atribuída. Há duas estratégias possíveis.

- Use o comando **médio da forma**, que permite que o tráfego superior seja protegido e enviado mais tarde. Esta lógica não é eficiente para o fluxo próprio da Voz ou do vídeo porque aqueles fluxos exigem o retardo e tremulação consistente; contudo, pode ser eficiente para sinalizar porque sinalizar pode levemente ser atrasada sem um efeito na qualidade da chamada. Na solução de acesso convirgida, os comandos shape não aceitam o que é chamada das “configurações cubetas,” que determinam quanto tráfego além da largura de banda atribuída pode ser protegido. Consequentemente, um comando second, a **relação 0 dos bufferes de fila**, deve ser adicionado a fim especificar que o tamanho da cubeta é 0. Se você inclui a sinalização no resto do tráfego e usa comandos shape, o tráfego de sinalização pôde ser deixado cair em período do congestionamento alto. Isto pôde, por sua vez, fazer com que o atendimento seja deixado cair porque uma ou outra extremidade determina que uma comunicação já não está ocorrendo.
- Para evitar o risco de chamadas descartada, 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 adiciona agora a sinalização à fila video.

A política usa o controle de admissão da chamada (CAC) para o fluxo de voz. O CAC visa o tráfego Wireless e combina um específico ACIMA (neste exemplo de configuração, ACIMA de 6 e de 7). O CAC determina então a quantidade máxima de largura de banda que este tráfego deve se usar. Em uma configuração onde você policie o tráfego de voz, o CAC deve ser atribuído um subconjunto da quantidade total de largura de banda atribuída para a Voz. Por exemplo, se a Voz é policiada ao 6 Mbps, o CAC não pode exceder o 6 Mbps. O CAC é configurado em um mapa de política (chamado uma política infantil) que é integrado no mapa de política a jusante do cano principal (chamado a política de parentes). O CAC é introduzido com o comando do **wmm-tspec do cac da admissão**, seguido pelo alvo levanta e a largura de banda atribuída ao tráfego visado.

Cada atendimento não consome toda a largura de banda atribuída para exprimir. Por exemplo, cada atendimento pode consumir 64 kbps cada maneira, que conduz aos kbps 128 do consumo de largura de banda bidirecional eficaz. A instrução da taxa determina cada consumo de largura de banda por chamada, quando a declaração de vigia determinar a largura de banda total atribuída ao tráfego de voz. Se todos os atendimentos que ocorrem dentro do uso da pilha perto da largura de banda permitida máxima, todo o atendimento novo que são iniciados de dentro da pilha e que fizer com que a largura de banda consumida exceda a largura de banda máxima permitida a Voz serão negados. Você pode ajustar este processo com a configuração do CAC a nível da faixa, como explicado em etapa 4: Limitação do atendimento com CAC.

Consequentemente, você precisa de configurar uma política infantil que contenham as instruções CAC e que seja integrada na política a jusante do cano principal. O CAC não é configurado no mapa de política ascendente. O CAC aplica-se às chamadas de voz iniciadas da pilha, mas, porque é uma resposta 2 aqueles atendimentos, o CAC é ajustado somente no mapa de política a jusante. O mapa de política ascendente será diferente. Você não pode usar os mapas de classe criados previamente porque estes mapas de classe visam o tráfego baseado em um ACL. O tráfego injetado na política SSID já atravessou a política de cliente, assim que você não deve executar a inspeção profunda nos pacotes um a segunda vez. Em lugar de, o tráfego do alvo com uma marcação de QoS essa resulta da política de cliente.

Se você decide não deixar a sinalização na classe padrão, você igualmente precisará de dar a prioridade à sinalização.

Neste exemplo, a sinalização e o vídeo estão na mesma classe, e mais largura de banda é atribuída a essa classe a fim acomodar a parte de sinalização; O 6 Mbps é atribuído para o tráfego de vídeo (um fluxo ponto a ponto da câmera de Tandberg), e o 1 Mbps é atribuído à sinalização para todas as chamadas de voz e o fluxo video:

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

A política infantil a jusante 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 de parentes a jusante 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 ascendente é o tráfego que vem dos clientes Wireless e está enviado ao WCM antes que o tráfego esteja enviado fora de uma porta prendida ou enviado a um outro SSID. Em ambos os casos, você pode configurar os política-mapas que definem a largura de banda atribuída a cada tipo de tráfego. A política diferirá provavelmente baseado sobre se o tráfego está enviado fora de uma porta prendida ou a um outro SSID.

Na direção de upstream, seu interesse principal é decidir a prioridade, não a largura de banda. Ou seja seu mapa de política ascendente não atribui a largura de banda a cada tipo de tráfego. Porque o tráfego está já no AP e tem cruzado já o gargalo formado pelo espaço wireless metade-frente e verso, seu objetivo é trazer este tráfego à função do controlador do Catalyst 3850 Switch ou do Cisco 5760 WLC para o processamento adicional. Quando o tráfego é recolhido a nível AP, você pode decidir se você confiar a marcação existente potencial de QoS a fim dar a prioridade aos fluxos de tráfego enviados ao controlador. Neste exemplo, os valores existentes DSCP podem ser confiados:

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

Uma vez que suas políticas são criadas, aplique os política-mapas ao WLAN. Neste exemplo, todo o dispositivo que conectar ao WLAN é esperado apoiar WMM, assim que WMM é exigido.

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

Passo 4: Limitação do atendimento com CAC

A última etapa é costurar o CAC a sua situação específica. Na configuração CAC explicada em etapa 3: O Gerenciamento da largura de banda e da prioridade a nível SSID, o AP deixa cair todo o pacote de voz que exceder a largura de banda atribuída.

A fim evitar o máximo da largura de banda., você igualmente precisa de configurar o WCM a fim reconhecer os atendimentos que são colocados e os atendimentos que farão com que a largura de banda seja excedida. Alguns telefones apoiam a especificação do tráfego WMM (TSPEC) e informam o infraestrutura Wireless da largura de banda que o atendimento projetado está esperado consumir. O WCM pode então recusar o atendimento antes que esteja colocado.

Alguns telefones do SORVO não apoiam TSPEC, mas o WCM e o AP podem ser ajustados para reconhecer os pacotes da iniciação de chamada enviados PARA SORVER portas e podem usar esta informação a fim estabelecer que um atendimento do SORVO está a ponto de ser colocada. Porque o telefone do SORVO não especifica a largura de banda que deve ser consumido pelo atendimento, o administrador deve determinar a largura de banda prevista, com base no codec, o tempo da amostra, e assim por diante.

O CAC calcula a largura de banda consumida a cada nível AP. O CAC pode ser ajustado para usar somente o consumo de largura de banda do cliente em seus cálculos (CAC estático) ou para considerar igualmente AP vizinhos e dispositivos no mesmo canal (CAC carga-baseado). Cisco recomenda que você usa o CAC estático para telefones do SORVO e o CAC carga-baseado para telefones TSPEC.

Finalmente, note que o CAC está ativado na pela base da faixa.

Neste exemplo, o SORVO do uso dos telefones um pouco do que TSPEC para sua iniciação de sessão, cada atendimento usa 64 kbps para cada sentido do córrego, o CAC carga-baseado é desabilitado quando o CAC estático é permitido, e 75% de cada largura de banda AP máxima está atribuído ao 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 faixa 2.4 gigahertz:

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

Uma vez que o CAC é aplicado para cada faixa, você igualmente precisa de aplicar o SORVO CAC a nível WLAN. Este processo permite o AP de examinar a informação da camada 4 (L4) do tráfego do cliente Wireless a fim identificar as perguntas enviadas ao UDP 5060 que indicam tentativas de chamada do SORVO. TSPEC opera-se a nível do 802.11 e é detectado nativamente por AP. Os telefones do SORVO não usam TSPEC, assim que o AP tem que executar uma inspeção de pacote de informação mais profunda a fim identificar o tráfego do SORVO. Porque você não quer o AP executar esta inspeção em todos os SSID, você precisa de determinar que SSID esperam o tráfego do SORVO. Você pode então permitir a espião do atendimento naqueles

SSID a fim procurar chamadas de voz. Você pode igualmente determinar que ação a executar se um atendimento do SORVO tem que ser rejeitado - dissociar o cliente do SORVO ou envie um mensagem de ocupado do SORVO.

Neste exemplo, a espião do atendimento é permitida, e um mensagem de ocupado é enviado se o atendimento do SORVO tem que ser rejeitado. Com a adição da política de QoS de etapa 3: O Gerenciamento da largura de banda e da prioridade a nível SSID, isto é a configuração SSID para o exemplo 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 a fim confirmar que sua configuração de QoS trabalha corretamente.

> Notas:
>
> Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.
>
> A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

mostre o mapa de classe

Este comando indica 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
```

mostre o mapa de política

Este comando indica os política-mapas 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
```

mostre wlan

Este comando indica os parâmetros da configuração e da serviço-política WLAN:

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

show policy-map interface

Este comando indica o mapa de política instalado para uma relação 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
```

mostre políticas de QoS da plataforma

Este comando indica as políticas de QoS instaladas para portas, rádios AP, SSID, e clientes. Observe que você pode verificar, mas não possa mudar, 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
```

mostre a serviço-política do <mac> do endereço MAC do cliente Wireless

Este comando indica os política-mapas aplicados a 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
```

Troubleshooting

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