Configurar, validar e solucionar problemas de QoS sem fio no 9800 WLC

Contents

Introdução

Este documento descreve maneiras de configurar, validar e solucionar problemas de Qualidade de Serviço (QoS - Quality of Service) sem fio em controladoras Wireless LAN (WLC - Wireless LAN Controller) 9800.

Componentes Utilizados

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

- WLC: C9800-40-K9 executando 17.12.03
- Ponto de acesso (AP): C9120-AX-D

- Switch: C9300-48P executando 17.03.05
- Cliente com e sem fio: Windows 10

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

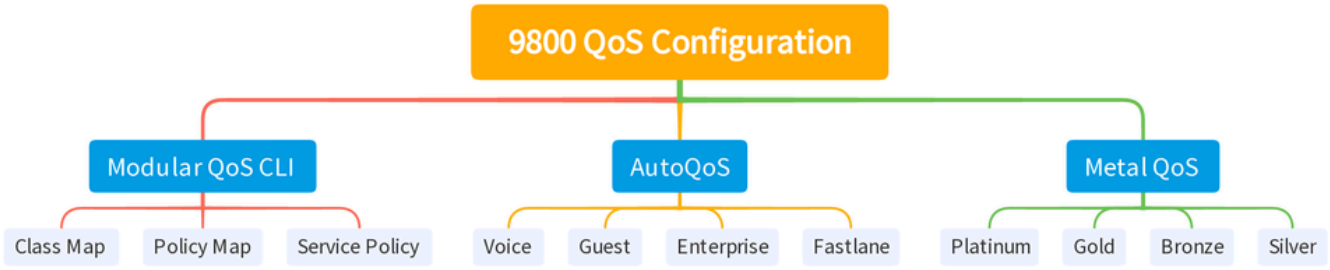
A QoS sem fio é essencial para garantir que os aplicativos críticos recebam a largura de banda necessária e a baixa latência necessária para o desempenho ideal. Este documento fornece um guia abrangente para configurar, validar e solucionar problemas de QoS em redes sem fio Cisco.

Este artigo pressupõe que os leitores tenham uma compreensão básica dos princípios de QoS com e sem fio. Espera-se também que os leitores dominem a configuração e o gerenciamento de WLCs e APs da Cisco.

Configuração

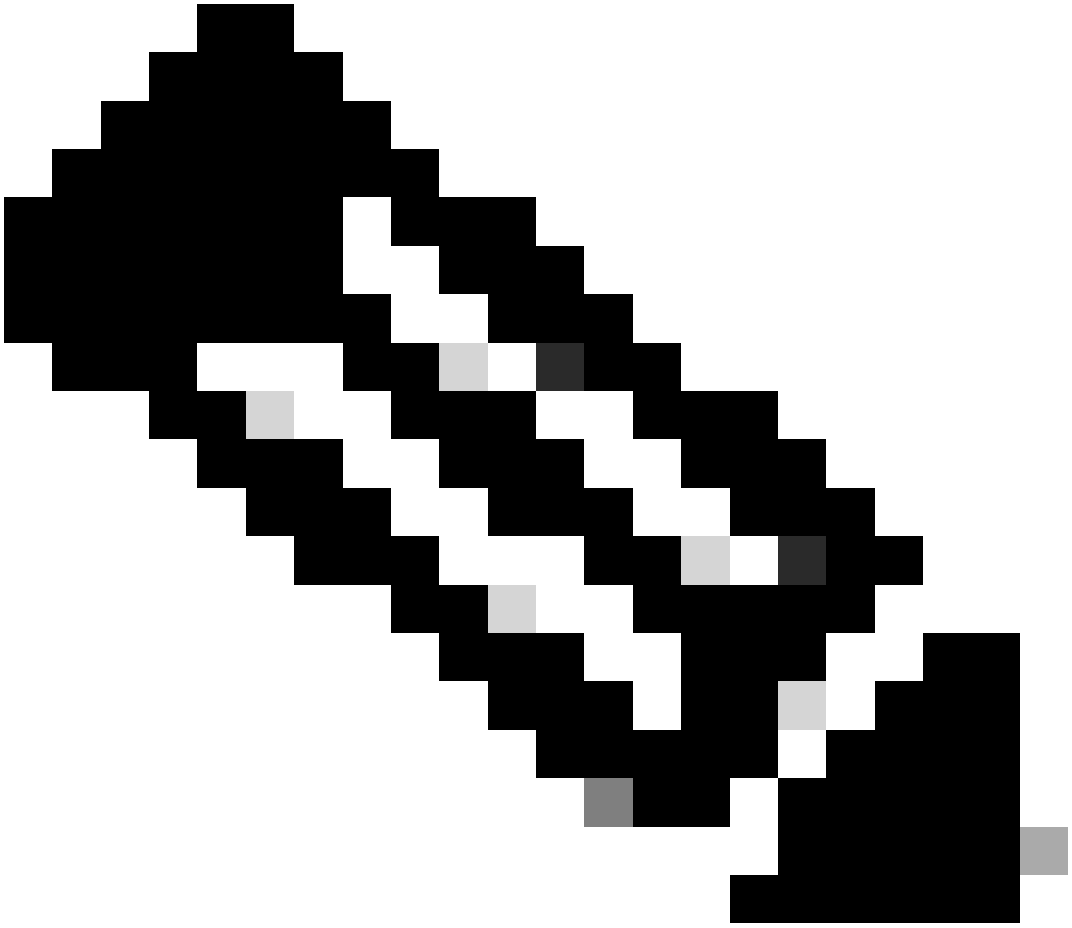
Esta seção se aprofunda na configuração de QoS em controladores sem fio 9800. Aproveitando essas configurações, você pode garantir que os aplicativos críticos recebam a largura de banda necessária e baixa latência, otimizando, assim, o desempenho geral da rede.

Você pode dividir a configuração de QoS da WLC 9800 principalmente em três categorias amplas diferentes.



Resumo da configuração de QOS da WLC 9800

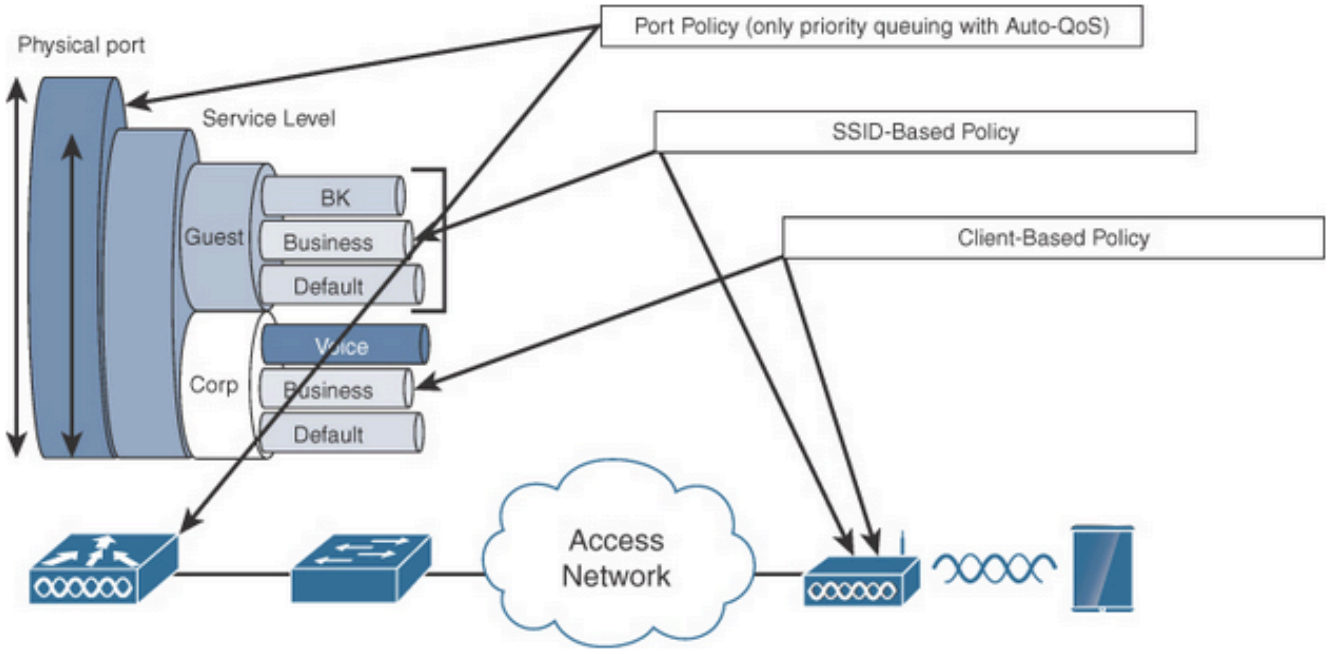
Este documento passa por cada seção, uma a uma, nas seções subsequentes.



Observação: este artigo se concentra no AP no modo local. O AP no modo Flexconnect não é discutido.

Destinos da política de QoS

Um destino de política é a construção de configuração onde uma política de QoS pode ser aplicada. A implementação de QoS no Catalyst 9800 é modular e flexível. O usuário pode decidir configurar políticas em três destinos diferentes: SSID, cliente e níveis de porta.



Destinos da política de QoS

A política de SSID é aplicável por AP por SSID. Você pode configurar políticas de vigilância e marcação no SSID.

As políticas do cliente são aplicáveis na direção de entrada e saída. Você pode configurar políticas de vigilância e marcação em clientes. AAA override também é suportado.

As políticas de QoS baseadas em porta podem ser aplicadas em uma porta física ou em uma porta lógica.

QoS automático

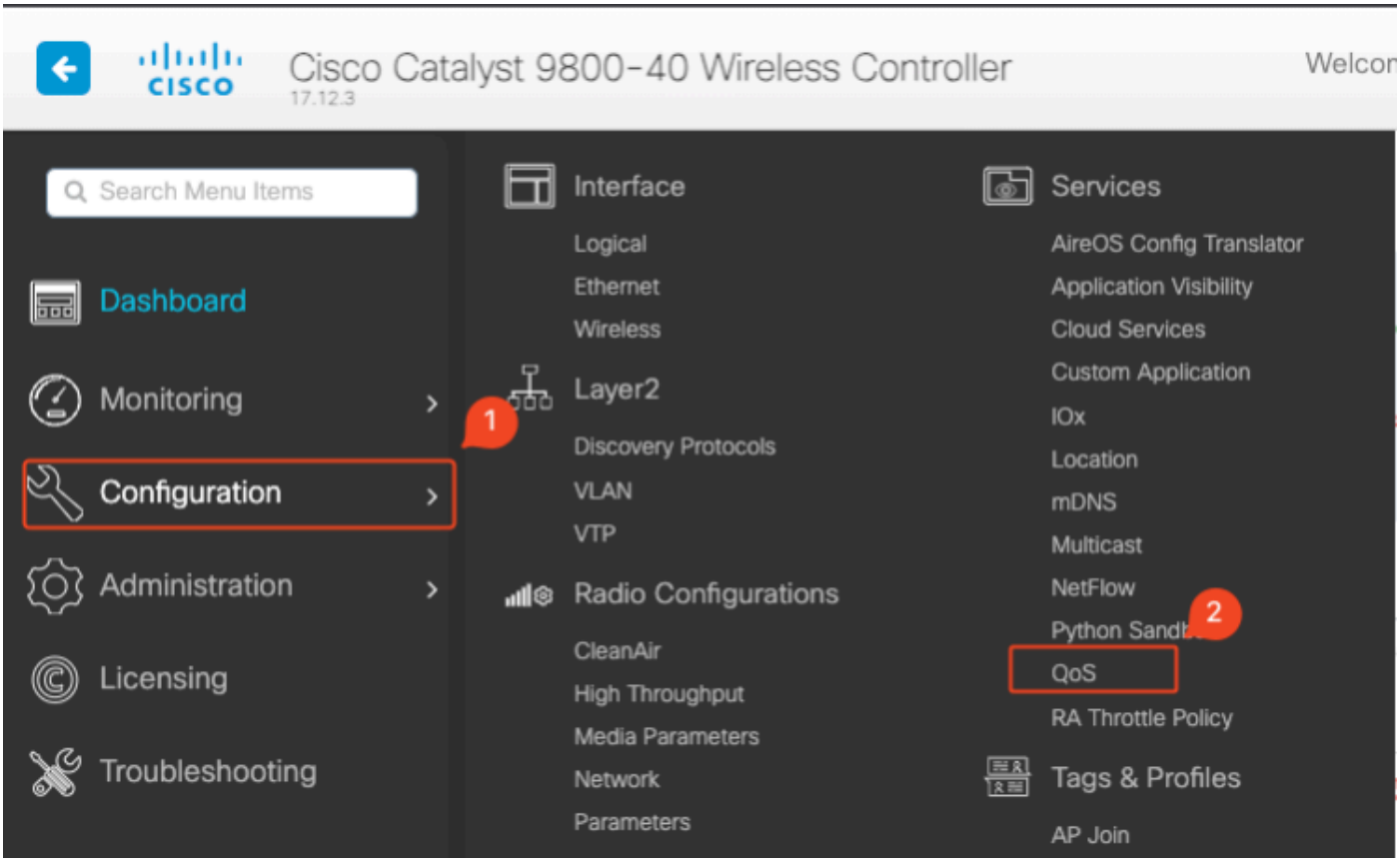
A QoS automática sem fio automatiza a implantação de recursos de QoS sem fio. Ele tem um conjunto de perfis predefinidos que podem ser modificados pelo administrador para priorizar fluxos de tráfego diferentes. A QoS automática corresponde ao tráfego e atribui cada pacote correspondente a grupos de QoS. Isso permite que o mapa de política de saída coloque grupos de QoS específicos em filas específicas, incluindo a fila de prioridade.

Modo	Ingresso do cliente	Saída do cliente	Entrada de BSSID	Saída de BSSID	Entrada de porta	Porta de saída	Rádio
Voz	N/A	N/A	Platinum-up	platinum	N/A	AutoQos-4.0-wlan-Port-Output-Policy	ACM em
Convidado	N/A	N/A	AutoQos-4.0-	AutoQos-4.0-	N/A	AutoQos-4.0-	

			wlan-GT-SSID-Input-Policy	wlan-GT-SSID-Output-Policy		wlan-Port-Output-Policy	
Fastlane	N/A	N/A	N/A	N/A	N/A	AutoQos-4.0-wlan-Port-Output-Policy	edca-parameters fastlane
Enterprise-avc	N/A	N/A	AutoQos-4.0-wlan-ET-SSID-Input-AVC-Policy	AutoQos-4.0-wlan-ET-SSID-Output-Policy	N/A	AutoQos-4.0-wlan-Port-Output-Policy	

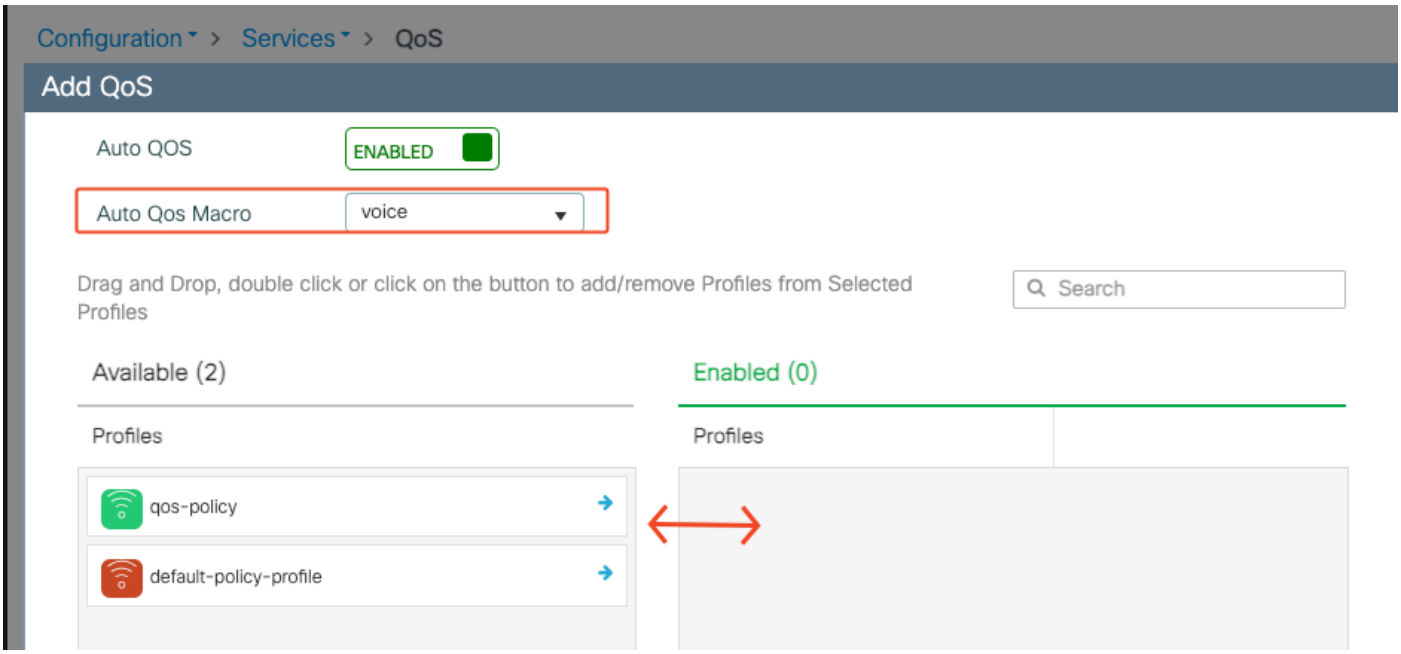
Esta tabela descreve as alterações de configuração que acontecem quando um perfil de QoS automático é aplicado.

Para configurar a QoS automática, navegue até Configuration > QoS



Fluxo de trabalho de QoS

Clique em Add e defina Auto QoS como enabled. Escolha a macro Auto QoS apropriada na lista. Para este exemplo, é usada a macro Voice para priorizar o tráfego de voz.



Mapeamento de voz AutoQoS

Quando a macro estiver habilitada, selecione a política que precisa ser anexada à política.

Configuração automática de QoS CLI

```
# enable
# wireless autoqos policy-profile default-policy-profile mode voice
```

Agora que a QoS automática está ativada, você pode ver as alterações que aconteceram. Esta seção lista as alterações de configuração para voz.

```
class-map match-any AutoQos-4.0-Output-CAPWAP-C-Class
 match access-group name AutoQos-4.0-Output-Acl-CAPWAP-C
class-map match-any AutoQos-4.0-Output-Voice-Class
 match dscp ef
policy-map AutoQos-4.0-wlan-Port-Output-Policy
 class AutoQos-4.0-Output-CAPWAP-C-Class
  priority level 1
 class AutoQos-4.0-Output-Voice-Class
  priority level 2
 class class-default
interface TenGigabitEthernet0/0/0
 service-policy output AutoQos-4.0-wlan-Port-Output-Policy
interface TenGigabitEthernet0/0/1
 service-policy output AutoQos-4.0-wlan-Port-Output-Policy
interface TenGigabitEthernet0/0/2
 service-policy output AutoQos-4.0-wlan-Port-Output-Policy
interface TenGigabitEthernet0/0/3
 service-policy output AutoQos-4.0-wlan-Port-Output-Policy
ip access-list extended AutoQos-4.0-Output-Acl-CAPWAP-C
 10 permit udp any eq 5246 16666 any
wireless profile policy qos-policy
```

```
 autoqos mode voice
 service-policy input platinum-up
 service-policy output platinum
ap dot11 24ghz cac voice acm
ap dot11 5ghz cac voice acm
ap dot11 6ghz cac voice acm
```

CLI QoS modular

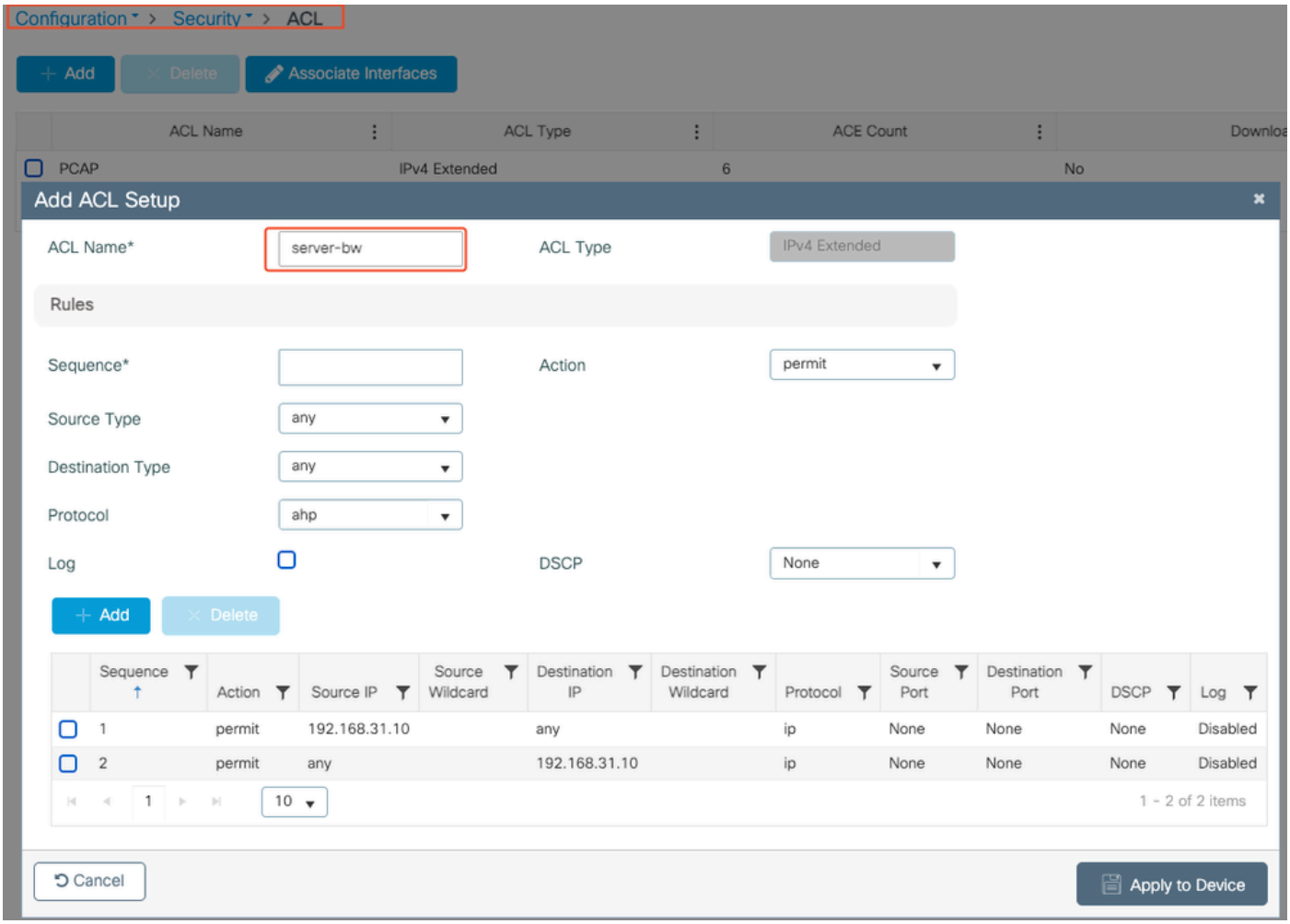
O MQC permite que você defina uma classe de tráfego, crie uma política de tráfego (mapa de políticas) e anexe a política de tráfego a uma interface. A política de tráfego contém o recurso de QoS que se aplica à classe de tráfego.

Fluxo de trabalho do MQS CLI

Este exemplo demonstra como usar Listas de Controle de Acesso (ACLs) para classificar o tráfego e aplicar restrições de largura de banda.

Crie uma ACL para identificar e classificar o tráfego específico que você deseja gerenciar. Isso pode ser feito definindo regras que correspondam ao tráfego com base em critérios como endereços IP, protocolos ou portas.

Navegue até Configuration > Security > ACL e adicione a ACL.

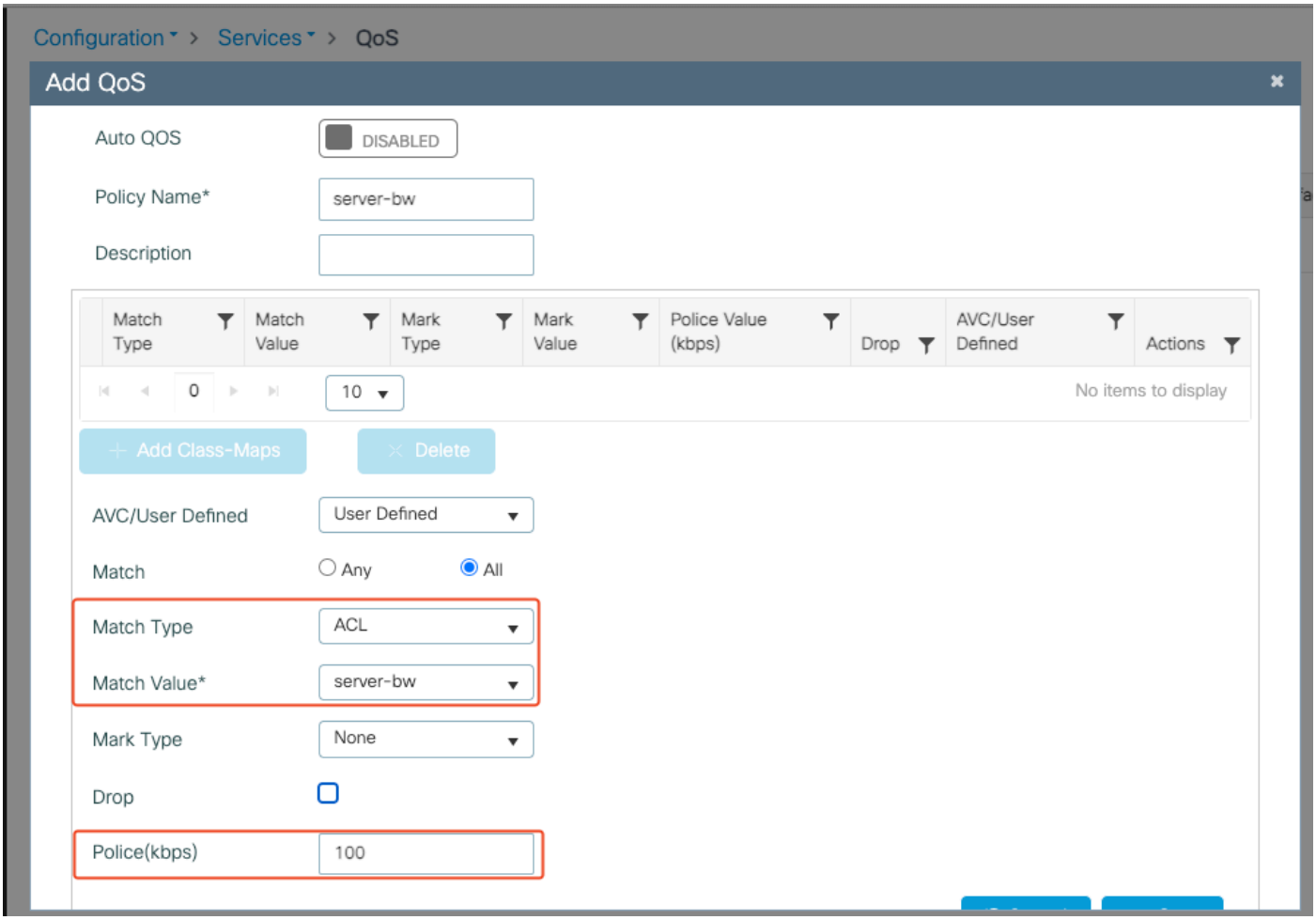


Configuração da ACL

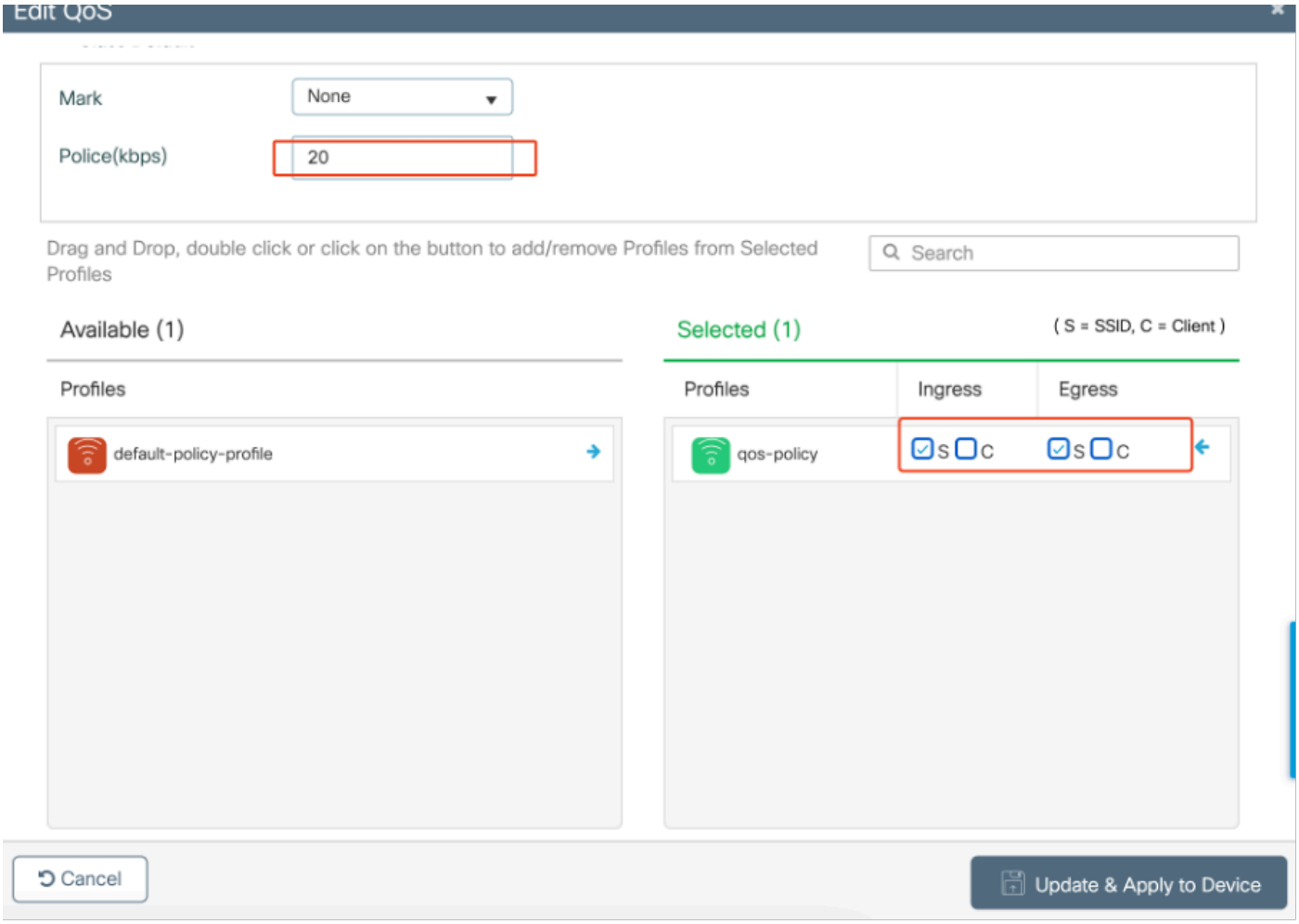
Depois que o tráfego for classificado usando a ACL, configure as restrições de largura de banda para controlar a quantidade de largura de banda alocada para esse tráfego.

Navegue até Configuration > Services > QoS e a política de QoS. Anexe a ACL dentro da política e aplique a polícia em kbps.

Role para baixo e selecione o perfil de política onde a QoS deve ser aplicada. Você pode selecionar a política na direção de entrada/ saída para SSID ou Cliente.



Política MQS



Perfil MQS

configuração MQS CLI

```
ip access-list extended server-bw
1 permit ip host 192.168.31.10  any
!
class-map match-any server-bw
match access-group name server-bw
!
policy-map server-bw
class server-bw
  police cir 100000
   conform-action transmit
   exceed-action drop
exit
class class-default
police cir 20000
conform-action transmit
exceed-action drop
exit
wireless profile policy default-policy-profile
service-policy input server-bw
service-policy output server-bw
exit
```

QoS de metal

A finalidade principal desses perfis de QoS é limitar os valores máximos de Differentiated Services Code Point (DSCP) permitidos em uma rede sem fio, controlando assim os valores de Prioridade do usuário (UP) 802.11.

No Cisco 9800 Wireless LAN Controller (WLC), os perfis de Metal QoS são predefinidos e não configuráveis. No entanto, você pode aplicar esses perfis a SSIDs ou clientes específicos para aplicar políticas de QoS.

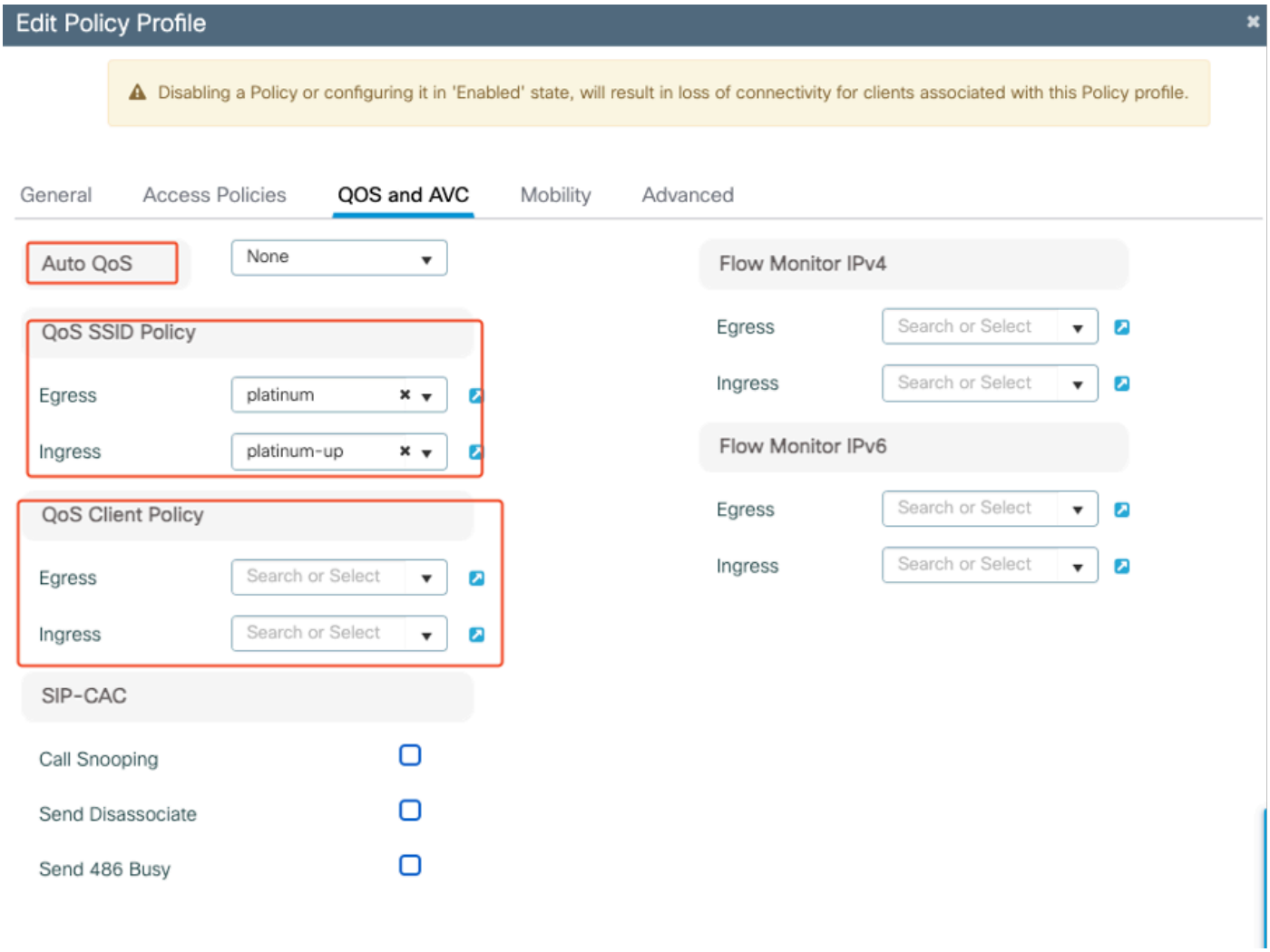
Há quatro perfis de QoS Metal disponíveis:

Perfil de QoS	DSCP máximo
Bronze	8
Prata	0
Ouro	34
Platinum	46

Para configurar o Metal QoS em um Cisco 9800 WLC:

Navegue até Configuration > Policy > QoS & AVC.

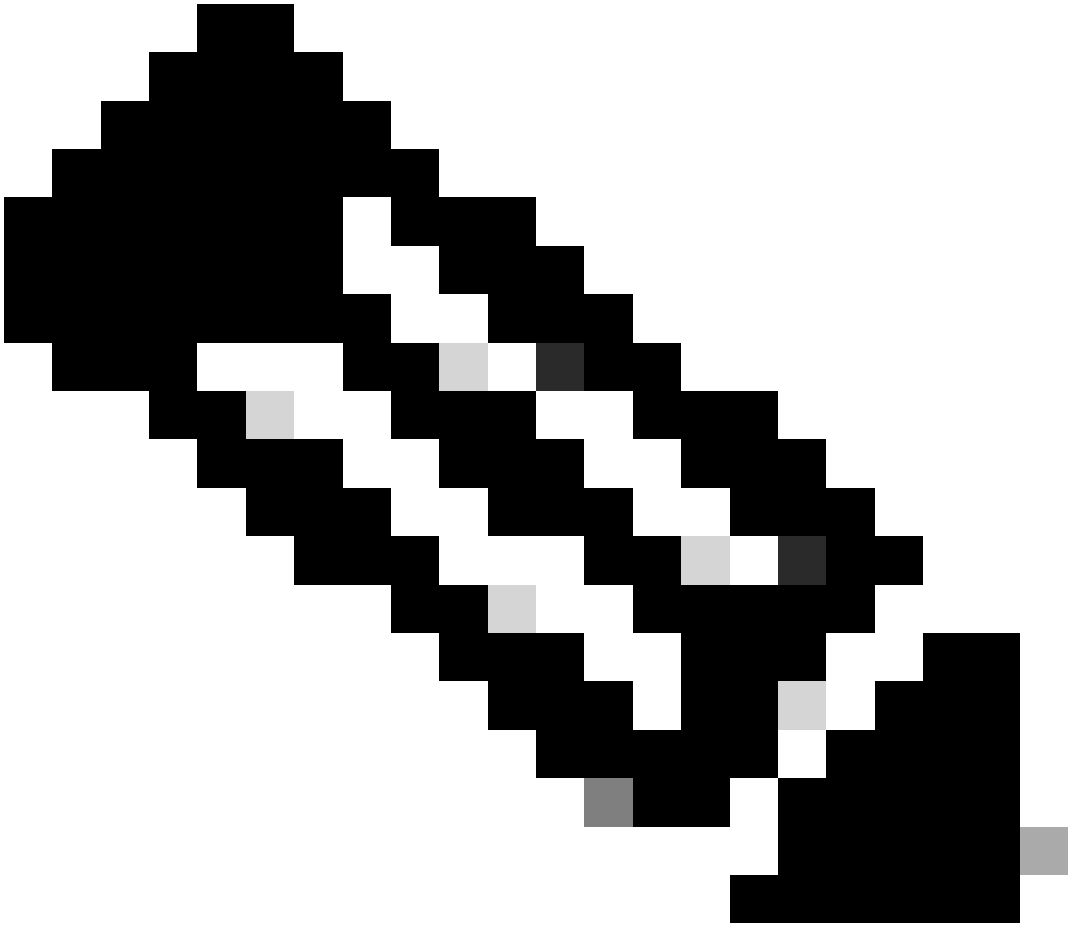
- Selecione o perfil Metal QoS desejado (Platinum, Gold, Silver ou Bronze).
- Aplique o perfil escolhido ao SSID ou cliente de destino.



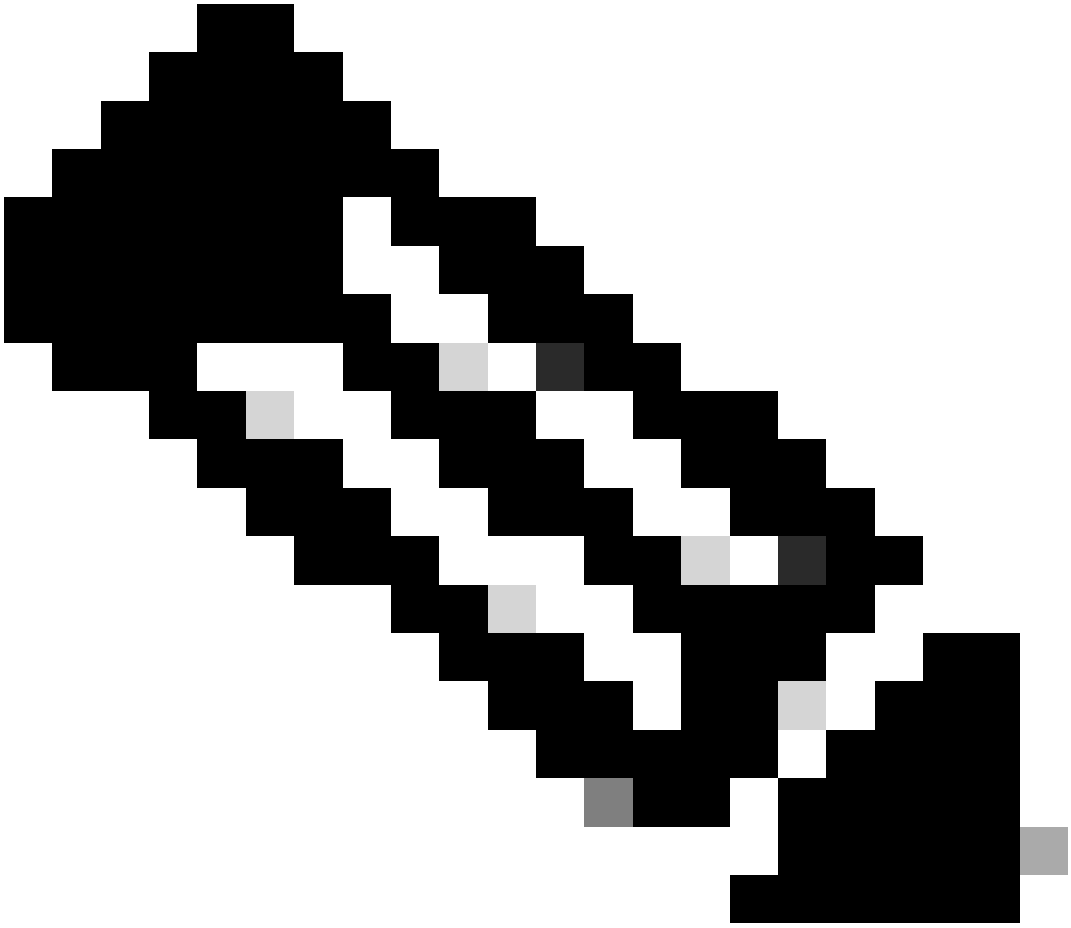
Perfil de QoS metálico

Configuração da CLI de QoS do Metal

```
#configure terminal
#wireless profile policy qos-policy
 service-policy input platinum-up
 service-policy output platinum
```



Observação: os contratos de largura de banda por usuário e SSID são configuráveis por meio de políticas de QoS e não diretamente no Metal QoS. Em 9800, o tráfego não correspondente passa para a classe padrão.



Observação: na GUI, você só pode definir o Metal QoS por SSID. Na CLI, você também pode configurá-la no destino do cliente.

Validar QoS de ponta a ponta com captura de pacotes

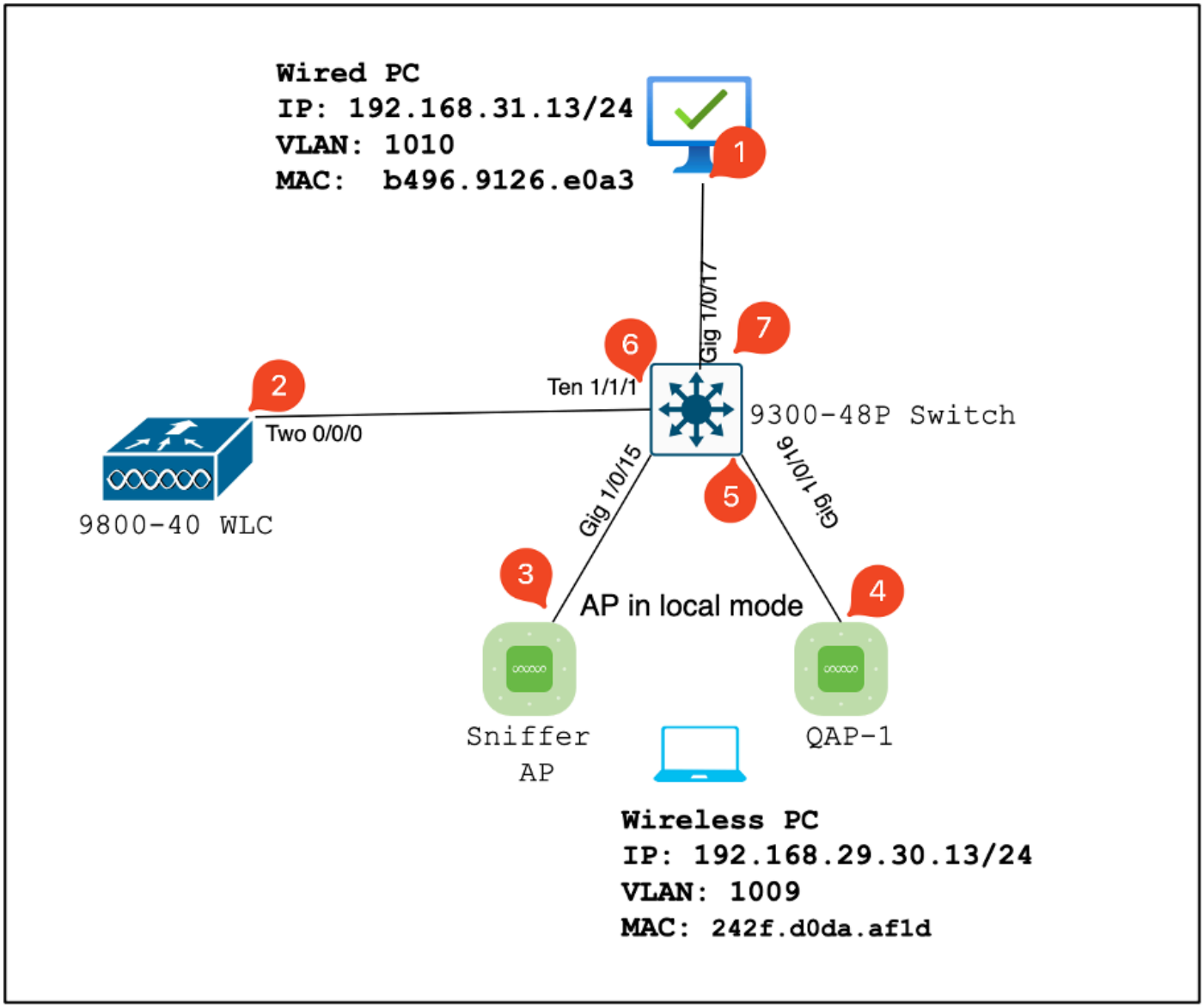
Agora que a configuração de QoS está concluída, é essencial examinar os pacotes de QoS e validar se as políticas de QoS estão funcionando corretamente de ponta a ponta. Isso pode ser obtido por meio da captura e análise de pacotes.

Para replicar e validar a configuração de QoS, um ambiente de laboratório de pequena escala é usado. O laboratório inclui estes componentes:

- WLC
- AP
- O Sniffer AP vai pegar o OTA
- PC com fio
- Switch

Todos esses componentes estão conectados ao mesmo switch no ambiente do laboratório. Os números destacados neste diagrama indicam os pontos em que as capturas de pacotes estão habilitadas para monitorar e analisar o fluxo de tráfego.

Diagrama de Rede



Topologia de laboratório

Componentes de laboratório e pontos de captura de pacotes

WLC:

- Gerencia as políticas e configurações de QoS para a rede sem fio.
- Ponto de captura de pacotes: Capture o tráfego entre a WLC, o AP e o switch.

AP:

- Fornece conectividade sem fio aos clientes e aplica políticas de QoS.
- Ponto de captura de pacote: Capture o tráfego entre o AP e o switch.

AP farejador:

- Atua como um dispositivo dedicado para capturar o tráfego sem fio.
- Ponto de captura de pacote: Capture o tráfego sem fio entre o AP e os clientes sem fio.

PC com fio:

- Conectado ao switch para simular tráfego com fio e validar QoS de ponta a ponta.
- Ponto de captura de pacote: Capture pacotes QoS transmitidos e recebidos pelo link com fio.

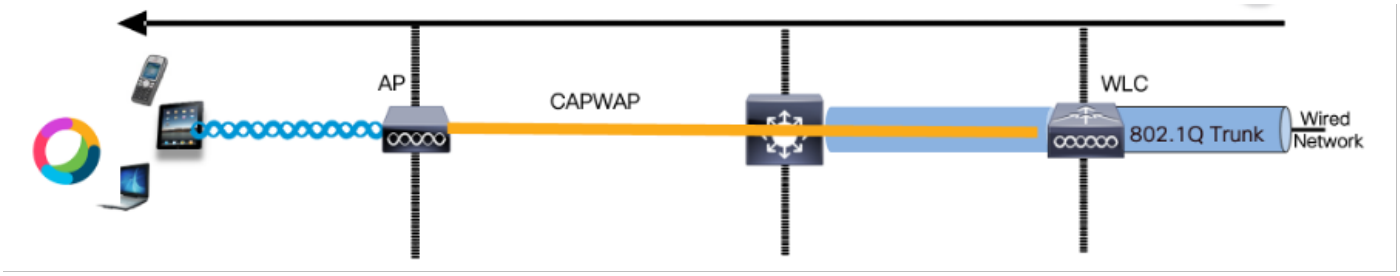
PC sem fio:

- Conectado à WLAN para simular tráfego sem fio e validar QoS de ponta a ponta.
- Ponto de captura de pacotes: Captura pacotes QoS transmitidos e recebidos pelo link sem fio.

Switch:

- O dispositivo central que interconecta todos os componentes do laboratório e facilita o fluxo do tráfego.
- Pontos de captura de pacotes: capturar o tráfego em várias portas de switch para validar a aplicação adequada da QoS.

Logicamente, a topologia do LAB pode ser desenhada assim.



Topologia de LABORATÓRIO Lógico

Para testar e validar a configuração de QoS, o iPerf é usado para gerar tráfego entre o cliente e o servidor. Esses comandos são usados para facilitar a comunicação iPerf, com as funções do servidor e do cliente intercambiadas com base na direção do teste de QoS.

Cenário de teste 1: validação de QoS downstream

O objetivo é validar a configuração de QoS downstream. A configuração envolve um PC com fio que envia pacotes com DSCP 46 para um PC sem fio.
A controladora Wireless LAN (WLC) é configurada com a política "Platinum QoS" para as direções downstream e upstream.

Configuração do teste:

- Fluxo de tráfego:

Fonte: PC com fio

Destino: PC sem fio

Tipo de tráfego: pacotes UDP com DSCP 46

- Configuração da política de QoS no WLC:

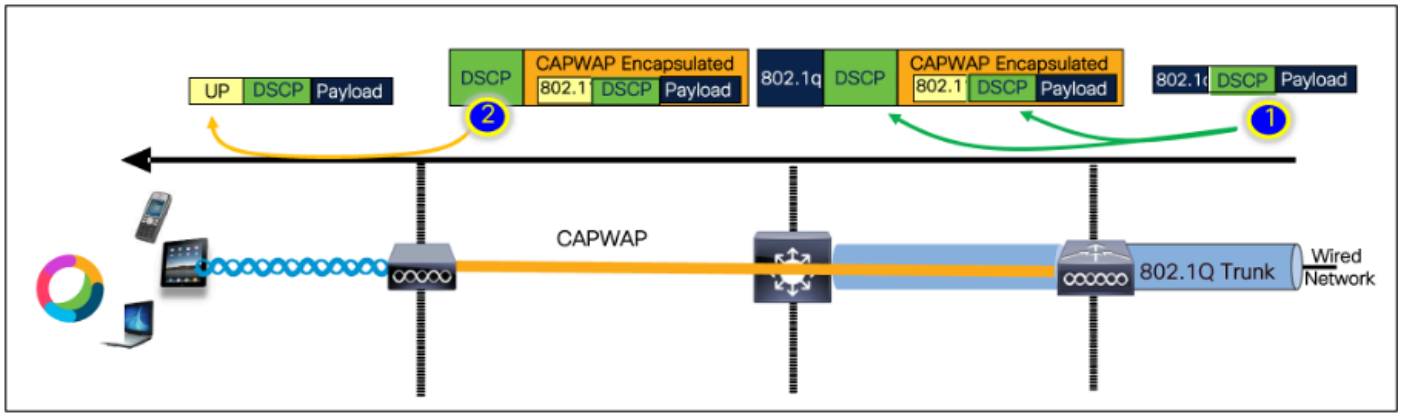
Perfil de QoS: QoS Metal - QoS Platinum

Direção: downstream e upstream

- Comandos de configuração de QoS de metal:

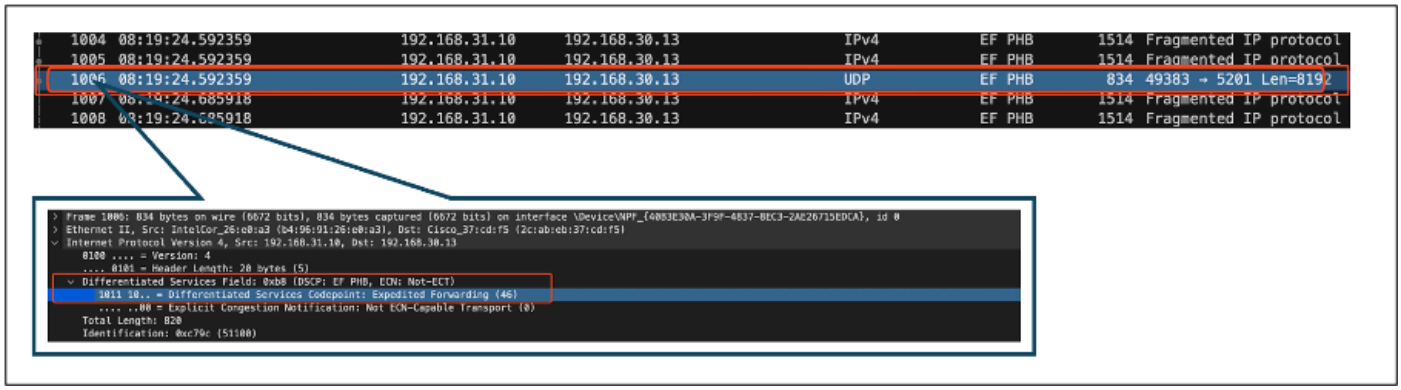
```
wireless profile policy qos-policy
service-policy input platinum-up
service-policy output platinum
```

Topologia lógica e conversação de DSCP na direção downstream.



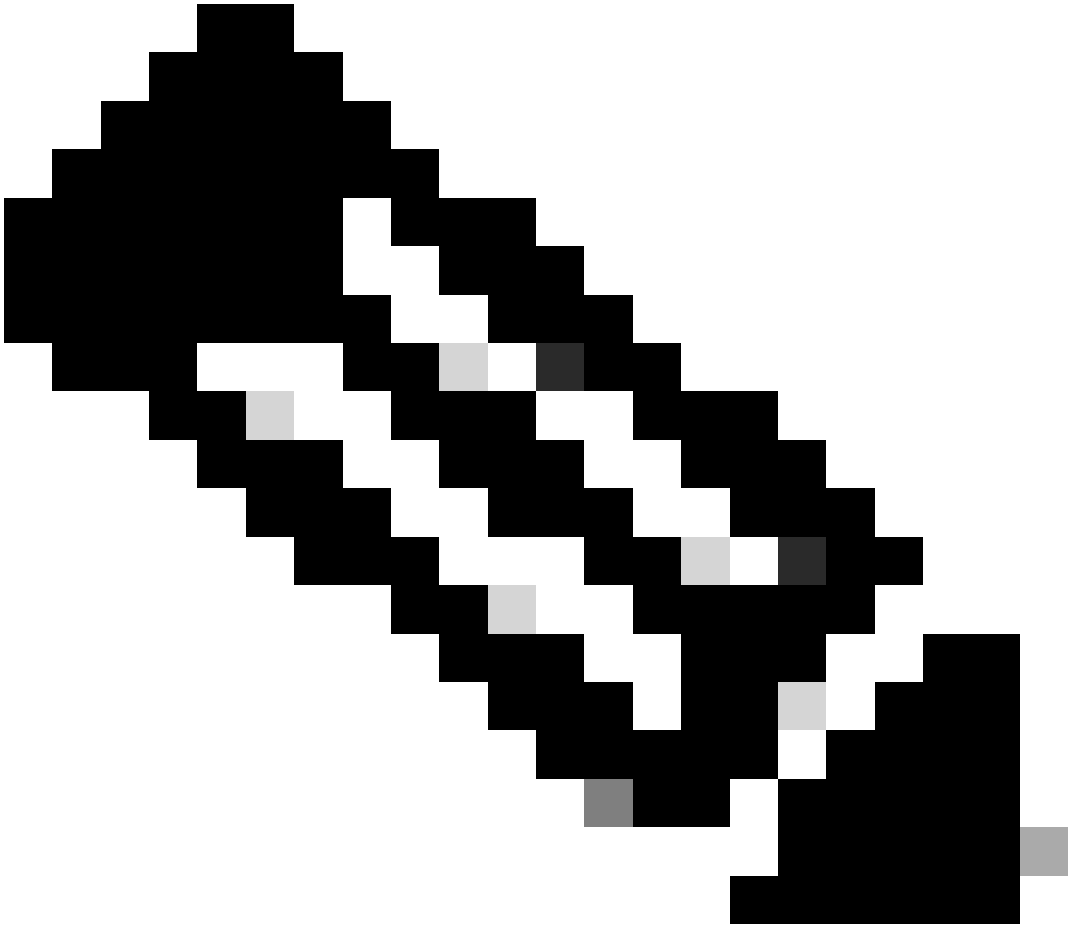
Ponto de conversação DSCP

Captura de pacotes realizada no PC com fio. Isso confirma que o PC com fio está enviando pacotes UDP para o IP de destino especificado 192.168.10.13 com a marcação de DSCP correta de 46.

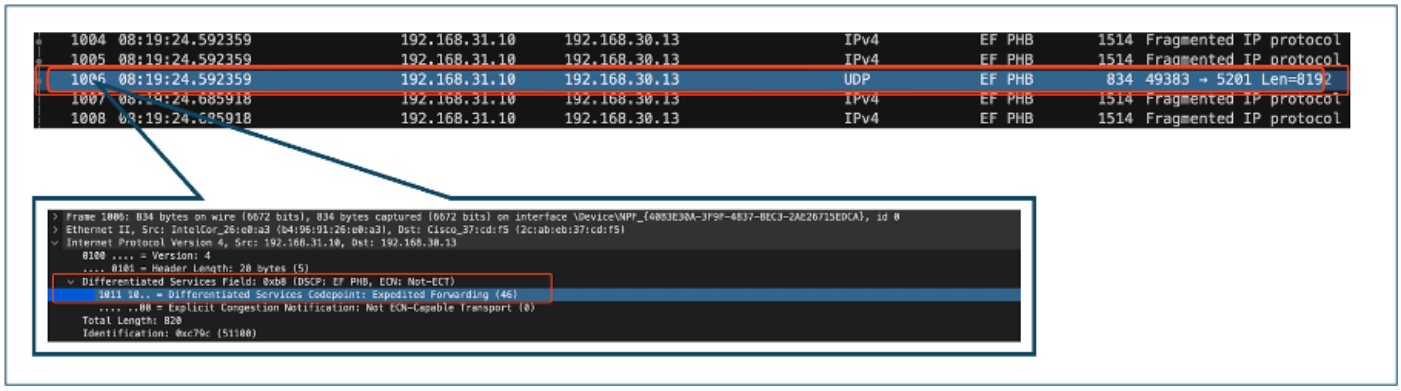


Captura de PC com fio - Direção de downstream

Em seguida, vamos examinar um pacote capturado no switch de uplink conectado ao PC com fio. O switch confia na marca DSCP e o valor de DSCP permanece inalterado em 46.

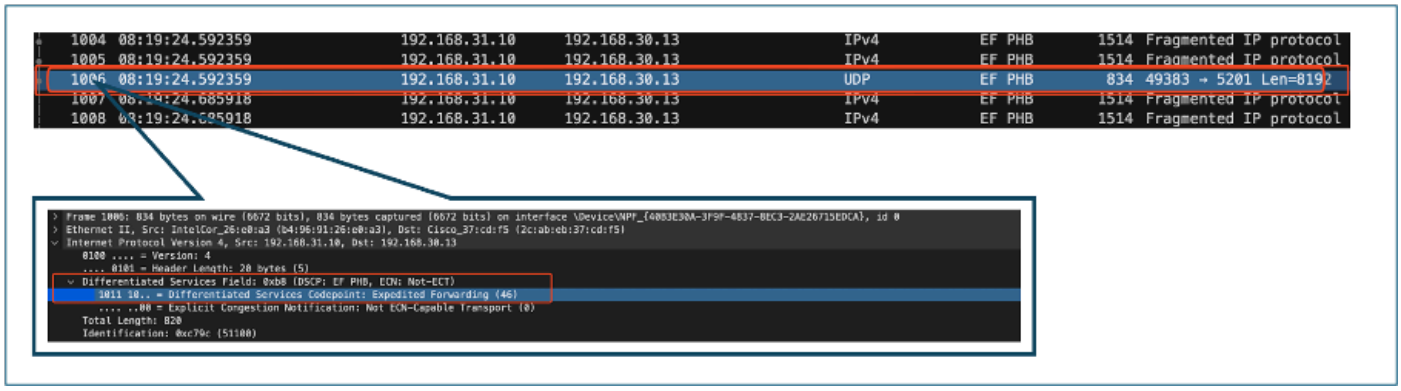


Observação: as portas do switch na série Catalyst 9000 assumem como padrão um estado confiável.



Captura de Interface de Uplink de PC com Fio

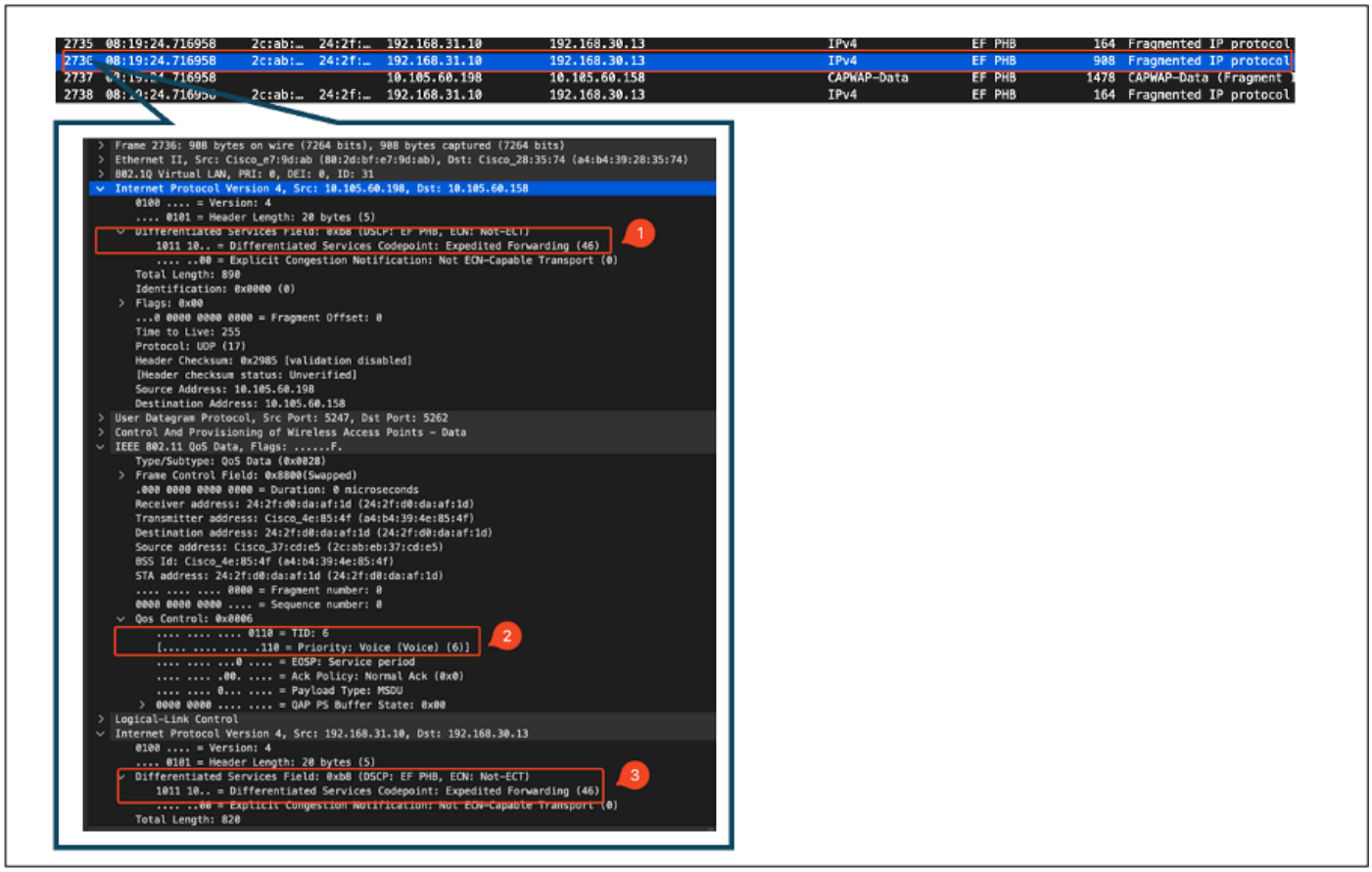
Ao examinar a captura de pacotes na WLC feita usando EPC, o pacote chega com a mesma marca de DSCP de 46 do switch de uplink. Isso confirma que a marcação de DSCP é preservada quando o pacote chega à WLC.



Direção de downstream de WLC EPC

Quando a WLC envia o pacote para o AP dentro de um túnel CAPWAP, é uma interseção crítica onde a WLC pode modificar o DSCP com base em sua configuração. Vamos dividir a captura de pacotes, que é destacada com pontos numerados para maior clareza:

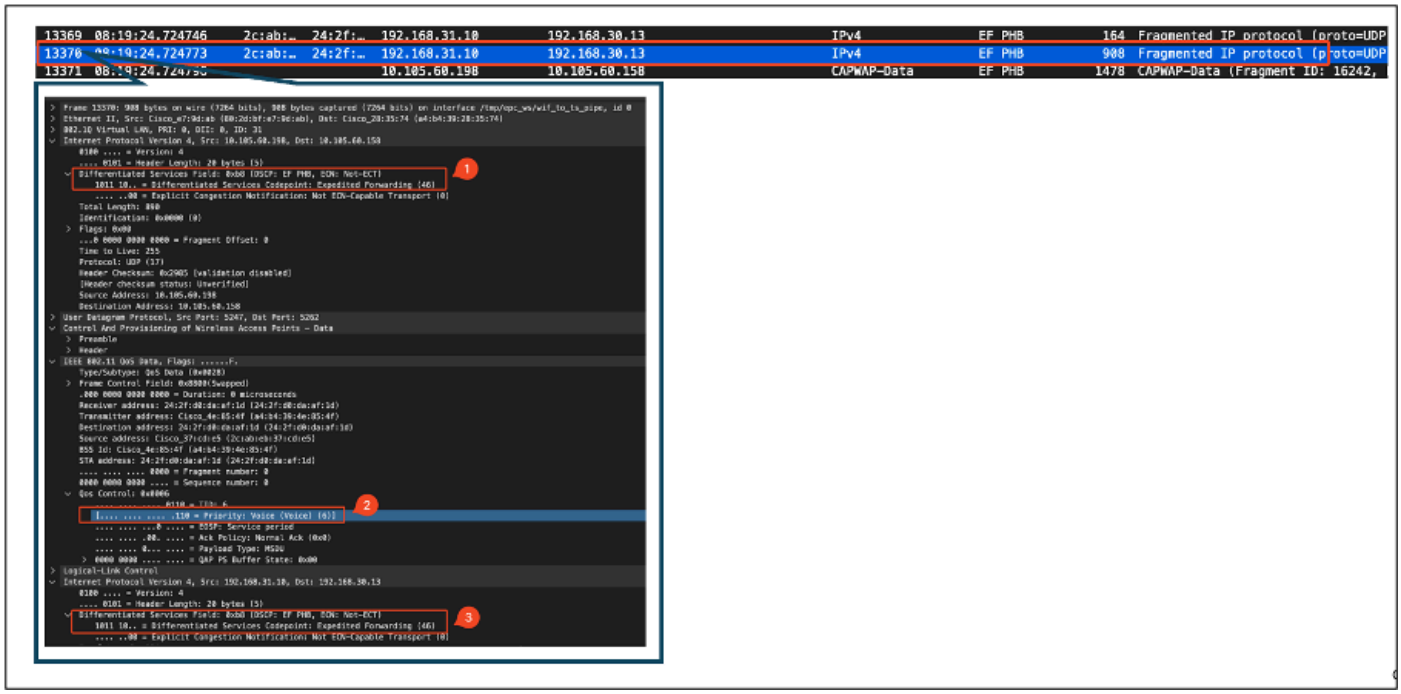
- CAPWAP Outer Layer: A camada externa do túnel CAPWAP mostra a marca DSCP como 46, que é o valor recebido da extremidade do switch.
- 802.11 UP Value Inside CAPWAP: Dentro do túnel CAPWAP, a WLC mapeia o DSCP 46 para 802.11 User Priority (UP) 6, que corresponde ao tráfego de voz.
- Valor de DSCP dentro do CAPWAP: o Cisco 9800 WLC opera com um modelo de DSCP confiável, de modo que o valor de DSCP dentro do túnel CAPWAP é mantido em 46 igual à camada de DSCP externa.



Marcações CAPWAP DSCP

Em seguida, verifique o mesmo pacote na porta do switch de uplink AP.

O valor de DSCP na camada CAPWAP externa permanece em 46. Para fins ilustrativos, o tráfego CAPWAP interno é destacado para mostrar a marcação.

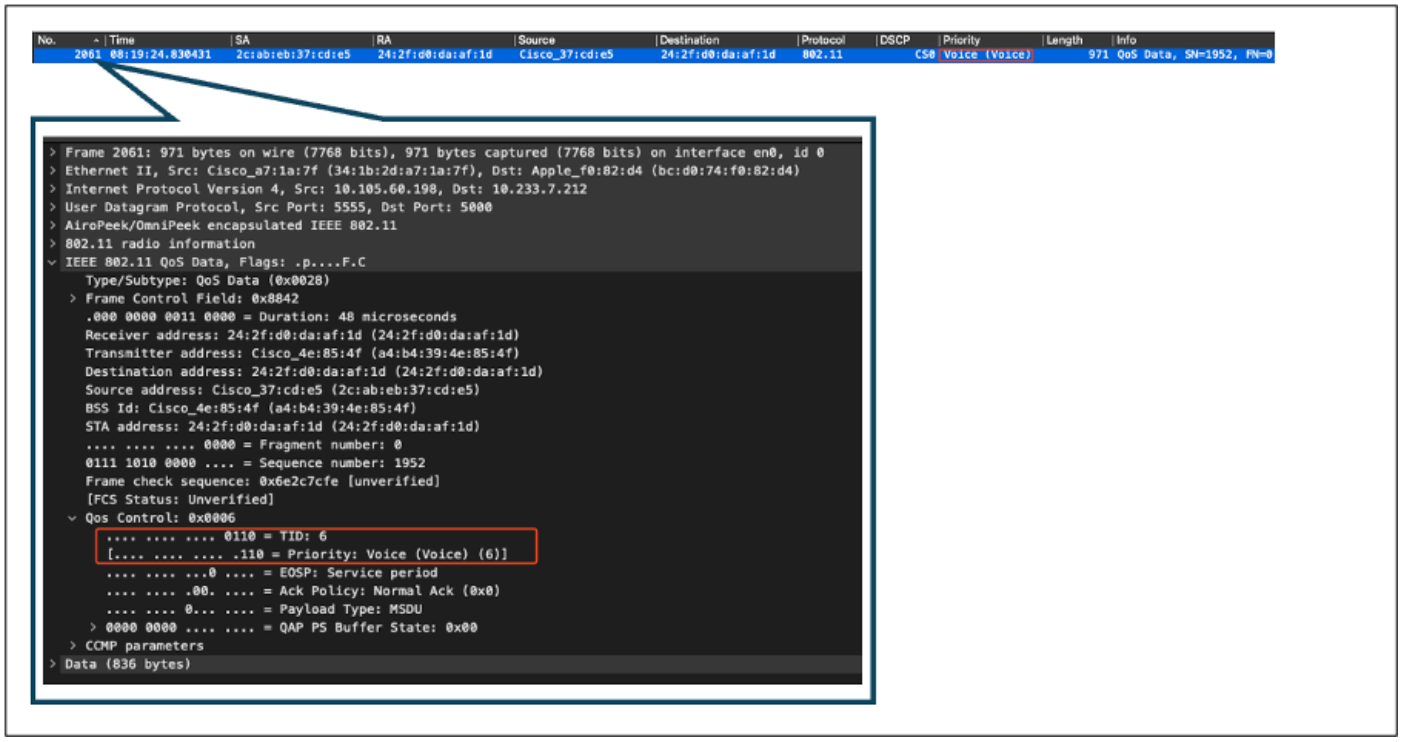


Captura da interface do switch de uplink AP

Uma vez que o AP recebe o pacote, ele transmite o pacote pelo ar. Para verificar a marcação UP

(User Priority, Prioridade de usuário), é usada uma captura OTA (Over-the-Air, No ar) feita com um sniffer AP.

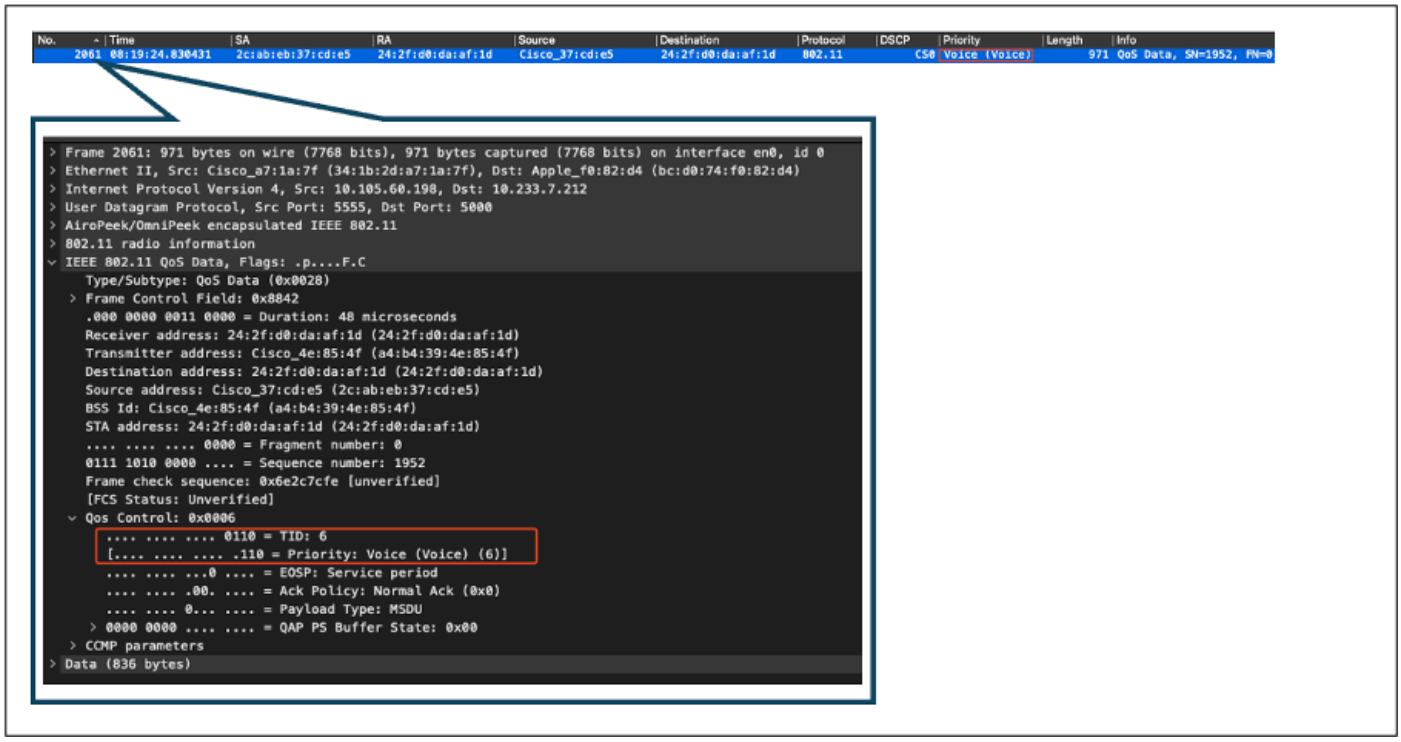
O AP encaminhou o quadro com um valor de UP de 6. Isso confirma que o AP mapeia corretamente o valor de DSCP para o valor de UP 802.11 apropriado (6), que corresponde ao tráfego de voz.



Captura OTA do AP para o cliente

Na etapa final, o pacote recebido pelo PC sem fio. O PC sem fio recebe o quadro com um valor de DSCP de 46.

Isso indica que a marcação de DSCP é preservada em todo o caminho de transmissão, do PC com fio ao PC sem fio. O valor consistente de DSCP de 46 confirma que as políticas de QoS são corretamente aplicadas e mantidas na direção de downstream.



Captura de PC sem fio

Cenário de teste 2: Validação de QoS upstream

Neste cenário de teste, o objetivo é validar a configuração de QoS upstream. A configuração envolve um PC sem fio que envia pacotes UDP com DSCP 46 para um PC com fio. A WLC é configurada com a política de "QoS Platinum" para as direções de upstream e downstream.

- Fluxo de tráfego:

Fonte: PC sem fio

Destino: PC com fio

Tipo de tráfego: pacotes UDP com DSCP 46

- Configuração da política de QoS no WLC:

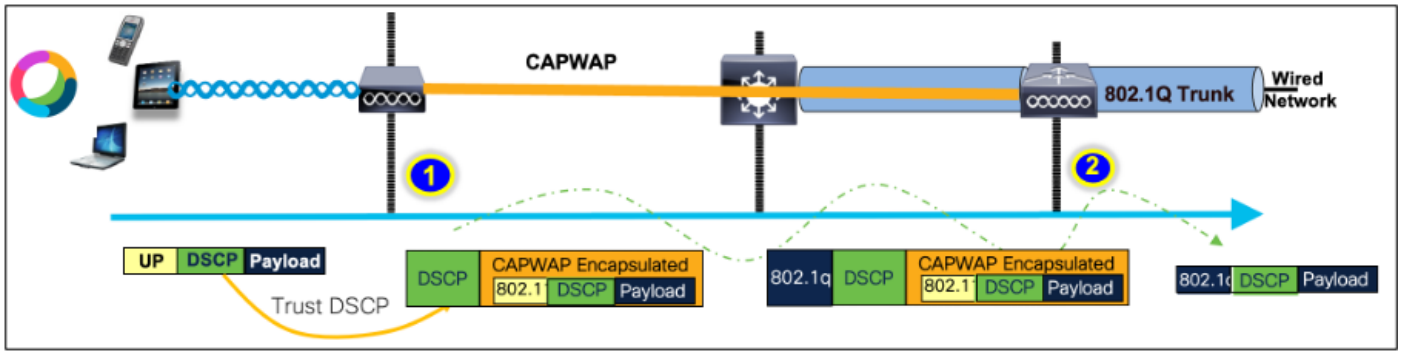
Perfil de QoS: QoS Platinum

Direção: upstream e downstream

- Comandos de configuração de QoS de metal:

```
wireless profile policy qos-policy
service-policy input platinum-up
service-policy output platinum
```

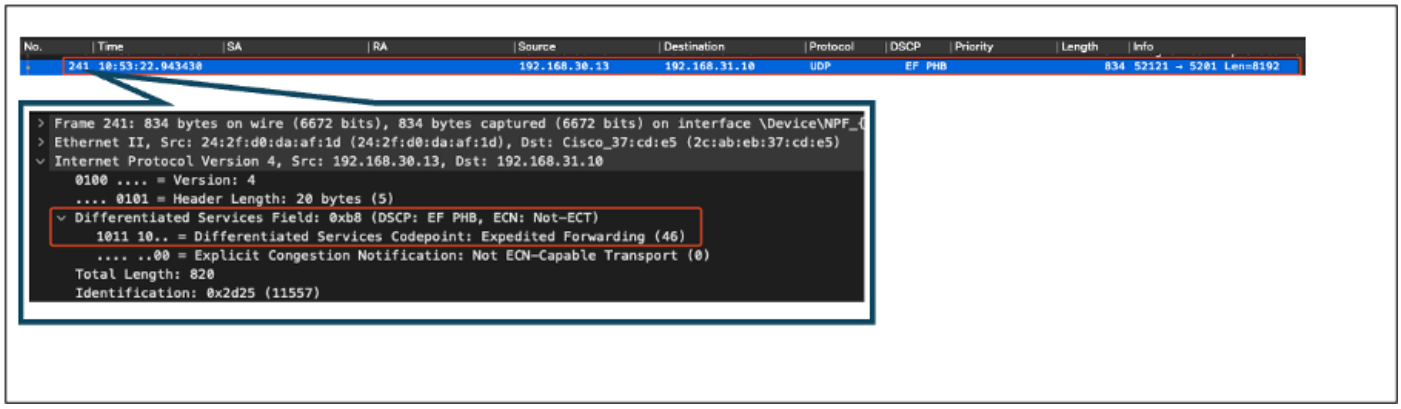
Topologia lógica e conversão de DSCP na direção upstream:



Topologia Lógica e Conversão de DSCP - Upstream

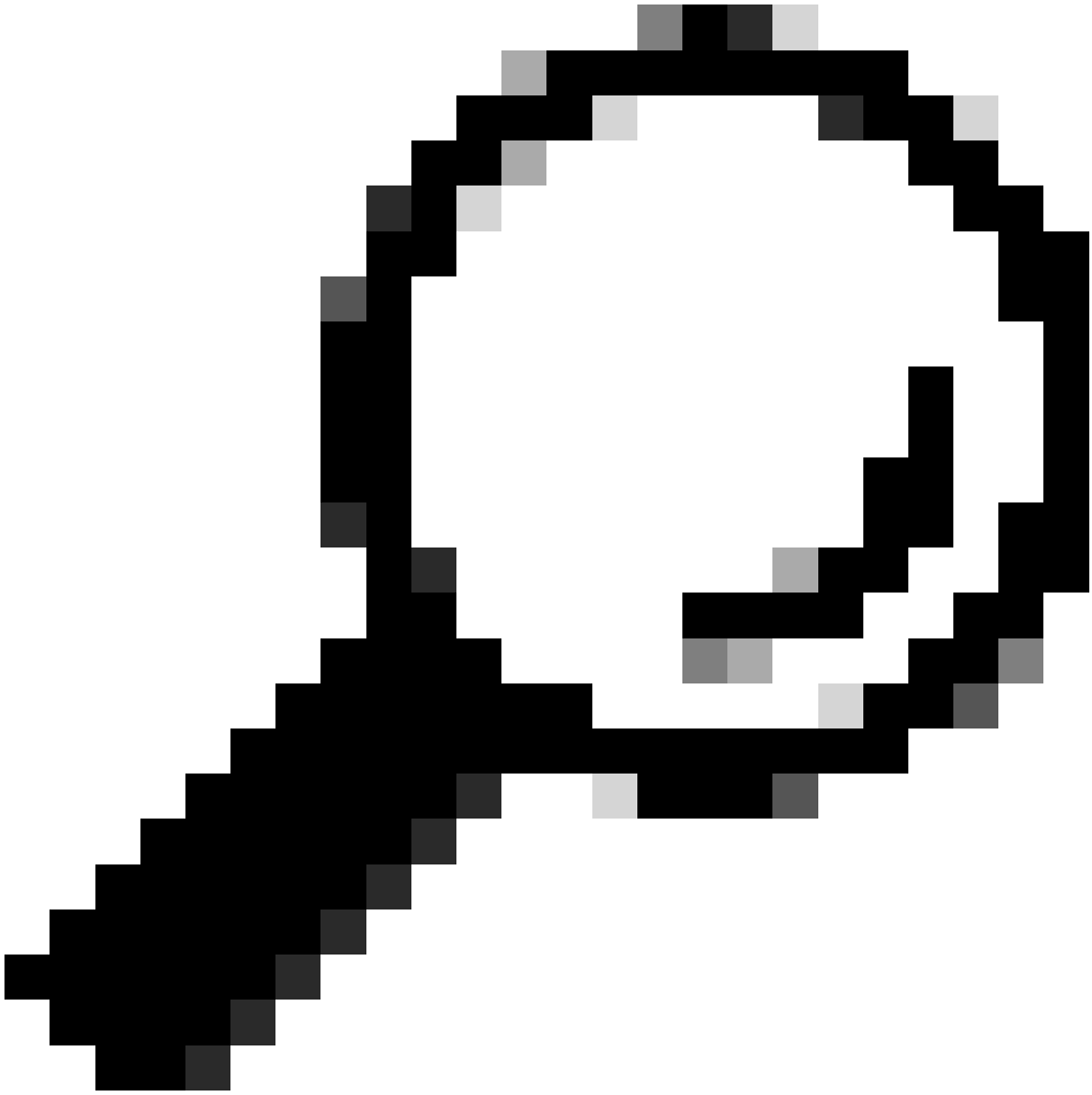
Pacotes enviados do PC sem fio para o PC com fio. Essa captura é feita no PC sem fio.

O PC sem fio envia pacotes UDP com DSCP 46.

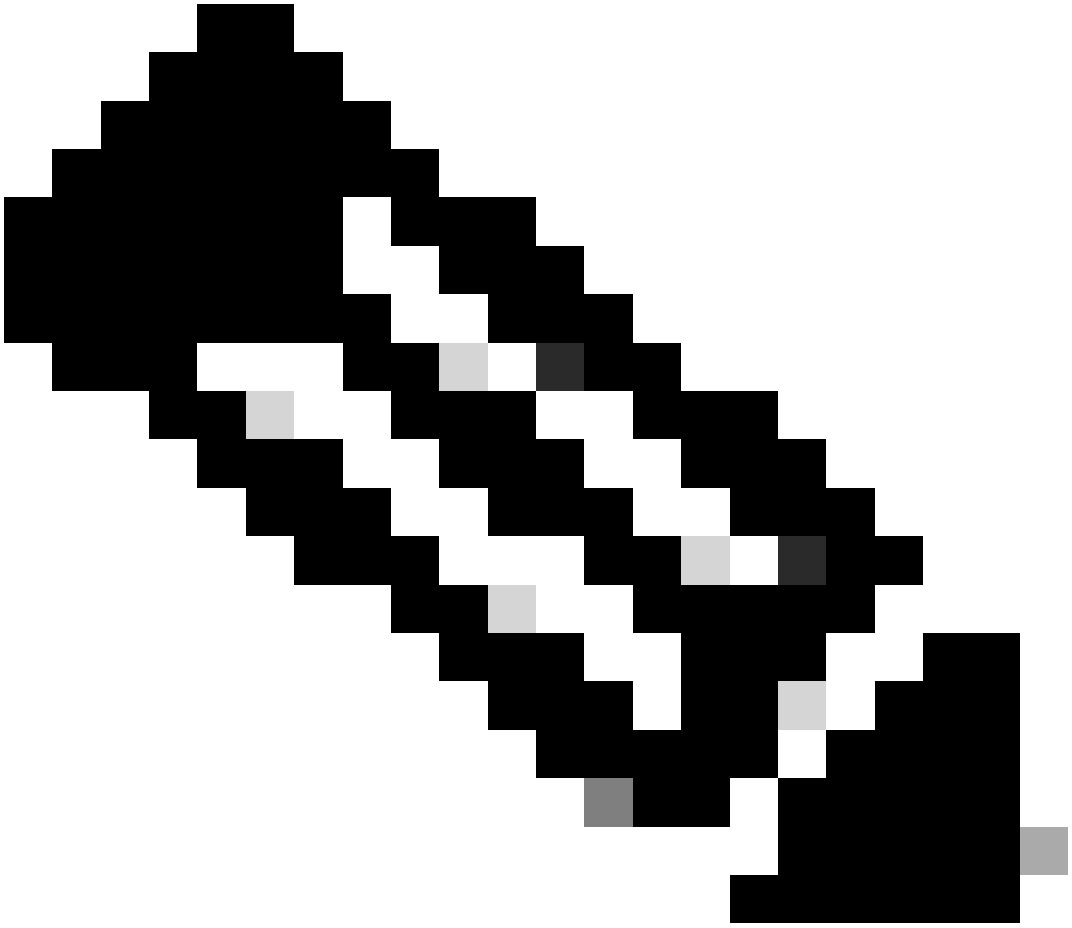


Captura de PC sem fio na direção upstream

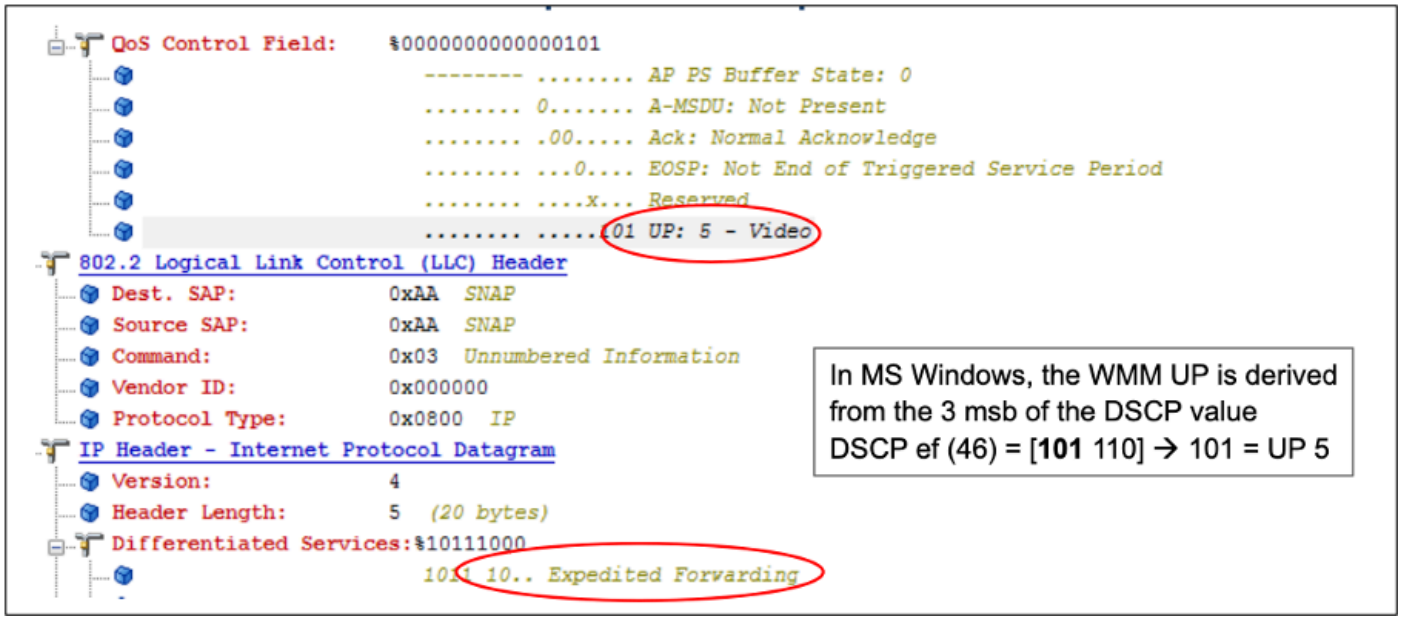
Em seguida, vejamos a captura OTA do cliente para o AP.



Dica: ao usar um PC sem fio Windows para enviar pacotes com DSCP 46, o Windows mapeia o DSCP 46 para um valor de UP (User Priority, Prioridade de usuário) de 5 (Vídeo). Como resultado, a captura OTA mostra os pacotes como tráfego de vídeo (UP 5). No entanto, se você descriptografar o pacote, o valor de DSCP permanecerá em 46.



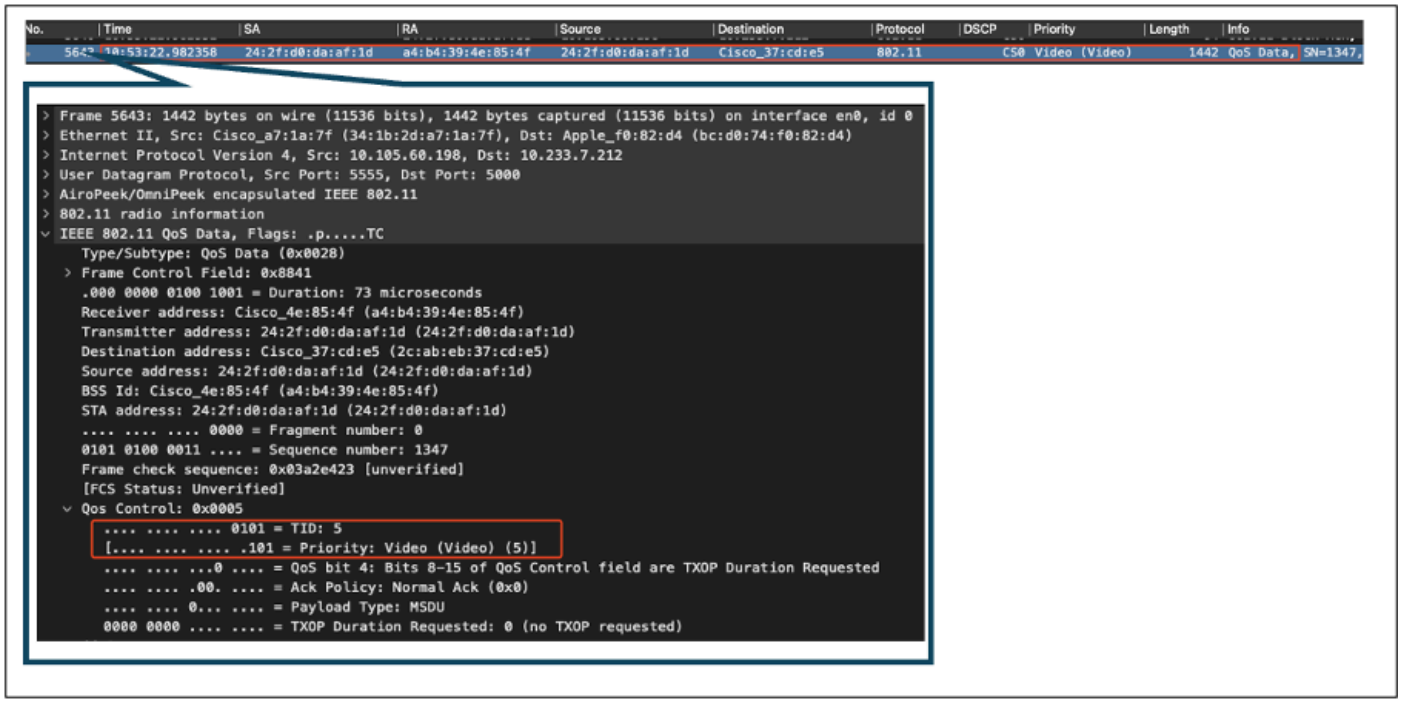
Observação: a partir da versão 17.4, o comportamento padrão do Cisco 9800 WLC é confiar no valor de DSCP no perfil de junção de AP. Isso garante que o valor de DSCP de 46 seja preservado e confiável pelo WLC, evitando qualquer problema relacionado ao comportamento de mapeamento de DSCP para UP do Windows.



Mapeamento de Windows UP para DSCP

A captura OTA criptografada tirada da configuração do laboratório é analisada para validar a configuração de QoS upstream.

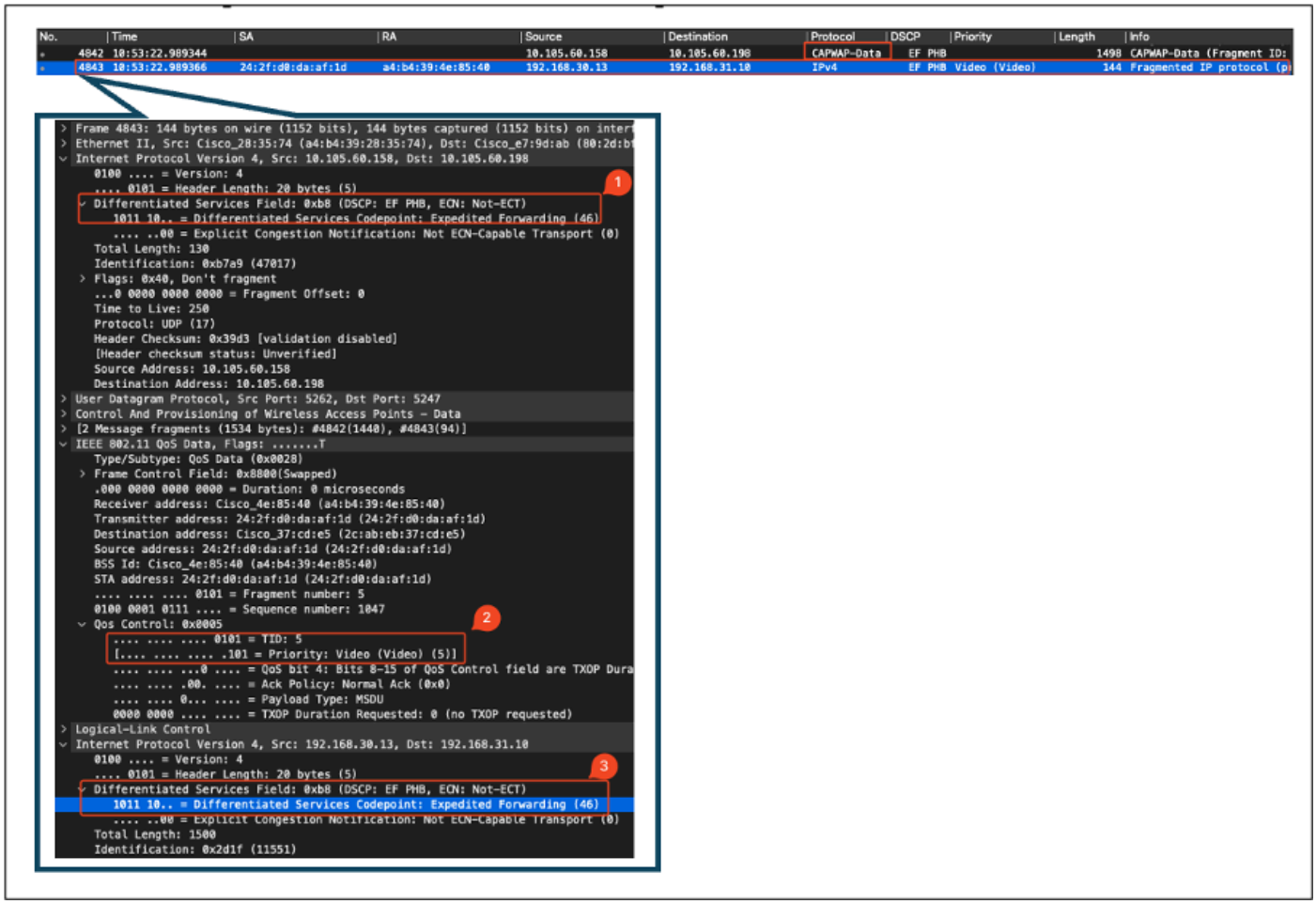
A captura OTA mostra os pacotes com um valor de User Priority (UP) de 5 (Vídeo). Embora a captura OTA mostre UP 5, o valor de DSCP dentro do pacote criptografado permanece em 46.



LAB Setup OTA in Upstream Direction (Configuração do OTA no sentido upstream)

Em seguida, a captura de pacotes na porta de uplink do AP é analisada para garantir que o valor de DSCP seja preservado à medida que o pacote se move do AP para o WLC.

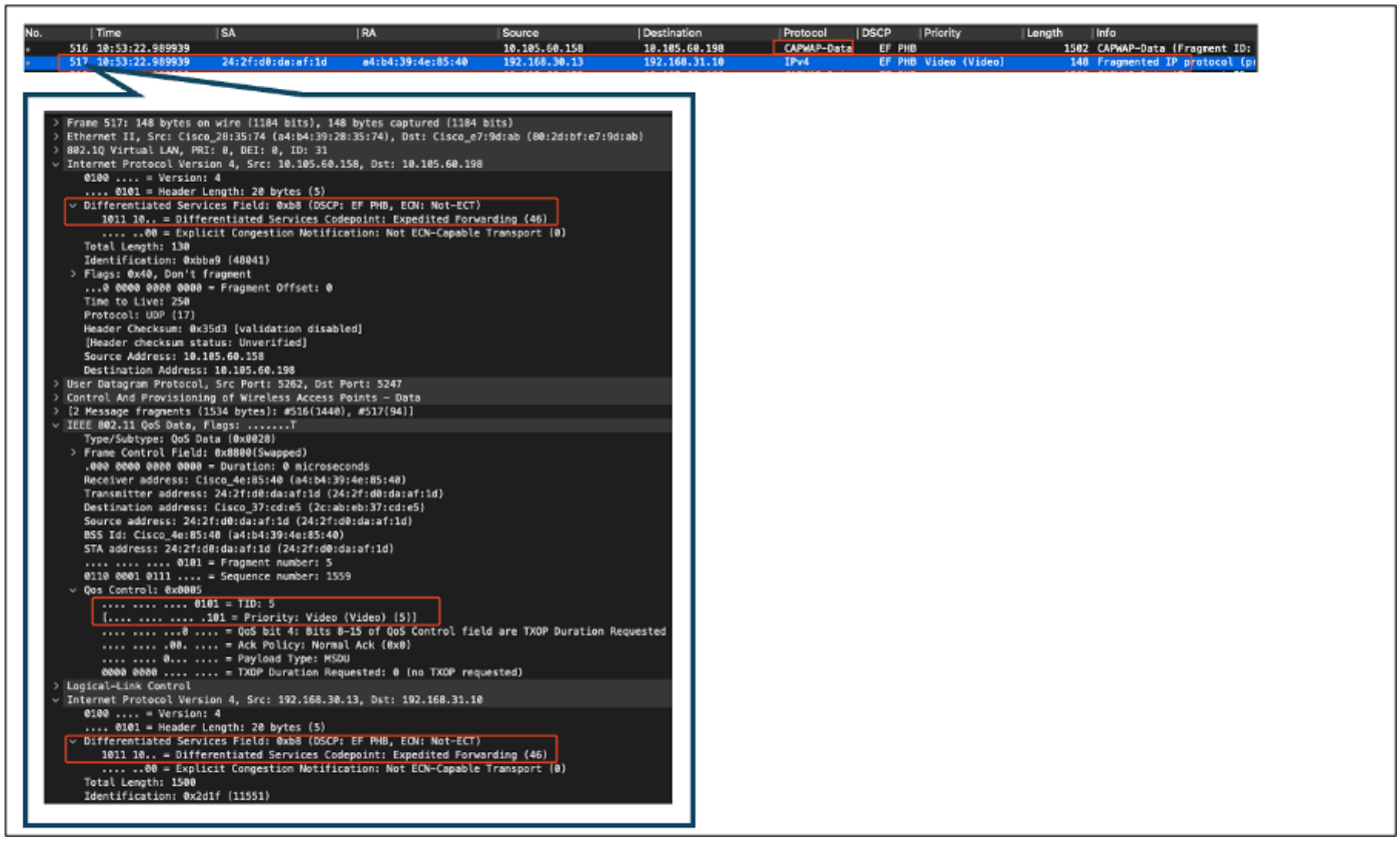
- O valor de DSCP na camada CAPWAP externa é mantido em 46.
- Dentro do túnel CAPWAP, o valor de DSCP também é mantido em 46.



Captura de Pplink AP na direção upstream

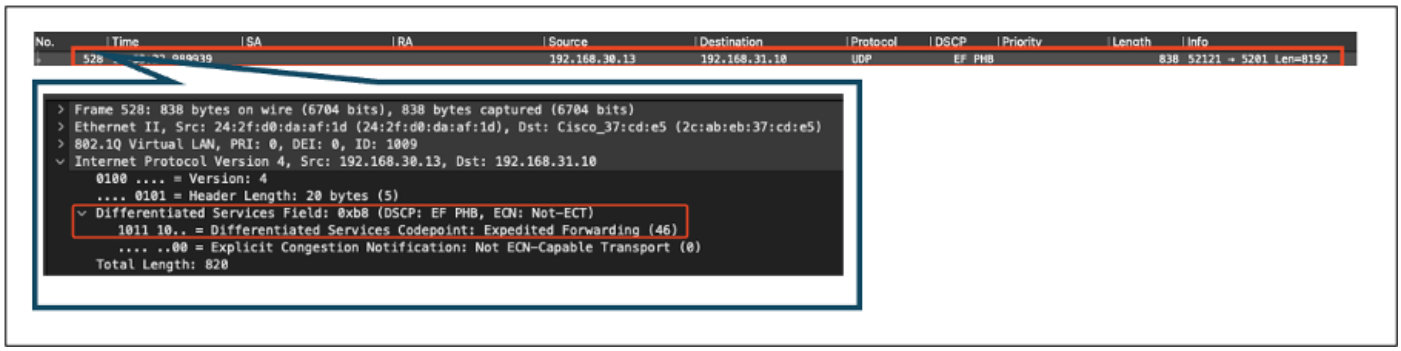
A captura é feita na WLC quando o pacote chega do switch.

- O pacote chega à WLC com o valor de DSCP de 46 na camada CAPWAP externa.
- Dentro do túnel CAPWAP, o valor de DSCP é mantido em 46.



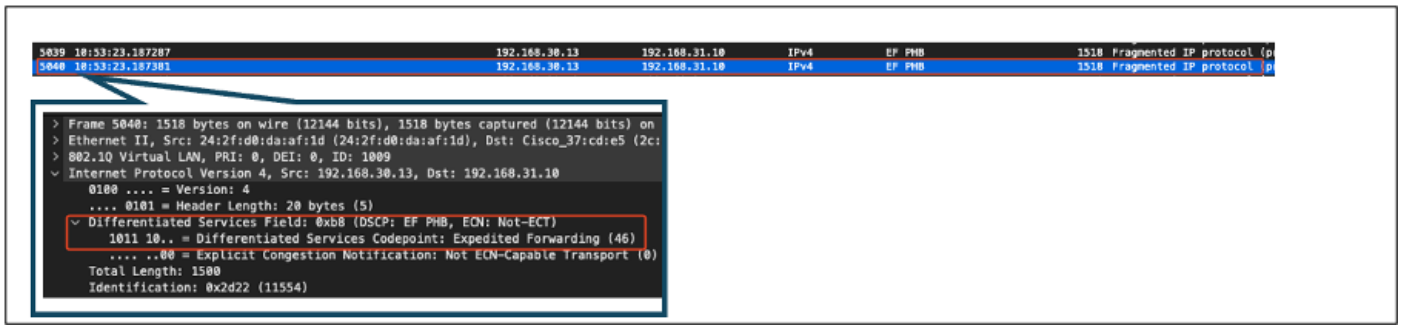
WLC EPC Mostrando Pacotes Vindo do AP

Depois que o pacote assume um giro de hairpin na WLC, ele é enviado de volta ao switch de uplink, destinado ao PC com fio. A WLC encaminha o pacote com o valor de DSCP de 46.



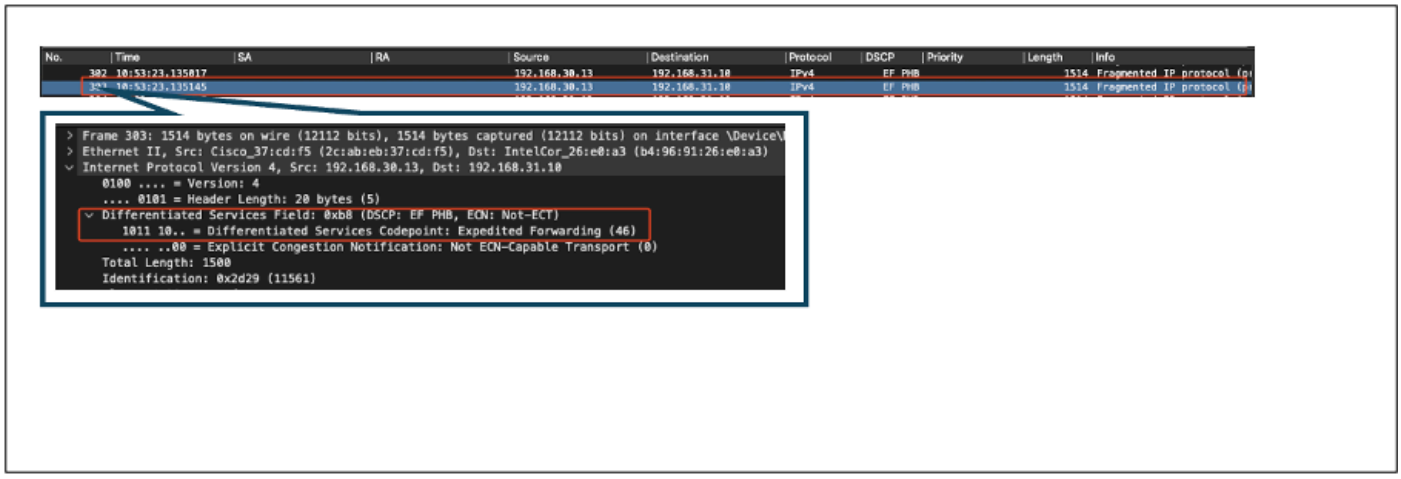
WLC EPC Mostrando os Pacotes Enviados ao PC com Fio

Finalmente, a captura de pacotes no uplink do PC com fio é analisada para garantir que o valor de DSCP seja preservado à medida que o pacote chega da WLC.



Captura do switch de uplink do PC com fio na direção upstream

No estágio final, o pacote recebido pelo PC com fio é analisado para garantir que o pacote chegue ao PC com fio com o valor de DSCP de 46.



Captura de PC com fio - Direção de upstream

O teste de QoS de upstream validou com êxito a configuração de QoS para o tráfego que flui do PC sem fio para o PC com fio. A preservação consistente do valor de DSCP de 46 em todo o caminho de transmissão confirma que as políticas de QoS são corretamente aplicadas e aplicadas.

Troubleshooting

Aplicativos de voz, vídeo e outros aplicativos em tempo real são particularmente sensíveis a problemas de desempenho de rede, e qualquer degradação na Qualidade de Serviço (QoS) pode ter efeitos nocivos e perceptíveis. Quando os pacotes de QoS são remarcados com valores de DSCP mais baixos, o impacto na voz e no vídeo pode ser significativo.

Impacto na voz:

- Maior latência: a comunicação de voz requer baixa latência para garantir que as conversas sejam naturais e fluidas. Valores de DSCP mais baixos podem resultar no atraso de pacotes de voz, causando um atraso notável nas conversações.
- Instabilidade: a variação nos tempos de chegada de pacotes (instabilidade) pode interromper a entrega sem problemas de pacotes de voz. Isso pode levar a áudio cortado ou distorcido, dificultando a compreensão do alto-falante.
- Perda de Pacotes: Os pacotes de voz são altamente sensíveis à perda de pacotes. Até mesmo uma pequena quantidade de perda de pacotes pode resultar na falta de palavras ou sílabas, levando a uma qualidade ruim da chamada e a mal-entendidos.
- Eco e Distorção: O aumento da latência e do jitter pode causar distorção de eco e áudio, degradando ainda mais a qualidade da chamada de voz.

Impacto no vídeo:

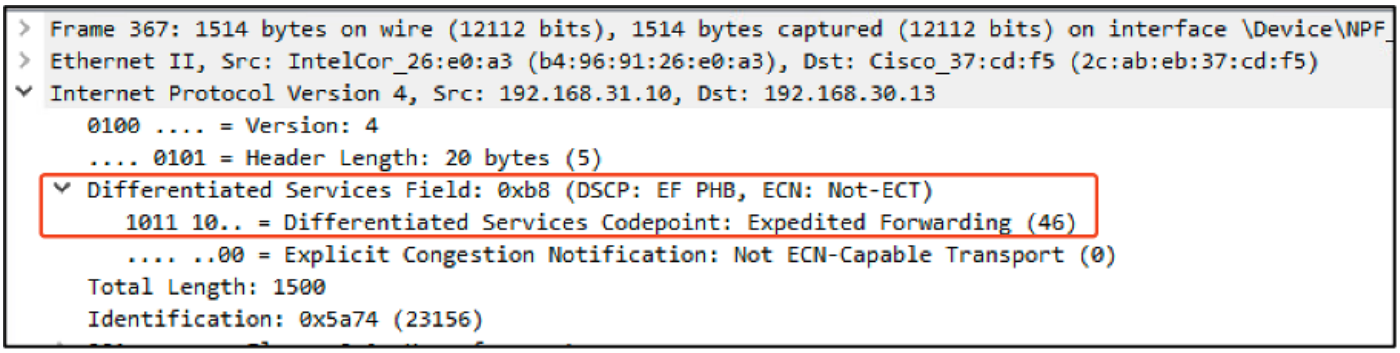
- Maior latência: a comunicação por vídeo requer baixa latência para manter a sincronização entre os fluxos de áudio e vídeo. O aumento da latência pode causar atrasos, dificultando interações em tempo real.

- Instabilidade: a instabilidade pode fazer com que os quadros de vídeo cheguem fora de ordem ou em intervalos irregulares, levando a uma experiência de vídeo instável ou irregular.
- Perda de Pacote: Pacotes perdidos podem resultar em quadros ausentes, o que pode fazer com que o vídeo congele ou exiba artefatos.
- Qualidade de vídeo reduzida: valores de DSCP mais baixos podem levar à alocação de largura de banda reduzida para fluxos de vídeo, resultando em resolução mais baixa e qualidade de vídeo pior. Isso pode dificultar a visualização de detalhes importantes no vídeo.

Cenário 1: Switch intermediário regrava a marcação de DSCP

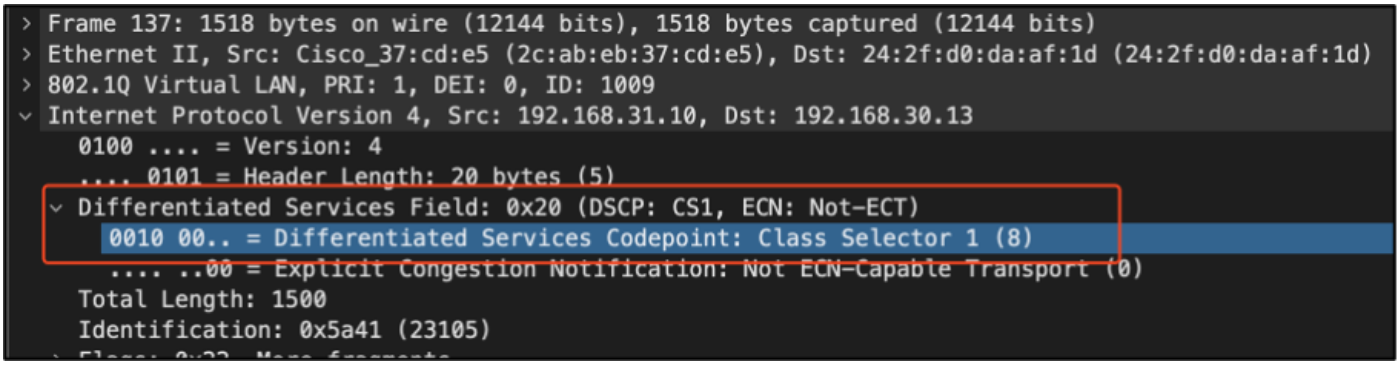
Neste cenário de Troubleshooting, o impacto de um switch intermediário regravando a marcação de DSCP no tráfego à medida que ele chega à WLC é investigado. Para replicar isso, o switch está configurado para regravar a marcação DSCP 46 em CS1 na interface de uplink do PC com fio.

O pacote é enviado do PC com fio com uma marca DSCP 46.



Pacote de Envio de PC com Fio com Marca DSCP 46

O pacote chega à WLC com um valor de DSCP de CS1 (DSCP 8). A alteração de DSCP 46 para DSCP 8 reduz significativamente a prioridade do pacote.

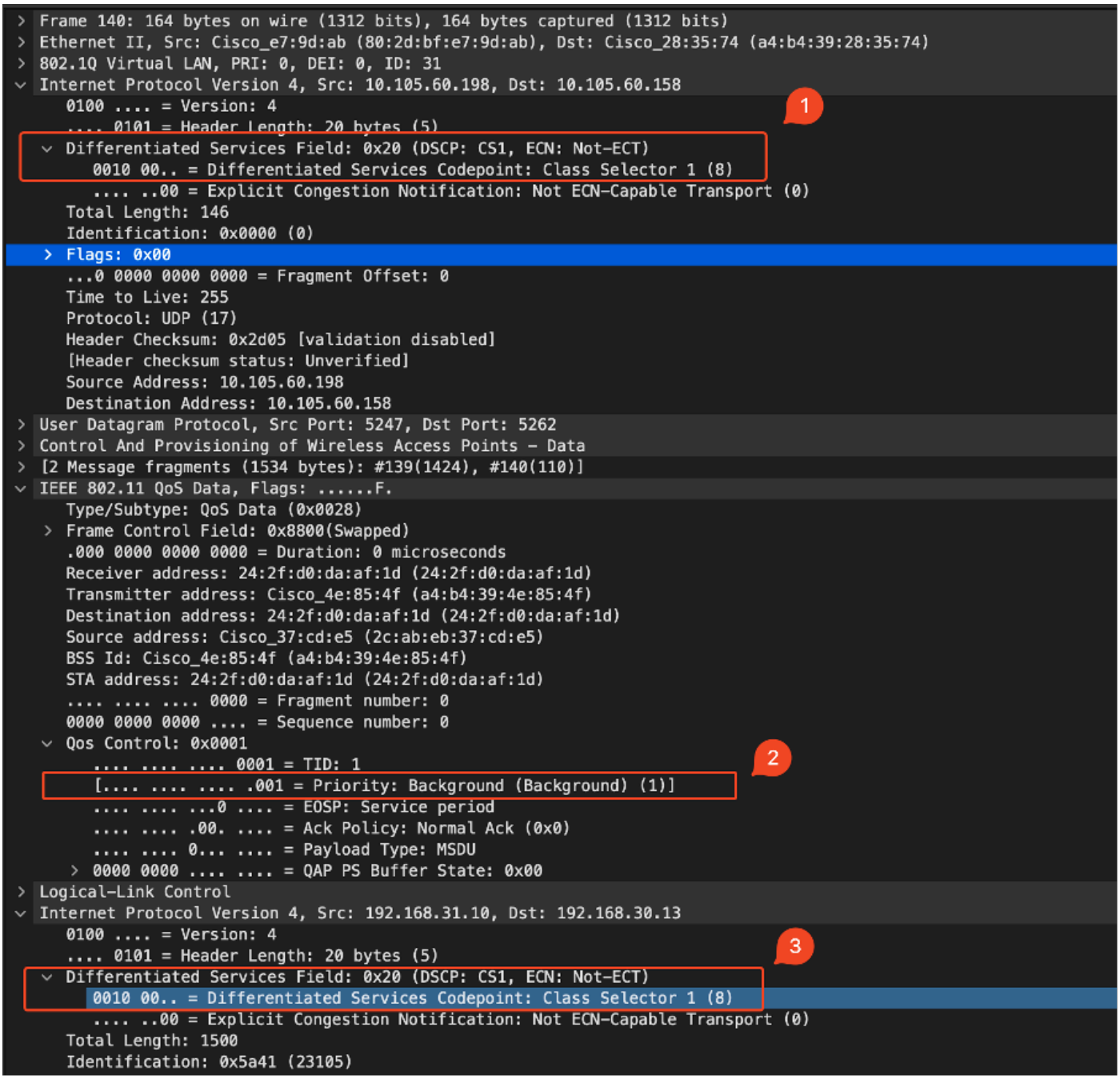


WLC EPC mostrando a marcação CS1

Nesta etapa, o pacote encaminhado pela WLC para o AP é analisado.

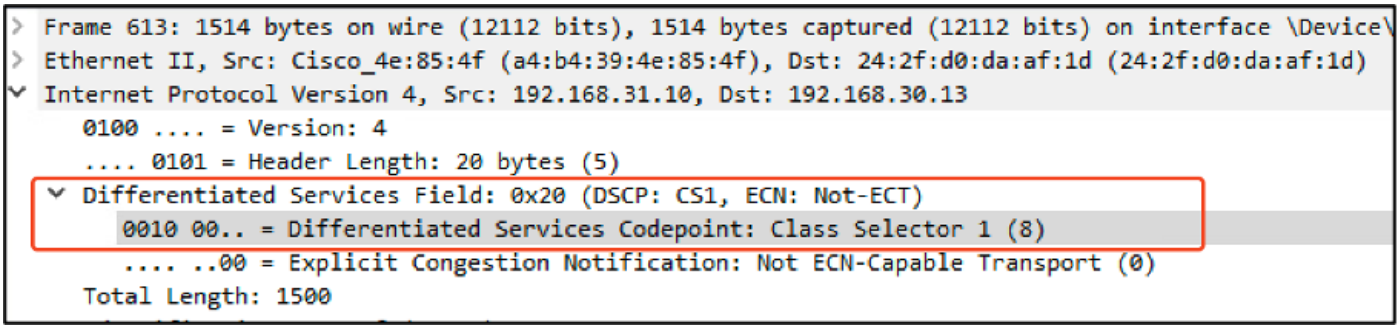
- O cabeçalho CAPWAP externo é marcado com CS1 (DSCP 8).
- O cabeçalho CAPWAP interno também é marcado com CS1 (DSCP 8).

- O valor de Prioridade do usuário (UP) é definido como BK (Segundo plano).



WLC EPC mostrando a marca CS1 no tráfego CAPWAP

O pacote chega ao PC sem fio com um valor de DSCP de CS1 (DSCP 8).



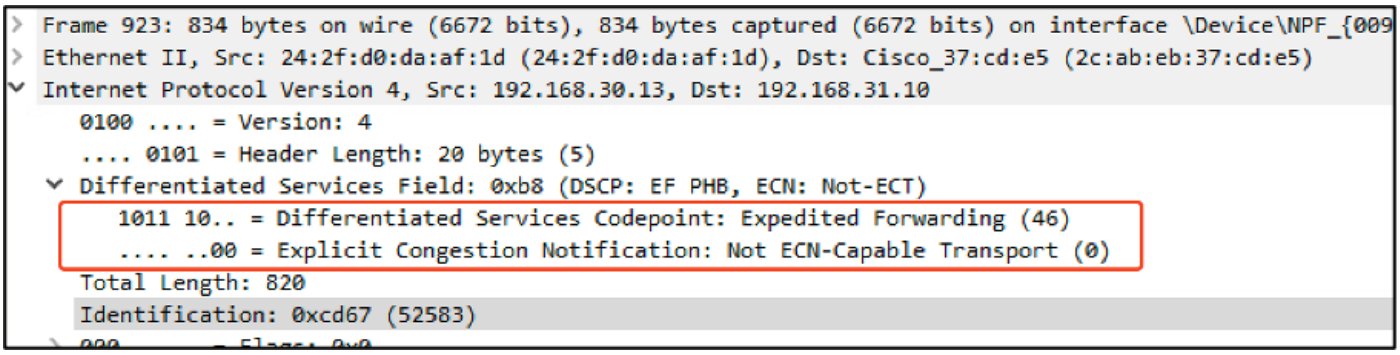
Captura de PC sem fio mostrando a marcação CS1

Este cenário demonstra como um erro de configuração em um switch intermediário pode quebrar a configuração de QoS, levando a desempenho degradado para tráfego de alta prioridade. Os pacotes de voz, inicialmente marcados para alta prioridade, foram tratados como tráfego de prioridade mais baixa devido à regravação de DSCP. Esse cenário enfatiza a importância de garantir que os dispositivos de rede intermediários preservem corretamente as marcações de QoS para manter a qualidade de serviço desejada para o tráfego de alta prioridade.

Cenário 2: Switch de link de AP regrava a marcação DSCP

Neste cenário, o impacto de um switch intermediário conectado ao AP reescrevendo a marcação DSCP no tráfego é investigado.

- O switch conectado ao AP é configurado para regravar a marcação DSCP 46 para um valor diferente CS1 na interface de uplink do AP.
- O pacote é enviado do PC com fio com uma marca DSCP de 46. Isso confirma que o tráfego está marcado corretamente com DSCP 46 na origem.

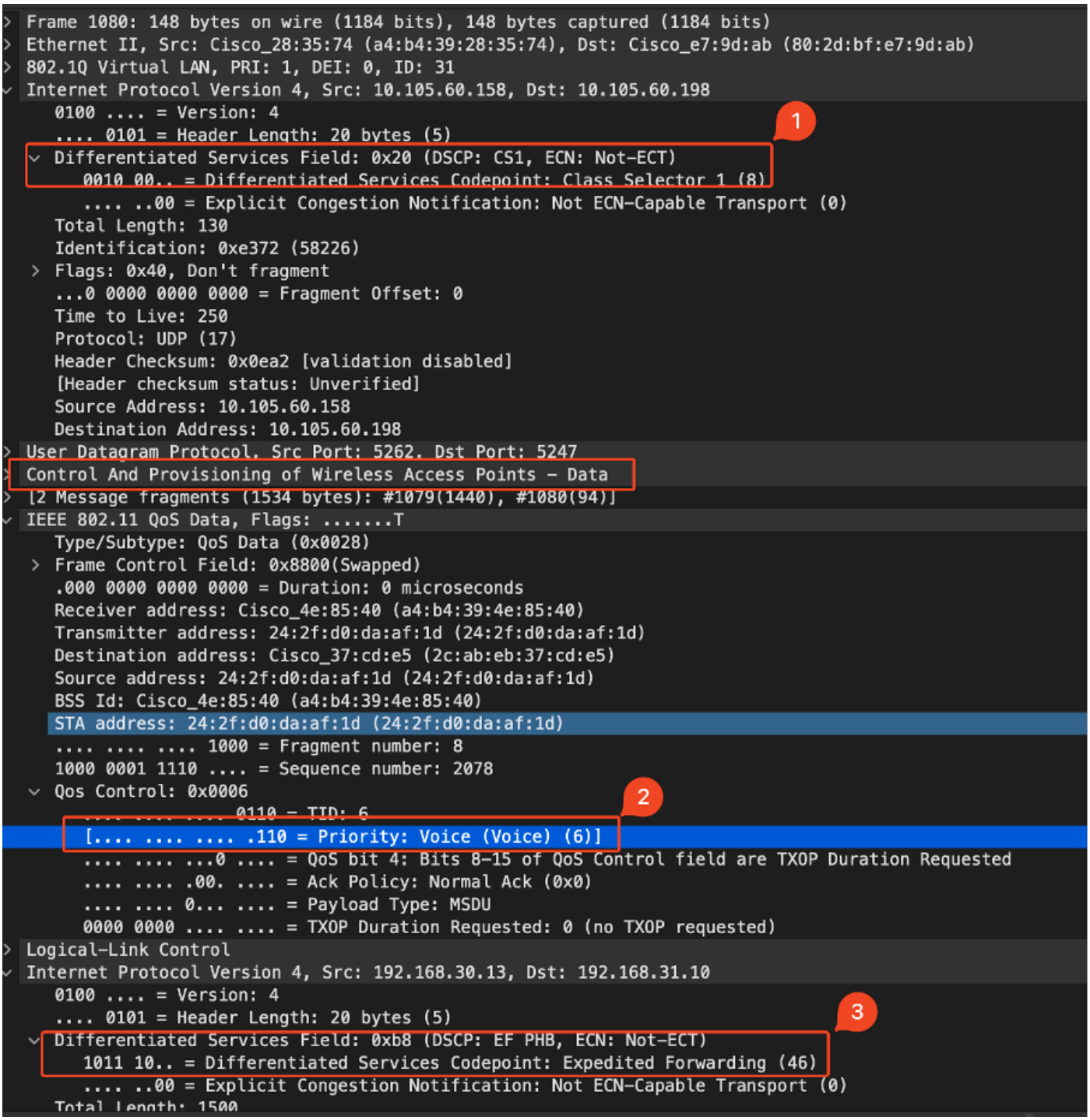


Captura de PC sem fio mostrando DSCP 46

A captura é feita na WLC quando o pacote chega do switch.

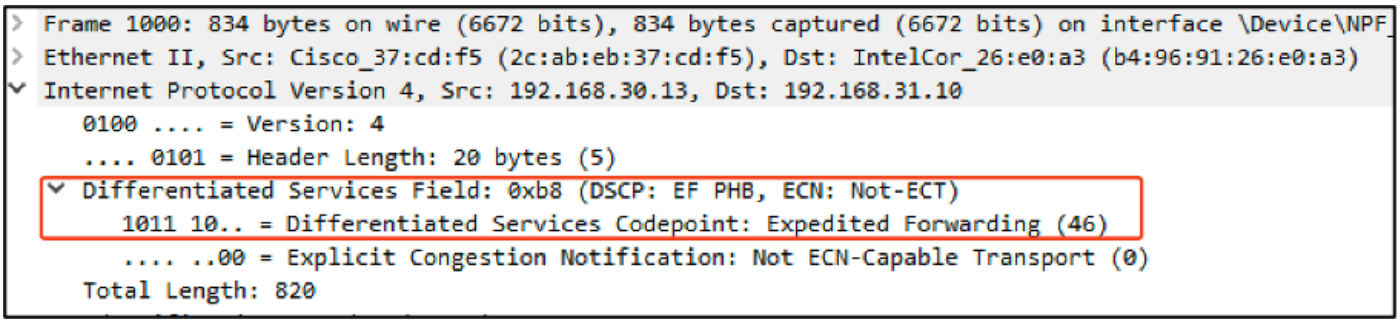
O pacote chega à WLC com o valor de DSCP do cabeçalho CAPWAP externo de CS1 (DSCP e o valor de DSCP interno de 46. Isso acontece porque o switch intermediário não pode ver o tráfego encapsulado dentro do túnel CAPWAP.

A WLC confia na marca DSCP dentro do túnel CAPWAP e encaminha o tráfego para o PC com fio com a marca DSCP interna de 46.



WLC EPC Mostrando Valores de CAPWAP DSCP

O pacote chega ao PC com fio com um valor de DSCP de 46. Confirma que o WLC encaminha corretamente o pacote com o valor de DSCP original de 46, preservando a marcação de alta prioridade.



O PC com fio recebeu o pacote com DSCP 46

Embora a WLC tenha encaminhado o tráfego com uma marca DSCP de 46, é importante entender que o tráfego do AP para a WLC foi tratado como de baixa prioridade devido à marca DSCP externa ser regravada em CS1 (DSCP 8).

Pode haver vários switches entre o AP e a WLC e, se o tráfego receber baixa prioridade, poderá chegar à WLC com atraso. Isso pode levar a um aumento de latência, instabilidade e perda potencial de pacotes, o que pode degradar a qualidade do serviço para tráfego de alta prioridade, como voz.

Dica de solução de problemas

1. Verifique a Marcação de DSCP Inicial: Capture pacotes na origem (por exemplo, PC com fio) para garantir que o tráfego seja marcado corretamente com o valor de DSCP pretendido.
2. Verificar Configurações de Dispositivos Intermediários: Revise a configuração de todos os switches e roteadores intermediários para garantir que eles não estejam inadvertidamente regravando valores de DSCP.
3. Capturar o tráfego nos pontos principais:
    1. Antes e depois do switch intermediário.
    2. Na WLC.
    3. No destino (por exemplo, PC sem fio).
4. Simular cenários de tráfego: use geradores de tráfego ou ferramentas de simulação de rede para criar tipos diferentes de tráfego e observe como a QoS é tratada pela rede sem fio.
5. Consulte o documento de práticas recomendadas do 9800: revise a documentação de práticas recomendadas do 9800 sobre como configurar as marcações de QoS e DSCP.

Verificação de configuração

<#root>

```
On the WLC, these commands can be used to verify the configuration.
# show run qos
# show policy-map <policy-map name>
# show class-map <policy-map name>
# show wireless profile policy detailed <policy-profile-name>

# show policy-map interface wireless ssid/client profile-name <name> radio type 2GHz|5GHz|6GHz ap name <
```

```
# show policy-map interface wireless client mac <MAC> input|output
# show wireless client mac <MAC> service-policy input|output

On AP, these commands can be used to check the QoS.
# show dot11 qos
# show controllers dot11Radio 1 | begin EDCA
```

Conclusão

Manter a configuração de QoS consistente em toda a rede é crucial para garantir que o tráfego de alta prioridade, como voz e vídeo, receba o nível apropriado de serviço e desempenho. É essencial validar as configurações de QoS regularmente para garantir que todos os dispositivos de rede estejam em conformidade com as políticas de QoS desejadas. Essa validação ajuda a identificar e corrigir qualquer configuração incorreta ou desvio que possa comprometer o desempenho da rede.

Referências

- Compreendendo e Troubleshooting de Cisco Catalyst 9800 Series Wireless Controllers
- Práticas recomendadas de configuração do Cisco Catalyst 9800 Series
- Guia de Configuração de Software do Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS® XE Dublin 17.12.x
- Guia de solução de problemas de VoWLAN (Voice Over Wireless LAN)
- Ativar marcação QoS DSCP em máquinas Windows

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.