

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

Contents

[Introdução](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configuração](#)

[Destinos da política de QoS](#)

[QoS automático](#)

[Configuração automática de QoS CLI](#)

[CLI QoS modular](#)

[configuração MQS CLI](#)

[QoS de metal](#)

[Configuração da CLI de QoS do Metal](#)

[Validar QoS de ponta a ponta com captura de pacotes](#)

[Diagrama de Rede](#)

[Componentes de laboratório e pontos de captura de pacotes](#)

[Cenário de teste 1: validação de QoS downstream](#)

[Cenário de teste 2: Validação de QoS upstream](#)

[Troubleshooting](#)

[Cenário 1: Switch intermediário regrava a marcação de DSCP](#)

[Cenário 2: Switch de link de AP regrava a marcação DSCP](#)

[Dica de solução de problemas](#)

[Verificação de configuração](#)

[Conclusão](#)

[Referências](#)

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

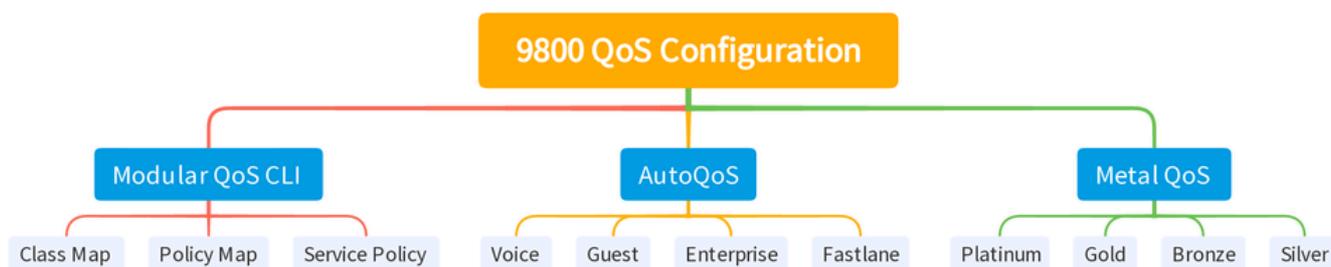
A QoS sem fio é essencial para garantir que os aplicativos críticos recebam a largura de banda necessária e a baixa latência necessária para o desempenho ideal. Este documento fornece um guia abrangente para configurar, validar e solucionar problemas de QoS em redes sem fio Cisco.

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

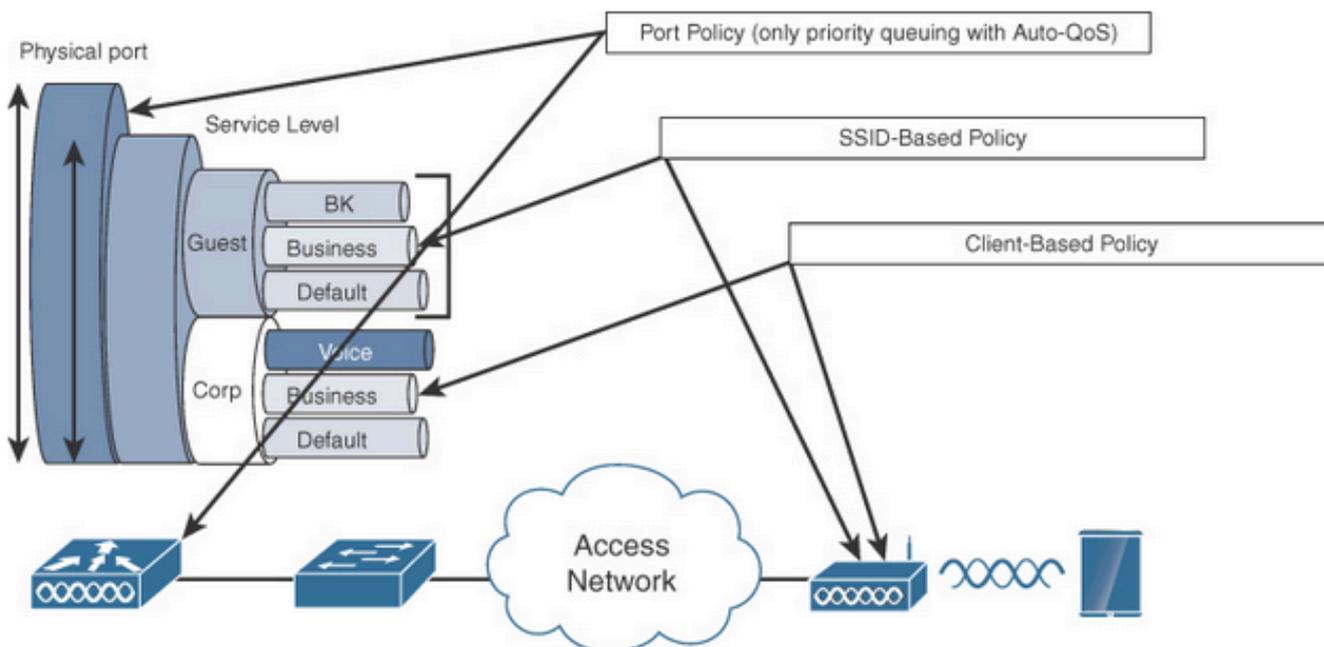
Este documento passa por cada seção, uma a uma, nas seções subsequentes.



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

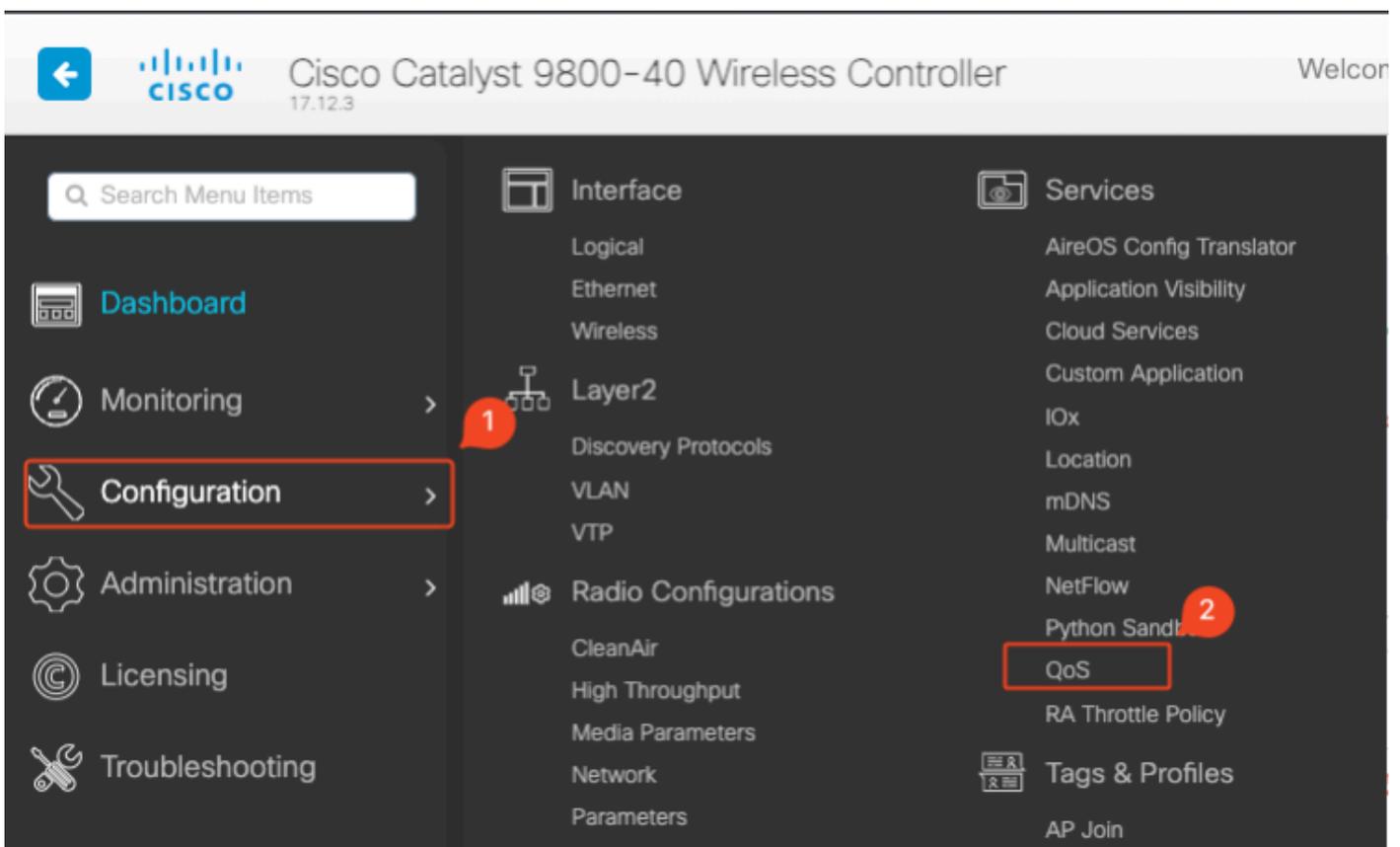
A QoS automática sem fio automatiza a implantação de recursos de QoS sem fio. Ele tem um conjunto de perfis predefinidos que podem ser modificados pelo administrador para priorizar fluxos de tráfego diferentes. A QoS automática corresponde ao tráfego e atribui cada pacote correspondente a grupos de QoS. 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	

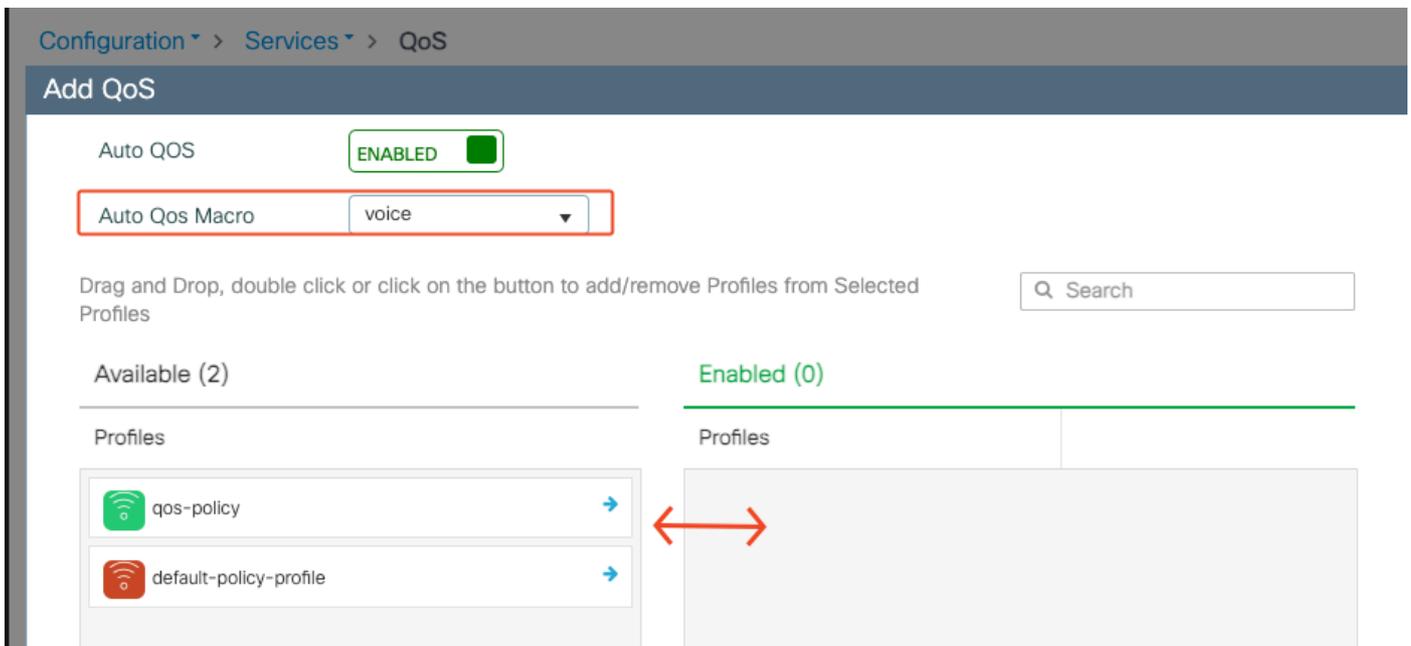
Esta tabela descreve as alterações de configuração que acontecem quando um perfil de QoS automático é aplicado.

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
```

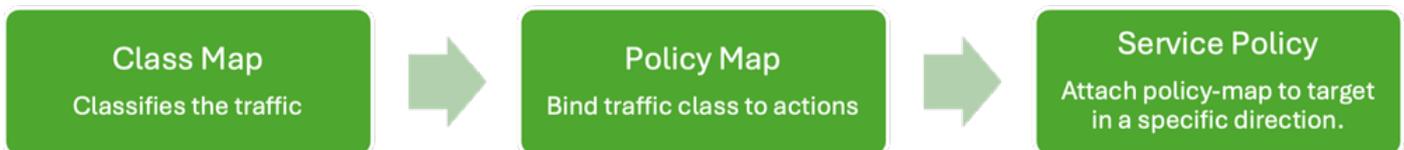
Agora que a QoS automática está ativada, você pode ver as alterações que aconteceram. Esta seção lista as alterações de configuração para voz.

```
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
```

```
auto qos 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.

Configuration > Security > ACL

+ Add - Delete Associate Interfaces

ACL Name	ACL Type	ACE Count	Download
<input type="checkbox"/> PCAP	IPv4 Extended	6	No

Add ACL Setup ✕

ACL Name* ACL Type

Rules

Sequence* Action

Source Type

Destination Type

Protocol

Log DSCP

+ Add - Delete

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/> 1	permit	192.168.31.10		any		ip	None	None	None	Disabled
<input type="checkbox"/> 2	permit	any		192.168.31.10		ip	None	None	None	Disabled

1 - 2 of 2 items

Cancel Apply to Device

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 política 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.

Add QoS

Auto QoS DISABLED

Policy Name*

Description

Match Type	Match Value	Mark Type	Mark Value	Police Value (kbps)	Drop	AVC/User Defined	Actions
No items to display							

+ Add Class-Maps

× Delete

AVC/User Defined

Match Any All

Match Type

Match Value*

Mark Type

Drop

Police(kbps)

Edit QoS

Mark: None

Police(kbps): 20

Drag and Drop, double click or click on the button to add/remove Profiles from Selected Profiles

Search

Available (1)

Profiles

default-policy-profile

Selected (1) (S = SSID, C = Client)

Profiles	Ingress	Egress
qos-policy	<input checked="" type="checkbox"/> S <input type="checkbox"/> C	<input checked="" type="checkbox"/> S <input type="checkbox"/> C

Cancel Update & Apply to Device

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.

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General Access Policies **QoS and AVC** Mobility Advanced

Auto QoS None

QoS SSID Policy

Egress platinum

Ingress platinum-up

QoS Client Policy

Egress Search or Select

Ingress Search or Select

SIP-CAC

Call Snooping

Send Disassociate

Send 486 Busy

Flow Monitor IPv4

Egress Search or Select

Ingress Search or Select

Flow Monitor IPv6

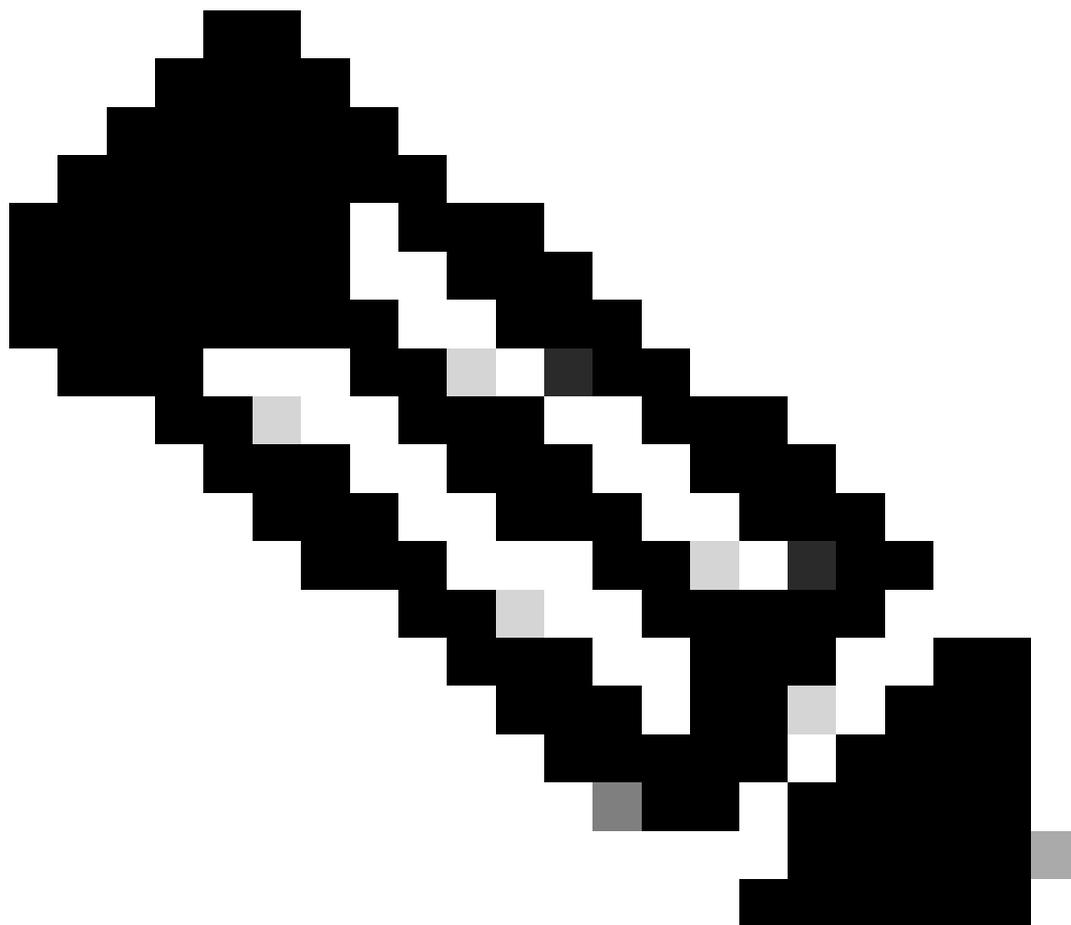
Egress Search or Select

Ingress Search or Select

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

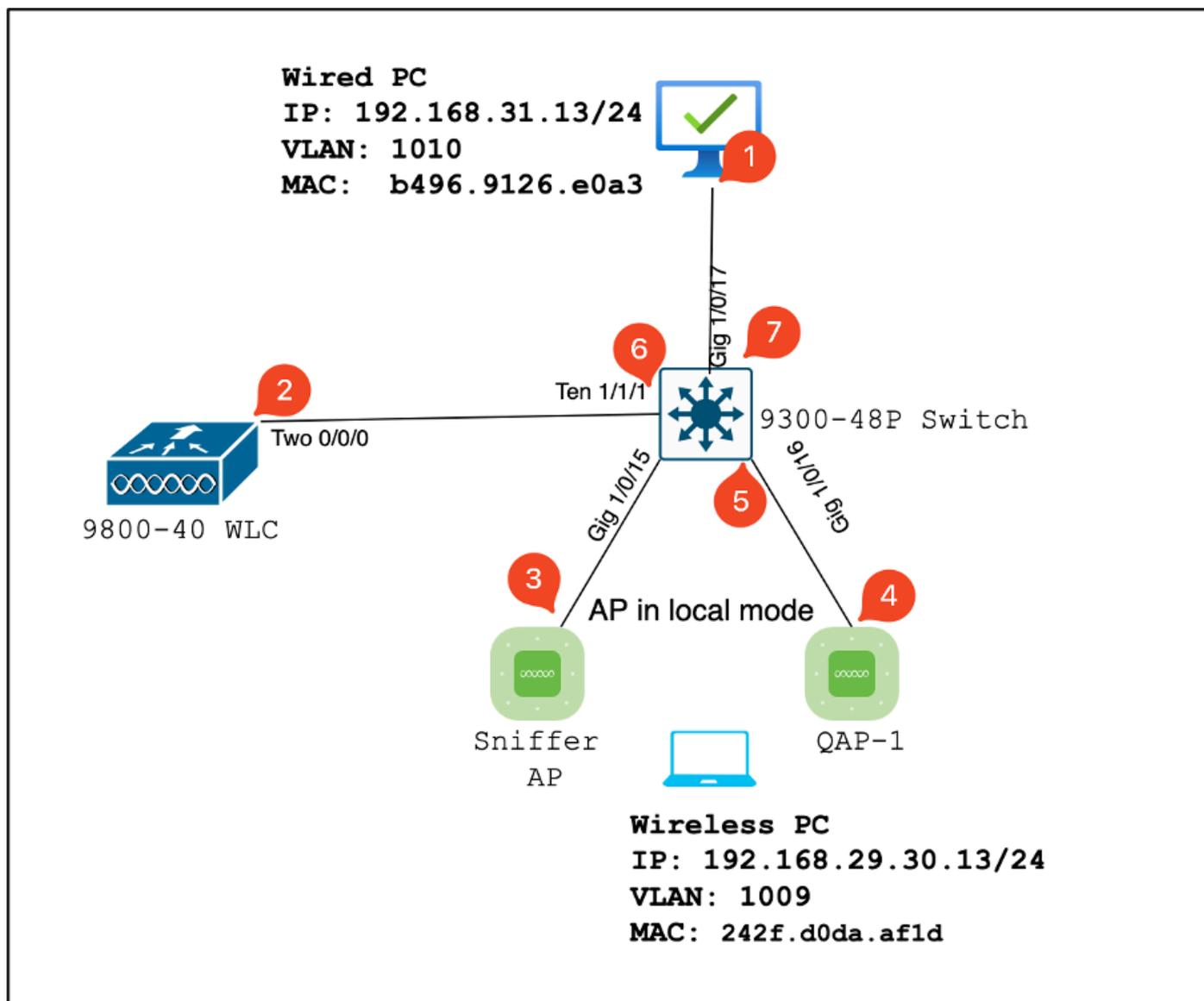
Agora que a configuração de QoS está concluída, é essencial examinar os pacotes de QoS e validar se as políticas de QoS estão funcionando corretamente de ponta a ponta. Isso pode ser obtido por meio da captura e análise de pacotes.

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.

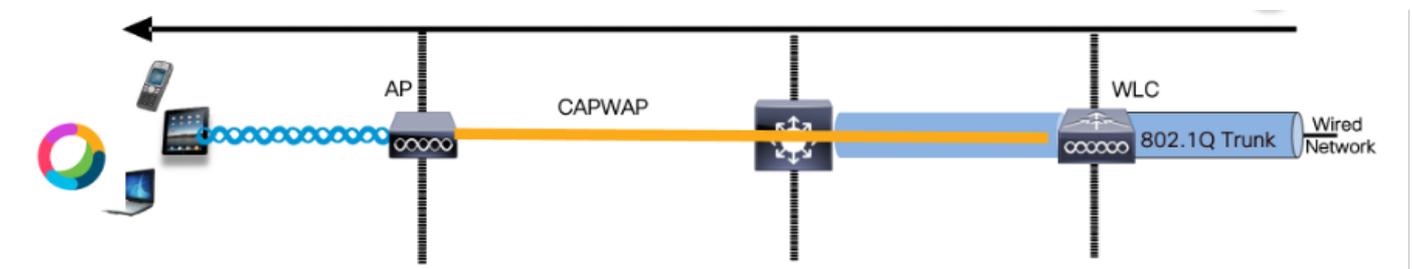
PC sem fio:

- 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

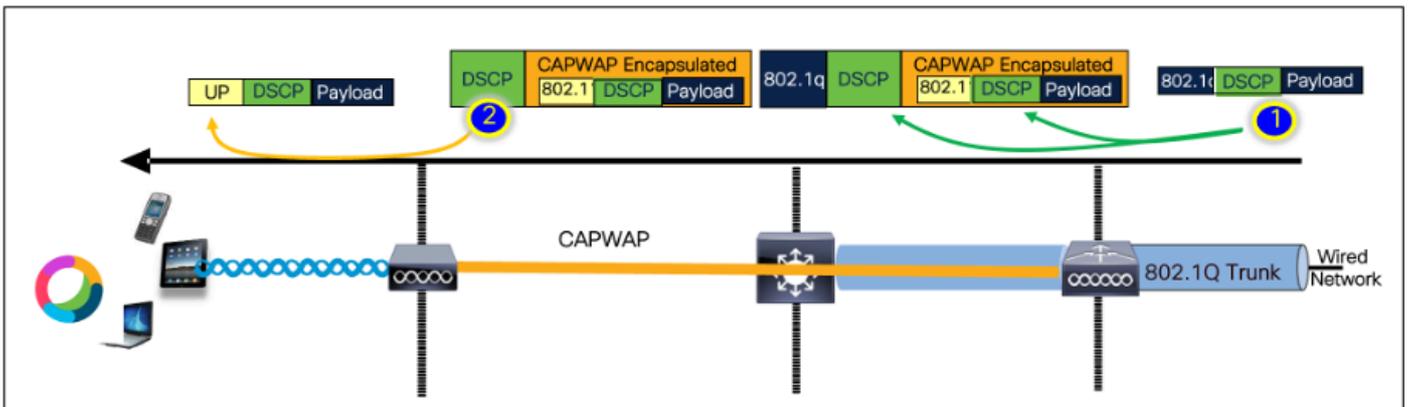
Destino: PC sem fio

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

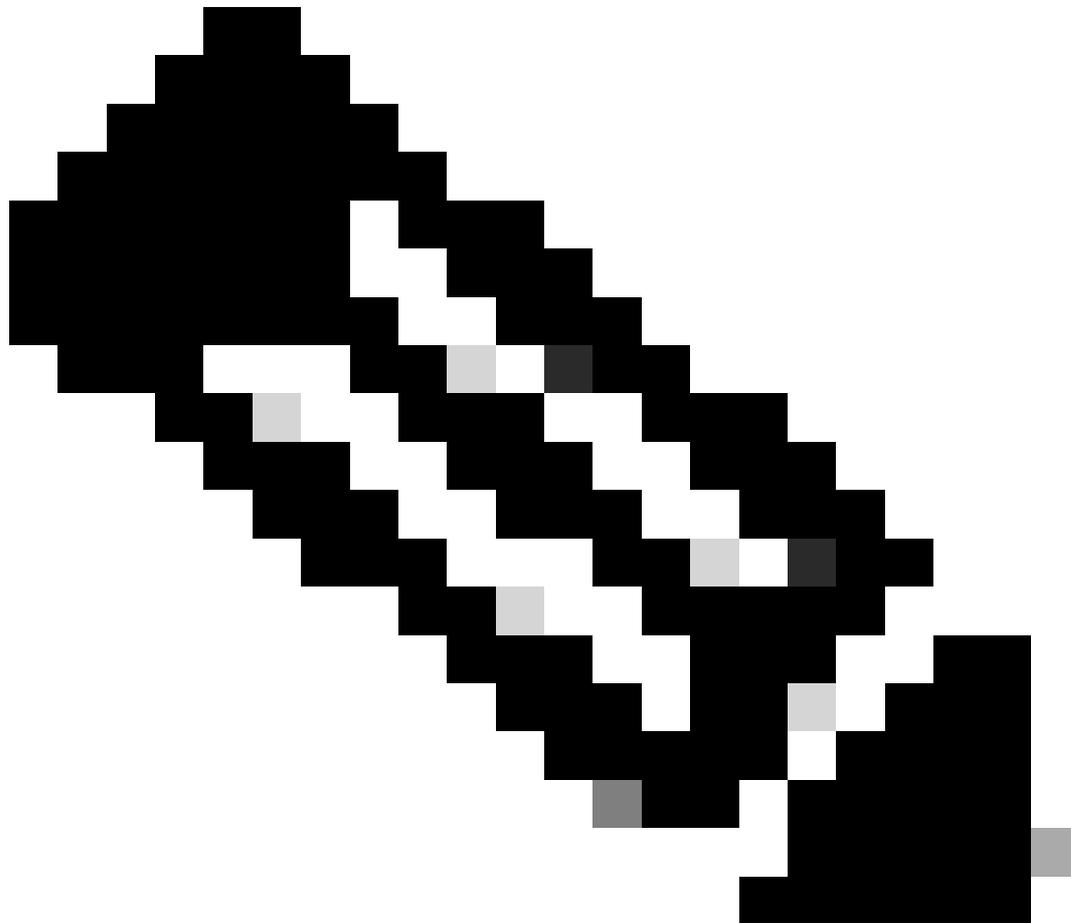
Captura de pacotes realizada no PC com fio. Isso confirma que o PC com fio está enviando pacotes UDP para o IP de destino especificado 192.168.10.13 com a marcação de DSCP correta de 46.

```
1004 08:19:24.592359 192.168.31.10 192.168.30.13 IPv4 EF PHB 1514 Fragmented IP protocol  
1005 08:19:24.592359 192.168.31.10 192.168.30.13 IPv4 EF PHB 1514 Fragmented IP protocol  
1006 08:19:24.592359 192.168.31.10 192.168.30.13 UDP EF PHB 834 49383 - 5201 Len=8192  
1007 08:19:24.685918 192.168.31.10 192.168.30.13 IPv4 EF PHB 1514 Fragmented IP protocol  
1008 08:19:24.685918 192.168.31.10 192.168.30.13 IPv4 EF PHB 1514 Fragmented IP protocol
```

```
> Frame 1006: 834 bytes on wire (6672 bits), 834 bytes captured (6672 bits) on interface \Device\NPF_{4083C30A-3F9F-4637-BE33-2AC26735E0CA}, id 0  
> Ethernet II, Src: IntelCor_26:e8:a3 (04:06:91:26:e8:a3), Dst: Cisco_37:cd:f5 (2c:1a:eb:b3:7d:f5)  
> Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13  
  8100 ... = Version: 4  
  ... 8185 = Header Length: 20 bytes (5)  
  > Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)  
    ... 1011 10... = Differentiated Services Codpoint: Expedited Forwarding (46)  
    ... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)  
  Total Length: 820  
  Identification: 0xc79c (51100)
```

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.



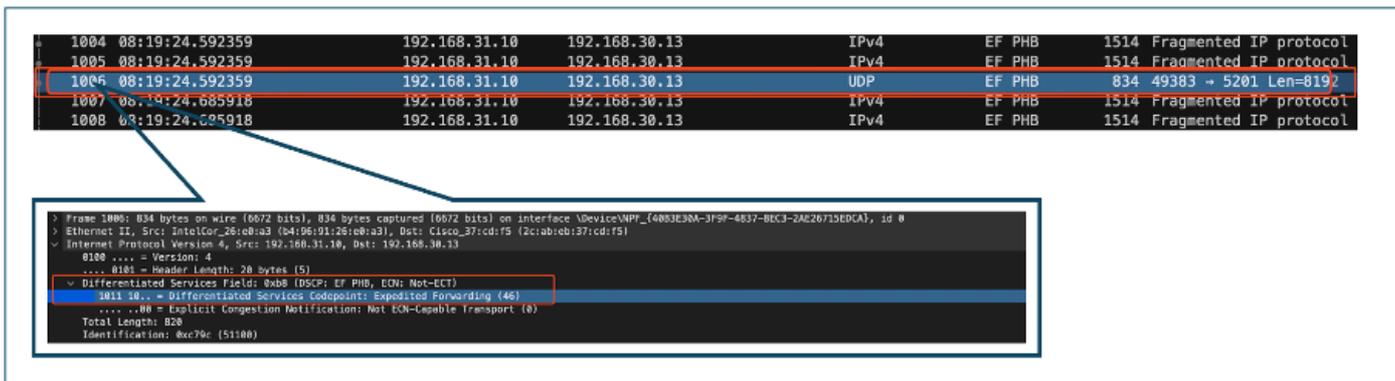
Observação: as portas do switch na série Catalyst 9000 assumem como padrão um estado confiável.

```
1004 08:19:24.592359      192.168.31.10      192.168.30.13      IPv4      EF PHB      1514 Fragmented IP protocol
1005 08:19:24.592359      192.168.31.10      192.168.30.13      IPv4      EF PHB      1514 Fragmented IP protocol
1006 08:19:24.592359      192.168.31.10      192.168.30.13      UDP       EF PHB      834 49383 -> 5201 Len=8192
1007 08:19:24.685918      192.168.31.10      192.168.30.13      IPv4      EF PHB      1514 Fragmented IP protocol
1008 08:19:24.685918      192.168.31.10      192.168.30.13      IPv4      EF PHB      1514 Fragmented IP protocol
```

```
> Frame 1006: 834 bytes on wire (6672 bits), 834 bytes captured (6672 bits) on interface VDeviceVNI_4003E30A-3F9F-4637-BE33-2AC26735E0CA, id 0
> Ethernet II, Src: IntelCor_26:e8:a3 (04:06:91:26:e8:a3), Dst: Cisco_37:cd:f5 (2c:1a:1e:b3:7cd:f5)
> Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13
  8100 ... = Version: 4
  ... 818 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codpoint: Expedited Forwarding (46)
    ... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 820
  Identification: 0xc79c (51100)
```

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.

2735	08:19:24:716958	2c:ab:..	24:2f:..	192.168.31.10	192.168.30.13	IPv4	EF PHB	164	Fragmented IP protocol
2736	08:19:24:716958	2c:ab:..	24:2f:..	192.168.31.10	192.168.30.13	IPv4	EF PHB	988	Fragmented IP protocol
2737	08:19:24:716958	2c:ab:..	24:2f:..	10.105.60.198	10.105.60.158	CAPWAP-Data	EF PHB	1478	CAPWAP-Data (Fragment
2738	08:19:24:716958	2c:ab:..	24:2f:..	192.168.31.10	192.168.30.13	IPv4	EF PHB	164	Fragmented IP protocol

```

> Frame 2736: 988 bytes on wire (7264 bits), 988 bytes captured (7264 bits)
> Ethernet II, Src: Cisco_e7:9d:ab (80:2d:b0:e7:9d:ab), Dst: Cisco_28:35:74 (a4:b4:39:28:35:74)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 31
> Internet Protocol Version 4, Src: 10.105.60.198, Dst: 10.105.60.158
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x08 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
    .... 0000 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 896
  Identification: 0x0000 (0)
  > Flags: 0x00
  ... 0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 255
  Protocol: UDP (17)
  Header Checksum: 0x2985 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.105.60.198
  Destination Address: 10.105.60.158
  > User Datagram Protocol, Src Port: 5247, Dst Port: 5262
  > Control And Provisioning of Wireless Access Points - Data
  > IEEE 802.11 QoS Data, Flags: .....F.
  Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x0000 (Swapped)
  ..000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: 24:2f:d0:daf:1d (24:2f:d0:daf:1d)
  Transmitter address: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
  Destination address: 24:2f:d0:daf:1d (24:2f:d0:daf:1d)
  Source address: Cisco_37:cd:e5 (2c:ab:eb:37:cd:e5)
  BSS Id: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
  STA address: 24:2f:d0:daf:1d (24:2f:d0:daf:1d)
  .... .... 0000 = Fragment number: 0
  0000 0000 0000 .... = Sequence number: 0
  > Qos Control: 0x0000
  .... .... 0110 = TID: 6
  .... .... 0000 0000 = Priority: Voice (Voice) (6)
  .... .... 0000 0000 = EOSP: Service period
  .... .... 0000 0000 = Ack Policy: Normal Ack (0x0)
  .... .... 0000 0000 = Payload Type: MSDU
  > 0000 0000 .... = QAP PS Buffer State: 0x00
  > Logical-Link Control
  > Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
    .... 0000 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 820
  
```

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.

13366	08:19:24:724746	2c:ab:..	24:2f:..	192.168.31.10	192.168.30.13	IPv4	EF PHB	164	Fragmented IP protocol (proto=UDP)
13376	08:19:24:724773	2c:ab:..	24:2f:..	192.168.31.10	192.168.30.13	IPv4	EF PHB	988	Fragmented IP protocol (proto=UDP)
13371	08:19:24:72475C	2c:ab:..	24:2f:..	10.105.60.198	10.105.60.158	CAPWAP-Data	EF PHB	1478	CAPWAP-Data (Fragment ID: 16242,

```

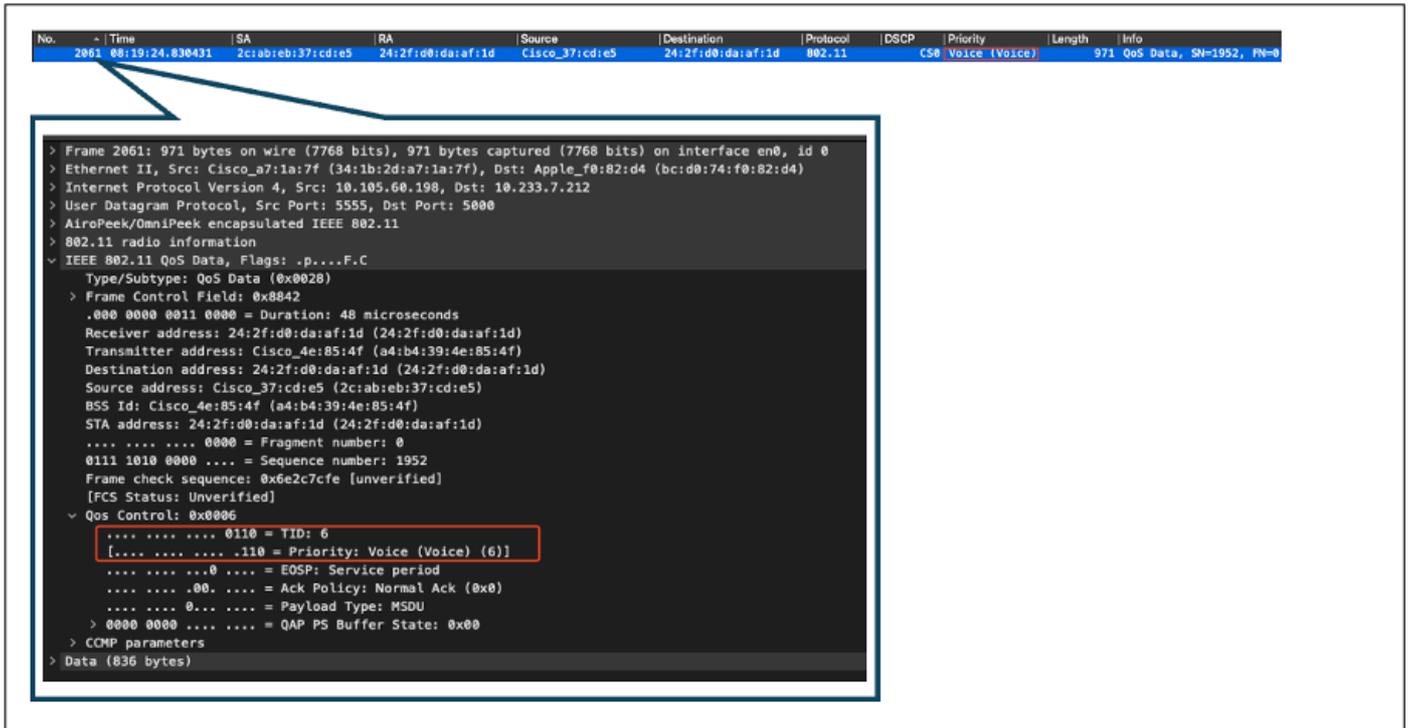
> Frame 13376: 988 bytes on wire (7264 bits), 988 bytes captured (7264 bits) on interface /tap/ap_wi_to_sw_upp, id 0
> Ethernet II, Src: Cisco_e7:9d:ab (80:2d:b0:e7:9d:ab), Dst: Cisco_28:35:74 (a4:b4:39:28:35:74)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 31
> Internet Protocol Version 4, Src: 10.105.60.198, Dst: 10.105.60.158
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x08 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
    .... 0000 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 896
  Identification: 0x0000 (0)
  > Flags: 0x00
  ... 0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 255
  Protocol: UDP (17)
  Header Checksum: 0x2985 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.105.60.198
  Destination Address: 10.105.60.158
  > User Datagram Protocol, Src Port: 5247, Dst Port: 5262
  > Control And Provisioning of Wireless Access Points - Data
  > Frame 13371
  > IEEE 802.11 QoS Data, Flags: .....F.
  Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x0000 (Swapped)
  ..000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: 24:2f:d0:daf:1d (24:2f:d0:daf:1d)
  Transmitter address: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
  Destination address: 24:2f:d0:daf:1d (24:2f:d0:daf:1d)
  Source address: Cisco_37:cd:e5 (2c:ab:eb:37:cd:e5)
  BSS Id: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
  STA address: 24:2f:d0:daf:1d (24:2f:d0:daf:1d)
  .... .... 0000 = Fragment number: 0
  0000 0000 0000 .... = Sequence number: 0
  > Qos Control: 0x0000
  .... .... 0110 = TID: 6
  .... .... 0000 0000 = Priority: Voice (Voice) (6)
  .... .... 0000 0000 = EOSP: Service period
  .... .... 0000 0000 = Ack Policy: Normal Ack (0x0)
  .... .... 0000 0000 = Payload Type: MSDU
  > 0000 0000 .... = QAP PS Buffer State: 0x00
  > Logical-Link Control
  > Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
    .... 0000 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 820
  
```

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.



```
No. | Time | SA | RA | Source | Destination | Protocol | DSCP | Priority | Length | Info
---|---|---|---|---|---|---|---|---|---|---
2061 | 08:19:24.830431 | 2c:ab:eb:37:cd:e5 | 24:2f:d0:da:af:1d | Cisco_37:cd:e5 | 24:2f:d0:da:af:1d | 802.11 | CS0 | Voice (Voice) | 971 | QoS Data, SN=1952, FN=0

> Frame 2061: 971 bytes on wire (7768 bits), 971 bytes captured (7768 bits) on interface en0, id 0
> Ethernet II, Src: Cisco_a7:1a:7f (34:1b:2d:a7:1a:7f), Dst: Apple_f0:82:d4 (bc:d0:74:f0:82:d4)
> Internet Protocol Version 4, Src: 10.105.60.198, Dst: 10.233.7.212
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AiroPeek/OmniPeek encapsulated IEEE 802.11
> 802.11 radio information
  > IEEE 802.11 QoS Data, Flags: .p...F.C
    Type/Subtype: QoS Data (0x0028)
    > Frame Control Field: 0x8842
      .000 0000 0011 0000 = Duration: 48 microseconds
      Receiver address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
      Transmitter address: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
      Destination address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
      Source address: Cisco_37:cd:e5 (2c:ab:eb:37:cd:e5)
      BSS Id: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
      STA address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
      .... 0000 = Fragment number: 0
      0111 1010 0000 .... = Sequence number: 1952
      Frame check sequence: 0x6e2c7cfe [unverified]
      [FCS Status: Unverified]
    > Qos Control: 0x0006
      .... 0110 = TID: 6
      [.... 0110 = Priority: Voice (Voice) (6)]
      .... 0000 = EOSP: Service period
      .... 0000 = Ack Policy: Normal Ack (0x0)
      .... 0000 = Payload Type: MSDU
      > 0000 0000 .... = QAP PS Buffer State: 0x00
    > CCMP parameters
  > Data (836 bytes)
```

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.

No.	Time	SA	RA	Source	Destination	Protocol	DSCP	Priority	Length	Info
2061	08:19:24.830431	2c:ab:eb:37:cd:e5	24:2f:d0:da:af:1d	Cisco_37:cd:e5	24:2f:d0:da:af:1d	802.11		CS0 Voice (Voice)	971	QoS Data, SN=1952, FN=8

```

> Frame 2061: 971 bytes on wire (7768 bits), 971 bytes captured (7768 bits) on interface en0, id 0
> Ethernet II, Src: Cisco_a7:1a:7f (34:1b:2d:a7:1a:7f), Dst: Apple_f0:82:d4 (bc:d0:74:f0:82:d4)
> Internet Protocol Version 4, Src: 10.105.60.198, Dst: 10.233.7.212
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AiroPeek/OmniPeek encapsulated IEEE 802.11
> 802.11 radio information
  IEEE 802.11 QoS Data, Flags: .p...F.C
    Type/Subtype: QoS Data (0x0028)
    Frame Control Field: 0x8842
    .000 0000 0011 0000 = Duration: 48 microseconds
    Receiver address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
    Transmitter address: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
    Destination address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
    Source address: Cisco_37:cd:e5 (2c:ab:eb:37:cd:e5)
    BSS Id: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
    STA address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
    .... .. 0000 = Fragment number: 0
    0111 1010 0000 .... = Sequence number: 1952
    Frame check sequence: 0x6e2c7cfe [unverified]
    [FCS Status: Unverified]
    QoS Control: 0x0006
      .... .. 0110 = TID: 6
      [.... .. .110 = Priority: Voice (Voice) (6)]
      .... .. 0000 = EOSP: Service period
      .... .. 00. .... = Ack Policy: Normal Ack (0x0)
      .... .. 0... .... = Payload Type: MSDU
      > 0000 0000 .... .... = QAP PS Buffer State: 0x00
    > CCM parameters
    > Data (836 bytes)
  
```

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:

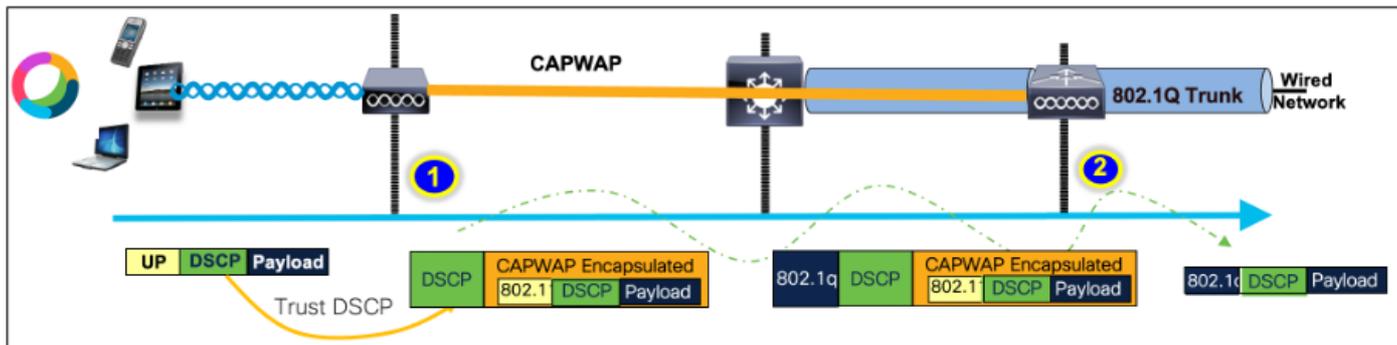
Perfil de QoS: QoS Platinum

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.

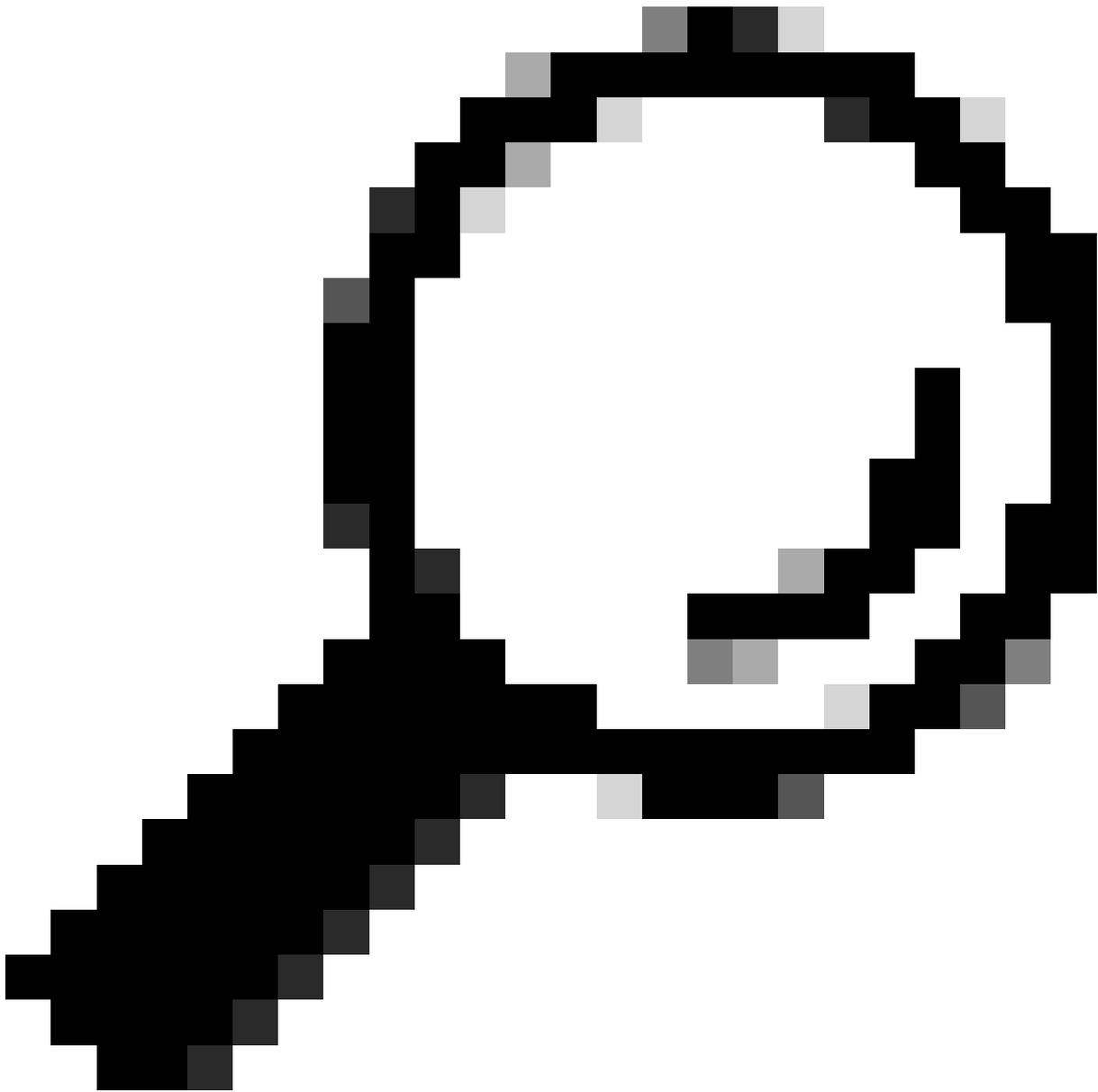
No.	Time	SA	RA	Source	Destination	Protocol	DSCP	Priority	Length	Info
241	10:53:22.943438			192.168.30.13	192.168.31.10	UDP	EF PHB		834	52121 - 5261 Len=6192

```

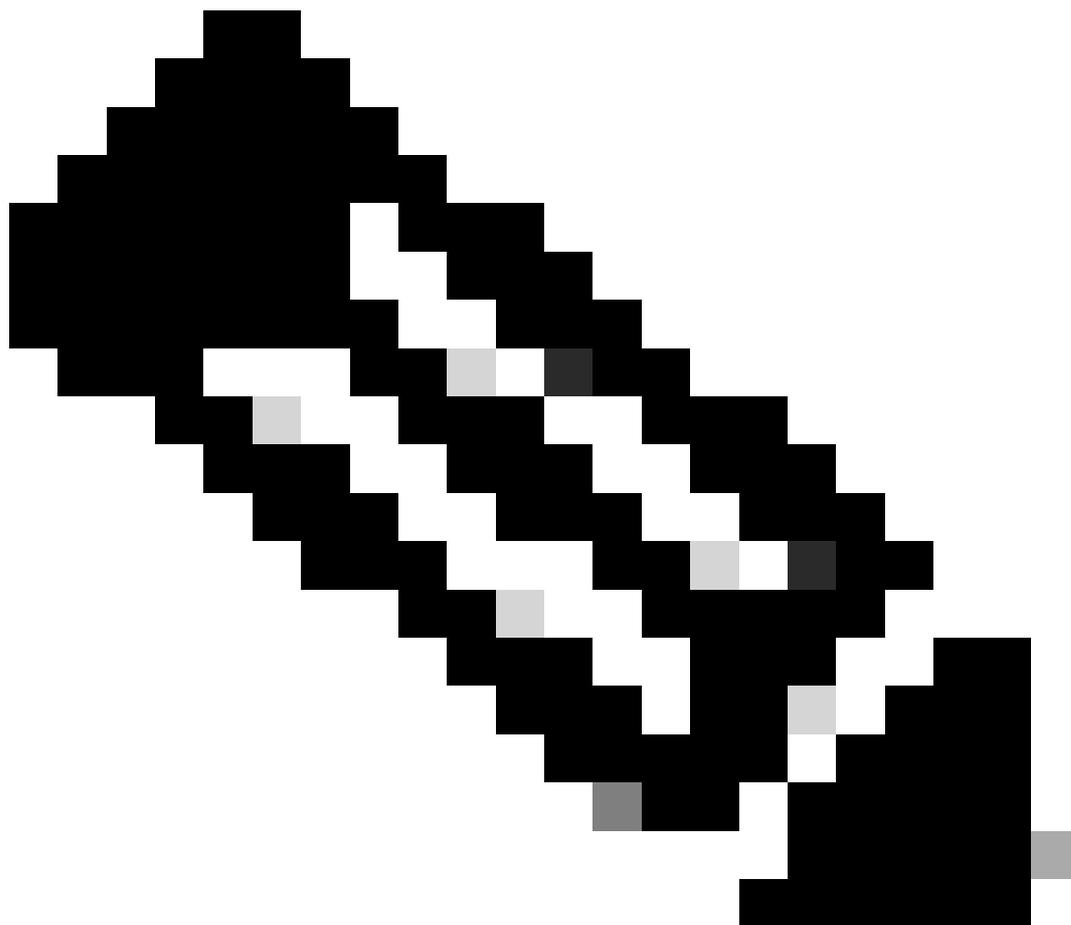
> Frame 241: 834 bytes on wire (6672 bits), 834 bytes captured (6672 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d), Dst: Cisco_37:cd:e5 (2c:ab:eb:37:cd:e5)
> Internet Protocol Version 4, Src: 192.168.30.13, Dst: 192.168.31.10
  0100 ... = Version: 4
  ... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 820
  Identification: 0x2d25 (11557)
  
```

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.

QoS Control Field: 0000000000000101

- AP PS Buffer State: 0
- 0..... A-MSDU: Not Present
-00..... Ack: Normal Acknowledge
-0.... EOSP: Not End of Triggered Service Period
-X... Reserved
-01 UP: 5 - Video

802.2 Logical Link Control (LLC) Header

- Dest. SAP: 0xAA SNAP
- Source SAP: 0xAA SNAP
- Command: 0x03 Unnumbered Information
- Vendor ID: 0x000000
- Protocol Type: 0x0800 IP

IP Header - Internet Protocol Datagram

- Version: 4
- Header Length: 5 (20 bytes)
- Differentiated Services: 10111000
- 10110.. Expedited Forwarding

In MS Windows, the WMM UP is derived from the 3 msb of the DSCP value
DSCP ef (46) = [101 110] → 101 = UP 5

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.

No.	Time	SA	RA	Source	Destination	Protocol	DSCP	Priority	Length	Info
5643	10.53122.982358	24:2f:d0:da:af:1d	a4:b4:39:4e:85:4f	24:2f:d0:da:af:1d	Cisco_37:cd:e5	802.11	C50	Video (Video)	1442	QoS Data, SN=1347

```

> Frame 5643: 1442 bytes on wire (11536 bits), 1442 bytes captured (11536 bits) on interface en0, id 0
> Ethernet II, Src: Cisco_a7:1a:7f (34:1b:2d:a7:1a:7f), Dst: Apple_f0:82:d4 (bc:d0:74:f0:82:d4)
> Internet Protocol Version 4, Src: 10.105.60.198, Dst: 10.233.7.212
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AiroPeek/OmniPeek encapsulated IEEE 802.11
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .p....TC
  Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8041
    .000 0000 0100 1001 = Duration: 73 microseconds
    Receiver address: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
    Transmitter address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
    Destination address: Cisco_37:cd:e5 (2c:ab:eb:37:cd:e5)
    Source address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
    BSS Id: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
    STA address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
    .... 0000 = Fragment number: 0
    0101 0100 0011 .... = Sequence number: 1347
    Frame check sequence: 0x03a2e423 [unverified]
    [FCS Status: Unverified]
  > QoS Control: 0x0005
    .... 0101 = TID: 5
    [.... 101 = Priority: Video (Video) (5)]
    .... 0000 = QoS bit 4: Bits 8-15 of QoS Control field are TXOP Duration Requested
    .... .00. .... = Ack Policy: Normal Ack (0x0)
    .... 0... .... = Payload Type: MSDU
    0000 0000 .... = TXOP Duration Requested: 0 (no TXOP requested)
  
```

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.

No.	Time	SA	RA	Source	Destination	Protocol	DSCP	Priority	Length	Info
4842	10:53:22.989344			10.105.60.158	10.105.60.198	CAPWAP-Data	EF PHB		1498	CAPWAP-Data (Fragment ID: 4843)
4843	10:53:22.989366	24:2f:d0:da:af:1d	a4:b4:39:4e:85:40	192.168.30.13	192.168.31.10	IPv4	EF PHB	Video (Video)	144	Fragmented IP protocol (p)


```

> Frame 4843: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface
> Ethernet II, Src: Cisco_28:35:74 (a4:b4:39:28:35:74), Dst: Cisco_e7:9d:ab (00:2d:0c:00:07:9d:ab)
> Internet Protocol Version 4, Src: 10.105.60.158, Dst: 10.105.60.198
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
  1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
  .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 130
  Identification: 0xb7a9 (47017)
  > Flags: 0x40, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 250
  Protocol: UDP (17)
  Header Checksum: 0x39d3 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.105.60.158
  Destination Address: 10.105.60.198
  > User Datagram Protocol, Src Port: 5262, Dst Port: 5247
  > Control And Provisioning of Wireless Access Points - Data
  > [2 Message fragments (1534 bytes): #4842(1440), #4843(94)]
  > IEEE 802.11 QoS Data, Flags: .....T
  Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0xb800(Swapped)
  .000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: Cisco_4e:85:40 (a4:b4:39:4e:85:40)
  Transmitter address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
  Destination address: Cisco_37:cd:e5 (2c:ab:eb:37:cd:e5)
  Source address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
  BSS Id: Cisco_4e:85:40 (a4:b4:39:4e:85:40)
  STA address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
  .... ..0101 = Fragment number: 5
  0100 0001 0111 .... = Sequence number: 1047
  > QoS Control: 0x0005
  [.... ..0101 = TID: 5]
  [.... ..0101 = Priority: Video (Video) (5)]
  .... ..0000 = QoS bit 4: Bits 8-15 of QoS Control field are TXOP Duration
  .... ..0000 = Ack Policy: Normal Ack (0x0)
  .... ..0000 = Payload Type: MSDU
  0000 0000 .... = TXOP Duration Requested: 0 (no TXOP requested)
  > Logical-Link Control
  > Internet Protocol Version 4, Src: 192.168.30.13, Dst: 192.168.31.10
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
  1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
  .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 1500
  Identification: 0x2d1f (11551)
  
```

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.

No.	Time	SA	RA	Source	Destination	Protocol	DSCP	Priority	Length	Info
516	10:53:22.989939	24:2f:d0:da:af:1d	a4:b4:39:4e:85:40	10.185.60.158	10.185.60.198	CAPWAP-Data	EF PHB		1582	CAPWAP-Data (Fragment ID: 517)
517	10:53:22.989939	24:2f:d0:da:af:1d	a4:b4:39:4e:85:40	192.168.30.13	192.168.31.10	IPv4	EF PHB	Video (Video)	148	Fragmented IP protocol (p

```

> Frame 517: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on 0
> Ethernet II, Src: Cisco_20:35:74 (a4:b4:39:28:35:74), Dst: Cisco_e7:9d:ab (00:2d:bf:e7:9d:ab)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 31
> Internet Protocol Version 4, Src: 10.185.60.158, Dst: 10.185.60.198
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
< Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
  1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
  .... 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 130
Identification: 0xbbe9 (48041)
> Flags: 0x0, Don't fragment
... 0000 0000 0000 = Fragment Offset: 0
Time to Live: 250
Protocol: UDP (17)
Header Checksum: 0x35d3 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.185.60.158
Destination Address: 10.185.60.198
> User Datagram Protocol, Src Port: 5262, Dst Port: 5247
> Control And Provisioning of Wireless Access Points - Data
> [2 Message fragments (1534 bytes): #516(1440), #517(94)]
< IEEE 802.11 QoS Data, Flags: .....T
Type/Subtype: QoS Data (0x0028)
> Frame Control Field: 0x0000(Swapped)
... 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Cisco_4e:85:40 (a4:b4:39:4e:85:40)
Transmitter address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
Destination address: Cisco_37:cd:e5 (2c:ab:eb:37:cd:e5)
Source address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
BSS Id: Cisco_4e:85:40 (a4:b4:39:4e:85:40)
STA address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
.... 0101 = Fragment number: 5
0110 0001 0111 .... = Sequence number: 1559
< QoS Control: 0x0005
.... 0101 = TID: 5
[.... 0101 = Priority: Video (Video) (5)]
.... 0000 0000 0000 = QoS bit 4: Bits 0-15 of QoS Control field are TXOP Duration Requested
.... 0000 0000 0000 = Ack Policy: Normal Ack (0x0)
.... 0000 0000 0000 = Payload Type: MSDU
0000 0000 .... = TXOP Duration Requested: 0 (no TXOP requested)
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.30.13, Dst: 192.168.31.10
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
< Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
  1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
  .... 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 1500
Identification: 0x2d1f (11551)

```

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.

No.	Time	SA	RA	Source	Destination	Protocol	DSCP	Priority	Length	Info
528	10:53:23.000000	192.168.30.13	192.168.31.10	192.168.30.13	192.168.31.10	UDP	EF PHB		838	52121 → 5201 Len=8192

```

> Frame 528: 838 bytes on wire (6704 bits), 838 bytes captured (6704 bits) on 0
> Ethernet II, Src: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d), Dst: Cisco_37:cd:e5 (2c:ab:eb:37:cd:e5)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1009
> Internet Protocol Version 4, Src: 192.168.30.13, Dst: 192.168.31.10
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
< Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
  1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
  .... 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 820

```

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.

No.	Time	SA	RA	Source	Destination	Protocol	DSCP	Priority	Length	Info
5039	10:33:23.187287	192.168.30.13	192.168.31.10	192.168.30.13	192.168.31.10	IPv4	EF PHB		1518	Fragmented IP protocol (p
5040	10:33:23.187381	192.168.30.13	192.168.31.10	192.168.30.13	192.168.31.10	IPv4	EF PHB		1518	Fragmented IP protocol (p

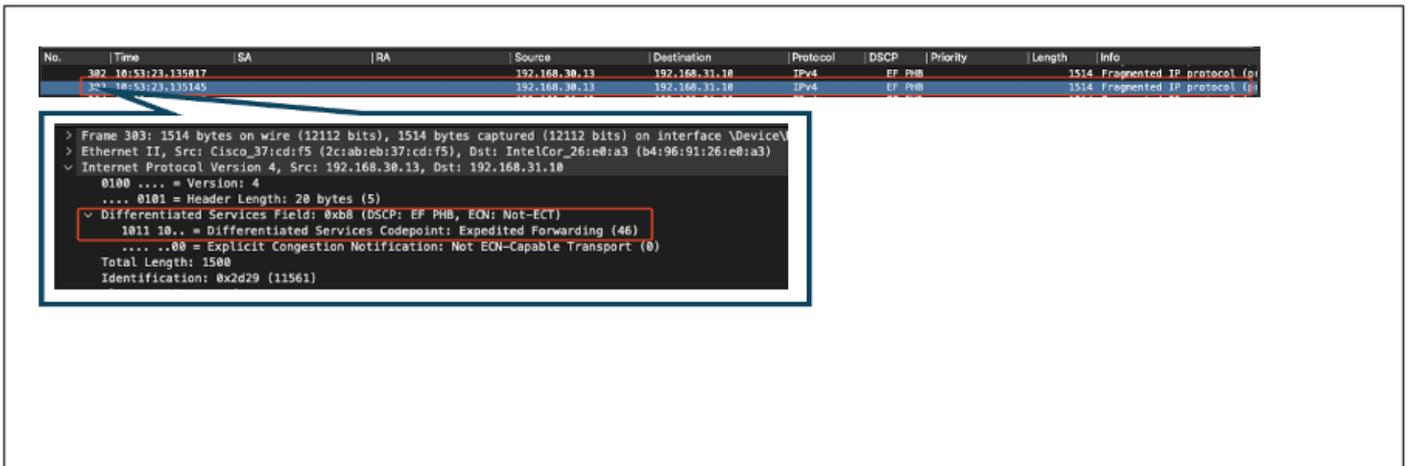
```

> Frame 5040: 1518 bytes on wire (12144 bits), 1518 bytes captured (12144 bits) on 0
> Ethernet II, Src: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d), Dst: Cisco_37:cd:e5 (2c:ab:eb:37:cd:e5)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1009
> Internet Protocol Version 4, Src: 192.168.30.13, Dst: 192.168.31.10
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
< Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
  1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
  .... 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 1500
Identification: 0x2d22 (11554)

```

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 regravava 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.

```
> Frame 367: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF...
> Ethernet II, Src: IntelCor_26:e0:a3 (b4:96:91:26:e0:a3), Dst: Cisco_37:cd:f5 (2c:ab:eb:37:cd:f5)
v Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 1500
  Identification: 0x5a74 (23156)
```

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.

```
> Frame 137: 1518 bytes on wire (12144 bits), 1518 bytes captured (12144 bits)
> Ethernet II, Src: Cisco_37:cd:e5 (2c:ab:eb:37:cd:e5), Dst: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
> 802.1Q Virtual LAN, PRI: 1, DEI: 0, ID: 1009
v Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (8)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 1500
  Identification: 0x5a41 (23105)
```

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).

```

> Frame 140: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits)
> Ethernet II, Src: Cisco_e7:9d:ab (80:2d:bf:e7:9d:ab), Dst: Cisco_28:35:74 (a4:b4:39:28:35:74)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 31
> Internet Protocol Version 4, Src: 10.105.60.198, Dst: 10.105.60.158
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  < Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (8)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 146
  Identification: 0x0000 (0)
> Flags: 0x00
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 255
  Protocol: UDP (17)
  Header Checksum: 0x2d05 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.105.60.198
  Destination Address: 10.105.60.158
> User Datagram Protocol, Src Port: 5247, Dst Port: 5262
> Control And Provisioning of Wireless Access Points - Data
> [2 Message fragments (1534 bytes): #139(1424), #140(110)]
> IEEE 802.11 QoS Data, Flags: .....F.
  Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8800(Swapped)
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
    Transmitter address: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
    Destination address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
    Source address: Cisco_37:cd:e5 (2c:ab:eb:37:cd:e5)
    BSS Id: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
    STA address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
    .... .... 0000 = Fragment number: 0
    0000 0000 0000 .... = Sequence number: 0
  < Qos Control: 0x0001
    .... .... 0001 = TID: 1
    [.... .... .001 = Priority: Background (Background) (1)]
    .... .... 0000 = EOSP: Service period
    .... .... .00. .... = Ack Policy: Normal Ack (0x0)
    .... .... 0... .... = Payload Type: MSDU
    > 0000 0000 .... .... = QAP PS Buffer State: 0x00
  > Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  < Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (8)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 1500
  Identification: 0x5a41 (23105)

```

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).

```

> Frame 613: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF...
> Ethernet II, Src: Cisco_4e:85:4f (a4:b4:39:4e:85:4f), Dst: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
> Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  < Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (8)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 1500

```

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.

```
> Frame 923: 834 bytes on wire (6672 bits), 834 bytes captured (6672 bits) on interface \Device\NPF_{009
> Ethernet II, Src: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d), Dst: Cisco_37:cd:e5 (2c:ab:eb:37:cd:e5)
v Internet Protocol Version 4, Src: 192.168.30.13, Dst: 192.168.31.10
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 820
  Identification: 0xcd67 (52583)
  \ 000 - Flags: 0x0
```

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.

```
> Frame 1080: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits)
> Ethernet II, Src: Cisco_28:35:74 (a4:b4:39:28:35:74), Dst: Cisco_e7:9d:ab (80:2d:bf:e7:9d:ab)
> 802.1Q Virtual LAN, PRI: 1, DEI: 0, ID: 31
✓ Internet Protocol Version 4, Src: 10.105.60.158, Dst: 10.105.60.198
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ✓ Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (8)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 130
  Identification: 0xe372 (58226)
  > Flags: 0x40, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 250
  Protocol: UDP (17)
  Header Checksum: 0x0ea2 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.105.60.158
  Destination Address: 10.105.60.198
> User Datagram Protocol, Src Port: 5262, Dst Port: 5247
> Control And Provisioning of Wireless Access Points - Data
> [2 Message fragments (1534 bytes): #1079(1440), #1080(94)]
✓ IEEE 802.11 QoS Data, Flags: .....T
  Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8800(Swapped)
  .000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: Cisco_4e:85:40 (a4:b4:39:4e:85:40)
  Transmitter address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
  Destination address: Cisco_37:cd:e5 (2c:ab:eb:37:cd:e5)
  Source address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
  BSS Id: Cisco_4e:85:40 (a4:b4:39:4e:85:40)
  STA address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
  .... .... 1000 = Fragment number: 8
  1000 0001 1110 .... = Sequence number: 2078
  ✓ Qos Control: 0x0006
    ..... 0110 - TID: 6
    [..... .110 = Priority: Voice (Voice) (6)]
    .... .... 0 .... = QoS bit 4: Bits 8-15 of QoS Control field are TXOP Duration Requested
    .... .... .00. .... = Ack Policy: Normal Ack (0x0)
    .... .... 0... .... = Payload Type: MSDU
    0000 0000 .... .... = TXOP Duration Requested: 0 (no TXOP requested)
> Logical-Link Control
✓ Internet Protocol Version 4, Src: 192.168.30.13, Dst: 192.168.31.10
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ✓ Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 1500
```

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.

```
> Frame 1000: 834 bytes on wire (6672 bits), 834 bytes captured (6672 bits) on interface \Device\NPF...
> Ethernet II, Src: Cisco_37:cd:f5 (2c:ab:eb:37:cd:f5), Dst: IntelCor_26:e0:a3 (b4:96:91:26:e0:a3)
v Internet Protocol Version 4, Src: 192.168.30.13, Dst: 192.168.31.10
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 820
```

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.