Configure Validar y solucionar problemas de QoS inalámbrica en el WLC 9800

Contenido

Introducción

Este documento describe maneras de configurar, validar y resolver problemas de calidad de servicio (QoS) inalámbrica en el controlador de LAN inalámbrica (WLC) 9800.

Componentes Utilizados

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

- WLC: C9800-40-K9 que ejecuta 17.12.03
- Punto de acceso (AP): C9120-AX-D

- Switch: C9300-48P que ejecuta 17.03.05
- Cliente por cable e inalámbrico: Windows 10

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

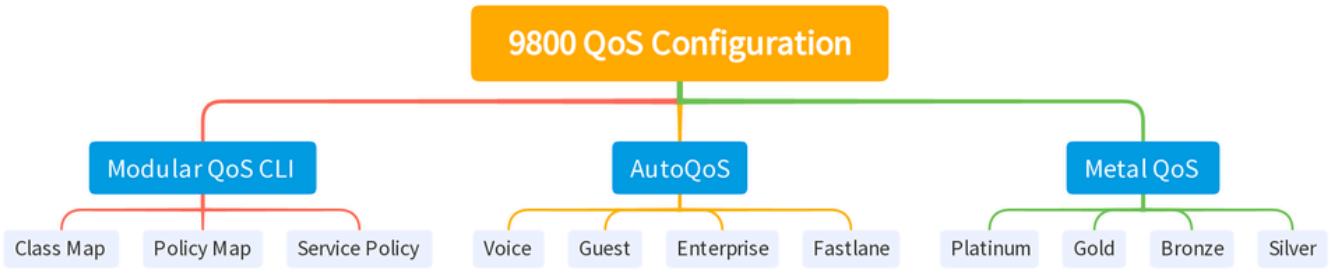
La QoS inalámbrica es esencial para garantizar que las aplicaciones críticas reciban el ancho de banda necesario y la baja latencia necesaria para obtener un rendimiento óptimo. Este documento proporciona una guía completa para configurar, validar y resolver problemas de QoS en redes inalámbricas de Cisco.

En este artículo se asume que los lectores tienen un conocimiento básico de los principios de QoS inalámbrica y por cable. También se espera que los lectores sean competentes en la configuración y administración de los WLC y AP de Cisco.

Configuración

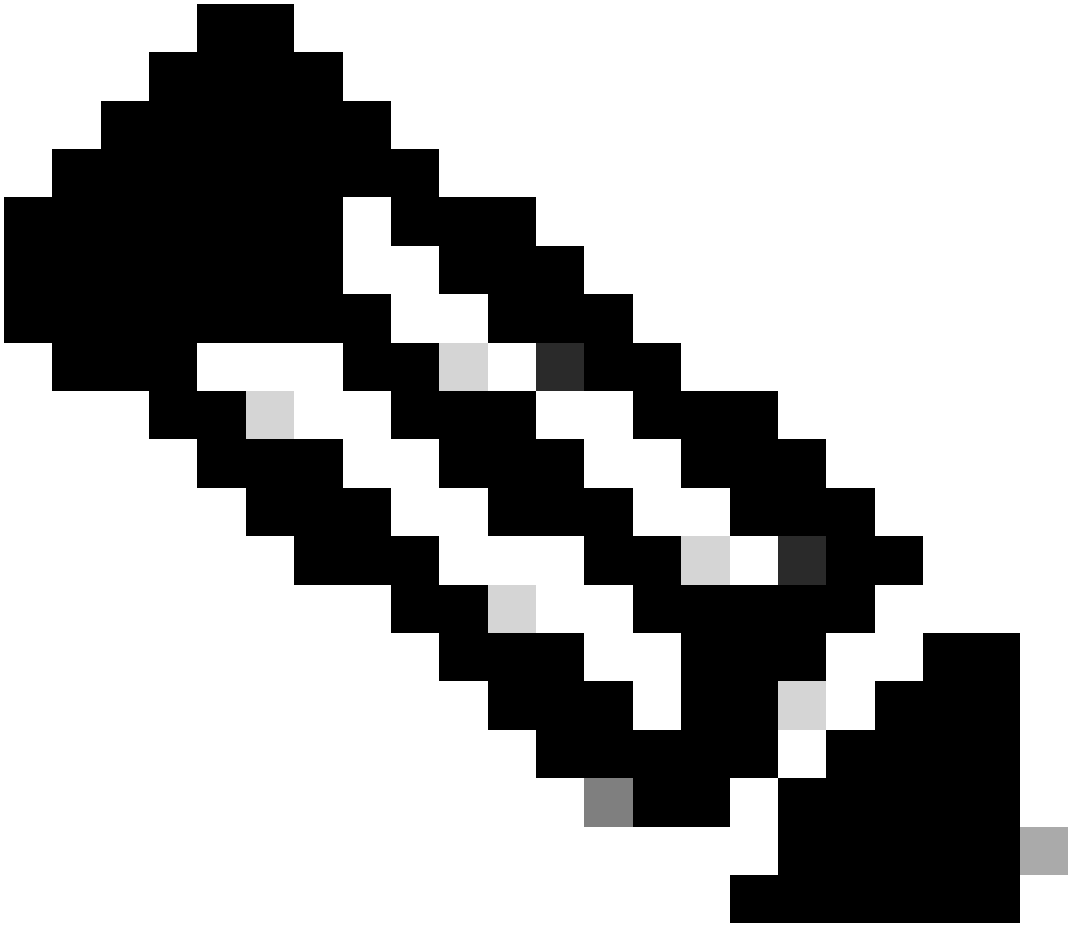
Esta sección profundiza en la configuración de QoS en los controladores inalámbricos 9800. Al aprovechar estas configuraciones, puede asegurarse de que las aplicaciones críticas reciban el ancho de banda necesario y una baja latencia, optimizando así el rendimiento general de la red.

Puede dividir la configuración de QoS del WLC 9800 en tres categorías generales diferentes principalmente.



Resumen de configuración de QOS del WLC 9800

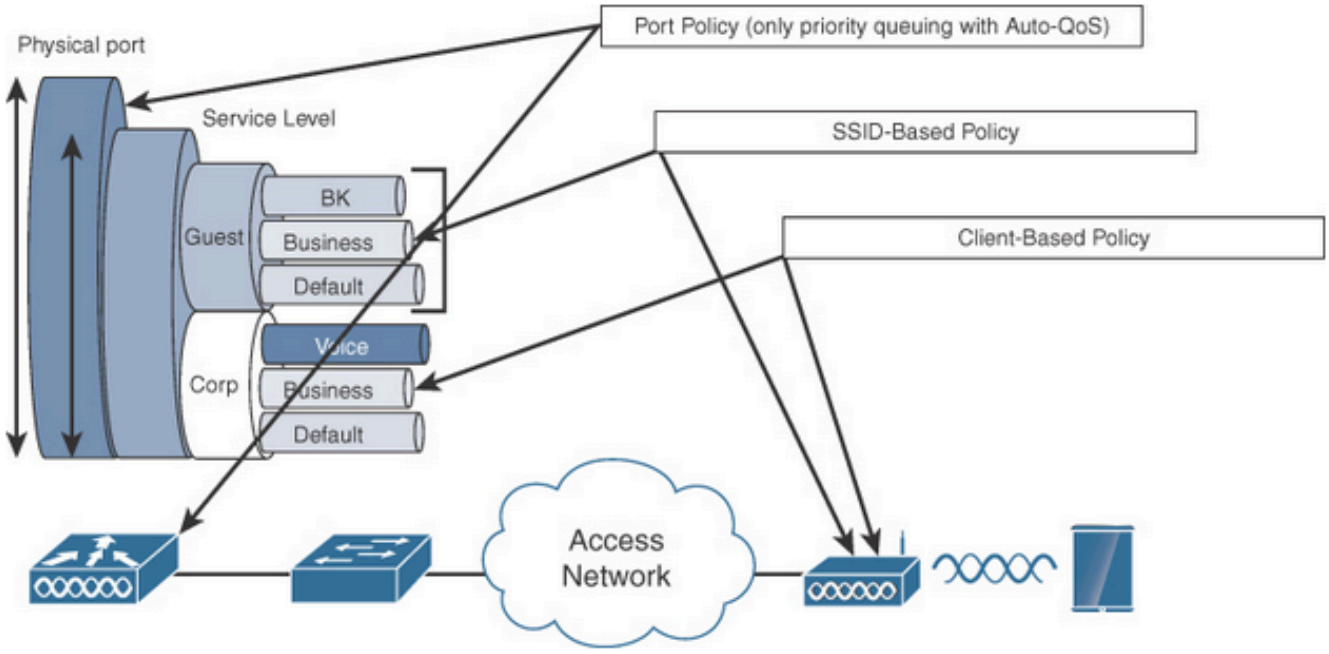
Este documento recorre cada sección una por una en las siguientes secciones.



Nota: Este artículo se centra en AP en modo local. El AP en el modo Flexconnect no se discute.

Destinos de política de QoS

Un destino de política es la construcción de configuración donde se puede aplicar una política de QoS. La implementación de QoS en el Catalyst 9800 es modular y flexible. El usuario puede decidir configurar directivas en tres destinos diferentes: el SSID, el cliente y los niveles de puerto.



Destinos de política de QoS

La política SSID es aplicable por AP por SSID. Puede configurar políticas de regulación y marcación en SSID.

Las políticas de cliente son aplicables en la dirección de entrada y salida. Puede configurar directivas de regulación y marcación en los clientes. También se admite la anulación de AAA.

Las políticas de QoS basadas en puerto se pueden aplicar en un puerto físico o lógico.

Auto QoS

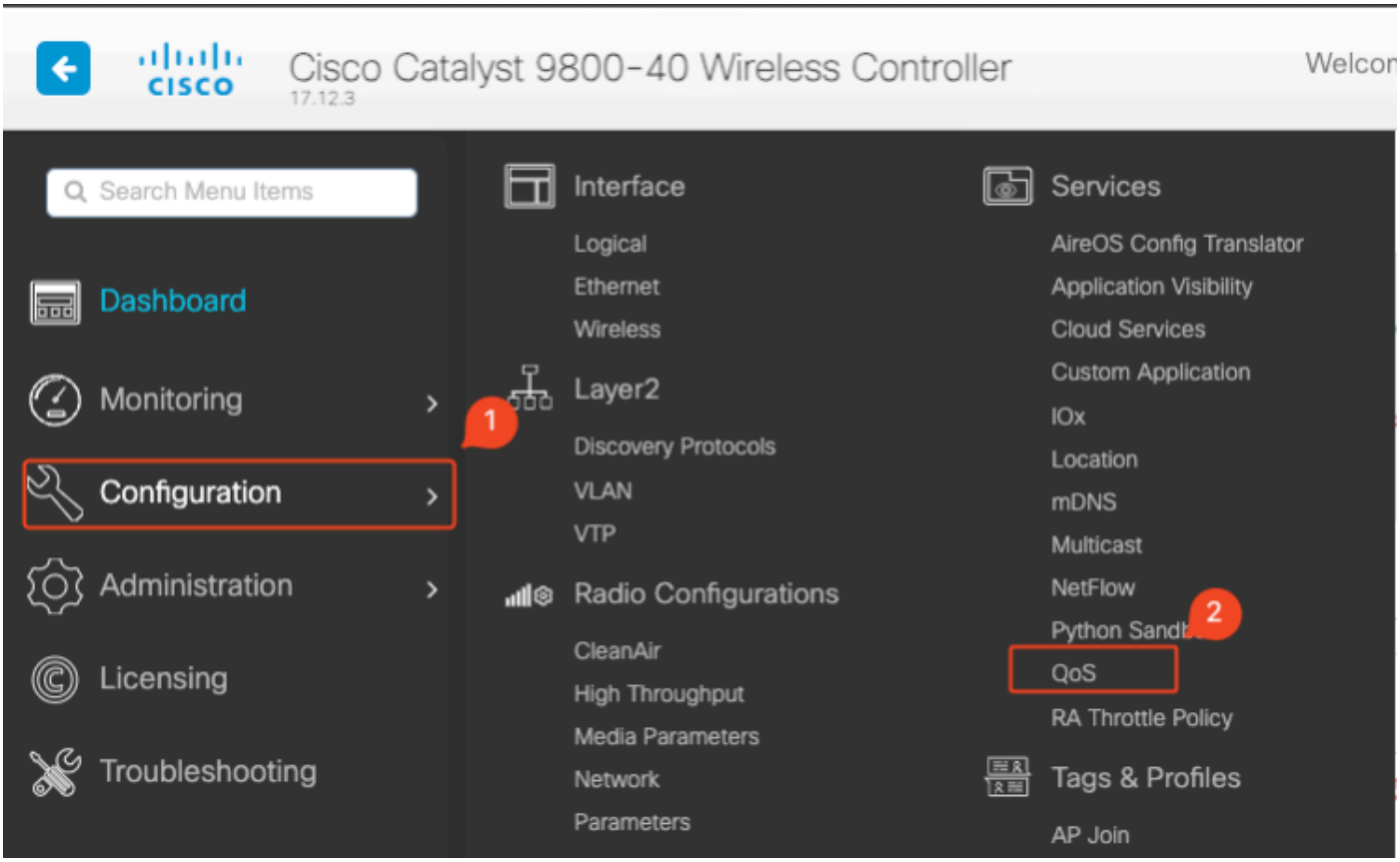
Wireless Auto QoS automatiza la implementación de las funciones de QoS inalámbrica. Dispone de un conjunto de perfiles predefinidos que el administrador puede modificar para dar prioridad a los distintos flujos de tráfico. Auto-QoS coincide con el tráfico y asigna cada paquete coincidente a los grupos de QoS. Esto permite que el mapa de política de salida coloque grupos de QoS específicos en colas específicas, incluida la cola de prioridad.

Modo	Ingreso de cliente	Salida de cliente	Ingreso de BSSID	Salida BSSID	Ingreso de puerto	Egreso de puerto	Radio
Voice	N/A	N/A	de platino	platino	N/A	AutoQos-4.0-wlan-Port-Output-Policy	ACM activado
Guest	N/A	N/A	AutoQos-4.0-wlan-GT-SSID-	AutoQos-4.0-wlan-GT-SSID-	N/A	AutoQos-4.0-wlan-Port-	

			Input-Policy	Output-Policy		Output-Policy	
Vía Rápida	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	

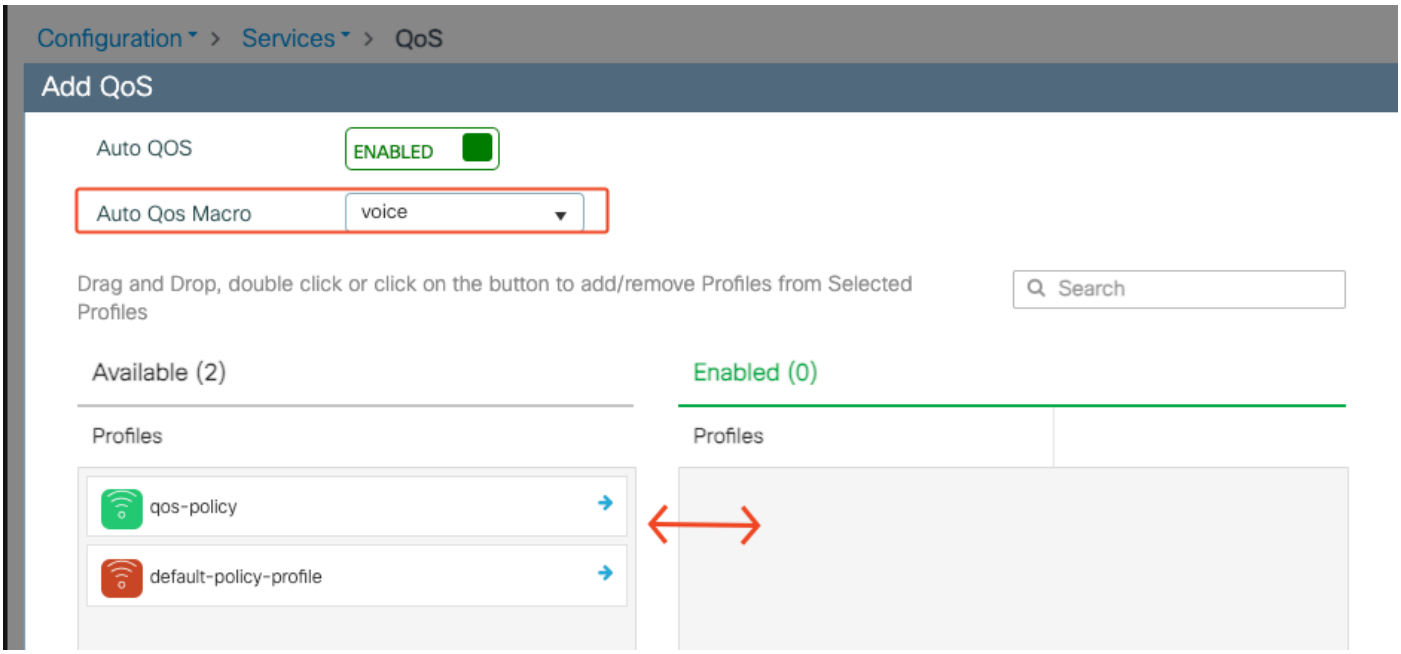
Esta tabla describe los cambios de configuración que se producen cuando se aplica un perfil de QoS automático.

Para configurar Auto QoS, navegue hasta Configuration > QoS



Flujo de trabajo QoS

Haga clic en Add y establezca Auto QoS en enabled. Elija la macro Auto QoS adecuada de la lista. Para este ejemplo, se utiliza la macro Voice para dar prioridad al tráfico de voz.



Asignación de voz AutoQoS

Una vez habilitada la macro, seleccione la directiva que debe adjuntarse a la directiva.

Configuración automática de QoS CLI

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

Ahora que Auto QoS está habilitado, puede ver los cambios que ocurrieron. Esta sección enumera los cambios de configuración para la 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 de QoS modular

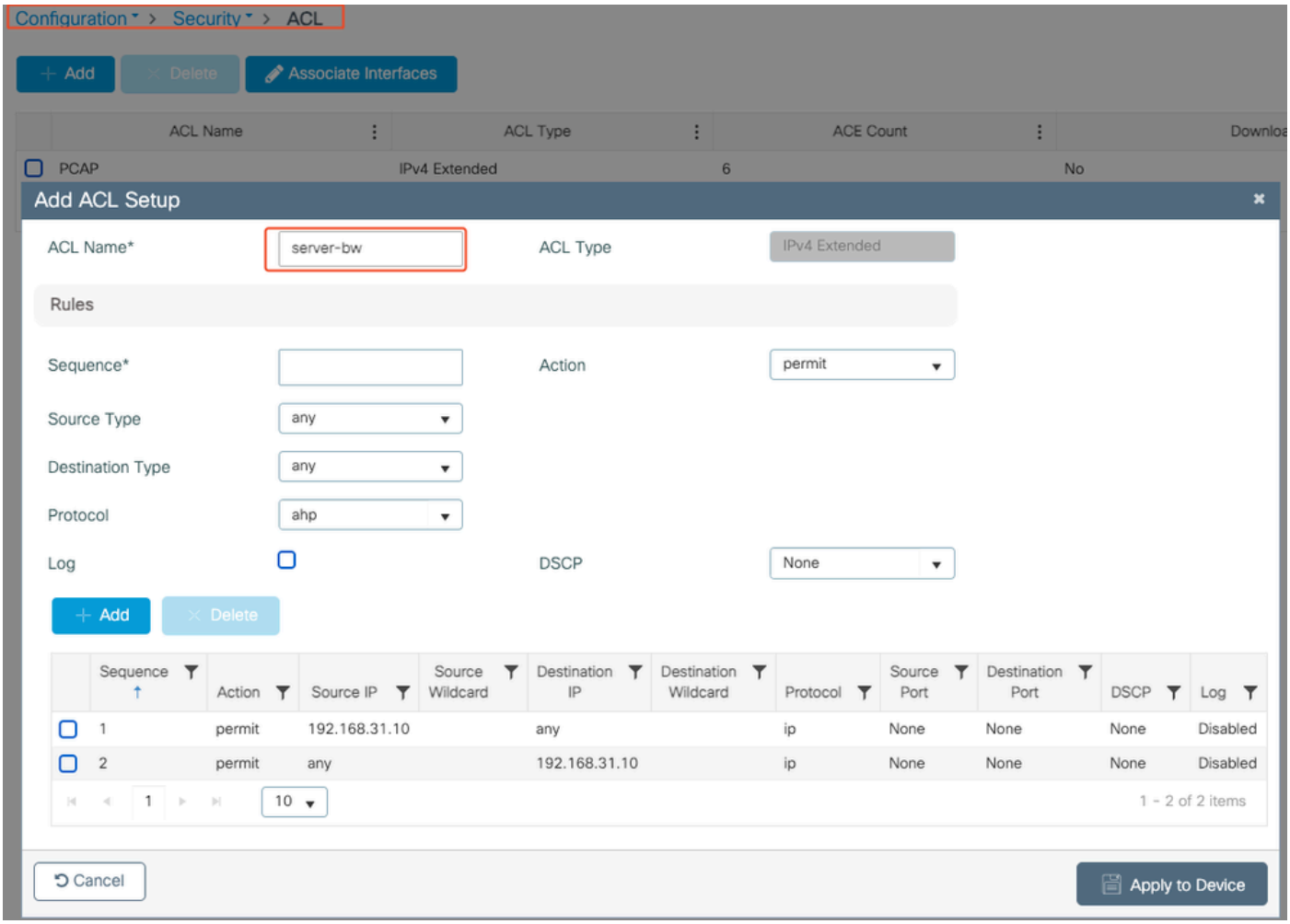
El MQC le permite definir una clase de tráfico, crear una política de tráfico (policy map) y adjuntar la política de tráfico a una interfaz. La política de tráfico contiene la función QoS que se aplica a la clase de tráfico.

Flujo de trabajo CLI MQS

Este ejemplo muestra cómo utilizar las listas de control de acceso (ACL) para clasificar el tráfico y aplicar restricciones de ancho de banda.

Cree una ACL para identificar y clasificar el tráfico específico que desea administrar. Esto se puede hacer mediante la definición de reglas que coincidan con el tráfico en función de criterios como las direcciones IP, los protocolos o los puertos.

Vaya a Configuration > Security > ACL y agregue la ACL.

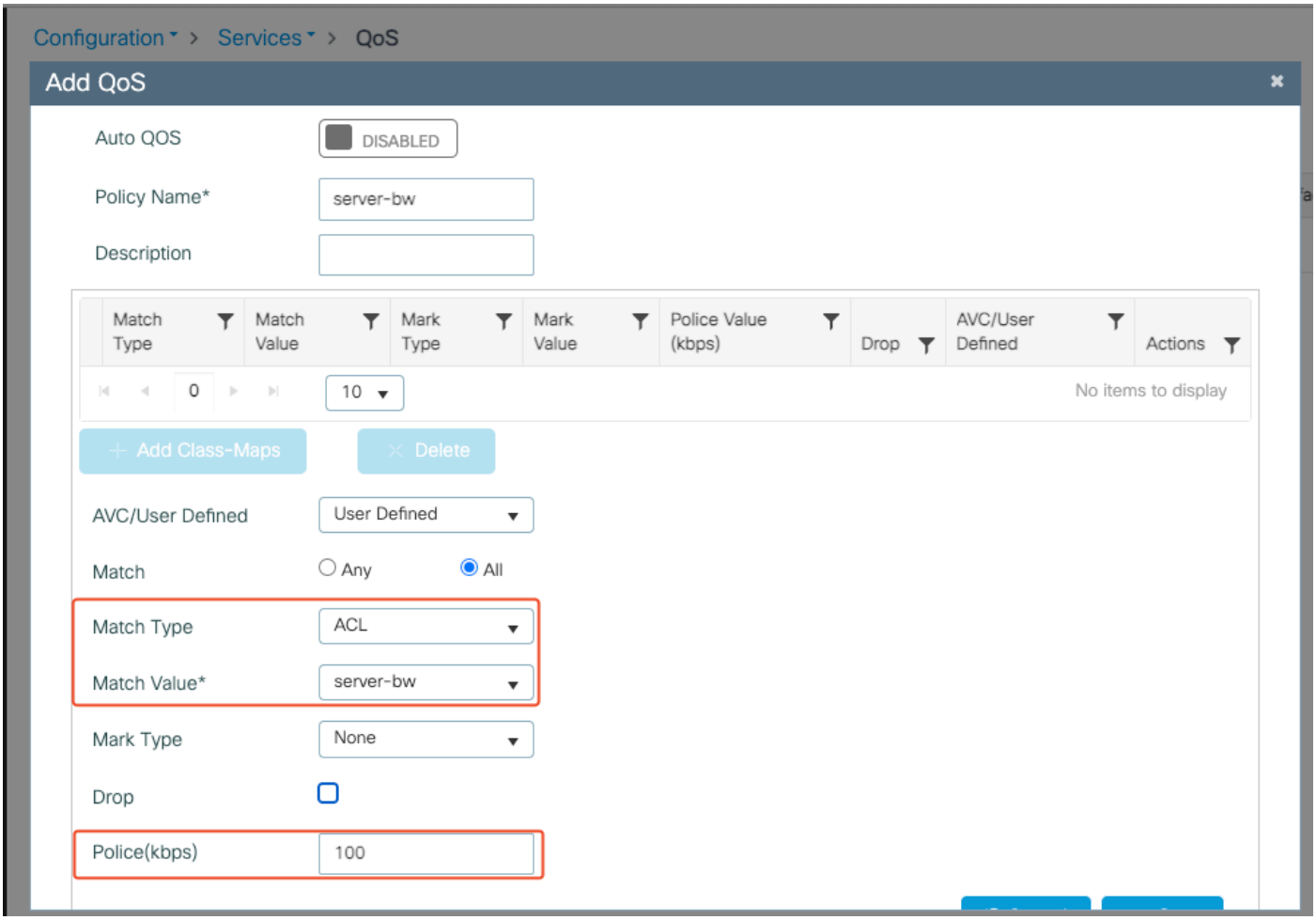


Configuración de ACL

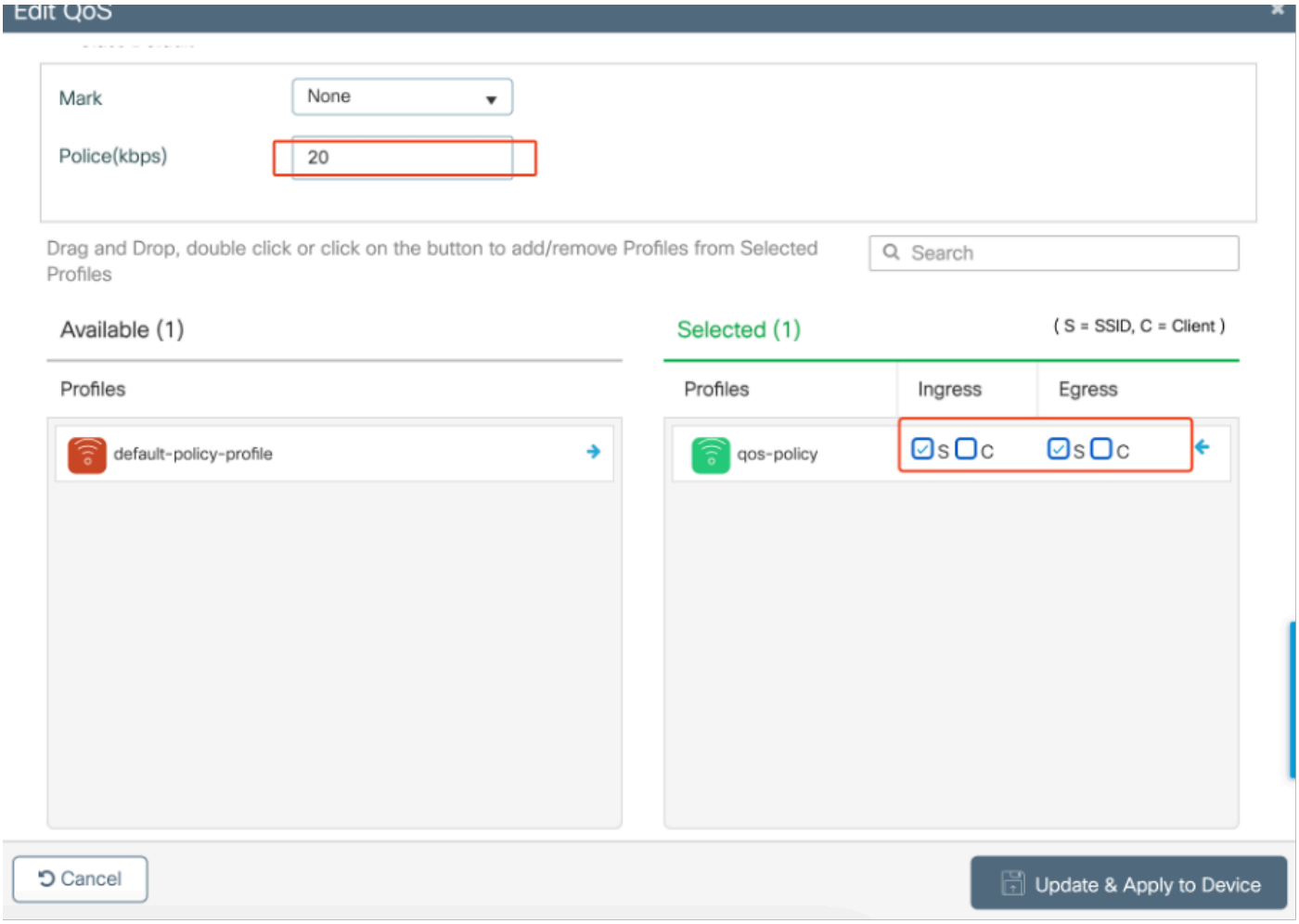
Una vez que el tráfico se clasifica mediante la ACL, configure las restricciones de ancho de banda para controlar la cantidad de ancho de banda asignado a este tráfico.

Navegue hasta Configuration > Services > QoS y la política de QoS. Adjunte la ACL dentro de la política y aplique la policía en kbps.

Desplácese hacia abajo y seleccione el perfil de política en el que se aplicará QoS. Puede seleccionar la política en la dirección de entrada/ salida tanto para SSID como para Cliente.



Política de MQS



Perfil MQS

configuración CLI de MQS

```
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

El objetivo principal de estos perfiles de QoS es limitar los valores máximos de punto de código de servicios diferenciados (DSCP) permitidos en una red inalámbrica, con lo que se controlan los valores de prioridad de usuario (UP) 802.11.

En el controlador de LAN inalámbrica (WLC) Cisco 9800, los perfiles de QoS de metal están predefinidos y no se pueden configurar. Sin embargo, puede aplicar estos perfiles a SSID o clientes específicos para aplicar políticas de QoS.

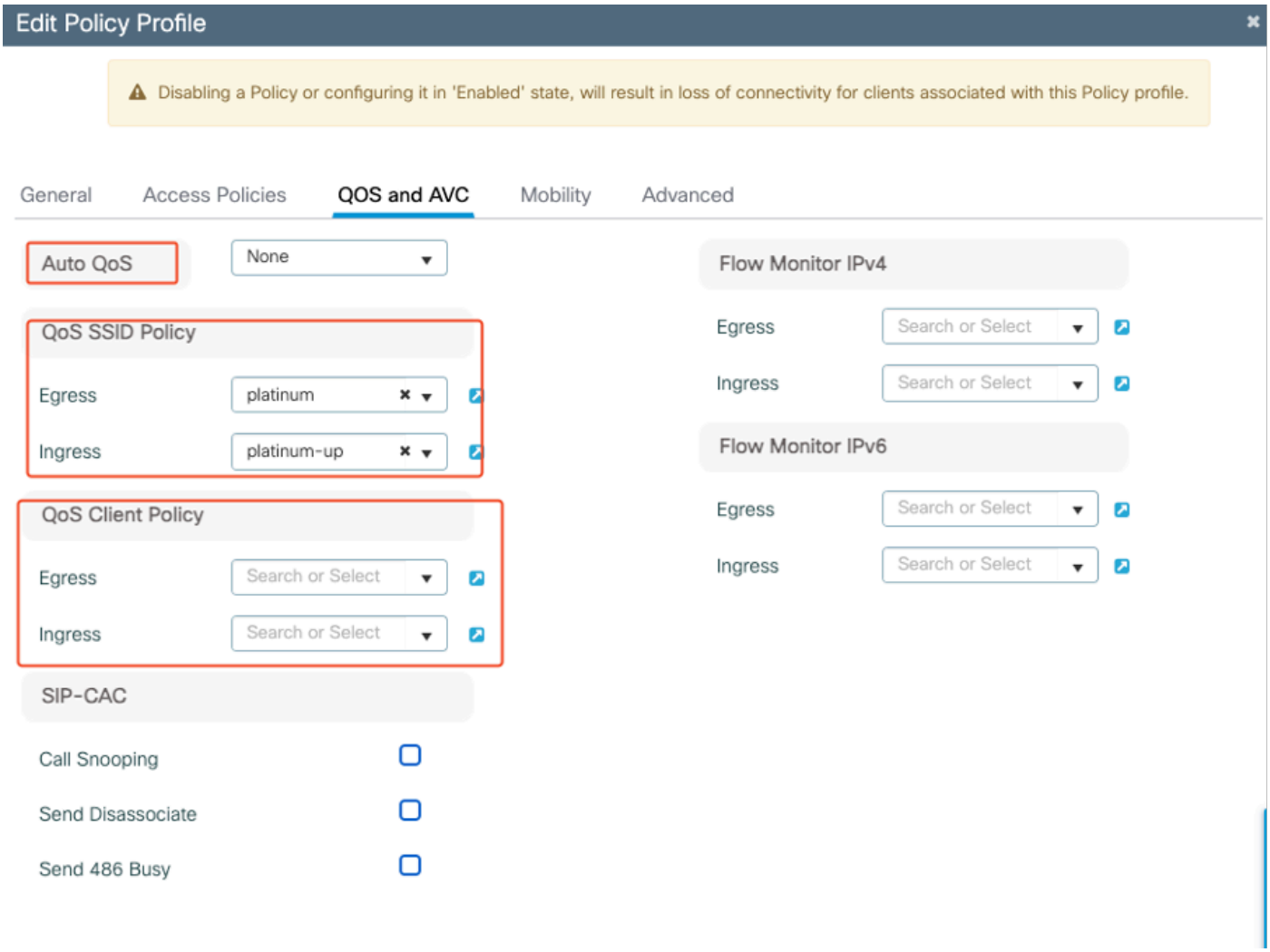
Hay cuatro perfiles de QoS de metal disponibles:

Perfil de Calidad de servicio (QoS)	DSCP máximo
Bronce	8
Plata	0
Oro	34
Platino	46

Para configurar Metal QoS en un Cisco 9800 WLC:

Vaya a Configuration > Policy > QoS & AVC.

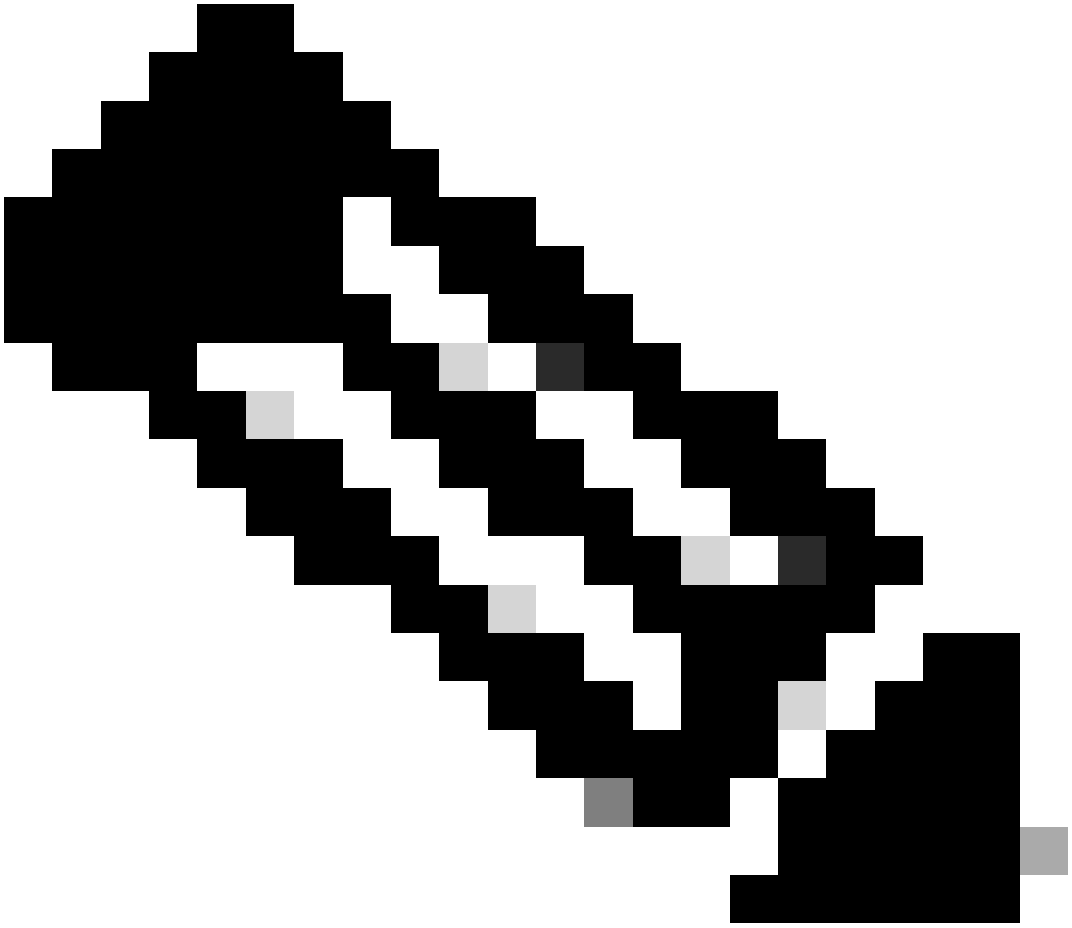
- Seleccione el perfil de QoS de metal que desee (Platino, Oro, Plata o Bronce).
- Aplique el perfil elegido al SSID o cliente de destino.



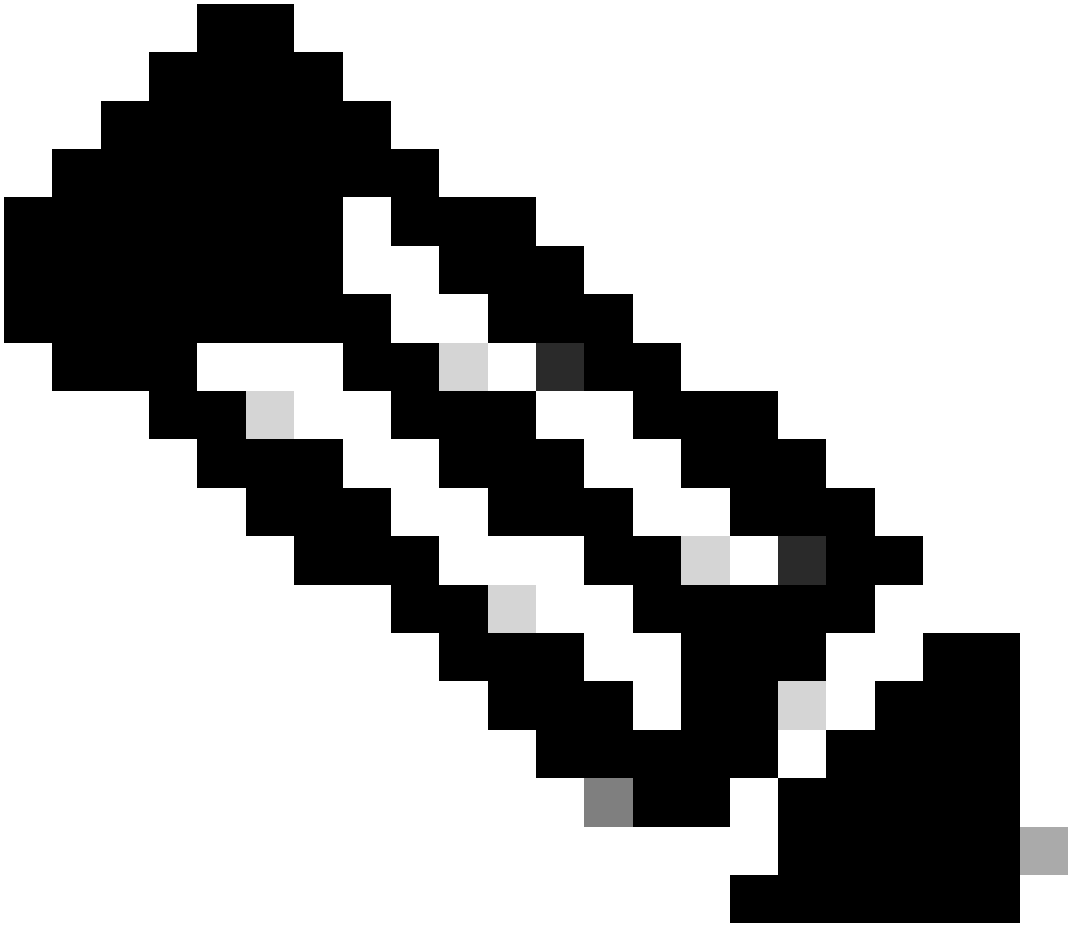
Perfil de QoS de metal

Configuración de Metal QoS CLI

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



Nota: los contratos de ancho de banda SSID y por usuario se pueden configurar mediante políticas de QoS y no directamente en Metal QoS. En el 9800, el tráfico no coincidente va en la clase predeterminada.



Nota: En la GUI, solo puede establecer la QoS de metal por SSID. En CLI también puede configurarlo en el destino del cliente.

Validar QoS de extremo a extremo con captura de paquetes

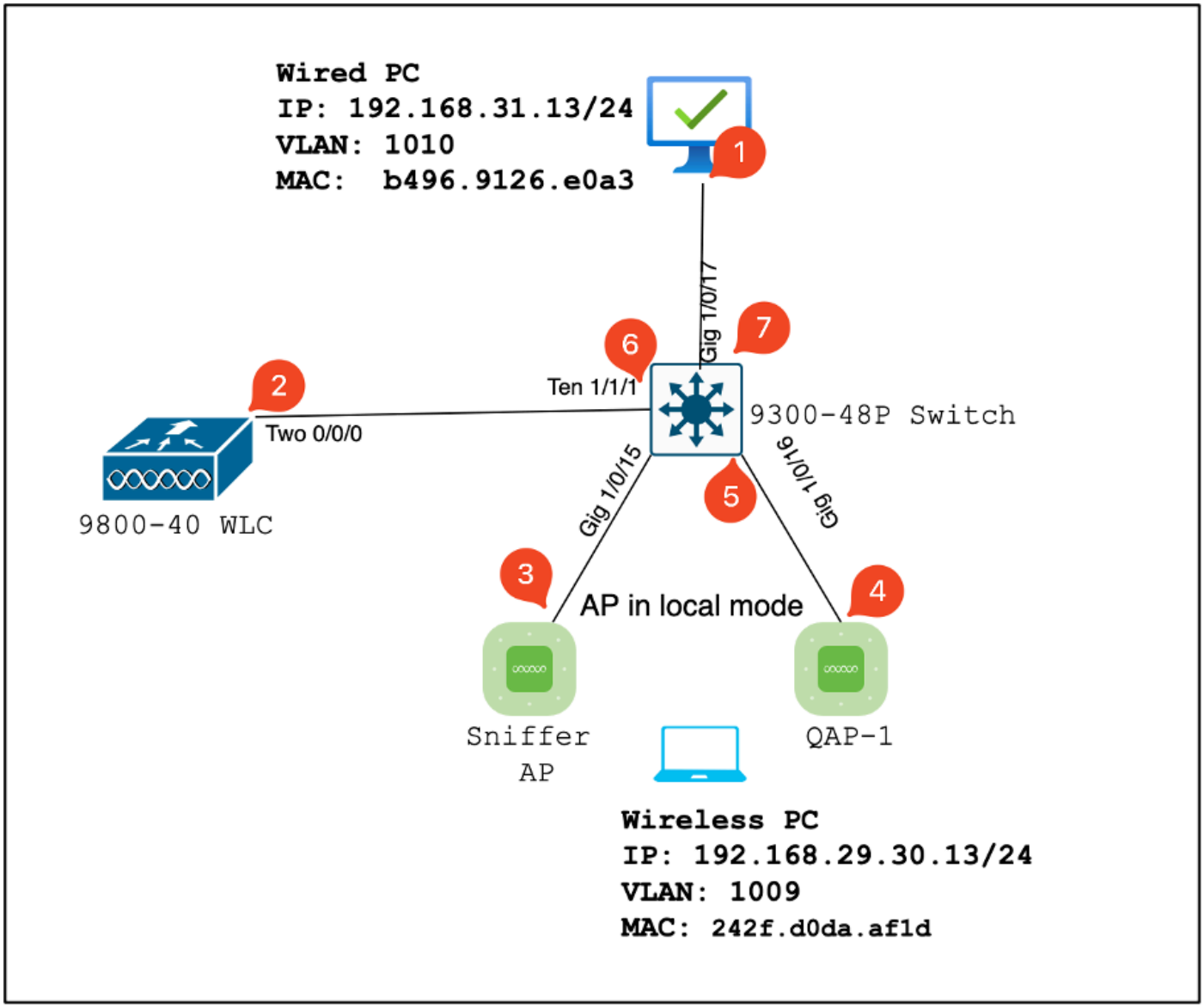
Ahora que se ha completado la configuración de QoS, es esencial examinar los paquetes de QoS y validar que las políticas de QoS funcionen correctamente de extremo a extremo. Esto puede lograrse mediante la captura y el análisis de paquetes.

Para replicar y validar la configuración de QoS, se utiliza un entorno de laboratorio a pequeña escala. El laboratorio incluye estos componentes:

- WLC
- AP
- Sniffer AP para tomar OTA
- PC con cables
- Switch

Todos estos componentes están conectados al mismo switch dentro del entorno de laboratorio. Los números resaltados en este diagrama indican los puntos donde las capturas de paquetes están habilitadas para monitorear y analizar el flujo de tráfico.

Diagrama de la red



Topología de laboratorio

Componentes de laboratorio y puntos de captura de paquetes

WLC:

- Administra las configuraciones y políticas de QoS para la red inalámbrica.
- Punto de captura de paquetes: captura el tráfico entre el WLC, el AP y el switch.

AP:

- Proporciona conectividad inalámbrica a los clientes y aplica las políticas de QoS.
- Punto de captura de paquetes: captura el tráfico entre el AP y el switch.

AP de sabueso:

- Actúa como un dispositivo dedicado para capturar tráfico inalámbrico.
- Punto de captura de paquetes: captura el tráfico inalámbrico entre el punto de acceso y los clientes inalámbricos.

PC con cables:

- Conectado al switch para simular el tráfico por cable y validar la calidad de servicio integral.
- Punto de captura de paquetes: captura de paquetes de QoS transmitidos y recibidos a través de un enlace por cable.

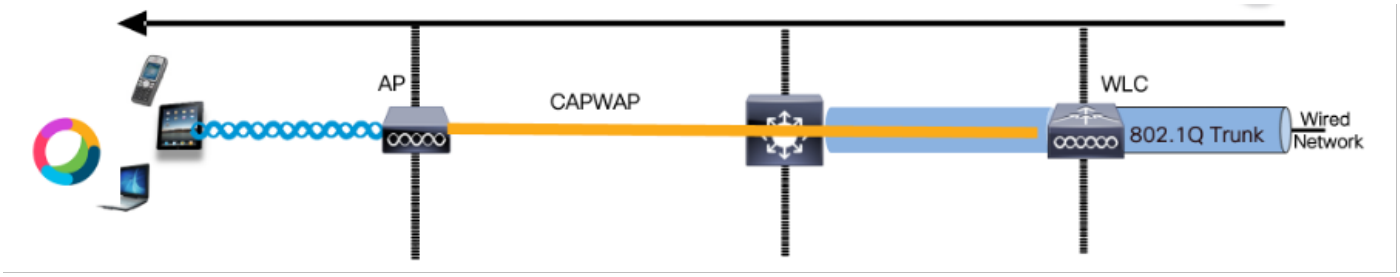
PC inalámbrico:

- Conectado a la WLAN para simular el tráfico inalámbrico y validar la calidad de servicio integral.
- Punto de captura de paquetes: captura de paquetes de QoS transmitidos y recibidos a través de un enlace inalámbrico.

Switch:

- El dispositivo central que interconecta todos los componentes del laboratorio y facilita el flujo de tráfico.
- Puntos de captura de paquetes: capture el tráfico en varios puertos de switch para validar la aplicación adecuada de QoS.

Lógicamente, la topología de LAB se puede dibujar así.



Topología de LAB lógico

Para probar y validar la configuración de QoS, se utiliza iPerf para generar tráfico entre el cliente y el servidor. Estos comandos se utilizan para facilitar la comunicación de iPerf, con las funciones del servidor y el cliente intercambiadas según la dirección de las pruebas de QoS.

Escenario de prueba 1: validación de QoS descendente

El objetivo es validar la configuración de QoS descendente. La configuración implica que un PC cableado envíe paquetes con DSCP 46 a un PC inalámbrico.
El controlador de LAN inalámbrica (WLC) se configura con la política "Platinum QoS" de metal para las direcciones de flujo ascendente y descendente.

Configuración de prueba:

- Flujo de tráfico:

  Fuente: PC con cables

  Destino: PC inalámbrico

  Tipo de tráfico: paquetes UDP con DSCP 46

- Configuración de política de QoS en WLC:

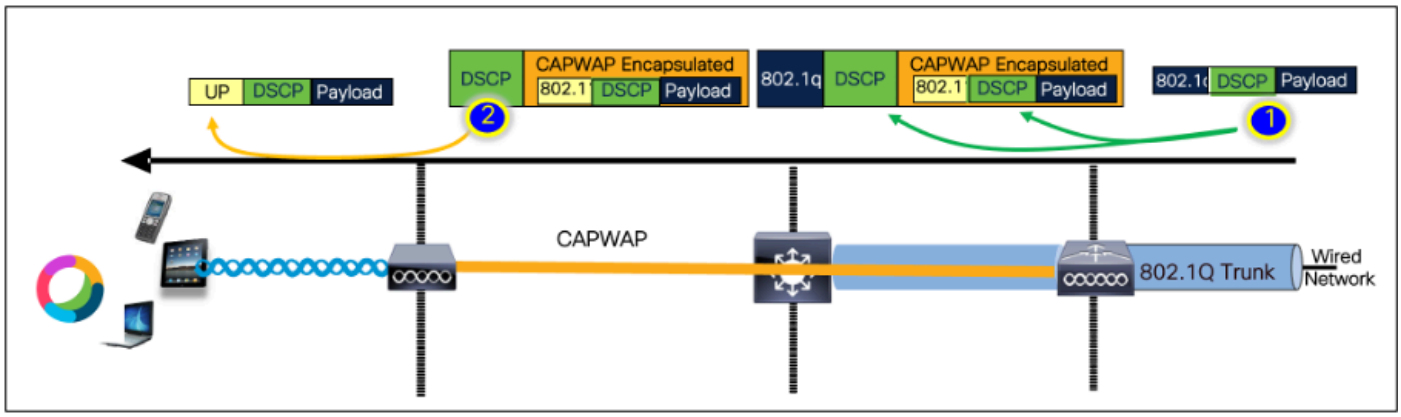
  Perfil de QoS: QoS de metal - QoS de platino

  Dirección: tanto aguas abajo como aguas arriba

- Comandos de configuración de QoS de metal:

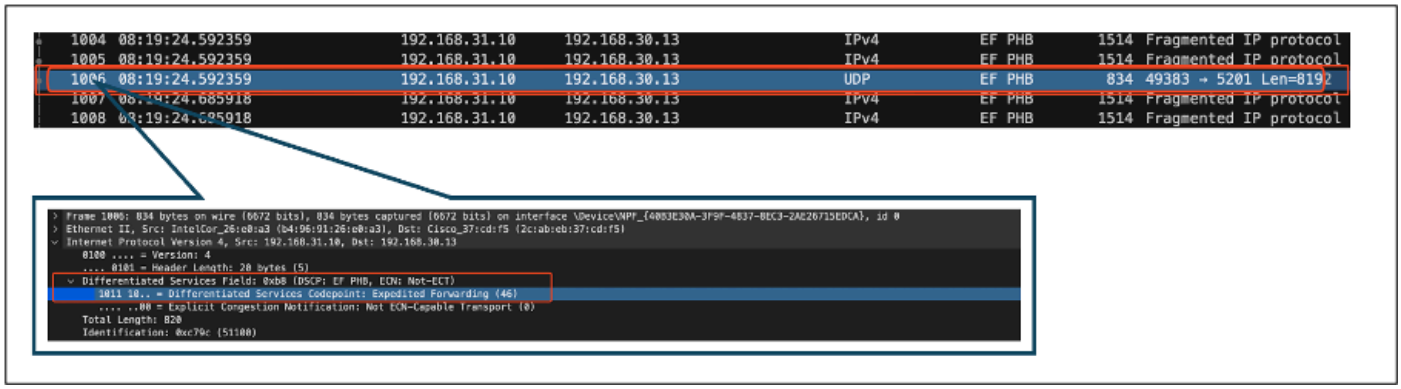
```
wireless profile policy qos-policy
service-policy input platinum-up
service-policy output platinum
```

Topología lógica y conversación DSCP en dirección descendente.



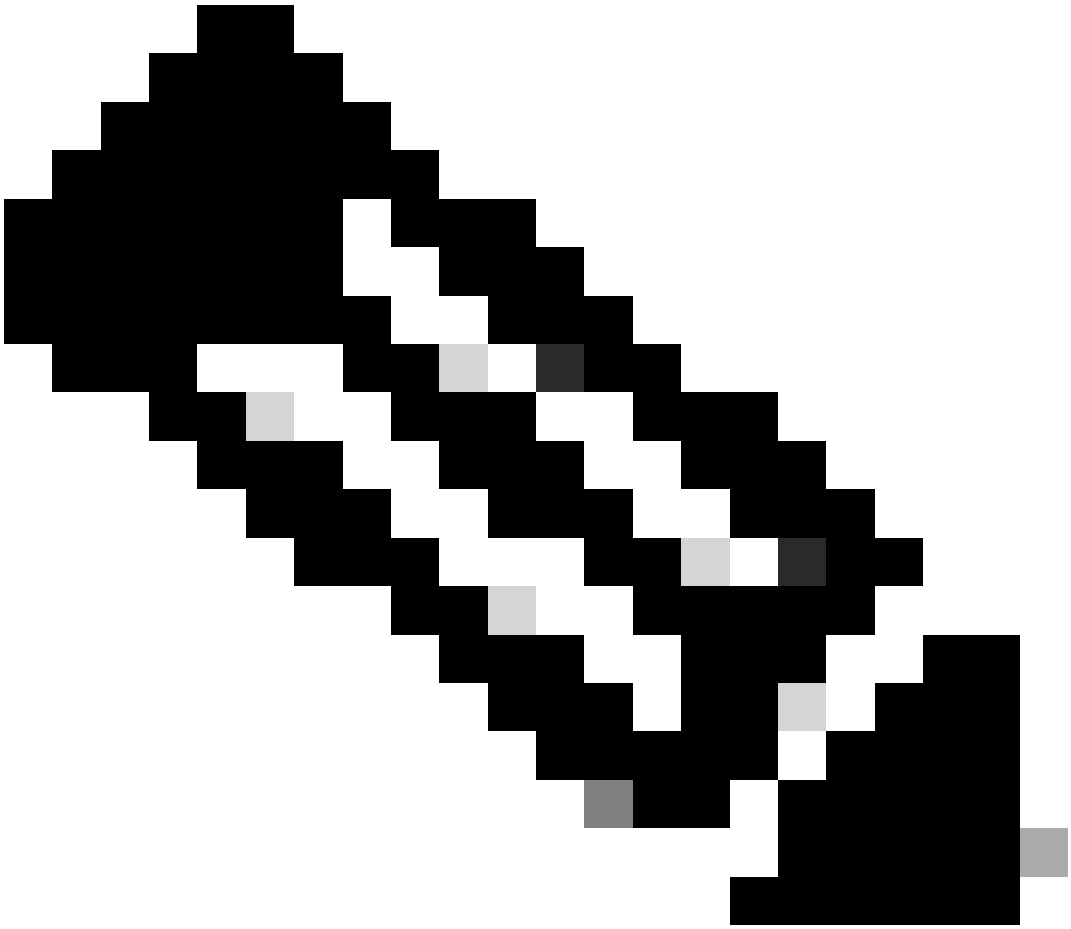
Punto de conversación DSCP

Captura de paquetes realizada en el PC con cables. Esto confirma que la PC cableada está enviando paquetes UDP a la IP de destino especificada 192.168.10.13 con la marca DSCP correcta de 46.

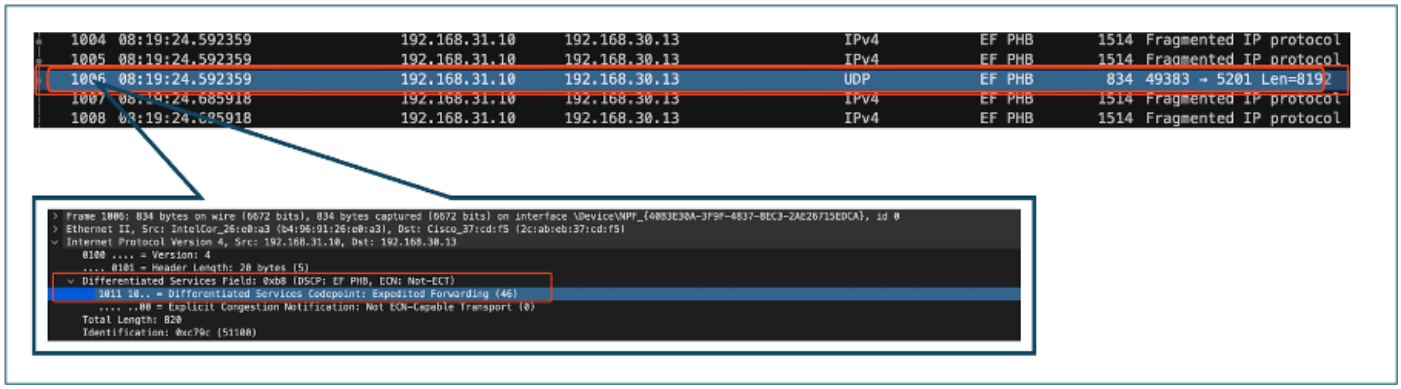


Captura de PC con cables - Dirección descendente

A continuación, examinemos un paquete capturado en el switch de enlace ascendente conectado al PC con cables. El switch confía en la etiqueta DSCP y el valor DSCP permanece inalterado en 46.

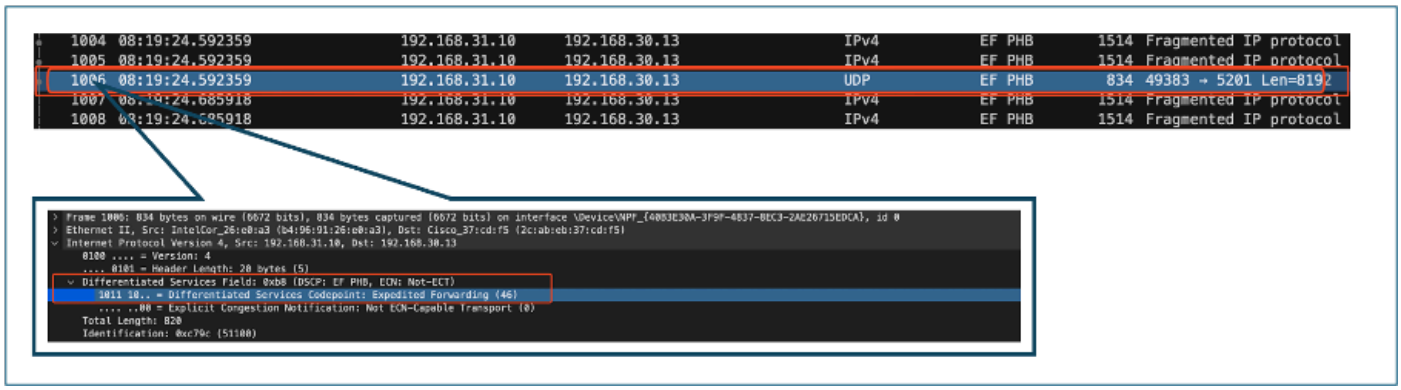


> Nota: Los puertos del switch de la serie Catalyst 9000 tienen un estado predeterminado de confianza.



Captura de interfaz de enlace ascendente de PC con cable

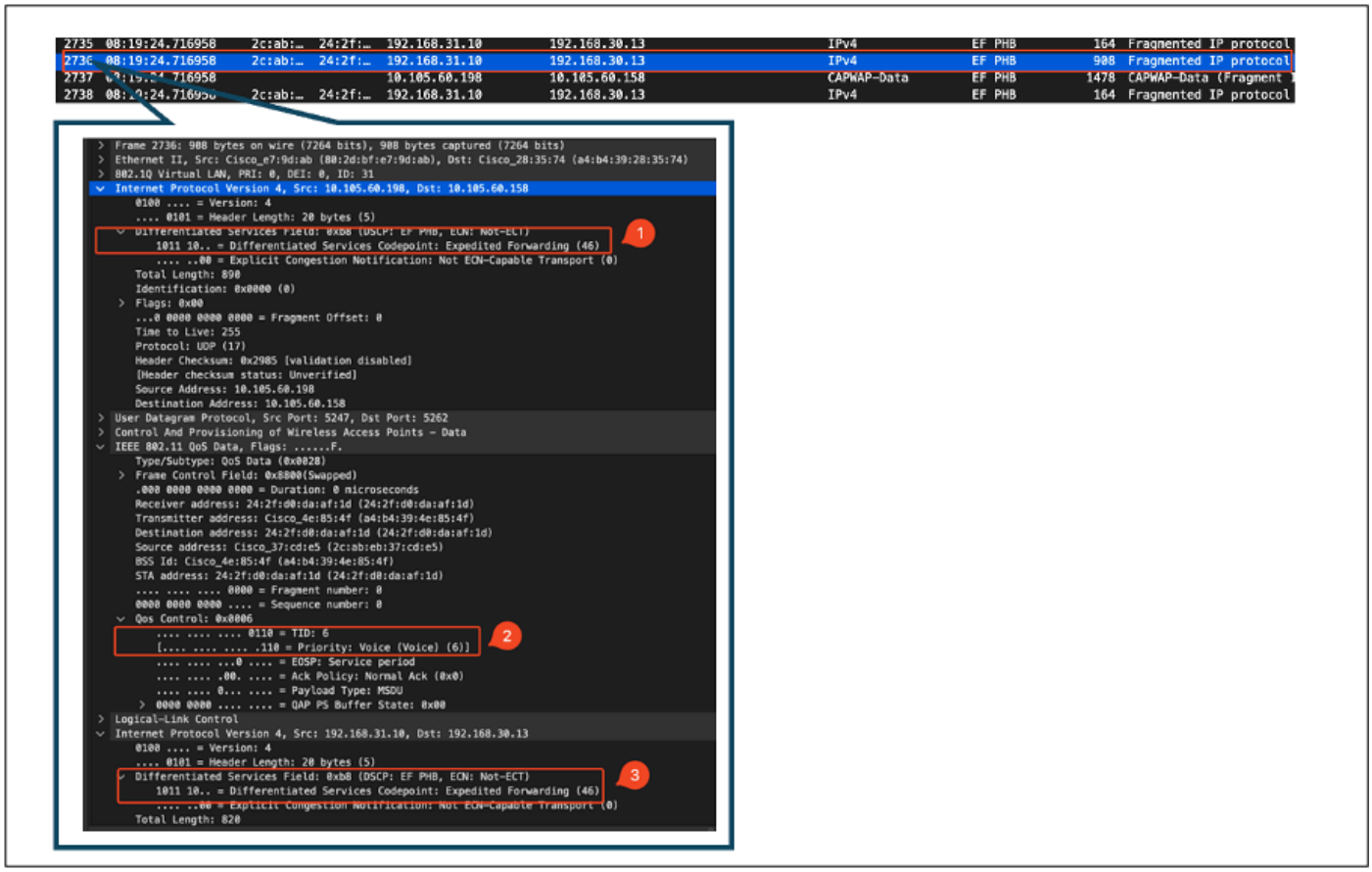
Al examinar la captura de paquetes en el WLC tomada usando EPC, el paquete llega con la misma etiqueta DSCP de 46 desde el switch de link ascendente. Esto confirma que el marcado DSCP se conserva cuando el paquete alcanza el WLC.



Dirección descendente de WLC EPC

Cuando el WLC envía el paquete al AP dentro de un túnel CAPWAP, es una intersección crítica donde el WLC puede modificar el DSCP basado en su configuración. Detallemos la captura de paquetes, que se resalta con puntos numerados para mayor claridad:

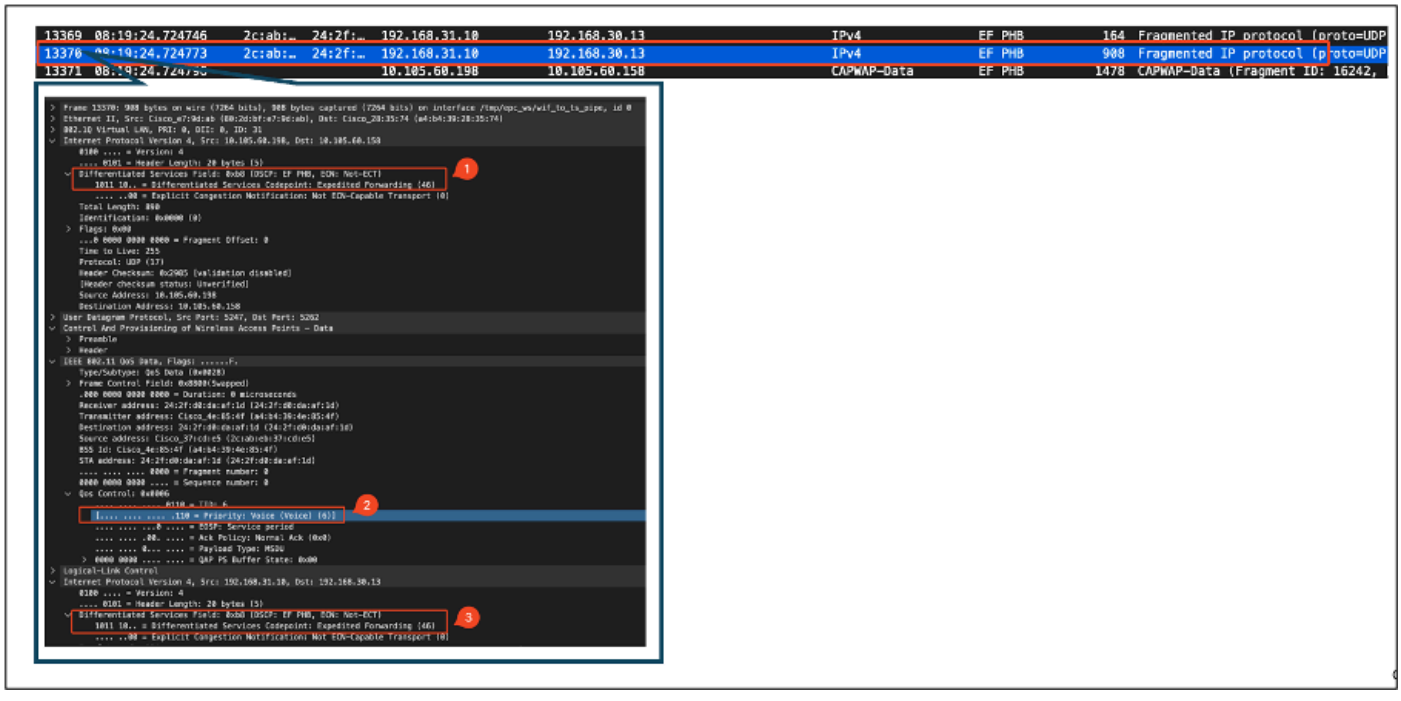
- Capa externa CAPWAP: La capa externa del túnel CAPWAP muestra la etiqueta DSCP como 46, que es el valor recibido del extremo del switch.
- Valor UP 802.11 dentro de CAPWAP: Dentro del túnel CAPWAP, el WLC mapea el DSCP 46 a la prioridad de usuario (UP) 6 802.11, que corresponde al tráfico de voz.
- Valor DSCP dentro de CAPWAP: El WLC Cisco 9800 funciona con un modelo DSCP de confianza, por lo que el valor DSCP dentro del túnel CAPWAP se mantiene en 46 igual que la capa DSCP externa.



Marcas CAPWAP DSCP

Luego, verifique el mismo paquete en el puerto del switch de link ascendente AP.

El valor DSCP en la capa CAPWAP externa permanece en 46. A título ilustrativo, se resalta el tráfico CAPWAP interno para mostrar el etiquetado.

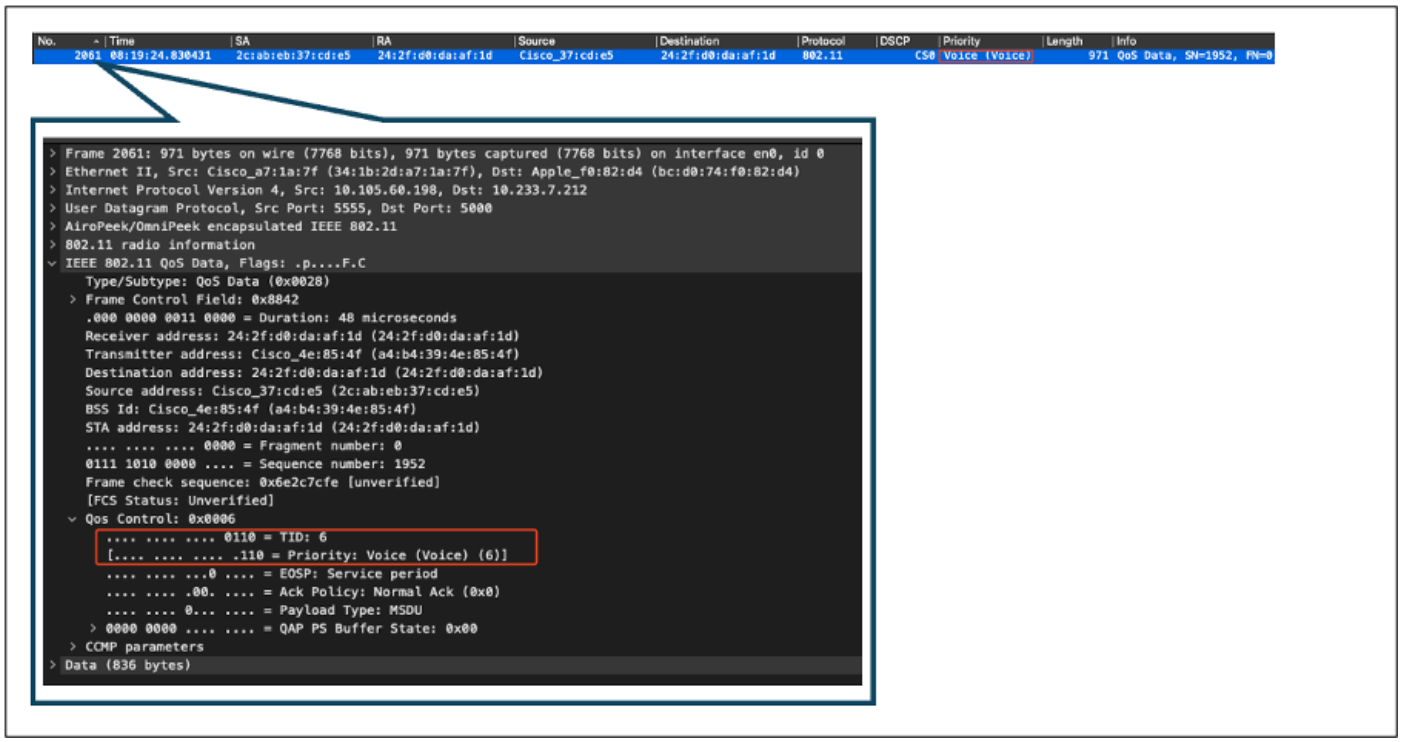


Captura de interfaz de switch de link ascendente AP

Una vez que el AP recibe el paquete, transmite el paquete por el aire. Para verificar el etiquetado

de prioridad de usuario (UP), se utiliza una captura OTA (Over-the-Air) tomada con un AP de sabueso.

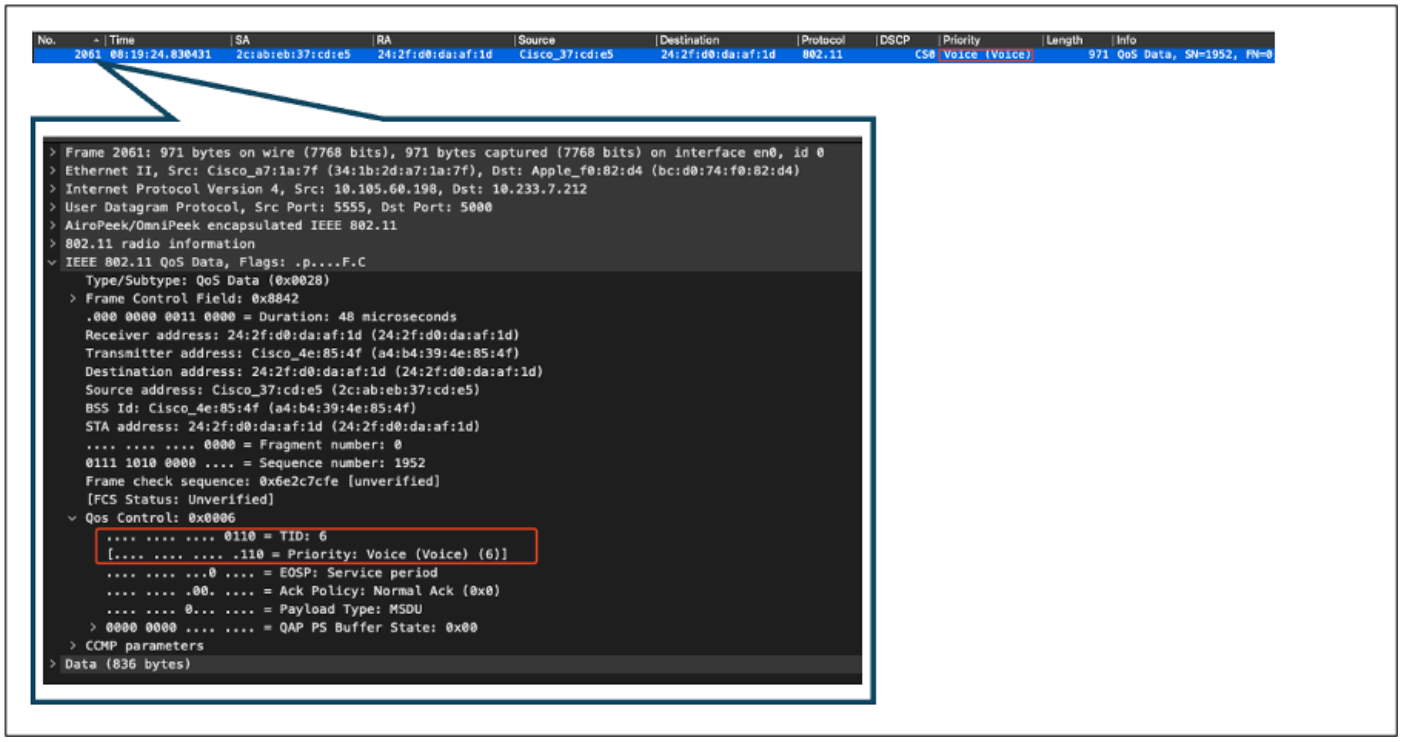
El AP ha reenviado la trama con un valor UP de 6. Esto confirma que el AP mapea correctamente el valor DSCP al valor UP 802.11 apropiado (6), que corresponde al tráfico de voz.



Captura de OTA del AP al cliente

En la etapa final, el paquete recibido por el PC inalámbrico. El PC inalámbrico recibe la trama con un valor DSCP de 46.

Esto indica que el marcado DSCP se conserva en toda la ruta de transmisión, desde el PC con cables hasta el PC inalámbrico. El valor DSCP coherente de 46 confirma que las políticas de QoS se aplican y se mantienen correctamente en la dirección descendente.



Captura de PC inalámbrico

Situación de prueba 2: validación de QoS ascendente

En este escenario de prueba, el objetivo es validar la configuración de QoS ascendente. La configuración implica un PC inalámbrico que envía paquetes UDP con DSCP 46 a un PC con cables. El WLC se configura con la política "Platinum QoS" del metal para las direcciones ascendentes y descendentes.

- Flujo de tráfico:

Fuente: PC inalámbrico

Destino: PC con cables

Tipo de tráfico: paquetes UDP con DSCP 46

- Configuración de política de QoS en WLC:

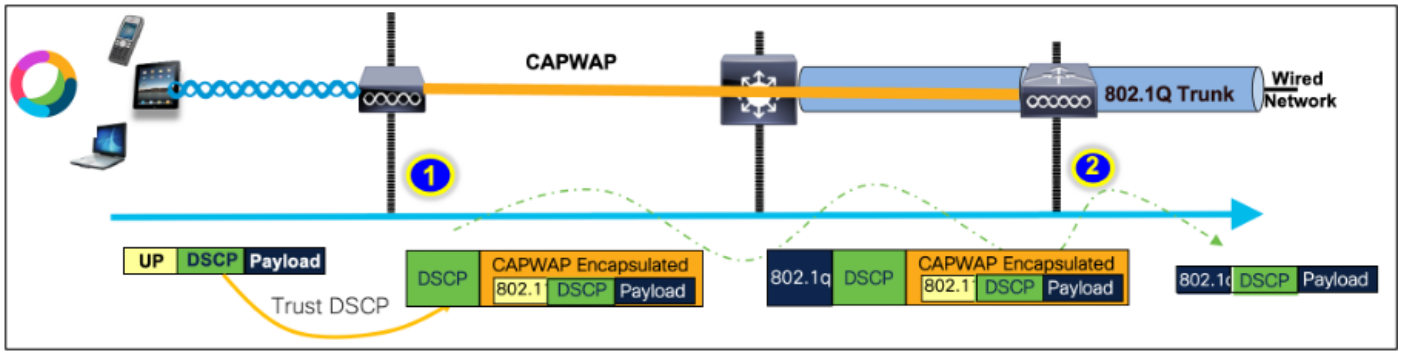
Perfil de QoS: QoS Platinum

Dirección: Ascendente y descendente

- Comandos de configuración de QoS de metal:

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

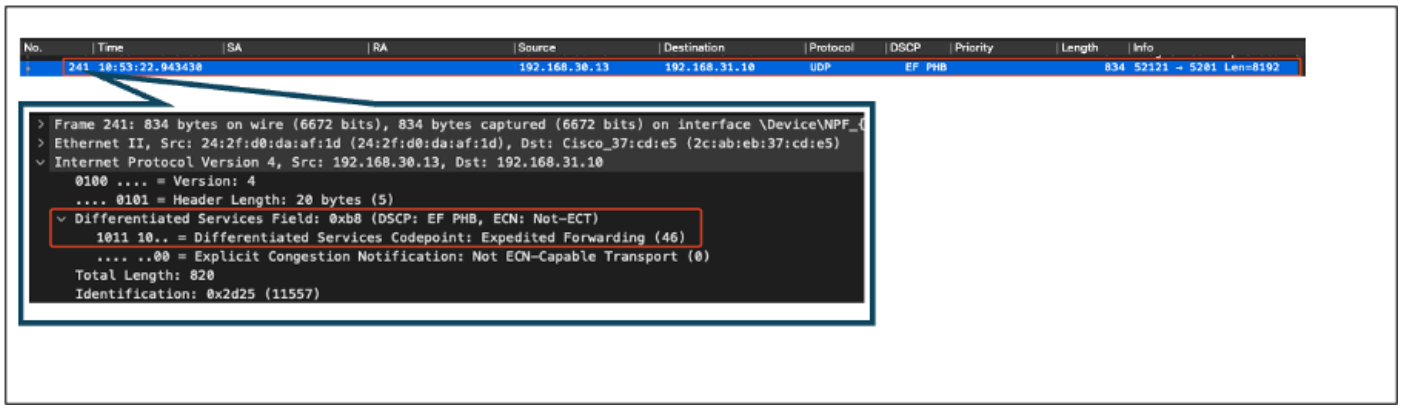
Conversión de DSCP y topología lógica en dirección ascendente:



Conversión de DSCP y topología lógica: flujo ascendente

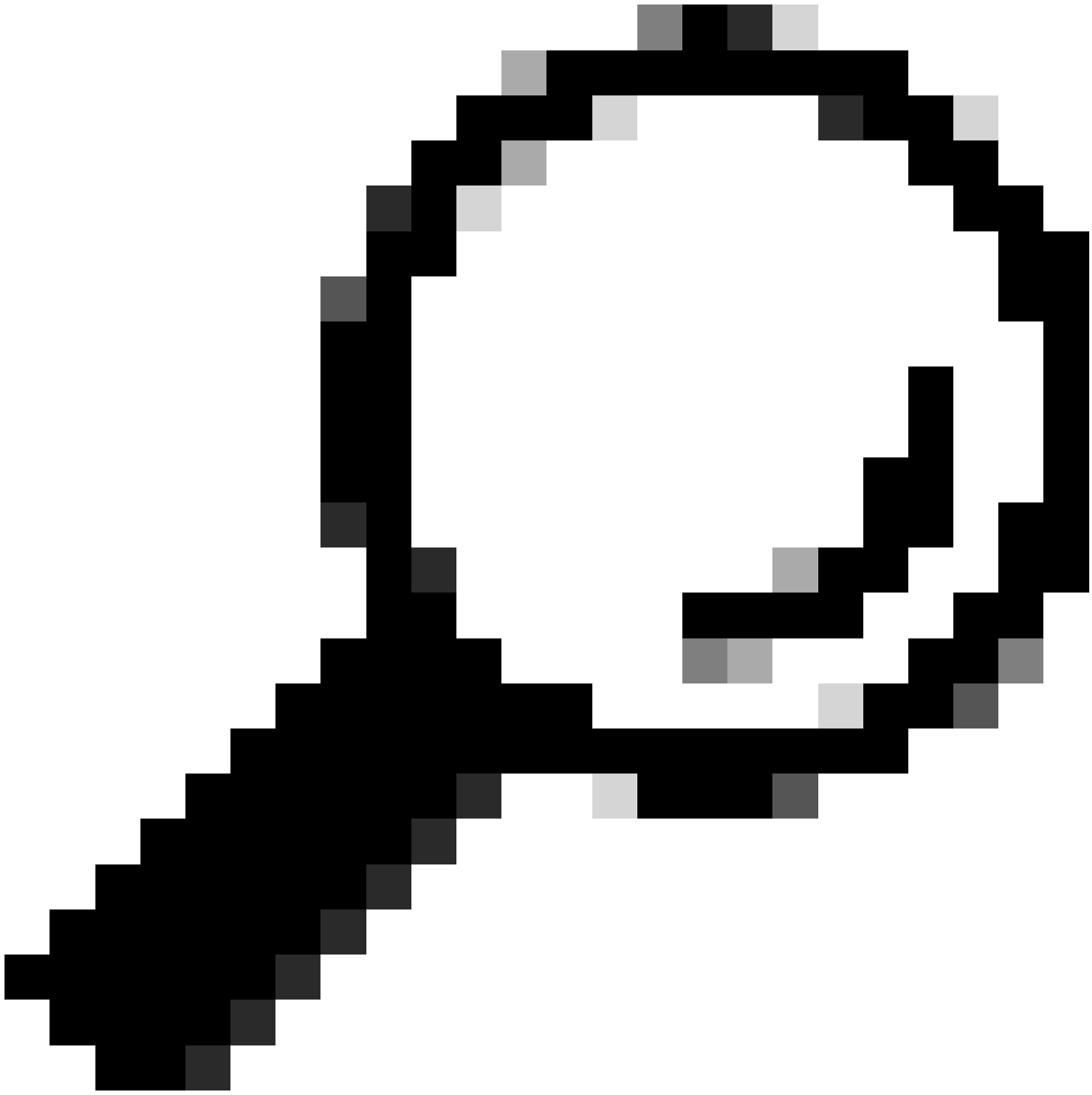
Paquetes enviados desde un PC inalámbrico a un PC con cables. Esta captura se realiza en el PC inalámbrico.

El PC inalámbrico envía paquetes UDP con DSCP 46.

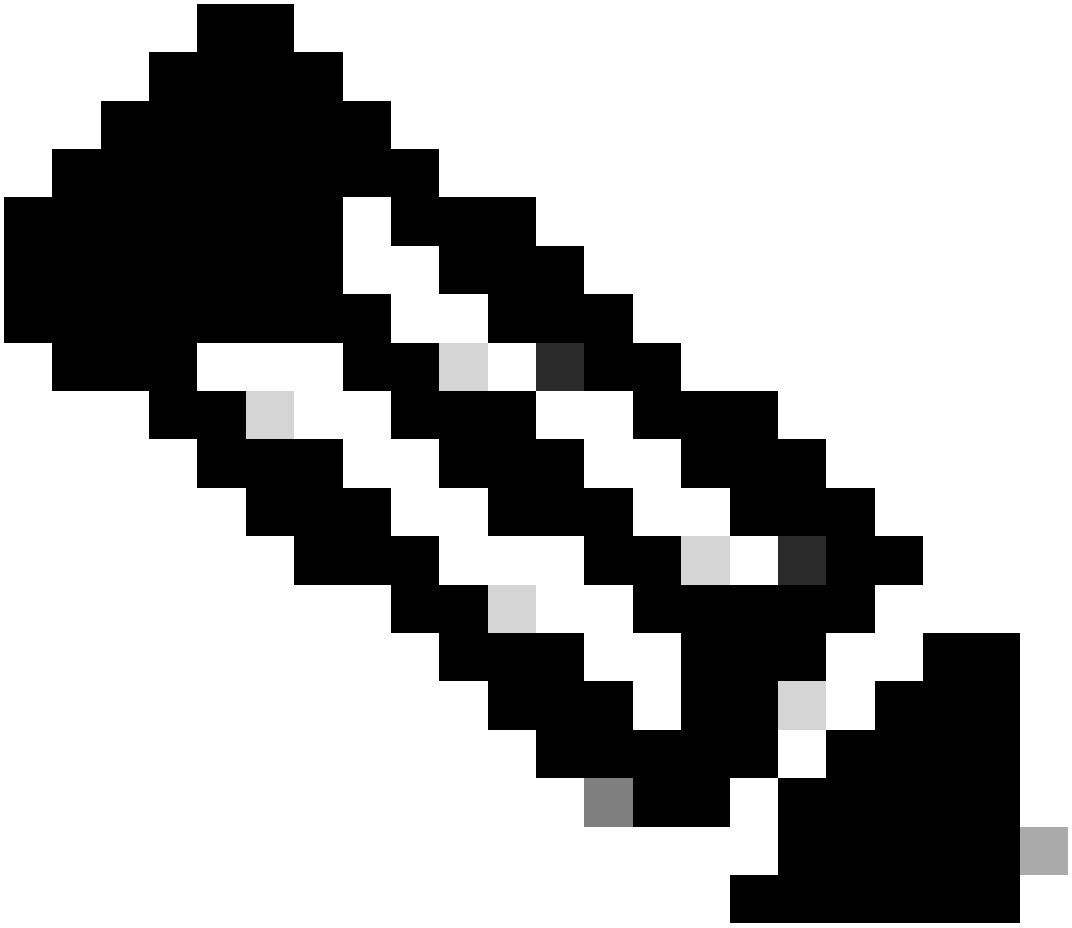


Captura de PC inalámbrico en dirección ascendente

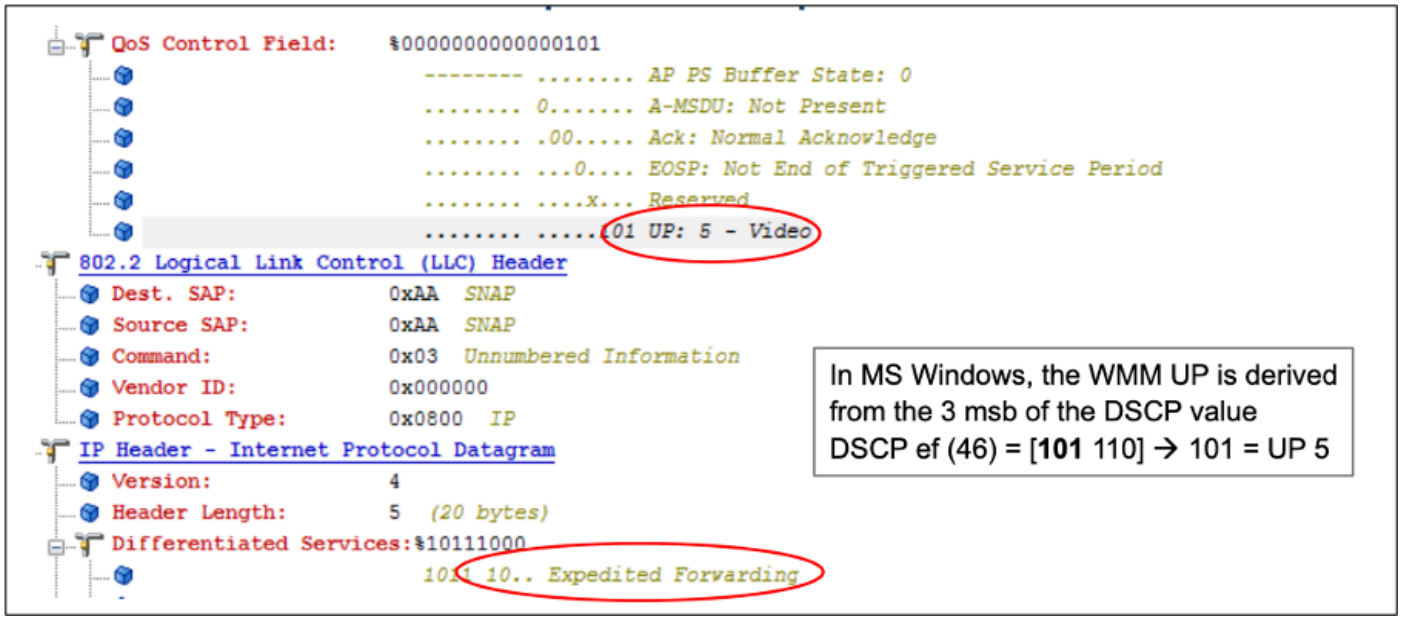
A continuación, veamos la captura de OTA del cliente al AP.



Sugerencia: al utilizar un PC inalámbrico de Windows para enviar paquetes con DSCP 46, Windows asigna DSCP 46 a un valor de prioridad de usuario (UP) de 5 (vídeo). Como resultado, la captura OTA muestra los paquetes como tráfico de vídeo (UP 5). Sin embargo, si descifra el paquete, el valor DSCP permanece en 46.



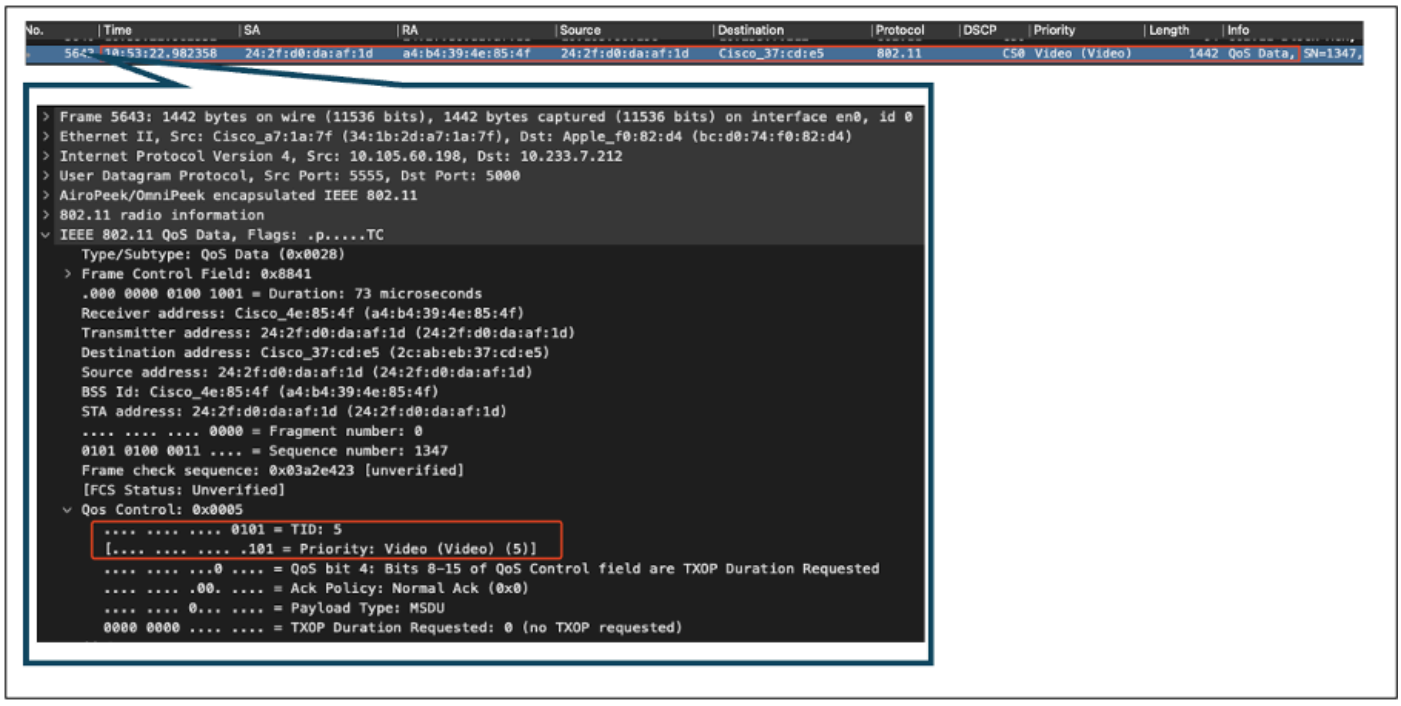
Nota: A partir de la versión 17.4, el comportamiento predeterminado para el WLC de Cisco 9800 es confiar en el valor DSCP en el perfil de unión AP. Esto asegura que el WLC conserve y confíe en el valor DSCP de 46, evitando cualquier problema relacionado con el comportamiento del mapeo DSCP a UP de Windows.



Asignación de Windows UP a DSCP

Se analiza la captura OTA (del inglés Encryption Over-the-Air, por sus siglas en inglés) tomada de la configuración del laboratorio para validar la configuración de QoS ascendente.

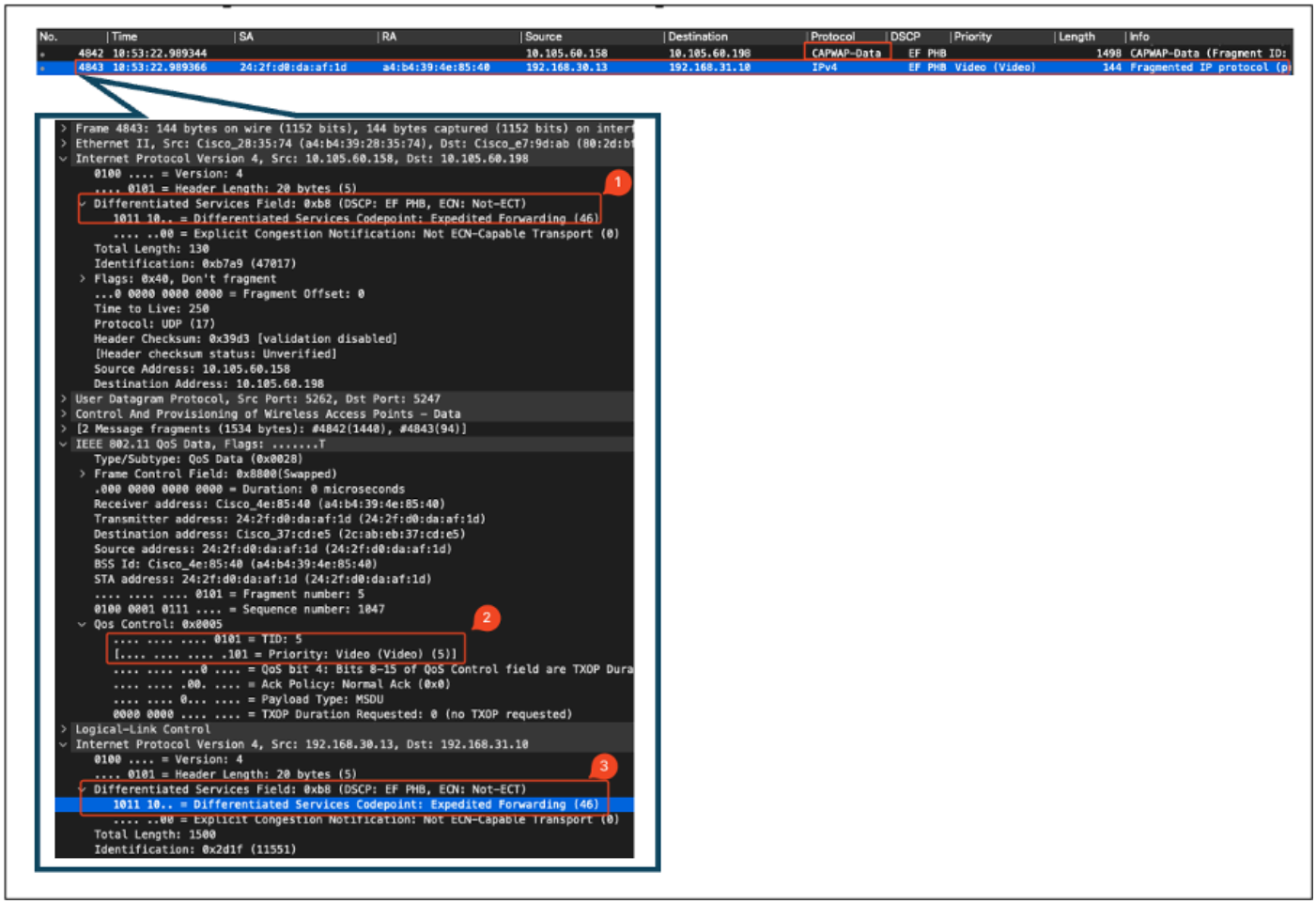
La captura OTA muestra los paquetes con un valor de prioridad de usuario (UP) de 5 (vídeo). Aunque la captura OTA muestra UP 5, el valor DSCP dentro del paquete cifrado permanece en 46.



LAB Setup OTA en dirección ascendente

A continuación, se analiza la captura de paquetes en el puerto de enlace ascendente del AP para garantizar que el valor DSCP se conserve a medida que el paquete se mueve del AP al WLC.

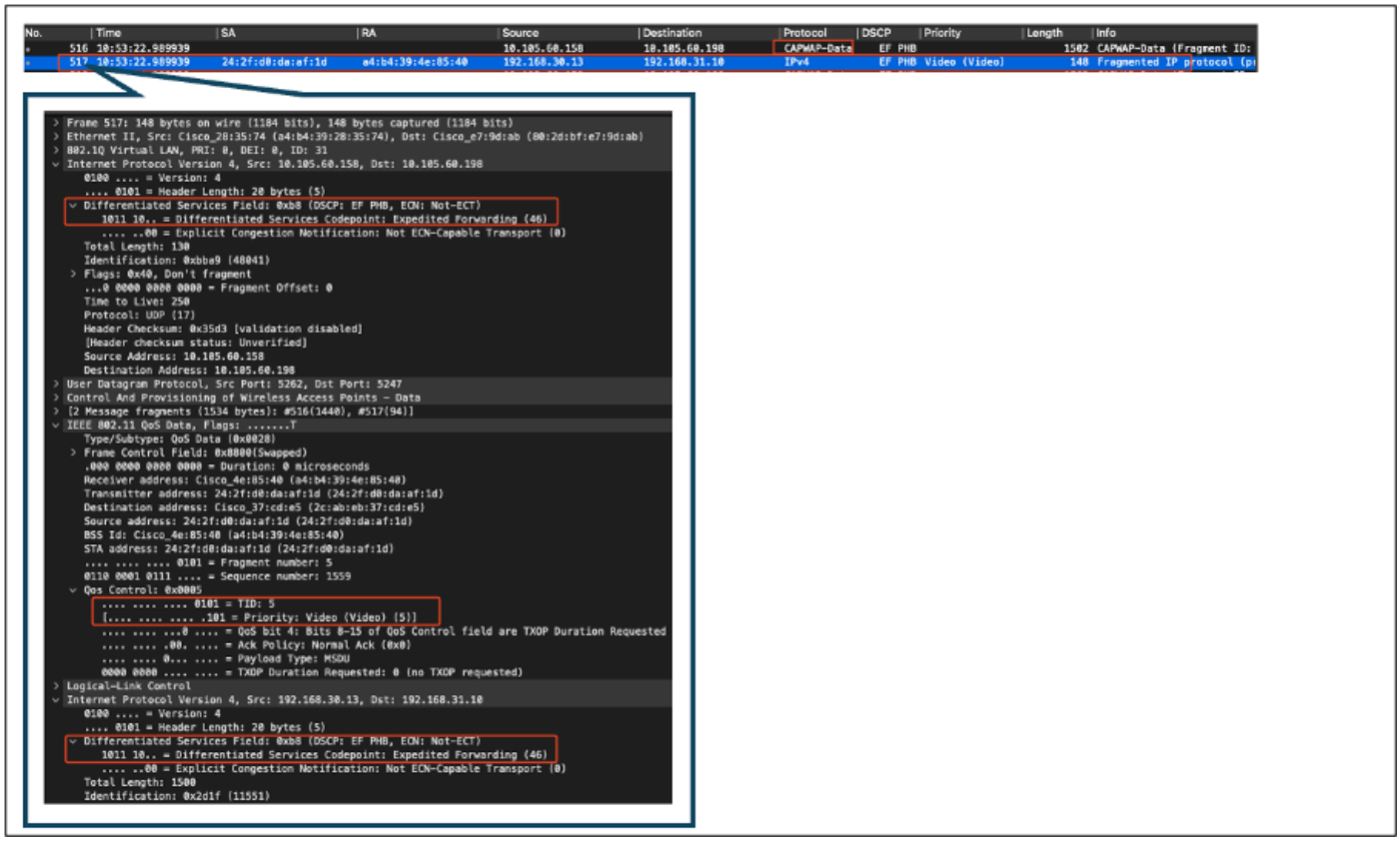
- El valor DSCP en la capa CAPWAP externa se mantiene en 46.
- Dentro del túnel CAPWAP, el valor DSCP también se mantiene en 46.



Captura de enlace ascendente de PA en dirección ascendente

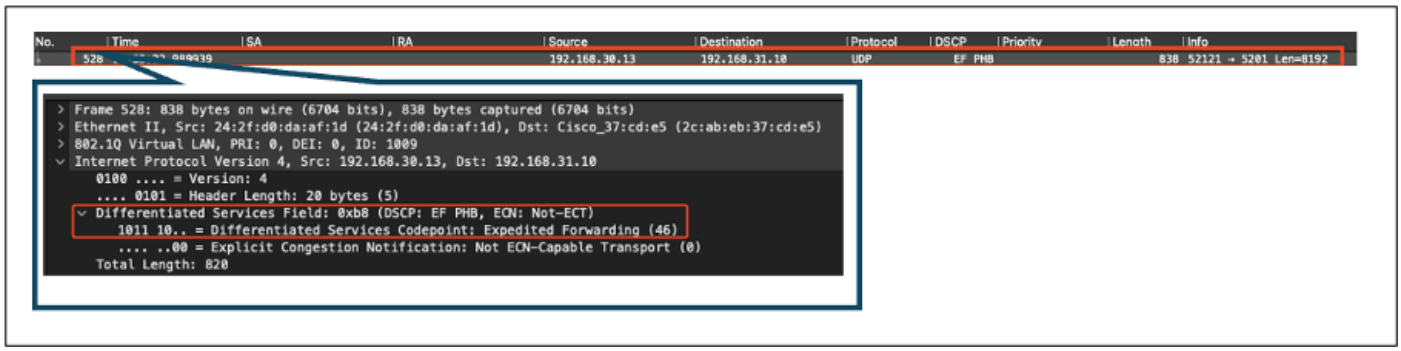
La captura se toma en el WLC cuando el paquete llega del switch.

- El paquete llega al WLC con el valor DSCP de 46 en la capa CAPWAP externa.
- Dentro del túnel CAPWAP, el valor DSCP se mantiene en 46.



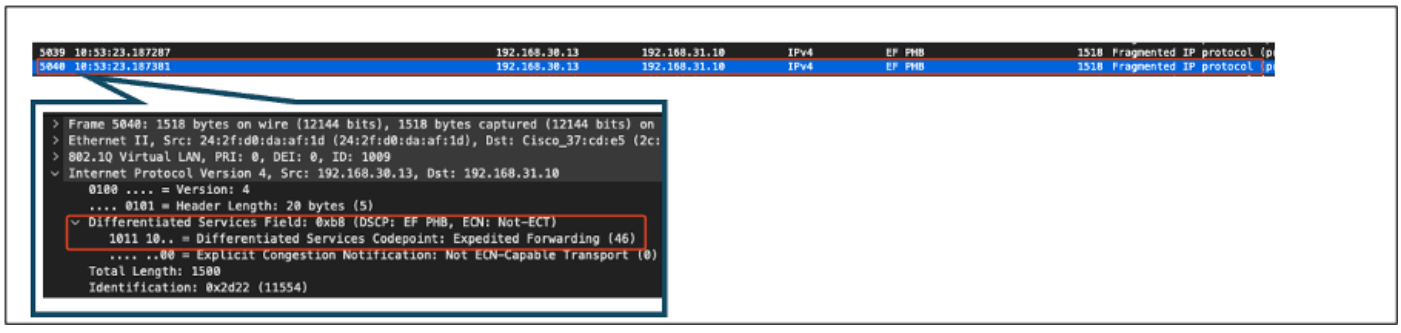
WLC EPC que muestra los paquetes que vienen de AP

Después de que el paquete toma un giro de horquilla en el WLC, se envía de nuevo al switch de uplink, destinado al PC cableado. El WLC reenvía el paquete con el valor DSCP de 46.



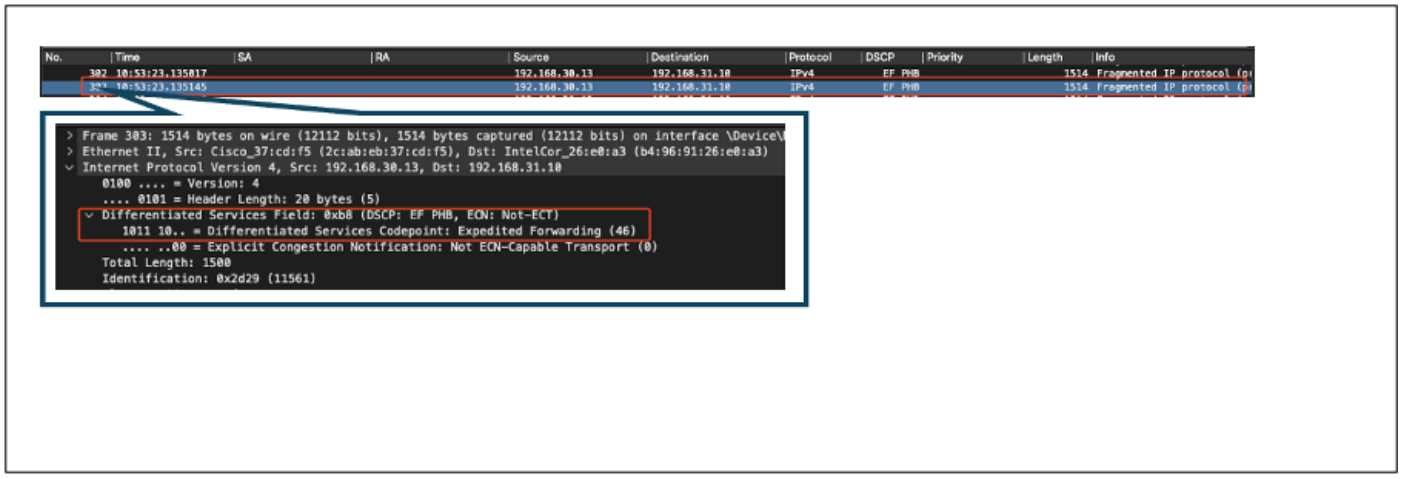
WLC EPC que muestra paquetes enviados a PC con cable

Finalmente, se analiza la captura de paquetes en el link ascendente de la PC cableada para garantizar que el valor DSCP se preserve a medida que el paquete llega del WLC.



Captura de switch de enlace ascendente de PC con cables en dirección ascendente

En la etapa final, se analiza el paquete recibido por la PC con cable para garantizar que el paquete llegue a la PC con cable con el valor DSCP de 46.



Captura de PC por cable: dirección ascendente

La prueba de QoS ascendente validó correctamente la configuración de QoS para el tráfico que fluye desde el PC inalámbrico al PC con cables. La preservación consistente del valor DSCP de 46 a lo largo de toda la trayectoria de transmisión confirma que las políticas de QoS se aplican y aplican correctamente.

Resolución de problemas

Las aplicaciones de voz, vídeo y otras aplicaciones en tiempo real son especialmente sensibles a los problemas de rendimiento de la red, y cualquier degradación en la calidad del servicio (QoS) puede tener efectos notables y perjudiciales. Cuando los paquetes de QoS se remarcan con valores DSCP más bajos, el impacto en la voz y el vídeo puede ser significativo.

Impacto en la voz:

- Mayor latencia: la comunicación de voz requiere baja latencia para garantizar que las conversaciones sean naturales y fluidas. Los valores DSCP más bajos pueden ocasionar que los paquetes de voz se demoren, lo que causa un retraso notable en las conversaciones.
- Fluctuación: la variabilidad en los tiempos de llegada de paquetes (fluctuación) puede interrumpir la entrega fluida de paquetes de voz. Esto puede producir audio entrecortado o confuso, lo que dificulta la comprensión del altavoz.
- Pérdida de paquetes: los paquetes de voz son altamente sensibles a la pérdida de paquetes. Incluso una pequeña cantidad de pérdida de paquetes puede dar lugar a la falta de palabras o sílabas, lo que conduce a una calidad de llamada deficiente y malentendidos.
- Eco y distorsión: el aumento de la latencia y la fluctuación puede provocar distorsiones de eco y de audio, lo que reduce aún más la calidad de la llamada de voz.

Impacto en el vídeo:

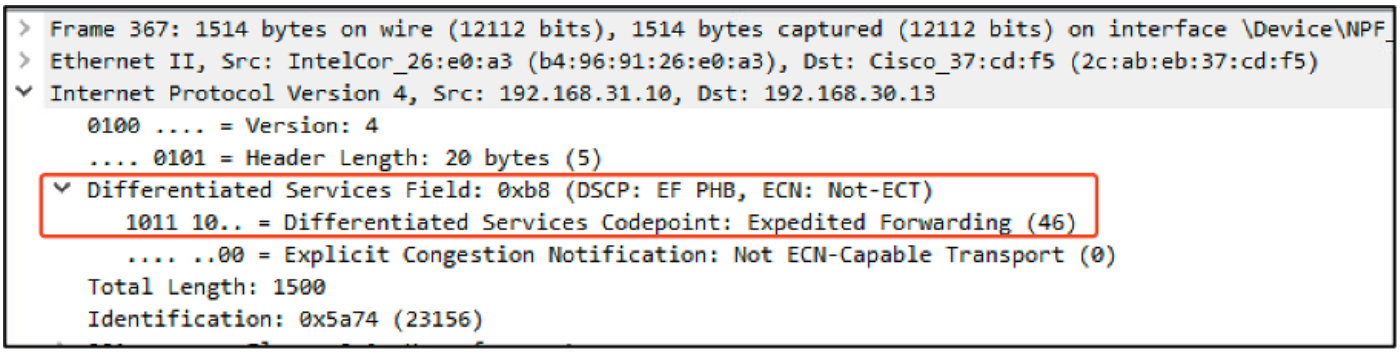
- Mayor latencia: la comunicación de vídeo requiere baja latencia para mantener la sincronización entre las transmisiones de audio y vídeo. El aumento de la latencia puede

causar retrasos, lo que dificulta las interacciones en tiempo real.
- Fluctuación: la fluctuación puede hacer que los fotogramas de vídeo lleguen fuera de servicio o a intervalos irregulares, lo que provoca una experiencia de vídeo irregular o entrecortada.
- Pérdida de paquetes: los paquetes perdidos pueden provocar la pérdida de tramas, lo que puede provocar que el vídeo se congele o muestre artefactos.
- Calidad de vídeo reducida: unos valores DSCP más bajos pueden reducir la asignación de ancho de banda para las transmisiones de vídeo, lo que se traduce en una resolución más baja y una calidad de vídeo inferior. Esto puede dificultar la visualización de detalles importantes en el vídeo.

Situación 1: El switch intermedio reescribe la marcación DSCP

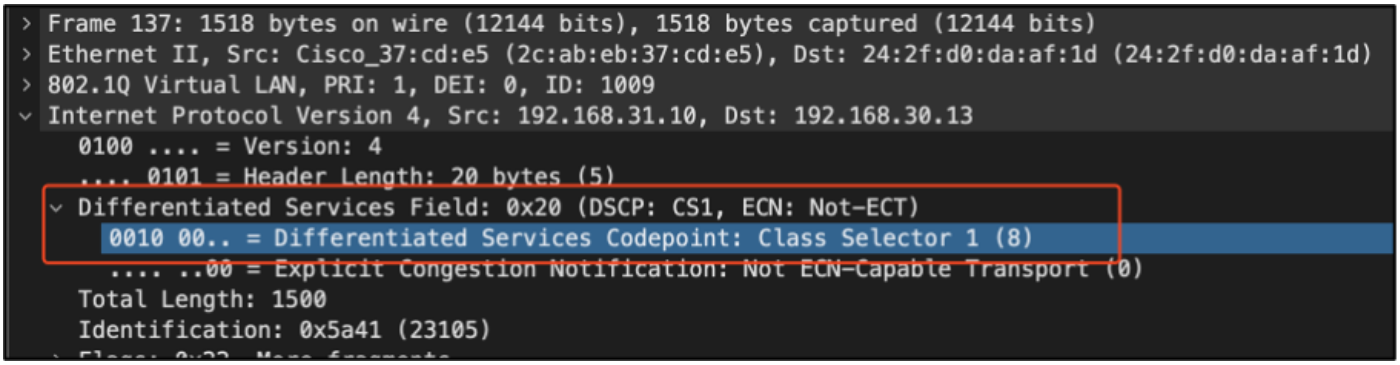
En este escenario de troubleshooting, se investiga el impacto de un switch intermedio que reescribe el marcado DSCP en el tráfico cuando llega al WLC. Para replicar esto, el switch está configurado para reescribir el marcado DSCP 46 en CS1 en la interfaz de enlace ascendente de PC con cable.

El paquete se envía desde el PC con cable con una etiqueta DSCP 46.



Paquete de envío de PC por cable con etiqueta DSCP 46

El paquete llega al WLC con un valor DSCP de CS1 (DSCP 8). El cambio de DSCP 46 a DSCP 8 reduce significativamente la prioridad del paquete.

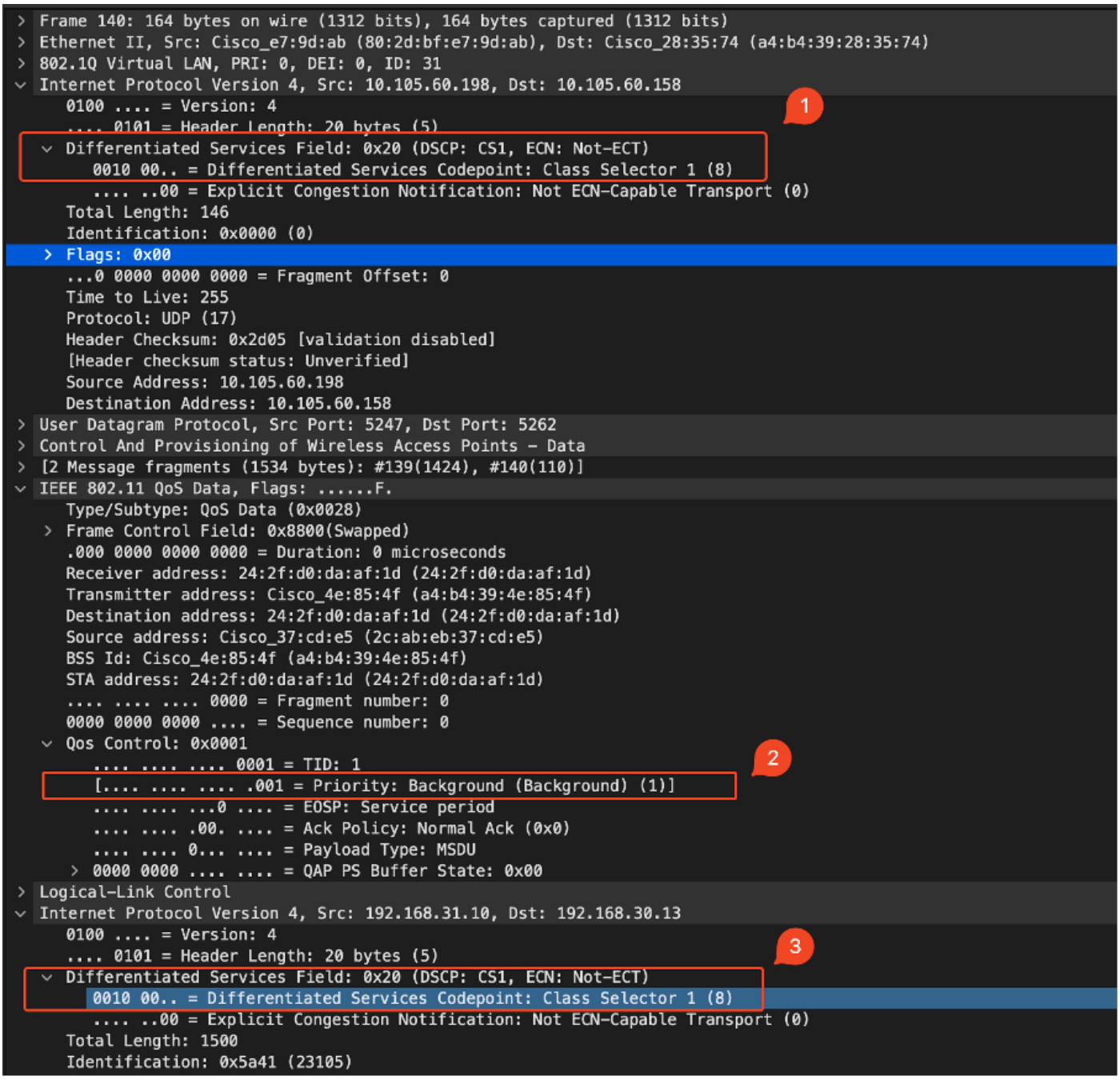


WLC EPC que muestra la marca CS1

En este paso, se analiza el paquete reenviado por el WLC al AP.

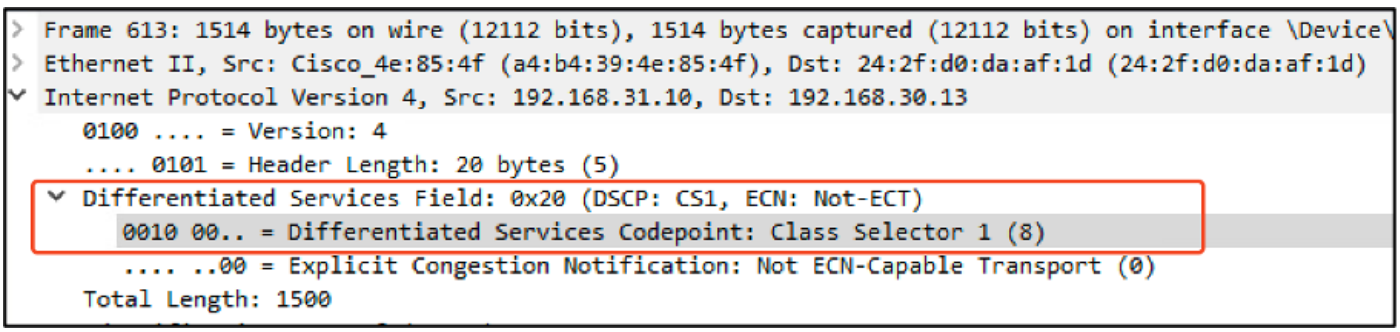
- El encabezado CAPWAP externo se etiqueta con CS1 (DSCP 8).

- El encabezado CAPWAP interno también se etiqueta con CS1 (DSCP 8).
- El valor de prioridad de usuario (UP) se establece en BK (fondo).



WLC EPC que muestra la etiqueta CS1 en el tráfico CAPWAP

El paquete llega al PC inalámbrico con un valor DSCP de CS1 (DSCP 8).



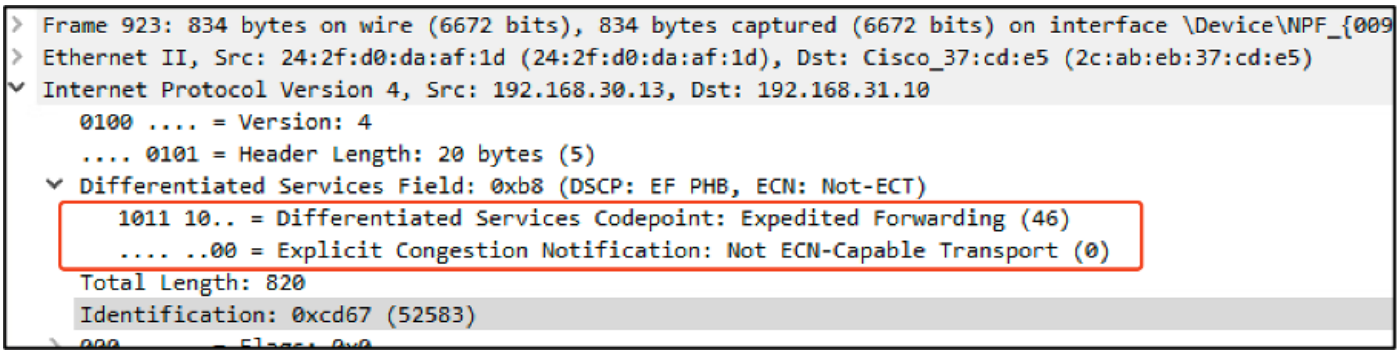
Captura inalámbrica de PC con marca CS1

Este escenario demuestra cómo un error de configuración en un switch intermedio puede interrumpir la configuración de QoS, lo que conduce a un rendimiento degradado para el tráfico de alta prioridad. Los paquetes de voz, inicialmente marcados como de alta prioridad, se trataron como tráfico de menor prioridad debido a la reescritura DSCP. Este escenario subraya la importancia de garantizar que los dispositivos de red intermedios preserven correctamente las marcas de QoS para mantener la calidad de servicio deseada para el tráfico de alta prioridad.

Escenario 2: El switch de link AP reescribe la marcación DSCP

En este escenario, se investiga el impacto de un switch intermedio conectado al AP que reescribe el marcado DSCP en el tráfico.

- El switch conectado al AP está configurado para reescribir el marcado DSCP 46 a un valor CS1 diferente en la interfaz de link ascendente del AP.
- El paquete se envía desde el PC con cable con una etiqueta DSCP de 46. Esto confirma que el tráfico está correctamente marcado con DSCP 46 en el origen.

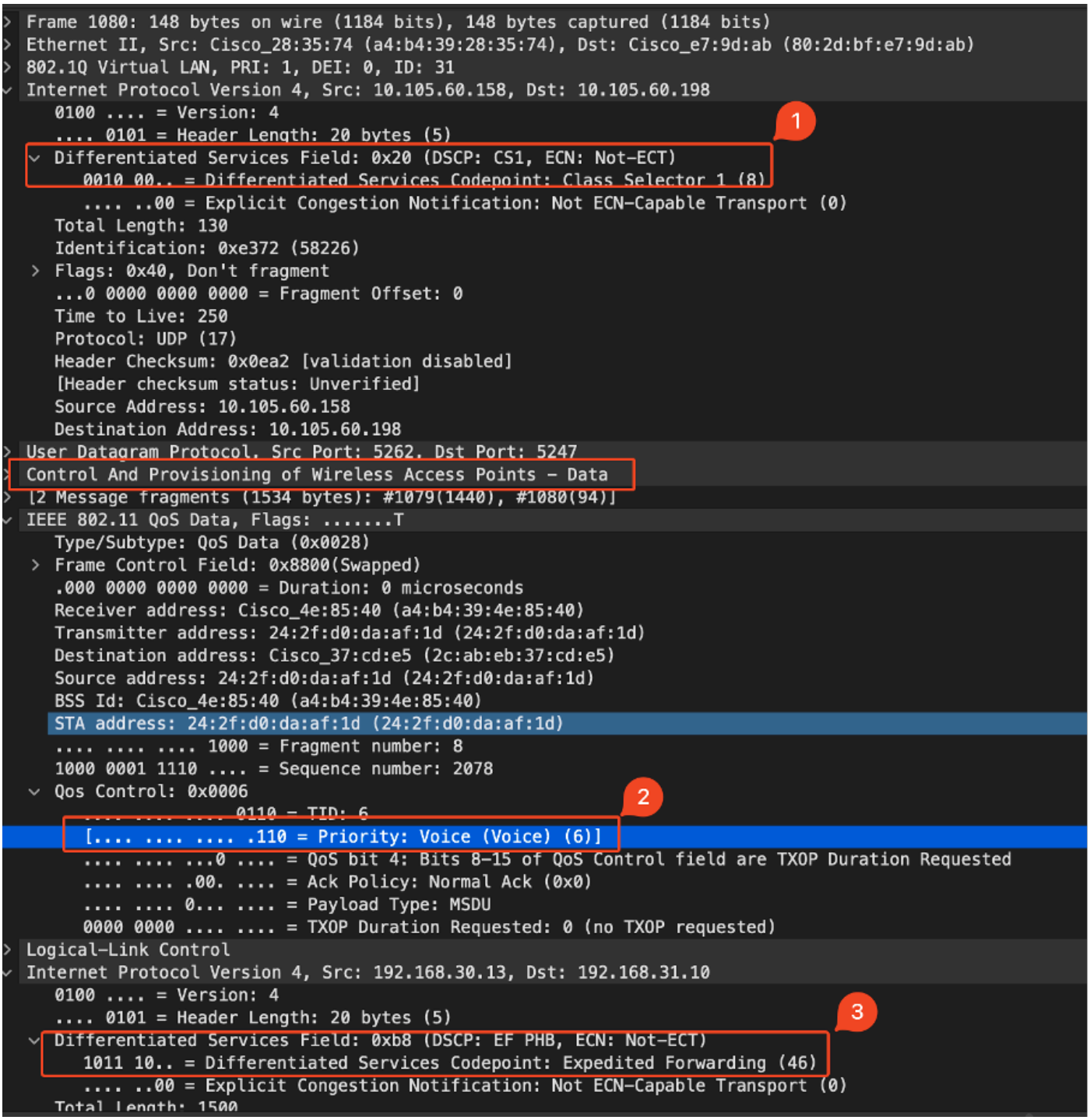


Captura inalámbrica de PC con DSCP 46

La captura se toma en el WLC cuando el paquete llega del switch.

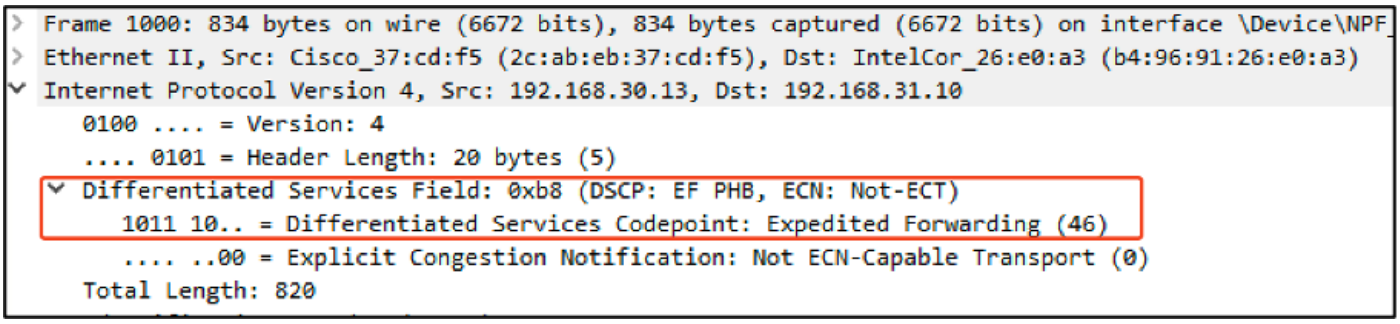
El paquete llega al WLC con el valor DSCP del encabezado CAPWAP externo de CS1 (DSCP) y el valor DSCP interno de 46. Esto sucede porque el switch intermedio no puede ver el tráfico encapsulado dentro del túnel CAPWAP.

El WLC confía en la etiqueta DSCP dentro del túnel CAPWAP y reenvía el tráfico al PC cableado con la etiqueta DSCP interna de 46.



WLC EPC que muestra los valores CAPWAP DSCP

El paquete llega al PC con cable con un valor DSCP de 46. Confirma que el WLC reenvía correctamente el paquete con el valor DSCP original de 46, preservando la marcación de alta prioridad.



PC con cables recibió el paquete con DSCP 46

Aunque el WLC reenvió el tráfico con una etiqueta DSCP de 46, es importante entender que el tráfico del AP al WLC fue tratado como prioridad baja debido a que la etiqueta DSCP externa se reescribe en CS1 (DSCP 8).

Puede haber múltiples switches entre el AP y el WLC, y si el tráfico se da prioridad baja, puede llegar tarde al WLC. Esto puede aumentar la latencia, la fluctuación y la pérdida potencial de paquetes, lo que puede degradar la calidad del servicio para el tráfico de alta prioridad como la voz.

Sugerencia de Troubleshooting

1. Verificar marca DSCP inicial: Capture paquetes en el origen (por ejemplo, PC cableado) para asegurarse de que el tráfico esté correctamente marcado con el valor DSCP deseado.
2. Verifique las Configuraciones de Dispositivos Intermedios: Revise la configuración de todos los switches y routers intermedios para asegurarse de que no estén reescribiendo inadvertidamente los valores DSCP.
3. Capturar tráfico en puntos clave:
    1. Antes y después del interruptor intermedio.
    2. En el WLC.
    3. En el destino (por ejemplo, un PC inalámbrico).
4. Simular escenarios de tráfico: utilice generadores de tráfico o herramientas de simulación de red para crear diferentes tipos de tráfico y observar cómo la red inalámbrica gestiona la QoS.
5. Consulte el documento de prácticas recomendadas de 9800: Revise la documentación de prácticas recomendadas de 9800 sobre la configuración de QoS y las marcas DSCP.

Verificación de configuración

<#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
```

Conclusión

Mantener una configuración de QoS uniforme en toda la red es fundamental para garantizar que el tráfico de alta prioridad, como el de voz y vídeo, reciba el nivel de servicio y rendimiento adecuados. Es esencial validar las configuraciones de QoS de forma regular para garantizar que todos los dispositivos de red cumplen las políticas de QoS esperadas. Esta validación ayuda a identificar y rectificar cualquier configuración incorrecta o desviación que pueda poner en peligro el rendimiento de la red.

Referencias

- Descripción y resolución de problemas de los controladores inalámbricos Cisco Catalyst serie 9800
- Prácticas recomendadas de configuración de Cisco Catalyst serie 9800
- Guía de configuración del software del controlador inalámbrico Cisco Catalyst serie 9800, Cisco IOS® XE Dublín 17.12.x
- Guía de solución de problemas de voz sobre LAN inalámbrica (VoWLAN)
- Habilitar el etiquetado de QoS DSCP en equipos con Windows

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).