Configuration, validation et dépannage de la QoS sans fil sur le WLC 9800

Table des matières

- Introduction
- Composants utilisés
- Informations générales
- Configuration
  - Cibles de stratégie QoS
  - QoS automatique
  - Configuration CLI Auto QoS
  - CLI QoS modulaire
  - Configuration CLI MQS
  - QoS métal
  - Configuration CLI QoS métallique
- Validation de la QoS de bout en bout avec capture de paquets
  - Diagramme du réseau
  - Composants des travaux pratiques et points de capture de paquets
  - Scénario de test 1 : validation QoS en aval
  - Scénario de test 2 : validation QoS en amont
- Dépannage
  - Scénario 1 : le commutateur intermédiaire réécrit le marquage DSCP
  - Scénario 2 : le commutateur de liaison AP réécrit le marquage DSCP
- Conseil de dépannage
- Vérification de la configuration
- Conclusion
- Références

Introduction

Ce document décrit les façons de configurer, valider et dépanner la qualité de service (QoS) sans fil sur le contrôleur LAN sans fil (WLC) 9800.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC : C980-40-K9 exécutant 17.12.03
- Point d'accès : C9120-AX-D

- Commutateur : C9300-48P exécutant 17.03.05
- Client filaire et sans fil : Windows 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

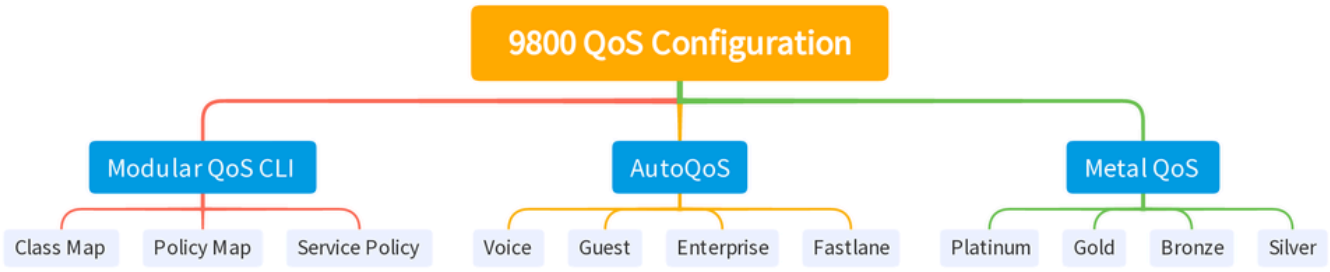
La QoS sans fil est essentielle pour garantir que les applications critiques reçoivent la bande passante et la faible latence nécessaires à des performances optimales. Ce document fournit un guide complet de configuration, de validation et de dépannage de la qualité de service sur les réseaux sans fil Cisco.

Cet article part du principe que les lecteurs ont une compréhension fondamentale des principes de QoS filaire et sans fil. Il est également attendu que les lecteurs soient compétents dans la configuration et la gestion des WLC et des AP Cisco.

Configuration

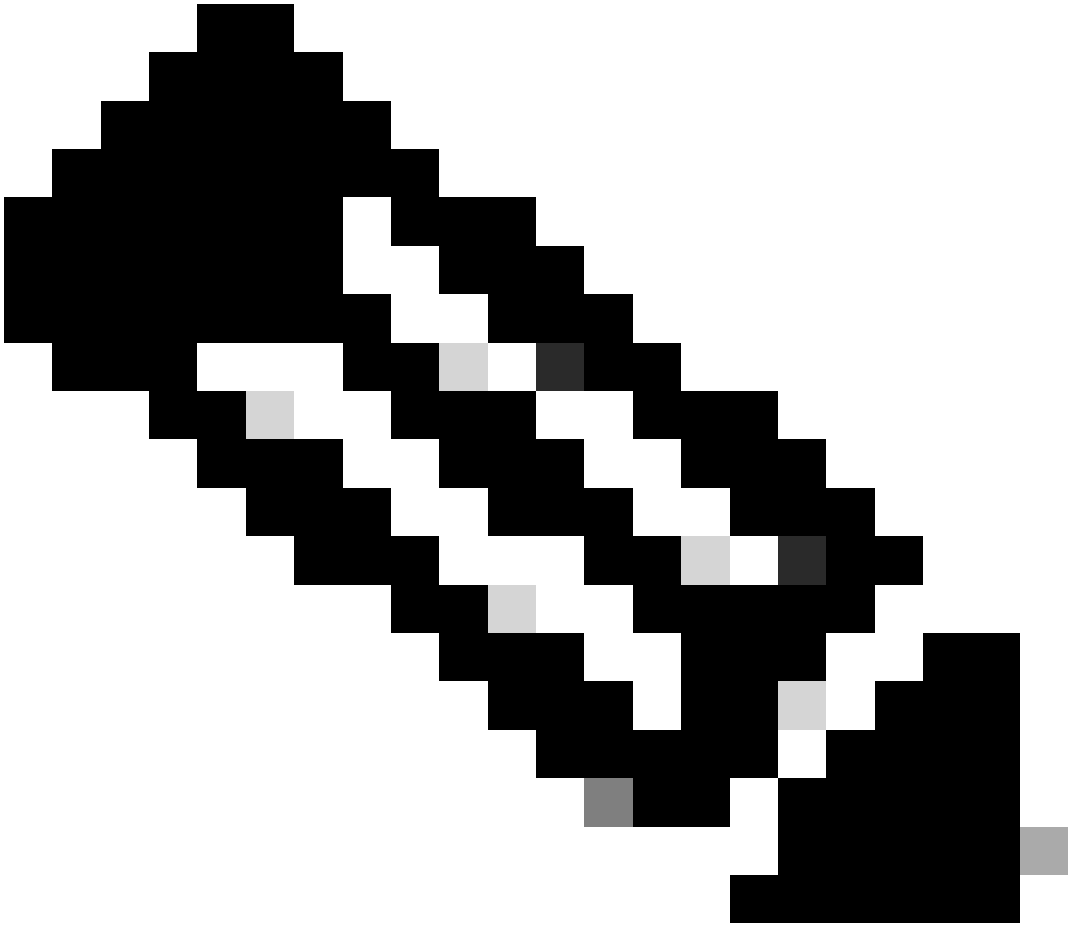
Cette section traite de la configuration de la QoS sur les contrôleurs sans fil 9800. En exploitant ces configurations, vous pouvez vous assurer que les applications critiques reçoivent la bande passante nécessaire et une faible latence, optimisant ainsi les performances globales du réseau.

Vous pouvez diviser la configuration QoS du WLC 9800 en trois grandes catégories.



Résumé de la configuration QOS du WLC 9800

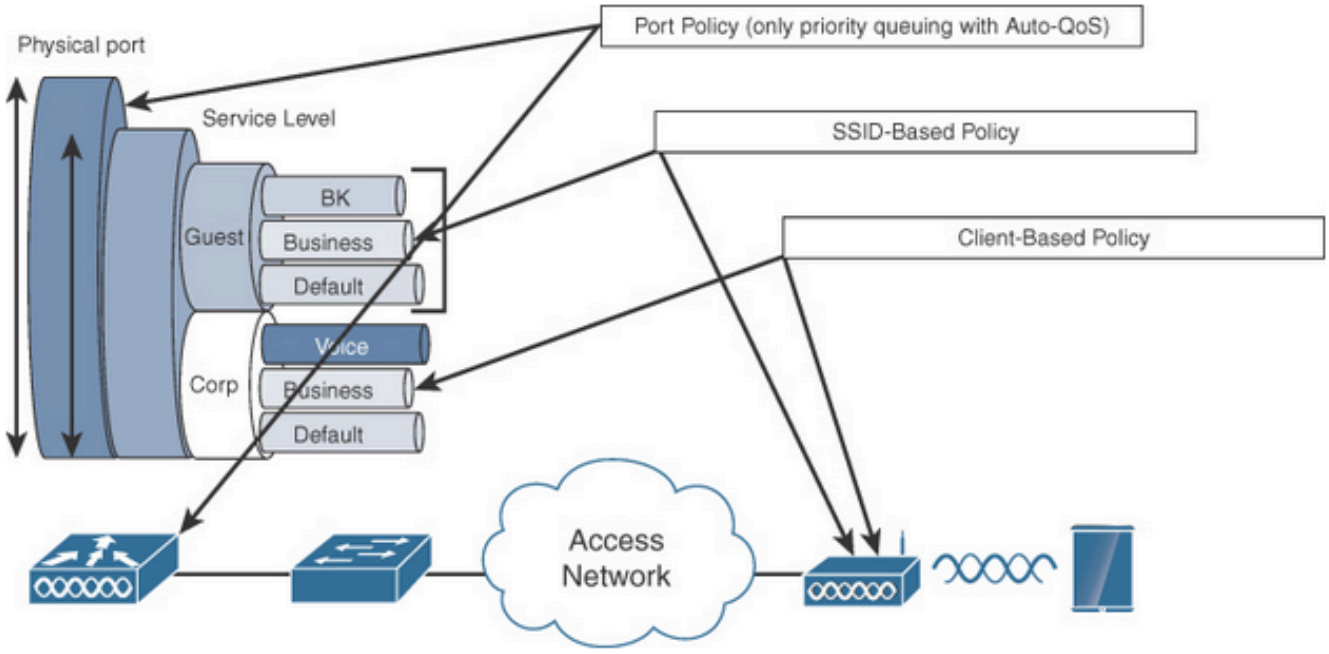
Ce document passe en revue chaque section une par une dans les sections suivantes.



Remarque : cet article se concentre sur le point d'accès en mode local. Le point d'accès en mode Flexconnect n'est pas abordé.

Cibles de stratégie QoS

Une cible de stratégie est la construction de configuration dans laquelle une stratégie QoS peut être appliquée. La mise en oeuvre de la QoS sur le Catalyst 9800 est modulaire et flexible. L'utilisateur peut décider de configurer les stratégies sur trois cibles différentes : le SSID, le client et les niveaux de port.



Cibles de stratégie QoS

La stratégie SSID est applicable par point d'accès et par SSID. Vous pouvez configurer des stratégies de contrôle et de marquage sur le SSID.

Les stratégies client s'appliquent dans le sens de l'entrée et de la sortie. Vous pouvez configurer des stratégies de contrôle et de marquage sur les clients. Le remplacement AAA est également pris en charge.

Les stratégies QoS basées sur les ports peuvent être appliquées à un port physique ou logique.

QoS automatique

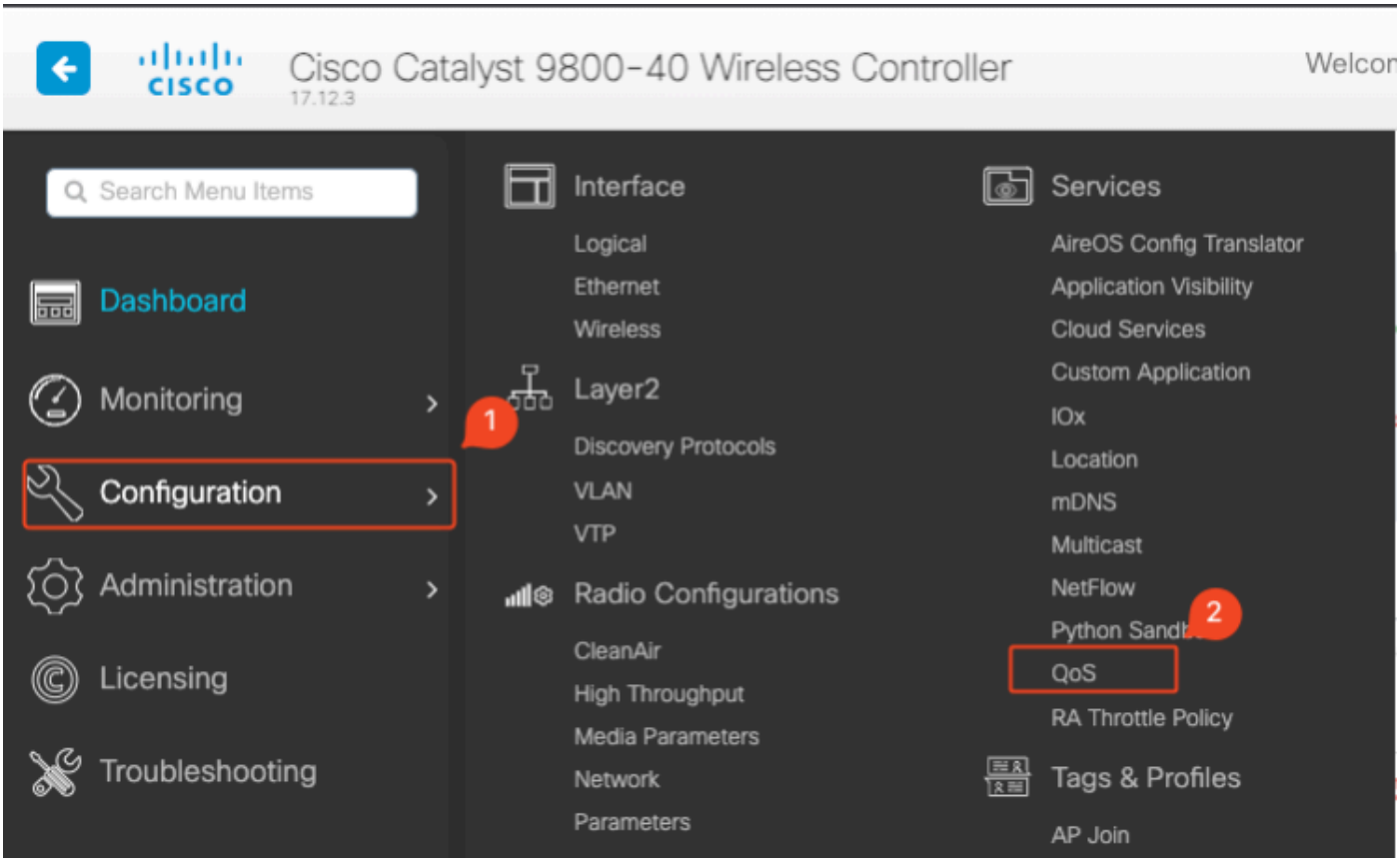
Wireless Auto QoS automatise le déploiement des fonctions QoS sans fil. Il dispose d'un ensemble de profils prédéfinis qui peuvent être modifiés par l'administrateur pour hiérarchiser différents flux de trafic. Auto-QoS fait correspondre le trafic et attribue chaque paquet correspondant à des groupes QoS. Cela permet au mappage de stratégie de sortie de placer des groupes QoS spécifiques dans des files d'attente spécifiques, y compris la file d'attente prioritaire.

Mode	Entrée client	Sortie client	BSSID entrant	Sortie BSSID	Entrée de port	Sortie de port	Radio
Voix	S/O	S/O	platiné	platine	S/O	AutoQos-4.0-wlan-Port-Output-Policy	ACM activé
Invité	S/O	S/O	AutoQos-4.0-wlan-	AutoQos-4.0-	S/O	AutoQos-4.0-	

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

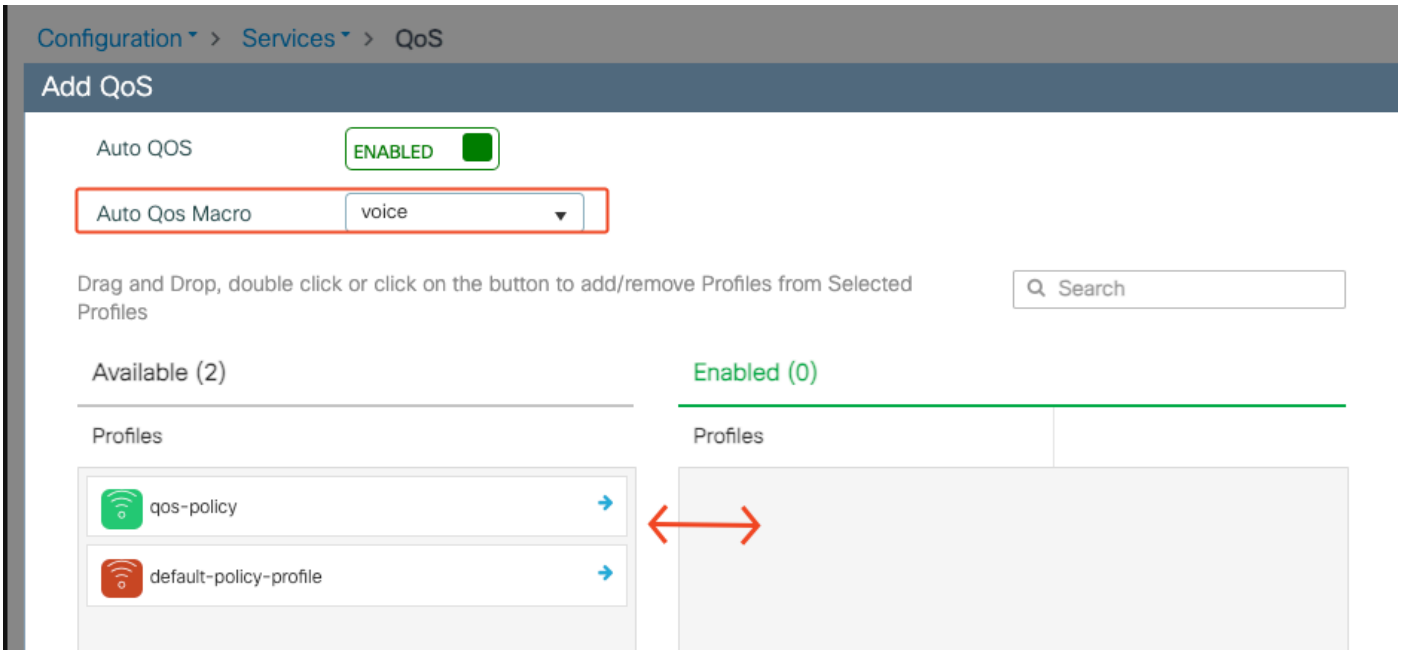
Ce tableau décrit les modifications de configuration qui se produisent lorsqu'un profil QoS automatique est appliqué.

Pour configurer Auto QoS, accédez à Configuration > QoS



Workflow QoS

Cliquez sur Add et définissez Auto QoS sur enabled. Sélectionnez la macro Auto QoS appropriée dans la liste. Dans cet exemple, la macro Voice est utilisée pour donner la priorité au trafic vocal.



Mappage vocal AutoQoS

Une fois la macro activée, sélectionnez la stratégie qui doit être attachée à la stratégie.

Configuration CLI Auto QoS

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

Maintenant qu'Auto QoS est activé, vous pouvez voir les modifications qui se sont produites. Cette section répertorie les modifications apportées à la configuration de la voix.

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

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

CLI QoS modulaire

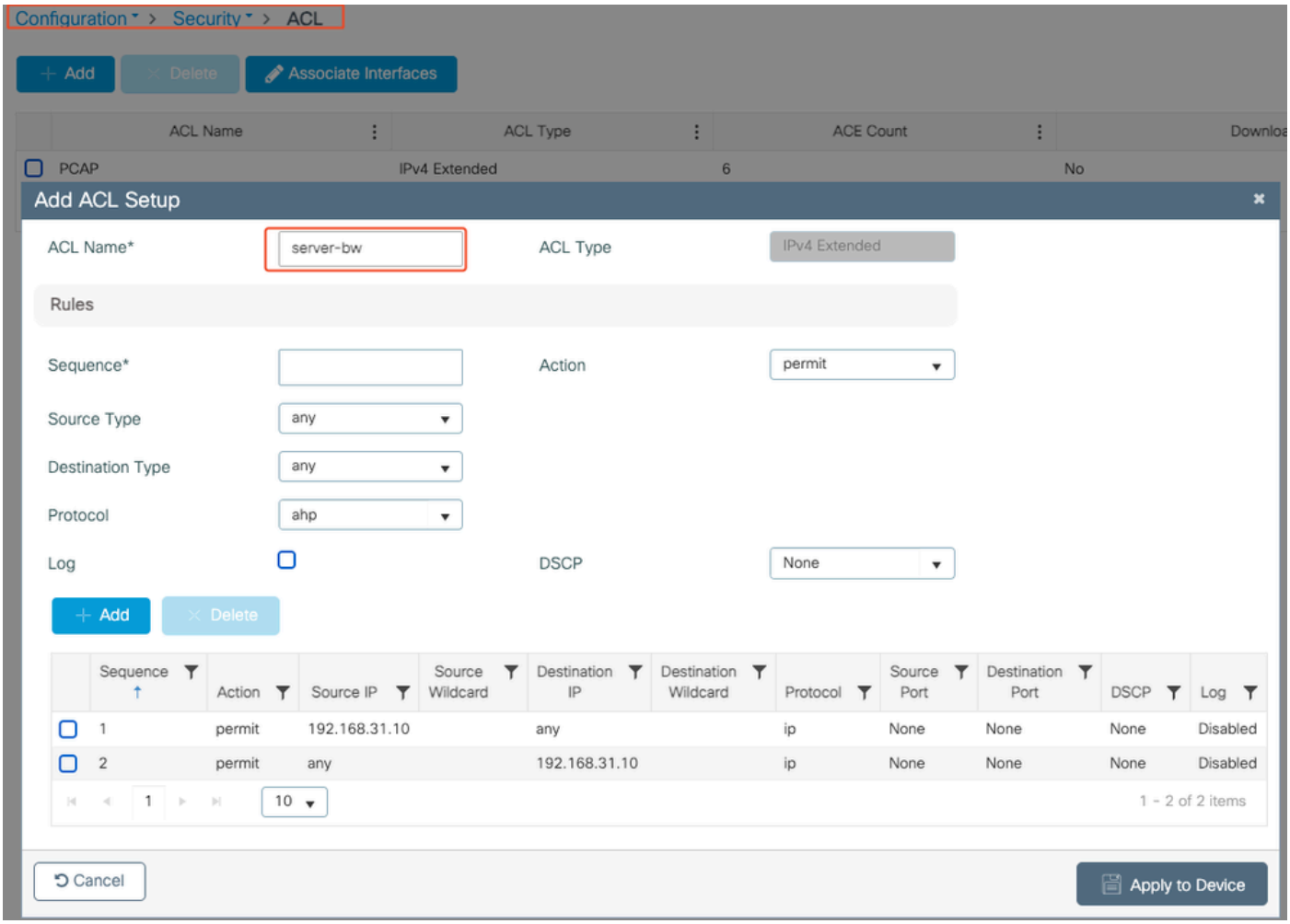
Le MQC vous permet de définir une classe de trafic, de créer une stratégie de trafic (carte de stratégie) et d'associer la stratégie de trafic à une interface. La stratégie de trafic contient la fonctionnalité QoS qui s'applique à la classe de trafic.

Workflow CLI MQS

Cet exemple montre comment utiliser des listes de contrôle d'accès (ACL) pour classer le trafic et appliquer des restrictions de bande passante.

Créez une liste de contrôle d’accès pour identifier et classer le trafic spécifique que vous souhaitez gérer. Pour ce faire, vous pouvez définir des règles qui correspondent au trafic en fonction de critères tels que les adresses IP, les protocoles ou les ports.

Accédez à Configuration > Security > ACL et ajoutez l'ACL.

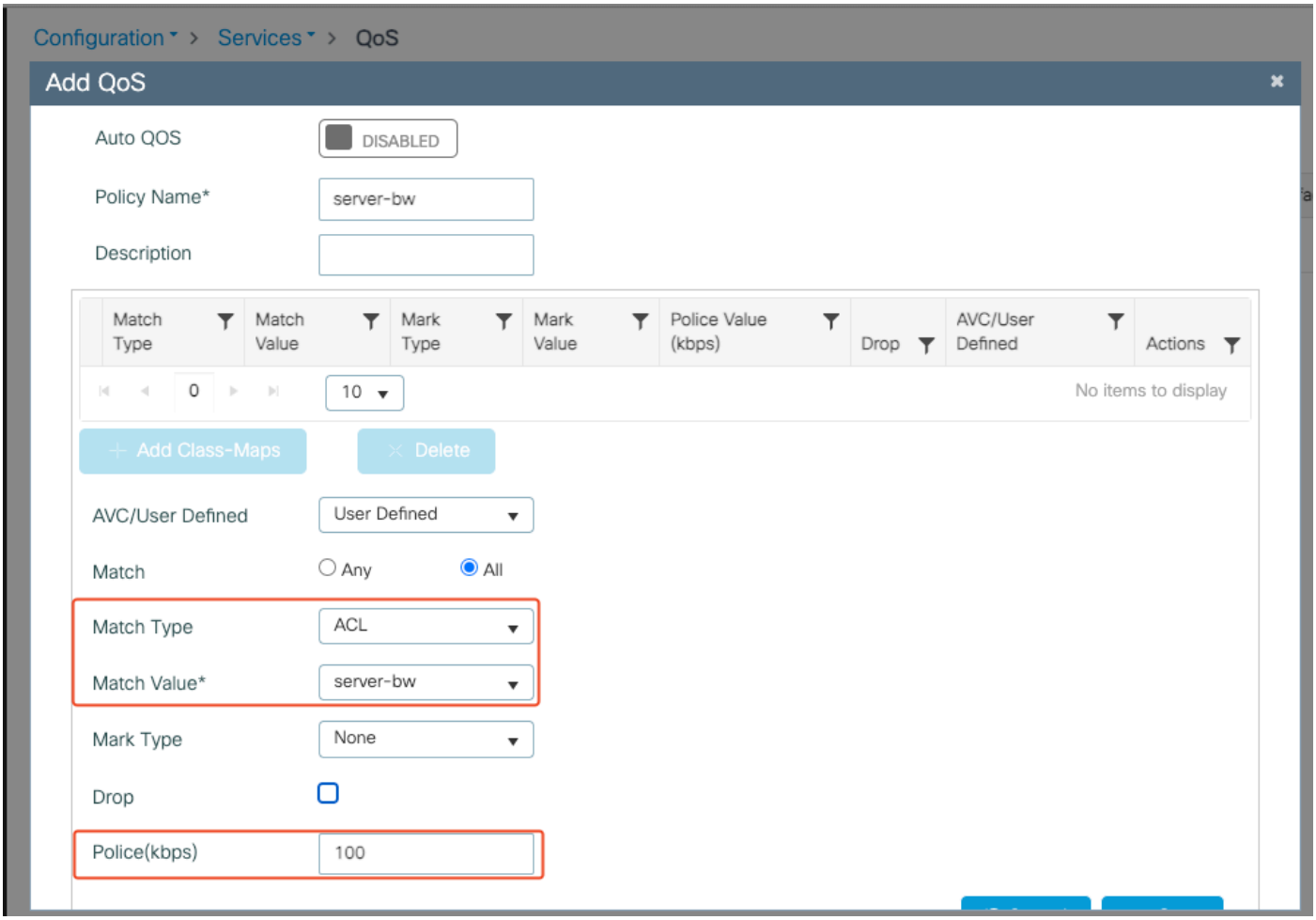


Configuration ACL

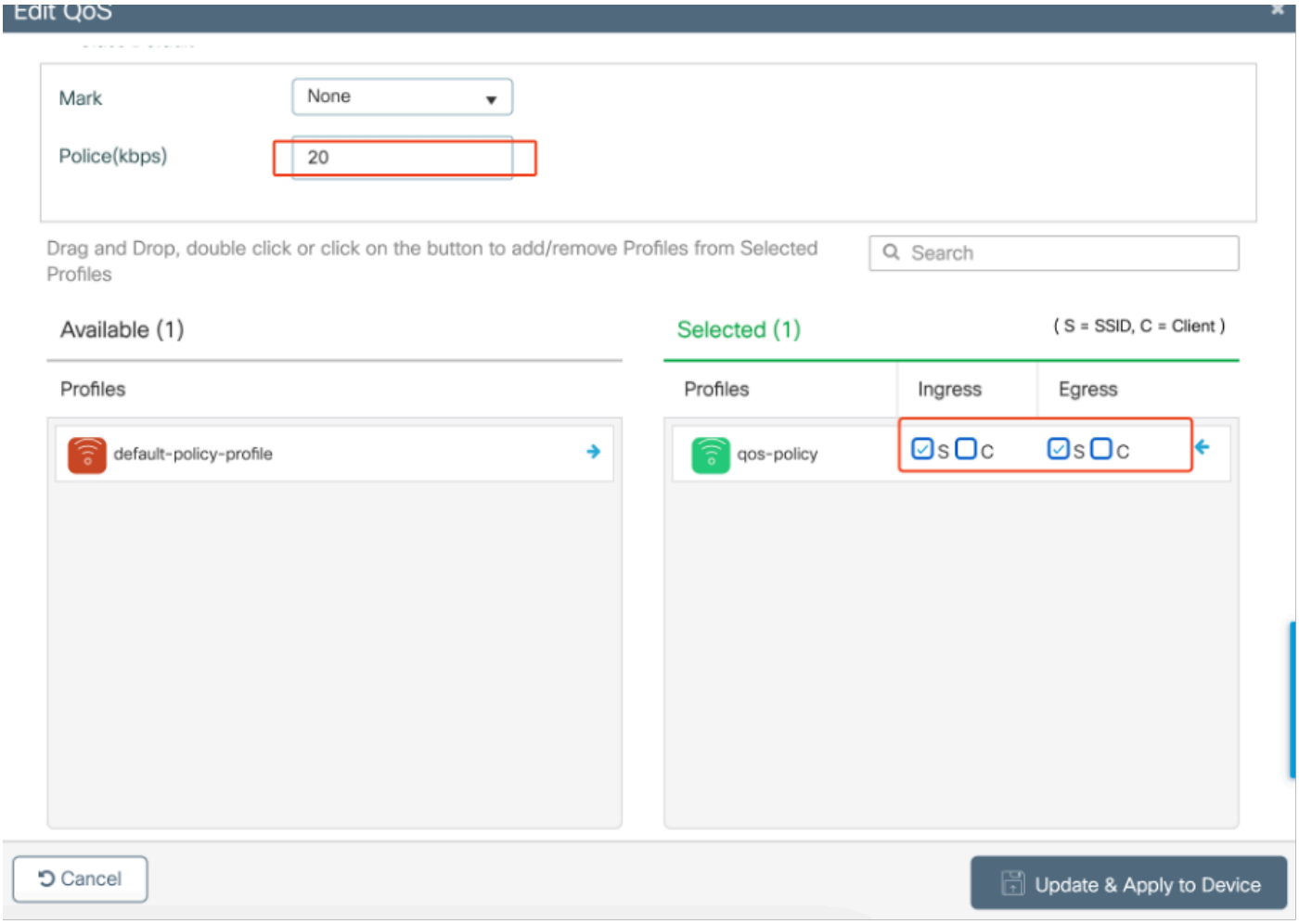
Une fois le trafic classifié à l'aide de la liste de contrôle d'accès, configurez les restrictions de bande passante pour contrôler la quantité de bande passante allouée à ce trafic.

Accédez à Configuration > Services > QoS et à la stratégie QoS. Raccordez la liste de contrôle d'accès à la stratégie et appliquez la police en kbits/s.

Faites défiler l'écran vers le bas et sélectionnez le profil de stratégie dans lequel la QoS doit être appliquée. Vous pouvez sélectionner la stratégie dans la direction d'entrée/sortie pour le SSID ou le client.



Politique MQS



Profil MQS

Configuration CLI 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 métal

L'objectif principal de ces profils QoS est de limiter les valeurs DSCP (Differentiated Services Code Point) maximales autorisées sur un réseau sans fil, contrôlant ainsi les valeurs UP (User Priority) 802.11.

Dans le contrôleur LAN sans fil (WLC) Cisco 9800, les profils QoS métalliques sont prédéfinis et ne sont pas configurables. Cependant, vous pouvez appliquer ces profils à des SSID ou à des clients spécifiques pour appliquer des stratégies QoS.

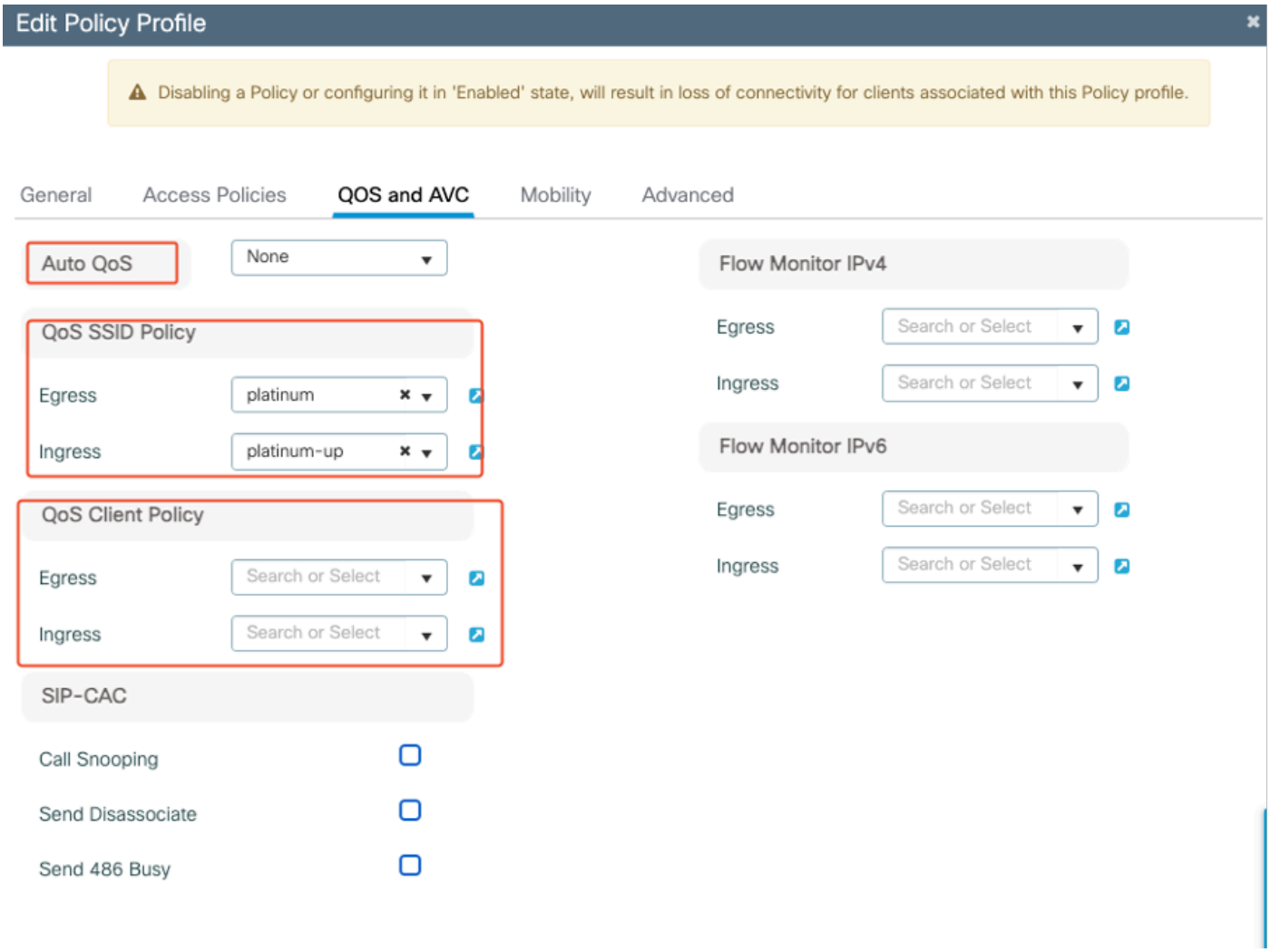
Quatre profils QoS métalliques sont disponibles :

Profil Qos	DSCP max.
Bronze	8
Argent	0
Or	34
Platine	46

Pour configurer la QoS métallique sur un WLC Cisco 9800 :

Accédez à Configuration > Policy > QoS & AVC.

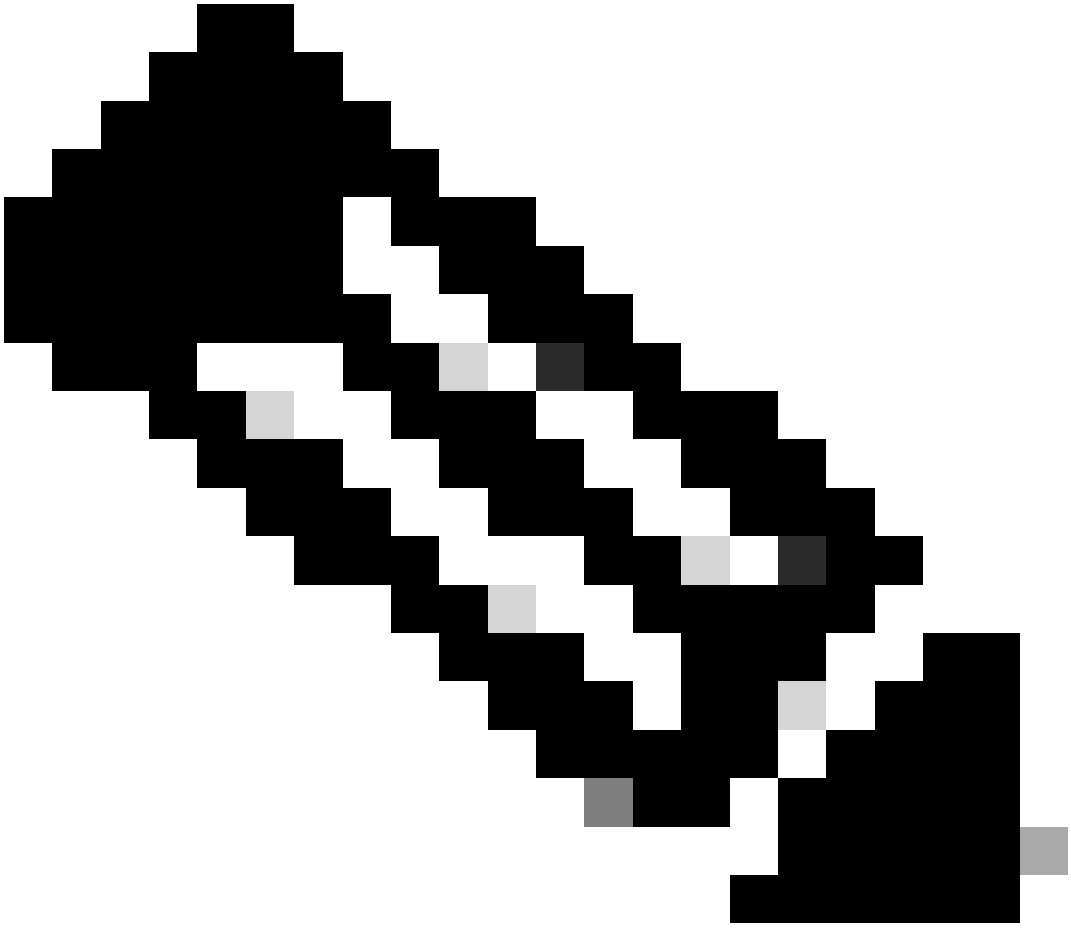
- Sélectionnez le profil QoS métal souhaité (Platinum, Gold, Silver ou Bronze).
- Appliquez le profil choisi au SSID ou au client cible.



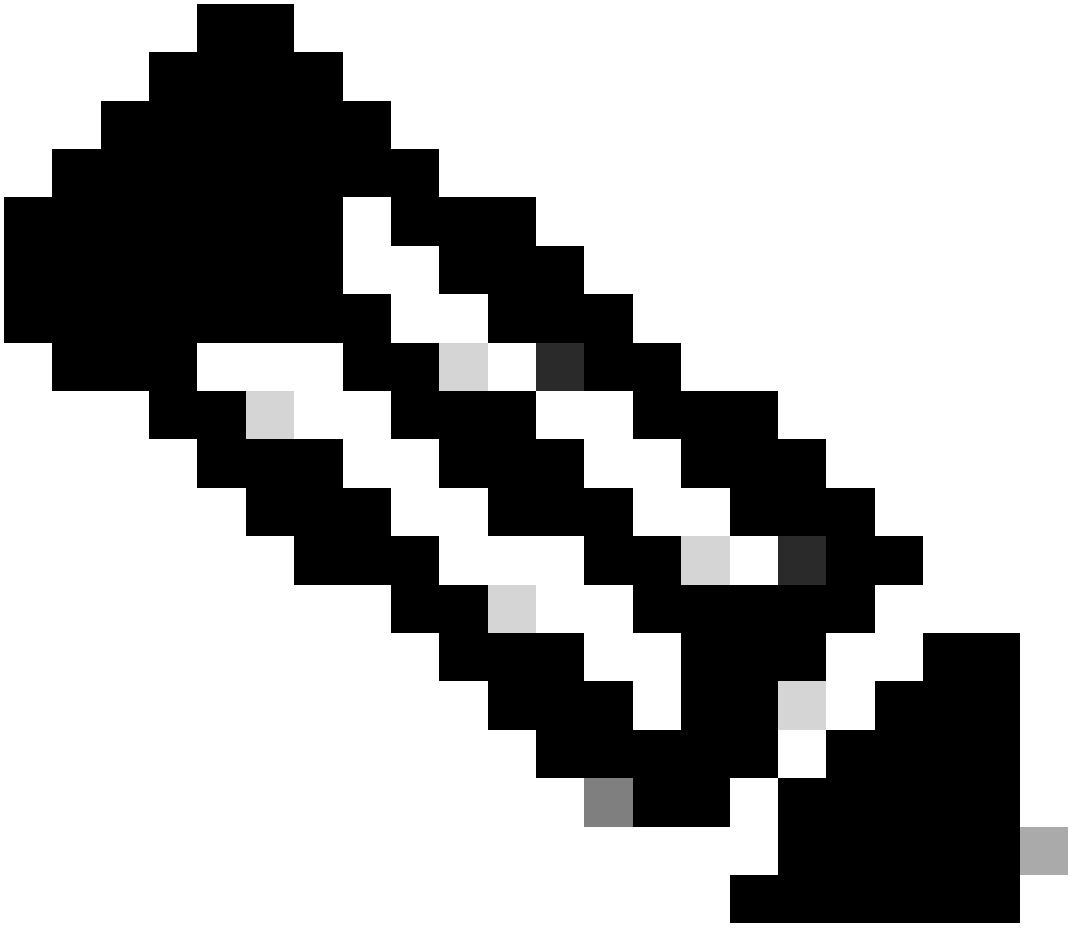
Profil QoS métallique

Configuration CLI QoS métallique

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



Remarque : le contrat de bande passante par utilisateur et SSID peut être configuré via des stratégies QoS et non directement sur la QoS métallique. Dans le 9800, le trafic non correspondant passe dans la classe par défaut.



Remarque : sur l'interface graphique utilisateur, vous pouvez uniquement définir la QoS métallique par SSID. Sur l'interface CLI, vous pouvez également la configurer sur la cible client.

Validation de la QoS de bout en bout avec capture de paquets

Maintenant que la configuration QoS est terminée, il est essentiel d'examiner les paquets QoS et de vérifier que les politiques QoS fonctionnent correctement de bout en bout. Cela peut être réalisé par la capture et l'analyse de paquets.

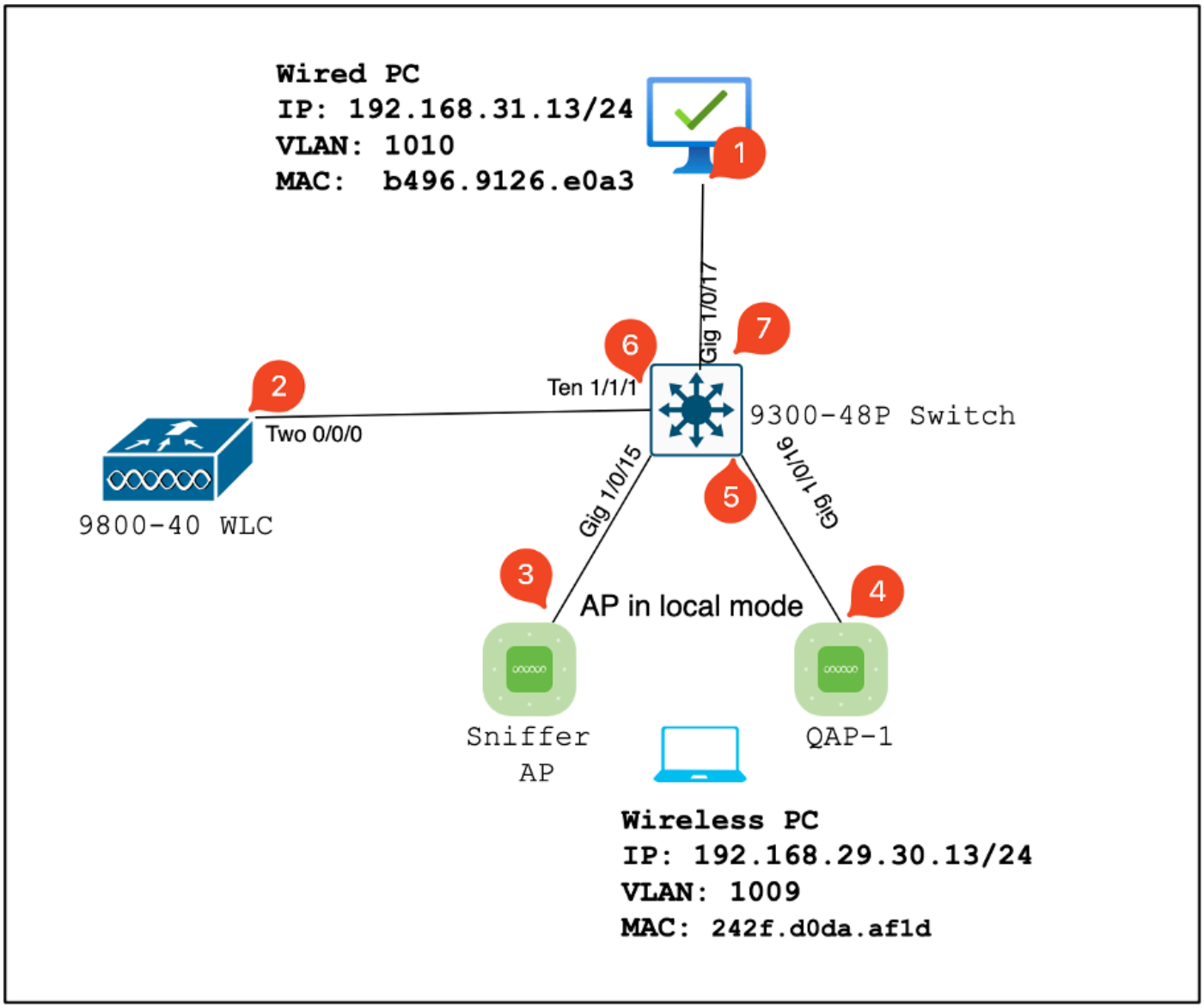
Pour répliquer et valider la configuration QoS, un environnement de TP à petite échelle est utilisé. Ces travaux pratiques comprennent les éléments suivants :

- WLC
- POINT D'ACCÈS
- Point d'accès Sniffer pour OTA
- PC câblé

- Commutateur

Tous ces composants sont connectés au même commutateur dans l'environnement des travaux pratiques. Les chiffres mis en évidence dans ce schéma indiquent les points où les captures de paquets sont activées pour surveiller et analyser le flux de trafic.

Diagramme du réseau



Topologie des travaux pratiques

Composants des travaux pratiques et points de capture de paquets

WLC :

- Gère les stratégies et les configurations QoS pour le réseau sans fil.
- Point de capture de paquets : capture du trafic entre le WLC, le point d'accès et le commutateur.

AP :

- Fournit une connectivité sans fil aux clients et applique les stratégies QoS.
- Point de capture de paquets : capture du trafic entre le point d'accès et le commutateur.

Point d'accès Sniffer :

- Agit comme un périphérique dédié pour capturer le trafic sans fil.
- Point de capture de paquets : capture du trafic sans fil entre le point d'accès et les clients sans fil.

PC filaire :

- Connecté au commutateur pour simuler le trafic filaire et valider la QoS de bout en bout.
- Point de capture de paquets : capture des paquets QoS transmis et reçus sur une liaison filaire.

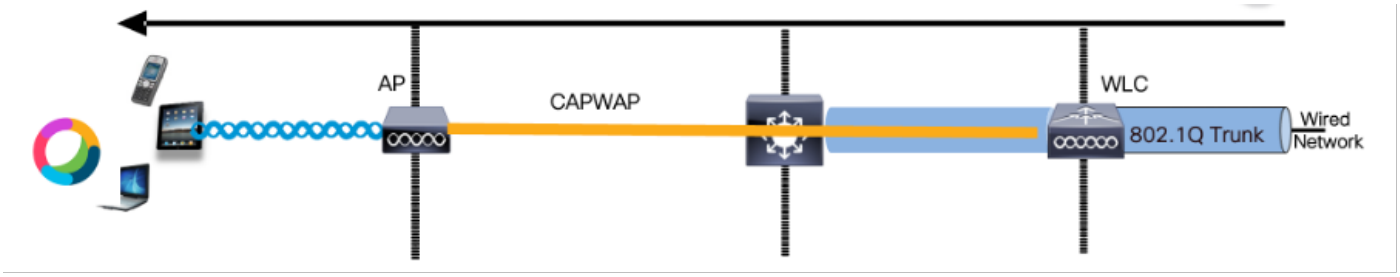
Ordinateur sans fil :

- Connecté au WLAN pour simuler le trafic sans fil et valider la QoS de bout en bout.
- Point de capture de paquets : capture des paquets QoS transmis et reçus sur une liaison sans fil.

Commutateur :

- Périphérique central qui interconnecte tous les composants des travaux pratiques et facilite la circulation du trafic.
- Points de capture de paquets : capture du trafic sur différents ports de commutation pour valider l'application de la qualité de service.

La topologie des travaux pratiques peut logiquement être tracée de la manière suivante.



Topologie logique de TP

Pour tester et valider la configuration QoS, iPerf est utilisé pour générer du trafic entre le client et le serveur. Ces commandes sont utilisées pour faciliter la communication iPerf, les rôles du serveur et du client étant interchangés en fonction de la direction du test QoS.

Scénario de test 1 : validation QoS en aval

L'objectif est de valider la configuration QoS en aval. La configuration implique qu'un PC filaire envoie des paquets avec DSCP 46 à un PC sans fil.
Le contrôleur de réseau local sans fil (WLC) est configuré avec la stratégie « Platinum QoS »

métallique pour les directions aval et amont.

Configuration du test :

- Flux de trafic :

  Source : PC filaire

  Destination : Wireless PC

  Type de trafic : paquets UDP avec DSCP 46

- Configuration de la stratégie QoS sur WLC :

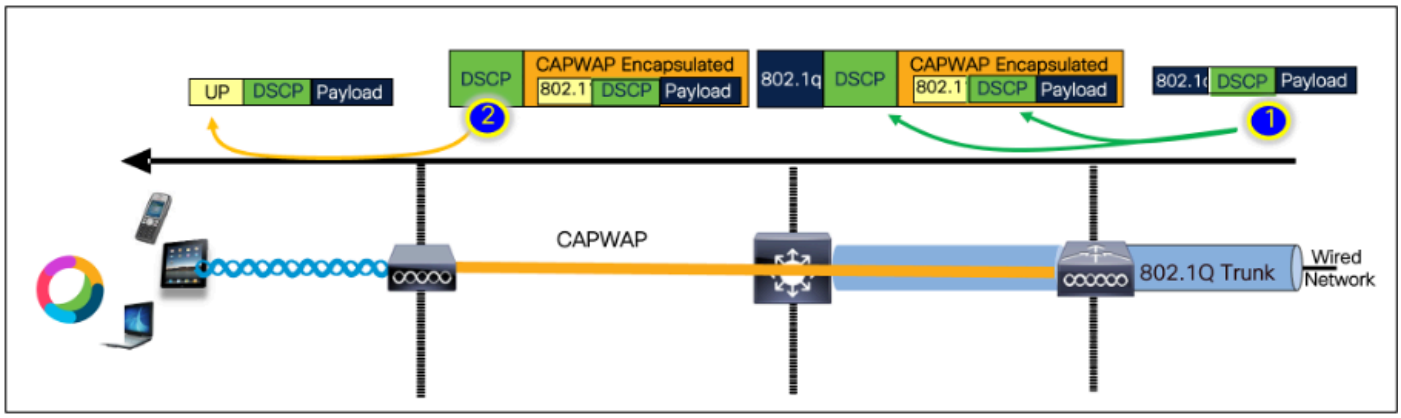
  Profil QoS : QoS métal - QoS Platinum

  Direction : aval et amont

- Commandes de configuration QoS métal :

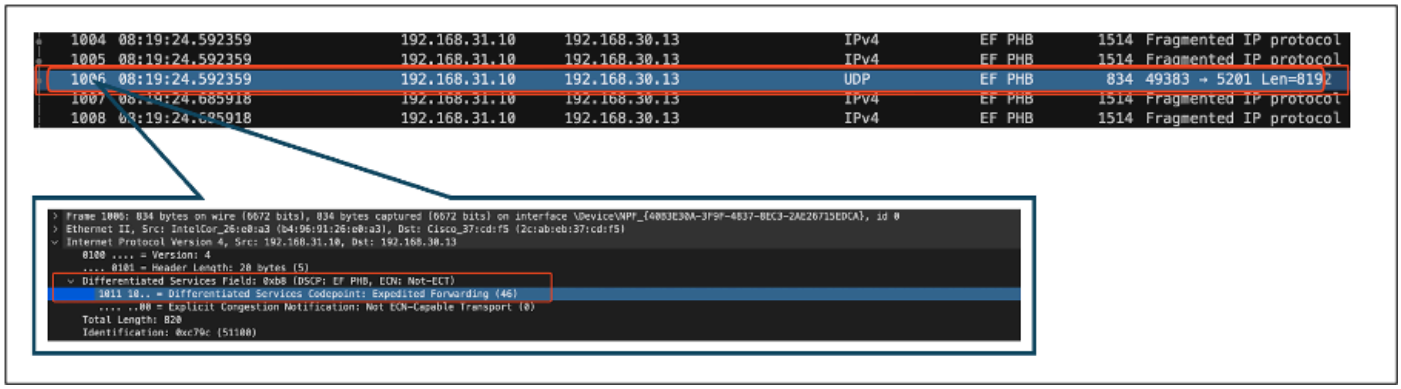
```
wireless profile policy qos-policy
service-policy input platinum-up
service-policy output platinum
```

Topologie logique et conversation DSCP en aval.



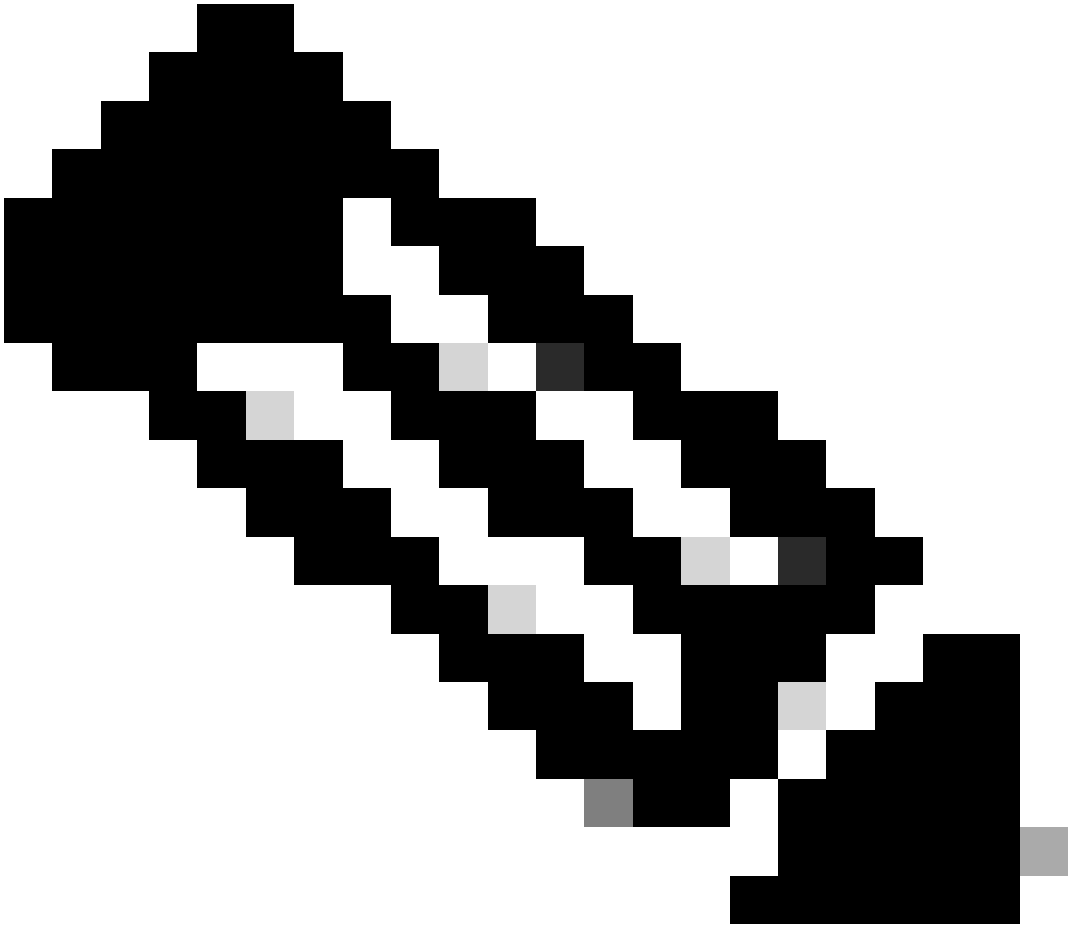
Point de conversation DSCP

Capture de paquets effectuée sur le PC filaire. Cela confirme que le PC filaire envoie des paquets UDP à l'adresse IP de destination spécifiée 192.168.10.13 avec le marquage DSCP correct de 46.

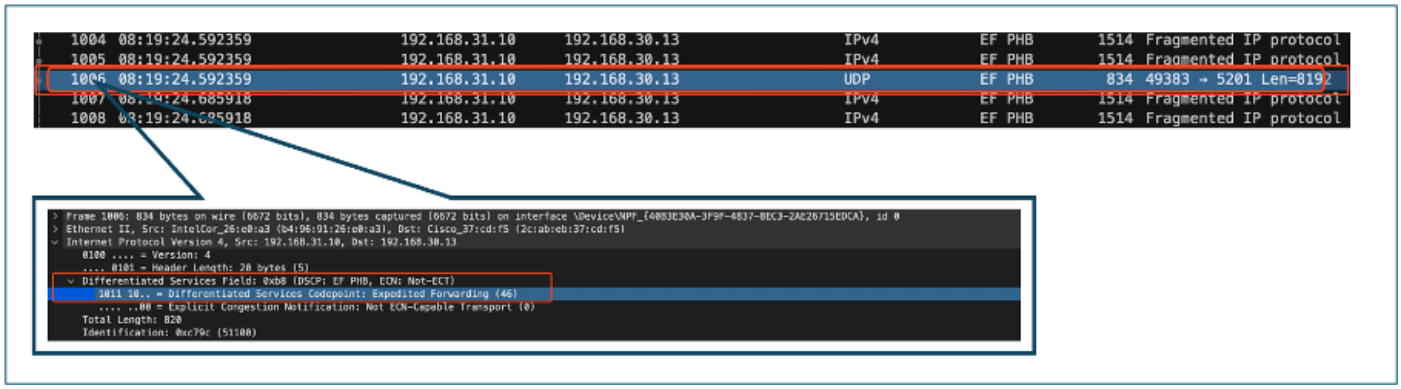


Capture de PC filaire - Direction aval

Examinons ensuite un paquet capturé sur le commutateur de liaison ascendante connecté au PC filaire. Le commutateur fait confiance à la balise DSCP et la valeur DSCP reste inchangée à 46.

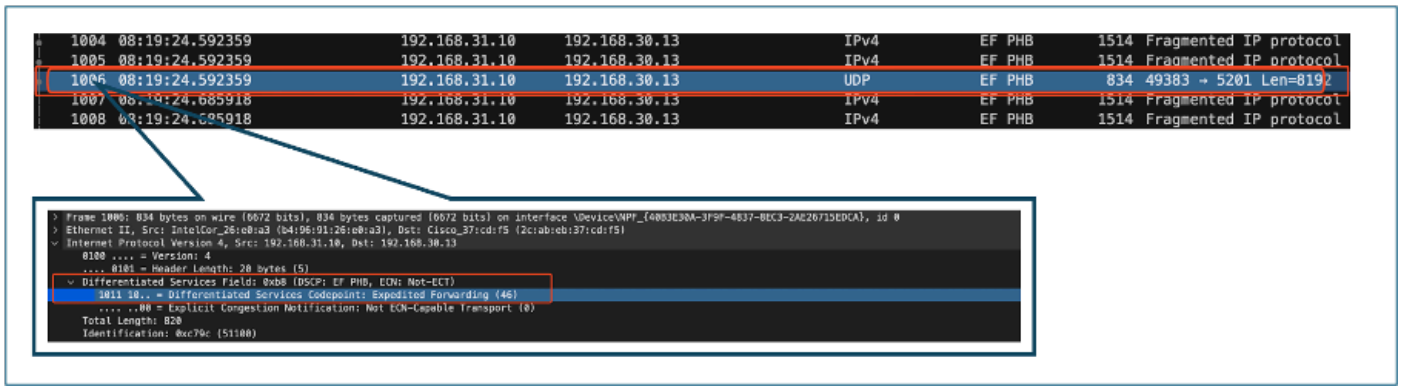


Remarque : les ports de commutateur de la gamme Catalyst 9000 sont par défaut à l'état de confiance.



Capture d'interface de liaison ascendante PC filaire

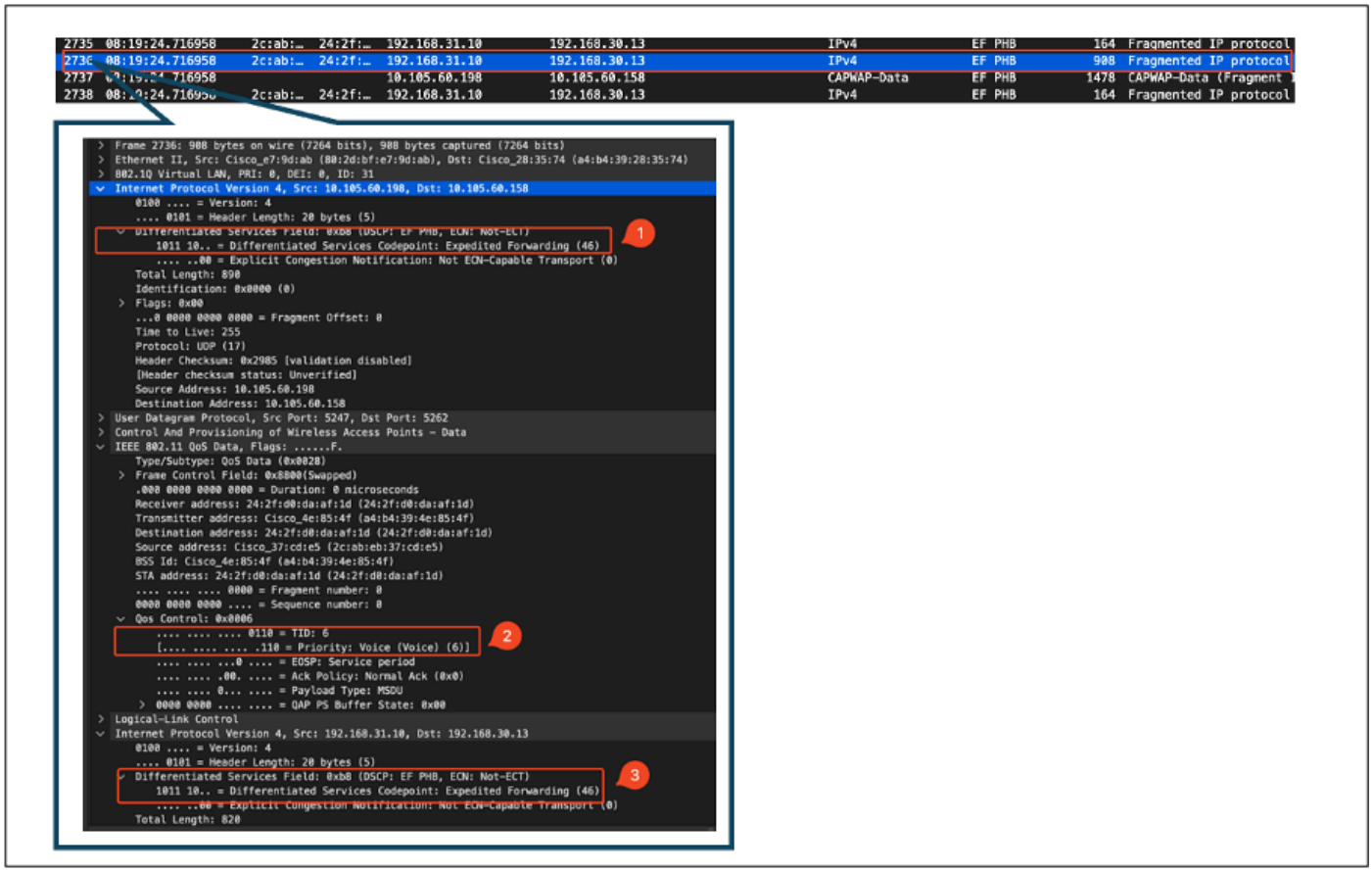
Lors de l'examen de la capture de paquets sur le WLC pris à l'aide de l'EPC, le paquet arrive avec la même étiquette DSCP de 46 du commutateur de liaison ascendante. Cela confirme que le marquage DSCP est conservé lorsque le paquet atteint le WLC.



Direction aval WLC EPC

Lorsque le WLC envoie le paquet au point d'accès à l'intérieur d'un tunnel CAPWAP, il s'agit d'une intersection critique où le WLC peut modifier le DSCP en fonction de sa configuration. Décomposons la capture des paquets, qui est mise en évidence par des points numérotés pour plus de clarté :

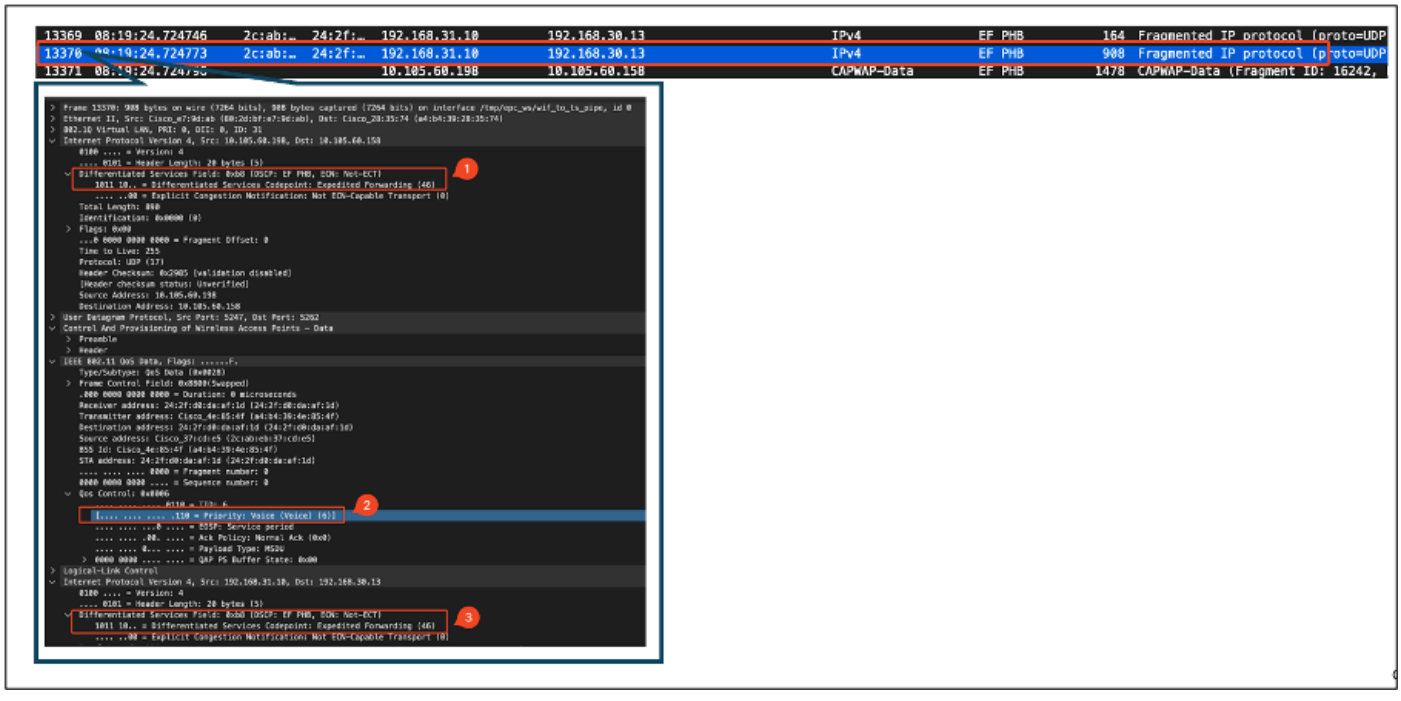
- Couche externe CAPWAP : la couche externe du tunnel CAPWAP affiche l'étiquette DSCP 46, qui est la valeur reçue de l'extrémité du commutateur.
- Valeur 802.11 UP dans CAPWAP : dans le tunnel CAPWAP, le WLC mappe le DSCP 46 à la priorité d'utilisateur (UP) 6 802.11, qui correspond au trafic vocal.
- Valeur DSCP dans CAPWAP : Le WLC Cisco 9800 fonctionne avec un modèle DSCP de confiance, de sorte que la valeur DSCP à l'intérieur du tunnel CAPWAP est maintenue à 46 identique à la couche DSCP externe.



Marques CAPWAP DSCP

Ensuite, vérifiez le même paquet sur le port de commutation de liaison ascendante AP.

La valeur DSCP sur la couche CAPWAP externe reste à 46. À titre d'illustration, le trafic CAPWAP interne est mis en surbrillance pour afficher l'étiquetage.

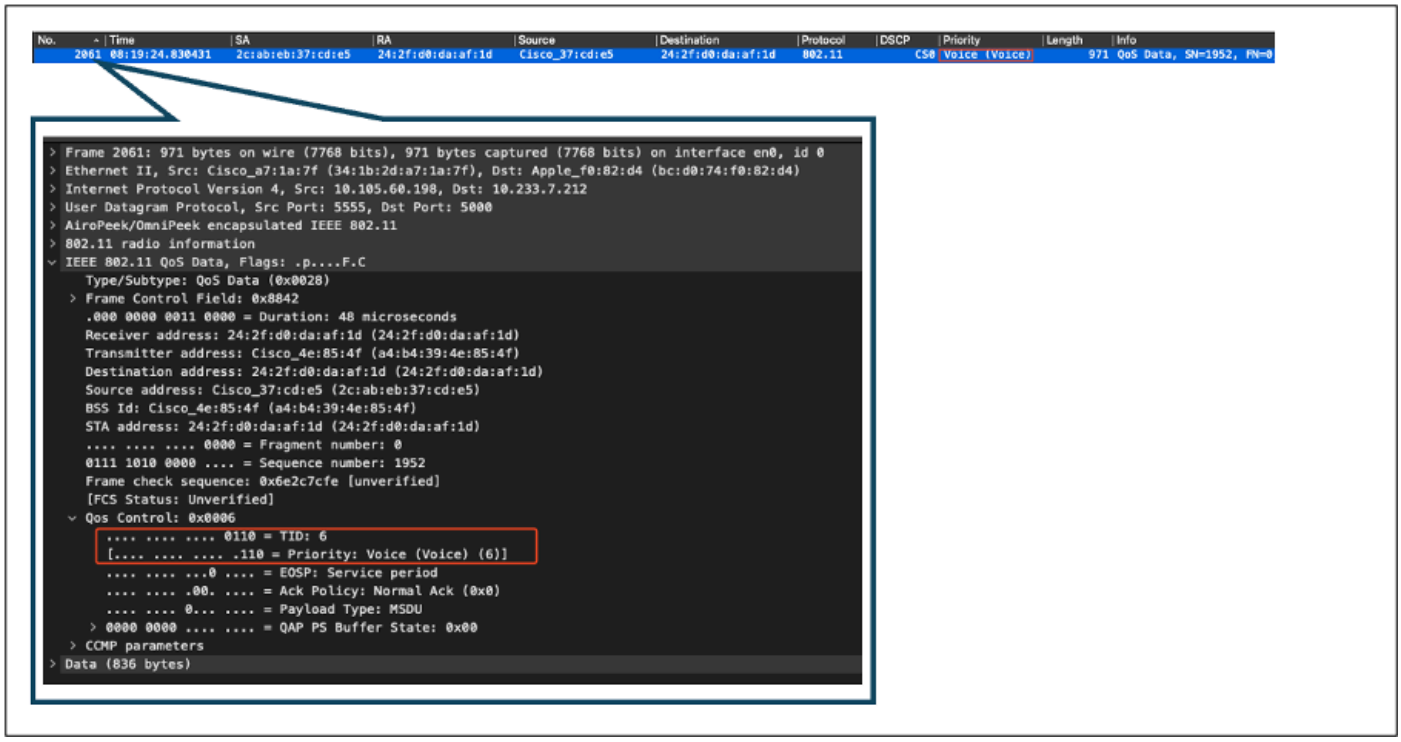


Capture d'interface de commutateur de liaison ascendante AP

Une fois que le point d'accès reçoit le paquet, il le transmet par voie aérienne. Pour vérifier le

marquage de priorité d'utilisateur (UP), une capture OTA (Over-the-Air) effectuée avec un point d'accès analyseur est utilisée.

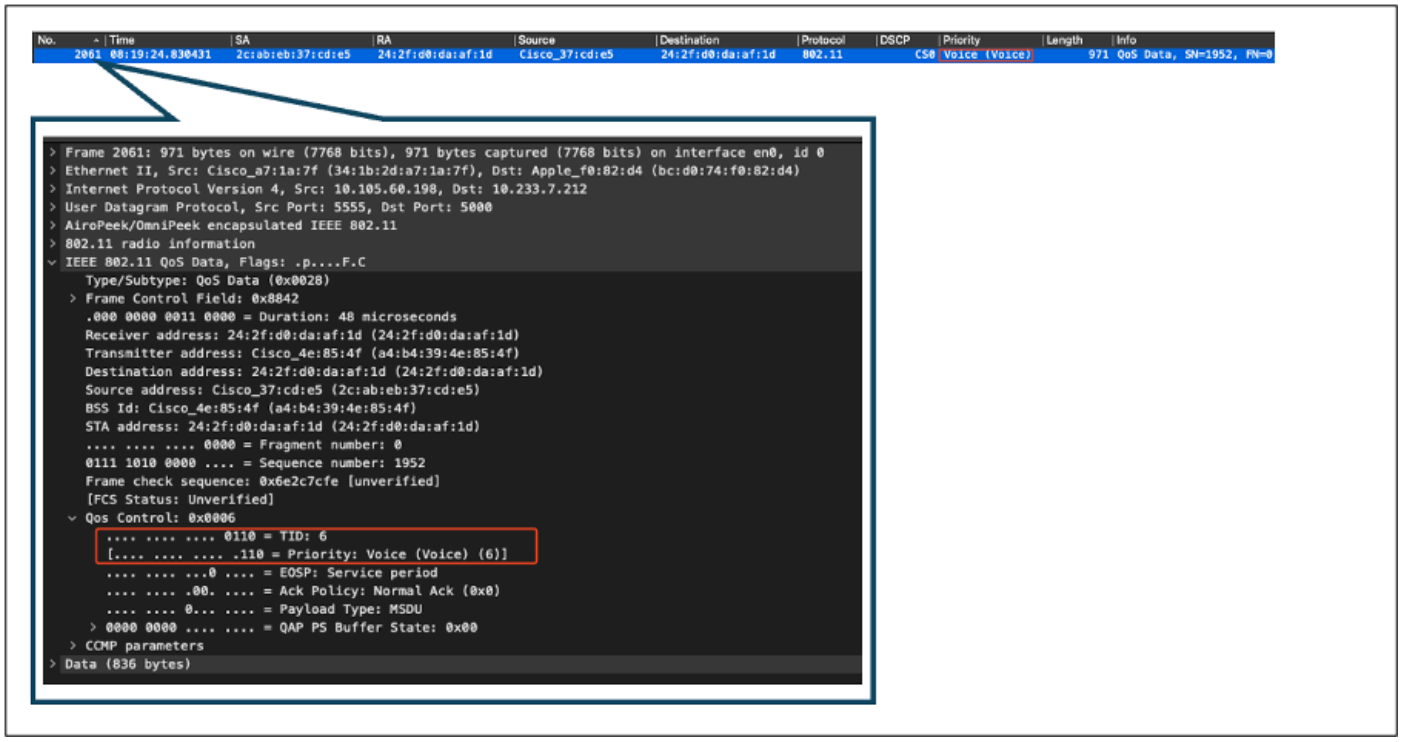
Le point d'accès a transféré la trame avec une valeur UP de 6. Cela confirme que le point d'accès mappe correctement la valeur DSCP à la valeur 802.11 UP appropriée (6), qui correspond au trafic vocal.



Capture OTA du point d'accès au client

Au stade final, le paquet est reçu par le PC sans fil. Le PC sans fil reçoit la trame avec une valeur DSCP de 46.

Cela indique que le marquage DSCP est préservé tout au long du chemin de transmission, du PC filaire au PC sans fil. La valeur DSCP cohérente de 46 confirme que les politiques QoS sont correctement appliquées et maintenues en aval.



Capture de PC sans fil

Scénario de test 2 : validation QoS en amont

Dans ce scénario de test, l'objectif est de valider la configuration QoS en amont. La configuration implique qu'un PC sans fil envoie des paquets UDP avec DSCP 46 à un PC câblé. Le WLC est configuré avec la politique « Platinum QoS » de Metal pour les directions amont et aval.

- Flux de trafic :

Source : Wireless PC

Destination : PC filaire

Type de trafic : paquets UDP avec DSCP 46

- Configuration de la stratégie QoS sur WLC :

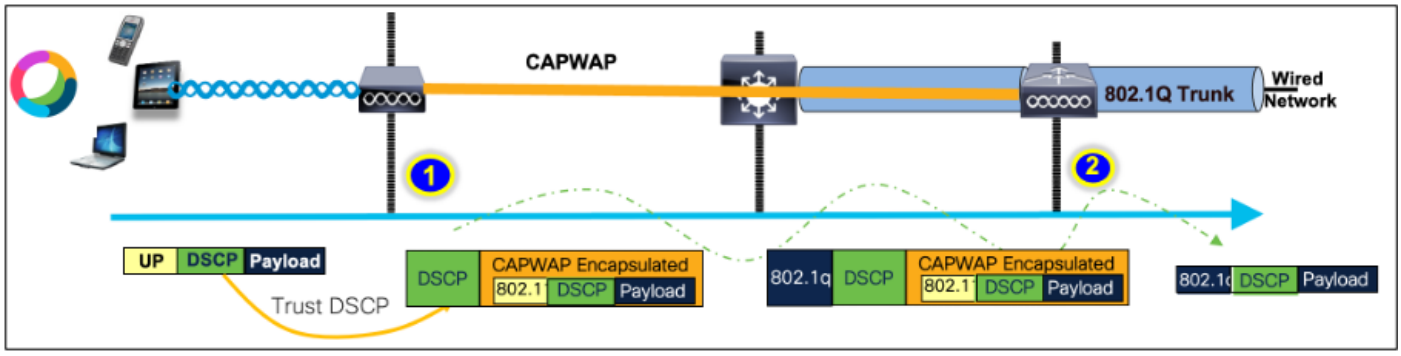
Profil QoS : QoS Platinum

Direction : amont et aval

- Commandes de configuration QoS métal :

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

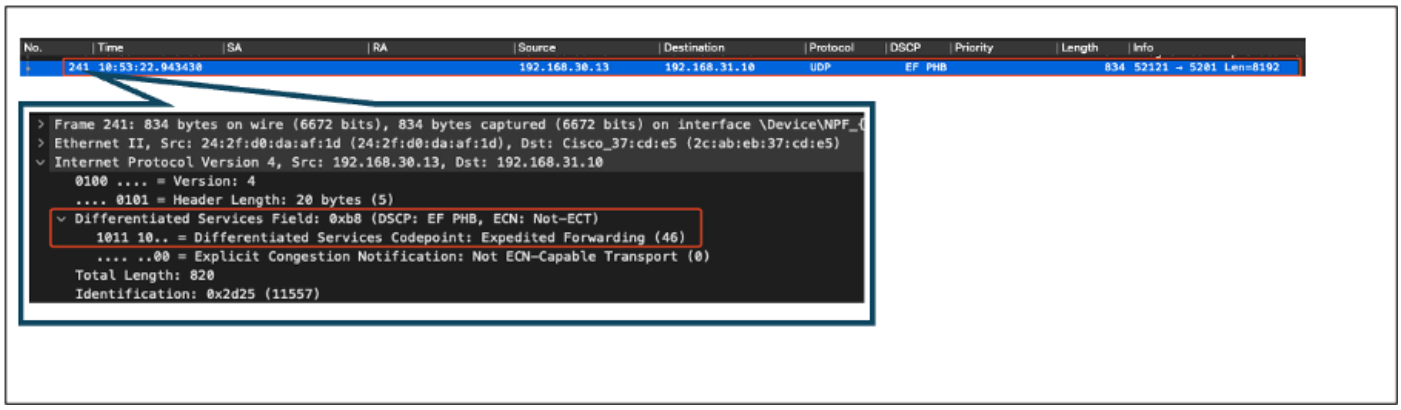
Topologie logique et conversion DSCP en amont :



Topologie logique et conversion DSCP - En amont

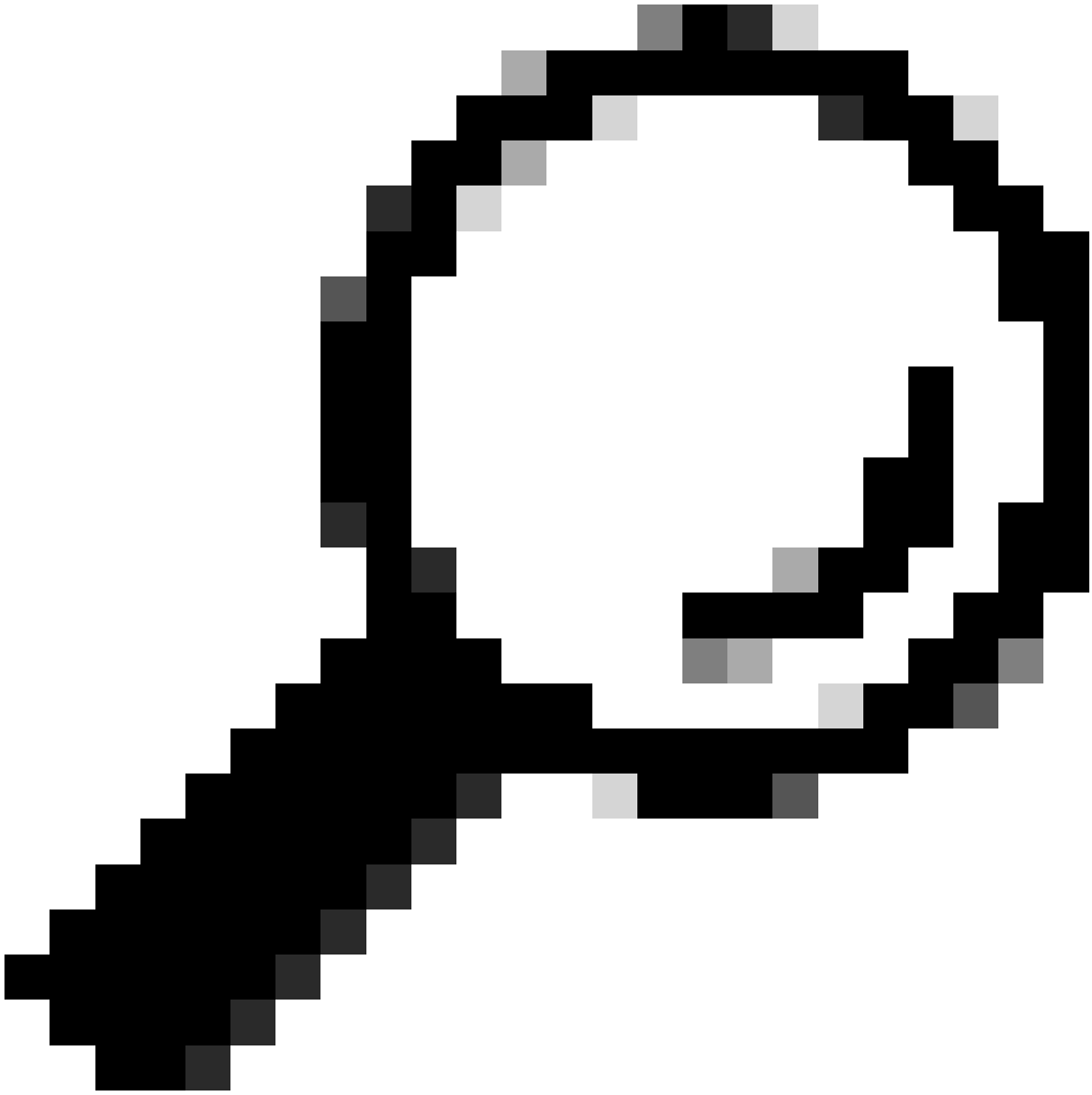
Paquets envoyés du PC sans fil au PC câblé. Cette capture est effectuée au niveau du PC sans fil.

Le PC sans fil envoie des paquets UDP avec DSCP 46.

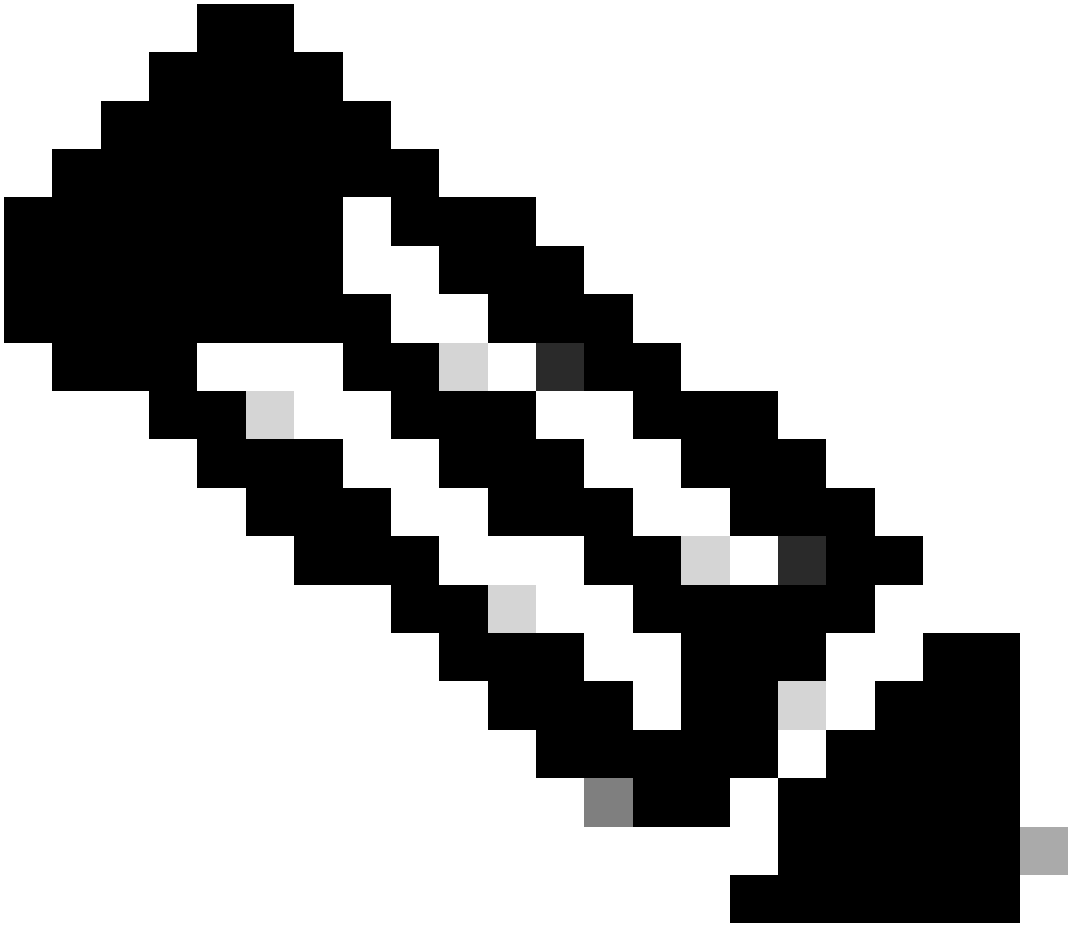


Capture de PC sans fil en amont

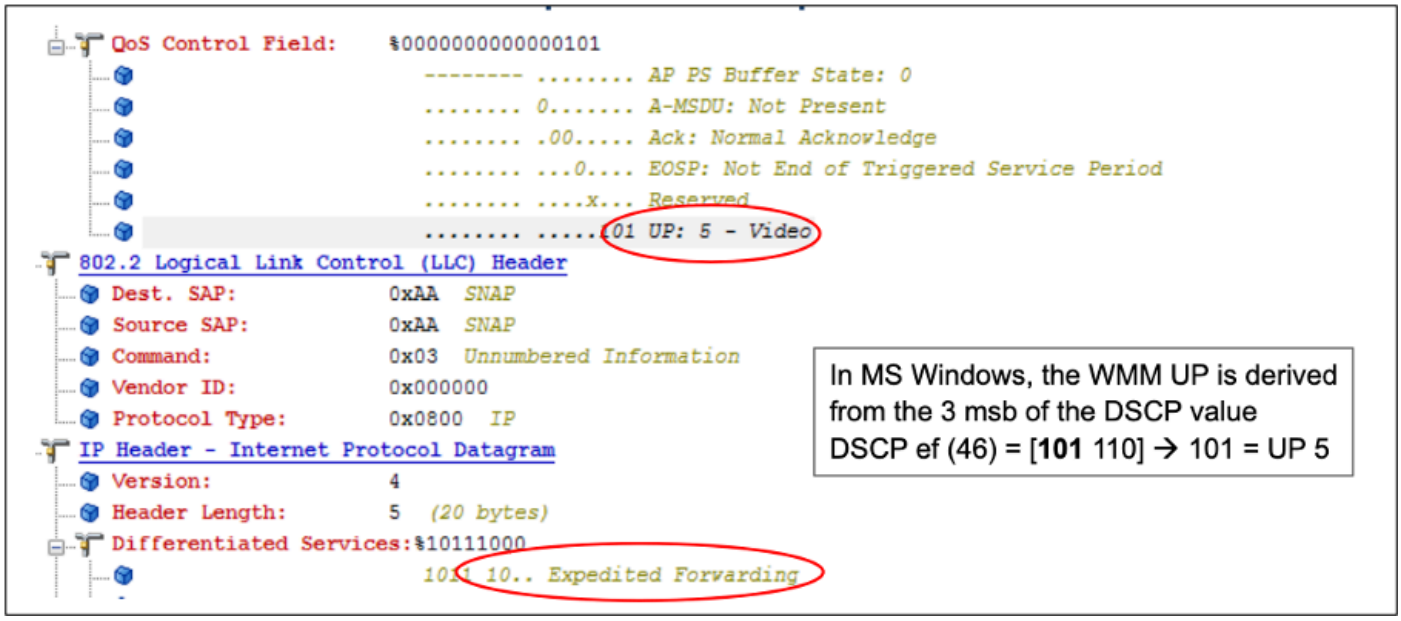
Examinons maintenant la capture OTA du client vers le point d'accès.



Conseil : lorsque vous utilisez un PC sans fil Windows pour envoyer des paquets avec DSCP 46, Windows mappe DSCP 46 à une valeur de priorité d'utilisateur (UP) de 5 (vidéo). Par conséquent, la capture OTA affiche les paquets comme trafic vidéo (UP 5). Cependant, si vous décryptez le paquet, la valeur DSCP reste à 46.



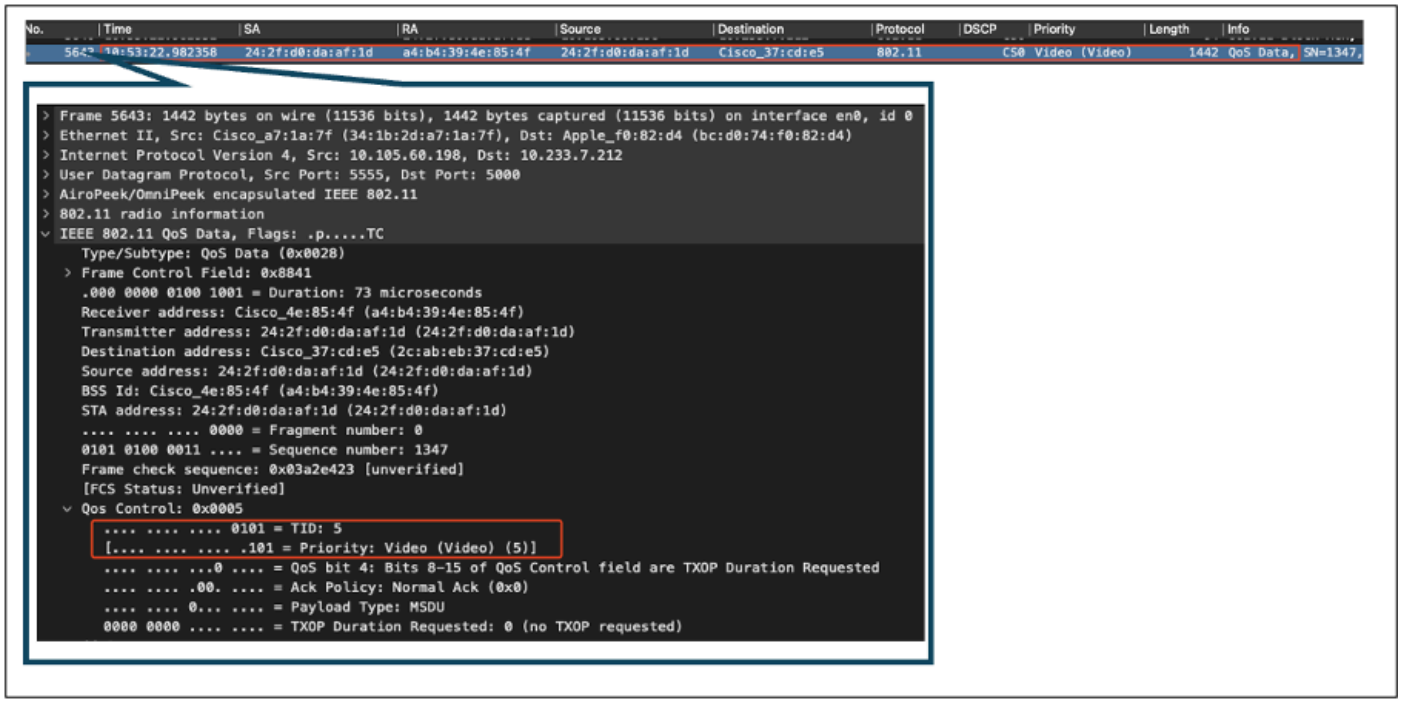
Remarque : à partir de la version 17.4, le comportement par défaut du WLC Cisco 9800 est d'approuver la valeur DSCP dans le profil de jointure AP. Cela garantit que la valeur DSCP de 46 est conservée et approuvée par le WLC, empêchant tout problème lié au comportement de mappage DSCP vers UP de Windows.



Mappage Windows UP vers DSCP

La capture OTA (Over-the-Air) cryptée issue de la configuration des travaux pratiques est analysée pour valider la configuration QoS en amont.

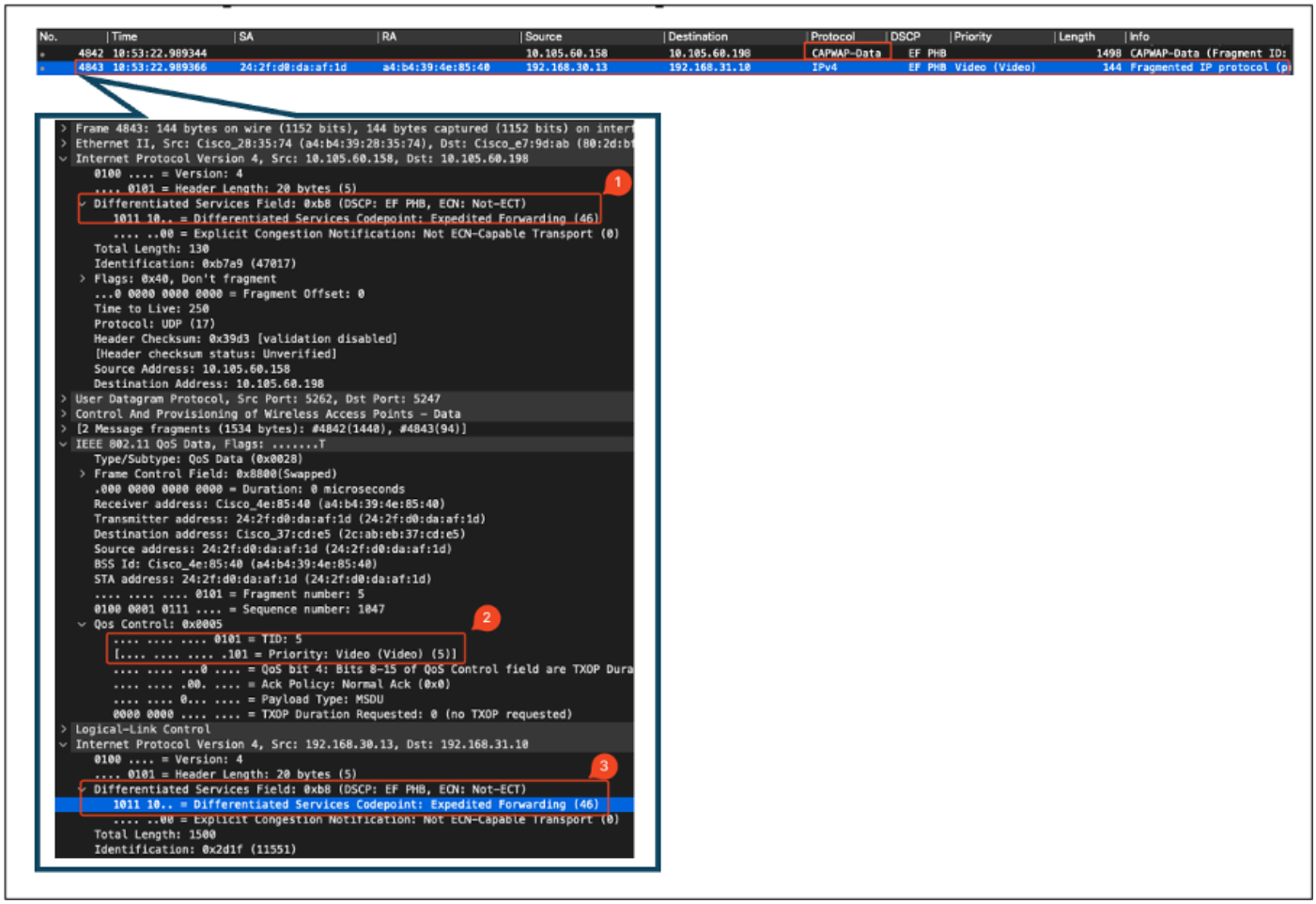
La capture OTA affiche les paquets avec une valeur de priorité utilisateur (UP) de 5 (vidéo). Bien que la capture OTA indique UP 5, la valeur DSCP à l'intérieur du paquet chiffré reste à 46.



LAB Setup OTA en amont

Ensuite, la capture de paquet sur le port de liaison ascendante AP est analysée pour s'assurer que la valeur DSCP est préservée pendant que le paquet se déplace du point d'accès au WLC.

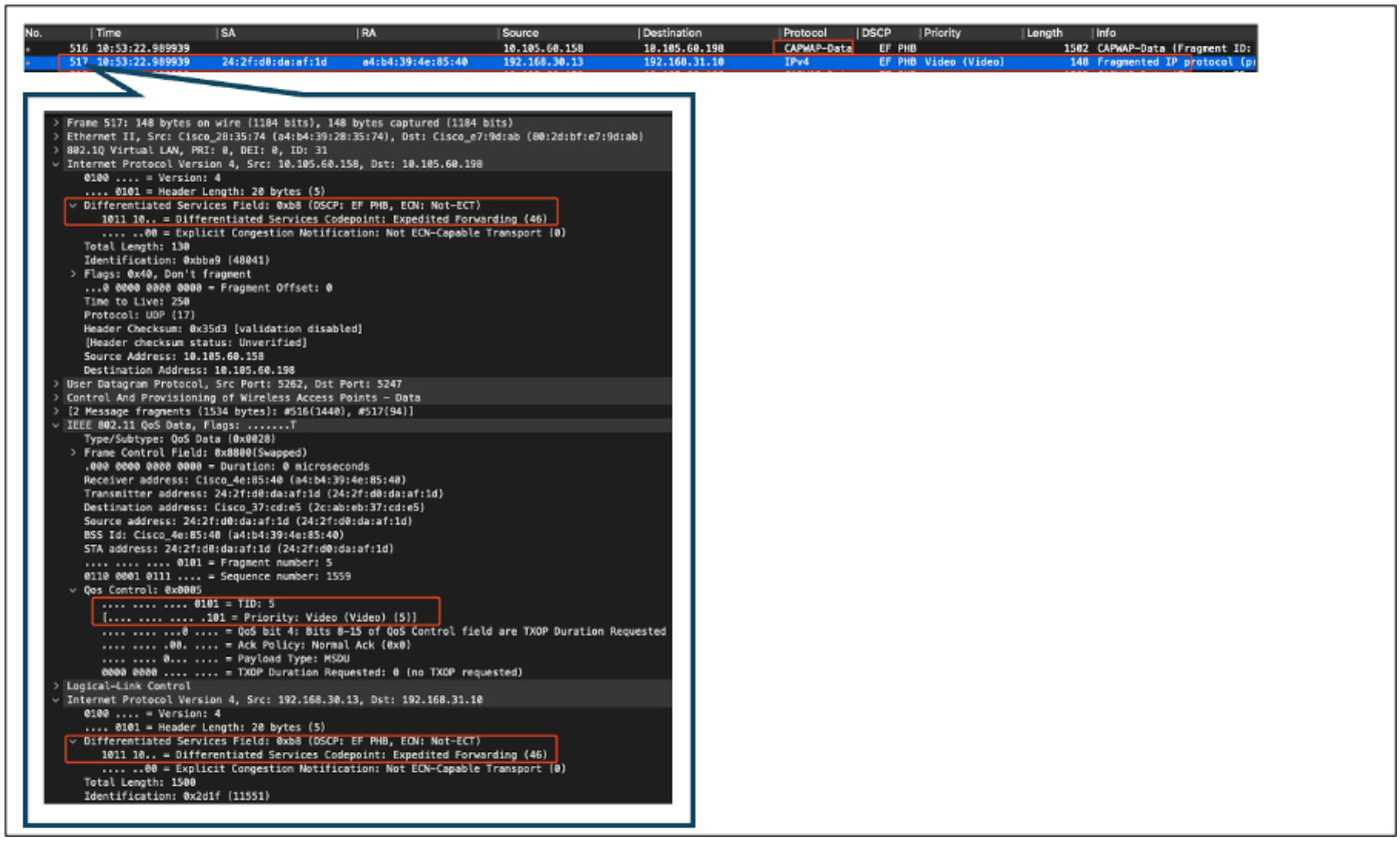
- La valeur DSCP sur la couche CAPWAP externe est maintenue à 46.
- Dans le tunnel CAPWAP, la valeur DSCP est également maintenue à 46.



AP Pplink Capture dans la direction amont

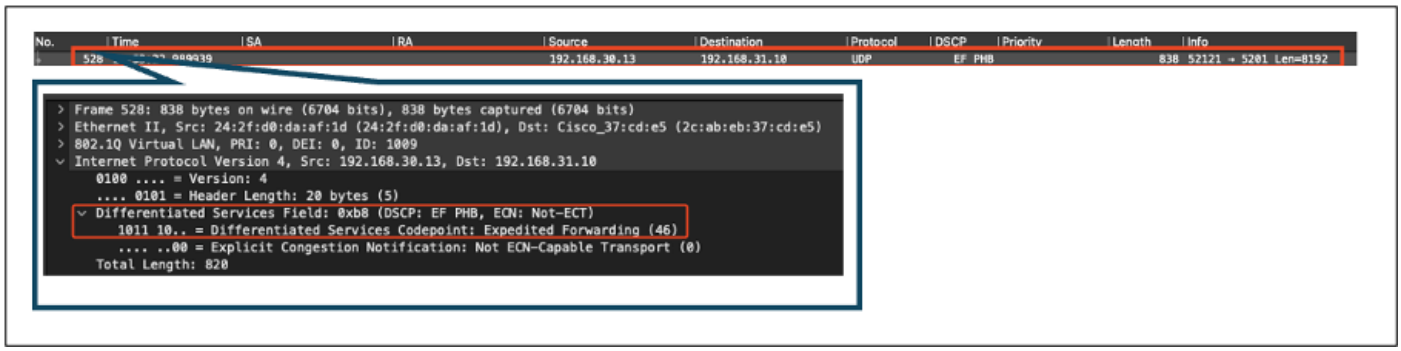
La capture est effectuée au niveau du WLC lorsque le paquet arrive du commutateur.

- Le paquet arrive au WLC avec la valeur DSCP de 46 sur la couche CAPWAP externe.
- Dans le tunnel CAPWAP, la valeur DSCP est maintenue à 46.



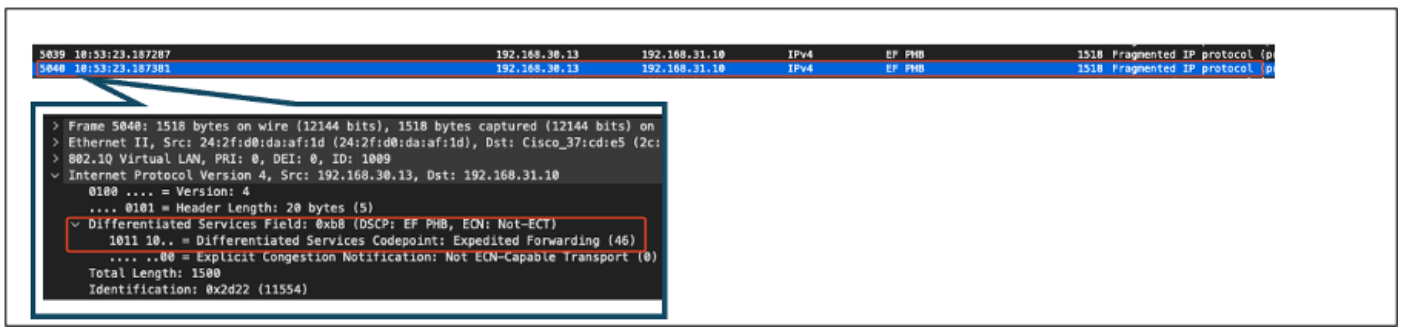
WLC EPC montrant les paquets provenant du point d'accès

Une fois que le paquet prend un tour en épingle à cheveux au niveau du WLC, il est renvoyé au commutateur de liaison ascendante, à destination du PC câblé. Le WLC transfère le paquet avec la valeur DSCP de 46.



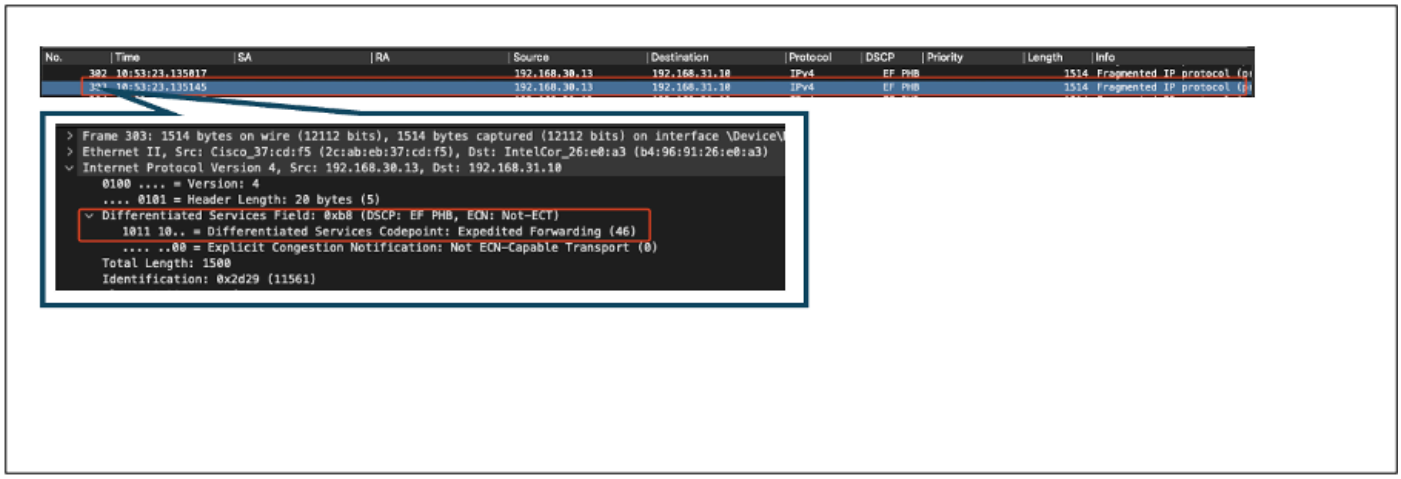
WLC EPC montrant les paquets envoyés au PC câblé

Enfin, la capture de paquets au niveau de la liaison ascendante du PC filaire est analysée pour s'assurer que la valeur DSCP est conservée lorsque le paquet arrive du WLC.



Capture du commutateur de liaison ascendante du PC filaire vers l'amont

Au stade final, le paquet reçu par le PC filaire est analysé pour s'assurer qu'il arrive au PC filaire avec la valeur DSCP de 46.



Capture de PC filaire - Direction amont

Le test QoS en amont a validé avec succès la configuration QoS pour le trafic circulant du PC sans fil vers le PC câblé. La préservation constante de la valeur DSCP de 46 sur l'ensemble du chemin de transmission confirme que les politiques de QoS sont correctement appliquées.

Dépannage

Les applications vocales, vidéo et autres applications en temps réel sont particulièrement sensibles aux problèmes de performances du réseau, et toute dégradation de la qualité de service (QoS) peut avoir des effets perceptibles et néfastes. Lorsque des paquets QoS sont signalés avec des valeurs DSCP inférieures, l'impact sur la voix et la vidéo peut être important.

Impact sur la voix :

- Latence accrue : la communication vocale nécessite une faible latence pour garantir des conversations naturelles et fluides. Des valeurs DSCP inférieures peuvent entraîner un retard des paquets vocaux, ce qui entraîne un retard notable dans les conversations.
- Gigue : la variation des temps d'arrivée des paquets (gigue) peut perturber la bonne livraison des paquets vocaux. Cela peut entraîner un son haché ou brouillé, ce qui rend difficile la compréhension du haut-parleur.
- Perte de paquets : les paquets vocaux sont très sensibles à la perte de paquets. Même une petite perte de paquets peut entraîner des mots ou des syllabes manquants, ce qui entraîne une mauvaise qualité des appels et des malentendus.
- Echo et distorsion : une latence et une gigue accrues peuvent entraîner une distorsion de l'écho et de l'audio, ce qui réduit encore la qualité de l'appel vocal.

Impact sur la vidéo :

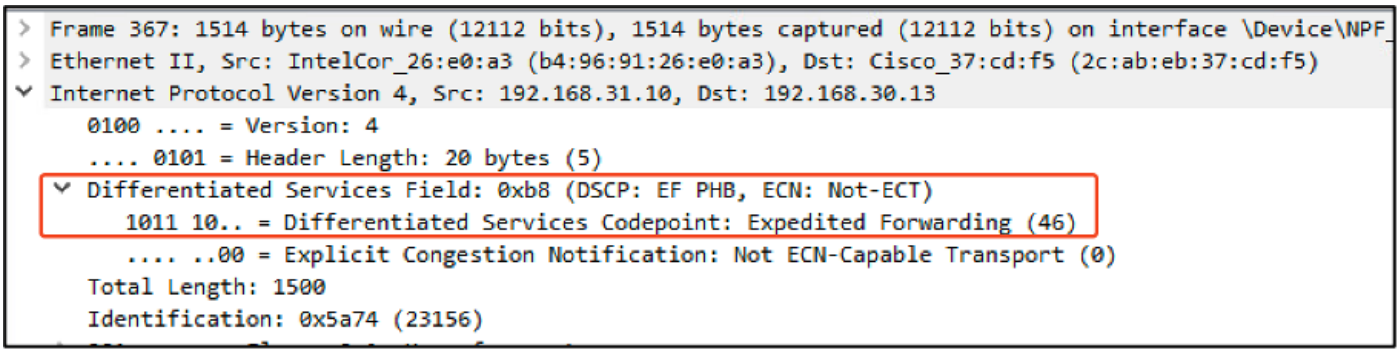
- Latence accrue : la communication vidéo nécessite une faible latence pour maintenir la synchronisation entre les flux audio et vidéo. L'augmentation de la latence peut entraîner des

retards, ce qui complique les interactions en temps réel.
- Gigue : la gigue peut provoquer l'arrivée d'images vidéo dans le désordre ou à des intervalles irréguliers, ce qui entraîne une expérience vidéo saccadée ou bégayante.
- Perte de paquets : la perte de paquets peut entraîner l'absence de trames, ce qui peut entraîner le blocage ou l'affichage d'artefacts.
- Qualité vidéo réduite : des valeurs DSCP inférieures peuvent entraîner une allocation de bande passante réduite pour les flux vidéo, ce qui entraîne une résolution inférieure et une qualité vidéo inférieure. Cela peut rendre difficile l'affichage de détails importants dans la vidéo.

Scénario 1 : le commutateur intermédiaire réécrit le marquage DSCP

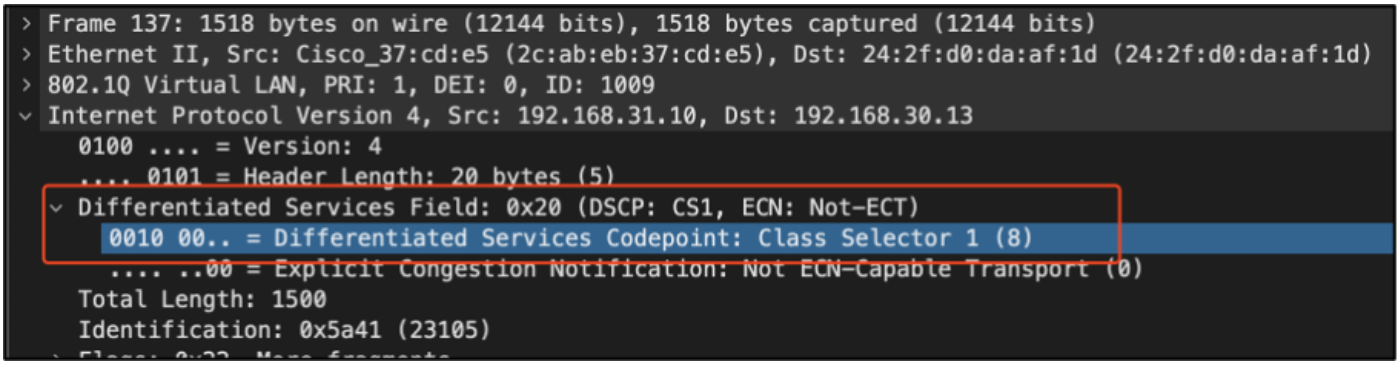
Dans ce scénario de dépannage, l'impact d'un commutateur intermédiaire réécrivant le marquage DSCP sur le trafic lorsqu'il arrive au WLC est examiné. Pour répliquer cela, le commutateur est configuré pour réécrire le marquage DSCP 46 sur CS1 sur l'interface de liaison ascendante du PC filaire.

Le paquet est envoyé à partir du PC câblé avec une balise DSCP 46.



PC filaire envoyant un paquet avec la balise DSCP 46

Le paquet arrive au WLC avec une valeur DSCP de CS1 (DSCP 8). Le passage de DSCP 46 à DSCP 8 réduit considérablement la priorité du paquet.

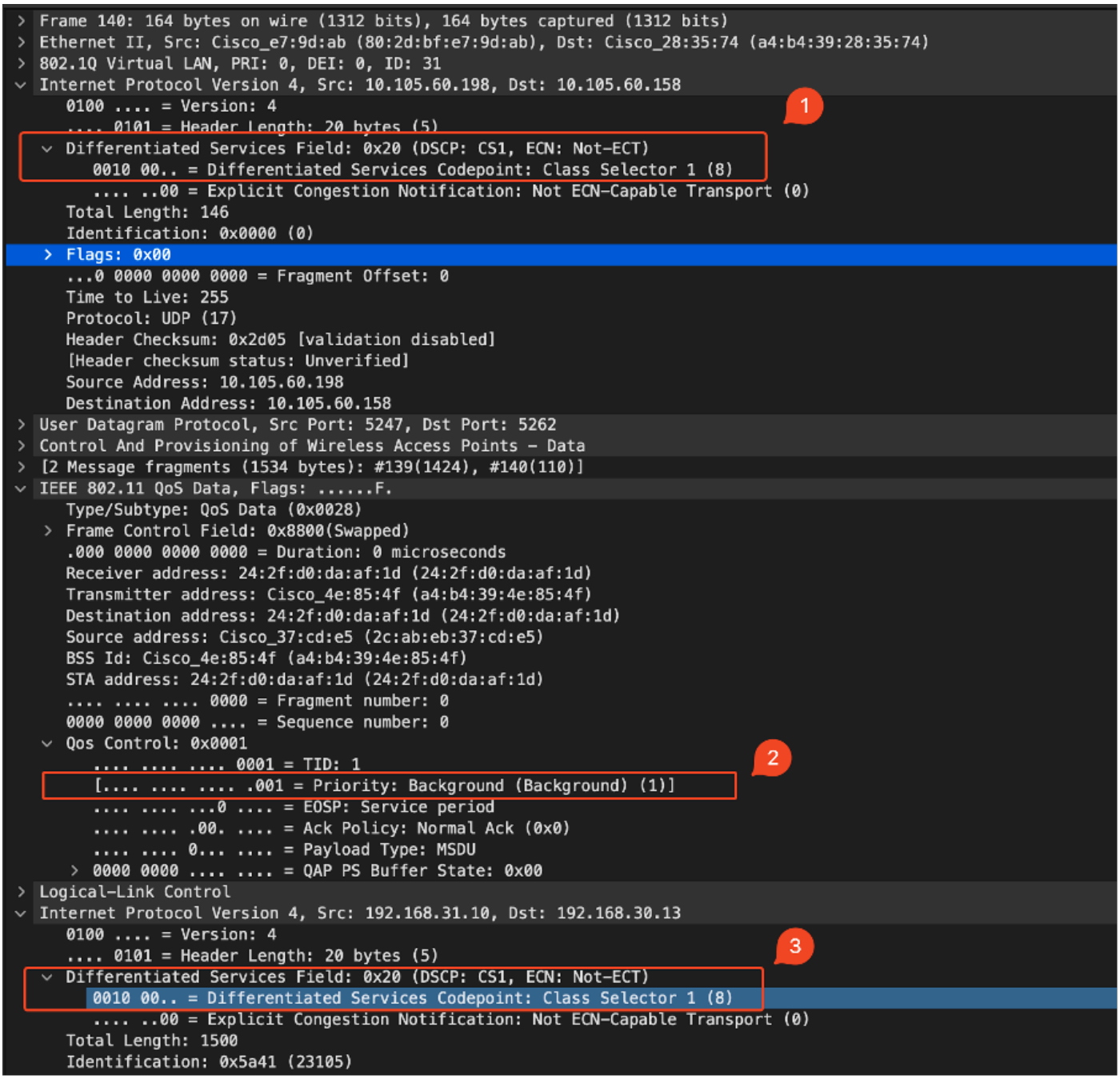


EPC WLC avec marquage CS1

Dans cette étape, le paquet transféré par le WLC au point d'accès est analysé.

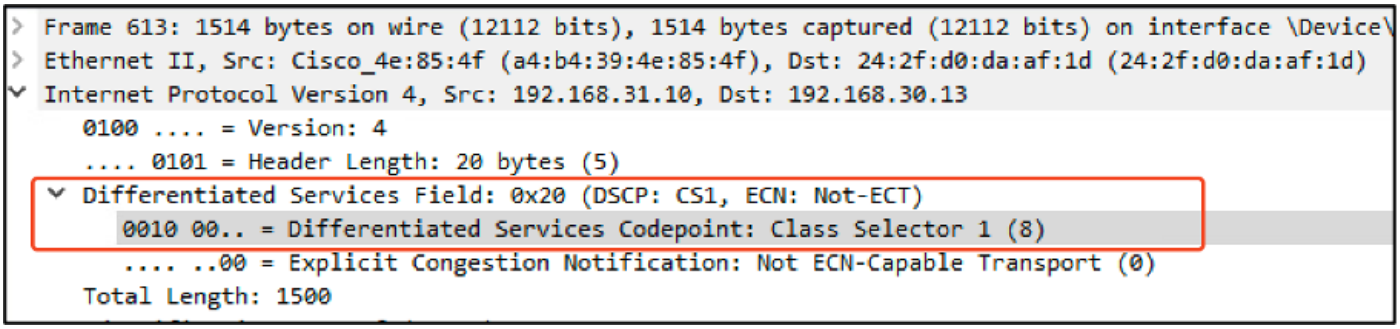
- L'en-tête CAPWAP externe est étiqueté avec CS1 (DSCP 8).
- L'en-tête CAPWAP interne est également étiqueté avec CS1 (DSCP 8).

- La valeur UP (priorité utilisateur) est définie sur BK (arrière-plan).



WLC EPC avec balise CS1 dans le trafic CAPWAP

Le paquet arrive au PC sans fil avec une valeur DSCP de CS1 (DSCP 8).



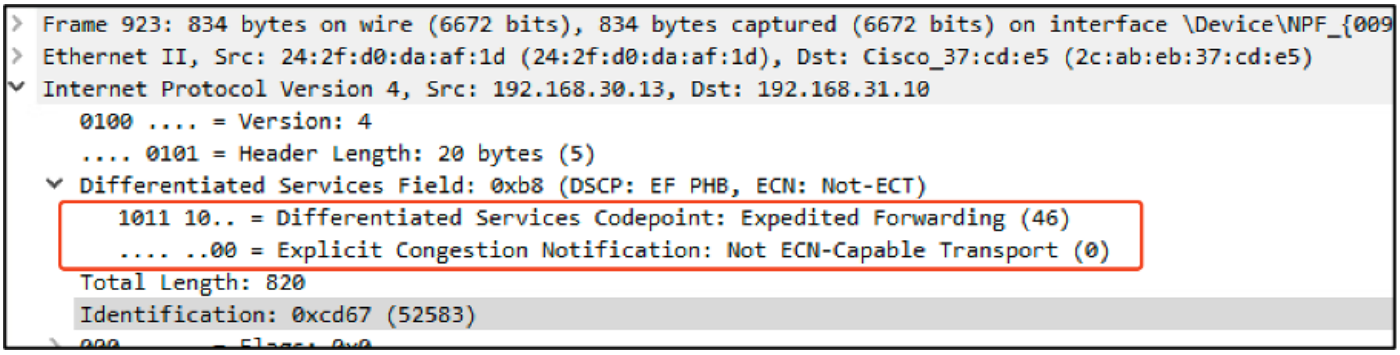
Capture de PC sans fil avec marquage CS1

Ce scénario montre comment une mauvaise configuration sur un commutateur intermédiaire peut rompre la configuration QoS, ce qui entraîne une dégradation des performances pour le trafic de priorité élevée. Les paquets vocaux, initialement marqués pour une priorité élevée, ont été traités comme du trafic de priorité inférieure en raison de la réécriture DSCP. Ce scénario souligne l'importance de s'assurer que les périphériques réseau intermédiaires conservent correctement les marquages QoS afin de maintenir la qualité de service souhaitée pour le trafic hautement prioritaire.

Scénario 2 : le commutateur de liaison AP réécrit le marquage DSCP

Dans ce scénario, l'impact d'un commutateur intermédiaire connecté au point d'accès réécrivant le marquage DSCP sur le trafic est examiné.

- Le commutateur connecté au point d'accès est configuré pour réécrire le marquage DSCP 46 sur une valeur différente CS1 sur l'interface de liaison ascendante du point d'accès.
- Le paquet est envoyé à partir du PC câblé avec une balise DSCP de 46. Cela confirme que le trafic est correctement marqué avec DSCP 46 à la source.

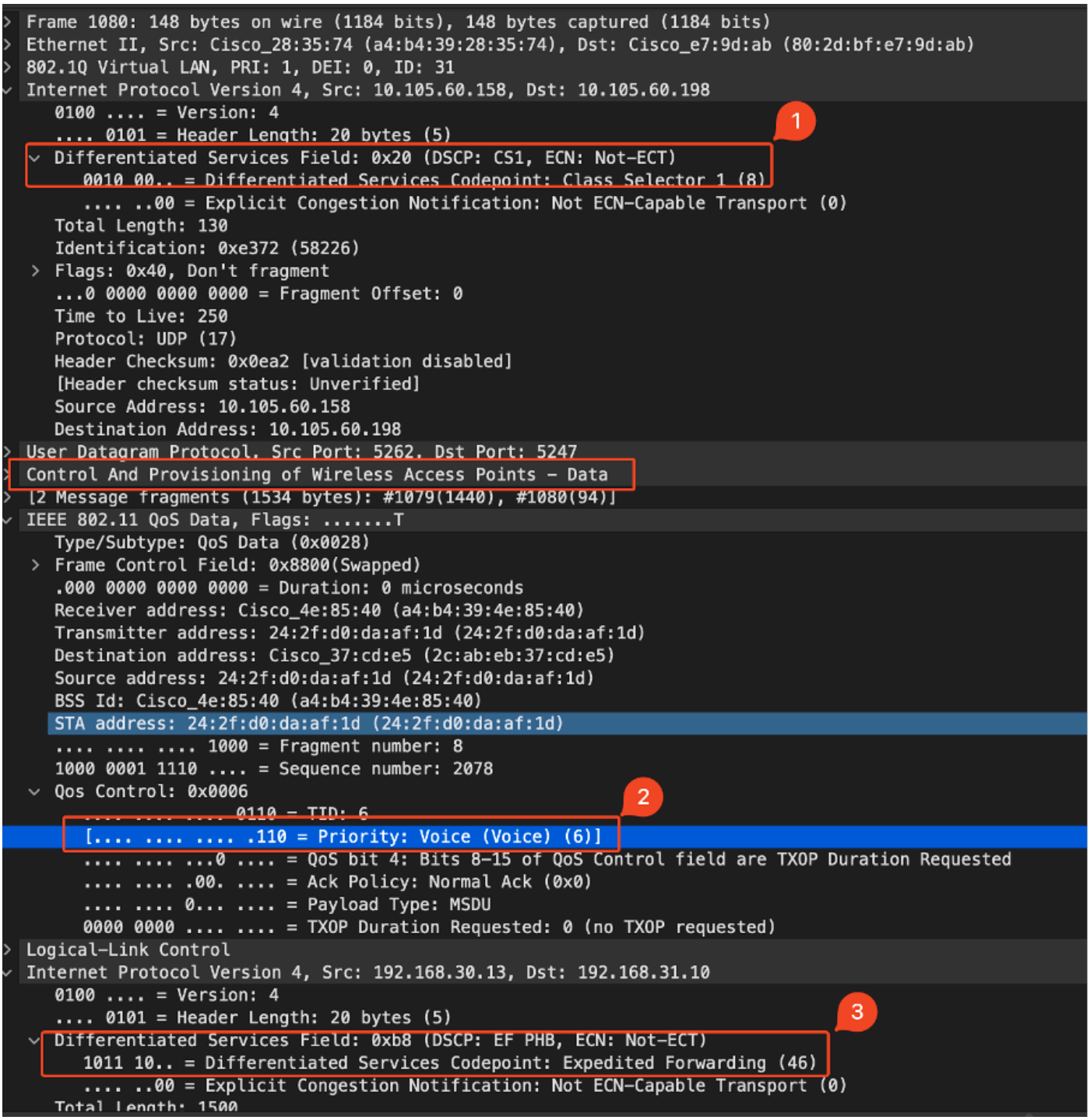


Capture de PC sans fil montrant DSCP 46

La capture est effectuée au niveau du WLC lorsque le paquet arrive du commutateur.

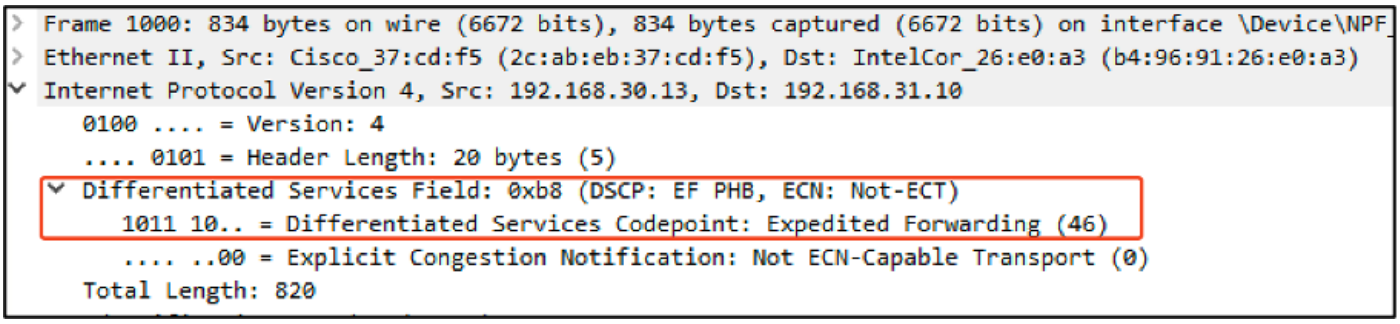
Le paquet arrive au WLC avec la valeur DSCP de l'en-tête CAPWAP externe de CS1 (DSCP) et la valeur DSCP interne de 46. Cela se produit parce que le commutateur intermédiaire ne peut pas voir le trafic encapsulé à l'intérieur du tunnel CAPWAP.

Le WLC fait confiance à l'étiquette DSCP à l'intérieur du tunnel CAPWAP et transfère le trafic vers le PC filaire avec l'étiquette DSCP interne de 46.



WLC EPC montrant les valeurs CAPWAP DSCP

Le paquet arrive au PC filaire avec une valeur DSCP de 46. Confirme que le WLC transfère correctement le paquet avec la valeur DSCP d'origine de 46, en préservant le marquage de priorité élevée.



Le PC filaire a reçu le paquet avec DSCP 46

Bien que le WLC ait transmis le trafic avec une balise DSCP de 46, il est important de comprendre que le trafic du point d'accès au WLC a été traité comme une priorité faible en raison de la réécriture de la balise DSCP externe sur CS1 (DSCP 8).

Il peut y avoir plusieurs commutateurs entre le point d'accès et le WLC, et si le trafic a une faible priorité, il peut arriver au WLC en retard. Cela peut entraîner une augmentation de la latence, de la gigue et de la perte potentielle de paquets, ce qui peut dégrader la qualité de service pour le trafic de haute priorité tel que la voix.

Conseil de dépannage

1. Vérification du marquage DSCP initial : capture des paquets à la source (par exemple, un PC câblé) pour s'assurer que le trafic est correctement marqué avec la valeur DSCP prévue.
2. Vérifier les configurations des périphériques intermédiaires : Examinez la configuration de tous les commutateurs et routeurs intermédiaires pour vous assurer qu'ils ne réécrivent pas par inadvertance des valeurs DSCP.
3. Capturer le trafic aux points clés :
    1. Avant et après le commutateur intermédiaire.
    2. Au niveau du WLC.
    3. À la destination (par exemple, un PC sans fil).
4. Simuler des scénarios de trafic : utilisez des générateurs de trafic ou des outils de simulation de réseau pour créer différents types de trafic et observer comment la qualité de service est gérée par le réseau sans fil.
5. Consultez le document des meilleures pratiques du 9800 : Consultez la documentation des meilleures pratiques du 9800 sur la configuration des marquages QoS et DSCP.

Vérification de la configuration

<#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
```

Conclusion

Le maintien d'une configuration QoS cohérente sur l'ensemble du réseau est essentiel pour garantir que le trafic hautement prioritaire, comme la voix et la vidéo, reçoive le niveau de service et de performances approprié. Il est essentiel de valider régulièrement les configurations QoS pour s'assurer que tous les périphériques réseau respectent les politiques QoS prévues. Cette validation permet d'identifier et de corriger toute erreur de configuration ou tout écart susceptible de compromettre les performances du réseau.

Références

- Présentation et dépannage des contrôleurs sans fil Cisco Catalyst 9800
- Meilleures pratiques de configuration de la gamme Cisco Catalyst 9800
- Guide de configuration du logiciel du contrôleur sans fil Cisco Catalyst 9800, Cisco IOS® XE Dublin 17.12.x
- Guide de dépannage VoWLAN (Voice Over Wireless LAN)
- Activer le marquage QoS DSCP sur les ordinateurs Windows

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.