# Configurazione della convalida e della risoluzione dei problemi di QoS wireless su 9800 WLC

## Sommario



## Introduzione

Questo documento descrive come configurare, convalidare e risolvere i problemi di QoS (Wireless Quality of Service) su controller WLC (9800 Wireless LAN Controller).

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- WLC: C9800-40-K9 con esecuzione il 17.12.03
- Access Point (AP): C9120-AX-D
- Switch: C9300-48P con versione 17.03.05
- Client cablati e wireless: Windows 10

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

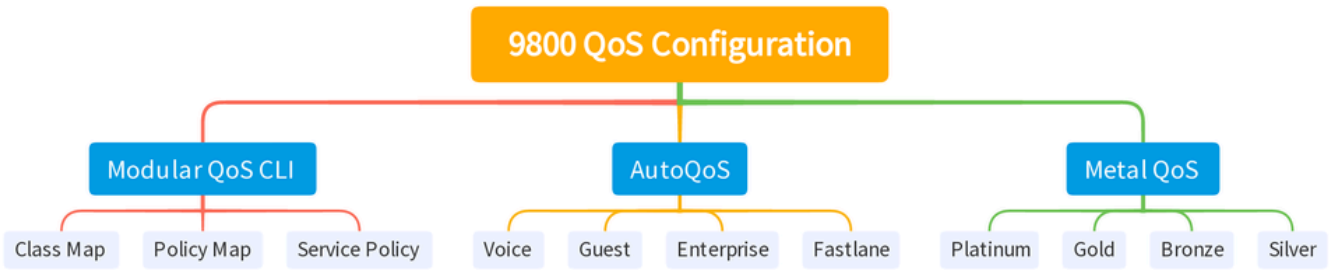
QoS wireless è essenziale per garantire che le applicazioni critiche ricevano la larghezza di banda necessaria e la bassa latenza necessaria per prestazioni ottimali. Questo documento offre una guida completa alla configurazione, convalida e risoluzione dei problemi QoS sulle reti wireless Cisco.

In questo articolo si presume che i lettori abbiano una conoscenza di base dei principi QoS sia wireless che cablata. Si prevede inoltre che i lettori siano esperti nella configurazione e nella gestione dei Cisco WLC e AP.

## Configurazione

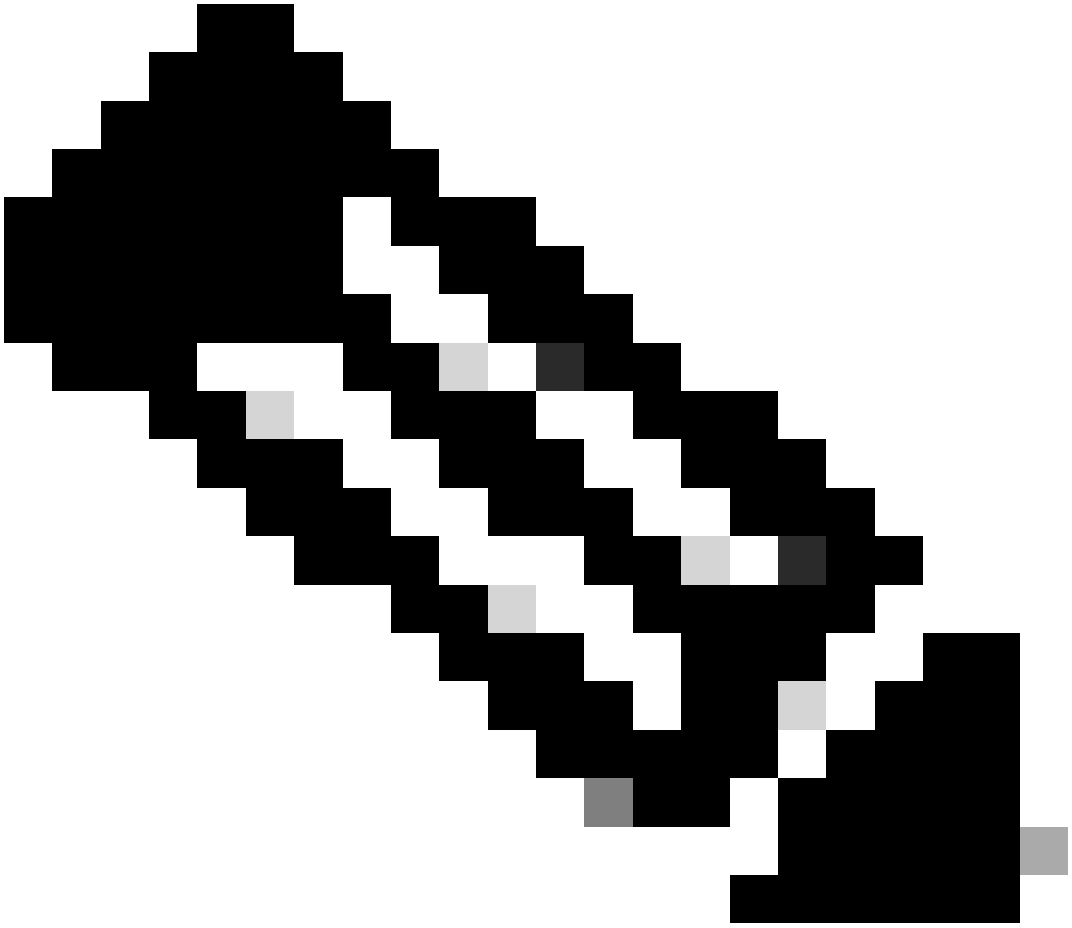
In questa sezione viene descritta la configurazione di QoS sui controller wireless 9800. Sfruttando queste configurazioni, è possibile garantire che le applicazioni critiche ricevano la larghezza di banda necessaria e una bassa latenza, ottimizzando in tal modo le prestazioni complessive della rete.

È possibile dividere la configurazione QoS del WLC 9800 in tre diverse categorie generali.




Riepilogo della configurazione QOS 9800 WLC

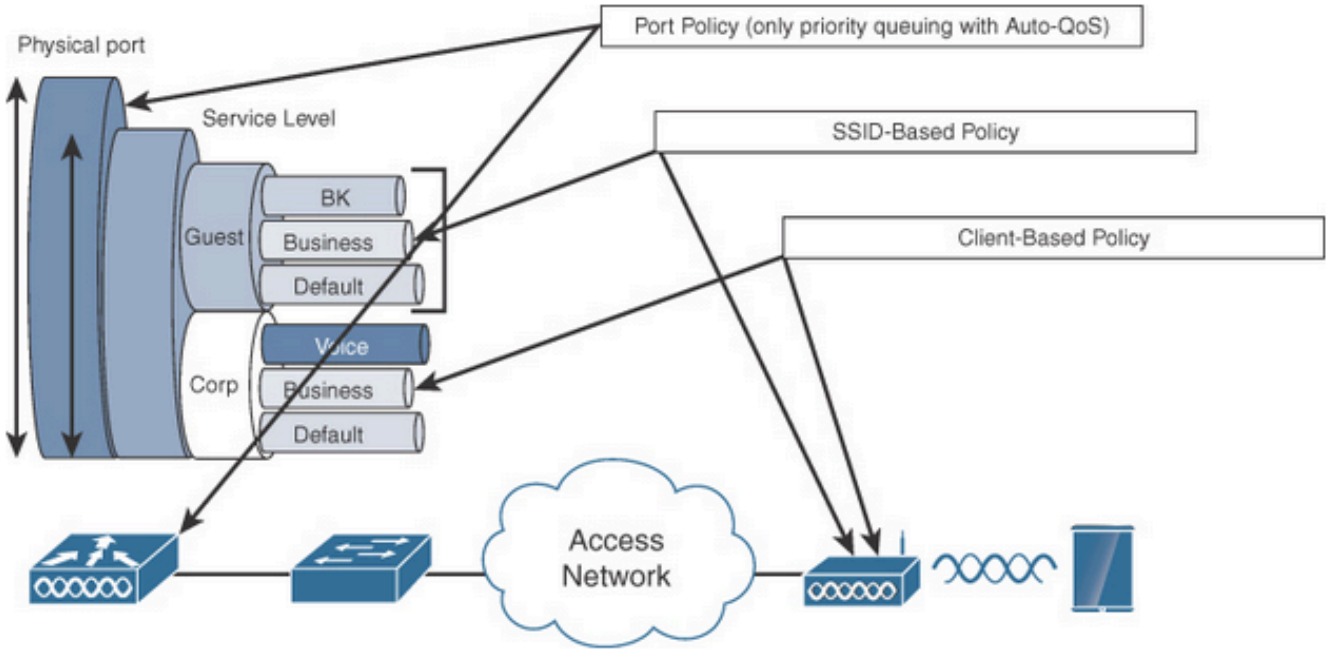
Questo documento scorre ciascuna sezione una alla volta nelle sezioni successive.



Nota: in questo articolo il punto di accesso è in modalità locale. Il punto di accesso in modalità Flexconnect non viene discusso.

## Destinazioni criteri QoS

Una destinazione criterio è il costrutto di configurazione in cui è possibile applicare un criterio QoS. L'implementazione QoS su Catalyst 9800 è modulare e flessibile. L'utente può decidere di configurare i criteri a tre destinazioni diverse: SSID, client e porte.




Destinazioni criteri QoS

I criteri SSID sono applicabili per ogni punto di accesso per ogni SSID. È possibile configurare criteri di policy e contrassegni su SSID.

I criteri client sono applicabili in entrata e in uscita. È possibile configurare criteri di controllo e contrassegno sui client. Inoltre, è supportata l'override AAA.

Le policy QoS basate sulla porta possono essere applicate a una porta fisica o a una porta logica.

## QoS automatico

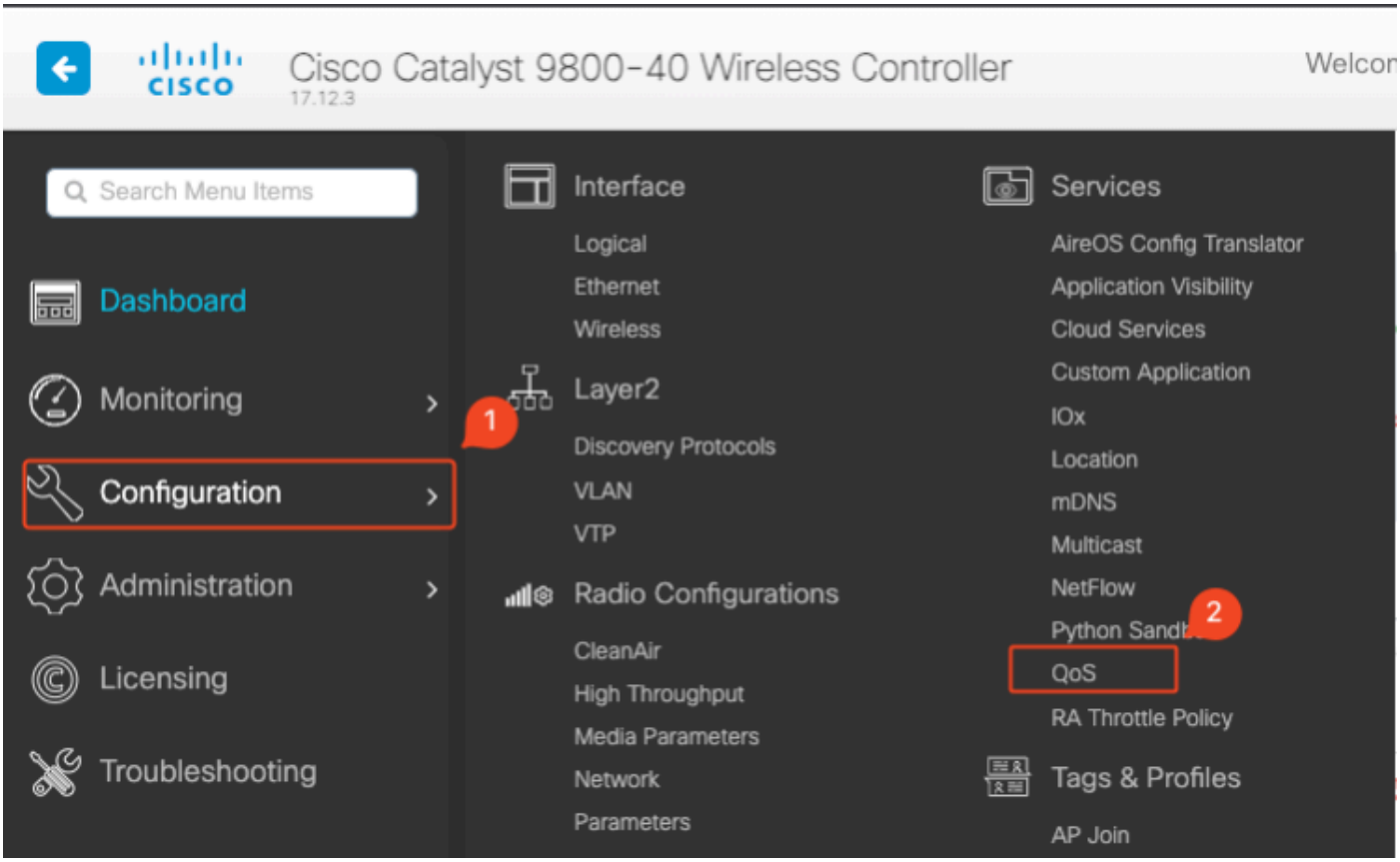
Wireless Auto QoS automatizza l'implementazione delle funzioni QoS wireless. Dispone di una serie di profili predefiniti che possono essere ulteriormente modificati dall'amministratore per assegnare la priorità ai diversi flussi di traffico. Auto-QoS associa il traffico e assegna ciascun pacchetto corrispondente ai gruppi QoS. Ciò consente alla mappa dei criteri di output di inserire gruppi QoS specifici in code specifiche, inclusa la coda di priorità.

| Modalità | Ingresso client | Uscita client | BSSID in ingresso | BSSID in uscita | Porta in ingresso | Uscita porta | Radio |
|---|---|---|---|---|---|---|---|
| Voce | N/D | N/D | platino | platino | N/D | AutoQos-4.0-wlan-Port-Output-Policy | ACM attivata |
| Guest | N/D | N/D | AutoQos-4.0-wlan-GT-SSID-Input-Policy | AutoQos-4.0-wlan-GT-SSID-Output-Policy | N/D | AutoQos-4.0-wlan-Port-Output-Policy | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Corsia | N/D | N/D | N/D | N/D | N/D | AutoQos-4.0-wlan-Port-Output-Policy | edca-parameters fastlane |
| Enterprise-avc | N/D | N/D | AutoQos-4.0-wlan-ET-SSID-Input-AVC-Policy | AutoQos-4.0-wlan-ET-SSID-Output-Policy | N/D | AutoQos-4.0-wlan-Port-Output-Policy | |

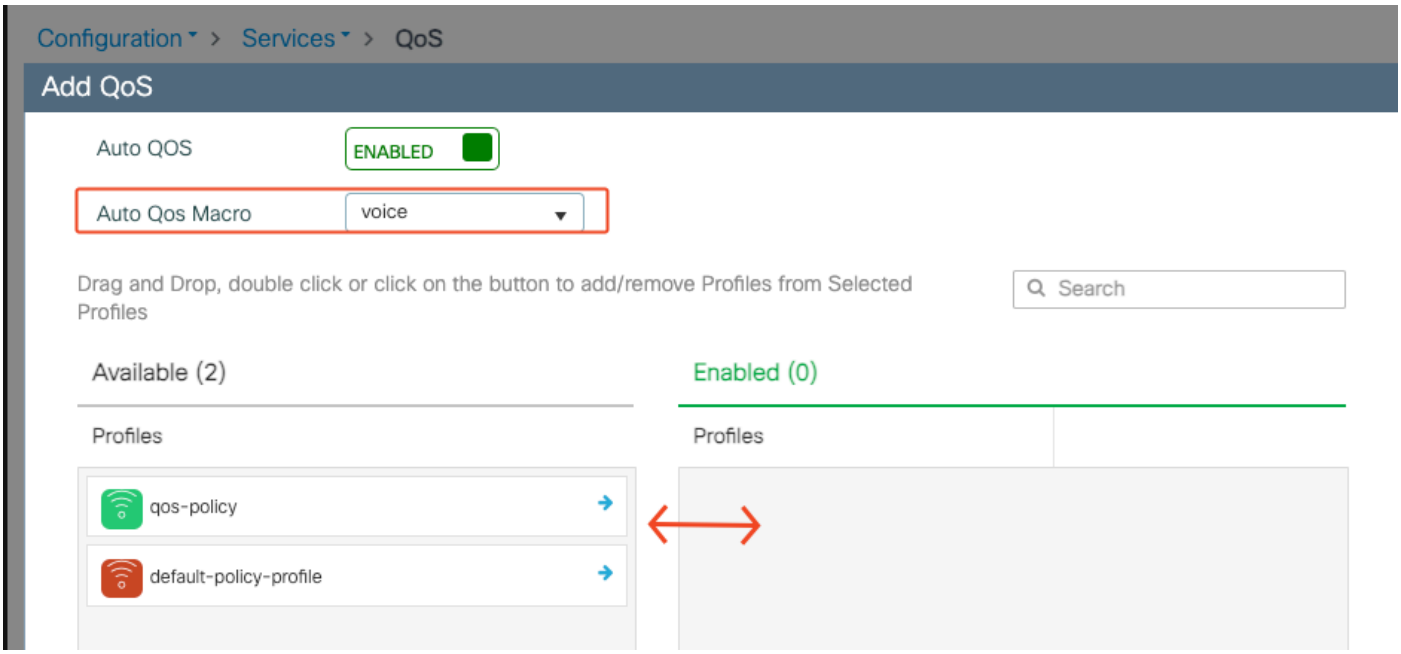
Questa tabella mostra le modifiche della configurazione che si verificano quando viene applicato un profilo QoS automatico.

Per configurare Auto QoS (QoS automatico) passare a Configuration > QoS (Configurazione > QoS)




Flusso di lavoro QoS

Fare clic su Add (Aggiungi) e impostare Auto QoS (QoS automatico) su Enabled (Abilitato). Selezionare la macro QoS automatica appropriata dall'elenco. In questo esempio, viene utilizzata una macro vocale per assegnare la priorità al traffico vocale.




AutoQoS Voice Mapping

Dopo aver attivato la macro, selezionare il criterio da associare al criterio.

## Configurazione automatica CLI QoS

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

Ora che Auto QoS è abilitato, è possibile vedere le modifiche che sono avvenute. In questa sezione vengono elencate le modifiche di configurazione per la voce.

```
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 modulare

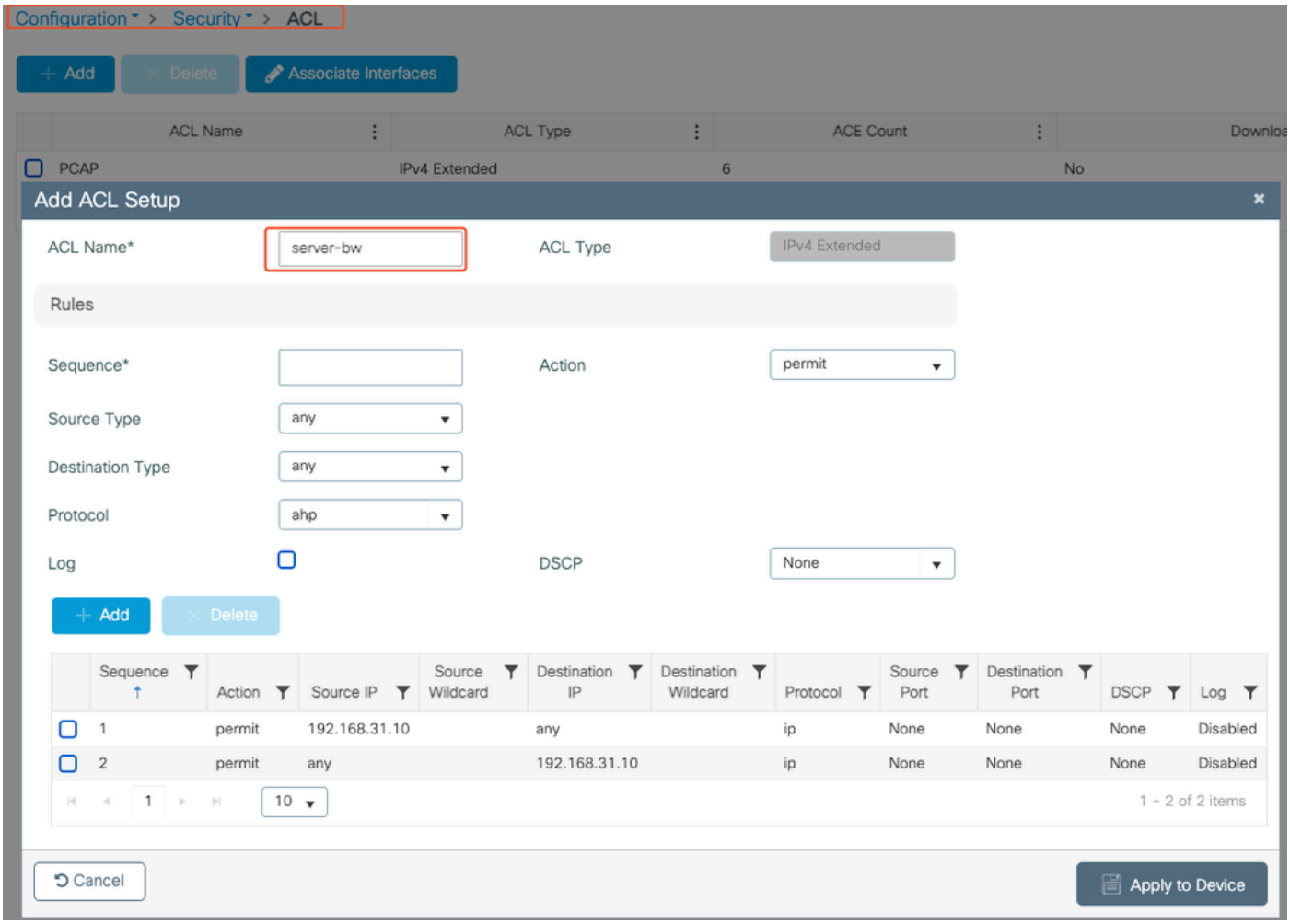
MQC consente di definire una classe di traffico, creare un criterio di traffico (mappa dei criteri) e collegarlo a un'interfaccia. I criteri del traffico contengono la funzionalità QoS che si applica alla classe del traffico.


Flusso di lavoro MQS CLI

Nell'esempio viene mostrato come usare gli Access Control Lists (ACL) per classificare il traffico e applicare le restrizioni alla larghezza di banda.

Creare un ACL per identificare e classificare il traffico specifico che si desidera gestire. A tale scopo, è possibile definire regole che soddisfino il traffico in base a criteri quali indirizzi IP, protocolli o porte.

Passare a Configurazione > Sicurezza > ACL e aggiungere l'ACL.

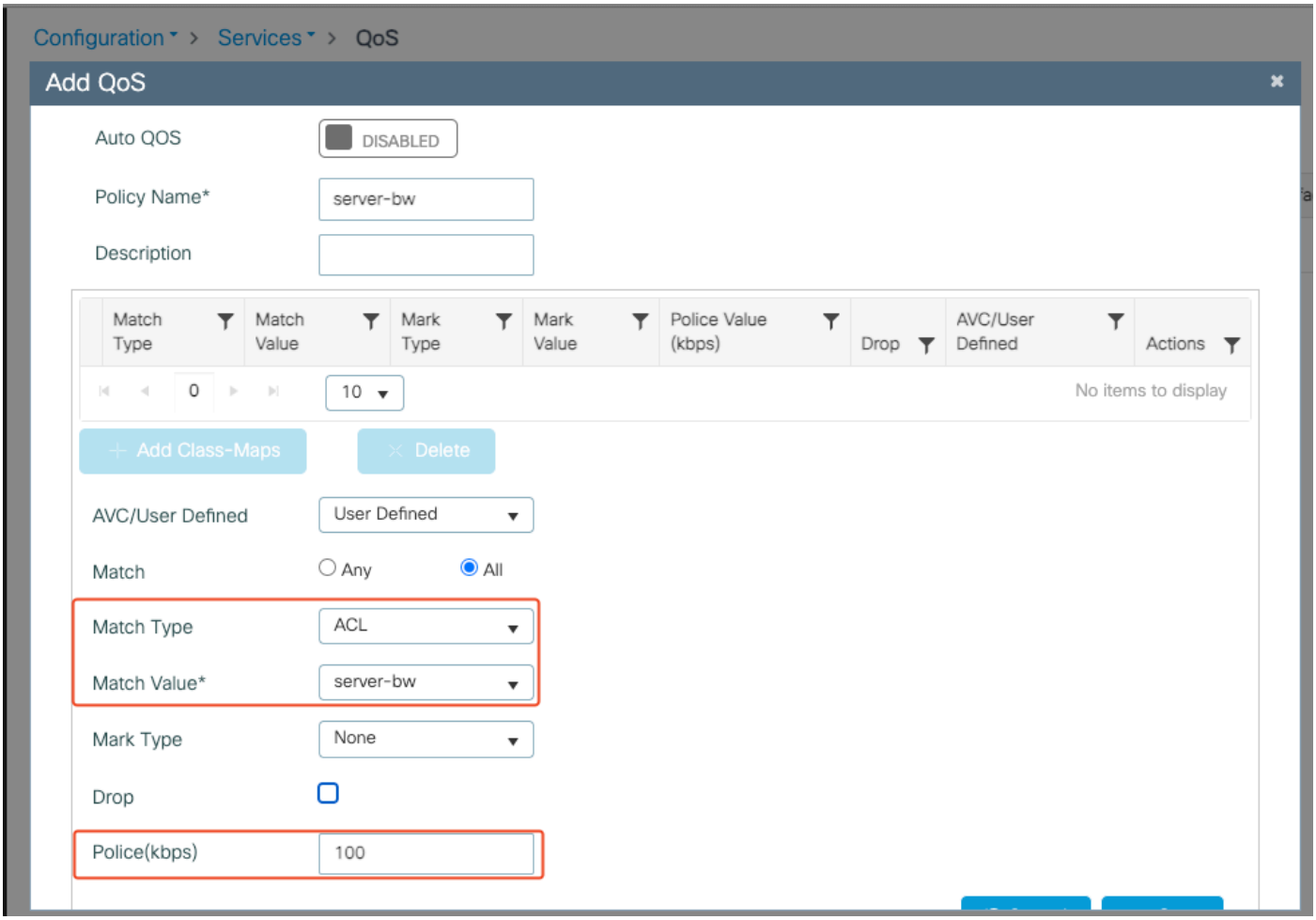



Configurazione ACL

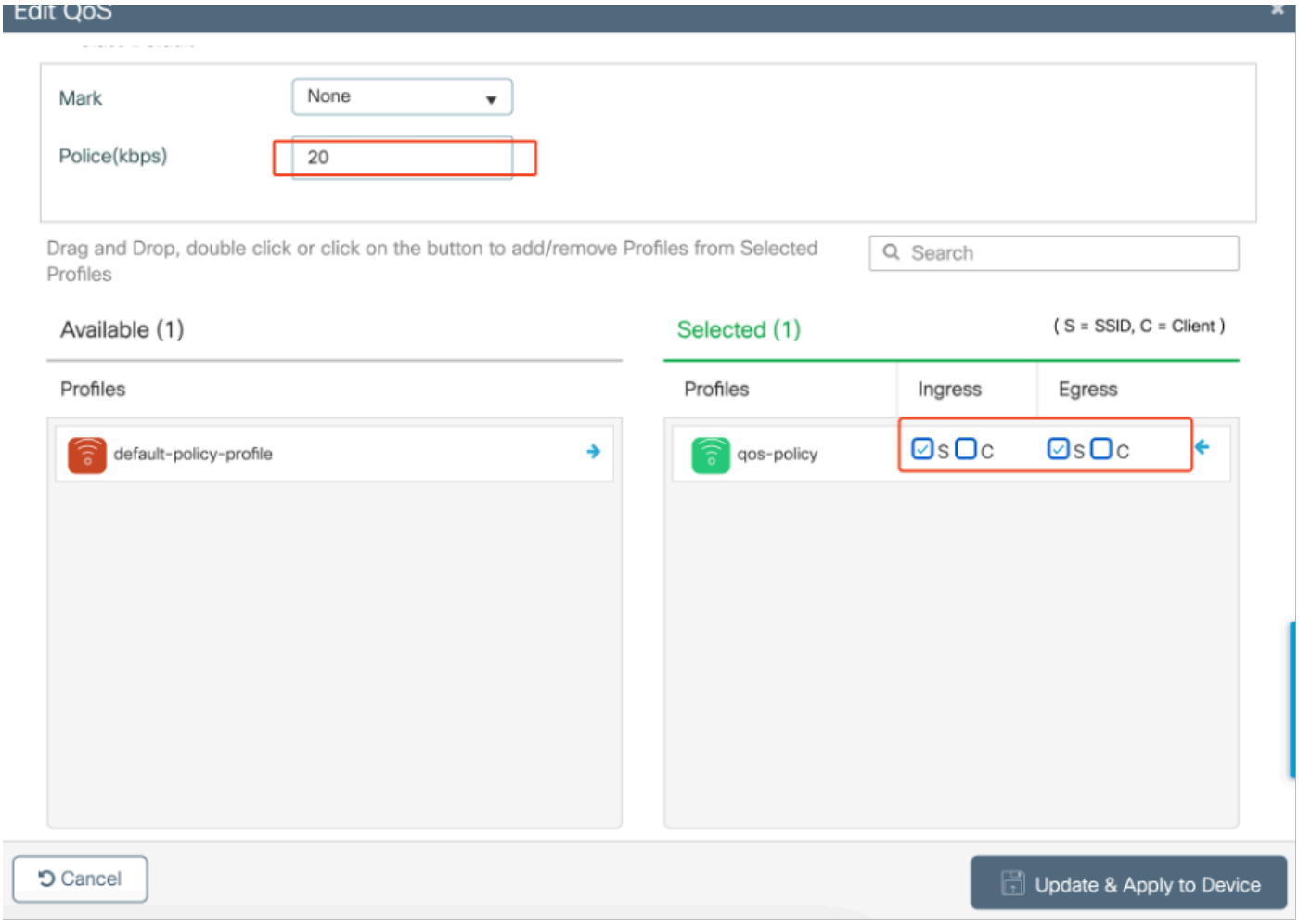
Dopo aver classificato il traffico con l'ACL, configurare le restrizioni della larghezza di banda per controllare la quantità di larghezza di banda allocata al traffico.

Selezionare Configurazione > Servizi > QoS e il criterio QoS. Collegare l'ACL all'interno della policy e applicare la polizia in kbps.

Scorrere verso il basso e selezionare il profilo dei criteri a cui applicare QoS. È possibile selezionare il criterio in entrata/uscita sia per SSID che per Client.


Configuration > Services > QoS
Add QoS
Auto QOS
DISABLED
Policy Name*
server-bw
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
User Defined
Match
Any
All
Match Type
ACL
Match Value*
server-bw
Mark Type
None
Drop
Police(kbps)
100

Criteri MQS




Profilo MQS

## Configurazione 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 metallo

Lo scopo principale di questi profili QoS è quello di limitare i valori DSCP (Differentiated Services Code Point) massimi consentiti su una rete wireless, controllando in tal modo i valori 802.11 User Priority (UP).

Nel Cisco 9800 Wireless LAN Controller (WLC), i profili Metal QoS sono predefiniti e non configurabili. Tuttavia, è possibile applicare questi profili a SSID o client specifici per applicare i criteri QoS.

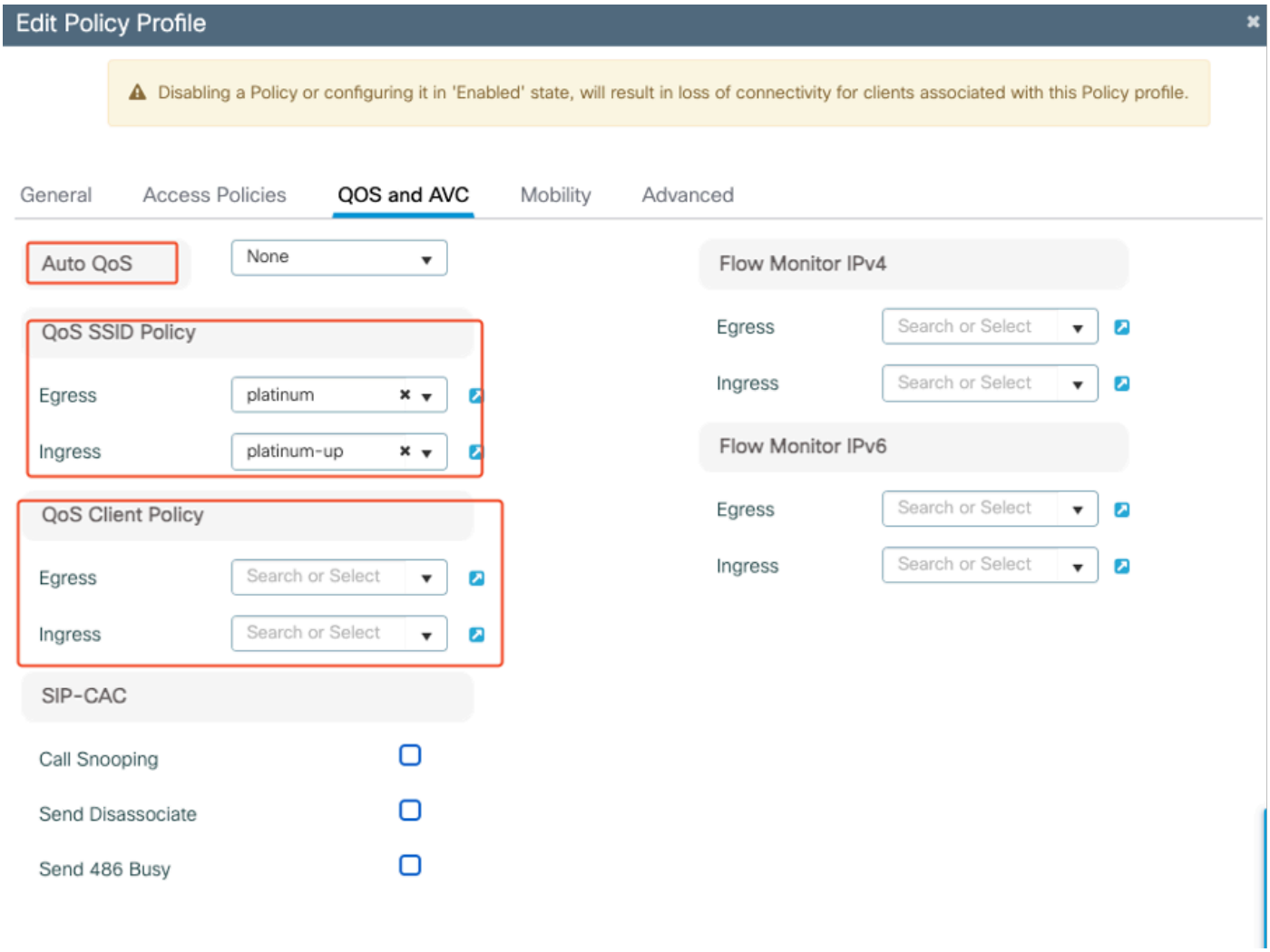
Sono disponibili quattro profili Metal QoS:

| Profilo Qos | DSCP max |
|---|---|
| Bronzo | 8 |
| Argento | 0 |
| Oro | 34 |
| Platino | 46 |

Per configurare Metal QoS su un Cisco 9800 WLC:

Selezionare Configurazione > Criteri > QoS e AVC.

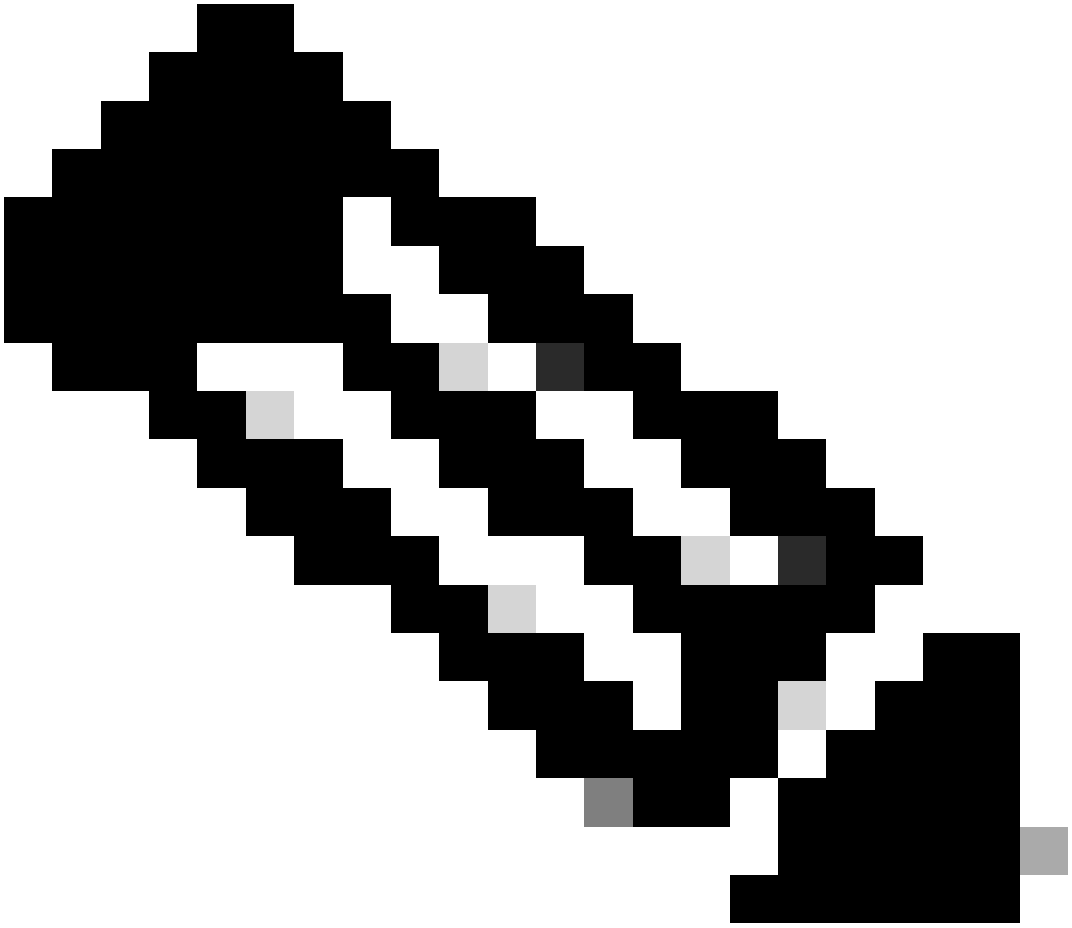
- Selezionare il profilo QoS Metal desiderato (Platinum, Gold, Silver o Bronze).
- Applicare il profilo scelto al client o all'SSID di destinazione.



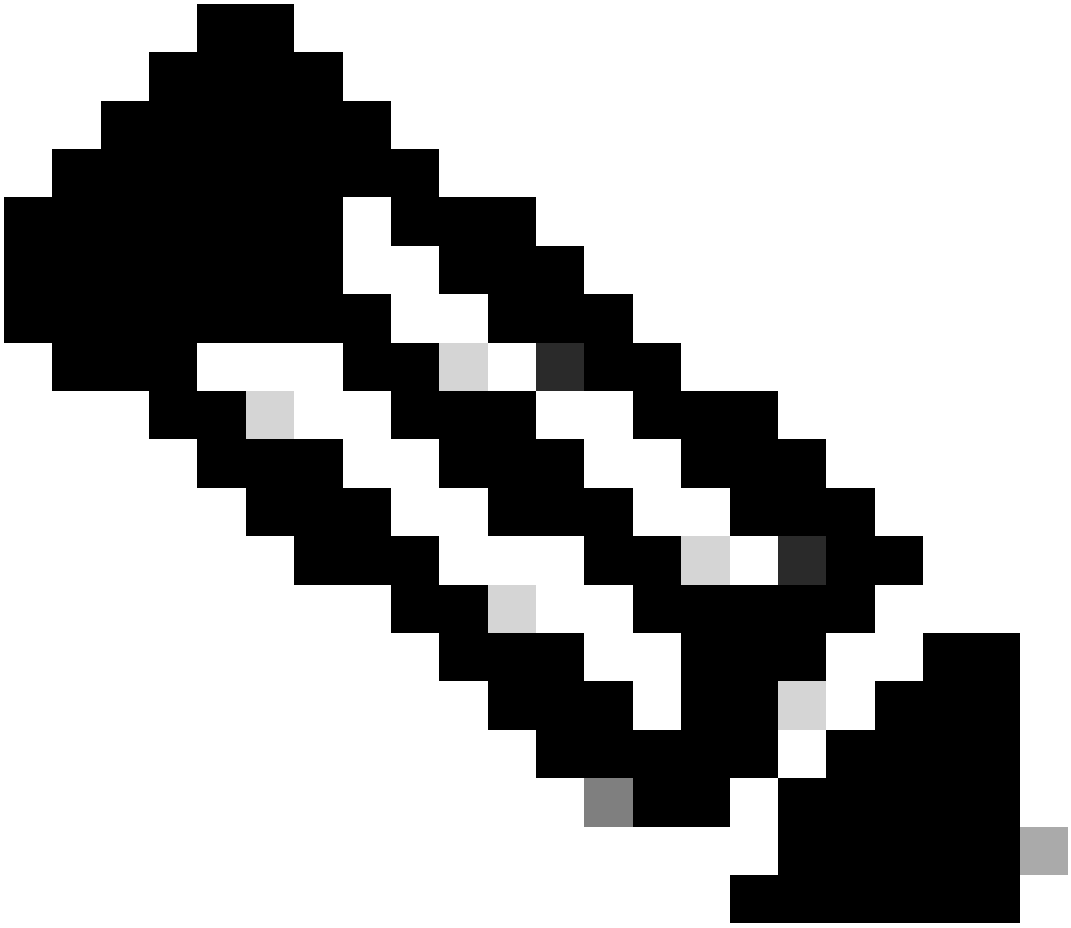

Profilo QoS metallico

## Configurazione CLI QoS Metal

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



Nota: i contratti per utente e larghezza di banda SSID sono configurabili tramite criteri QoS e non direttamente sul QoS Metal. Nello switch 9800 il traffico non corrispondente viene classificato nella classe predefinita.



Nota: sulla GUI, è possibile impostare solo la QoS Metal per SSID. Dalla CLI è possibile anche configurarlo sulla destinazione client.

## Convalida di QoS end-to-end con acquisizione pacchetti

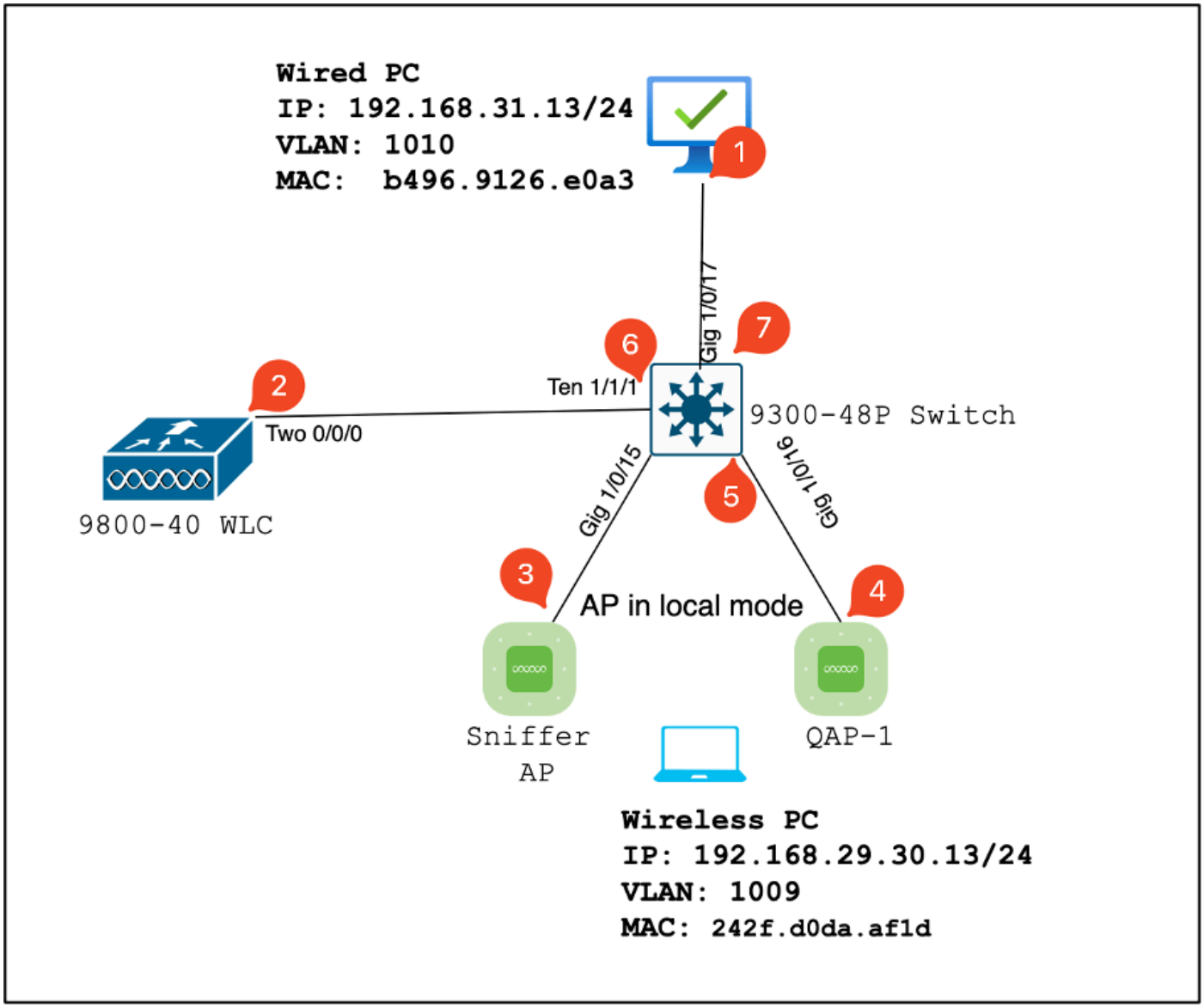
Ora che la configurazione QoS è stata completata, è essenziale esaminare i pacchetti QoS e verificare che i criteri QoS funzionino correttamente. Questo può essere ottenuto attraverso l'acquisizione e l'analisi dei pacchetti.

Per replicare e convalidare la configurazione QoS, viene utilizzato un ambiente lab su piccola scala. L'esercitazione comprende i seguenti componenti:

- WLC
- AP
- Sniffer AP per prendere OTA
- PC cablato
- Interruttore

Tutti questi componenti sono collegati allo stesso switch all'interno dell'ambiente lab. I numeri evidenziati in questo diagramma indicano i punti in cui le acquisizioni dei pacchetti sono abilitate per monitorare e analizzare il flusso del traffico.

## Esempio di rete




Topologia LAB

## Componenti Lab e punti di acquisizione del pacchetto

WLC:

- Gestisce le policy e le configurazioni QoS per la rete wireless.
- Punto di acquisizione del pacchetto: acquisire il traffico tra il WLC, il punto di accesso e lo switch.

Punto di accesso:

- Fornisce connettività wireless ai client e applica i criteri QoS.

- Punto di acquisizione del pacchetto: acquisire il traffico tra il punto di accesso e lo switch.

Sniffer AP:

- Funge da dispositivo dedicato per l'acquisizione del traffico wireless.
- Punto di acquisizione pacchetto: consente di acquisire il traffico wireless tra il punto di accesso e i client wireless.

PC cablato:

- Collegato allo switch per simulare il traffico cablato e convalidare la funzionalità QoS end-to-end.
- Punto di acquisizione del pacchetto: acquisizione dei pacchetti QoS trasmessi e ricevuti su un collegamento cablato.

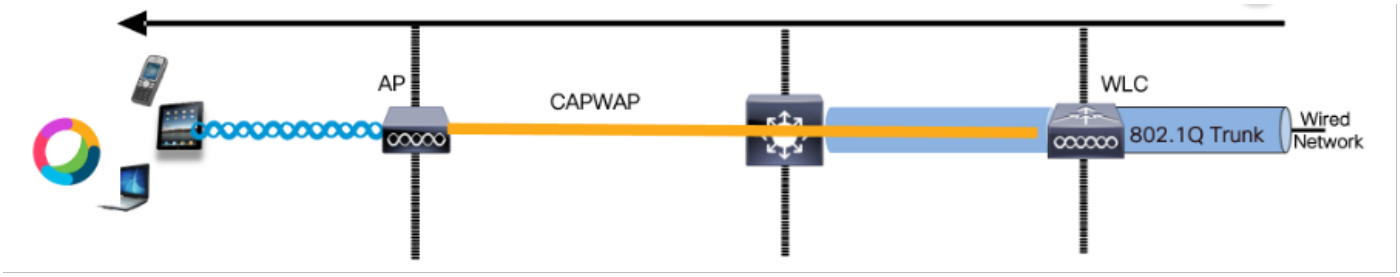
PC wireless:

- Connesso alla WLAN per simulare il traffico wireless e convalidare la funzionalità QoS end-to-end.
- Punto di acquisizione del pacchetto: consente di acquisire pacchetti QoS trasmessi e ricevuti tramite collegamento wireless.

Interruttore:

- Il dispositivo centrale che interconnette tutti i componenti lab e facilita il flusso del traffico.
- Punti di acquisizione del pacchetto: acquisizione del traffico a varie porte dello switch per convalidare la corretta applicazione QoS.

Logicamente, la topologia LAB può essere disegnata in questo modo.




Topologia Logical LAB

Per verificare e convalidare la configurazione QoS, viene utilizzato iPerf per generare traffico tra il client e il server. Questi comandi vengono utilizzati per facilitare la comunicazione iPerf, con lo scambio dei ruoli del server e del client in base alla direzione del test QoS.

## Scenario di test 1: convalida QoS downstream

Lo scopo è convalidare la configurazione QoS a valle. La configurazione prevede l'invio di pacchetti con DSCP 46 da un PC cablato a un PC wireless.
Il controller WLC (Wireless LAN Controller) è configurato con la policy Metal "Platinum QoS" sia

per le direzioni a valle che a monte.

Configurazione test:

- Flusso traffico:

  Fonte: PC cablato

  Destinazione: PC wireless

  Tipo di traffico: pacchetti UDP con DSCP 46

- Configurazione dei criteri QoS sul WLC:

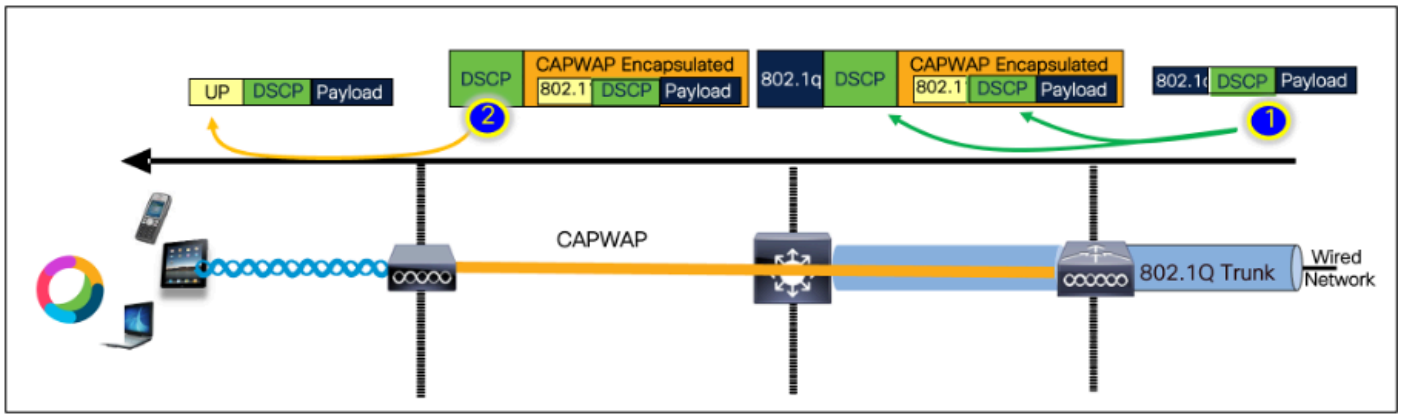
  Profilo QoS: QoS metallico - QoS Platinum

  Direzione: sia a valle che a monte

- Comandi di configurazione QoS metal:

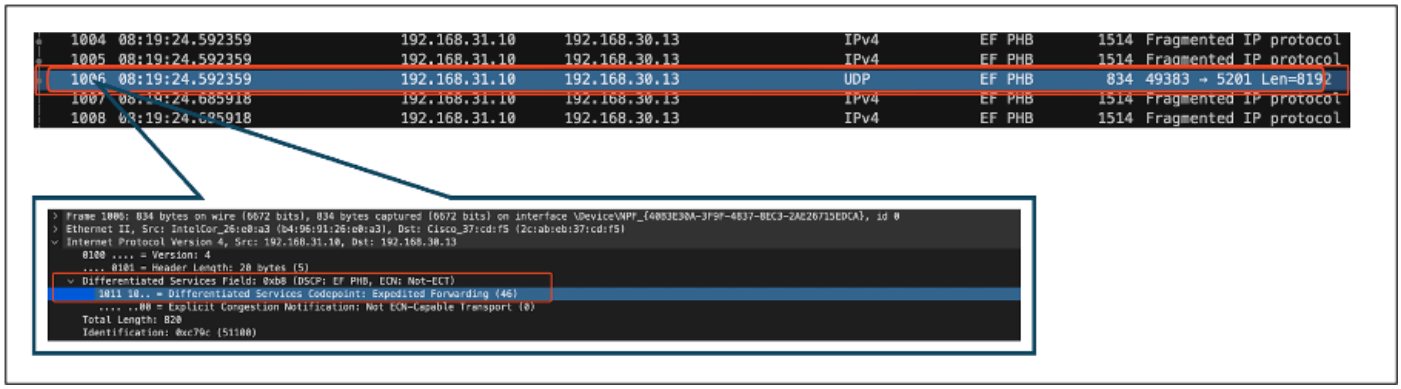
```
wireless profile policy qos-policy
service-policy input platinum-up
service-policy output platinum
```

Topologia logica e conversazione DSCP nella direzione a valle.




Punto di conversazione DSCP

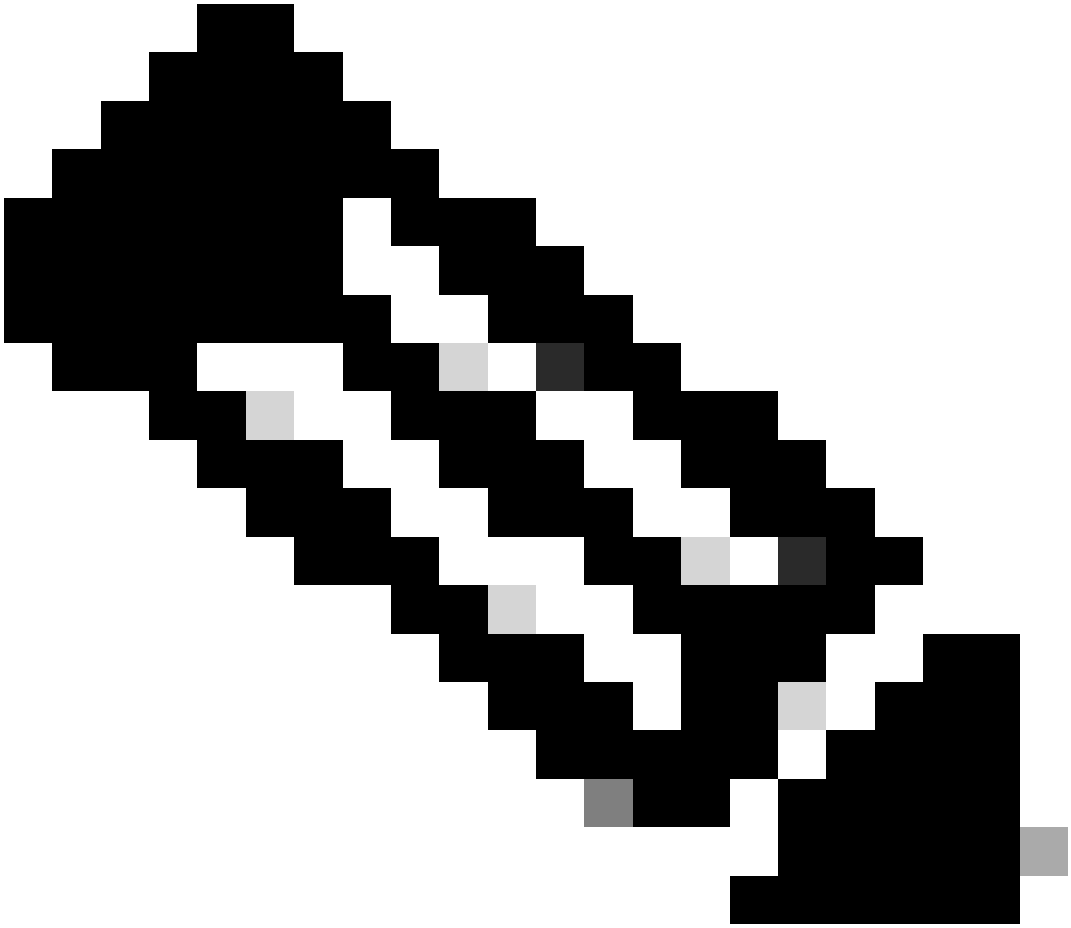
Acquisizione di pacchetti sul PC cablato. Ciò conferma che il PC cablato sta inviando i pacchetti UDP alla destinazione IP 192.168.10.13 specificata con il contrassegno DSCP corretto di 46.




Acquisizione da PC con cavo - Direzione downstream

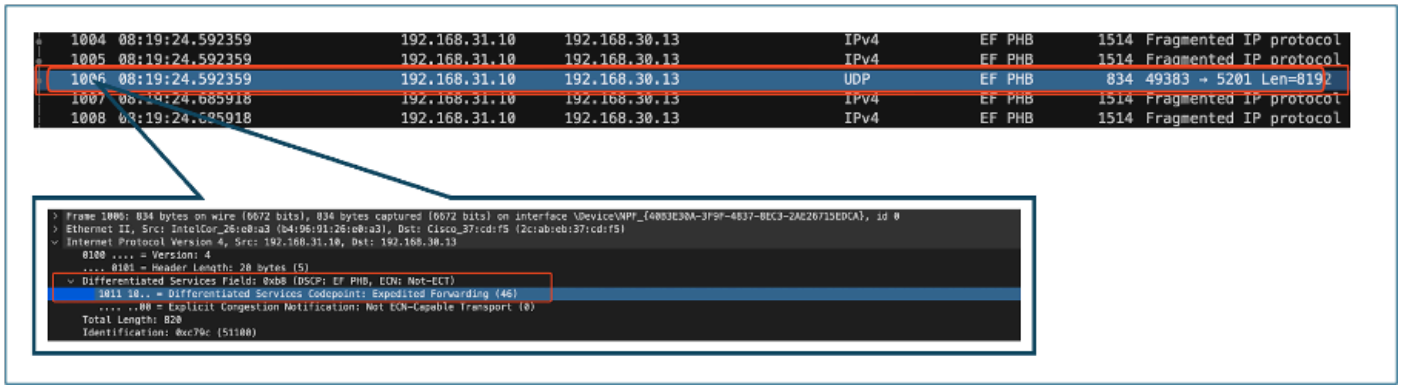
Esaminiamo quindi un pacchetto acquisito sullo switch uplink collegato al PC cablato. Lo switch considera attendibile il tag DSCP e il valore DSCP rimane invariato a 46.

---



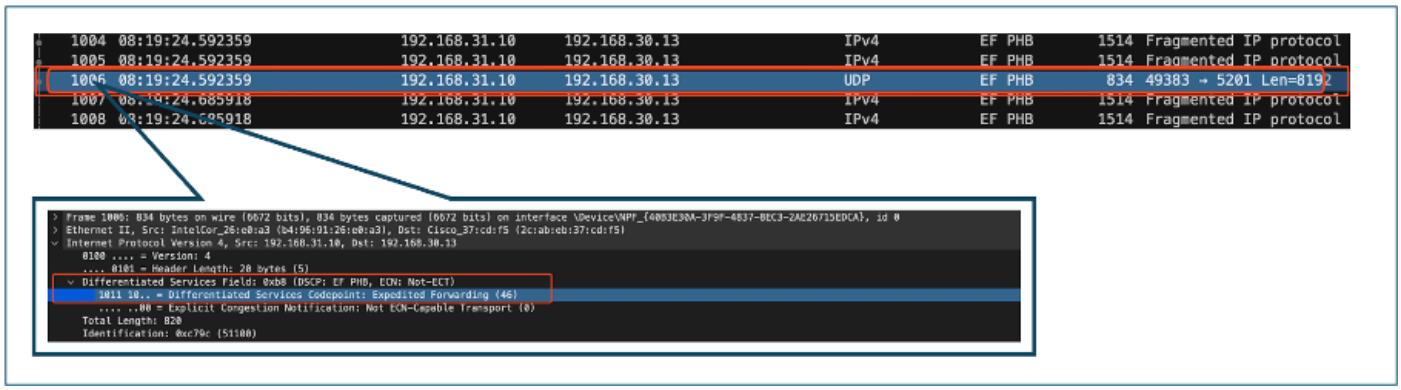
Nota: per impostazione predefinita, le porte degli switch in Catalyst serie 9000 sono impostate su uno stato trusted.

---




Acquisizione interfaccia uplink PC cablato

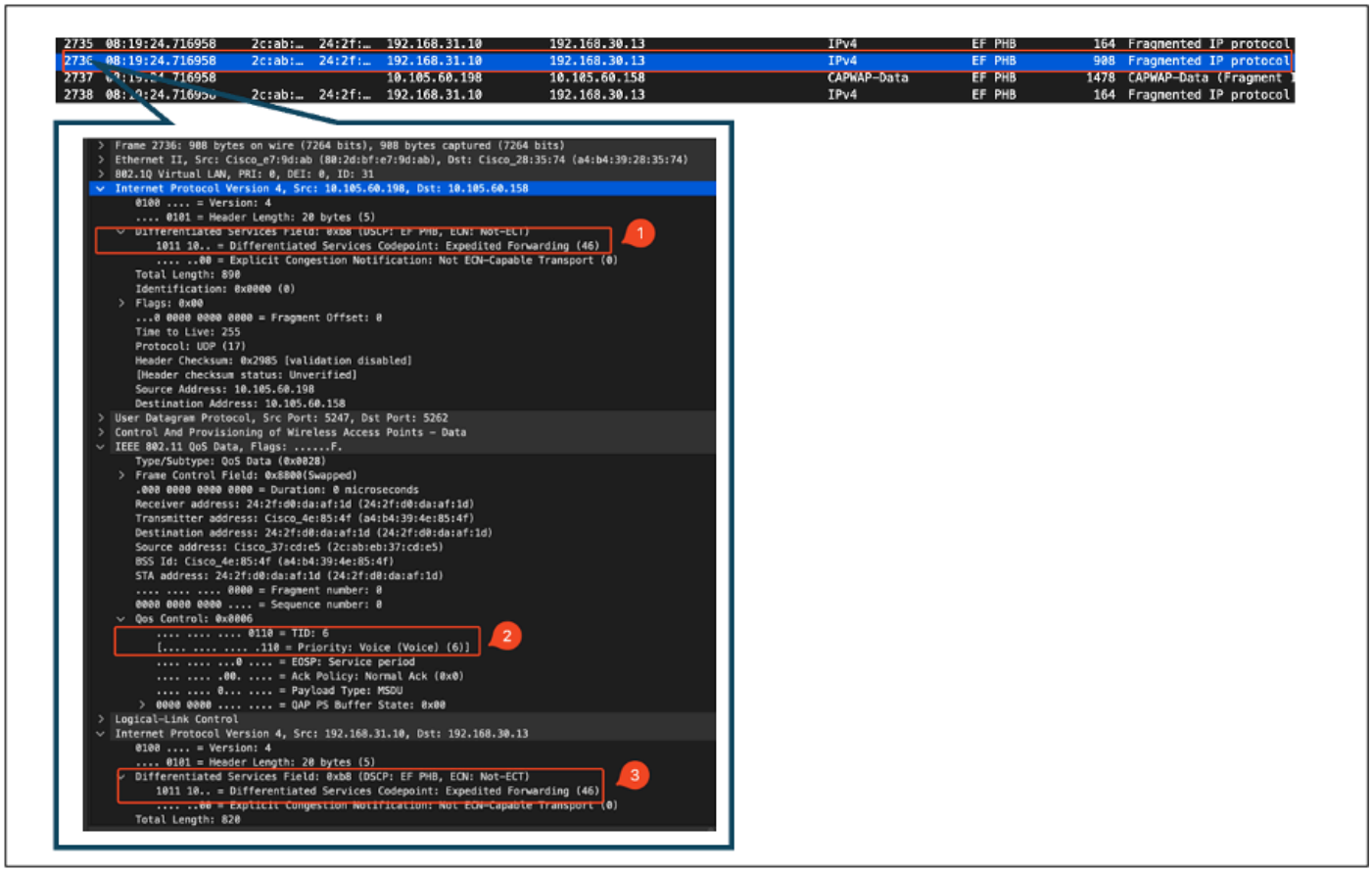
Dopo aver esaminato l'acquisizione del pacchetto sul WLC presa con EPC, il pacchetto arriva con lo stesso tag DSCP di 46 dallo switch uplink.  Ciò conferma che il contrassegno DSCP viene mantenuto quando il pacchetto raggiunge il WLC.




Direzione downstream EPC WLC

Quando il WLC invia il pacchetto all'access point all'interno di un tunnel CAPWAP, si tratta di un'intersezione critica in cui il WLC può modificare il DSCP in base alla sua configurazione. Suddividiamo l'acquisizione dei pacchetti, evidenziata con i punti numerati per maggiore chiarezza:

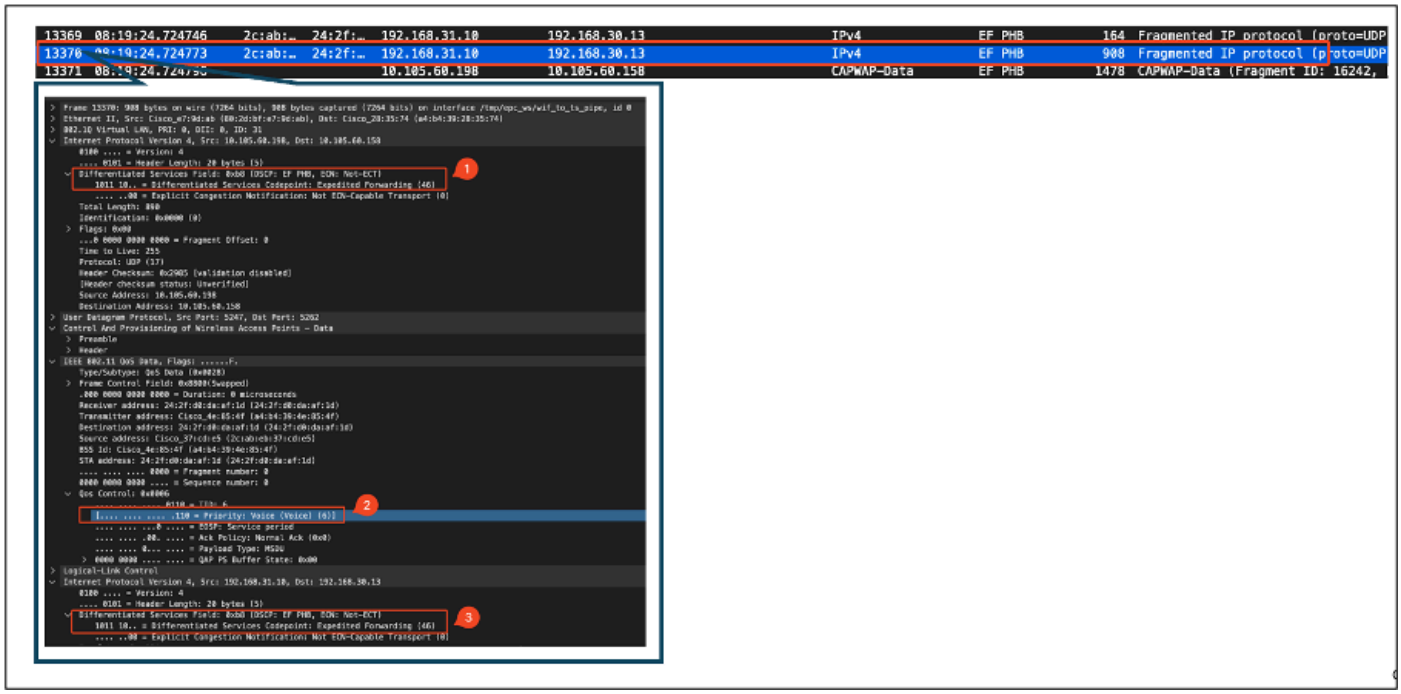
- CAPWAP Outer Layer: il layer esterno del tunnel CAPWAP visualizza il tag DSCP come 46, ossia il valore ricevuto dall'estremità dello switch.
- Valore 802.11 UP all'interno di CAPWAP: all'interno del tunnel CAPWAP, il WLC mappa il DSCP 46 alla priorità utente 802.11 (UP) 6, che corrisponde al traffico vocale.
- Valore DSCP all'interno di CAPWAP: il WLC di Cisco 9800 funziona con un modello DSCP di fiducia, quindi il valore DSCP all'interno del tunnel CAPWAP viene mantenuto su 46 come livello DSCP esterno.




Contrassegni DSCP CAPWAP

Quindi, controllare lo stesso pacchetto sulla porta dello switch di uplink AP.

Il valore DSCP sul livello CAPWAP esterno rimane 46. A scopo illustrativo, il traffico CAPWAP interno viene evidenziato per mostrare l'etichetta.

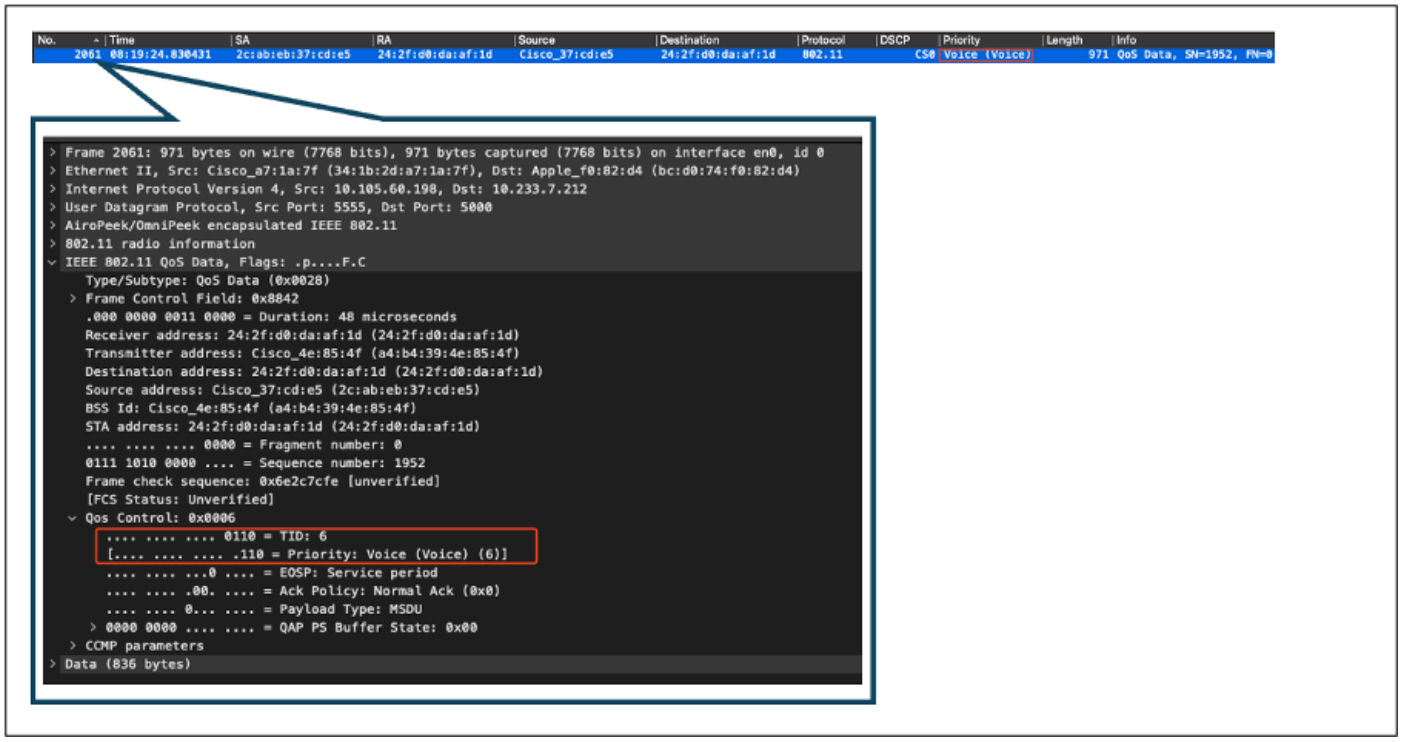



Acquisizione interfaccia switch uplink AP

Una volta ricevuto il pacchetto, l'access point lo trasmette via etere. Per verificare l'assegnazione

di tag Priorità utente (UP), viene utilizzata un'acquisizione OTA (Over-the-Air) eseguita con un access point sniffer.

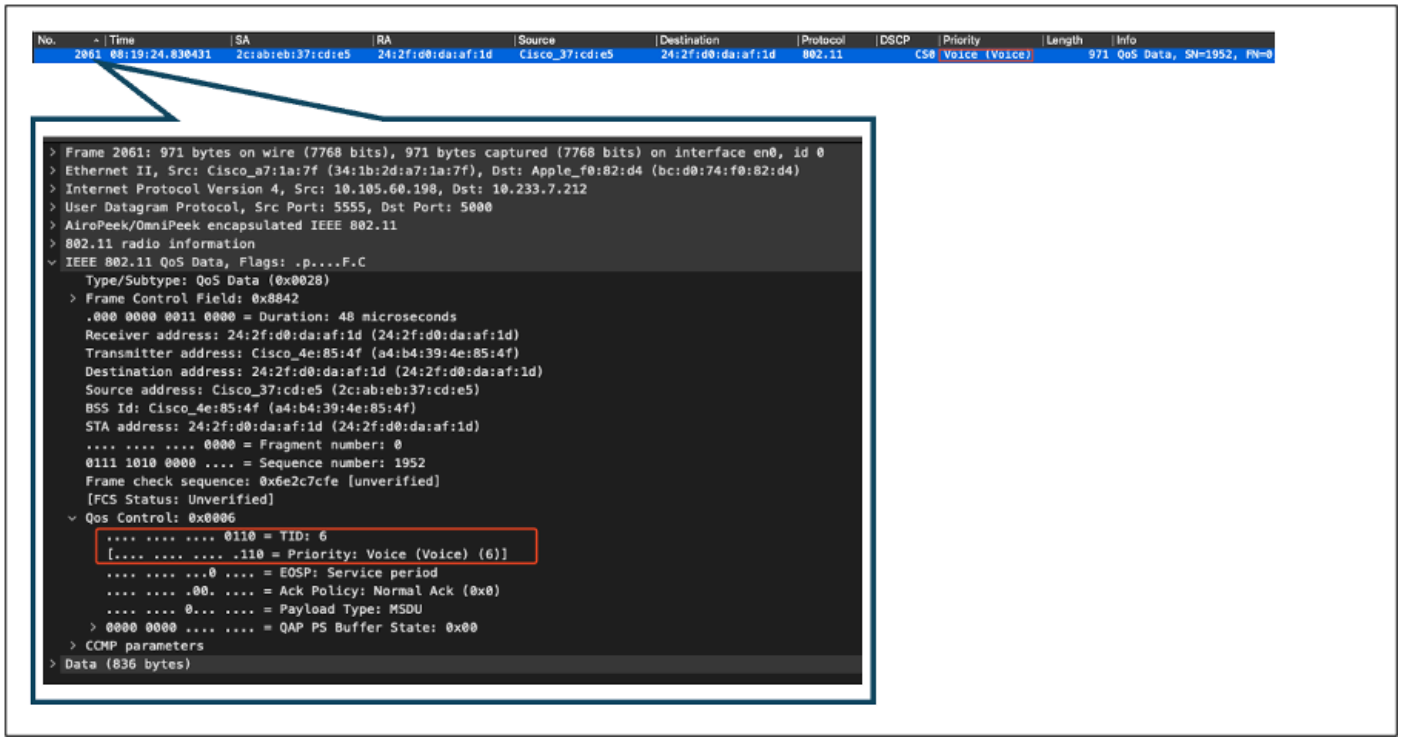
L'access point ha inoltrato il frame con un valore UP pari a 6. Ciò conferma che l'access point mappa correttamente il valore DSCP al valore 802.11 UP appropriato (6), che corrisponde al traffico vocale.




Acquisizione OTA dal punto di accesso al client

Nella fase finale, il pacchetto ricevuto dal PC wireless. Il PC wireless riceve il frame con un valore DSCP di 46.

Ciò significa che il contrassegno DSCP viene mantenuto per l'intero percorso di trasmissione, dal PC cablato al PC wireless. Il valore DSCP coerente di 46 conferma che le politiche QoS sono correttamente applicate e gestite nella direzione a valle.




Acquisizione di PC wireless

## Scenario di test 2: convalida QoS upstream

In questo scenario di test, lo scopo è convalidare la configurazione QoS a monte. La configurazione prevede l'invio di pacchetti UDP con DSCP 46 da un PC wireless a un PC cablato. Il WLC è configurato con la policy "Platinum QoS" per entrambe le direzioni a monte e a valle.

- Flusso traffico:

Fonte: PC wireless

Destinazione: PC cablato

Tipo di traffico: pacchetti UDP con DSCP 46

- Configurazione dei criteri QoS sul WLC:

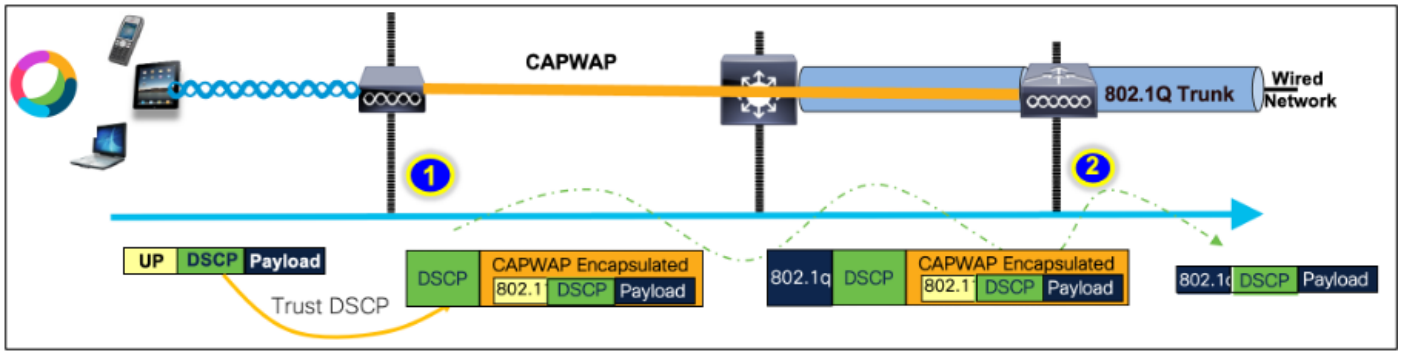
Profilo QoS: QoS Platinum

Direzione: sia a monte che a valle

- Comandi di configurazione QoS metal:

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

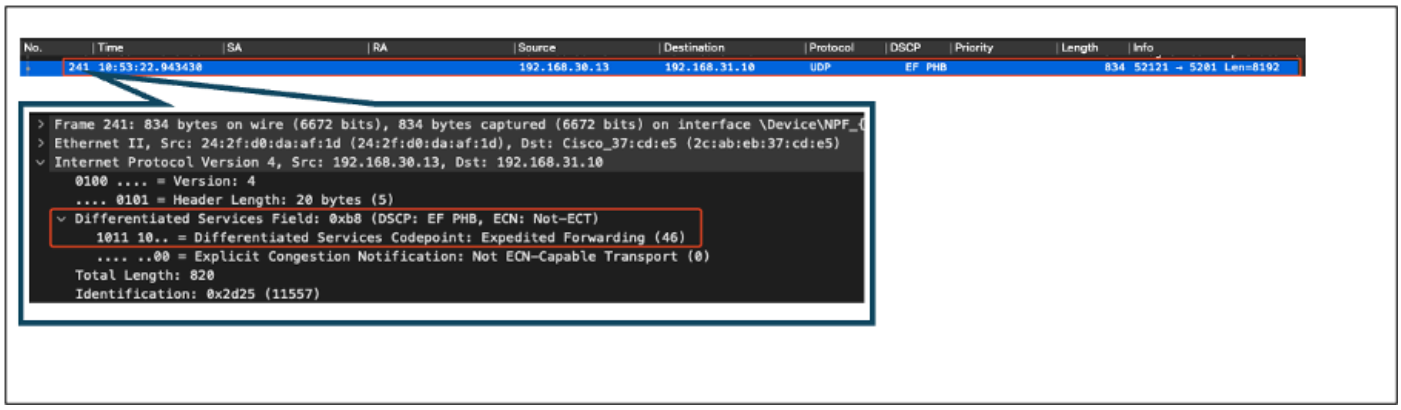
Topologia logica e conversione DSCP nella direzione a monte:




Topologia logica e conversione DSCP - Upstream

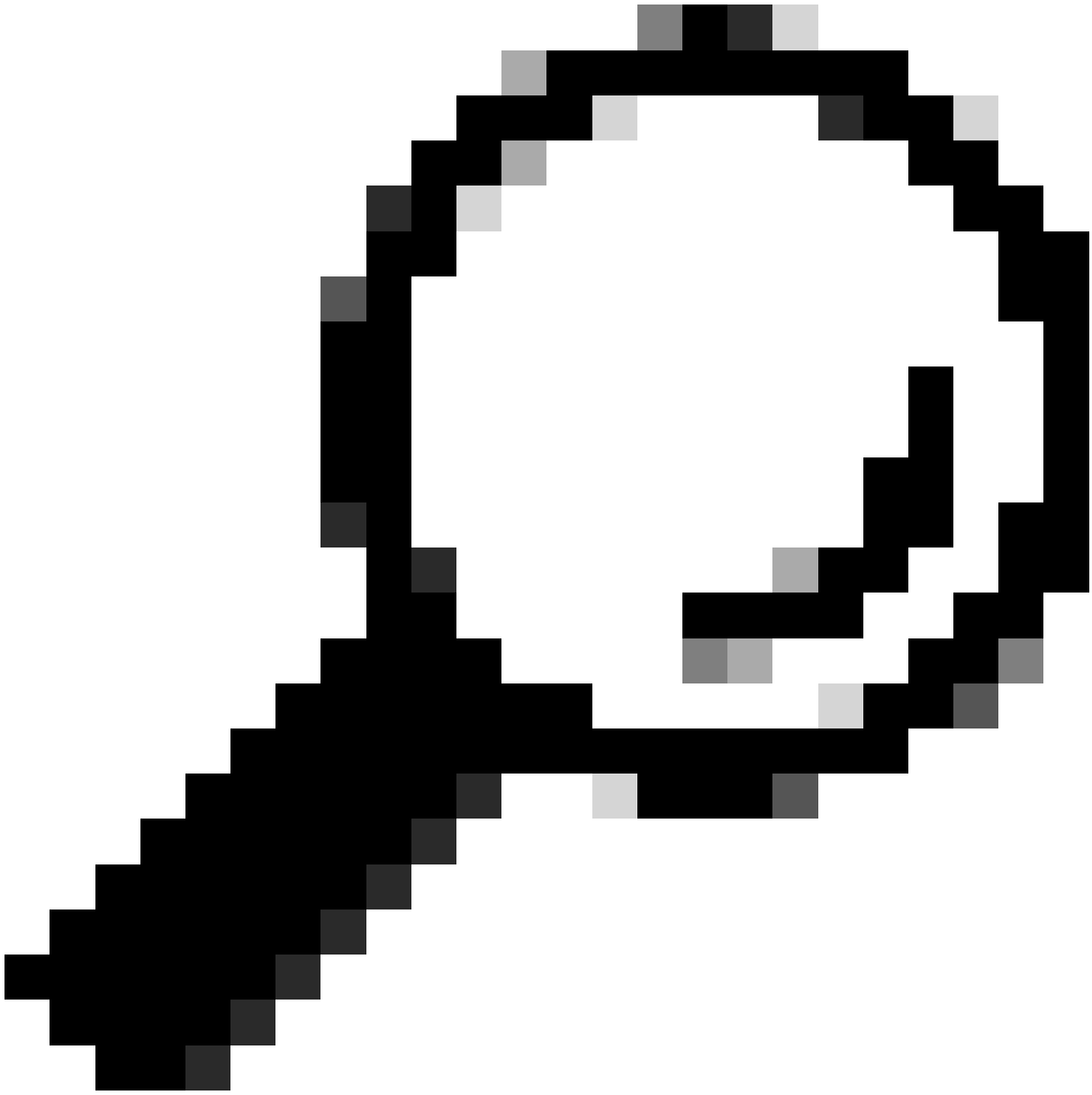
Pacchetti inviati dal PC wireless al PC cablato. Questa acquisizione viene effettuata sul PC wireless.

Il PC wireless invia pacchetti UDP con DSCP 46.

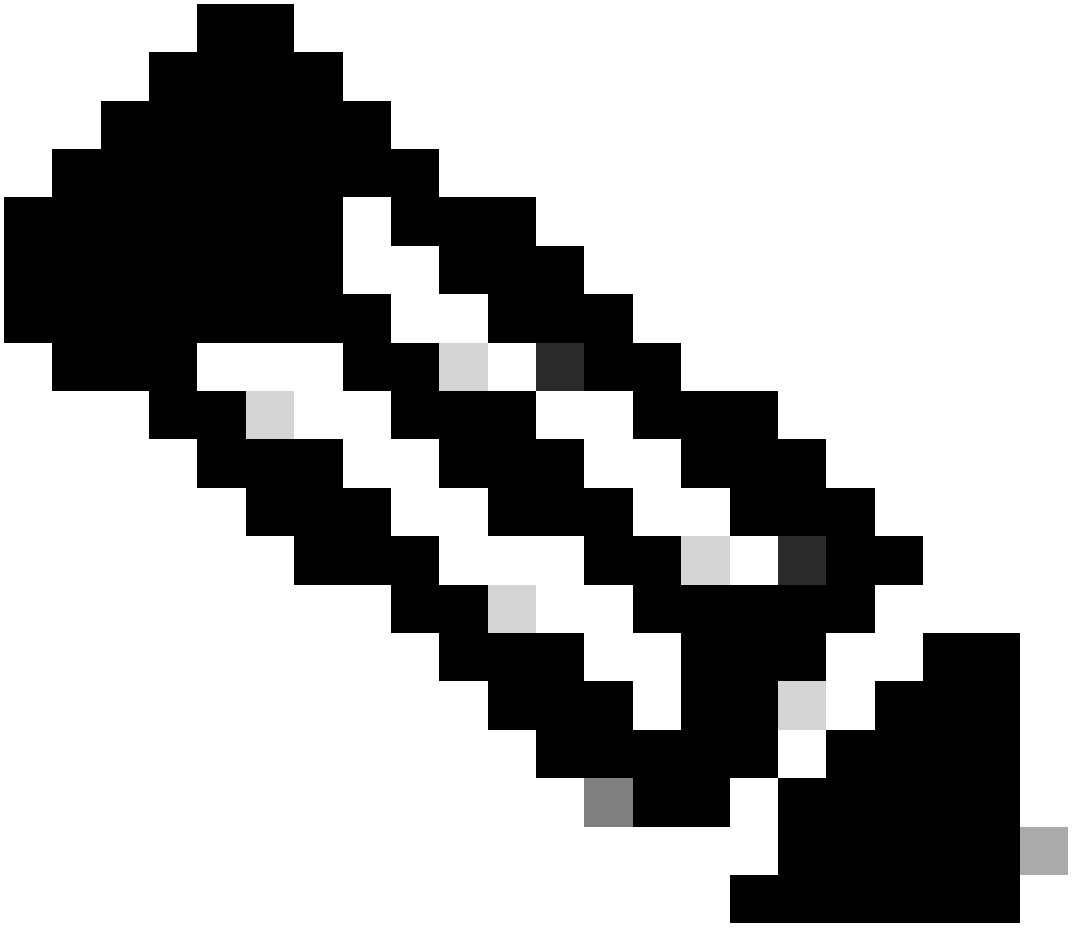



Acquisizione di PC wireless in upstream

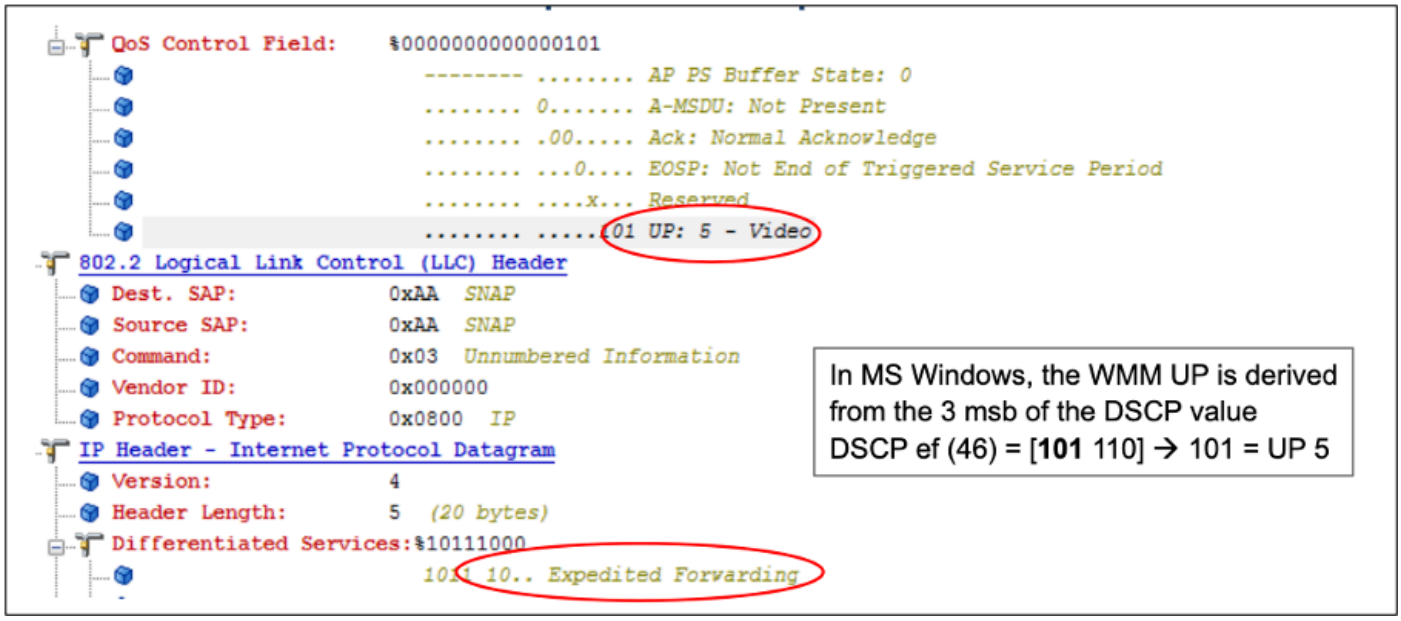
A questo punto è possibile esaminare l'acquisizione OTA dal client all'access point.



Suggerimento: quando si utilizza un PC wireless Windows per inviare pacchetti con DSCP 46, Windows mappa DSCP 46 a un valore di priorità utente (UP) pari a 5 (Video). Di conseguenza, l'acquisizione OTA mostra i pacchetti come traffico video (UP 5). Tuttavia, se il pacchetto viene decriptato, il valore DSCP rimane 46.



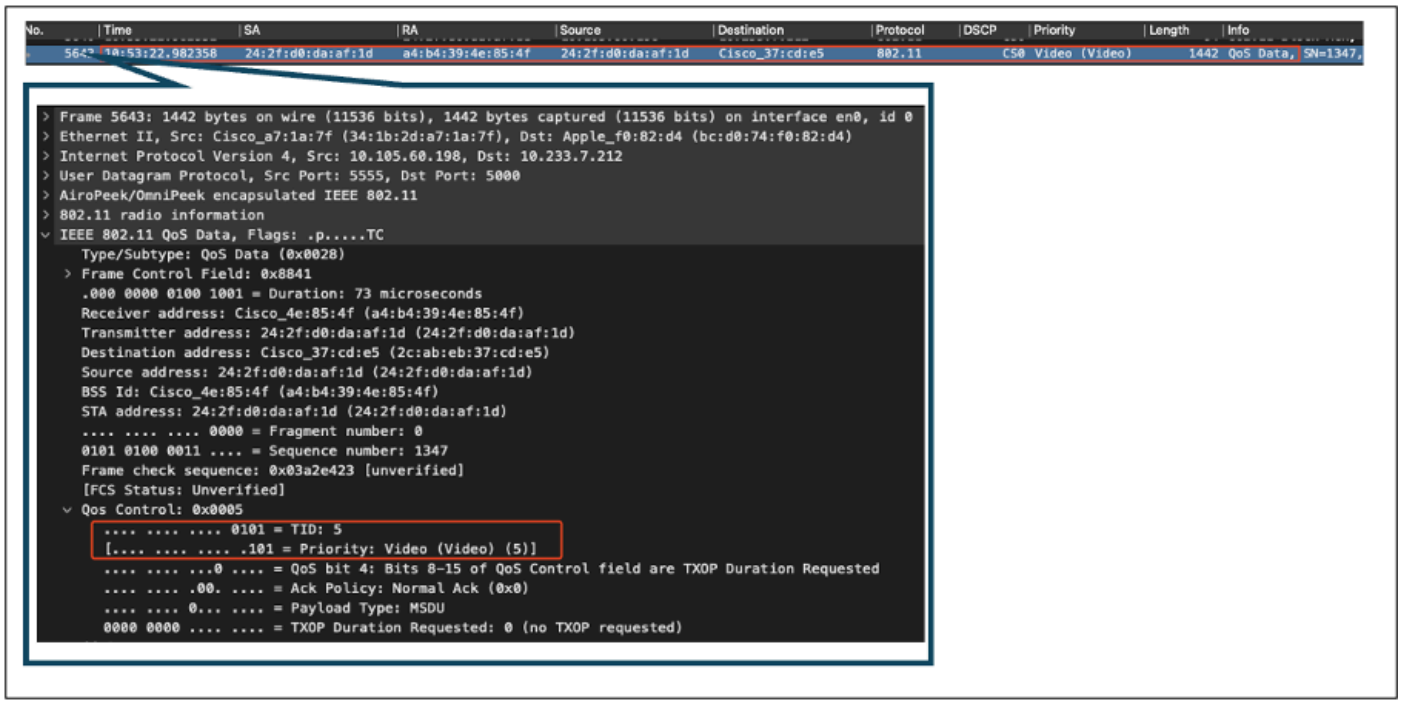
Nota: a partire dalla versione 17.4, per impostazione predefinita, Cisco 9800 WLC considera attendibile il valore DSCP nel profilo di join AP. In questo modo il valore DSCP di 46 viene mantenuto e considerato attendibile dal WLC, impedendo qualsiasi problema relativo al comportamento del mapping da DSCP a UP di Windows.




Mapping da Windows UP a DSCP

L'acquisizione OTA (Over-the-Air) crittografata presa dalla configurazione lab viene analizzata per convalidare la configurazione QoS upstream.

L'acquisizione OTA visualizza i pacchetti con un valore di priorità utente (UP) pari a 5 (Video). Anche se l'acquisizione OTA mostra UP 5, il valore DSCP all'interno del pacchetto crittografato rimane 46.

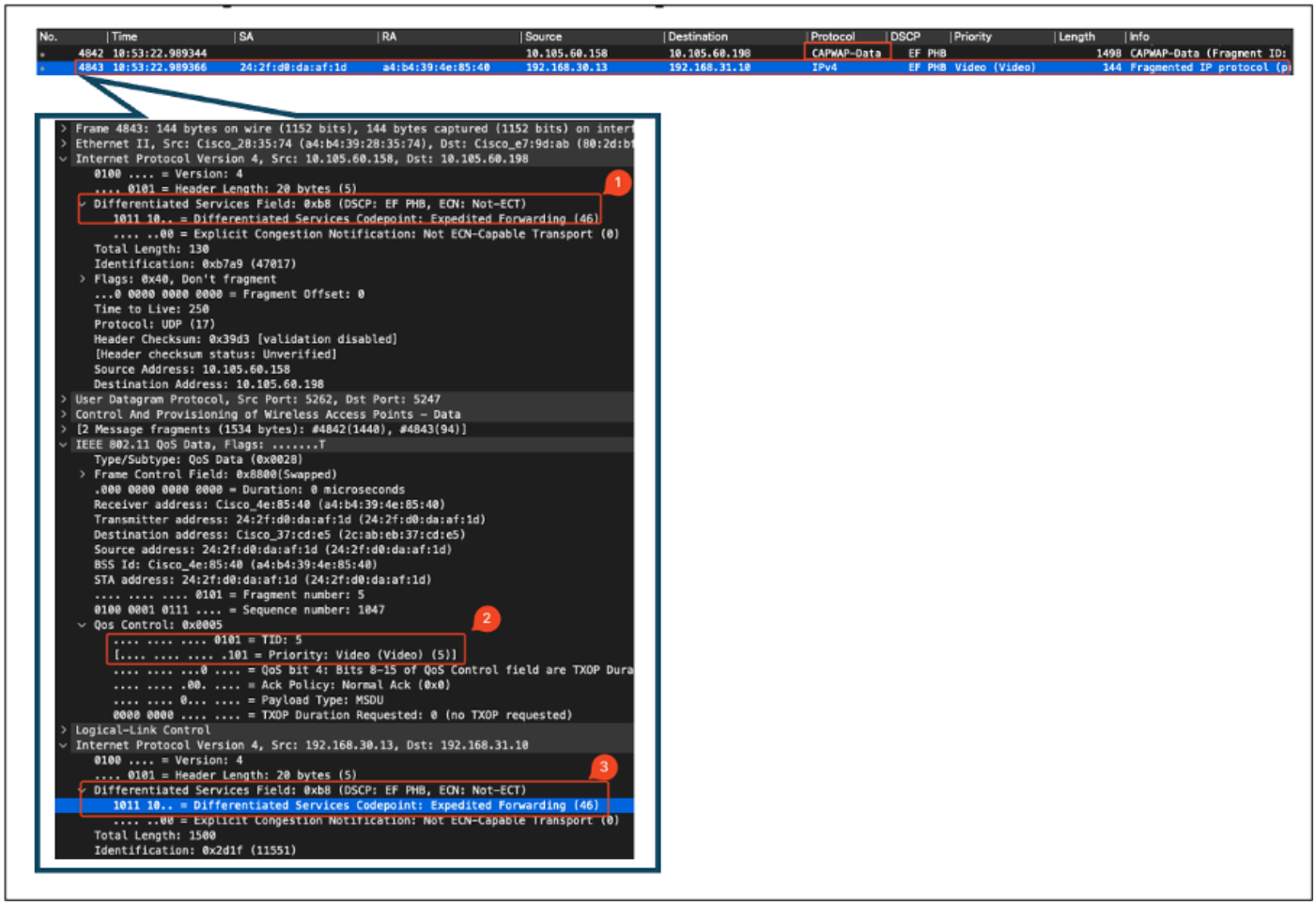



OTA impostazione LAB in direzione upstream

Successivamente, viene analizzata l'acquisizione del pacchetto sulla porta uplink dell'access point per assicurarsi che il valore DSCP venga mantenuto mentre il pacchetto si sposta dall'access point al WLC.

- Il valore DSCP sul livello CAPWAP esterno viene mantenuto a 46.

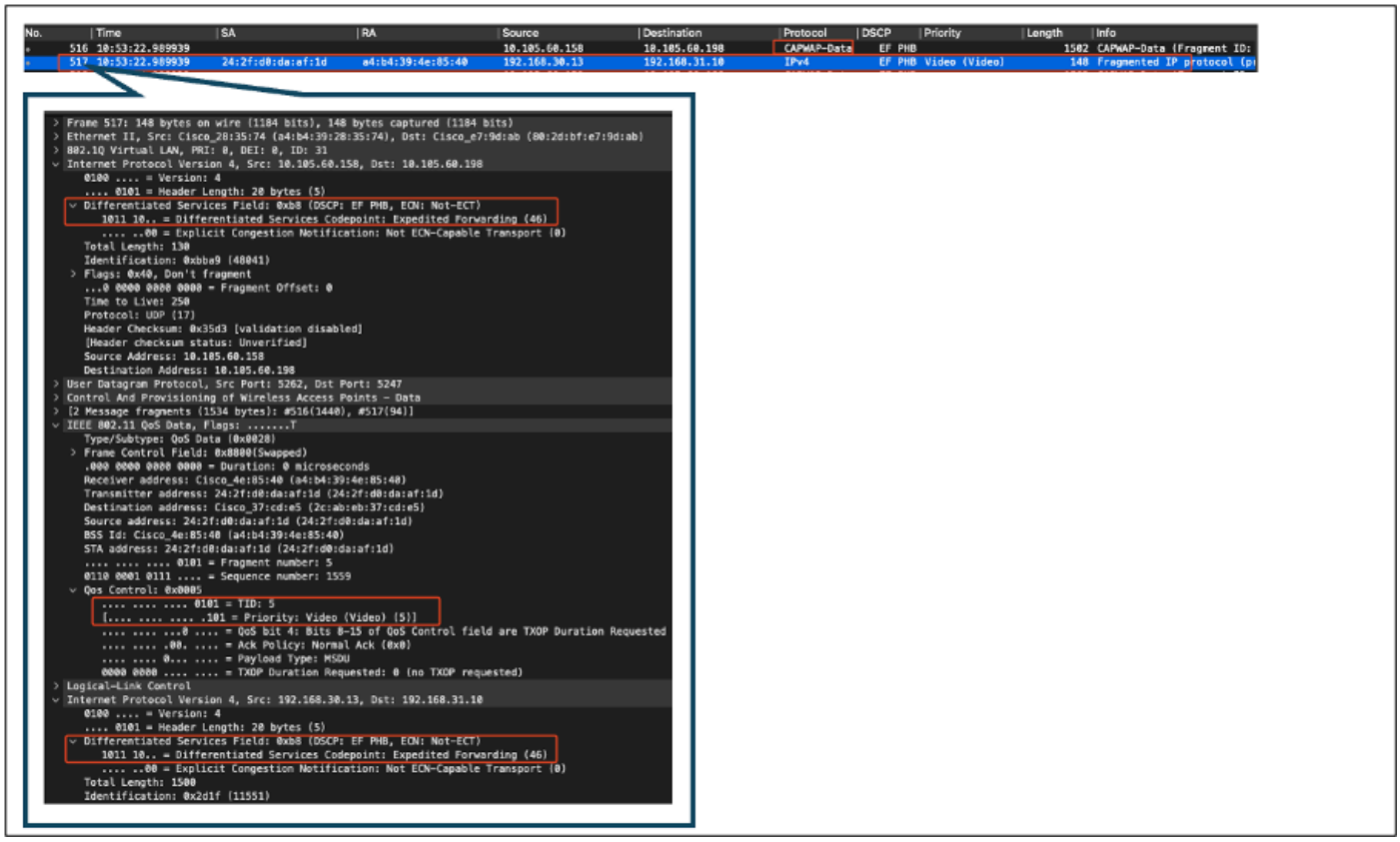
- All'interno del tunnel CAPWAP, anche il valore DSCP viene mantenuto a 46.



Acquisizione Pplink AP in direzione upstream

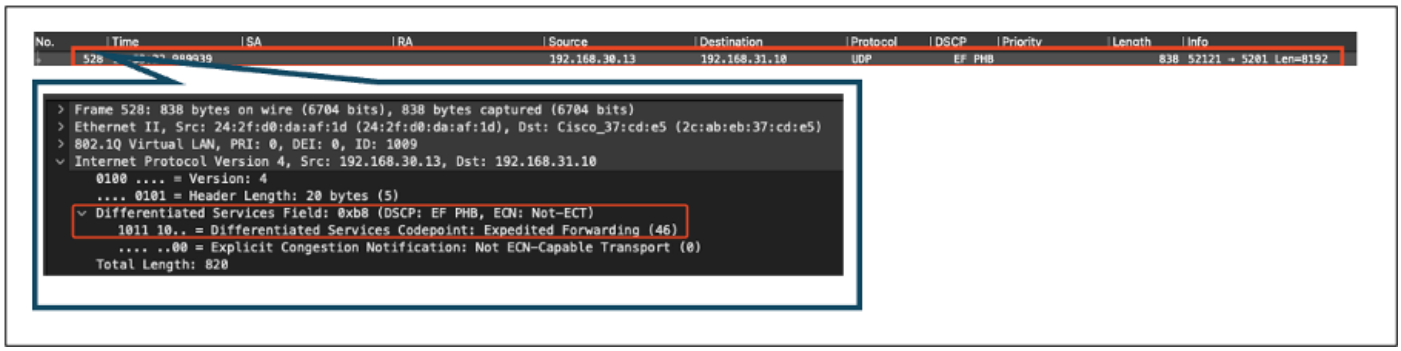
L'acquisizione viene effettuata sul WLC quando il pacchetto arriva dallo switch.

- Il pacchetto arriva al WLC con il valore DSCP di 46 sul livello CAPWAP esterno.
- All'interno del tunnel CAPWAP, il valore DSCP viene mantenuto a 46.



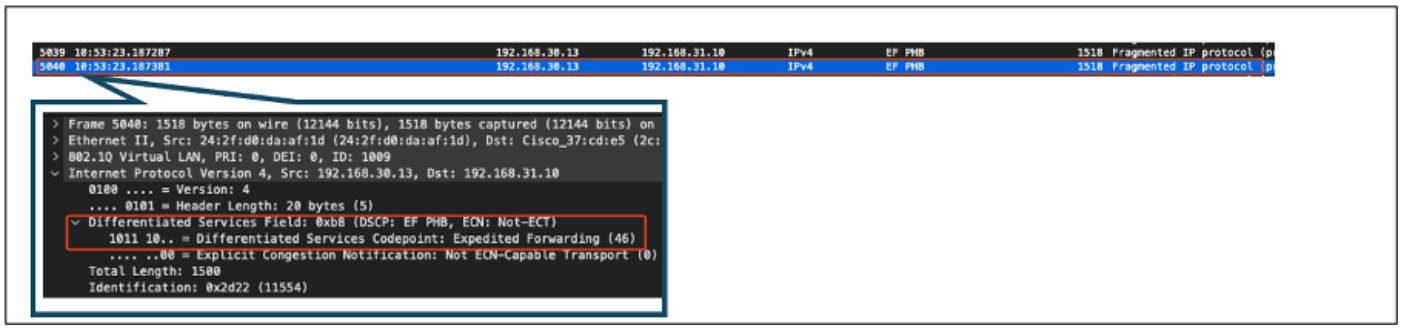

EPC WLC con visualizzazione dei pacchetti provenienti dall'access point

Dopo aver ruotato il pacchetto verso il WLC, il pacchetto viene rimandato allo switch uplink destinato al PC cablato. Il WLC inoltra il pacchetto con il valore DSCP di 46.



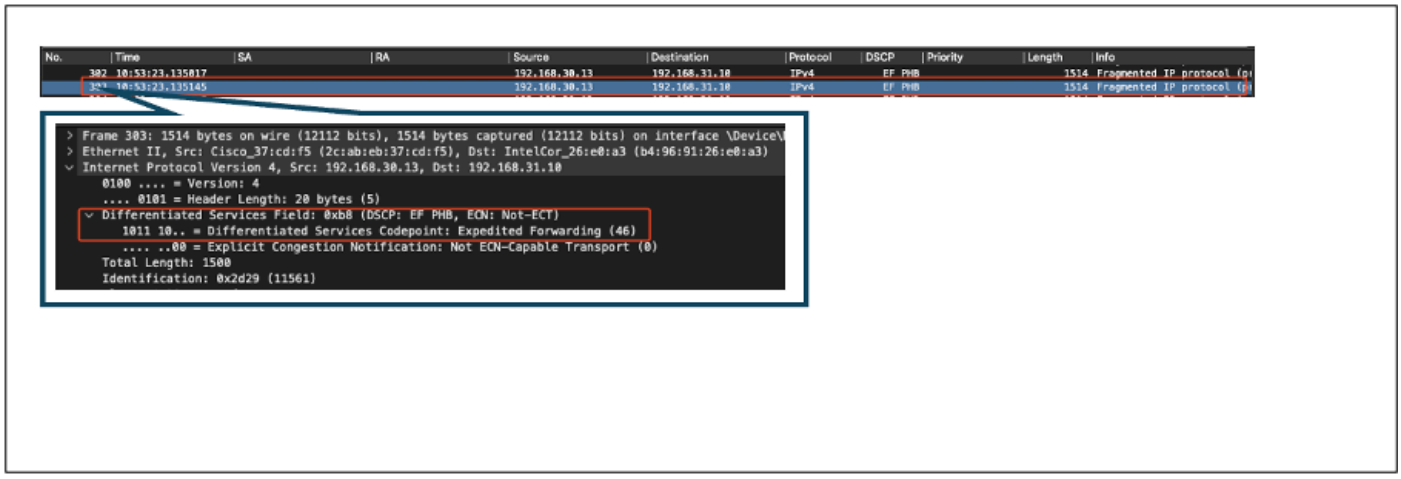

EPC WLC con visualizzazione dei pacchetti inviati al PC cablato

Infine, viene analizzata l'acquisizione del pacchetto sull'uplink del PC cablato per verificare che il valore DSCP venga mantenuto quando il pacchetto arriva dal WLC.




Acquisizione switch uplink PC cablato in direzione upstream

Nella fase finale, il pacchetto ricevuto dal PC cablato viene analizzato per verificare che arrivi al PC con il valore DSCP di 46.




Cattura di PC cablati - Verso l'alto

Il test QoS upstream ha convalidato la configurazione QoS per il traffico dal PC wireless al PC cablato. Il costante mantenimento del valore DSCP di 46 in tutto il percorso di trasmissione conferma che i criteri QoS sono applicati e applicati correttamente.

## Risoluzione dei problemi

La voce, i video e altre applicazioni in tempo reale sono particolarmente sensibili ai problemi di prestazioni della rete e qualsiasi deterioramento nella qualità del servizio (QoS) può avere effetti negativi e evidenti. Quando i pacchetti QoS vengono contrassegnati con valori DSCP inferiori, l'impatto sulla voce e sul video può essere significativo.

Impatto sulla voce:

- Maggiore latenza: la comunicazione vocale richiede una bassa latenza per garantire conversazioni fluide e naturali. Valori DSCP più bassi possono causare ritardi dei pacchetti vocali, con conseguenti ritardi nelle conversazioni.
- Jitter: la variabilità dei tempi di arrivo dei pacchetti (jitter) può interrompere la consegna dei pacchetti voce. Ciò può causare audio discontinuo o alterato, rendendo difficile la comprensione dell'altoparlante.
- Perdita di pacchetti: i pacchetti voce sono altamente sensibili alla perdita di pacchetti. Anche una piccola quantità di perdita di pacchetti può causare la perdita di parole o sillabe, con conseguente scarsa qualità delle chiamate e incomprensioni.
- Eco e distorsione: l'aumento della latenza e del jitter può causare una distorsione dell'eco e dell'audio, riducendo ulteriormente la qualità della chiamata vocale.

Impatto sul video:

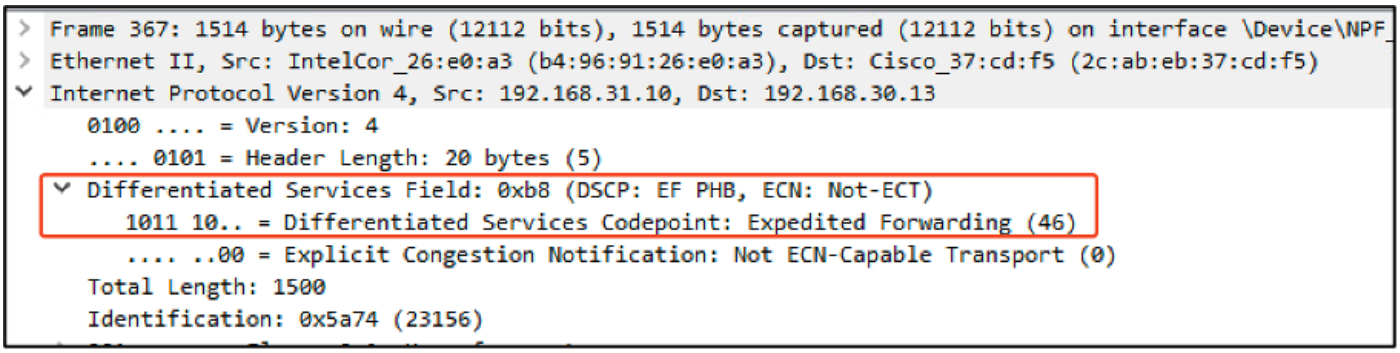
- Maggiore latenza: la comunicazione video richiede una bassa latenza per mantenere la sincronizzazione tra i flussi audio e video. Una maggiore latenza può causare ritardi, rendendo difficile l'interazione in tempo reale.
- Jitter: lo jitter può causare l'arrivo di fotogrammi video non ordinati o a intervalli irregolari, con

conseguente riproduzione irregolare o balbettante del video.
- Perdita di pacchetti: la perdita di pacchetti può causare la perdita di fotogrammi, che possono causare il blocco del video o la visualizzazione di artefatti.
- Qualità video ridotta: valori DSCP inferiori possono ridurre l'allocazione della larghezza di banda per i flussi video, con conseguente risoluzione inferiore e qualità video inferiore. Ciò può rendere difficile la visualizzazione di dettagli importanti nel video.

## Scenario 1: contrassegno DSCP riscritto dallo switch intermedio

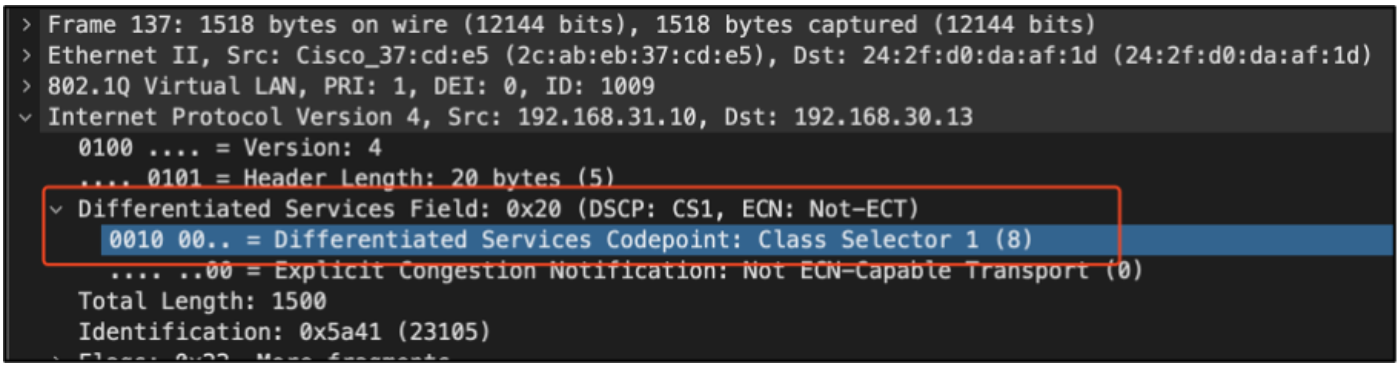
In questo scenario di risoluzione dei problemi, viene esaminato l'impatto che una commutazione intermedia riscrive il contrassegno DSCP sul traffico quando arriva al WLC. Per replicare questo problema, lo switch è configurato in modo da riscrivere il contrassegno DSCP 46 su CS1 sull'interfaccia uplink del PC cablato.

Il pacchetto viene inviato dal PC cablato con un tag DSCP 46.




PC cablato che invia il pacchetto con tag DSCP 46

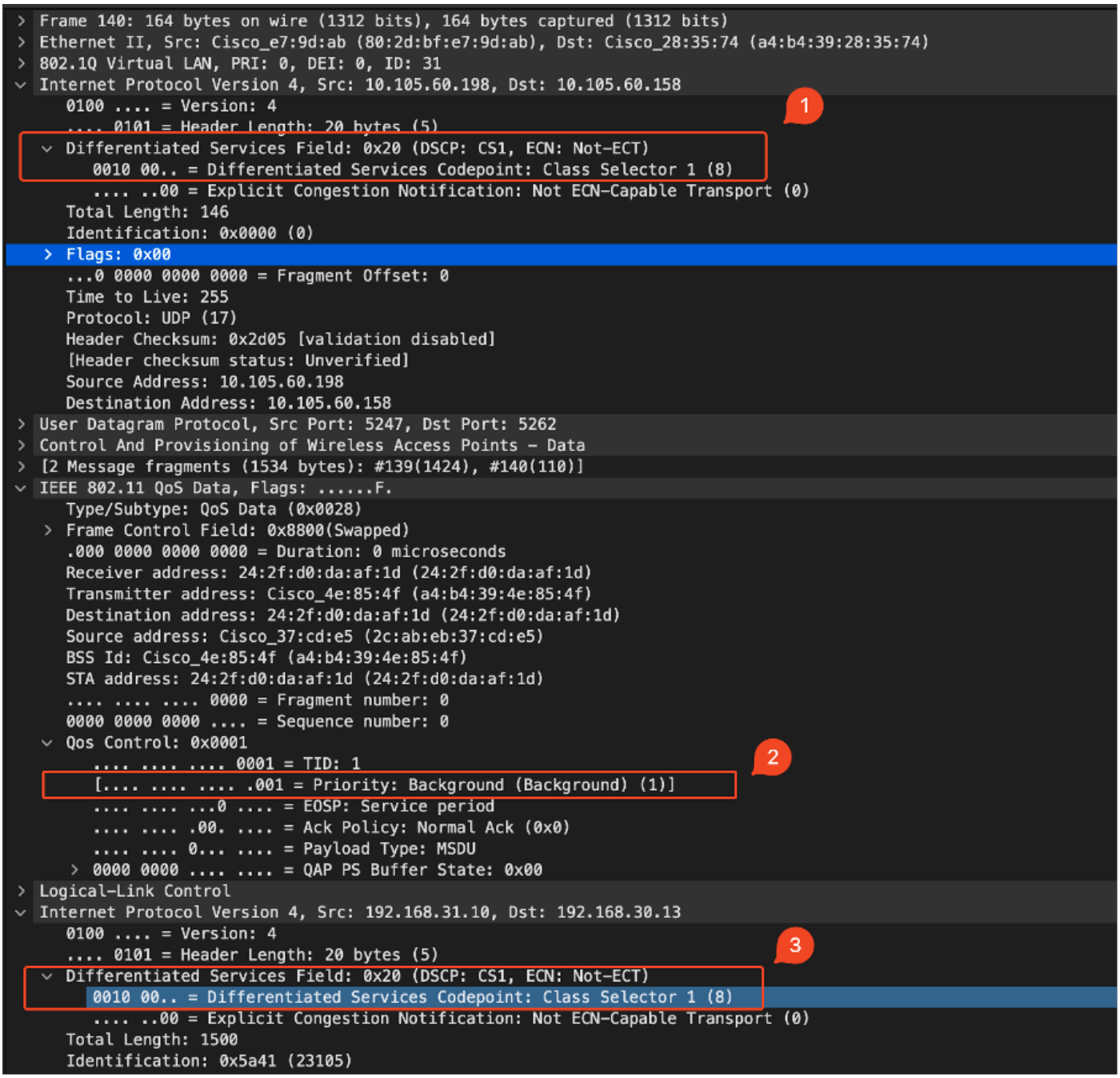
Il pacchetto arriva al WLC con un valore DSCP di CS1 (DSCP 8). Il passaggio da DSCP 46 a DSCP 8 riduce significativamente la priorità del pacchetto.




EPC WLC con contrassegno CS1

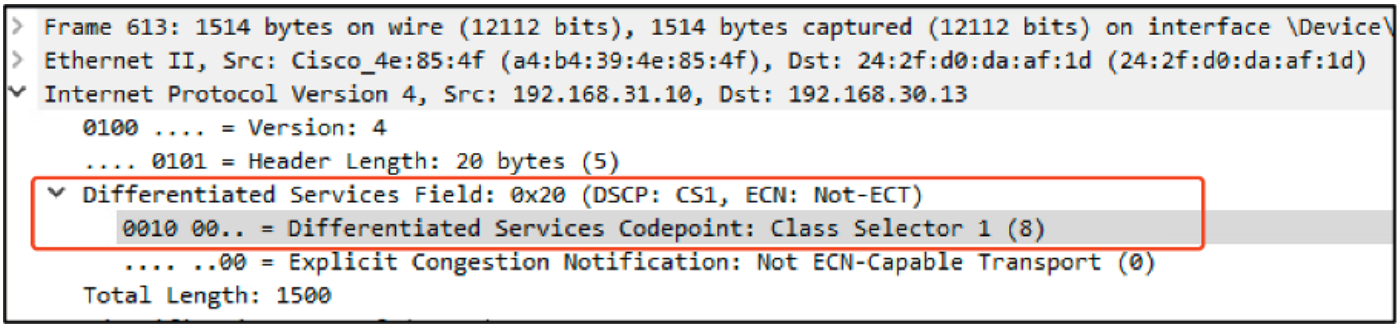
In questo passaggio, viene analizzato il pacchetto inoltrato dal WLC all'access point.

- L'intestazione CAPWAP esterna è contrassegnata con CS1 (DSCP 8).
- Anche l'intestazione CAPWAP interna è contrassegnata con CS1 (DSCP 8).
- Il valore di Priorità utente (UP) è impostato su BK (Background).




EPC WLC con codice CS1 nel traffico CAPWAP

Il pacchetto arriva al PC wireless con un valore DSCP di CS1 (DSCP 8).




Acquisizione di PC wireless con contrassegno CS1

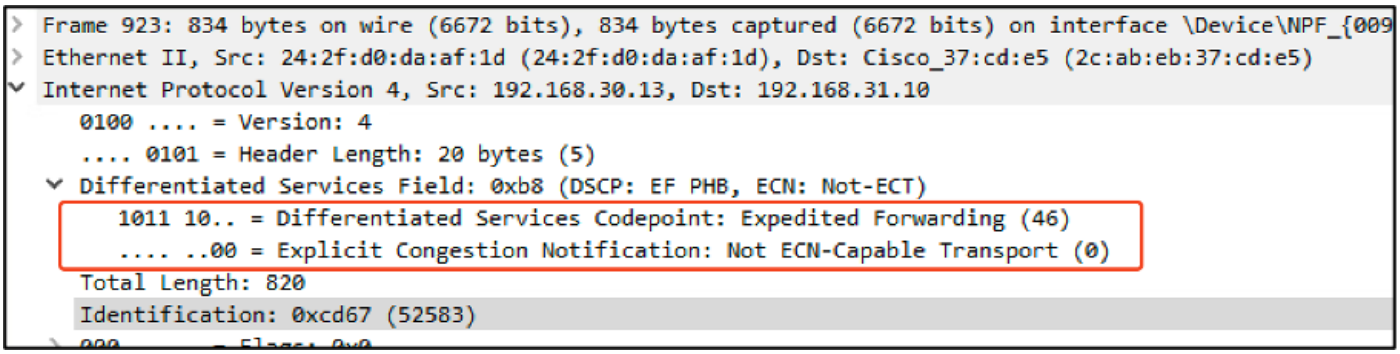
In questo scenario viene mostrato come una configurazione errata su uno switch intermedio possa

interrompere la configurazione QoS, riducendo le prestazioni del traffico ad alta priorità. I pacchetti voce, inizialmente contrassegnati per l'alta priorità, sono stati trattati come traffico con priorità inferiore a causa della riscrittura DSCP. Questo scenario sottolinea l'importanza di garantire che i dispositivi di rete intermedi conservino correttamente i contrassegni QoS per mantenere la qualità di servizio desiderata per il traffico ad alta priorità.

## Scenario 2: lo switch di collegamento AP riscrive il contrassegno DSCP

In questo scenario, viene esaminato l'impatto sul traffico di uno switch intermedio collegato all'access point che riscrive il contrassegno DSCP.

- Lo switch collegato all'access point è configurato in modo da riscrivere il contrassegno DSCP 46 su un valore diverso di CS1 sull'interfaccia di uplink dell'access point.
- Il pacchetto viene inviato dal PC cablato con un tag DSCP di 46. Ciò conferma che il traffico è contrassegnato correttamente con DSCP 46 all'origine.

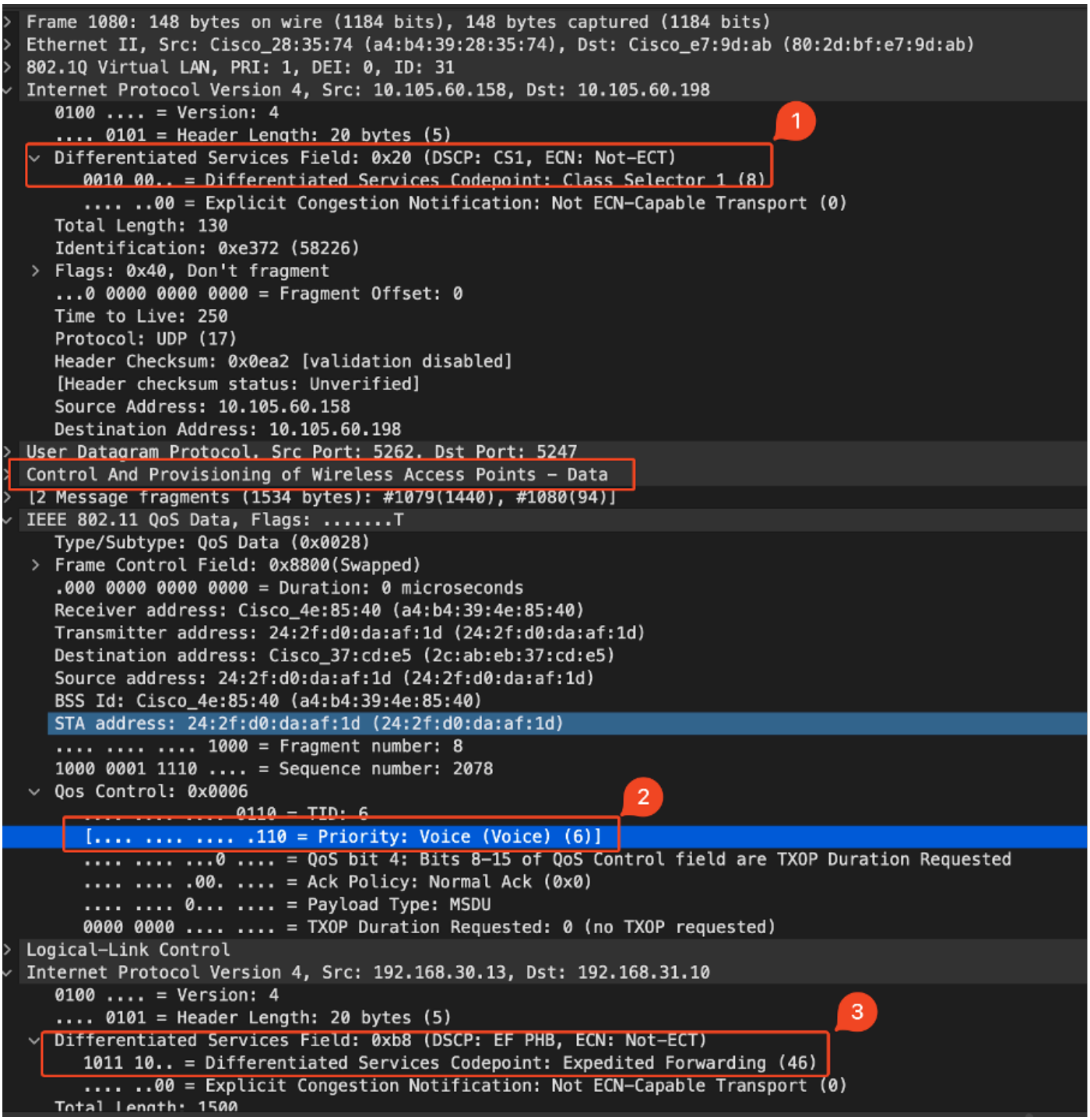


Acquisizione di PC wireless con DSCP 46

L'acquisizione viene effettuata sul WLC quando il pacchetto arriva dallo switch.

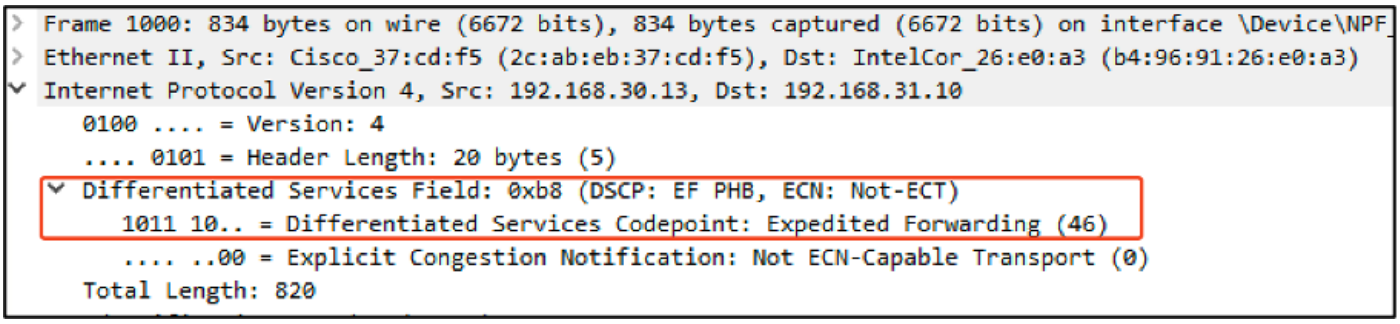
Il pacchetto arriva al WLC con il valore DSCP dell'intestazione CAPWAP esterna di CS1 (DSCP) e il valore DSCP interno di 46. Questo problema si verifica perché lo switch intermedio non può visualizzare il traffico incapsulato nel tunnel CAPWAP.

Il WLC considera attendibile il tag DSCP all'interno del tunnel CAPWAP e inoltra il traffico al PC cablato con il tag DSCP interno di 46.




EPC WLC con valori CAPWAP DSCP

Il pacchetto arriva al PC cablato con un valore DSCP di 46. Conferma che il WLC inoltra correttamente il pacchetto con il valore DSCP originale di 46, mantenendo il contrassegno di priorità alta.




Il PC cablato ha ricevuto il pacchetto con DSCP 46

Anche se il WLC ha inoltrato il traffico con un tag DSCP di 46, è importante capire che il traffico tra l'AP e il WLC è stato trattato come traffico a bassa priorità a causa del tag DSCP esterno riscritto sul CS1 (DSCP 8).

Possono esistere più switch tra l'AP e il WLC e, se al traffico viene assegnata una priorità bassa, può arrivare in ritardo al WLC. Ciò può aumentare la latenza, l'instabilità e la potenziale perdita di pacchetti, compromettendo la qualità del servizio per il traffico ad alta priorità, ad esempio la voce.

## Suggerimento per la risoluzione dei problemi

1. Verifica contrassegno DSCP iniziale: acquisire pacchetti all'origine (ad esempio, PC cablato) per garantire che il traffico venga contrassegnato correttamente con il valore DSCP previsto.
2. Controllare le configurazioni dei dispositivi intermedi: rivedere la configurazione di tutti gli switch intermedi e i router per verificare che non stiano inavvertitamente riscrivendo i valori DSCP.
3. Acquisire il traffico nei punti chiave:
    1. Prima e dopo lo switch intermedio.
    2. Al WLC.
    3. Nella destinazione (ad esempio, PC wireless).
4. Simulare scenari di traffico: utilizzare generatori di traffico o strumenti di simulazione della rete per creare diversi tipi di traffico e osservare come QoS viene gestito dalla rete wireless.
5. Consultare il documento sulle best practice per 9800: rivedere la documentazione sulle best practice per 9800 sulla configurazione delle marcature QoS e DSCP.

## Verifica della configurazione

<#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
```

## Conclusioni

Mantenere una configurazione QoS coerente sulla rete è fondamentale per garantire che il traffico ad alta priorità, come voce e video, riceva il livello appropriato di servizio e di prestazioni. È essenziale convalidare regolarmente le configurazioni QoS per garantire che tutti i dispositivi di rete siano conformi alle policy QoS previste. Questa convalida consente di identificare e correggere eventuali configurazioni errate o deviazioni che potrebbero compromettere le prestazioni della rete.

## Riferimenti

- Descrizione e risoluzione dei problemi dei Cisco Catalyst serie 9800 Wireless Controller
- Best practice per la configurazione di Cisco Catalyst serie 9800
- Guida alla configurazione del software Cisco Catalyst serie 9800 Wireless Controller, Cisco IOS® XE Dublin 17.12.x
- Guida alla risoluzione dei problemi VoWLAN (Voice over Wireless LAN)
- Abilita tag QoS DSCP su computer Windows

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).