

Configuratie van valideren en probleemoplossing voor draadloze QoS op 9800 WLC

Inhoud

[Inleiding](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configuratie](#)

[QoS-beleidsdoelstellingen](#)

[Auto QoS](#)

[Auto QoS CLI-configuratie](#)

[Modulaire QoS CLI](#)

[MQS CLI-configuratie](#)

[Metaal QoS](#)

[Configuratie van Metal QoS CLI](#)

[End-to-end QoS met pakketvastlegging valideren](#)

[Netwerkdigram](#)

[Lab-componenten en pakketopnamepunten](#)

[Testscenario 1: Downstream QoS-validatie](#)

[Testscenario 2: Upstream QoS-validatie](#)

[Probleemoplossing](#)

[Scenario 1: Intermediate Switch herschrijft DSCP-markering](#)

[Scenario 2: AP link Switch herschrijft DSCP-markering](#)

[Tip voor probleemoplossing](#)

[Configuratieverificatie](#)

[Conclusie](#)

[Referenties](#)

Inleiding

Dit document beschrijft manieren om Wireless LAN Quality of Service (QoS) op 9800 draadloze LAN-controller (WLC) te configureren, te valideren en problemen op te lossen.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- WLC: C9800-40-K9 met 17.12.03
- access point (AP): C9120-AX-D
- Switch: C9300-48P met 17.03.05

- Draadloze en bekabelde client: Windows 10

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

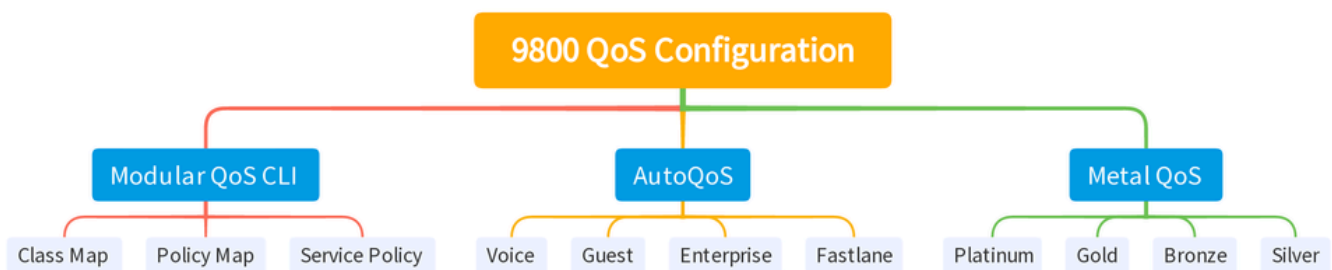
Draadloze QoS is essentieel om ervoor te zorgen dat kritieke toepassingen de benodigde bandbreedte en lage latentie ontvangen die nodig zijn voor optimale prestaties. Dit document biedt een uitgebreide handleiding voor het configureren, valideren en oplossen van problemen met QoS op draadloze Cisco-netwerken.

Dit artikel gaat ervan uit dat lezers een fundamenteel begrip hebben van zowel draadloze als bekabelde QoS-principes. Er wordt ook verwacht dat lezers ervaring hebben met het configureren en beheren van Cisco WLC's en AP's.

Configuratie

In dit gedeelte wordt ingegaan op de configuratie van QoS op 9800 draadloze controllers. Door gebruik te maken van deze configuraties, kunt u ervoor zorgen dat kritieke toepassingen de benodigde bandbreedte en lage latentie ontvangen, waardoor de algehele netwerkprestaties worden geoptimaliseerd.

U kunt de 9800 WLC QoS-configuratie in voornamelijk drie verschillende brede categorieën verdelen.



Samenvatting van QoS-configuratie 9800 WLC

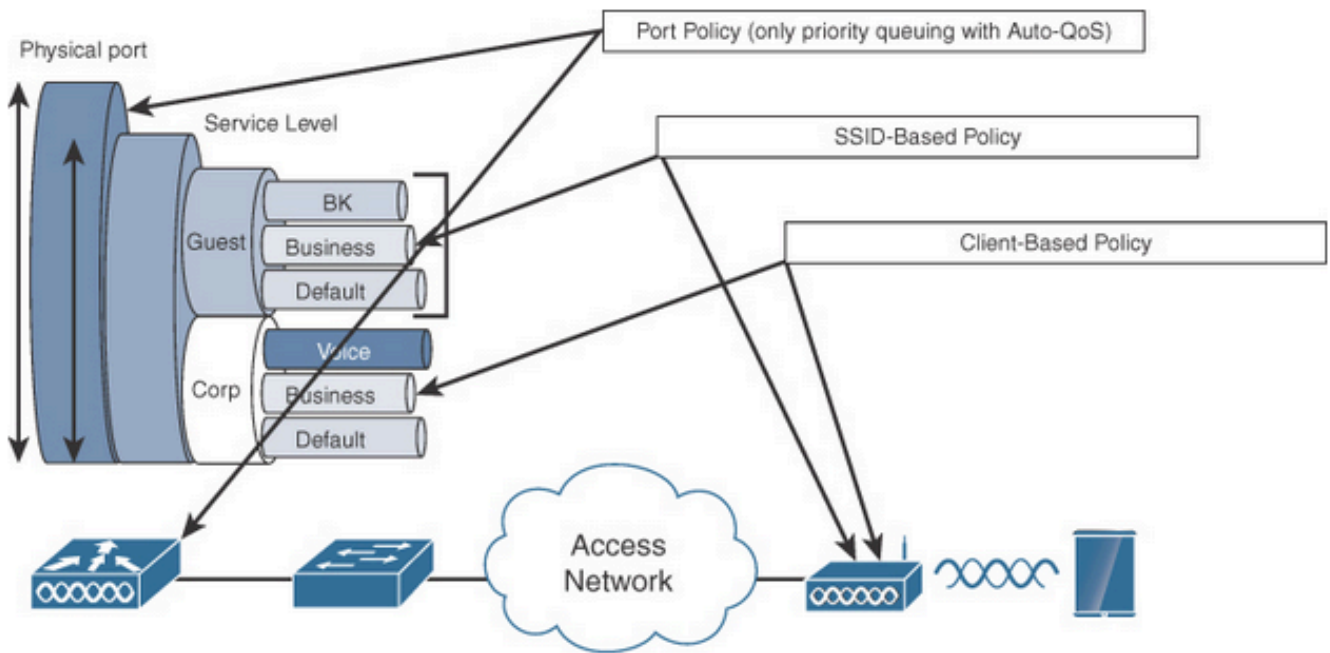
Dit document doorloopt elke sectie één voor één in de volgende secties.



Opmerking: dit artikel richt zich op AP in lokale modus. AP in de Flexconnect modus wordt niet besproken.

QoS-beleidsdoelstellingen

Een beleidsdoel is de configuratie waar een QoS-beleid kan worden toegepast. De QoS-implementatie op Catalyst 9800 is modulair en flexibel. De gebruiker kan besluiten beleid te configureren op drie verschillende doelen: de SSID, client en poortniveaus.



QoS-beleidsdoelstellingen

Het SSID-beleid is van toepassing per AP per SSID. U kunt beleid voor toezicht en markering op SSID configureren.

Clientbeleid is van toepassing in de in- en uitrijrichting. U kunt beleid voor toezicht en markering op clients configureren. AAA-opheffing wordt ook ondersteund.

Het op poort gebaseerde QoS-beleid kan worden toegepast op een fysieke of logische poort.

Auto QoS

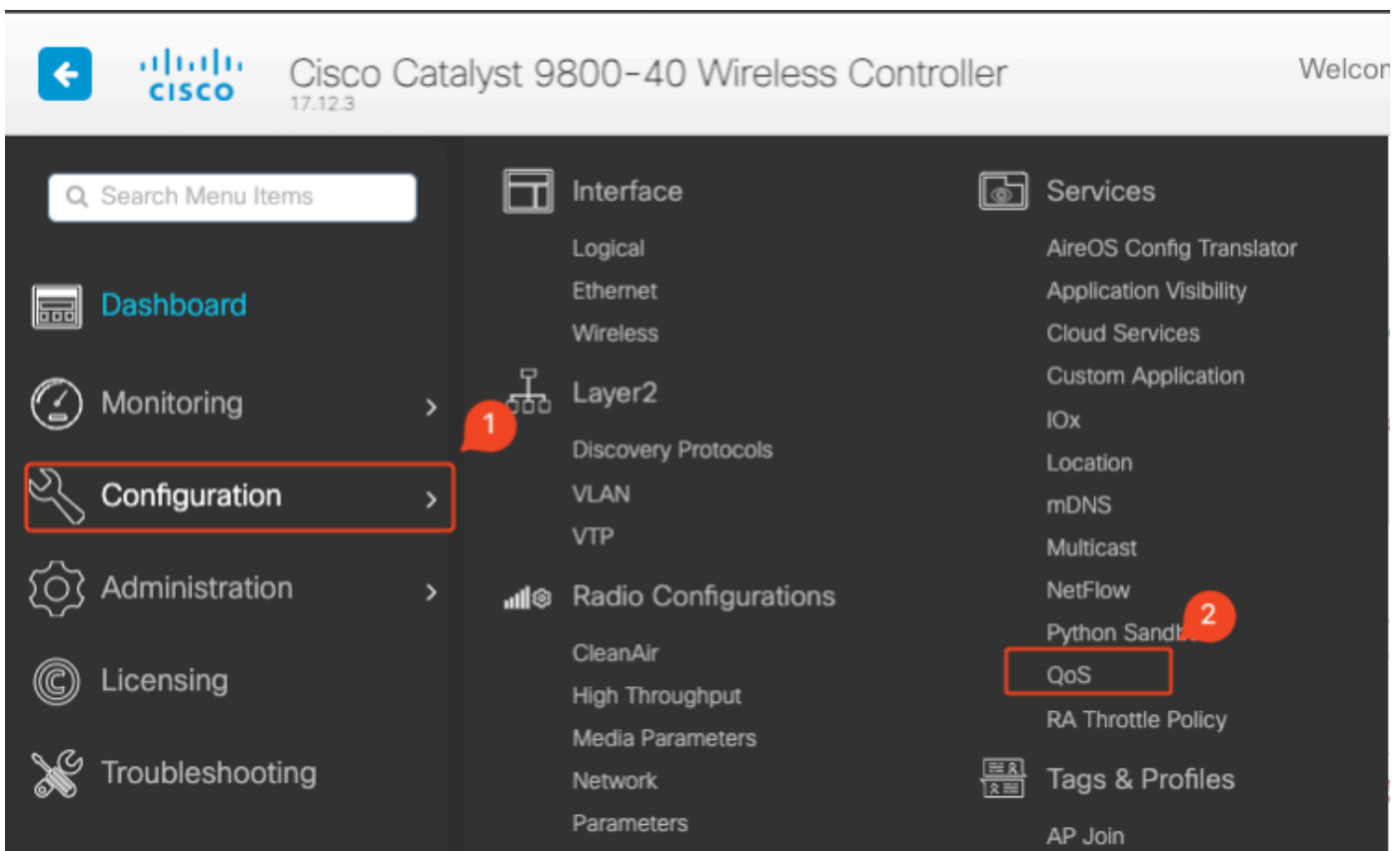
Draadloze Auto QoS automatiseert de implementatie van draadloze QoS-functies. Het heeft een set van vooraf gedefinieerde profielen die verder kan worden aangepast door de beheerder om prioriteit te geven aan verschillende verkeersstromen. Auto-QoS past verkeer aan en wijst elk aangepast pakket toe aan QoS-groepen. Dit staat de kaart van het outputbeleid toe om specifieke QoS groepen in specifieke rijen, met inbegrip van de prioriteitsrij te zetten.

Modus	Clientingang	Uitgang client	BSSID Ingress	BSSID uitgaande	Poortinvoer	Poortuitgang	Radio
Spraak	N.v.t.	N.v.t.	platina	platina	N.v.t.	AutoQoS-4.0-WLAN-poortuitvoerbeleid	ACM ingeschakeld
gast	N.v.t.	N.v.t.	AutoQoS-4.0-WLAN-	AutoQoS-4.0-WLAN-	N.v.t.	AutoQoS-4.0-WLAN-poortuitvoerbeleid	

			GT-SSID-I/O-beleid	GT-SSID-uitvoer-beleid			
Fastlane	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.	AutoQoS-4.0-WLAN-poortuitvoerbeleid	edca-parameters fastlane
Enterprise-AVC	N.v.t.	N.v.t.	AutoQoS-4.0-WLAN-ET-SSID-Invoer-AVC-beleid	AutoQoS-4.0-VLAN-ET-SSID-uitgang-beleid	N.v.t.	AutoQoS-4.0-WLAN-poortuitvoerbeleid	

Deze tabel geeft de configuratiewijzigingen weer die plaatsvinden wanneer een automatisch QoS-profiel wordt toegepast.

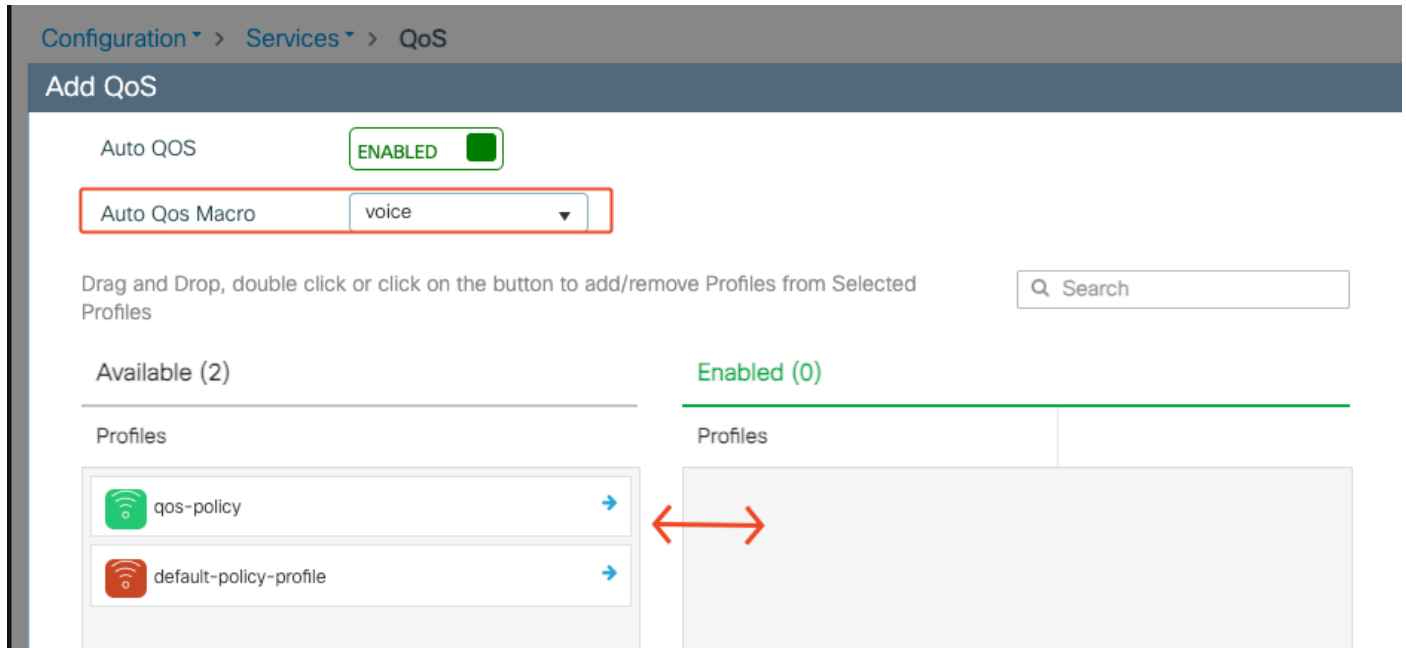
Auto QoS configureren navigeren naar configuratie > QoS



QoS-werkstroom

Klik op Add en stel Auto QoS in op enabled. Kies de juiste Auto QoS-macro in de lijst. In dit

voorbeeld wordt spraakmacro gebruikt om spraakverkeer prioriteit te geven.



AutoQoS-spraaktoewijzing

Als de macro is ingeschakeld, selecteert u het beleid dat aan het beleid moet worden gekoppeld.

Auto QoS CLI-configuratie

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

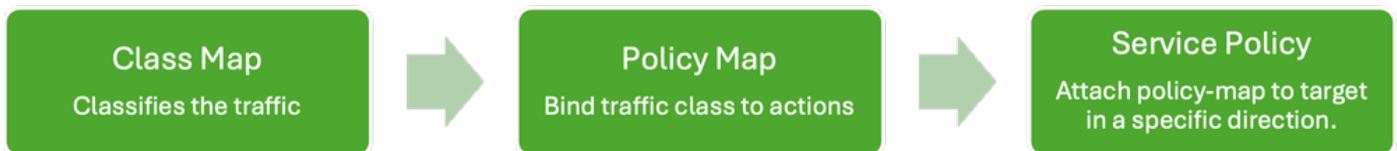
Nu Auto QoS is ingeschakeld, kunt u de veranderingen zien die hebben plaatsgevonden. In deze sectie worden de configuratiewijzigingen voor spraak weergegeven.

```
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
```

Modulaire QoS CLI

MQC staat u toe om een verkeersklasse te bepalen, een verkeersbeleid (beleidskaart) te creëren, en het verkeersbeleid aan een interface vast te maken. Het verkeersbeleid bevat de QoS-functie die van toepassing is op de verkeersklasse.



MQS CLI-werkstroom

Dit voorbeeld toont aan hoe u toegangscontrolelijsten (ACL's) kunt gebruiken om verkeer te classificeren en bandbreedtebeperkingen toe te passen.

Maak een ACL om het specifieke verkeer te identificeren en te classificeren dat u wilt beheren. Dit kan worden gedaan door regels te definiëren die verkeer aanpassen op basis van criteria zoals IP-adressen, protocollen of poorten.

Navigeer naar Configuratie > Beveiliging > ACL en voeg de ACL toe.

Configuration > Security > ACL

+ Add - Delete Associate Interfaces

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

Add ACL Setup ✕

ACL Name* ACL Type

Rules

Sequence* Action

Source Type

Destination Type

Protocol

Log DSCP

+ Add - Delete

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

1 - 2 of 2 items

ACL-configuratie

Zodra het verkeer is geclassificeerd met behulp van de ACL, configureer bandbreedtebeperkingen om de hoeveelheid bandbreedte te bepalen die aan dit verkeer is toegewezen.

Ga naar Configuration > Services > QoS en het QoS-beleid. Hang de ACL binnen het beleid en pas de politie in kbps toe.

Scroll naar beneden en selecteer het beleidsprofiel waar de QoS moet worden toegepast. U kunt het beleid in ingangsrichting selecteren voor zowel SSID als Cliënt.

Add QoS

Auto QoS DISABLED

Policy Name*

Description

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

+ Add Class-Maps

× Delete

AVC/User Defined

Match Any All

Match Type

Match Value*

Mark Type

Drop

Police(kbps)

Edit QoS

Mark:

Police(kbps):

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

Available (1)	Selected (1)				
<p>Profiles</p> <p> default-policy-profile →</p>	<p>Profiles</p> <table border="1"> <thead> <tr> <th>Ingress</th> <th>Egress</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> S <input type="checkbox"/> C</td> <td><input checked="" type="checkbox"/> S <input type="checkbox"/> C ←</td> </tr> </tbody> </table> <p> qos-policy</p>	Ingress	Egress	<input checked="" type="checkbox"/> S <input type="checkbox"/> C	<input checked="" type="checkbox"/> S <input type="checkbox"/> C ←
Ingress	Egress				
<input checked="" type="checkbox"/> S <input type="checkbox"/> C	<input checked="" type="checkbox"/> S <input type="checkbox"/> C ←				

MQS-profiel

MQS CLI-configuratie

```

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

```

Metaal QoS

Het belangrijkste doel van deze QoS-profielen is de maximale DSCP-waarden (Differentiated Services Code Point) die zijn toegestaan op een draadloos netwerk te beperken, waarbij de 802.11 User Priority (UP)-waarden worden bepaald.

In de Cisco 9800 draadloze LAN-controller (WLC) zijn de metalen QoS-profielen vooraf gedefinieerd en niet configureerbaar. U kunt deze profielen echter toepassen op specifieke SSID's of clients om QoS-beleid af te dwingen.

Er zijn vier Metal QoS profielen beschikbaar:

QoS-profiel	Max DSCP
Brons	8
Zilver	0
Goud	34
Platina	46

Zo configureert u metalen QoS op een Cisco 9800 WLC:

Ga naar Configuration > Policy > QoS en AVC.

- Selecteer het gewenste Metaal QoS profiel (Platinum, Goud, Zilver, of Brons).
- Pas het gekozen profiel toe op de doel-SSID of -client.

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

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

Auto QoS None

QoS SSID Policy

Egress platinum

Ingress platinum-up

QoS Client Policy

Egress Search or Select

Ingress Search or Select

SIP-CAC

Call Snooping

Send Disassociate

Send 486 Busy

Flow Monitor IPv4

Egress Search or Select

Ingress Search or Select

Flow Monitor IPv6

Egress Search or Select

Ingress Search or Select

Metal QoS profiel

Configuratie van Metal QoS CLI

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



Opmerking: per-gebruiker en SSID bandbreedtecontract zijn configureerbaar via QoS-beleid en niet direct op de Metal QoS. In 9800 gaat het niet-overeenkomende verkeer in de standaardklasse.



Opmerking: op de GUI kunt u alleen de Metal QoS per SSID instellen. Op CLI kunt u het ook configureren op het doel van de client.

End-to-end QoS met pakketvastlegging valideren

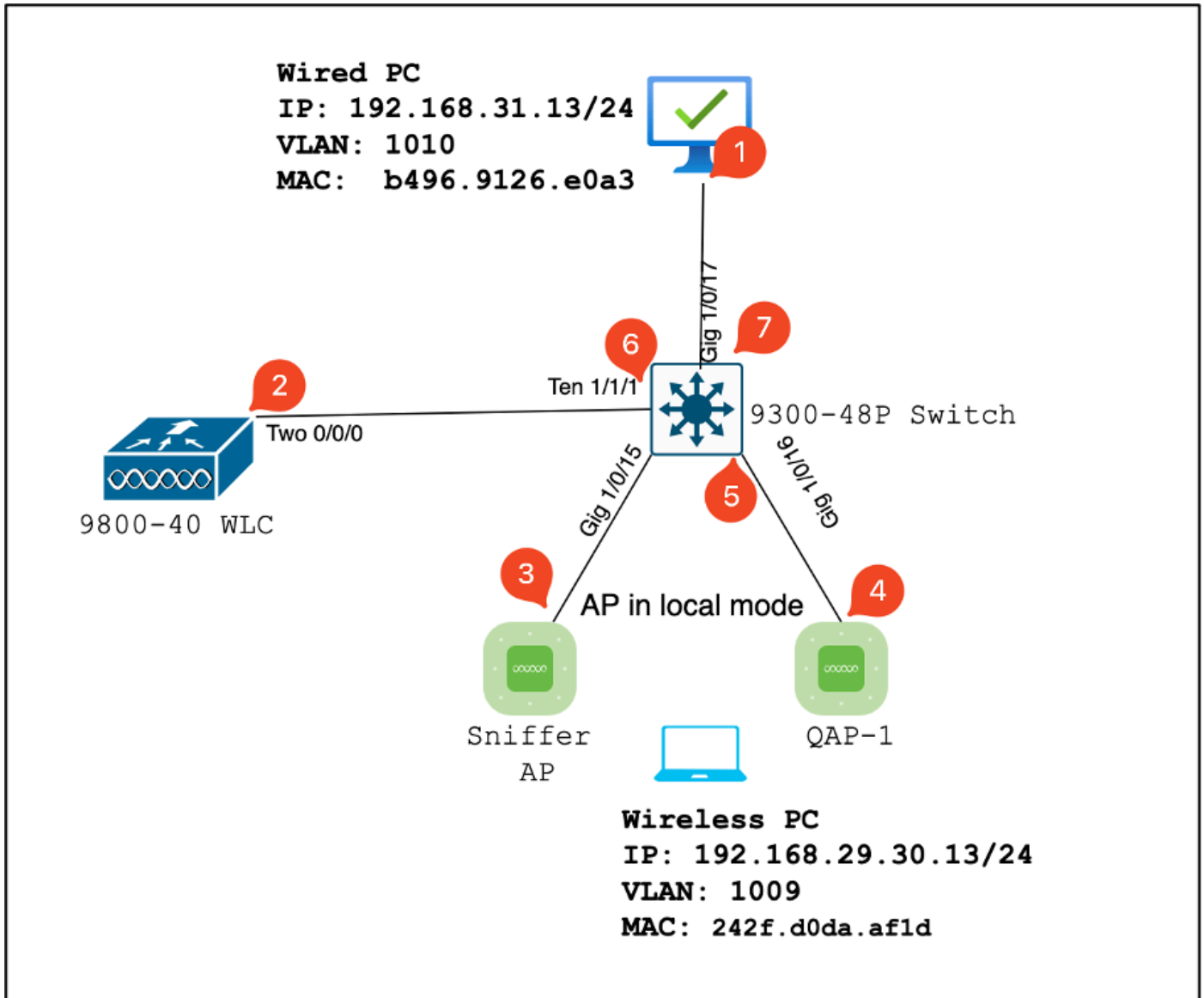
Nu de QoS-configuratie is voltooid, is het van essentieel belang om QoS-pakketten te onderzoeken en te valideren dat het QoS-beleid correct werkt van begin tot eind. Dit kan worden bereikt door pakketopname en -analyse.

Om de QoS-configuratie te repliceren en te valideren wordt een kleinschalige laboratoriumomgeving gebruikt. Het laboratorium omvat deze componenten:

- WLC
- AP
- Sniffer AP om OTA te nemen
- Bedrade pc
- Switch

Al deze onderdelen zijn verbonden met dezelfde switch in de laboratoriumomgeving. De gemarkeerde nummers in dit diagram geven de punten aan waar pakketopnamen ingeschakeld zijn om de verkeersstroom te bewaken en te analyseren.

Netwerkdigram



LAB-topologie

Lab-componenten en pakketopnamepunten

WLC:

- Beheert het QoS-beleid en de QoS-configuraties voor het draadloze netwerk.
- Packet-opnamepunt: neem verkeer op tussen WLC, AP en switch.

AP:

- Biedt draadloze connectiviteit met clients en dwingt QoS-beleid af.
- Packet-opnamepunt: neem verkeer tussen het toegangspunt en de switch op.

Sniffer AP:

- Handelt als een speciaal apparaat voor het opnemen van draadloos verkeer.
- Packet Capture point: Leg draadloos verkeer vast tussen het toegangspunt en draadloze clients.

Bedrade pc:

- Verbonden met de switch om bekabeld verkeer te simuleren en end-to-end QoS te valideren.
- Packet-opnamepunt: opname van verzonden en ontvangen QoS-pakketten via bekabelde link.

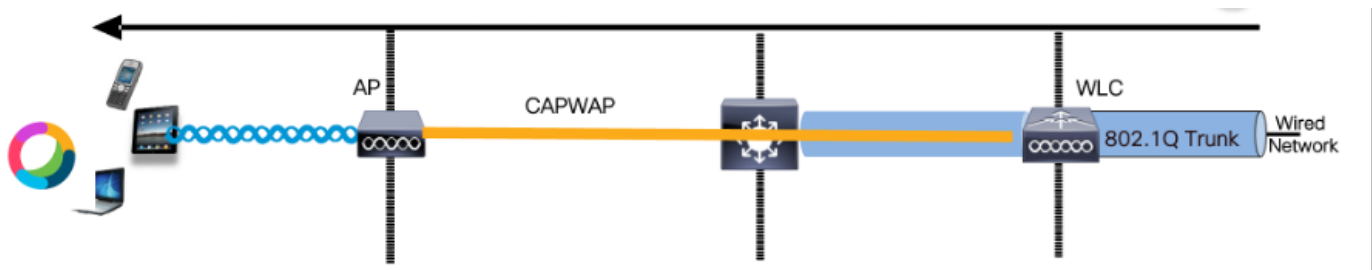
Draadloze pc:

- Verbonden met het WLAN om draadloos verkeer te simuleren en end-to-end QoS te valideren.
- Packet Capture point: Leg verzonden en ontvangen QoS-pakketten vast via draadloze link.

Switch:

- Het centrale apparaat dat alle laboratoriumcomponenten met elkaar verbindt en verkeersstroom vergemakkelijkt.
- Packet-opnamepunten: Leg verkeer op verschillende switch-poorten vast om de juiste QoS-handhaving te valideren.

Logisch gezien kan de LAB topologie als dit getekend worden.



Logische LAB-topologie

Om de QoS-configuratie te testen en te valideren, wordt Perf gebruikt om verkeer tussen de client en de server te genereren. Deze opdrachten worden gebruikt om de iPerf-communicatie te vergemakkelijken, waarbij de rollen van de server en de client worden uitgewisseld op basis van de richting van de QoS-tests.

Testscenario 1: Downstream QoS-validatie

Het doel om de downstream QoS-configuratie te valideren. De setup omvat een bekabelde PC die pakketten met DSCP 46 naar een draadloze pc stuurt.

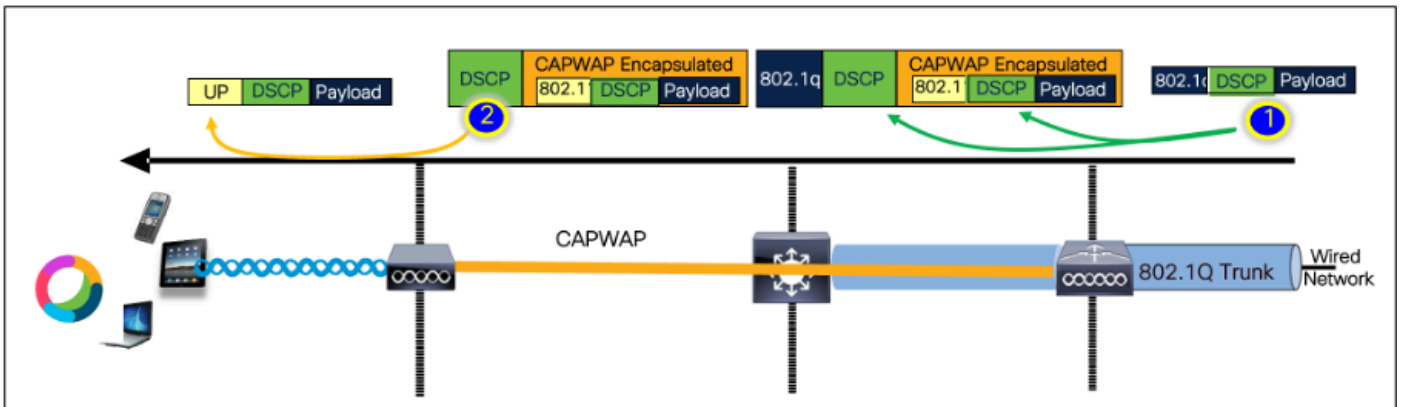
De draadloze LAN-controller (WLC) is geconfigureerd met het metalen "Platinum QoS"-beleid voor zowel downstream als upstream.

Testinstelling:

- Traffic Flow:
Bron: bekabelde pc
Bestemming: draadloze pc
Traffic Type: UDP-pakketten met DSCP 46
- QoS-beleidsconfiguratie op WLC:
QoS-profiel: Metal QoS - Platinum QoS
Richting: zowel downstream als upstream
- Opdrachten voor Metal QoS-configuratie:

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

Logische topologie en het DSCP gesprek op stroomafwaartse richting.



DSCP-conversiepoint

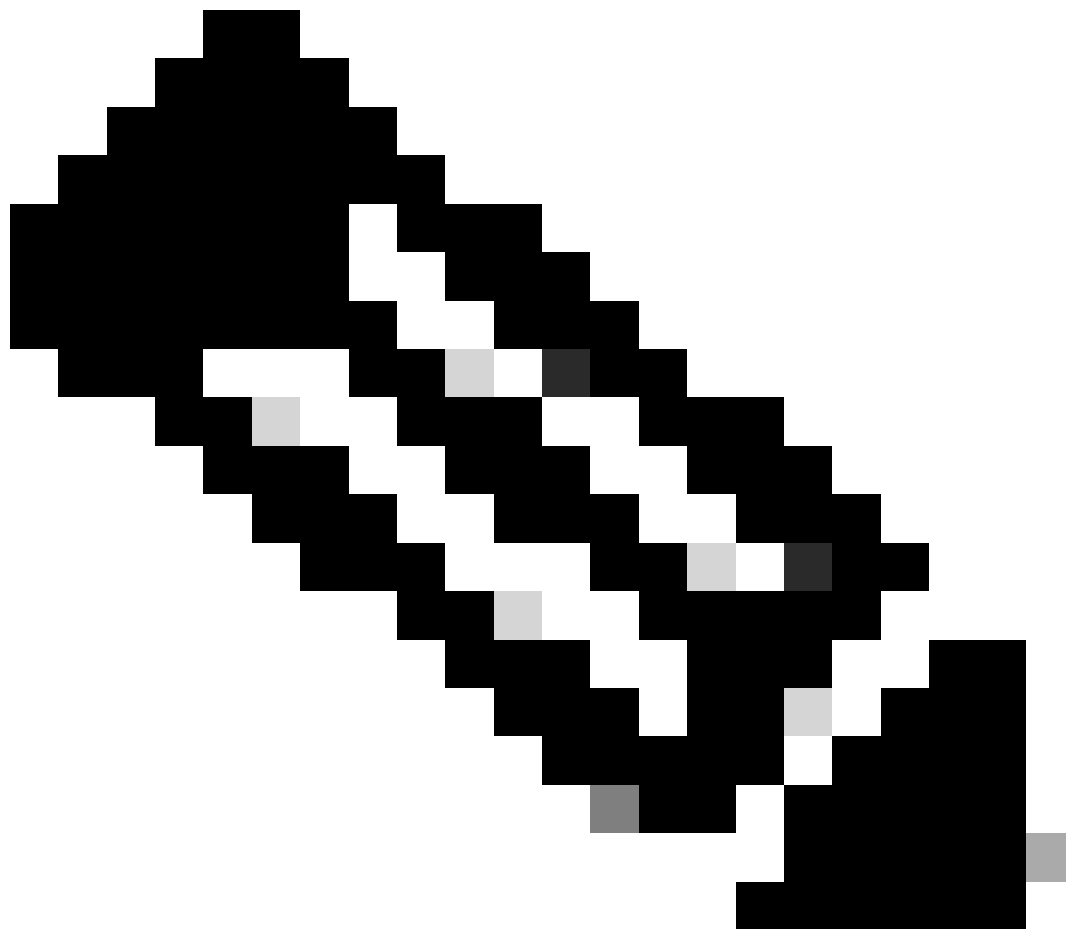
Packet Capture op de bekabelde pc. Dit bevestigt dat de bekabelde pc UDP-pakketten naar de opgegeven bestemming IP 192.168.10.13 verstuurt met de juiste DSCP-markering van 46.

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

```
> Frame 1006: 834 bytes on wire (6672 bits), 834 bytes captured (6672 bits) on interface \Device\NPF_{4003E30A-3F9F-4837-BE03-2A020715ED0A}, id 0
> Ethernet II, Src: IntelCor_26:8e8:83 (04:26:91:26:8e:83), Dst: Cisco_37:cd:f5 (2c:ab:eb:37:cd:f5)
> Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13
  .... 0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  .. 0101 00... = Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    .. 0101 00... = Differentiated Services Codepoint: Expedited Forwarding (46)
  .... 0000 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 820
  Identification: 0xc79c (51100)
```

Bedrade PC Capture - Downstream directie

Laten we vervolgens een pakket onderzoeken dat is opgenomen in de uplink-switch die is aangesloten op de bekabelde pc. De switch vertrouwt op de DSCP-tag en de DSCP-waarde blijft ongewijzigd op 46.



Opmerking: Switch poorten op de Catalyst 9000 Series zijn standaard ingesteld op een vertrouwde status.

```

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

```



```

> Frame 1006: 834 bytes on wire (6672 bits), 834 bytes captured (6672 bits) on interface \Device\NPF_{4803E30A-3F9F-4837-BEC3-2A26715EDCA}, id 0
> Ethernet II, Src: IntelCor_26:ea:8a3 (04:9e:91:26:ea:8a3), Dst: Cisco_37:cd:f5 (2c:ab:eb:37:cd:f5)
> Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13
... .. = Version: 4
... .. = Header Length: 20 bytes (5)
... .. = Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
... .. = 1011 10... = Differentiated Services Codepoint: Expedited Forwarding (46)
... .. = 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 820
Identification: 0xc79c (51108)

```

Opname van bekabelde pc-uplink-interface

Na het bestuderen van de pakketopname op de WLC genomen met behulp van EPC, komt het pakket met dezelfde DSCP-tag van 46 vanuit de uplink-switch. Dit bevestigt dat de DSCP-markering behouden blijft wanneer het pakket de WLC bereikt.

```

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

```



```

> Frame 1006: 834 bytes on wire (6672 bits), 834 bytes captured (6672 bits) on interface \Device\NPF_{4803E30A-3F9F-4837-BEC3-2A26715EDCA}, id 0
> Ethernet II, Src: IntelCor_26:ea:8a3 (04:9e:91:26:ea:8a3), Dst: Cisco_37:cd:f5 (2c:ab:eb:37:cd:f5)
> Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13
... .. = Version: 4
... .. = Header Length: 20 bytes (5)
... .. = Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
... .. = 1011 10... = Differentiated Services Codepoint: Expedited Forwarding (46)
... .. = 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 820
Identification: 0xc79c (51108)

```

WLC EPC downstream richting

Wanneer de WLC het pakket naar de AP verstuurt binnen een CAPWAP-tunnel, is het een kritieke kruising waar de WLC de DSCP kan aanpassen op basis van zijn configuratie. Laten we de pakketopname opsplitsen, die voor de duidelijkheid is gemarkeerd met genummerde punten:

- CAPWAP Buitenlaag: De buitenste laag van de CAPWAP-tunnel toont de DSCP-tag als 46, wat de waarde is die van de switch wordt ontvangen.
- 802.11 UP-waarde Inside CAPWAP: Binnen de CAPWAP-tunnel WLC brengt DSCP 46 to 802.11 User Priority (UP) 6 in kaart, die overeenkomt met het spraakverkeer.
- DSCP-waarde in CAPWAP: de Cisco 9800 WLC werkt met een DSCP-model van trust, zodat de DSCP-waarde in de CAPWAP-tunnel op 46 hetzelfde wordt gehouden als de buitenste DSCP-laag.

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

```

> Frame 2736: 988 bytes on wire (7264 bits), 988 bytes captured (7264 bits)
> Ethernet II, Src: Cisco_e7:9d:ab (08:00:0c:28:35:74), Dst: Cisco_28:35:74 (04:b4:39:28:35:74)
> IEEE 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 31
> Internet Protocol Version 4, Src: 10.105.60.198, Dst: 10.105.60.158
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x08 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
    .... 0000 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 896
  Identification: 0x0000 (0)
  > Flags: 0x00
  ... 0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 255
  Protocol: UDP (17)
  Header checksum: 0x2985 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.105.60.198
  Destination Address: 10.105.60.158
> User Datagram Protocol, Src Port: 5247, Dst Port: 5262
> Control And Provisioning of Wireless Access Points - Data
  > IEEE 802.11 QoS Data, Flags: .....F.
  Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x0000 (Swapped)
  ..000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: 24:2f:d8:d8:af:1d (24:2f:d8:d8:af:1d)
  Transmitter address: Cisco_4e:85:4f (04:b4:39:4e:85:4f)
  Destination address: 24:2f:d8:d8:af:1d (24:2f:d8:d8:af:1d)
  Source address: Cisco_37:cd:e5 (2c:ab:eb:37:cd:e5)
  BSS Id: Cisco_4e:85:4f (04:b4:39:4e:85:4f)
  STA address: 24:2f:d8:d8:af:1d (24:2f:d8:d8:af:1d)
  .... .... 0000 = Fragment number: 0
  0000 0000 0000 .... = Sequence number: 0
  > QoS Control: 0x0000
  .... .... 0110 = TID: 6
  .... .... 0000 0000 = Priority: Voice (Voice) (6)
  .... .... 0000 0000 = EOSP: Service period
  .... .... 0000 0000 = Ack Policy: Normal Ack (0x0)
  .... .... 0000 0000 = Payload Type: MSDU
  > 0000 0000 .... = QAP PS Buffer State: 0x00
  > Logical-Link Control
  > Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
    .... 0000 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 826
  
```

CAPWAP DSCP-markeringen

Controleer vervolgens hetzelfde pakket op de poort van de AP uplink switch.

De DSCP-waarde op de buitenste CAPWAP-laag blijft op 46. Voor illustratieve doeleinden wordt het interne CAPWAP-verkeer gemarkeerd om de codering weer te geven.

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

```

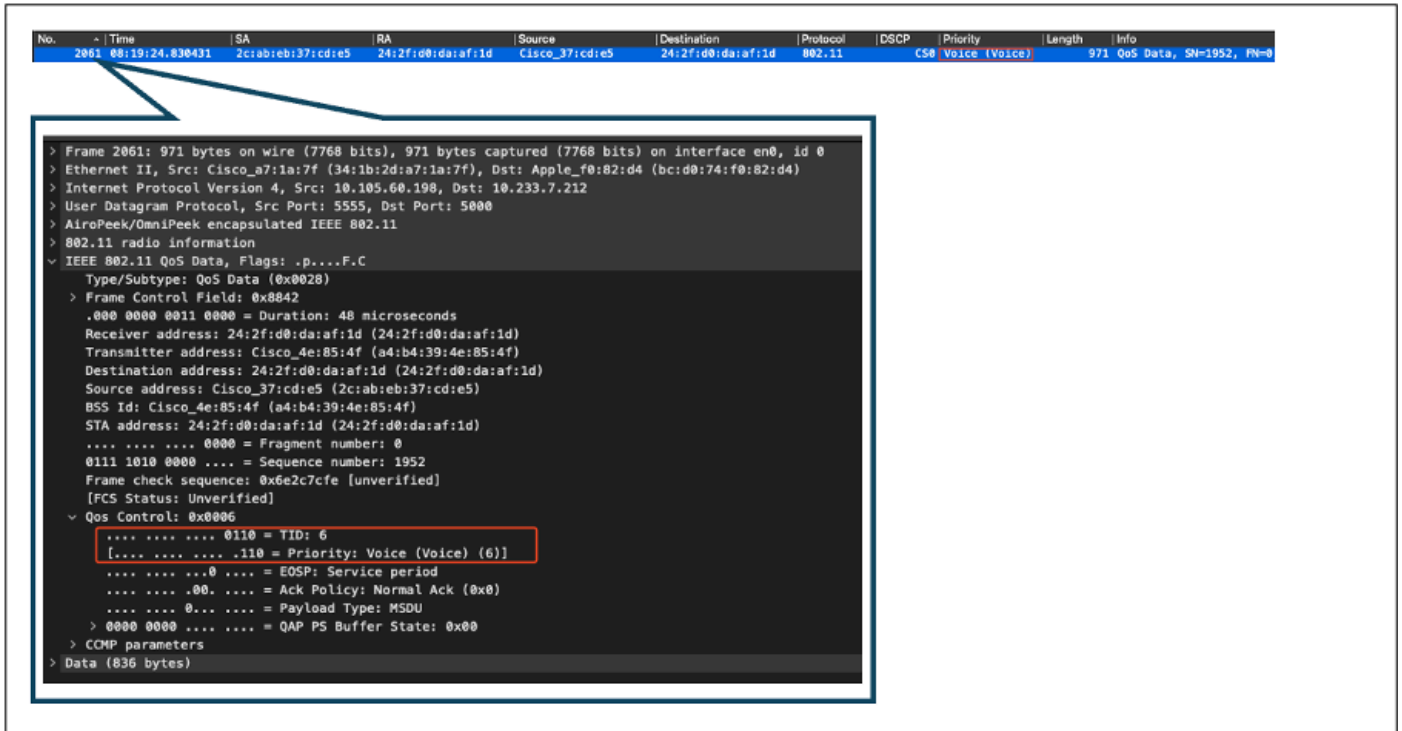
> Frame 13376: 988 bytes on wire (7264 bits), 988 bytes captured (7264 bits) on interface /tap/np_wx/wifi_to_la_uppe, id 0
> Ethernet II, Src: Cisco_e7:9d:ab (08:00:0c:28:35:74), Dst: Cisco_28:35:74 (04:b4:39:28:35:74)
> IEEE 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 31
> Internet Protocol Version 4, Src: 10.105.60.198, Dst: 10.105.60.158
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x08 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
    .... 0000 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 896
  Identification: 0x0000 (0)
  > Flags: 0x00
  ... 0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 255
  Protocol: UDP (17)
  Header checksum: 0x2985 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.105.60.198
  Destination Address: 10.105.60.158
> User Datagram Protocol, Src Port: 5247, Dst Port: 5262
> Control And Provisioning of Wireless Access Points - Data
  > Frame 1
  > Header
  > IEEE 802.11 QoS Data, Flags: .....F.
  Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x0000 (Swapped)
  ..000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: 24:2f:d8:d8:af:1d (24:2f:d8:d8:af:1d)
  Transmitter address: Cisco_4e:85:4f (04:b4:39:4e:85:4f)
  Destination address: 24:2f:d8:d8:af:1d (24:2f:d8:d8:af:1d)
  Source address: Cisco_37:cd:e5 (2c:ab:eb:37:cd:e5)
  BSS Id: Cisco_4e:85:4f (04:b4:39:4e:85:4f)
  STA address: 24:2f:d8:d8:af:1d (24:2f:d8:d8:af:1d)
  .... .... 0000 = Fragment number: 0
  0000 0000 0000 .... = Sequence number: 0
  > QoS Control: 0x0000
  .... .... 0110 = TID: 6
  .... .... 0000 0000 = Priority: Voice (Voice) (6)
  .... .... 0000 0000 = EOSP: Service period
  .... .... 0000 0000 = Ack Policy: Normal Ack (0x0)
  .... .... 0000 0000 = Payload Type: MSDU
  > 0000 0000 .... = QAP PS Buffer State: 0x00
  > Logical-Link Control
  > Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
    .... 0000 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  
```

AP Uplink Switch Interface Capture

Zodra AP het pakket ontvangt, brengt het het pakket over de lucht over. Om de User Priority (UP)-

markering te verifiëren, wordt een Over-the-Air (OTA) opname die met een snuffeltoegangspunt is genomen, gebruikt.

AP heeft het kader met een UP waarde van 6 door:sturen. Dit bevestigt dat het toegangspunt de DSCP-waarde correct toewijst aan de juiste 802.11 UP-waarde (6), die overeenkomt met het spraakverkeer.



The image shows a Wireshark packet capture of an IEEE 802.11 radio frame. The top table lists the packet details: No. 2061, Time 08:19:24.830431, SA 2c:ab:eb:37:cd:e5, RA 24:2f:d0:da:af:1d, Source Cisco_37:cd:e5, Destination 24:2f:d0:da:af:1d, Protocol 802.11, DSCP CS0 Voice (Voice), Priority CS0 Voice (Voice), Length 971, Info QoS Data, SN=1952, FN=0. Below the table, the packet details pane shows the IEEE 802.11 radio information, including the QoS Data section. The QoS Control field is expanded to show the TID (0110) and Priority (0110) fields, both of which are highlighted with a red box. The TID field is labeled 'TID: 6' and the Priority field is labeled 'Priority: Voice (Voice) (6)'. Other fields shown include Duration (48 microseconds), Receiver address (24:2f:d0:da:af:1d), Transmitter address (Cisco_4e:85:4f), Destination address (24:2f:d0:da:af:1d), Source address (Cisco_37:cd:e5), BSS Id (Cisco_4e:85:4f), STA address (24:2f:d0:da:af:1d), Fragment number (0), Sequence number (0111 1010 0000), Frame check sequence (0x6e2c7cfe), and QAP PS Buffer State (0x00).

OTA-opname van AP naar client

In de laatste fase wordt het pakket ontvangen door de draadloze pc. De draadloze pc ontvangt het frame met een DSCP-waarde van 46.

Dit geeft aan dat de DSCP-markering in het gehele transmissiepad behouden blijft, van de bekabelde pc tot de draadloze pc. De consistente DSCP-waarde van 46 bevestigt dat het QoS-beleid correct wordt toegepast en in de downstream-richting wordt onderhouden.

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


```

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

Draadloze pc-vastlegging

Testscenario 2: Upstream QoS-validatie

In dit testscenario is het doel de upstream QoS-configuratie te valideren. De setup omvat een draadloze PC die UDP-pakketten met DSCP 46 naar een bekabelde pc stuurt. De WLC is geconfigureerd met het Metal "Platinum QoS" beleid voor zowel upstream als downstream richtingen.

- Traffic Flow:

Bron: draadloze pc

Bestemming: bekabelde pc

Traffic Type: UDP-pakketten met DSCP 46

- QoS-beleidsconfiguratie op WLC:

QoS-profiel: Platinum QoS

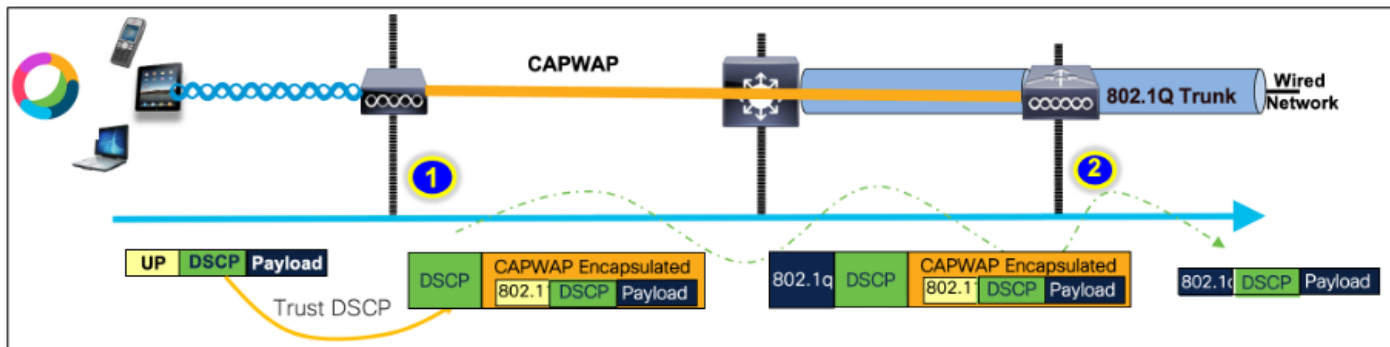
Richting: zowel upstream als downstream

- Opdrachten voor Metal QoS-configuratie:

```

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

Logische topologie en DSCP-conversie in upstream-richting:



Logische topologie en DSCP-conversie - upstream

Pakketten die van draadloze PC naar bekabelde PC worden verzonden. Deze opname wordt genomen op de draadloze pc.

De draadloze pc stuurt UDP-pakketten met DSCP 46.

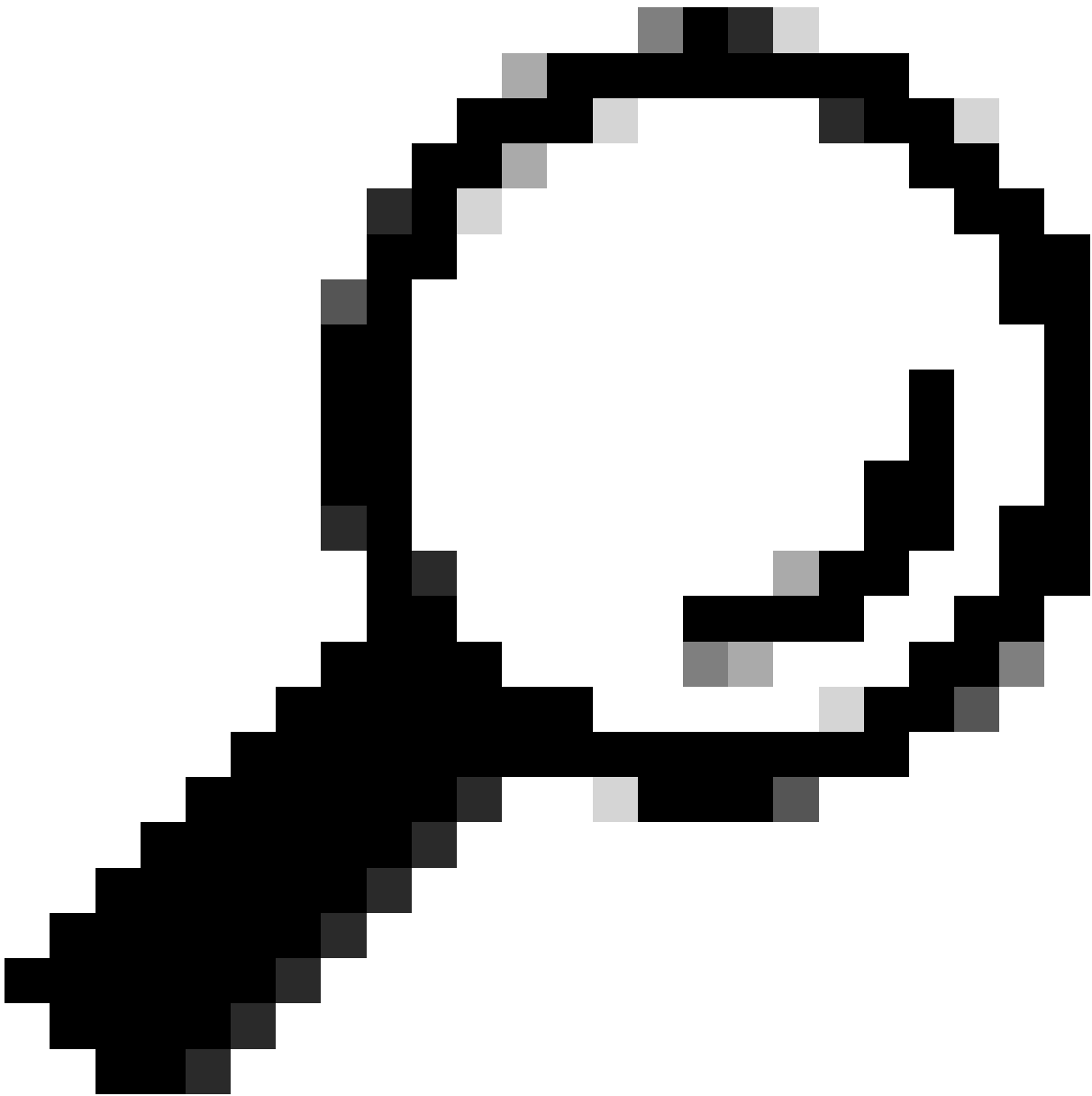
No.	Time	SA	RA	Source	Destination	Protocol	DSCP	Priority	Length	Info
241	10:53:22.943438			192.168.30.13	192.168.31.10	UDP	EF PHB		834	52121 → 5201 Len=8192

```

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

Draadloze PC Capture in upstream richting

Laten we vervolgens kijken naar de OTA-opname van client naar AP.



Tip: wanneer u een draadloze Windows-pc gebruikt om pakketten met DSCP 46 te verzenden, wijst Windows DSCP 46 toe aan een User Priority (UP)-waarde van 5 (Video). Dientengevolge, toont OTA de pakketten als Videoverkeer (UP 5). Als u het pakket echter decodeert, blijft de DSCP-waarde 46.



Opmerking: vanaf versie 17.4 is het standaardgedrag voor de Cisco 9800 WLC dat de DSCP-waarde in het AP-samenvoegprofiel wordt vertrouwd. Dit waarborgt dat de waarde DSCP van 46 wordt bewaard en door WLC vertrouwd op, die om het even welke kwesties verhindert met betrekking tot Windows DSCP aan het in kaart brengen van gedrag.

QoS Control Field: \$0000000000000101

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

802.2 Logical Link Control (LLC) Header

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

IP Header - Internet Protocol Datagram

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

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

Toewijzing van Windows UP naar DSCP

De versleutelde over-the-air (OTA) opname die is genomen uit de laboratoriumopstelling wordt geanalyseerd om de upstream QoS-configuratie te valideren.

De OTA-opname toont de pakketten met een User Priority (UP) waarde van 5 (Video). Hoewel de OTA-opname 5 weergeeft, blijft de DSCP-waarde in het gecodeerde pakket op 46.

No.	Time	SA	RA	Source	Destination	Protocol	DSCP	Priority	Length	Info
5643	10:53:22.982358	24:2f:d0:da:af:1d	a4:b4:39:4e:85:4f	24:2f:d0:da:af:1d	Cisco_37:cd:e5	802.11	CS0	Video (Video)	1442	QoS Data, SN=1347

```

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

LAB Setup OTA in upstream richting

Vervolgens wordt de pakketopname op de AP uplink-poort geanalyseerd om ervoor te zorgen dat de DSCP-waarde behouden blijft terwijl het pakket van de AP naar de WLC beweegt.

- De DSCP-waarde op de buitenste CAPWAP-laag wordt op 46 gehandhaafd.
- Binnen de CAPWAP-tunnel wordt de DSCP-waarde ook op 46 gehouden.

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


```

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

AP PpLink Capture in upstream directie

De opname wordt genomen bij WLC als het pakket uit de switch komt.

- Het pakket komt bij WLC met de waarde DSCP van 46 op de buitenlaag van CAPWAP aan.
- In de CAPWAP-tunnel blijft de DSCP-waarde 46.

No.	Time	SA	RA	Source	Destination	Protocol	DSCP	Priority	Length	Info
516	10:53:22.989939	24:2f:d0:da:af:1d	a4:b4:39:4e:85:40	10.185.60.158	10.185.60.198	CAPWAP-Data	EF PHB		1502	CAPWAP-Data (Fragment ID: 148)
517	10:53:22.989939	24:2f:d0:da:af:1d	a4:b4:39:4e:85:40	192.168.30.13	192.168.31.10	IPv4	EF PHB	Video (Video)	148	Fragmented IP protocol (p)

```

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

```

WLC EPC die pakketten toont die uit AP komen

Nadat het pakket een haarspeldbocht bij WLC neemt, wordt het teruggestuurd naar de opstraalverbinding switch, bestemd voor de bekabelde PC. WLC doorsturen het pakket met de waarde DSCP van 46.

No.	Time	SA	RA	Source	Destination	Protocol	DSCP	Priority	Length	Info
528	10:53:23.000000	24:2f:d0:da:af:1d	2c:ab:eb:37:cd:e5	192.168.30.13	192.168.31.10	UDP	EF PHB		838	52121 → 5201 Len=8192

```

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

```

WLC EPC toont pakketten die naar bekabelde pc worden verzonden

Tenslotte wordt de pakketopname bij de bekabelde pc-uplink geanalyseerd om ervoor te zorgen dat de DSCP-waarde behouden blijft aangezien het pakket uit de WLC komt.

5039	10:53:23.187287	192.168.30.13	192.168.31.10	IPv4	EF PHB	1518	Fragmented IP protocol (p)
5040	10:53:23.187381	192.168.30.13	192.168.31.10	IPv4	EF PHB	1518	Fragmented IP protocol (p)

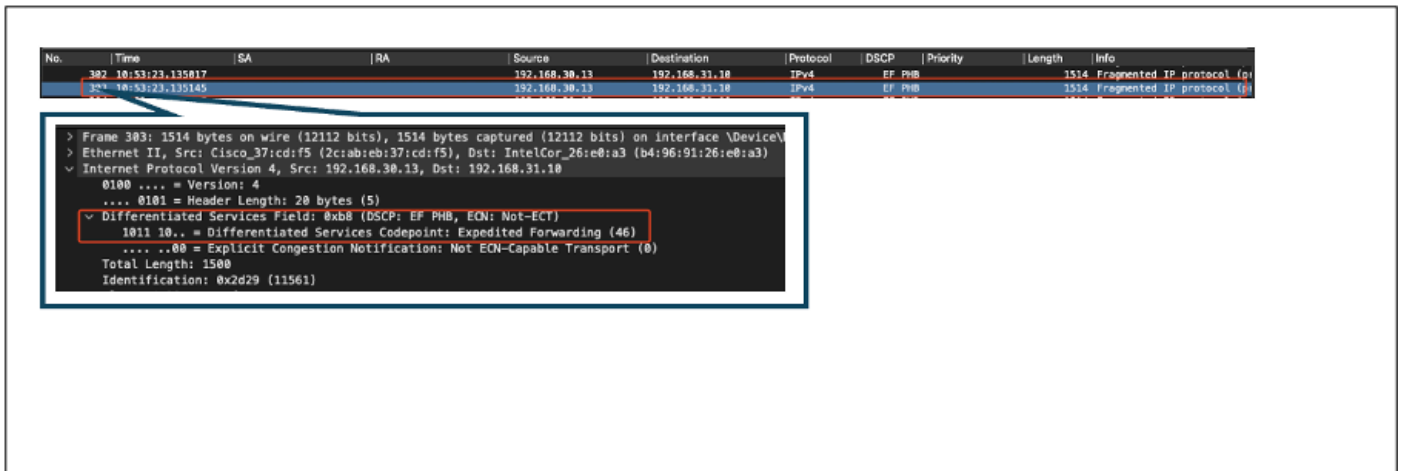
```

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

```

Opname van bekabelde pc-uplink-Switch in upstream-richting

In de laatste fase wordt het pakket dat door de bekabelde pc wordt ontvangen, geanalyseerd om er zeker van te zijn dat het pakket op de bekabelde pc aankomt met de DSCP-waarde 46.



Bedrade pc-opname - stroomopwaartse richting

De upstream QoS-test heeft de QoS-configuratie voor verkeer dat van de draadloze pc naar de bekabelde pc loopt, met succes gevalideerd. Het consequente behoud van de DSCP-waarde van 46 over het gehele transmissiepad bevestigt dat het QoS-beleid correct wordt toegepast en afgedwongen.

Probleemoplossing

Spraak, video en andere real-time toepassingen zijn bijzonder gevoelig voor problemen met netwerkprestaties en elke verslechtering van de Quality of Service (QoS) kan opmerkelijke en schadelijke effecten hebben. Wanneer QoS-pakketten worden gemerkt met lagere DSCP-waarden, kan het effect op spraak en video significant zijn.

Impact op spraak:

- Verhoogde Latency: de communicatie van de stem vereist lage latentie om ervoor te zorgen dat de gesprekken natuurlijk en vloeiend zijn. De lagere waarden DSCP kunnen in spraakpakketten resulteren die worden vertraagd, veroorzakend merkbare vertraging in gesprekken.
- Jitter: Variabiliteit in pakketaankomsttijden (jitter) kan de soepele levering van spraakpakketten verstoren. Dit kan leiden tot choppy of vervormde audio, waardoor het moeilijk is om de luidspreker te begrijpen.
- Packet Loss: spraakpakketten zijn zeer gevoelig voor pakketverlies. Zelfs een kleine hoeveelheid pakketverlies kan resulteren in ontbrekende woorden of lettergrepen, wat kan leiden tot slechte gesprekskwaliteit en misverstanden.
- Echo en vervorming: verhoogde latentie en jitter kunnen echo en audiovervalsing veroorzaken, wat de kwaliteit van de spraakoproep verder kan aantasten.

Impact op video:

- Verhoogde latentie: voor videocommunicatie is lage latentie nodig om de synchronisatie tussen audio- en videostreamen te behouden. Verhoogde latentie kan vertragingen veroorzaken, die het moeilijk maken om interactie in real time te hebben.
- Jitter: Jitter kan ervoor zorgen dat videoframes niet goed of op onregelmatige tijdstippen uitkomen, wat leidt tot een schokkerige of stotterende video-ervaring.
- Packet Loss: Verloren pakketten kunnen resulteren in ontbrekende frames, wat ervoor kan zorgen dat de video bevriest of artefacten weergeeft.
- Verminderde videokwaliteit: lagere DSCP-waarden kunnen leiden tot verminderde bandbreedte-toewijzing voor videostreamen, wat leidt tot een lagere resolutie en een slechtere videokwaliteit. Dit kan het moeilijk maken om belangrijke details in de video te zien.

Scenario 1: Intermediate Switch herschrijft DSCP-markering

In dit probleemoplossingscenario wordt de impact van een tussenliggende switch die de DSCP-markering op het verkeer herschrijft wanneer deze bij de WLC aankomt, onderzocht. Om dit te herhalen, wordt de switch geconfigureerd om de DSCP 46-markering te herschrijven naar CS1 op de bekabelde pc-uplinkinterface.

Het pakket wordt verzonden vanaf de bekabelde pc met een DSCP 46-tag.

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

Bedrade PC die pakket met DSCP 46 Markering verzenden

Het pakket komt bij WLC met een waarde DSCP van CS1 (DSCP 8) aan. De verandering van DSCP 46 in DSCP 8 vermindert beduidend de prioriteit van het pakket.

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

WLC EPC met CS1-markering

In deze stap wordt het pakket dat door de WLC naar de AP wordt doorgestuurd, geanalyseerd.

- De buitenste CAPWAP header is getagd met CS1 (DSCP 8).

- De binnenste CAPWAP header is ook gelabeld met CS1 (DSCP 8).
- De waarde Gebruiker Prioriteit (UP) is ingesteld op BK (Achtergrond).

```

> Frame 140: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits)
> Ethernet II, Src: Cisco_e7:9d:ab (80:2d:bf:e7:9d:ab), Dst: Cisco_28:35:74 (a4:b4:39:28:35:74)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 31
> Internet Protocol Version 4, Src: 10.105.60.198, Dst: 10.105.60.158
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  <span style="color:red; font-weight:bold; border: 1px solid red; padding: 2px;">> Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (8)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 146
  Identification: 0x0000 (0)
  <span style="color:red; font-weight:bold; border: 1px solid red; border-radius: 50%; padding: 2px; float: right;">1
  > Flags: 0x00
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 255
  Protocol: UDP (17)
  Header Checksum: 0x2d05 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.105.60.198
  Destination Address: 10.105.60.158
  > User Datagram Protocol, Src Port: 5247, Dst Port: 5262
  > Control And Provisioning of Wireless Access Points - Data
  > [2 Message fragments (1534 bytes): #139(1424), #140(110)]
  > IEEE 802.11 QoS Data, Flags: .....F.
  Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8800(Swapped)
  .000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
  Transmitter address: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
  Destination address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
  Source address: Cisco_37:cd:e5 (2c:ab:eb:37:cd:e5)
  BSS Id: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
  STA address: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d)
  .... .... 0000 = Fragment number: 0
  0000 0000 0000 .... = Sequence number: 0
  > Qos Control: 0x0001
  .... .... 0001 = TID: 1
  <span style="color:red; font-weight:bold; border: 1px solid red; padding: 2px;">[.... .... 001 = Priority: Background (Background) (1)]
  .... .... 00.. = EOSP: Service period
  .... .... 00.. = Ack Policy: Normal Ack (0x0)
  .... .... 0... = Payload Type: MSDU
  > 0000 0000 .... = QAP PS Buffer State: 0x00
  > Logical-Link Control
  > Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  <span style="color:red; font-weight:bold; border: 1px solid red; padding: 2px;">> Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (8)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 1500
  Identification: 0x5a41 (23105)
  <span style="color:red; font-weight:bold; border: 1px solid red; border-radius: 50%; padding: 2px; float: right;">3
  <span style="color:red; font-weight:bold; border: 1px solid red; border-radius: 50%; padding: 2px; float: right; margin-top: -100px; margin-left: 100px;">2

```

WLC EPC laat CS1-tag zien in CAPWAP Traffic

Het pakket komt bij draadloze PC met een waarde DSCP van CS1 (DSCP 8) aan.

```

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

```

Dit scenario toont aan hoe een misconfiguratie op een intermediaire switch de QoS-configuratie kan doorbreken, wat leidt tot verslechterde prestaties voor prioritair verkeer. De spraakpakketten, die aanvankelijk gemarkeerd waren voor hoge prioriteit, werden behandeld als verkeer met een lagere prioriteit vanwege de DSCP-herschrijving. Dit scenario onderstreept het belang om ervoor te zorgen dat de middennetwerkapparaten correct de markeringen van QoS bewaren om de gewenste kwaliteit van de dienst voor prioritair verkeer te handhaven.

Scenario 2: AP link Switch herschrijft DSCP-markering

In dit scenario wordt de impact onderzocht van een intermediaire switch die is aangesloten op de AP die de DSCP-markering herschrijft op het verkeer.

- De switch die is aangesloten op het toegangspunt is geconfigureerd om de DSCP 46-markering te herschrijven naar een andere waarde CS1 op de AP-uplinkinterface.
- Het pakket wordt verzonden vanaf de bekabelde pc met een DSCP-tag van 46. Dit bevestigt dat het verkeer correct met DSCP 46 bij de bron wordt gemarkeerd.

```
> Frame 923: 834 bytes on wire (6672 bits), 834 bytes captured (6672 bits) on interface \Device\NPF_{009
> Ethernet II, Src: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d), Dst: Cisco_37:cd:e5 (2c:ab:eb:37:cd:e5)
v Internet Protocol Version 4, Src: 192.168.30.13, Dst: 192.168.31.10
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 820
  Identification: 0xcd67 (52583)
  v 0000 .....
```

De opname wordt genomen bij WLC als het pakket uit de switch komt.

Het pakket komt bij WLC met de router CAPWAP header DSCP waarde van CS1 (DSCP) en de binnen DSCP waarde van 46. Dit gebeurt omdat de tussenliggende switch het verkeer niet kan zien dat ingekapseld is in de CAPWAP-tunnel.

De WLC vertrouwt op de DSCP-tag in de CAPWAP-tunnel en stuurt het verkeer door naar de bekabelde pc met de interne DSCP-tag van 46.


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

WLC EPC met CAPWAP DSCP-waarden

Het pakket wordt op de bekabelde pc ontvangen met een DSCP-waarde van 46. Bevestigt dat WLC het pakket met de originele waarde DSCP van 46 correct door:sturen, die de prioriteitsmarkering bewaart.

```

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

```

Bedrade pc ontvangen pakket met DSCP 46

Hoewel de WLC het verkeer doorstuurt met een DSCP-tag van 46, is het belangrijk om te begrijpen dat het verkeer van de AP naar de WLC als lage prioriteit werd behandeld doordat de buitenste DSCP-tag werd herschreven naar CS1 (DSCP 8).

Er kunnen meerdere switches zijn tussen de AP en de WLC, en als het verkeer een lage prioriteit heeft, kan het laat bij de WLC aankomen. Dit kan leiden tot verhoogde latentie, jitter en mogelijk pakketverlies, wat de kwaliteit van de service voor verkeer met hoge prioriteit zoals spraak kan verslechteren.

Tip voor probleemoplossing

1. Controleer de eerste DSCP-markering: Leg pakketten vast aan de bron (bijvoorbeeld bekabelde pc) om er zeker van te zijn dat het verkeer correct is gemarkeerd met de beoogde DSCP-waarde.
2. Controleer de configuraties van intermediaire apparaten: controleer de configuratie van alle intermediaire switches en routers om er zeker van te zijn dat ze niet per ongeluk DSCP-waarden herschrijven.
3. Leg verkeer op belangrijke punten vast:
 1. Voor en na de tussenliggende switch.
 2. Bij de WLC.
 3. Op de bestemming (bijvoorbeeld draadloze pc).
4. Simuleer verkeersscenario's: gebruik verkeersgeneratoren of netwerksimulatie tools om verschillende soorten verkeer te maken en observeer hoe QoS wordt verwerkt door het draadloze netwerk.
5. Raadpleeg het best practice-document van 9800: bekijk de documentatie over best practices van 9800 over het configureren van QoS- en DSCP-markeringen.

Configuratieverificatie

<#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
```

Conclusie

Het handhaven van consistente QoS-configuratie over het netwerk is cruciaal om ervoor te zorgen dat verkeer met hoge prioriteit, zoals spraak en video, het juiste niveau van service en prestaties ontvangt. Het is essentieel om QoS-configuraties regelmatig te valideren om ervoor te zorgen dat alle netwerkapparaten voldoen aan het beoogde QoS-beleid. Deze validatie helpt bij het identificeren en corrigeren van fouten in de configuratie of afwijkingen die de netwerkprestaties in gevaar kunnen brengen.

Referenties

- [Inzicht in en probleemoplossing voor Cisco Catalyst 9800 Series draadloze controllers](#)
- [Beste praktijken voor Cisco Catalyst 9800 Series configuratie](#)
- [Software voor Cisco Catalyst 9800 Series softwareconfiguratiehandleiding voor draadloze controllers, Cisco IOS® XE Dublin 17.12.x](#)
- [Handleiding voor probleemoplossing bij Voice over Wireless LAN \(VoWLAN\)](#)
- [DSCP QoS-tagging op Windows-machines inschakelen](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.