

# Konfigurieren von Validierung und Fehlerbehebung für Wireless QoS auf dem 9800 WLC

## Inhalt

---

[Einleitung](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfiguration](#)

[QoS-Richtlinienziele](#)

[Automatische QoS](#)

[Konfiguration der Auto QoS CLI](#)

[Modulare QoS-CLI](#)

[MQS-CLI-Konfiguration](#)

[Metall-QoS](#)

[Konfiguration der Metall-QoS-CLI](#)

[Validierung der End-to-End-QoS mit Paketerfassung](#)

[Netzwerkdiagramm](#)

[Laborkomponenten und Paketerfassungspunkte](#)

[Testszenario 1: Downstream-QoS-Validierung](#)

[Testszenario 2: Upstream-QoS-Validierung](#)

[Fehlerbehebung](#)

[Szenario 1: Zwischen-Switch schreibt DSCP-Markierung um](#)

[Szenario 2: AP-Link-Switch überschreibt DSCP-Markierung](#)

[Tipp zur Fehlerbehebung](#)

[Konfigurationsverifizierung](#)

[Schlussfolgerung](#)

[Referenzen](#)

---

## Einleitung

In diesem Dokument werden Möglichkeiten zur Konfiguration, Validierung und Fehlerbehebung von Wireless Quality of Service (QoS) auf dem Wireless LAN Controller (WLC) der Serie 9800 beschrieben.

## Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- WLC: C9800-40-K9 mit 17.12.03
- Access Point (AP): C9120-AX-D
- Switch: C9300-48P mit 17.03.05
- Kabelgebundener und Wireless-Client: Windows 10

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Hintergrundinformationen

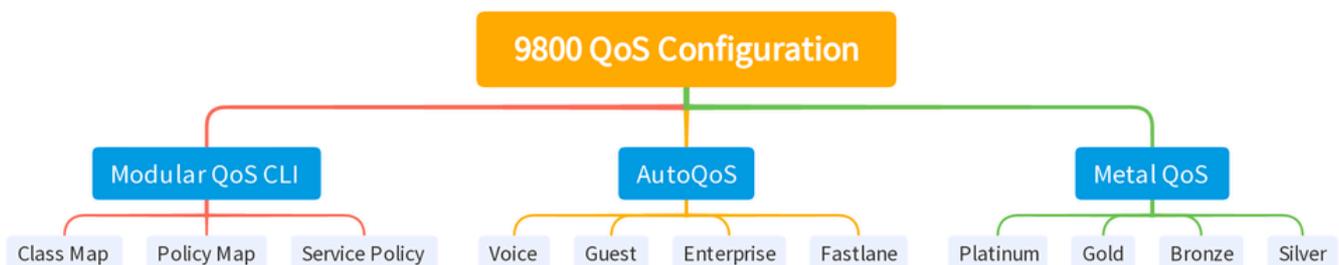
Wireless QoS ist eine wichtige Voraussetzung, um sicherzustellen, dass wichtige Anwendungen die für eine optimale Leistung erforderliche Bandbreite und niedrige Latenz erhalten. Dieses Dokument bietet einen umfassenden Leitfaden für die Konfiguration, Validierung und Fehlerbehebung von QoS in Cisco Wireless-Netzwerken.

In diesem Artikel wird davon ausgegangen, dass die Leser grundlegende Kenntnisse der QoS-Prinzipien für Wireless und kabelgebundene Netzwerke haben. Es wird außerdem erwartet, dass die Leser mit der Konfiguration und Verwaltung von Cisco WLCs und APs vertraut sind.

## Konfiguration

In diesem Abschnitt wird die Konfiguration der QoS auf Wireless Controllern der Serie 9800 beschrieben. Durch die Nutzung dieser Konfigurationen können Sie sicherstellen, dass wichtige Anwendungen die erforderliche Bandbreite und niedrige Latenz erhalten und dadurch die Netzwerkleistung insgesamt optimieren.

Sie können die QoS-Konfiguration des Cisco Catalyst 9800 WLC in drei grobe Kategorien unterteilen.



Zusammenfassung der QoS-Konfiguration des 9800 WLC

Dieses Dokument wird in den folgenden Abschnitten Schritt für Schritt durch die einzelnen Abschnitte geführt.

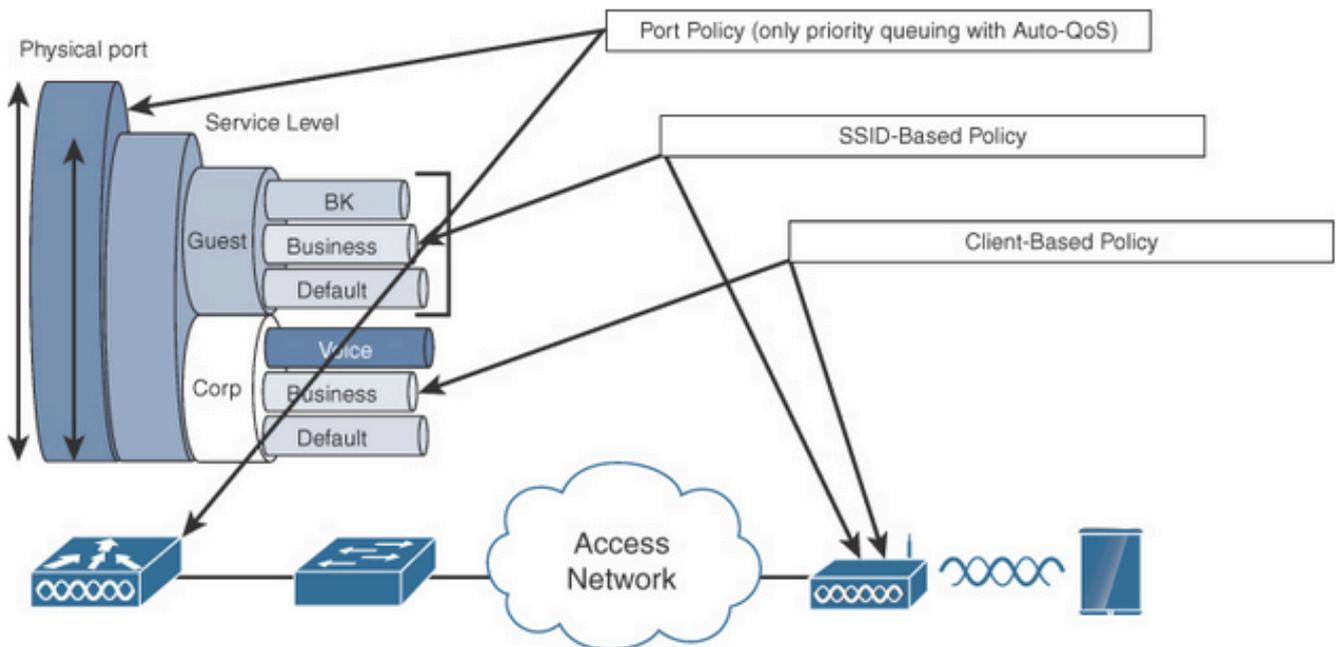


Hinweis: In diesem Artikel wird AP im lokalen Modus behandelt. Der Access Point im Flexconnect-Modus wird nicht behandelt.

---

## QoS-Richtlinienziele

Ein Richtlinienziel ist das Konfigurationskonstrukt, auf das eine QoS-Richtlinie angewendet werden kann. Die QoS-Implementierung auf dem Catalyst 9800 ist modular und flexibel. Der Benutzer kann sich für die Konfiguration von Richtlinien auf drei verschiedenen Ebenen entscheiden: SSID, Client und Port.



#### QoS-Richtlinienziele

Die SSID-Richtlinie gilt für jeden Access Point und jede SSID. Sie können Richtlinien und Marking-Richtlinien für SSID konfigurieren.

Client-Richtlinien gelten in Eingangs- und Ausgangsrichtung. Sie können Richtlinien für Richtlinien und Markierungen auf Clients konfigurieren. AAA override wird ebenfalls unterstützt.

Die portbasierten QoS-Richtlinien können an einem physischen oder an einem logischen Port angewendet werden.

#### Automatische QoS

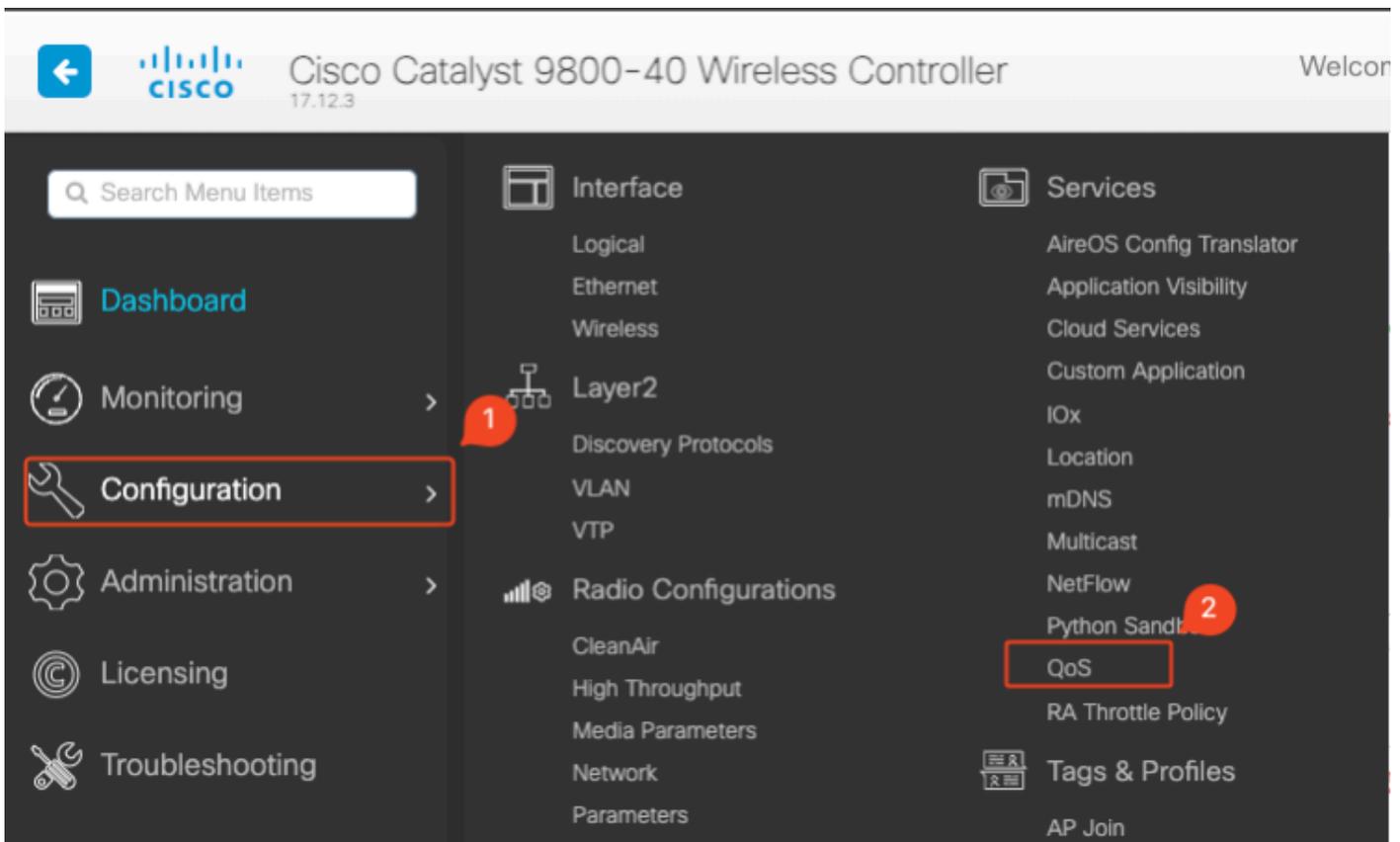
Wireless Auto QoS automatisiert die Bereitstellung von Wireless QoS-Funktionen. Er verfügt über eine Reihe vordefinierter Profile, die vom Administrator weiter geändert werden können, um verschiedene Datenverkehrsflüsse zu priorisieren. Auto-QoS gleicht den Datenverkehr ab und weist jedes zugeordnete Paket QoS-Gruppen zu. Auf diese Weise kann die Ausgaberrichtlinienkarte bestimmte QoS-Gruppen in bestimmte Warteschlangen einordnen, einschließlich der Prioritätswarteschlange.

Modus	Client-Eingang	Client-Ausgang	BSSID-Eingang	BSSID-Ausgang	Port-Eingang	Port-Ausgang	Funk
Voice	–	–	Platin-Up	Platin	–	AutoQoS-4.0-wlan-port-output-policy	ACM ein

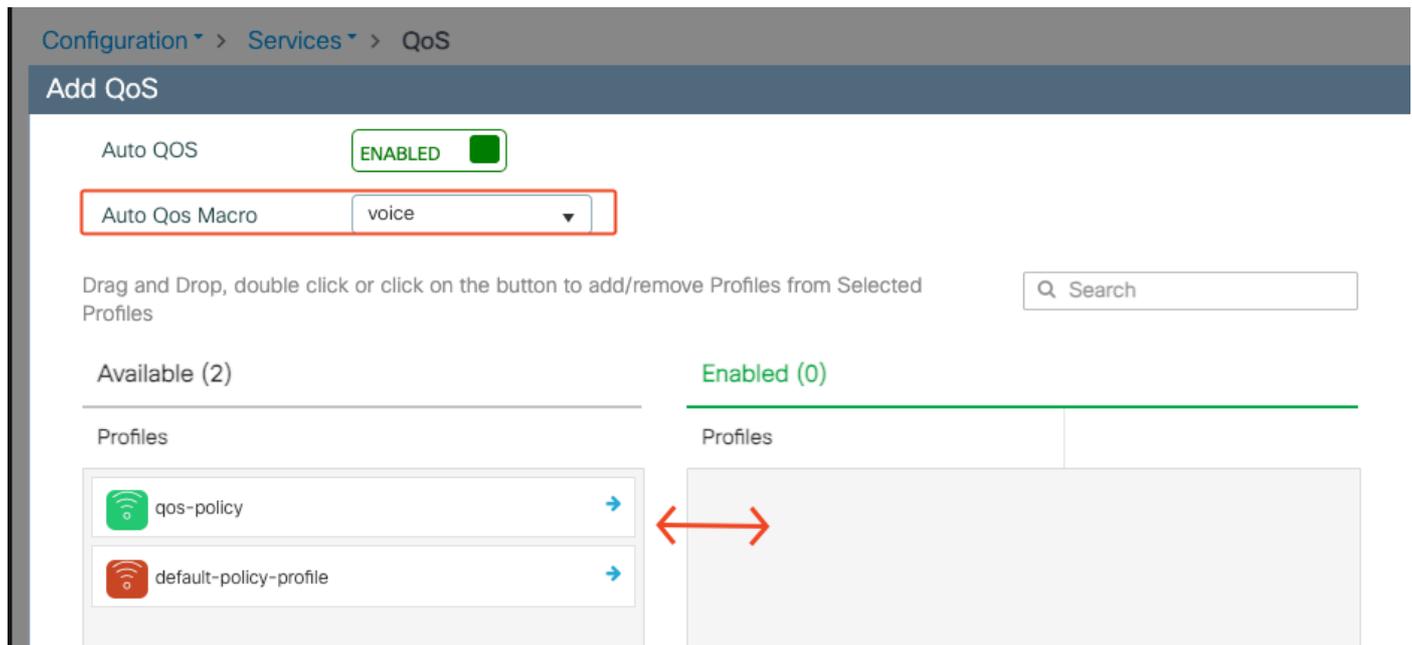
Gast	-	-	AutoQos-4.0-wlan-GT-SSID-Eingaberichtlinie	AutoQos-4.0-wlan-GT-SSID-Ausgaberichtlinie	-	AutoQoS-4.0-wlan-port-output-policy	
Fastlane	-	-			-	AutoQoS-4.0-wlan-port-output-policy	edca-parameter fastlane
Enterprise-AVC	-	-	AutoQos-4.0-wlan-ET-SSID-Eingabe-AVC-Richtlinie	AutoQos-4.0-wlan-ET-SSID-Ausgaberichtlinie	-	AutoQoS-4.0-wlan-port-output-policy	

Diese Tabelle zeigt die Konfigurationsänderungen, die bei der Anwendung eines automatischen QoS-Profiles vorgenommen werden.

Um die automatische QoS zu konfigurieren, navigieren Sie zu Configuration > QoS.



Klicken Sie auf Add (Hinzufügen), und setzen Sie Auto QoS auf enabled (aktiviert). Wählen Sie das entsprechende AutoQoS-Makro aus der Liste aus. In diesem Beispiel wird ein Sprachmakro zur Priorisierung des Sprachdatenverkehrs verwendet.



Configuration > Services > QoS

### Add QoS

Auto QoS **ENABLED**

Auto Qos Macro voice

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

Available (2) Enabled (0)

Profiles

- qos-policy
- default-policy-profile

AutoQoS-Sprachzuordnung

Wählen Sie nach dem Aktivieren des Makros die Richtlinie aus, die der Richtlinie hinzugefügt werden soll.

## Konfiguration der Auto QoS CLI

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

Nachdem die automatische QoS aktiviert wurde, können Sie die vorgenommenen Änderungen sehen. In diesem Abschnitt werden die Konfigurationsänderungen für Sprache aufgeführt.

```
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
```

## Modulare QoS-CLI

Mit dem MQC können Sie eine Datenverkehrsklasse definieren, eine Datenverkehrsrichtlinie erstellen (Richtlinienzuordnung) und die Datenverkehrsrichtlinie an eine Schnittstelle anhängen. Die Datenverkehrsrichtlinie enthält die QoS-Funktion, die für die Datenverkehrsklasse gilt.



MQS-CLI-Workflow

In diesem Beispiel wird veranschaulicht, wie Zugriffskontrolllisten (ACLs) verwendet werden, um Datenverkehr zu klassifizieren und Bandbreitenbeschränkungen anzuwenden.

Erstellen Sie eine ACL, um den spezifischen Datenverkehr zu identifizieren und zu klassifizieren, den Sie verwalten möchten. Hierzu können Regeln definiert werden, die Datenverkehr anhand von Kriterien wie IP-Adressen, Protokollen oder Ports zuordnen.

Navigieren Sie zu Configuration > Security > ACL, und fügen Sie die ACL hinzu.

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-Konfiguration

Nachdem der Datenverkehr mithilfe der ACL klassifiziert wurde, konfigurieren Sie Bandbreitenbeschränkungen, um die diesem Datenverkehr zugewiesene Bandbreite zu steuern.

Navigieren Sie zu Konfiguration > Services > QoS und zur QoS-Richtlinie. Verknüpfen Sie die ACL mit der Richtlinie, und wenden Sie die Richtlinie in Kbit/s an.

Blättern Sie nach unten, und wählen Sie das Richtlinienprofil aus, auf das die QoS angewendet werden soll. Sie können die Richtlinie sowohl für die SSID als auch für den Client in Eingangs-/Ausgangsrichtung auswählen.

### 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](#) [x Delete](#)

AVC/User Defined

Match  Any  All

Match Type   
Match Value\*

Mark Type

Drop

Police(kbps)

Edit QoS

Mark: None

Police(kbps): 20

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

Search

Available (1)

Profiles

default-policy-profile

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

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

Cancel Update & Apply to Device

MQS-Profil

## MQS-CLI-Konfiguration

```

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

```

## Metall-QoS

Der Hauptzweck dieser QoS-Profile besteht darin, die in einem Wireless-Netzwerk maximal zulässigen Differentiated Services Code Point (DSCP)-Werte einzuschränken und dadurch die 802.11 User Priority (UP)-Werte zu steuern.

Im Cisco Wireless LAN Controller (WLC) der Serie 9800 sind die QoS-Profile für Metalle vordefiniert und nicht konfigurierbar. Sie können diese Profile jedoch auf bestimmte SSIDs oder Clients anwenden, um QoS-Richtlinien durchzusetzen.

Es stehen vier Metall-QoS-Profile zur Verfügung:

QoS-Profil	Max. DSCP
Bronze	8
Silber	0
Gold	34
Platin	46

So konfigurieren Sie die Metall-QoS auf einem Cisco 9800 WLC:

Navigieren Sie zu Konfiguration > Richtlinie > QoS & AVC.

- Wählen Sie das gewünschte Metall-QoS-Profil aus (Platinum, Gold, Silver oder Bronze).
- Wenden Sie das ausgewählte Profil auf die Ziel-SSID oder den Client an.

⚠ 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

Metall-QoS-Profil

## Konfiguration der Metall-QoS-CLI

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



Hinweis: Benutzerspezifische und SSID-Bandbreitenverträge können über QoS-Richtlinien und nicht direkt über die Metall-QoS konfiguriert werden. Im Jahr 9800 wird der nicht übereinstimmende Datenverkehr der Standardklasse zugewiesen.

---



Hinweis: In der GUI können Sie nur die Metall-QoS pro SSID festlegen. In CLI können Sie sie auch auf dem Client-Ziel konfigurieren.

---

## Validierung der End-to-End-QoS mit Paketerfassung

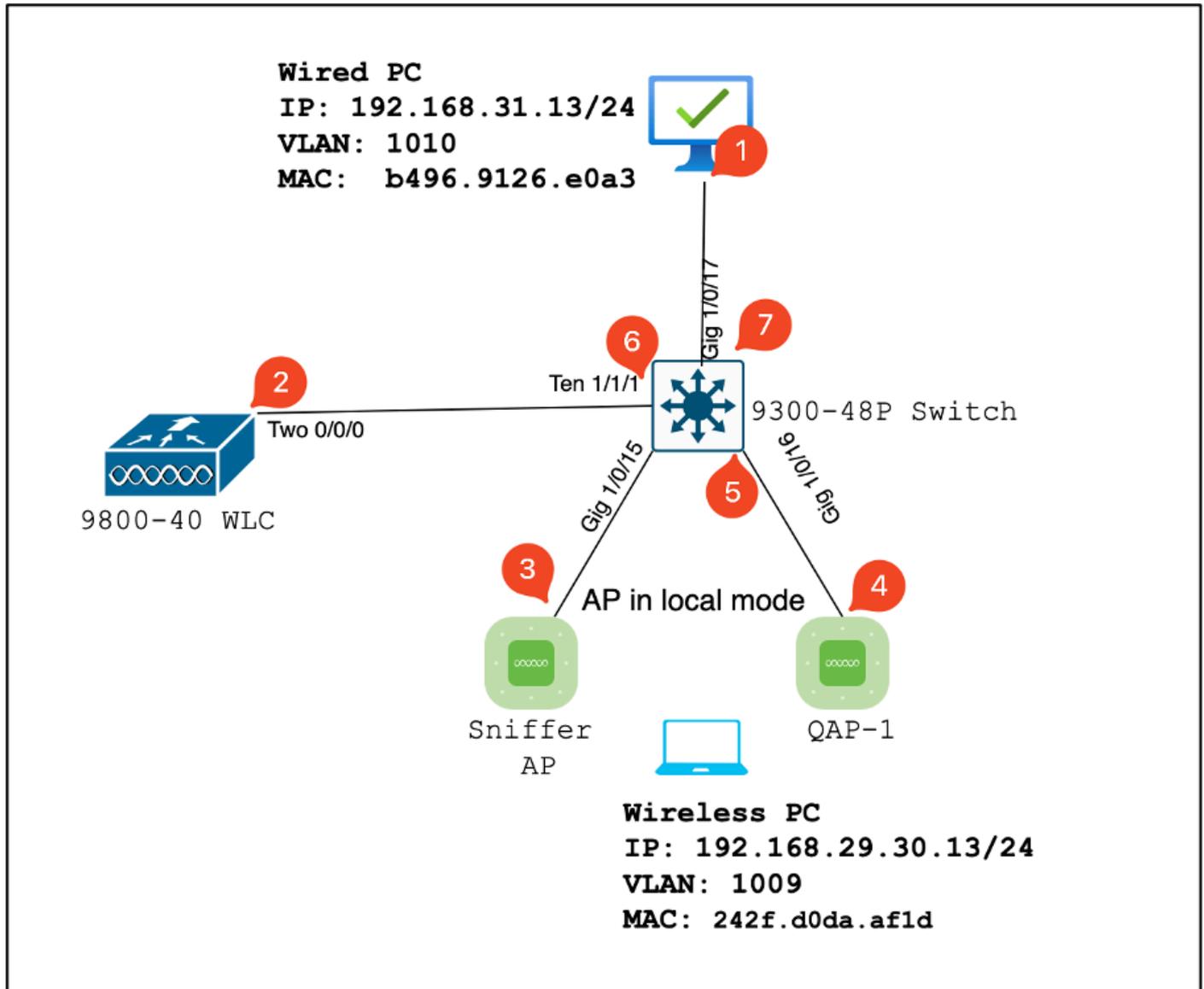
Nach Abschluss der QoS-Konfiguration müssen die QoS-Pakete überprüft und validiert werden, ob die QoS-Richtlinien durchgängig korrekt funktionieren. Dies kann durch Paketerfassung und -analyse erreicht werden.

Für die Replizierung und Validierung der QoS-Konfiguration wird eine Laborumgebung in kleinem Umfang verwendet. Die Übung umfasst folgende Komponenten:

- WLC
- AP
- Sniffer AP zur Einnahme von OTA
- Kabelgebundener PC
- Switch

Alle diese Komponenten sind mit demselben Switch in der Laborumgebung verbunden. Die markierten Zahlen in diesem Diagramm zeigen die Punkte an, an denen die Paketerfassung zur Überwachung und Analyse des Datenverkehrs aktiviert ist.

## Netzwerkdiagramm



LAB-Topologie

## Laborkomponenten und Paketerfassungspunkte

WLC:

- Verwaltung der QoS-Richtlinien und -Konfigurationen für das Wireless-Netzwerk
- Paketerfassungspunkt: Erfassen Sie den Datenverkehr zwischen dem WLC, dem AP und dem Switch.

Zugangspunkt:

- Bietet Wireless-Verbindungen zu Clients und setzt QoS-Richtlinien durch.

- Paketerfassungspunkt: Erfassen Sie den Datenverkehr zwischen dem Access Point und dem Switch.

#### Sniffer-AP:

- Dient als dediziertes Gerät zur Erfassung des Wireless-Datenverkehrs.
- Paketerfassungspunkt: Erfassen Sie den Wireless-Datenverkehr zwischen dem Access Point und den Wireless-Clients.

#### Kabelgebundener PC:

- Mit dem Switch verbunden, um kabelgebundenen Datenverkehr zu simulieren und die End-to-End-QoS zu validieren.
- Paketerfassungspunkt: Erfasst übertragene und empfangene QoS-Pakete über eine kabelgebundene Verbindung.

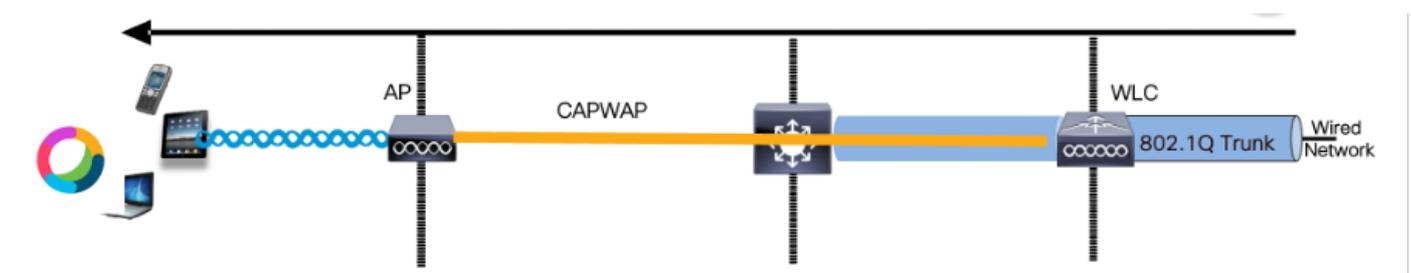
#### Wireless-PC:

- Mit dem WLAN verbunden, um den Wireless-Datenverkehr zu simulieren und die End-to-End-QoS zu validieren.
- Paketerfassungspunkt: Erfassen übertragener und empfangener QoS-Pakete über eine Wireless-Verbindung.

#### Switch:

- Das zentrale Gerät verbindet alle Komponenten der Übungseinheit miteinander und vereinfacht den Datenfluss.
- Paketerfassungspunkte: Erfassen Sie Datenverkehr an verschiedenen Switch-Ports, um die ordnungsgemäße QoS-Durchsetzung zu validieren.

Die LAB-Topologie kann logischerweise folgendermaßen gezeichnet werden:



Logische LAB-Topologie

Zum Testen und Validieren der QoS-Konfiguration wird iPerf verwendet, um Datenverkehr zwischen Client und Server zu generieren. Diese Befehle werden verwendet, um die iPerf-Kommunikation zu erleichtern. Dabei werden die Rollen von Server und Client basierend auf der Richtung der QoS-Tests ausgetauscht.

### TestszENARIO 1: Downstream-QoS-Validierung

Ziel ist die Validierung der Downstream-QoS-Konfiguration. Bei der Konfiguration sendet ein

kabelgebundener PC Pakete mit DSCP 46 an einen Wireless-PC.

Der Wireless LAN Controller (WLC) wird mit der metallischen "Platinum QoS"-Richtlinie sowohl für die Downstream- als auch die Upstream-Richtung konfiguriert.

Test-Setup:

- Datenverkehrsfluss:

Quelle: Kabelgebundener PC

Ziel: Wireless-PC

Datenverkehrstyp: UDP-Pakete mit DSCP 46

- Konfiguration der QoS-Richtlinie auf dem WLC:

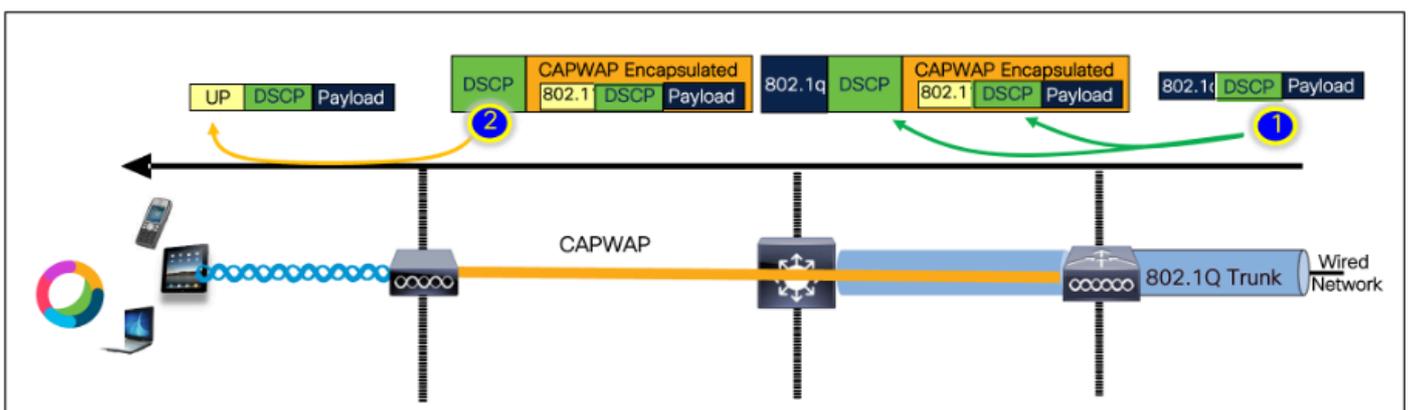
QoS-Profil: Metall-QoS - Platin-QoS

Richtung: sowohl flussabwärts als auch flussaufwärts

- Metal QoS-Konfigurationsbefehle:

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

Logische Topologie und DSCP-Konversation in Downstream-Richtung.



DSCP-Gesprächspunkt

Die Paketerfassung wurde auf dem kabelgebundenen PC übernommen. Dies bestätigt, dass der kabelgebundene PC UDP-Pakete an die angegebene Ziel-IP-Adresse 192.168.10.13 mit der korrekten DSCP-Markierung 46 sendet.

```

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

```

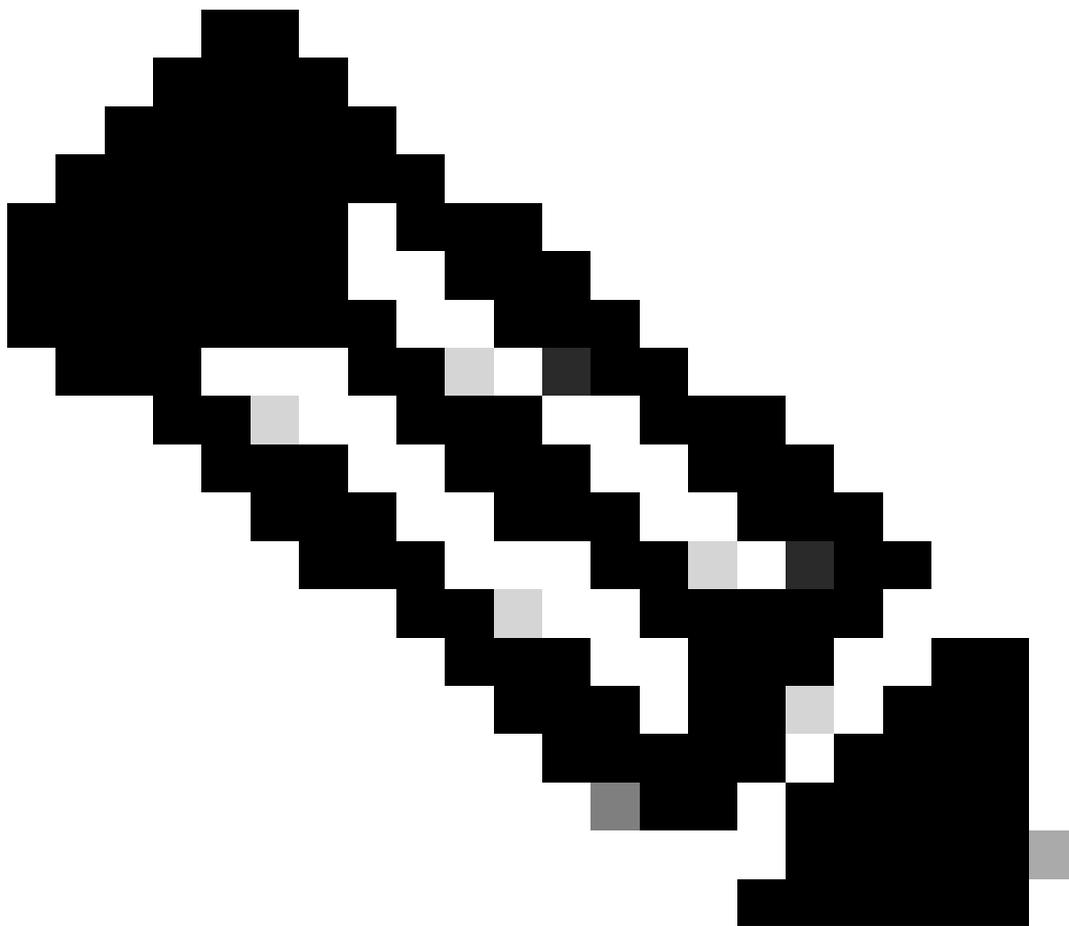
```

> Frame 1006: 834 bytes on wire (6672 bits), 834 bytes captured (6672 bits) on interface \Device\NPF_{4083E30A-3F9F-4837-BEC3-2AC20713EDCA}, id 0
> Ethernet II, Src: IntelCor_26:8e8:83 (04:28:91:26:8e: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)
  .... 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 820
  Identification: 0xc79c (51108)

```

Erfassung kabelgebundener PCs - Downstream-Richtung

Als Nächstes untersuchen wir ein Paket, das auf dem mit dem kabelgebundenen PC verbundenen Uplink-Switch erfasst wurde. Der Switch vertraut dem DSCP-Tag, und der DSCP-Wert bleibt unverändert bei 46.



Hinweis: Switch-Ports der Catalyst Serie 9000 haben standardmäßig einen vertrauenswürdigen 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-ZAC26715EDCA}, id 0
> Ethernet II, Src: IntelCor_26:0e:0a:3 (04:9e:91:26:0e:0a:3), 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
  .... 0100 = 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)

```

Erfassung der Uplink-Schnittstelle des kabelgebundenen Computers

Beim Untersuchen der Paketerfassung auf dem WLC mithilfe von EPC kommt das Paket mit dem gleichen DSCP-Tag von 46 vom Uplink-Switch an. Dadurch wird bestätigt, dass die DSCP-Markierung beibehalten wird, wenn das Paket den WLC erreicht.

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-ZAC26715EDCA}, id 0
> Ethernet II, Src: IntelCor_26:0e:0a:3 (04:9e:91:26:0e:0a:3), 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
  .... 0100 = 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)

```

Downstream-Richtung WLC-EPC

Wenn der WLC das Paket innerhalb eines CAPWAP-Tunnels an den WAP sendet, handelt es sich um einen kritischen Schnittpunkt, an dem der WLC den DSCP auf Grundlage seiner Konfiguration ändern kann. Unterteilen wir die Paketerfassung, die zur Verdeutlichung durch nummerierte Punkte hervorgehoben wird:

- Äußere CAPWAP-Schicht: Die äußere Schicht des CAPWAP-Tunnels zeigt das DSCP-Tag als 46 an. Hierbei handelt es sich um den vom Switch-Ende empfangenen Wert.
- 802.11 UP-Wert innerhalb von CAPWAP: Innerhalb des CAPWAP-Tunnels ordnet WLC die DSCP 46 der 802.11-Benutzerpriorität (UP) 6 zu, die dem Sprachverkehr entspricht.
- DSCP Value Inside CAPWAP: Der Cisco 9800 WLC arbeitet mit einem vertrauenswürdigen DSCP-Modell, sodass der DSCP-Wert innerhalb des CAPWAP-Tunnels bei 46 Punkten gehalten wird, genau wie die äußere DSCP-Ebene.

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

```

> Frame 2736: 988 bytes on wire (7264 bits), 988 bytes captured (7264 bits)
> Ethernet II, Src: Cisco_e7:9d:ab (80:2d:b0:e7:9d:ab), Dst: Cisco_28:35:74 (a4:b4:39:28:35:74)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 31
> Internet Protocol Version 4, Src: 10.105.60.198, Dst: 10.105.60.158
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x08 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
    .... 0000 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 896
  Identification: 0x0000 (0)
  > Flags: 0x00
  ... 0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 255
  Protocol: UDP (17)
  Header Checksum: 0x2985 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.105.60.198
  Destination Address: 10.105.60.158
  > User Datagram Protocol, Src Port: 5247, Dst Port: 5262
  > Control And Provisioning of Wireless Access Points - Data
  > IEEE 802.11 QoS Data, Flags: .....F.
  Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x0000 (Swapped)
  ..000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: 24:2f:d0: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: 0x0000
  .... .... 0110 = TID: 6
  .... .... 0000 110 = 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-Markierungen

Überprüfen Sie anschließend dasselbe Paket am Uplink-Switch-Port des AP.

Der DSCP-Wert auf der äußeren CAPWAP-Schicht bleibt bei 46. Zur Veranschaulichung wird der innere CAPWAP-Datenverkehr hervorgehoben, um das Tagging anzuzeigen.

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_sw_1p_10
> Ethernet II, Src: Cisco_e7:9d:ab (80:2d:b0:e7:9d:ab), Dst: Cisco_28:35:74 (a4:b4:39:28:35:74)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 31
> Internet Protocol Version 4, Src: 10.105.60.198, Dst: 10.105.60.158
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x08 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
    .... 0000 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 896
  Identification: 0x0000 (0)
  > Flags: 0x00
  ... 0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 255
  Protocol: UDP (17)
  Header Checksum: 0x2985 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.105.60.198
  Destination Address: 10.105.60.158
  > User Datagram Protocol, Src Port: 5247, Dst Port: 5262
  > Control And Provisioning of Wireless Access Points - Data
  > Frame 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: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: 0x0000
  .... .... 0110 = TID: 6
  .... .... 0000 110 = 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
  
```

AP-Uplink-Switch-Schnittstellenerfassung

Sobald der WAP das Paket empfängt, überträgt er es per Funk. Zum Verifizieren des User Priority

(UP)-Tagging wird eine Over-the-Air (OTA)-Erfassung mit einem Sniffer-AP verwendet.

Der WAP hat den Frame mit einem UP-Wert von 6 weitergeleitet. Dadurch wird bestätigt, dass der AP den DSCP-Wert korrekt dem entsprechenden 802.11-UP-Wert (6) zuordnet, der dem Sprachdatenverkehr entspricht.

The screenshot shows a network traffic capture interface. At the top, a table lists packet details for packet number 2061. The table has columns for No., Time, SA, RA, Source, Destination, Protocol, DSCP, Priority, Length, and Info. The row for packet 2061 shows a time of 08:19:24.830431, SA of 2c:ab:eb:37:cd:e5, RA of 24:2f:d0:da:af:1d, Source of Cisco\_37:cd:e5, Destination of 24:2f:d0:da:af:1d, Protocol of 802.11, DSCP of CS0, Priority of Voice (Voice), Length of 971, and Info of QoS Data, SN=1952, FN=0. Below the table, a detailed view of the packet structure is shown. The packet is 971 bytes on wire (7768 bits) and 971 bytes captured (7768 bits) on interface en0, id 0. It is an Ethernet II frame with source Cisco\_a7:1a:7f (34:1b:2d:a7:1a:7f) and destination Apple\_f0:82:d4 (bc:d0:74:f0:82:d4). The payload is an Internet Protocol Version 4 packet with source 10.105.60.198 and destination 10.233.7.212. The User Datagram Protocol (UDP) has source port 5555 and destination port 5000. The packet is encapsulated in IEEE 802.11 radio information. The IEEE 802.11 QoS Data has flags .p...F.C. The Type/Subtype is QoS Data (0x0028). The Frame Control Field is 0x8842. The Duration is 48 microseconds. The Receiver address is 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d). The Transmitter address is Cisco\_4e:85:4f (a4:b4:39:4e:85:4f). The Destination address is 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d). The Source address is Cisco\_37:cd:e5 (2c:ab:eb:37:cd:e5). The BSS Id is Cisco\_4e:85:4f (a4:b4:39:4e:85:4f). The STA address is 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d). The Fragment number is 0. The Sequence number is 1952. The Frame check sequence is 0x6e2c7cfe [unverified]. The FCS Status is Unverified. The QoS Control field is 0x0006. The QoS Control field is broken down as follows: 0110 = TID: 6, 110 = Priority: Voice (Voice) (6), 0 = EOSP: Service period, 00 = Ack Policy: Normal Ack (0x0), 0 = Payload Type: MSDU, 0000 0000 = QAP PS Buffer State: 0x00. The packet ends with COMP parameters and 836 bytes of data.

OTA-Erfassung vom AP zum Client

In der Endphase wird das vom Wireless-PC empfangene Paket angezeigt. Der Wireless-PC empfängt den Frame mit einem DSCP-Wert von 46.

Dies zeigt an, dass die DSCP-Markierung im gesamten Übertragungspfad vom kabelgebundenen PC bis zum Wireless-PC erhalten bleibt. Der konsistente DSCP-Wert von 46 bestätigt, dass die QoS-Richtlinien korrekt in Downstream-Richtung angewendet und beibehalten werden.

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
    > CMP parameters
  > Data (836 bytes)
  
```

Wireless-PC-Erfassung

## TestszENARIO 2: Upstream-QoS-Validierung

In diesem TestszENARIO soll die Upstream-QoS-Konfiguration validiert werden. Bei der Konfiguration sendet ein Wireless-PC UDP-Pakete mit DSCP 46 an einen kabelgebundenen PC. Der WLC wird mit der Metal "Platinum QoS"-Richtlinie für die Upstream- und Downstream-Richtung konfiguriert.

- Datenverkehrsfluss:

Quelle: Wireless-PC

Ziel: Kabelgebundener PC

Datenverkehrstyp: UDP-Pakete mit DSCP 46

- Konfiguration der QoS-Richtlinie auf dem WLC:

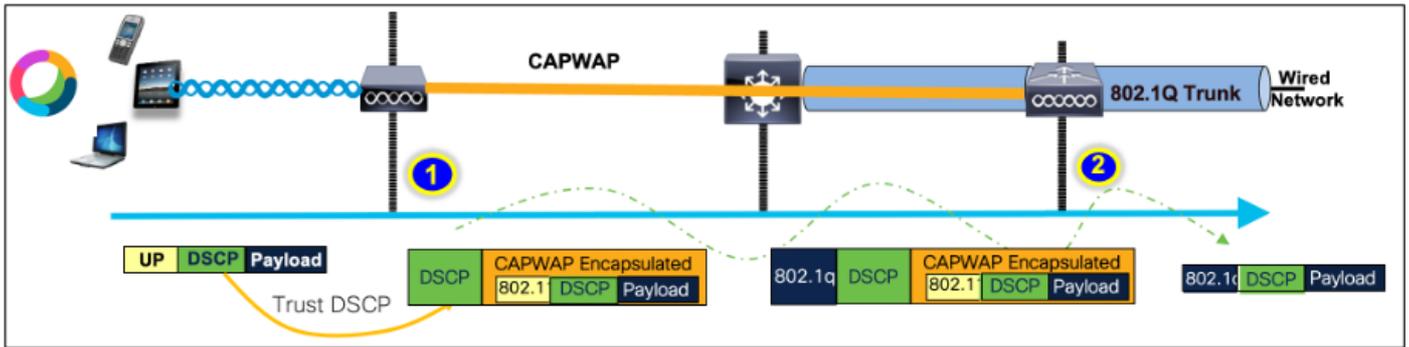
QoS-Profil: Platin-QoS

Richtung: sowohl vor- als auch nachgelagert

- Metal QoS-Konfigurationsbefehle:

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

## Logische Topologie- und DSCP-Umwandlung in Upstream-Richtung:



Logische Topologie- und DSCP-Umwandlung - Upstream

Pakete, die vom Wireless-PC an den kabelgebundenen PC gesendet werden. Diese Aufnahme wird auf dem Wireless-PC gemacht.

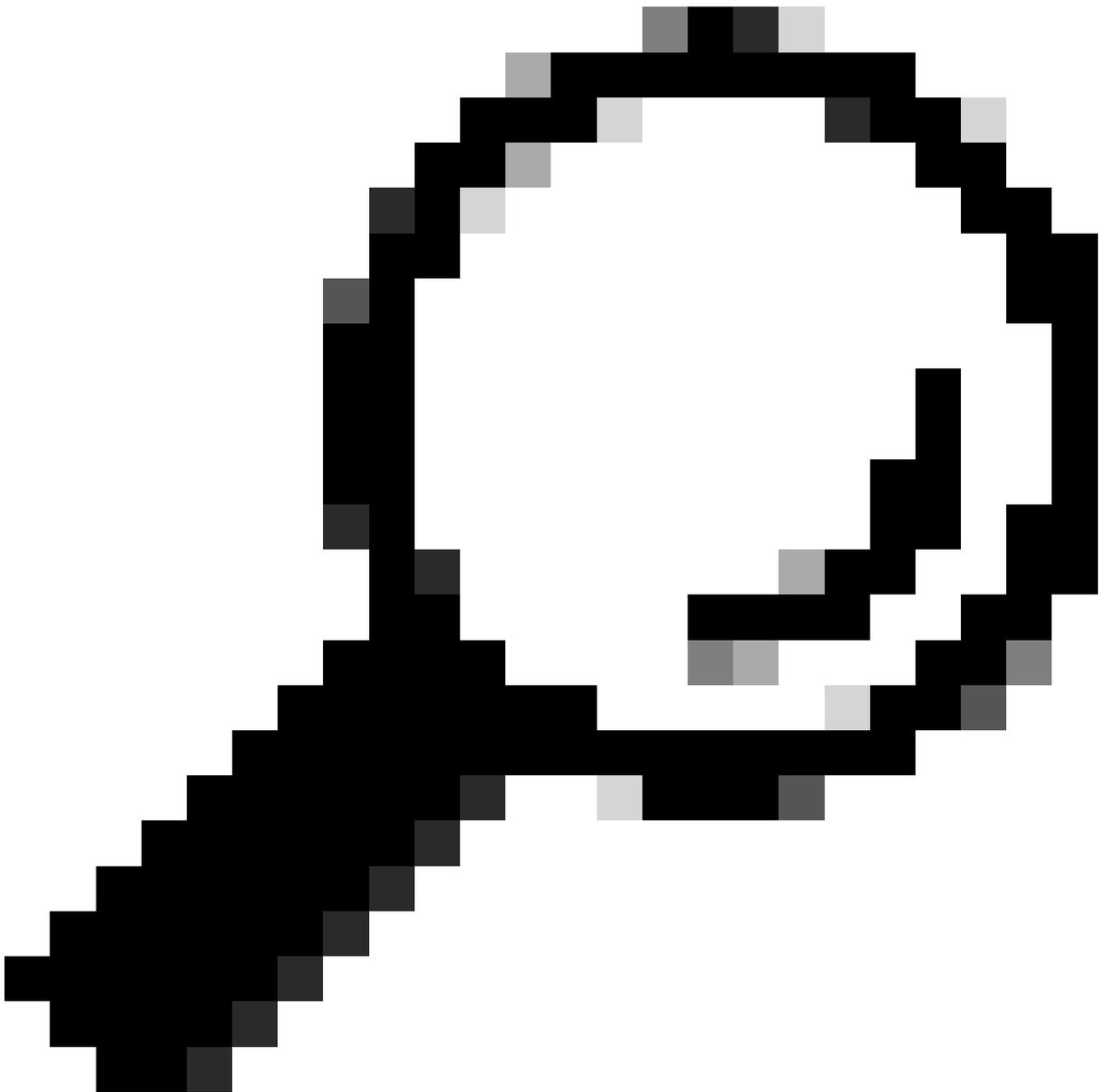
Der Wireless-PC sendet UDP-Pakete mit DSCP 46.

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:b: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)
```

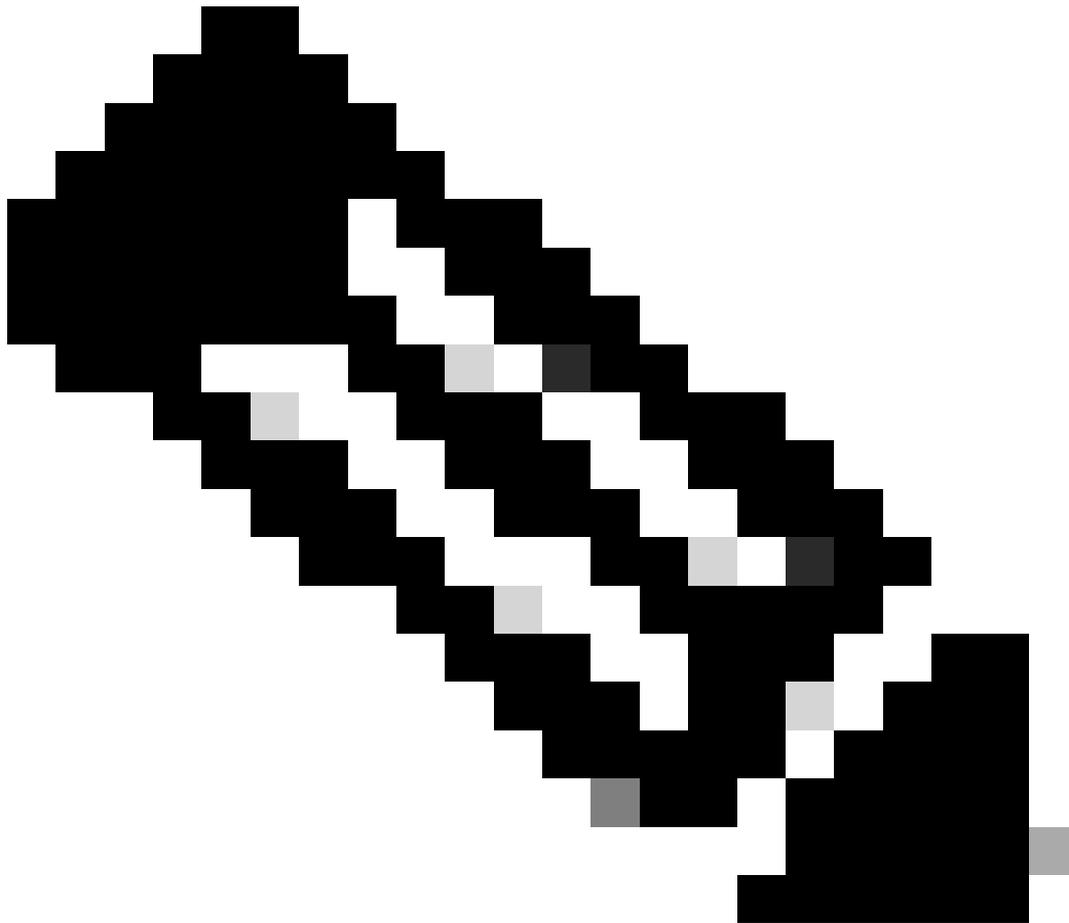
Wireless-PC-Erfassung in Upstream-Richtung

Als Nächstes sehen wir uns die OTA-Erfassung vom Client zum AP an.



Tipp: Wenn ein Windows-Wireless-PC zum Senden von Paketen mit DSCP 46 verwendet wird, ordnet Windows DSCP 46 einem Wert für die Benutzerpriorität (UP) von 5 (Video) zu. Daher zeigt die OTA-Erfassung die Pakete als Videodatenverkehr (UP 5) an. Wenn Sie das Paket entschlüsseln, bleibt der DSCP-Wert jedoch bei 46.

---



Hinweis: Ab Version 17.4 vertraut der Cisco 9800 WLC standardmäßig dem DSCP-Wert im AP-Join-Profil. Auf diese Weise wird sichergestellt, dass der DSCP-Wert 46 vom WLC beibehalten und als vertrauenswürdig eingestuft wird. Dadurch werden Probleme im Zusammenhang mit dem Zuordnungsverhalten zwischen Windows DSCP und UP vermieden.

---

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
- 101100.. 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

Windows - Zuordnung bis zu DSCP

Die verschlüsselte OTA-Erfassung (Over-the-Air) aus dem Labor wird analysiert, um die Upstream-QoS-Konfiguration zu validieren.

Die OTA-Aufzeichnung zeigt die Pakete mit dem User Priority (UP)-Wert 5 (Video). Obwohl bei der OTA-Erfassung UP 5 angezeigt wird, bleibt der DSCP-Wert im verschlüsselten Paket bei 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	C50 Video (Video)	5	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
      [.... 0101 = Priority: Video (Video) (5)]
      .... 0000 = QoS bit 4: Bits 8-15 of QoS Control field are TXOP Duration Requested
      .... .00. .... = Ack Policy: Normal Ack (0x0)
      .... 0... .... = Payload Type: MSDU
      0000 0000 .... = TXOP Duration Requested: 0 (no TXOP requested)
  
```

OTA für LAB-Einrichtung in Upstream-Richtung

Anschließend wird die Paketerfassung am Uplink-Port des Access Points analysiert, um sicherzustellen, dass der DSCP-Wert erhalten bleibt, wenn das Paket vom Access Point zum WLC übertragen wird.

- Der DSCP-Wert auf der äußeren CAPWAP-Schicht wird auf 46 gehalten.
- Innerhalb des CAPWAP-Tunnels wird der DSCP-Wert ebenfalls bei 46 gehalten.

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-Plink-Erfassung in Upstream-Richtung

Die Erfassung wird am WLC durchgeführt, sobald das Paket vom Switch ankommt.

- Das Paket erreicht den WLC mit dem DSCP-Wert 46 auf der äußeren CAPWAP-Schicht.
- Innerhalb des CAPWAP-Tunnels wird der DSCP-Wert bei 46 gehalten.

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 0000 = QoS bit 4: Bits 0-15 of QoS Control field are TXOP Duration Requested
... .. 0000 0000 = Ack Policy: Normal Ack (0x0)
... .. 0000 0000 = Payload Type: MSDU
0000 0000 .... = TXOP Duration Requested: 0 [no TXOP requested]
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.30.13, Dst: 192.168.31.10
0100 .... = Version: 4
... 0101 = Header Length: 20 bytes (5)
< Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
  1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
  .... 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 1500
Identification: 0x2d1f (11551)

```

WLC-EPC zeigt Pakete vom AP

Nachdem das Paket am WLC eine Haarnadelkurve eingelegt hat, wird es zurück an den Uplink-Switch gesendet, der für den kabelgebundenen PC bestimmt ist. Der WLC leitet das Paket mit dem DSCP-Wert 46 weiter.

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 zeigt an kabelgebundenen PC gesendete Pakete

Schließlich wird die Paketerfassung am kabelgebundenen PC-Uplink analysiert, um sicherzustellen, dass der DSCP-Wert beim Eintreffen des Pakets vom WLC erhalten bleibt.

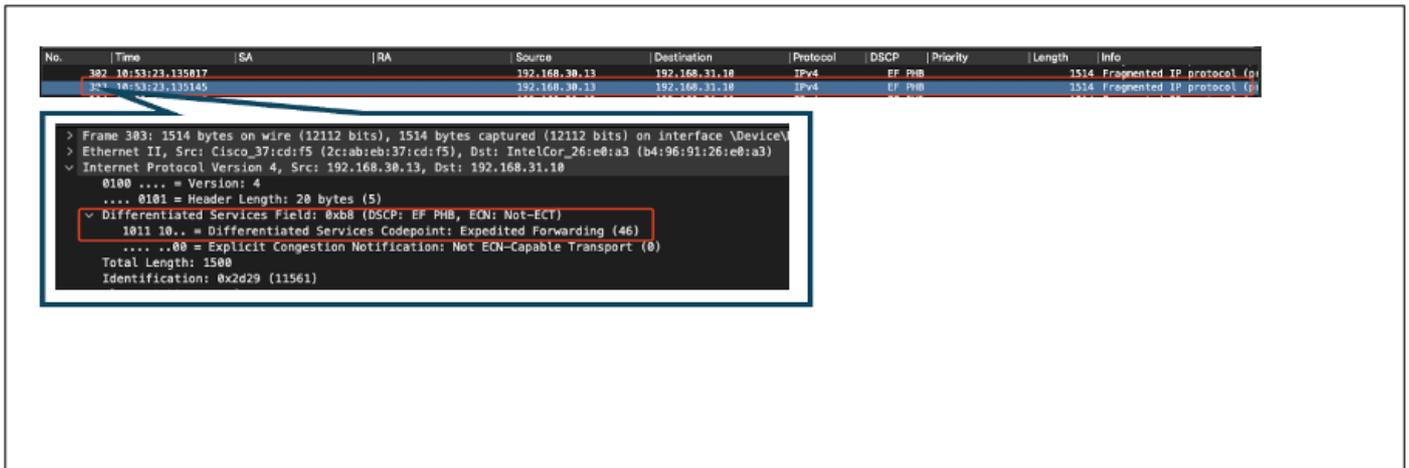
5039	10:53:23.187287			192.168.30.13	192.168.31.10	IPv4	EF PHB		1518	Fragmented IP protocol (p)
5040	10:53:23.187381			192.168.30.13	192.168.31.10	IPv4	EF PHB		1518	Fragmented IP protocol (p)

```

> 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)

```

In der letzten Phase wird das vom kabelgebundenen PC empfangene Paket analysiert, um sicherzustellen, dass das Paket den kabelgebundenen PC mit dem DSCP-Wert 46 erreicht.



Erfassung von kabelgebundenen PCs - Upstream-Richtung

Der Upstream-QoS-Test hat die QoS-Konfiguration für den Datenverkehr, der vom Wireless-PC zum kabelgebundenen PC fließt, erfolgreich validiert. Die konsistente Beibehaltung des DSCP-Werts von 46 über den gesamten Übertragungsweg bestätigt, dass die QoS-Richtlinien korrekt angewendet und durchgesetzt werden.

## Fehlerbehebung

Sprach-, Video- und andere Echtzeitanwendungen reagieren besonders empfindlich auf Probleme mit der Netzwerkleistung, und eine Verschlechterung der Quality of Service (QoS) kann erhebliche negative Auswirkungen haben. Wenn QoS-Pakete mit niedrigeren DSCP-Werten gekennzeichnet werden, kann dies erhebliche Auswirkungen auf Sprache und Video haben.

Auswirkungen auf die Sprachkommunikation:

- Höhere Latenz: Sprachkommunikation erfordert eine niedrige Latenz, um eine natürliche und reibungslose Kommunikation zu gewährleisten. Niedrigere DSCP-Werte können dazu führen, dass Sprachpakete verzögert werden, was zu einer merklichen Verzögerung der Gespräche führt.
- Jitter: Schwankende Paketankunftszeiten (Jitter) können die reibungslose Übermittlung von Sprachpaketen beeinträchtigen. Dies kann zu abgehackten oder verstümmelten Audioinhalten führen, sodass der Lautsprecher nur schwer zu verstehen ist.
- Paketverlust: Sprachpakete reagieren sehr empfindlich auf Paketverlust. Selbst ein geringer Paketverlust kann zu fehlenden Wörtern oder Silben führen, was zu schlechter Anrufqualität und Missverständnissen führt.
- Echo und Verzerrung: Höhere Latenz und Jitter können zu Echos und Audioverzerrungen führen und so die Qualität des Sprachanrufs weiter beeinträchtigen.

Auswirkungen auf Video:

- Höhere Latenz: Videokommunikation erfordert eine niedrige Latenz, um die Synchronisierung zwischen Audio- und Videostreams aufrecht zu erhalten. Eine erhöhte Latenz kann zu Verzögerungen führen, was Interaktionen in Echtzeit erschwert.
- Jitter: Jitter kann dazu führen, dass Videobilder ungeordnet oder in unregelmäßigen Intervallen ankommen, was zu ruckartigen oder stotternden Videoerlebnissen führt.
- Paketverlust: verlorene Pakete können zu fehlenden Frames führen, was dazu führen kann, dass das Video einfriert oder Artefakte angezeigt werden.
- Geringere Videoqualität: Niedrigere DSCP-Werte können zu einer reduzierten Bandbreitenzuweisung für Videostreams führen, was zu einer niedrigeren Auflösung und schlechterer Videoqualität führt. Dies kann die Anzeige wichtiger Details im Video erschweren.

## Szenario 1: Zwischen-Switch schreibt DSCP-Markierung um

In diesem Fehlerbehebungsszenario wird untersucht, wie sich ein zwischengeschalteter Switch, der die DSCP-Markierung umschreibt, auf den Datenverkehr auswirkt, der beim WLC eingeht. Um dies zu replizieren, ist der Switch so konfiguriert, dass die DSCP 46-Markierung auf der kabelgebundenen PC-Uplink-Schnittstelle in CS1 umgeschrieben wird.

Das Paket wird vom kabelgebundenen PC mit einem DSCP 46-Tag gesendet.

```
> 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)
> 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)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 1500
  Identification: 0x5a74 (23156)
```

Kabelgebundenes PC-Sendepaket mit DSCP 46-Tag

Das Paket erreicht den WLC mit einem DSCP-Wert von CS1 (DSCP 8). Durch den Wechsel von DSCP 46 zu DSCP 8 wird die Priorität des Pakets deutlich reduziert.

```
> 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
> Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    0010 00.. = Differentiated Services Codepoint: Class Selector 1 (8)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 1500
  Identification: 0x5a41 (23105)
```

WLC-EPC mit CS1-Markierung

In diesem Schritt wird das vom WLC an den AP weitergeleitete Paket analysiert.

- Der äußere CAPWAP-Header ist mit CS1 (DSCP 8) gekennzeichnet.
- Der innere CAPWAP-Header ist ebenfalls mit CS1 (DSCP 8) gekennzeichnet.
- Der Wert User Priority (UP) wird auf BK (Background) gesetzt.

```

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

```

WLC EPC zeigt CS1-Tag im CAPWAP-Datenverkehr

Das Paket erreicht den Wireless-PC mit einem DSCP-Wert von CS1 (DSCP 8).

```

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

```

Dieses Szenario zeigt, wie eine fehlerhafte Konfiguration auf einem zwischengeschalteten Switch die QoS-Konfiguration unterbrechen kann, was zu einer Beeinträchtigung der Leistung bei Datenverkehr mit hoher Priorität führen kann. Die Sprachpakete, die anfangs mit hoher Priorität gekennzeichnet waren, wurden aufgrund des DSCP Rewrite als Datenverkehr mit niedrigerer Priorität behandelt. Dieses Szenario unterstreicht, wie wichtig es ist, sicherzustellen, dass zwischengeschaltete Netzwerkgeräte die QoS-Markierungen korrekt beibehalten, um die gewünschte Quality of Service für Datenverkehr mit hoher Priorität aufrechtzuerhalten.

## Szenario 2: AP-Link-Switch überschreibt DSCP-Markierung

In diesem Szenario werden die Auswirkungen eines zwischengeschalteten Switches, der mit dem Access Point verbunden ist und die DSCP-Markierung neu schreibt, auf den Datenverkehr untersucht.

- Der mit dem AP verbundene Switch ist so konfiguriert, dass die DSCP 46-Markierung auf einen anderen Wert CS1 an der AP-Uplink-Schnittstelle umgeschrieben wird.
- Das Paket wird vom kabelgebundenen PC mit dem DSCP-Tag 46 gesendet. Dadurch wird bestätigt, dass der Datenverkehr an der Quelle korrekt mit DSCP 46 markiert ist.

```
> 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)
  0000 .....
```

Die Erfassung wird am WLC durchgeführt, sobald das Paket vom Switch ankommt.

Das Paket erreicht den WLC mit dem äußeren CAPWAP-Header-DSCP-Wert CS1 (DSCP) und dem inneren DSCP-Wert 46. Der Grund hierfür ist, dass der zwischengeschaltete Switch den im CAPWAP-Tunnel eingebetteten Datenverkehr nicht sehen kann.

Der WLC vertraut dem DSCP-Tag im CAPWAP-Tunnel und leitet den Datenverkehr mit dem inneren DSCP-Tag 46 an den kabelgebundenen PC weiter.

```
> 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
    [..... 0110 = 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 mit CAPWAP-DSCP-Werten

Das Paket erreicht den kabelgebundenen PC mit einem DSCP-Wert von 46. Bestätigt, dass der WLC das Paket korrekt mit dem ursprünglichen DSCP-Wert 46 weiterleitet, wobei die Markierung mit hoher Priorität erhalten bleibt.

```

> 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

```

Paket mit DSCP 46 empfangen

Obwohl der WLC den Datenverkehr mit einem DSCP-Tag von 46 weitergeleitet hat, ist es wichtig zu verstehen, dass der Datenverkehr vom AP zum WLC aufgrund der Umschreibung des äußeren DSCP-Tags in CS1 (DSCP 8) als niedrige Priorität behandelt wurde.

Es können mehrere Switches zwischen dem AP und dem WLC vorhanden sein. Wenn der Datenverkehr eine niedrige Priorität erhält, kann er zu spät am WLC eintreffen. Dies kann zu erhöhter Latenz, Jitter und einem potenziellen Paketverlust führen, wodurch die Quality of Service für Datenverkehr mit hoher Priorität, z. B. für Sprache, beeinträchtigt werden kann.

## Tipp zur Fehlerbehebung

1. Überprüfung der anfänglichen DSCP-Markierung: Erfassen Sie Pakete an der Quelle (z. B. kabelgebundene PCs), um sicherzustellen, dass der Datenverkehr korrekt mit dem beabsichtigten DSCP-Wert markiert ist.
2. Prüfen Sie die Zwischengerätekonfigurationen: Überprüfen Sie die Konfiguration aller zwischengeschalteten Switches und Router, um sicherzustellen, dass sie nicht versehentlich DSCP-Werte neu schreiben.
3. Erfassung von Datenverkehr an wichtigen Punkten:
  1. Vor und nach dem Zwischenschalter.
  2. Am WLC.
  3. Am Ziel (z. B. Wireless-PC).
4. Simulieren von Verkehrsszenarien: Verwenden Sie Traffic-Generatoren oder Netzwerksimulations-Tools, um verschiedene Arten von Datenverkehr zu erstellen und zu beobachten, wie QoS vom Wireless-Netzwerk verarbeitet wird.
5. Weitere Informationen finden Sie im Dokument mit den Best Practices für den 9800: Lesen Sie die Dokumentation mit den Best Practices für den 9800 hinsichtlich der Konfiguration von QoS- und DSCP-Markierungen.

## Konfigurationsverifizierung

<#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 <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
```

## Schlussfolgerung

Die Aufrechterhaltung einer konsistenten QoS-Konfiguration im gesamten Netzwerk ist von entscheidender Bedeutung, um sicherzustellen, dass Datenverkehr mit hoher Priorität, z. B. Sprache und Video, ein angemessenes Maß an Service und Leistung erhält. QoS-Konfigurationen müssen regelmäßig validiert werden, um sicherzustellen, dass alle Netzwerkgeräte die beabsichtigten QoS-Richtlinien erfüllen. Diese Validierung hilft bei der Identifizierung und Behebung von Fehlkonfigurationen und Abweichungen, die die Netzwerkleistung beeinträchtigen könnten.

## Referenzen

- [Cisco Catalyst Wireless Controller der Serie 9800 - Überblick und Fehlerbehebung](#)
- [Cisco Catalyst Serie 9800 - Best Practices für die Konfiguration](#)
- [Software-Konfigurationsanleitung für Cisco Catalyst Wireless Controller der Serie 9800, Cisco IOS® XE Dublin 17.12.x](#)
- [Leitfaden zur Fehlerbehebung für Voice over Wireless LAN \(VoWLAN\)](#)
- [Aktivieren von DSCP QoS-Tagging auf Windows-Computern](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.