

Configure Validate and Troubleshoot Wireless QoS on 9800 WLC

Contents

[Introduction](#)

[Components Used](#)

[Background Information](#)

[Configuration](#)

[QoS Policy Targets](#)

[Auto QoS](#)

[Auto QoS CLI configuration](#)

[Modular QoS CLI](#)

[MQS CLI configuration](#)

[Metal QoS](#)

[Metal QoS CLI Configuration](#)

[Validate End-to-End QoS with Packet Capture](#)

[Network Diagram](#)

[Lab Components and Packet Capture Points](#)

[Test Scenario 1: Downstream QoS validation](#)

[Test Scenario 2: Upstream QoS Validation](#)

[Troubleshooting](#)

[Scenario 1: Intermediate Switch Rewrites DSCP Marking](#)

[Scenario 2: AP link Switch Rewrites DSCP Marking](#)

[Troubleshooting Tip](#)

[Configuration Verification](#)

[Conclusion](#)

[References](#)

Introduction

This document describes ways to configure, validate and troubleshoot wireless Quality of Service (QoS) on 9800 Wireless LAN Controller (WLC).

Components Used

The information in this document is based on these software and hardware versions:

- **WLC:** C9800-40-K9 running 17.12.03
- **Access Point (AP):** C9120-AXE-D
- **Switch:** C9300-48P running 17.03.05
- **Wired and Wireless Client:** Windows 10

The information in this document was created from the devices in a specific lab environment. All of the

devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

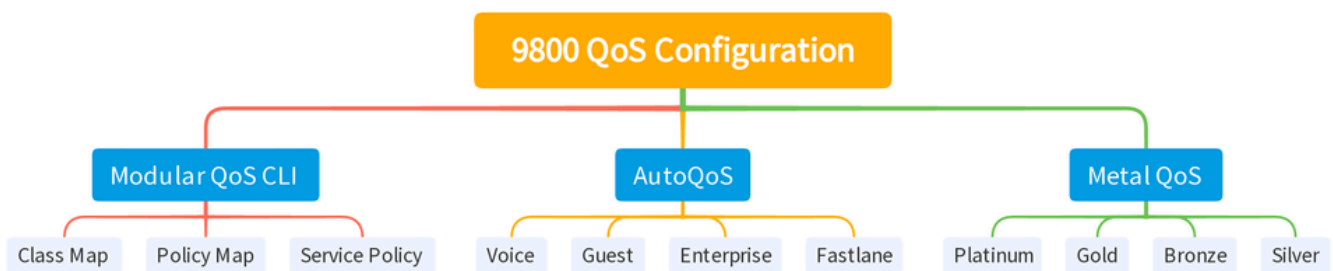
Wireless QoS is essential for ensuring that critical applications receive the necessary bandwidth and low latency required for optimal performance. This document provides a comprehensive guide to configuring, validating, and troubleshooting QoS on Cisco wireless networks.

This article assumes that readers have a foundational understanding of both wireless and wired QoS principles. It is also expected that readers are proficient in configuring and managing Cisco WLCs and APs.

Configuration

This section delves into the configuration of QoS on 9800 wireless controllers. By leveraging these configurations, you can ensure that critical applications receive the necessary bandwidth and low latency, thereby optimizing overall network performance.

You can divide the 9800 WLC QoS configuration into mainly three different broad categories.



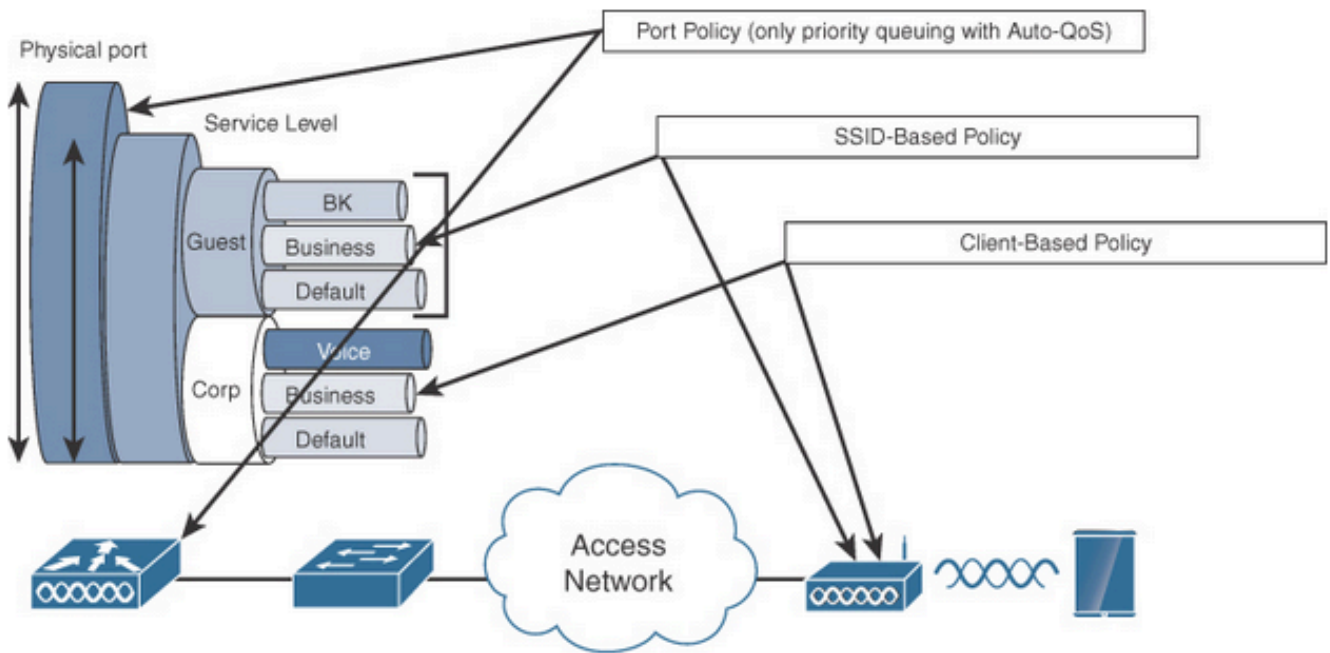
9800 WLC QoS Configuration Summary

This document goes through each section one by one in the subsequent sections.

Note: This article focuses on AP in local mode. AP in Flexconnect mode is not discussed.

QoS Policy Targets

A policy target is the configuration construct where a QoS policy can be applied. The QoS implementation on the Catalyst 9800 is modular and flexible. The user can decide to configure policies at three different targets: the SSID, client, and port levels.



QoS Policy Targets

The SSID policy is applicable per AP per SSID. You can configure policing and marking policies on SSID.

Client policies are applicable in the ingress and egress direction. You can configure policing and marking policies on clients. AAA override is also supported.

The port-based QoS policies can be applied at a physical or at a logical port.

Auto QoS

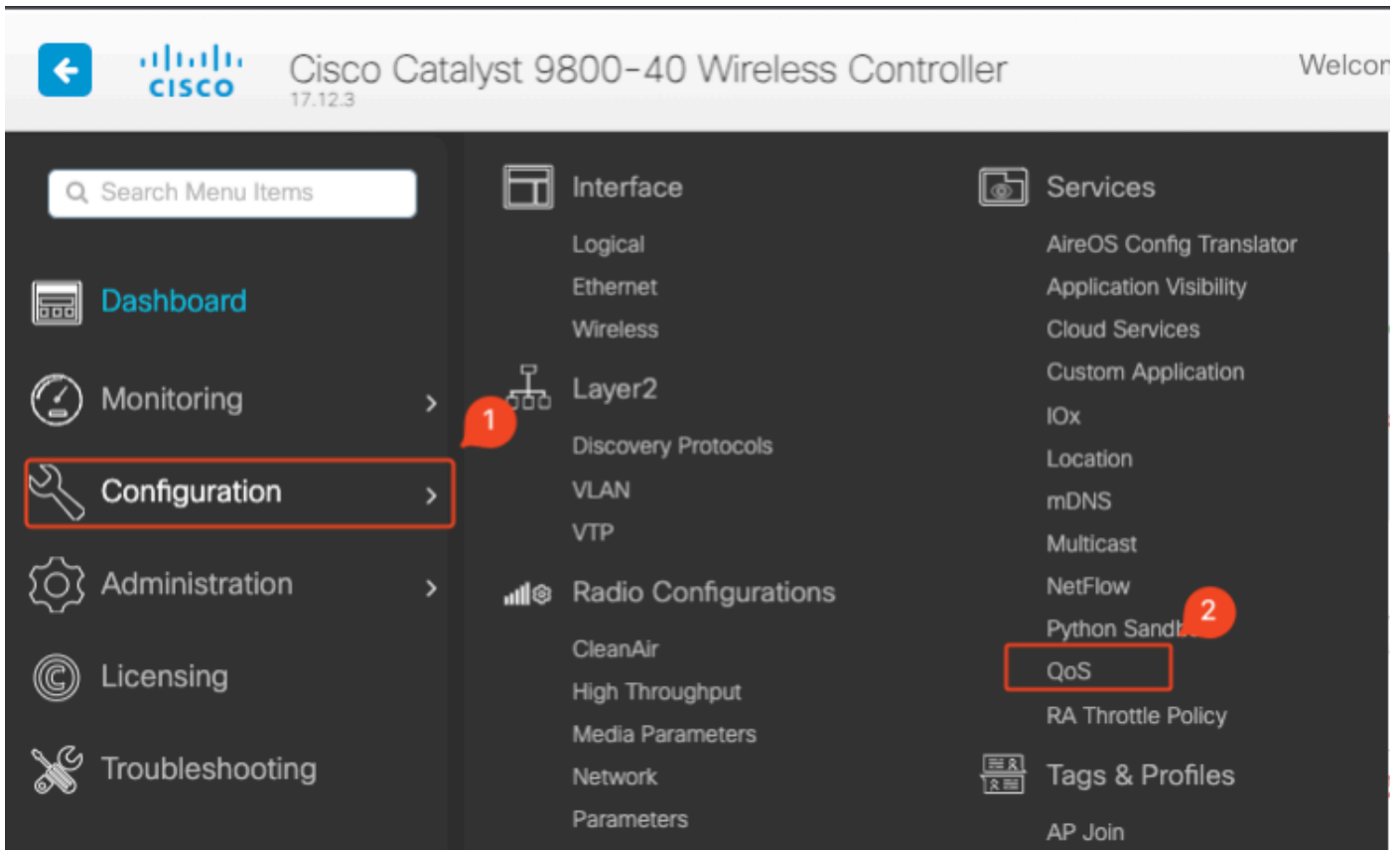
Wireless Auto QoS automates the deployment of wireless QoS features. It has a set of predefined profiles that can be further modified by the admin to prioritize different traffic flows. Auto-QoS matches traffic and assigns each matched packet to QoS groups. This allows the output policy map to put specific QoS groups into specific queues, including the priority queue.

Mode	Client Ingress	Client Egress	BSSID Ingress	BSSID Egress	Port Ingress	Port Egress	Radio
Voice	N/A	N/A	platinum-up	platinum	N/A	AutoQos-4.0-wlan-Port-Output-Policy	ACM on
Guest	N/A	N/A	AutoQos-4.0-wlan-GT-SSID-Input-Policy	AutoQos-4.0-wlan-GT-SSID-Output-Policy	N/A	AutoQos-4.0-wlan-Port-Output-Policy	
Fastlane	N/A	N/A	N/A	N/A	N/A	AutoQos-4.0-wlan-Port-Output-Policy	edca-parameters fastlane

Enterprise- avc	N/A	N/A	AutoQos-4.0-wlan- ET-SSID-Input- AVC-Policy	AutoQos-4.0-wlan- ET-SSID-Output- Policy	N/A	AutoQos-4.0- wlan-Port- Output-Policy	
----------------------------	-----	-----	---	--	-----	---	--

This table depicts the configuration changes that happen when an auto QoS profile is applied.

To configure Auto QoS navigate to **Configuration > QoS**



QoS Workflow

Click on **Add** and set **Auto QoS** to enabled. Choose the appropriate Auto QoS macro from the list. For this example, **Voice** macro to prioritize voice traffic is used.

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 Q Search

Available (2)	Enabled (0)
<p>Profiles</p> <div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;"> qos-policy → </div> <div style="border: 1px solid gray; padding: 5px;"> default-policy-profile → </div>	<p>Profiles</p> <div style="border: 1px solid gray; height: 80px; width: 100%;"></div>

AutoQoS Voice Mapping

Once the macro is enabled, select the policy that needs to be attached to the policy.

Auto QoS CLI configuration

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

Now that Auto QoS is enabled you can see the changes that happened. This section lists the configuration changes for voice.

```
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

```

Modular QoS CLI

The MQC allows you to define a traffic class, create a traffic policy (policy map), and attach the traffic policy to an interface. The traffic policy contains the QoS feature that applies to the traffic class.



MQS CLI Workflow

This example demonstrates how to use Access Control Lists (ACLs) to classify traffic and apply bandwidth restrictions.

Create an ACL to identify and classify the specific traffic you want to manage. This can be done by defining rules that match traffic based on criteria such as IP addresses, protocols, or ports.

Navigate to **Configuration > Security > ACL** and add the ACL.

Configuration > Security > ACL

+ Add × Delete Associate Interfaces

ACL Name	ACL Type	ACE Count	Download
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

Cancel Apply to Device

Once the traffic is classified using the ACL, configure bandwidth restrictions to control the amount of bandwidth allocated to this traffic.

Navigate to **Configuration > Services > QoS** and the QoS policy. Attach the ACL inside the policy and apply the police in kbps.

Scroll down and select the policy profile where the QoS is to be applied. You can select the policy in ingress/ egress direction for both SSID or Client.

Configuration > Services > QoS

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							

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

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 Profile

MQS CLI configuration

```

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
  
```

Metal QoS

The primary purpose of these QoS profiles is to limit the maximum Differentiated Services Code Point (DSCP) values allowed on a wireless network, thereby controlling the 802.11 User Priority (UP) values.

In the Cisco 9800 Wireless LAN Controller (WLC), the Metal QoS profiles are predefined and not configurable. However, you can apply these profiles to specific SSIDs or clients to enforce QoS policies.

There are four Metal QoS profiles available:

Qos Profile	Max DSCP
Bronze	8
Silver	0
Gold	34
Platinum	46

To configure Metal QoS on a Cisco 9800 WLC:

Navigate to **Configuration > Policy > QoS & AVC**.

- Select the desired Metal QoS profile (Platinum, Gold, Silver, or Bronze).
- Apply the chosen profile to the target SSID or 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 x ↕

Ingress platinum-up x ↕

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 ▼ ↕

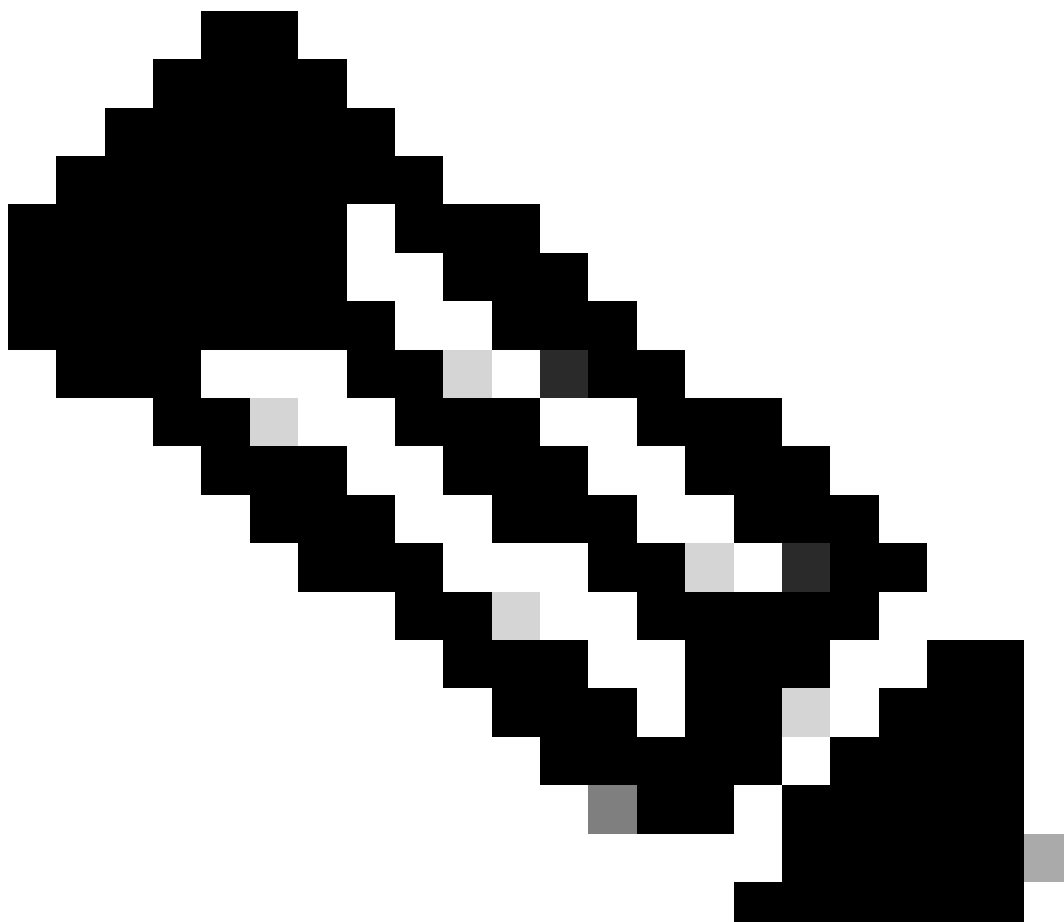
Metal QoS Profile

Metal QoS CLI Configuration

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



Note: Per-user and SSID bandwidth contract are configurable via QoS policies and not directly on the Metal QoS. In 9800 the non-matching traffic goes in the default class.



Note: On the GUI, you can only set the Metal QoS per SSID. On CLI you can also configure it on the client target.

Validate End-to-End QoS with Packet Capture

Now that the QoS configuration is completed, it is essential to examine QoS packets and validate that the QoS policies are functioning correctly from end to end. This can be achieved through packet capture and analysis.

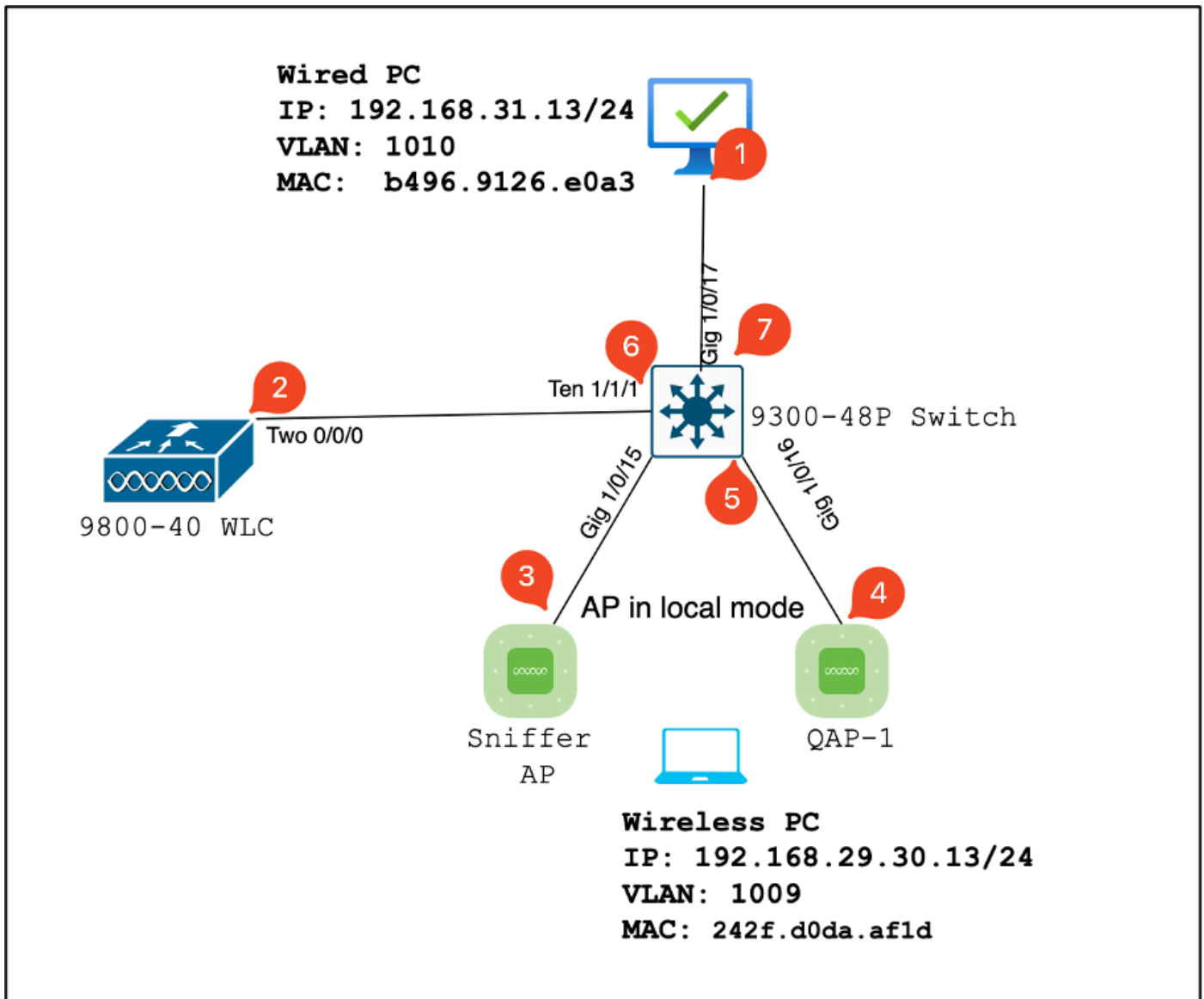
To replicate and validate the QoS configuration, a small-scale lab environment is used. The lab includes these components:

- WLC
- AP
- Sniffer AP to take OTA
- Wired PC
- Switch

All these components are connected to the same switch within the lab environment. The highlighted

numbers in this diagram indicate the points where packet captures are enabled to monitor and analyze the traffic flow.

Network Diagram



LAB Topology

Lab Components and Packet Capture Points

WLC:

- Manages the QoS policies and configurations for the wireless network.
- Packet capture point: Capture traffic between the WLC, AP and switch.

AP:

- Provides wireless connectivity to clients and enforces QoS policies.
- Packet capture point: Capture traffic between the AP and the switch.

Sniffer AP:

- Acts as a dedicated device for capturing wireless traffic.

- Packet capture point: Capture wireless traffic between the AP and wireless clients.

Wired PC:

- Connected to the switch to simulate wired traffic and validate end-to-end QoS.
- Packet capture point: Capture transmitted and received QoS packets over wired link.

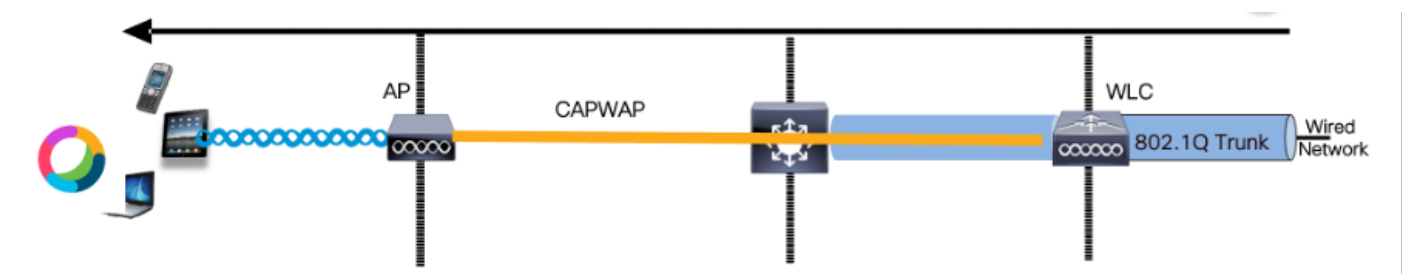
Wireless PC:

- Connected to the WLAN to simulate wireless traffic and validate end-to-end QoS.
- Packet capture point: Capture transmitted and received QoS packets over wireless link.

Switch:

- The central device that interconnects all lab components and facilitates traffic flow.
- Packet capture points: Capture traffic at various switch ports to validate proper QoS enforcement.

Logically the LAB topology can be drawn like this.



Logical LAB Topology

To test and validate the QoS configuration, iPerf is used to generate traffic between the client and the server. These commands are used to facilitate iPerf communication, with the roles of the server and client interchanged based on the direction of the QoS testing.

Test Scenario 1: Downstream QoS validation

The aim to validate the downstream QoS configuration. The setup involves a wired PC sending packets with DSCP 46 to a wireless PC.

The Wireless LAN Controller (WLC) is configured with the Metal "Platinum QoS" policy for both downstream and upstream directions.

Test Setup:

- **Traffic Flow:**

Source: Wired PC

Destination: Wireless PC

Traffic Type: UDP Packets with DSCP 46

- **QoS Policy Configuration on WLC:**

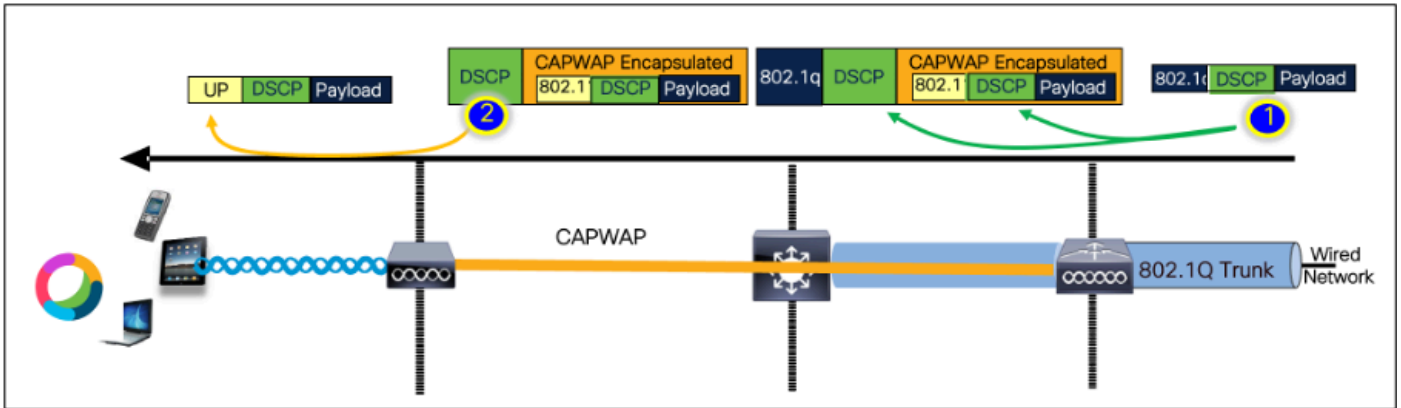
QoS Profile: Metal QoS - Platinum QoS

Direction: Both downstream and upstream

- **Metal QoS Configuration Commands:**

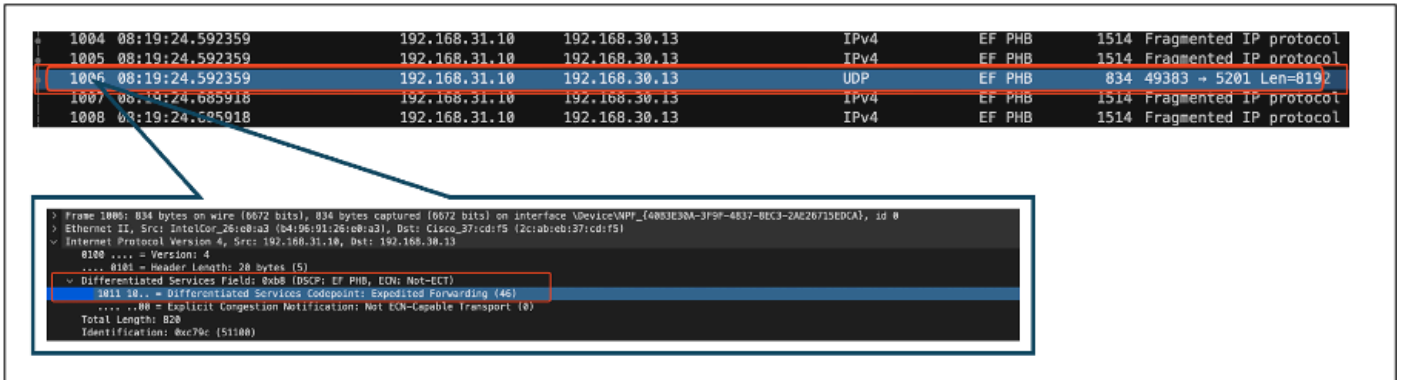
```
wireless profile policy qos-policy
service-policy input platinum-up
service-policy output platinum
```

Logical topology and the DSCP conversation at downstream direction.



DSCP Conversation Point

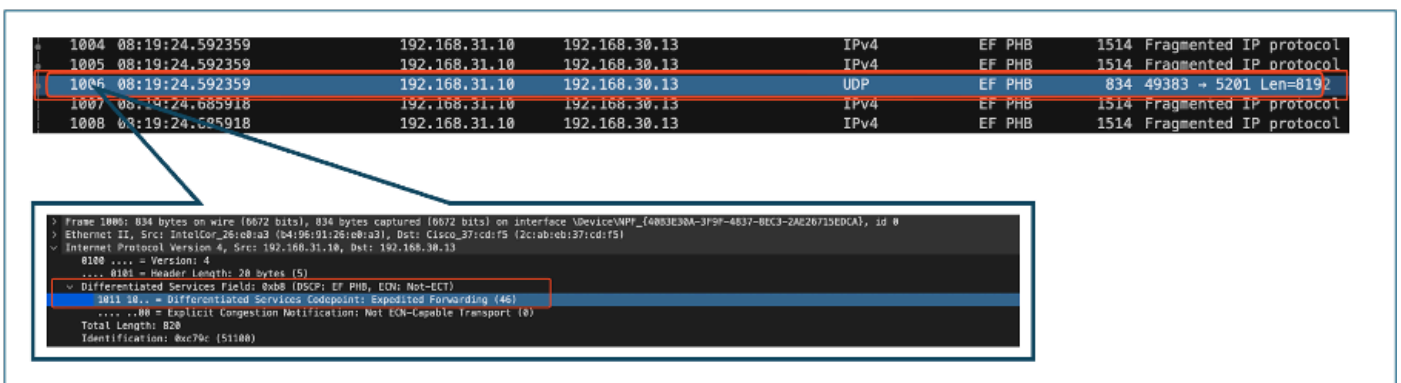
Packet Capture taken on the wired PC. This confirms that the wired PC is sending UDP packets to the specified destination IP 192.168.10.13 with the correct DSCP marking of 46.



Wired PC Capture - Downstream Direction

Next, let us examine a packet captured on the uplink switch connected to the wired PC. The switch trusts the DSCP tag and the DSCP value remains unchanged at 46.

Note: Switch ports on the Catalyst 9000 series default to a trusted state.



The image displays a network traffic capture interface. The top section shows a list of captured packets with columns for time, source IP, destination IP, protocol, DSCP marking, and length. Packet 1006 is highlighted in blue, showing a source IP of 192.168.31.10, destination IP of 192.168.30.13, protocol of UDP, and a DSCP marking of EF PHB. A red box highlights the DSCP field in the packet details below, showing a value of 46 (Expedited Forwarding). The packet details also show the DSCP field as 0xb8 (DSCP: EF PHB, ECN: Not-ECT).

Time	Source IP	Destination IP	Protocol	DSCP	Length	
1004	08:19:24.592359	192.168.31.10	192.168.30.13	IPv4	EF PHB	1514
1005	08:19:24.592359	192.168.31.10	192.168.30.13	IPv4	EF PHB	1514
1006	08:19:24.592359	192.168.31.10	192.168.30.13	UDP	EF PHB	834
1007	08:19:24.605918	192.168.31.10	192.168.30.13	IPv4	EF PHB	1514
1008	08:19:24.605918	192.168.31.10	192.168.30.13	IPv4	EF PHB	1514

```
> Frame 1006: 834 bytes on wire (6672 bits), 834 bytes captured (6672 bits) on interface \Device\NPF_{4083E30A-3F9F-4837-BEC3-2A26715EDCA}, id 0
> Ethernet II, Src: IntelCor_26:e8:a3 (04:96:91:26:e8:a3), Dst: Cisco_37:cd:f5 (2c:1a:eb:b7:cd:f5)
> Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13
8180 ... = Version: 4
... 8181 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
... 1011 10... = Differentiated Services Codpoint: Expedited Forwarding (46)
... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 820
Identification: 0xc79c (51100)
```

Wired PC Uplink Interface Capture

Upon examining the packet capture on the WLC taken using EPC, The packet arrives with the same DSCP tag of 46 from the uplink switch. This confirms that the DSCP marking is preserved as the packet reaches the WLC.

```

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-BECC-2AC20715EDCA}, id 0
> Ethernet II, Src: IntelCor_26:8b33 (84:95:91:26:8b33), Dst: Cisco_37:cd:f5 (2c:ab:cb: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: 820
  Identification: 0xc79c (51108)

```

WLC EPC Downstream Direction

When the WLC sends the packet to the AP inside a CAPWAP tunnel, it is a critical intersection where the WLC can modify the DSCP based on its configuration. Let us break down the packet capture, which is highlighted with numbered points for clarity:

- **CAPWAP Outer Layer:** The outer layer of the CAPWAP tunnel shows the DSCP tag as 46, which is the value received from the switch end.
- **802.11 UP Value Inside CAPWAP:** Inside the CAPWAP tunnel WLC maps the DSCP 46 to 802.11 User Priority (UP) 6, which corresponds to Voice traffic.
- **DSCP Value Inside CAPWAP:** The Cisco 9800 WLC operates with a trust DSCP model, so the DSCP value inside the CAPWAP tunnel is kept at 46 same as the outer DSCP layer.

```

2735 08:19:24.716958      2c:ab:37:cd:f5:19  24:2f:d0:d8:af:1d  192.168.31.10      192.168.30.13      IPv4      EF PHB      164 Fragmented IP protocol
2736 08:19:24.716958      2c:ab:37:cd:f5:19  24:2f:d0:d8:af:1d  192.168.31.10      192.168.30.13      IPv4      EF PHB      988 Fragmented IP protocol
2737 08:19:24.716958      10:105:60:198      10.105.60.158      CAPWAP-Data  EF PHB      1478 CAPWAP-data (Fragment
2738 08:19:24.716958      2c:ab:37:cd:f5:19  24:2f:d0:d8:af:1d  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 (88:2d:bfe7:9d:ab), Dst: Cisco_28:35:74 (a4:b4:39:28:35:74)
> 802.1Q Virtual LAN, PVID: 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: 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: 898
  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: 0x8000 (Swapped)
      .000 0000 0000 0000 = Duration: 0 microseconds
      Receiver address: 24:2f:d0:d8:af:1d (24:2f:d0:d8:af:1d)
      Transmitter address: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
      Destination address: 24:2f:d0:d8:af:1d (24:2f:d0:d8:af:1d)
      Source address: Cisco_37:cd:f5 (2c:ab:cb:37:cd:f5)
      BSS Id: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
      STA address: 24:2f:d0:d8:af:1d (24:2f:d0:d8:af:1d)
      .... ..00 = Fragment number: 0
      0000 0000 0000 .... = Sequence number: 0
    > QoS Control: 0x0006
      .... ..0110 = TID: 6
      [.... ..0110 = Priority: Voice (Voice) (6)]
      .... ..00 .... = EDSP: 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: 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

```

CAPWAP DSCP Markings

Next, check the same packet on the AP uplink switch port.

The DSCP value on the outer CAPWAP layer remains at 46. For illustrative purposes, the inner CAPWAP

traffic is highlighted to show the tagging.

The image shows a network traffic capture with three packets highlighted in blue. The first packet (No. 13369) is from 192.168.31.10 to 192.168.30.13, protocol IPv4, DSCP EF PHB, length 164. The second packet (No. 13370) is from 192.168.31.10 to 192.168.30.13, protocol IPv4, DSCP EF PHB, length 988. The third packet (No. 13371) is from 10.105.60.198 to 10.105.60.158, protocol CAPWAP-Data, DSCP EF PHB, length 1478. Below the packet list is a detailed view of the second packet, showing its structure: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and IEEE 802.11 QoS Data. The QoS Data field is expanded to show: Type/Subtype: QoS Data (0x0028), Frame Control Field: 0x8028, Duration: 0 microseconds, Receiver address: 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, 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, Fragment number: 0, Sequence number: 0, and QoS Control: 0x0006. The QoS Control field is expanded to show: TID: 6, Priority: Voice (Voice) (6), EOSP: Service period, Ack Policy: Normal Ack (0x0), and Payload Type: MSDU.

AP Uplink Switch Interface Capture

Once the AP receives the packet, it transmits the packet over the air. To verify the User Priority (UP) tagging, an Over-the-Air (OTA) capture taken with a sniffer AP is used.

The AP has forwarded the frame with a UP value of 6. This confirms that the AP correctly maps the DSCP value to the appropriate 802.11 UP value (6), which corresponds to Voice traffic.

The image shows a network traffic capture with one packet highlighted in blue. The packet (No. 2061) is from 10.105.60.198 to 10.233.7.212, protocol 002.11, DSCP CS0 Voice (Voice), length 971. Below the packet list is a detailed view of the packet, showing its structure: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and IEEE 802.11 radio information. The radio information field is expanded to show: IEEE 802.11 QoS Data, Flags: .p...F.C, Type/Subtype: QoS Data (0x0028), Frame Control Field: 0x8842, Duration: 48 microseconds, Receiver address: 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, 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, Fragment number: 0, Sequence number: 1952, Frame check sequence: 0x6e2c7cfe [unverified], [FCS Status: Unverified], QoS Control: 0x0006. The QoS Control field is expanded to show: TID: 6, Priority: Voice (Voice) (6), EOSP: Service period, Ack Policy: Normal Ack (0x0), and Payload Type: MSDU.

OTA Capture From AP to Client

At the final stage, the packet received by the wireless PC. The wireless PC receives the frame with a DSCP value of 46.

This indicates that the DSCP marking is preserved throughout the entire transmission path, from the wired PC to the wireless PC. The consistent DSCP value of 46 confirms that the QoS policies are correctly applied and maintained in the downstream direction.

```

No. 2061 68:19:24:830431 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=0
    > 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
        > CCMP parameters
        > Data (836 bytes)
    
```

Wireless PC Capture

Test Scenario 2: Upstream QoS Validation

In this test scenario, the aim is to validate the upstream QoS configuration. The setup involves a wireless PC sending UDP packets with DSCP 46 to a wired PC. The WLC is configured with the Metal "Platinum QoS" policy for both upstream and downstream directions.

- **Traffic Flow:**

Source: Wireless PC

Destination: Wired PC

Traffic Type: UDP packets with DSCP 46

- **QoS Policy Configuration on WLC:**

QoS Profile: Platinum QoS

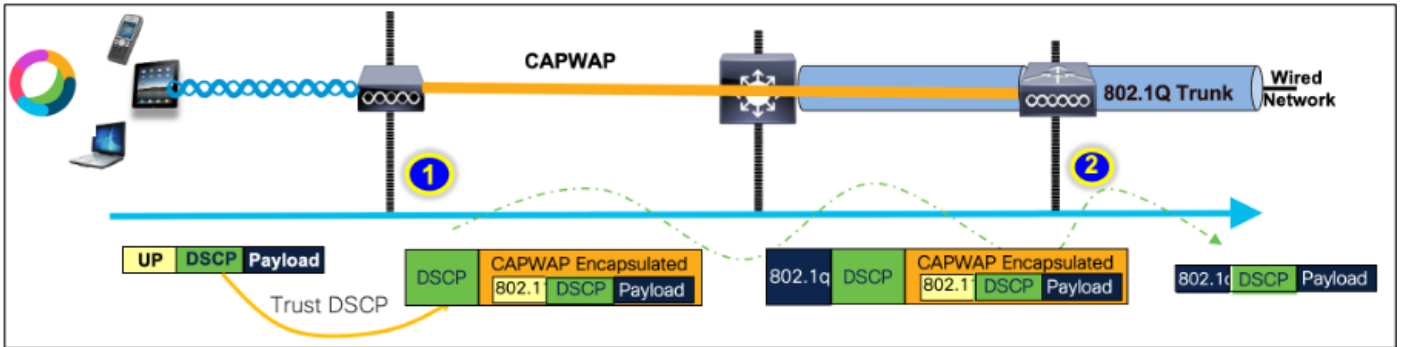
Direction: Both upstream and downstream

- **Metal QoS Configuration Commands:**

```

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

Logical Topology and DSCP Conversion in upstream direction:



Logical Topology and DSCP Conversion - Upstream

Packets sent from wireless PC to wired PC. This capture is taken at the wireless PC.

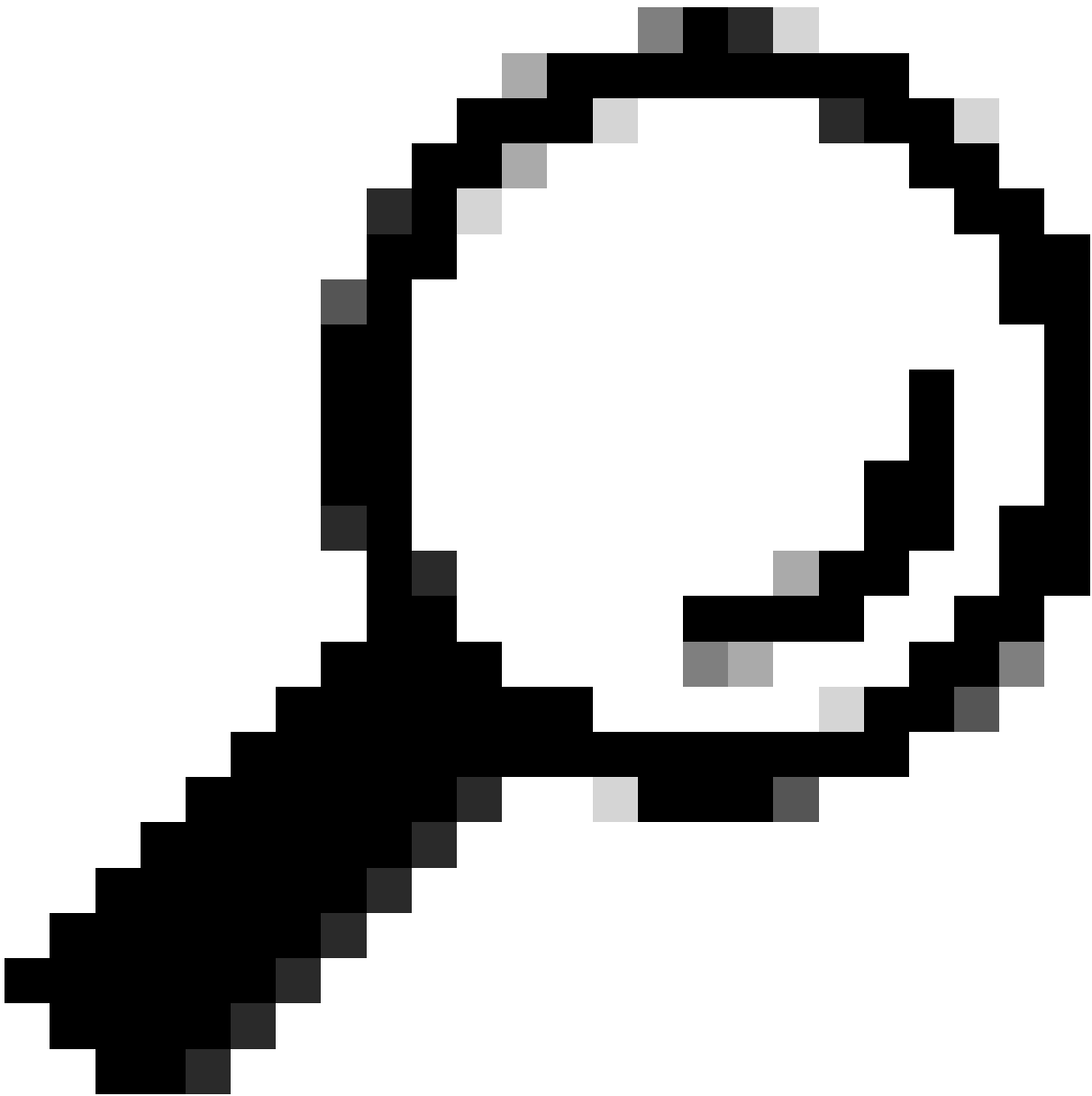
The wireless PC sends UDP packets with DSCP 46.

```
No. | Time | SA | RA | Source | Destination | Protocol | DSCP | Priority | Length | Info
---|---|---|---|---|---|---|---|---|---|---
241 | 10:53:22.943430 | | | 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:ci:ab: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)
  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 Capture in Upstream Direction

Next let us look at the OTA capture from Client to AP.



Tip: When using a Windows wireless PC to send packets with DSCP 46, Windows maps DSCP 46 to a User Priority (UP) value of 5 (Video). As a result, the OTA capture shows the packets as Video traffic (UP 5). However, if you decrypt the packet, the DSCP value remains at 46.



Note: Starting from version 17.4, the default behaviour for the Cisco 9800 WLC is to trust the DSCP value in AP join profile. This ensures that the DSCP value of 46 is preserved and trusted by the WLC, preventing any issues related to the Windows DSCP to UP mapping behaviour.

```

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
1011 10.. 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 UP to DSCP Mapping

The encrypted Over-the-Air (OTA) capture taken from the lab setup is analyzed to validate the upstream QoS configuration.

The OTA capture shows the packets with a User Priority (UP) value of 5 (Video). Although the OTA capture shows UP 5, the DSCP value inside the encrypted packet remains at 46.

No.	Time	SA	RA	Source	Destination	Protocol	DSCP	Priority	Length	Info
5643	14:53:22.982358	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)	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 Direction

Next, the packet capture on the AP uplink port is analyzed to ensure that the DSCP value is preserved as the packet moves from the AP to the WLC.

- The DSCP value on the outer CAPWAP layer is maintained at 46.
- Inside the CAPWAP tunnel, the DSCP value is also kept at 46.

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: 0xb7e9 (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 Capture in Upstream Direction

The capture is taken at the WLC as the packet arrives from the switch.

- The packet arrives at the WLC with the DSCP value of 46 on the outer CAPWAP layer.
- Inside the CAPWAP tunnel, the DSCP value is kept at 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: 1502)
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)
> Ethernet II, Src: Cisco_28:35:74 (a4:b4:39:28:35:74), Dst: Cisco_e7:9d:ab (08:2d: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 Fields (0x0004 Sweaped)
... 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 0000 = QoS bit 4: Bits 0-15 of QoS Control field are TXOP Duration Requested
.... 0000 0000 0000 = Ack Policy: Normal Ack (0x0)
.... 0000 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 Showing Packets Coming From AP

After the packet takes a hairpin turn at the WLC, it is sent back to the uplink switch, destined for the wired PC. The WLC forwards the packet with the DSCP value of 46.

No.	Time	SA	RA	Source	Destination	Protocol	DSCP	Priority	Length	Info
526	10:53:23.187287	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)
> 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 Showing Packets Sent to Wired PC

Finally, the packet capture at the wired PC uplink is analyzed to ensure that the DSCP value is preserved as the packet arrives from the WLC.

No.	Time	SA	RA	Source	Destination	Protocol	DSCP	Priority	Length	Info
5039	10:53:23.187287	24:2f:d0:da:af:1d	2c:ab:eb:37:cd:e5	192.168.30.13	192.168.31.10	IPv4	EF PHB		1518	Fragmented IP protocol (p)
5040	10:53:23.187381	24:2f:d0:da:af:1d	2c:ab:eb:37:cd:e5	192.168.30.13	192.168.31.10	IPv4	EF PHB		1518	Fragmented IP protocol (p)

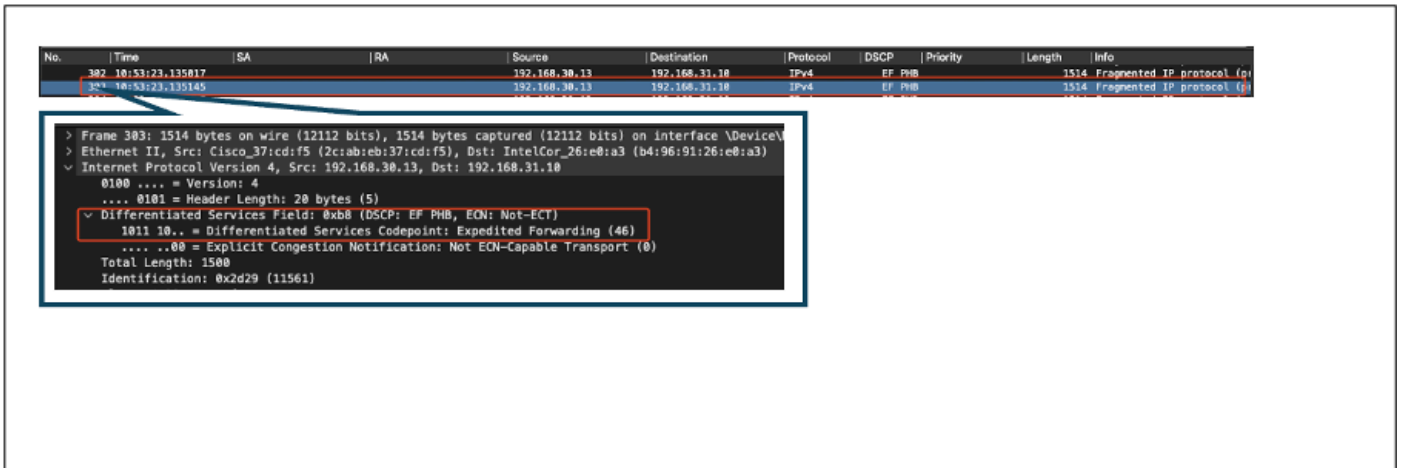
```

> Frame 5040: 1518 bytes on wire (12144 bits), 1518 bytes captured (12144 bits) on
> 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)

```

Wired PC Uplink Switch Capture in Upstream Direction

At the final stage, the packet received by the wired PC is analyzed to ensure that the packet arrives at the wired PC with the DSCP value of 46.



Wired PC Capture - Upstream Direction

The upstream QoS test successfully validated the QoS configuration for traffic flowing from the wireless PC to the wired PC. The consistent preservation of the DSCP value of 46 throughout the entire transmission path confirms that the QoS policies are correctly applied and enforced.

Troubleshooting

Voice, video and other real-time applications are particularly sensitive to network performance issues, and any degradation in Quality of Service (QoS) can have noticeable and detrimental effects. When QoS packets are remarked with lower DSCP values, the impact on voice and video can be significant.

Impact on Voice:

- **Increased Latency:** Voice communication requires low latency to ensure that conversations are natural and fluid. Lower DSCP values can result in voice packets being delayed, causing noticeable lag in conversations.
- **Jitter:** Variability in packet arrival times (jitter) can disrupt the smooth delivery of voice packets. This can lead to choppy or garbled audio, making it difficult to understand the speaker.
- **Packet Loss:** Voice packets are highly sensitive to packet loss. Even a small amount of packet loss can result in missing words or syllables, leading to poor call quality and misunderstandings.
- **Echo and Distortion:** Increased latency and jitter can cause echo and audio distortion, further degrading the quality of the voice call.

Impact on Video:

- **Increased Latency:** Video communication requires low latency to maintain synchronization between audio and video streams. Increased latency can cause delays, making it difficult to have real-time interactions.
- **Jitter:** Jitter can cause video frames to arrive out of order or at irregular intervals, leading to a jerky or stuttering video experience.
- **Packet Loss:** Lost packets can result in missing frames, which can cause the video to freeze or display artifacts.
- **Reduced Video Quality:** Lower DSCP values can lead to reduced bandwidth allocation for video streams, resulting in lower resolution and poorer video quality. This can make it difficult to see important details in the video.

Scenario 1: Intermediate Switch Rewrites DSCP Marking

In this troubleshooting scenario, the impact of an intermediate switch rewriting the DSCP marking on traffic as it arrives at the WLC is investigated. To replicate this, the switch is configured to rewrite the DSCP 46 marking to CS1 on the wired PC uplink interface.

The packet is sent from the wired PC with a 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)
```

Wired PC Sending Packet With DSCP 46 Tag

The packet arrives at the WLC with a DSCP value of CS1 (DSCP 8). The change from DSCP 46 to DSCP 8 significantly lowers the priority of the packet.

```
> 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 Showing CS1 Marking

In this step, the packet forwarded by the WLC to the AP is analyzed.

- The outer CAPWAP header is tagged with CS1 (DSCP 8).
- The inner CAPWAP header is also tagged with CS1 (DSCP 8).
- The User Priority (UP) value is set to BK (Background).

```

> 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)]
  .... .... 0000 = EOSP: Service period
  .... .... 0000 = Ack Policy: Normal Ack (0x0)
  .... .... 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: 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)

```

1

2

3

WLC EPC Showing CSI Tag in CAPWAP Traffic

The packet arrives at the wireless PC with a DSCP value of CS1 (DSCP 8).

```

> Frame 613: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\
> 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

```

Wireless PC Capture Showing CSI Marking

This scenario demonstrates how a misconfiguration on an intermediate switch can break the QoS

configuration, leading to degraded performance for high-priority traffic. The voice packets, initially marked for high priority, were treated as lower-priority traffic due to the DSCP rewrite. This scenario underscores the importance of ensuring that intermediate network devices correctly preserve QoS markings to maintain the desired quality of service for high-priority traffic.

Scenario 2: AP link Switch Rewrites DSCP Marking

In this scenario, the impact of an intermediate switch connected to the AP rewriting the DSCP marking on traffic is investigated.

- The switch connected to the AP is configured to rewrite the DSCP 46 marking to a different value CS1 on the AP uplink interface.
- The packet is sent from the wired PC with a DSCP tag of 46. This confirms that the traffic is correctly marked with DSCP 46 at the source.

```
> 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 = Flags: 0x0
```

Wireless PC Capture Showing DSCP 46

The capture is taken at the WLC as the packet arrives from the switch.

The packet arrives at the WLC with the outer CAPWAP header DSCP value of CS1 (DSCP and the inner DSCP value of 46. This happens because the intermediate switch can not see the traffic encapsulated inside the CAPWAP tunnel.

The WLC trusts the DSCP tag inside the CAPWAP tunnel and forwards the traffic to the wired PC with the inner DSCP tag of 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
    [..... 0110 = Priority: Voice (Voice) (6)]
    .... .... 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)
> 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 Showing CAPWAP DSCP Values

The packet arrives at the wired PC with a DSCP value of 46. Confirms that the WLC correctly forwards the packet with the original DSCP value of 46, preserving the high-priority marking.

```

> 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)
✓ 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

```

Although the WLC forwarded the traffic with a DSCP tag of 46, it is important to understand that the traffic from the AP to the WLC was treated as low priority due to the outer DSCP tag being rewritten to CS1 (DSCP 8).

There can be multiple switches between the AP and the WLC, and if the traffic is given low priority, it can arrive at the WLC late. This can lead to increased latency, jitter, and potential packet loss, which can degrade the quality of service for high-priority traffic such as voice.

Troubleshooting Tip

1. **Verify Initial DSCP Marking:** Capture packets at the source (for example, wired PC) to ensure that the traffic is correctly marked with the intended DSCP value.
2. **Check Intermediate Device Configurations:** Review the configuration of all intermediate switches and routers to ensure they are not inadvertently rewriting DSCP values.
3. **Capture Traffic at Key Points:**
 1. Before and after the intermediate switch.
 2. At the WLC.
 3. At the destination (for example, wireless PC).
4. **Simulate Traffic Scenarios:** Use traffic generators or network simulation tools to create different types of traffic and observe how QoS is handled by the wireless network.
5. **Consult 9800 best practice document:** Review the 9800 best practice documentation on configuring QoS and DSCP markings.

Configuration Verification

<#root>

On the WLC, these commands can be used to verify the configuration.

```
# show run qos
```

```
# show policy-map <policy-map name>
```

```
# show class-map <policy-map name>
```

```
# show wireless profile policy detailed <policy-profile-name>
```

```
# show policy-map interface wireless ssid/client profile-name <name> radio type 2GHz|5GHz|6GHz ap name <
```

```
# show policy-map interface wireless client mac <MAC> input|output
```

```
# show wireless client mac <MAC> service-policy input|output
```

On AP, these commands can be used to check the QoS.

```
# show dot11 qos
```

```
# show controllers dot11Radio 1 | begin EDCA
```

Conclusion

Maintaining consistent QoS configuration across the network is crucial to ensure that high-priority traffic, such as voice and video, receives the appropriate level of service and performance. It is essential to validate QoS configurations regularly to ensure that all network devices are complying with the intended QoS policies. This validation helps identify and rectify any misconfiguration or deviations that could compromise network performance.

References

- [Understanding and Troubleshooting Cisco Catalyst 9800 Series Wireless Controllers](#)
- [Cisco Catalyst 9800 Series Configuration Best Practices](#)
- [Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS® XE Dublin 17.12.x](#)
- [Voice Over Wireless LAN \(VoWLAN\) Troubleshooting Guide](#)
- [Enable DSCP QoS Tagging on Windows Machines](#)