

配置9800 WLC上的無線QoS驗證和故障排除

目錄

[簡介](#)

[採用元件](#)

[背景資訊](#)

[組態](#)

[QoS策略目標](#)

[自動QoS](#)

[自動QoS CLI配置](#)

[模組化QoS CLI](#)

[MQS CLI配置](#)

[金屬QoS](#)

[金屬QoS CLI配置](#)

[驗證使用資料包捕獲的端到端QoS](#)

[網路圖表](#)

[實驗元件和資料包捕獲點](#)

[測試場景1：下游QoS驗證](#)

[測試場景2：上游QoS驗證](#)

[疑難排解](#)

[方案1：中間交換機重寫DSCP標籤](#)

[方案2：AP鏈路交換機重寫DSCP標籤](#)

[疑難排解提示](#)

[組態驗證](#)

[結論](#)

[參考資料](#)

簡介

本檔案介紹在9800無線LAN控制器(WLC)上設定、驗證無線服務品質(QoS)和對其進行疑難排解的方法。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- WLC：C9800-40-K9運行17.12.03
- 存取點(AP)：C9120-AX-D
- 交換機：運行17.03.05的C9300-48P
- 有線和無線客戶端：Windows 10

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

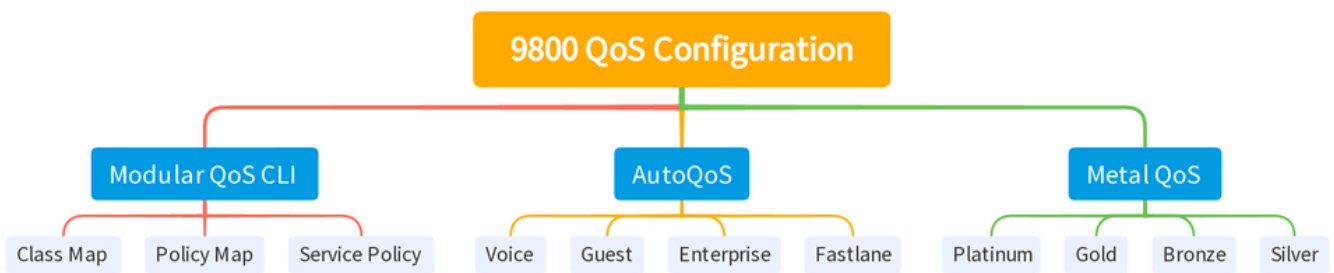
無線QoS對於確保關鍵應用程式獲得最佳化效能所需的必要頻寬和低延遲至關重要。本文檔提供在Cisco無線網路上配置、驗證和排除QoS故障的全面指南。

本文假設讀者對無線和有線QoS原則有基本的瞭解。此外，讀者應精通配置和管理Cisco WLC和AP。

組態

本節深入探討9800無線控制器上的QoS配置。利用這些配置，您可以確保關鍵應用程式獲得所需的頻寬和低延遲，從而最佳化整體網路效能。

您可以將9800 WLC QoS組態主要分為三個不同的廣泛類別。



9800 WLC QOS配置摘要

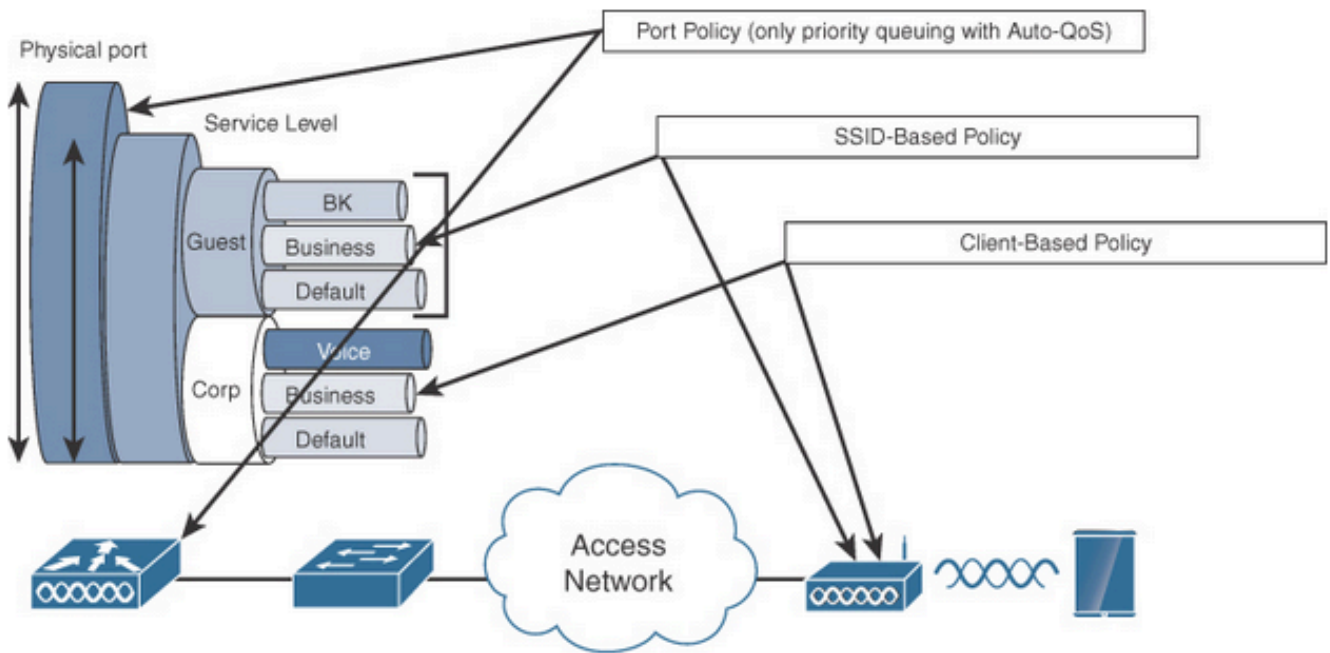
本文檔將在後續章節中逐一介紹每個章節。



注意：本文重點介紹本地模式下的AP。不討論Flexconnect模式下的AP。

QoS策略目標

策略目標是可以應用QoS策略的配置結構。Catalyst 9800上的QoS實施是模組化和靈活的。使用者可以決定在三個不同目標上配置策略：SSID、客戶端和埠級別。



QoS策略目標

SSID策略適用於每個SSID的每個AP。您可以在SSID上配置策略和標籤策略。

客戶端策略適用於入口和出口方向。您可以在客戶端上配置策略和標籤策略。還支援AAA覆蓋。

基於埠的QoS策略可以在物理埠或邏輯埠應用。

自動QoS

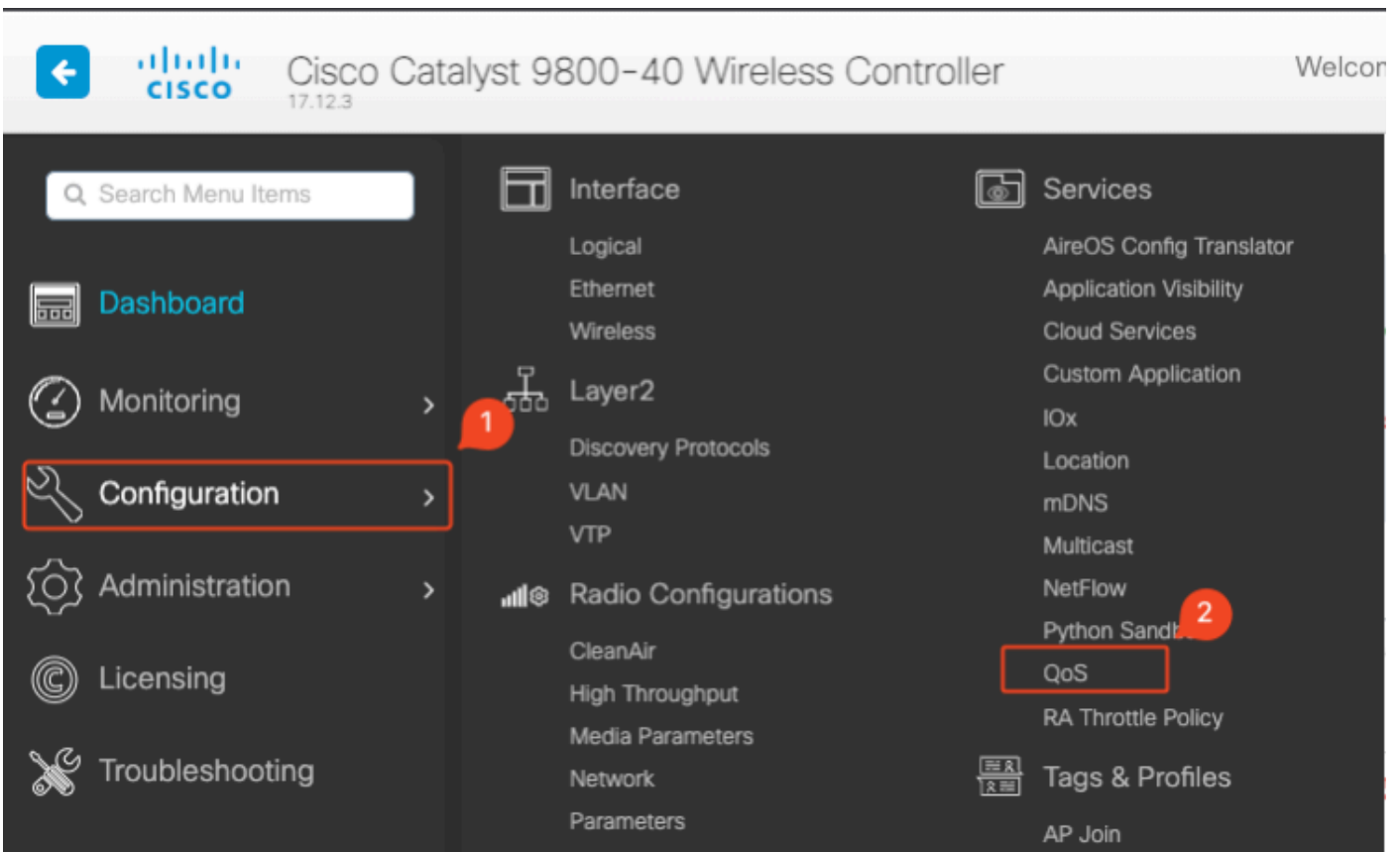
無線自動QoS可自動部署無線QoS功能。它有一組預定義配置檔案，管理員可進一步修改這些配置檔案以區分不同流量的優先順序。自動QoS匹配流量並將每個匹配的資料包分配給QoS組。這允許輸出策略對映將特定QoS組放入特定隊列，包括優先順序隊列。

模式	入口客戶端	客戶端出口	入口的BSSID	出口BSSID	入口埠	出口埠	無線電
語音	不適用	不適用	白金級	白金	不適用	AutoQos-4.0-wlan-Port-Output-Policy	ACM開啟
訪客	不適用	不適用	AutoQos-4.0-wlan-GT-SSID-Input-Policy	AutoQos-4.0-wlan-GT-SSID-Output-Policy	不適用	AutoQos-4.0-wlan-Port-Output-Policy	
快速通道	不適用	不適用	不適用	不適用	不適用	AutoQos-4.0-	edca-

	用	用			用	wlan-Port-Output-Policy	parameters fastlane
Enterprise-avc	不適用	不適用	AutoQos-4.0-wlan-ET-SSID-Input-AVC-Policy	AutoQos-4.0-wlan-ET-SSID-Output-Policy	不適用	AutoQos-4.0-wlan-Port-Output-Policy	

此表描述了在應用自動QoS配置檔案後發生的配置更改。

要配置自動QoS，請導航到配置> QoS



QoS工作流程

按一下Add，然後將Auto QoS設定為enabled。從清單中選擇相應的Auto QoS宏。在本示例中，使用了用於排列語音流量優先順序的Voice宏。

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: 100px; width: 100%;"></div>

AutoQoS語音對應

啟用巨集之後，選取需要附加到原則的策略。

自動QoS CLI配置

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

啟用Auto QoS後，您可以看到發生的更改。本部分列出了語音的配置更改。

```
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
```

模組化QoS CLI

MQC允許您定義流量類、建立流量策略 (策略對映) 並將流量策略附加到介面。流量策略包含應用於流量類的QoS功能。



MQS CLI工作流程

此示例演示如何使用訪問控制清單(ACL)對流量進行分類並應用頻寬限制。

建立ACL以標識和分類要管理的特定流量。這可以透過根據IP地址、協定或埠等條件定義匹配流量的規則來實現。

導航到Configuration > Security > ACL , 然後增加ACL。

Configuration > Security > ACL

+ Add × Delete Associate Interfaces

ACL Name	ACL Type	ACE Count	Download
server-bw	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
1	permit	192.168.31.10		any		ip	None	None	None	Disabled
2	permit	any		192.168.31.10		ip	None	None	None	Disabled

1 - 2 of 2 items

Cancel Apply to Device

ACL配置

使用ACL對流量進行分類後，配置頻寬限制以控制分配給此流量的頻寬量。

導航到配置>服務> QoS和QoS策略。將ACL附加到策略內，然後以kbps為單位應用策略。

向下滾動並選擇要應用QoS的策略配置檔案。您可以為SSID或客戶端選擇入口/出口方向的策略。

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
0	10						No items to display

[+ Add Class-Maps](#) [× Delete](#)

AVC/User Defined

Match Any All

Match Type

Match Value*

Mark Type

Drop

Police(kbps)

MQS策略

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設定檔

MQS CLI配置

```

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
  
```

金屬QoS

這些QoS設定檔的主要目的是限制無線網路上允許的最大區別服務代碼點(DSCP)值，進而控制802.11使用者優先順序(UP)值。

在Cisco 9800無線LAN控制器(WLC)中，金屬QoS設定檔是預先定義的，無法設定。但是，您可以將這些配置檔案應用到特定SSID或客戶端以實施QoS策略。

有四個可用的金屬QoS配置檔案：

QoS設定檔	最大DSCP
銅牌	8
銀色	0
金牌	34
白金級	46

要在Cisco 9800 WLC上配置金屬QoS，請執行以下操作：

導航到配置>策略> QoS和AVC。

- 選擇所需的金屬QoS配置檔案（白金級、金級、銀級或銅級）。
- 將選取的設定檔套用至目標SSID或使用者端。

⚠ 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

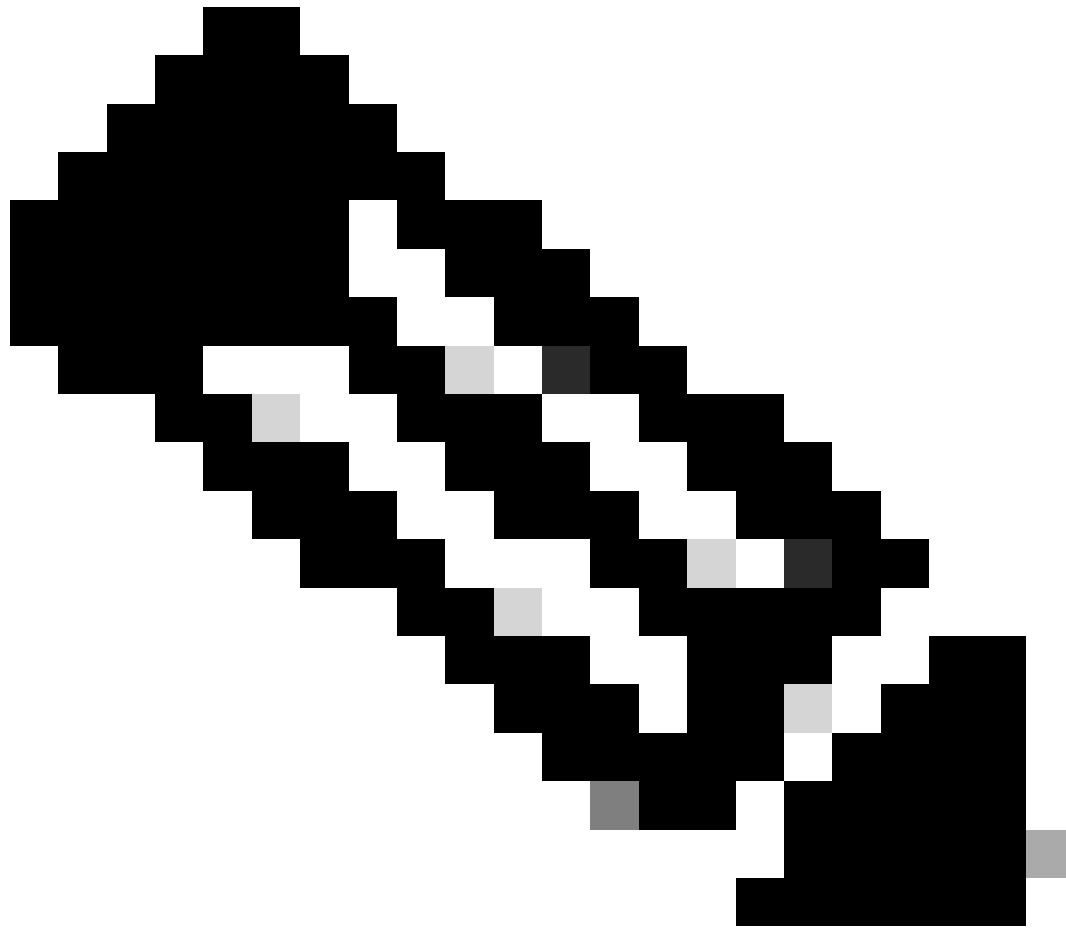
Egress Search or Select

Ingress Search or Select

金屬QoS配置檔案

金屬QoS CLI配置

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



注意：每個使用者和SSID頻寬合約可以透過QoS策略進行配置，不能直接在金屬QoS上配置。在9800中，非匹配流量使用預設類。



注意：在GUI上，只能設定每個SSID的金屬QoS。在CLI上，您也可以在客戶端目標上進行配置。

驗證使用資料包捕獲的端到端QoS

現在，QoS配置已完成，必須檢查QoS資料包，並驗證QoS策略在端到端的運行是否正常。這可以透過資料包捕獲和分析來實現。

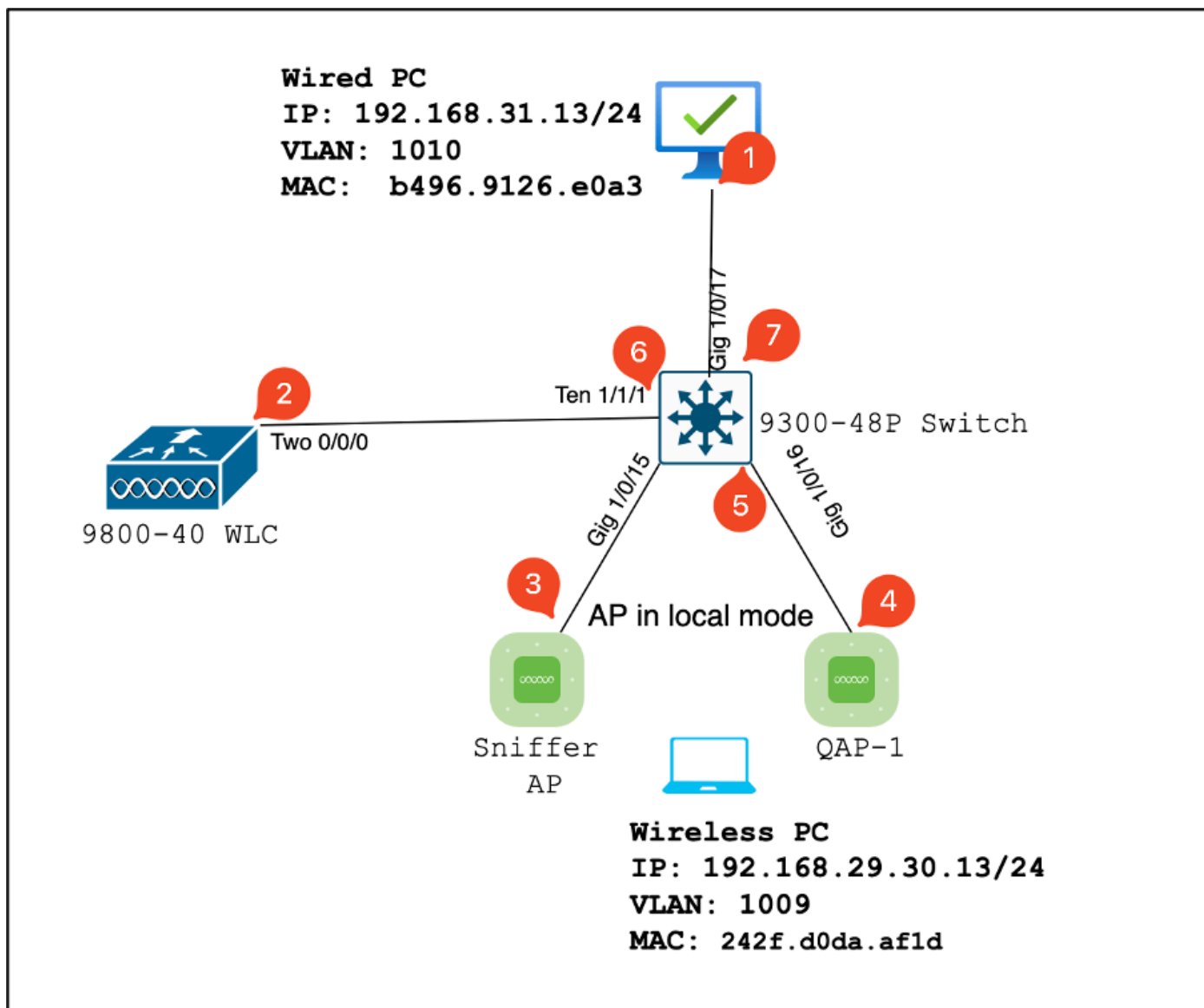
要複製和驗證QoS配置，需要使用小規模實驗環境。本實驗包括以下元件：

- WLC
- AP
- 監聽器AP將接受OTA
- 有線PC
- 交換器

所有這些元件都連線到實驗環境中的同一台交換機。此圖中的突出顯示數字表示啟用資料包捕獲以

監控和分析流量流的點。

網路圖表



實驗室拓撲

實驗元件和資料包捕獲點

WLC :

- 管理無線網路的QoS策略和配置。
- 資料包捕獲點：捕獲WLC、AP和交換機之間的流量。

AP :

- 為客戶端提供無線連線並實施QoS策略。
- 資料包捕獲點：捕獲AP與交換機之間的流量。

監聽器AP :

- 充當用於捕獲無線流量的專用裝置。
- 資料包捕獲點：捕獲AP與無線客戶端之間的無線流量。

有線PC：

- 連線到交換機以模擬有線流量並驗證端到端QoS。
- 資料包捕獲點：透過有線鏈路捕獲傳輸和接收的QoS資料包。

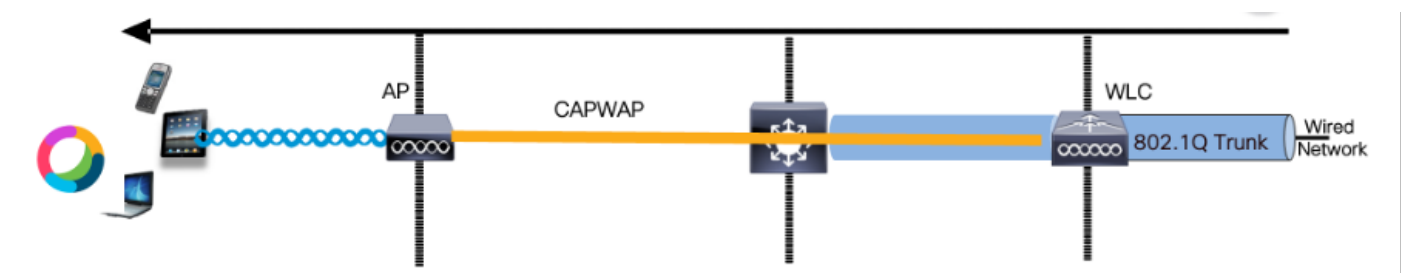
無線PC：

- 連線到WLAN以模擬無線流量並驗證端到端QoS。
- 資料包捕獲點：透過無線鏈路捕獲傳輸和接收的QoS資料包。

交換器：

- 連線所有實驗元件並促進流量傳輸的中央裝置。
- 資料包捕獲點：捕獲各種交換機埠上的流量以驗證正確的QoS實施。

從邏輯上講，LAB拓撲可以這樣繪製。



邏輯LAB拓撲

為了測試和驗證QoS配置，iPerf用於生成客戶端和伺服器之間的流量。這些命令用於促進iPerf通訊，伺服器和客戶端的角色根據QoS測試方向進行互換。

測試場景1：下游QoS驗證

目的是驗證下游QoS配置。設定涉及有線PC使用DSCP 46向無線PC傳送資料包。無線區域網路控制器(WLC)為下游和上游方向設定金屬「白金服務」原則。

測試設定：

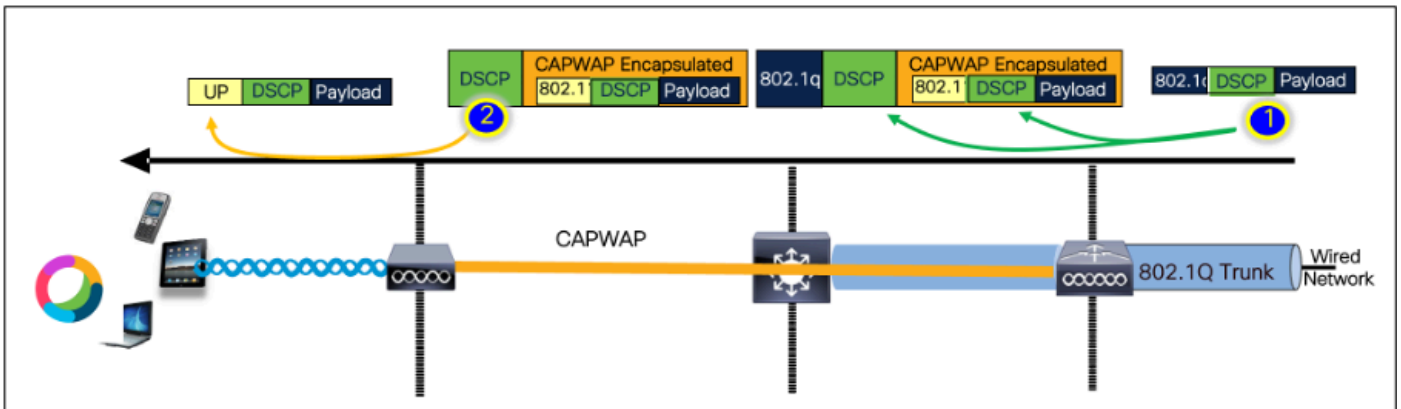
- 流量傳輸：
 - 來源：有線PC
 - 目的地：無線PC
 - 流量型別：使用DSCP 46的UDP資料包
- WLC上的QoS策略配置：
 - QoS配置檔案：金屬QoS -白金QoS

方向：下游與上游

- 金屬Qos配置命令：

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

下游方向的邏輯拓撲和DSCP會話。



DSCP通話點

有線PC上的資料包捕獲。這確認有線PC正在向指定的目標IP 192.168.10.13傳送UDP資料包，且正確的DSCP標籤為46。

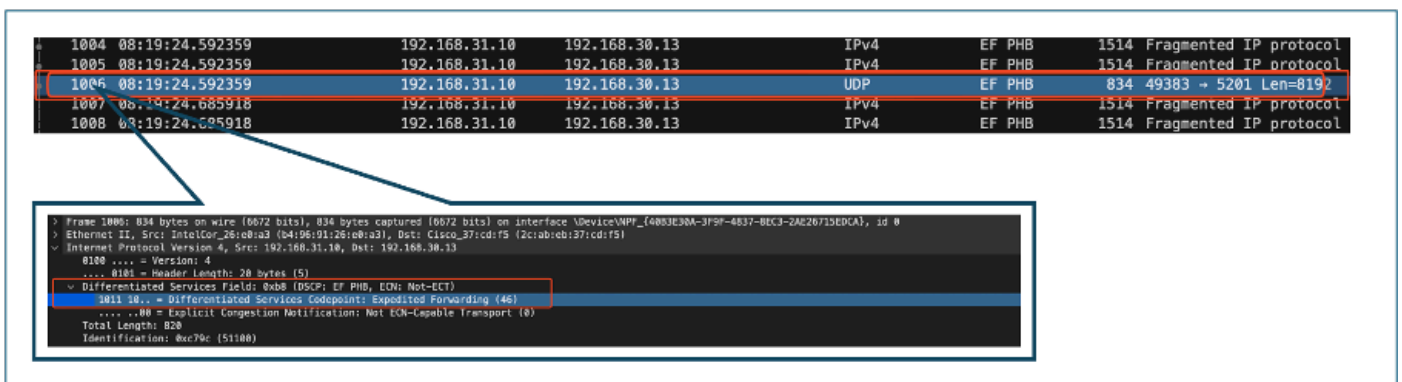
```
1004 08:19:24.592359 192.168.31.10 192.168.30.13 IPv4 EF PHB 1514 Fragmented IP protocol  
1005 08:19:24.592359 192.168.31.10 192.168.30.13 IPv4 EF PHB 1514 Fragmented IP protocol  
1006 08:19:24.592359 192.168.31.10 192.168.30.13 UDP EF PHB 834 49383 - 5201 Len=8192  
1007 08:19:24.685918 192.168.31.10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

```
> Frame 1006: 834 bytes on wire (6672 bits), 834 bytes captured (6672 bits) on interface \Device\NPF_{4083E30A-3F9F-4637-BE33-2AC2673E0CA}, id 0  
> Ethernet II, Src: IntelCor_26:e8:a3 (04:06:91:26:e8:a3), Dst: Cisco_37:cd:f5 (2c:1a:1b:37:cd:f5)  
> Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13  
  8100 ... = Version: 4  
  ... 8100 = 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)
```

有線PC捕獲-下行方向

接下來，讓我們檢查在連線到有線PC的上行鏈路交換機上捕獲的資料包。交換機信任DSCP標籤，並且DSCP值在46時保持不變。

注意：Catalyst 9000系列上的交換機埠預設為受信任狀態。



The image displays two screenshots from a network analysis tool. The top screenshot is a packet capture table with the following data:

Time	Source	Destination	Protocol	Priority	Length	Details
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

The bottom screenshot shows a detailed view of a packet header:

```
> Frame 1006: 834 bytes on wire (6672 bits), 834 bytes captured (6672 bits) on interface \Device\NPF_{4883E30A-3F9F-4637-BE33-2AC26713EDCA}, id 0
> Ethernet II, Src: IntelCor_26:e0:a3 (04:06:91:26:e0:a3), Dst: Cisco_37:cd:f5 (2c:a3:eb:b3:7c:d:f5)
> Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13
  8100 ... = Version: 4
  ... 0100 = 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)
```

有線PC上行鏈路介面捕獲

使用EPC檢查WLC上的資料包捕獲後，資料包到達時與來自上行鏈路交換機的不同DSCP標籤46。這確認在資料包到達WLC時，DSCP標籤被保留。

```

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-BECC-2AC20713EDCA}, id 0
> Ethernet II, Src: IntelCor_26:c8:b3 (84:95:91:26:c8:b3), 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
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
  .... --80 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 820
  Identification: 0xc79c (51108)

```

WLC EPC下游方向

當WLC將資料包傳送到CAPWAP隧道內的AP時，它是WLC可以根據其配置修改DSCP的重要交叉點。讓我們分析資料包捕獲，它以編號點突出顯示，以方便檢視：

- CAPWAP外層：CAPWAP隧道外層的DSCP標籤顯示為46，這是從交換機端接收的值。
- CAPWAP中的802.11 UP值：CAPWAP隧道WLC將DSCP 46對映到802.11使用者優先順序 (UP) 6，這對應於語音流量。
- CAPWAP中的DSCP值：Cisco 9800 WLC使用信任DSCP模型運行，因此CAPWAP隧道中的DSCP值保持為與外部DSCP層相同的46。

```

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 (88:7d:b1: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
  ....., 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)
  .... --80 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 890
  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:d8:da:af:1d (24:2f:d8:da:af:1d)
  Transmitter address: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
  Destination address: 24:2f:d8:da:af:1d (24:2f:d8: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:d8:da:af:1d (24:2f:d8:da:af:1d)
  .... 0000 = Fragment number: 0
  0000 0000 0000 .... = Sequence number: 0
  > QoS Control: 0x0006
  .... 0000 0000 0110 = TID: 6
  [.... 0000 0000 0110 = Priority: Voice (Voice) (6)]
  .... 0000 0000 .... = EDSP: 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
  ....., 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)
  .... --80 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 820

```

CAPWAP DSCP標籤

接下來，檢查AP上行鏈路交換機埠上的相同資料包。

外部CAPWAP層上的DSCP值保持在46。為了便於說明，內部CAPWAP流量會突出顯示，以顯示標籤。

13369	08:19:24:724776	2c:ab:1b:24:2f:1b	192.168.31.10	192.168.30.13	IPv4	EF PHB	164	Fragmented IP protocol (proto=UDP
13370	08:19:24:724773	2c:ab:1b:24:2f:1b	192.168.31.10	192.168.30.13	IPv4	EF PHB	988	Fragmented IP protocol (proto=UDP
13371	08:19:24:72475C		10.105.60.198	10.105.60.158	CAPWAP-Data	EF PHB	1478	CAPWAP-Data (Fragment ID: 16242,

```

> Frame 13370: 988 bytes on wire (7904 bits), 988 bytes captured (7904 bits) on interface /tap/osp_wx/wifi_to_ks_snpce, id 0
> Ethernet II, Src: Cisco_a7:8d:a8 (48:20:01:a7:8d:a8), Dst: Cisco_20:35:74 (48:d4:35:20:35:74)
> 802.1Q Virtual LAN, PVID: 9, QoS: 0, TO: 21
> Internet Protocol Version 4, Src: 10.105.60.198, Dst: 10.105.60.158
  0100 ... = Version 4
  .... 0101 ... = Header Length: 20 bytes (15)
  > Differentiated Services Field: 0x00 (DSCP: EF PHB, CS0: Not-ECT1)
  1011 10... = Differentiated Services Codepoint: Expedited Forwarding (46)
  .... 0x00 ... = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 888
  Identification: 0x0000 (0)
  > Flags: 0000
  ... 0x0000 0000 0000 = Fragment Offset: 0
  Time to Live: 255
  Protocol: UDP (17)
  Header Checksum: 0x0005 (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: 5202
  > Control And Provisioning of Wireless Access Points - Data
  > Frame 11
  > Header
  > IEEE 802.11 QoS Data, Flags: .....F.
  Type/Subtype: 0x0 Data (0x0013)
  > Frame Control Field: 0x0000 (Supp)
  0000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: 24:2f:d0:daf:1d (24:2f:d0:daf:1d)
  Transmitter address: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
  Destination address: 24:2f:d0:daf:1d (24:2f:d0:daf:1d)
  Source address: Cisco_37:cd:e5 (2c:ab:1b:37:cd:e5)
  BSS Id: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
  STA address: 24:2f:d0:daf:1d (24:2f:d0:daf:1d)
  .... 0000 ... = Fragment number: 0
  0000 0000 0000 ... = Sequence number: 0
  > QoS Control: 0x0006
  0110 ... 100... =
  ..... 0110 ... = TID: 6
  [..... 0110 ... = Priority: Voice (Voice) (6)]
  .... 0000 ... = EOSP: Service period
  .... 0000 ... = Ack Policy: Normal Ack (0x0)
  .... 0000 ... = Payload Type: MSDU
  > 0000 0000 ... = QAP PS Buffer State: 0x00
  > CCM parameters
  > Data (836 bytes)
  > Logical-Link Control
  > Internet Protocol Version 4, Src: 10.105.60.198, Dst: 10.105.60.158
  0100 ... = Version 4
  .... 0101 ... = Header Length: 20 bytes (15)
  > Differentiated Services Field: 0x00 (DSCP: EF PHB, CS0: Not-ECT1)
  1011 10... = Differentiated Services Codepoint: Expedited Forwarding (46)
  .... 0x00 ... = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  
```

AP上行鏈路交換機介面捕獲

一旦AP收到資料包，便會透過空中傳輸該資料包。要驗證使用者優先順序(UP)標籤，使用透過嗅探器AP進行的空中(OTA)捕獲。

AP已轉發UP值為6的幀。這可以確認AP已正確將DSCP值對映到相應的802.11 UP值(6)，該值對應於語音流量。

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

```

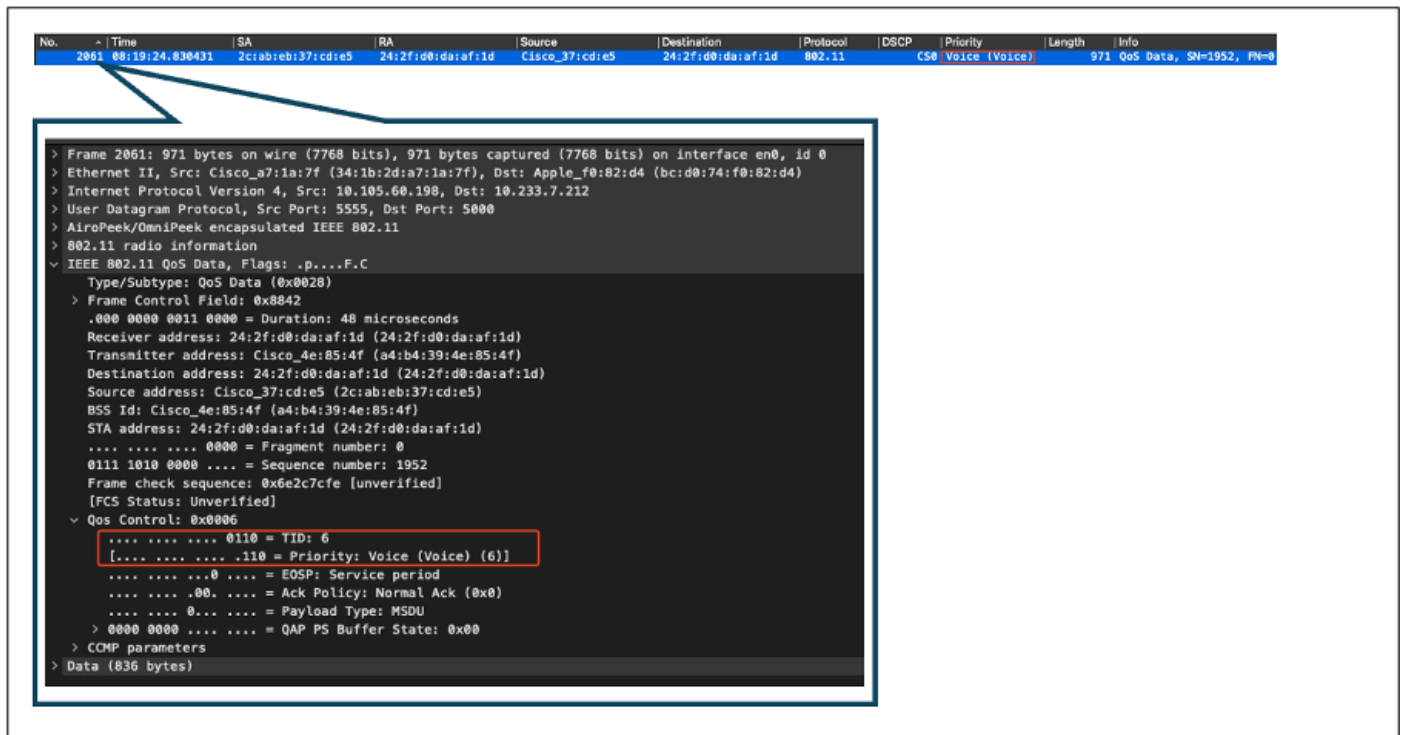
> Frame 2061: 971 bytes on wire (7768 bits), 971 bytes captured (7768 bits) on interface en0, id 0
> Ethernet II, Src: Cisco_a7:1a:7f (34:1b:2d:a7:1a:7f), Dst: Apple_f0:82:d4 (bc:d0:74:f0:82:d4)
> Internet Protocol Version 4, Src: 10.105.60.198, Dst: 10.233.7.212
> User Datagram Protocol, Src Port: 5555, 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
  0000 0000 0011 0000 = Duration: 48 microseconds
  Receiver address: 24:2f:d0:daf:1d (24:2f:d0:daf:1d)
  Transmitter address: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
  Destination address: 24:2f:d0:daf:1d (24:2f:d0:daf:1d)
  Source address: Cisco_37:cd:e5 (2c:ab:1b:37:cd:e5)
  BSS Id: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
  STA address: 24:2f:d0:daf:1d (24:2f:d0:daf: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
  [..... 0110 ... = Priority: Voice (Voice) (6)]
  .... 0000 ... = EOSP: Service period
  .... 0000 ... = Ack Policy: Normal Ack (0x0)
  .... 0000 ... = Payload Type: MSDU
  > 0000 0000 ... = QAP PS Buffer State: 0x00
  > CCM parameters
  > Data (836 bytes)
  
```

從AP到客戶端的OTA捕獲

在最後階段，無線PC接收的資料包。無線PC接收DSCP值為46的幀。

這表明DSCP標籤在從有線PC到無線PC的整個傳輸路徑中都保留。一致的DSCP值46可確認QoS策

略在下游方向正確應用和維護。



無線PC捕獲

測試場景2：上游QoS驗證

在此測試場景中，目的是驗證上行QoS配置。設定涉及無線PC使用DSCP 46向有線PC傳送UDP資料包。WLC配置了上行和下行方向的金屬「白金QoS」策略。

- 流量傳輸：

來源：無線PC

目的地：有線PC

流量型別：使用DSCP 46的UDP資料包

- WLC上的QoS策略配置：

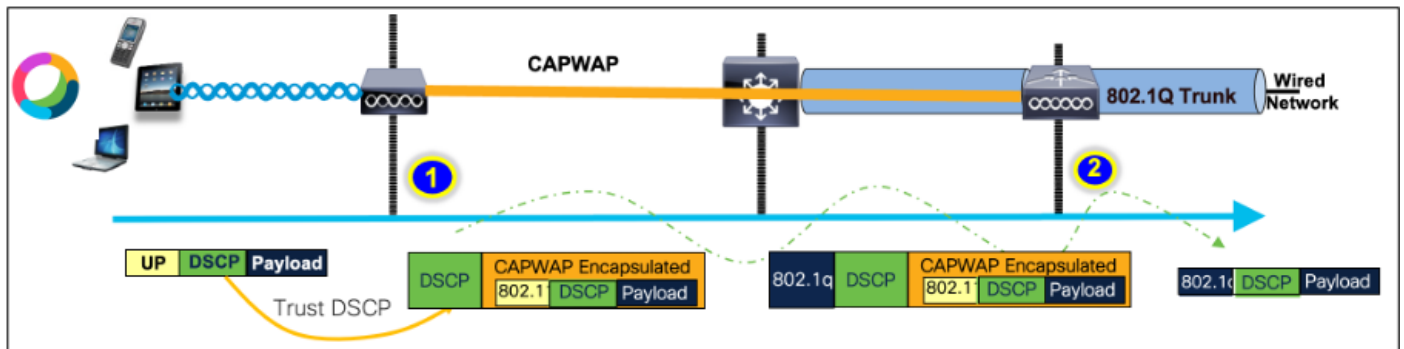
QoS配置檔案：白金QoS

方向：上游與下游

- 金屬QoS配置命令：

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

上行方向的邏輯拓撲和DSCP轉換：



邏輯拓撲和DSCP轉換-上游

從無線PC傳送到有線PC的資料包。此擷取是在無線PC上擷取的。

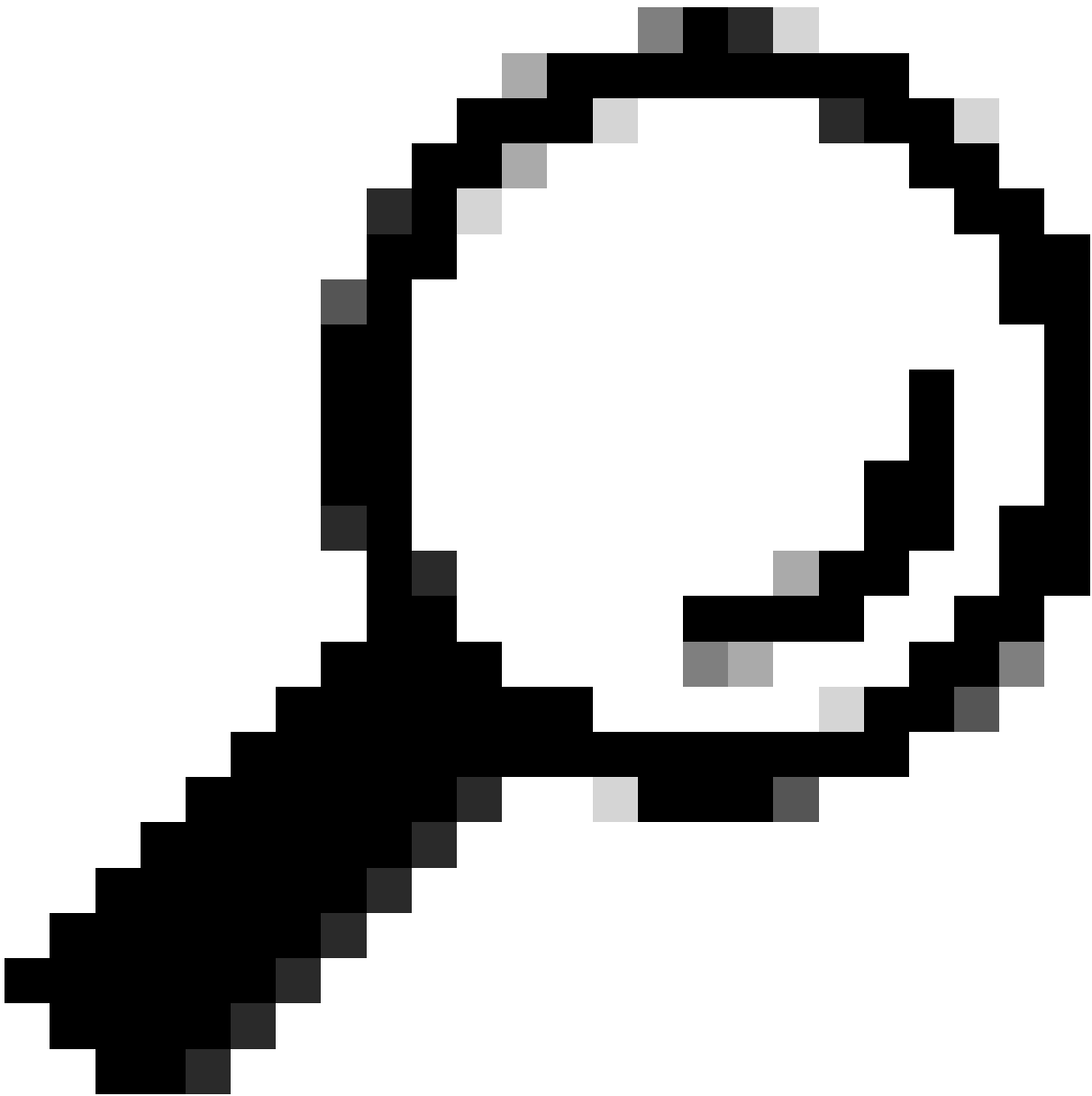
無線PC使用DSCP 46傳送UDP資料包。

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 - 5261 Len=6192

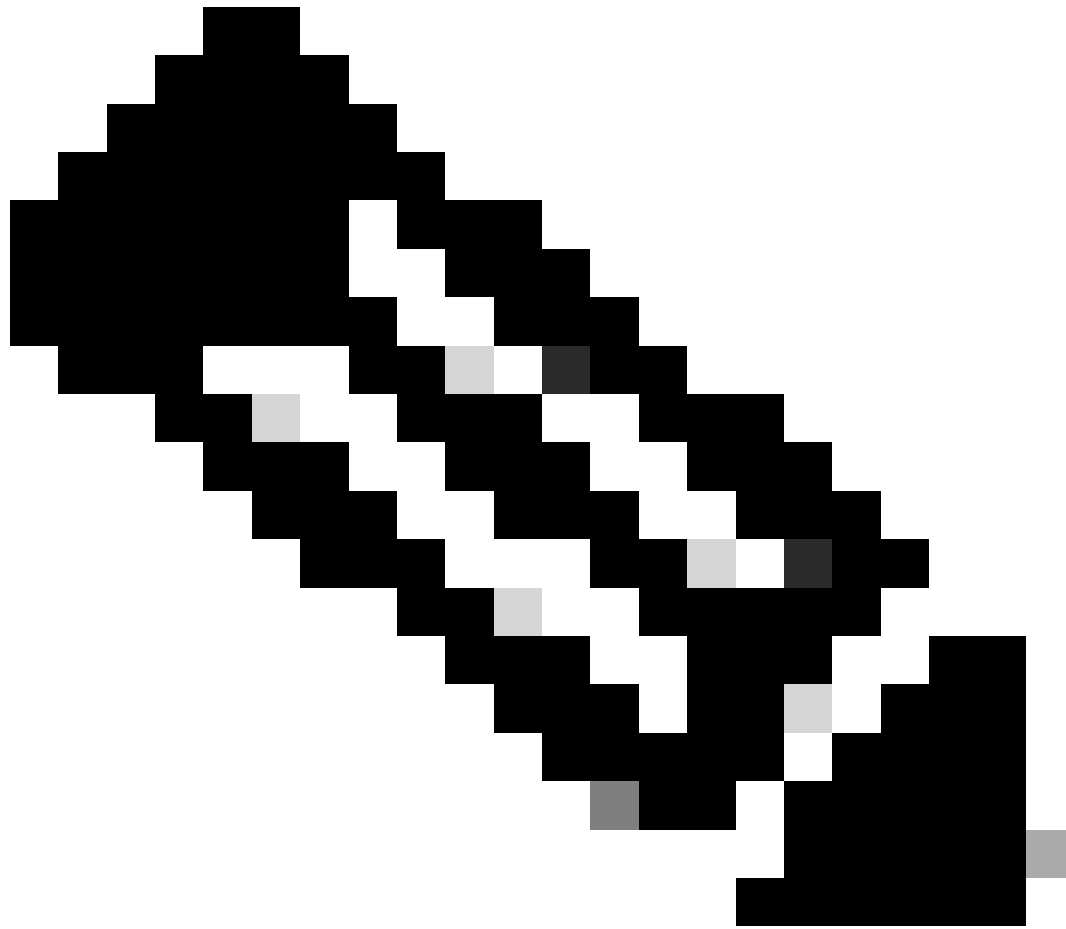
```
> Frame 241: 834 bytes on wire (6672 bits), 834 bytes captured (6672 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d), Dst: Cisco_37:cd:e5 (2c:ab:eb:37:cd:e5)
> Internet Protocol Version 4, Src: 192.168.30.13, Dst: 192.168.31.10
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > 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)
```

上行方向的無線PC捕獲

接下來，讓我們看一下從客戶端到AP的OTA捕獲。



提示：使用Windows無線PC透過DSCP 46傳送資料包時，Windows會將DSCP 46對映到使用者優先順序(UP)值5（影片）。因此，OTA捕獲將資料包顯示為影片流量(UP 5)。但是，如果解密資料包，則DSCP值仍為46。



注意：從版本17.4開始，Cisco 9800 WLC的預設行為是信任AP加入配置檔案中的DSCP值。這可以確保WLC保留並信任DSCP值46，從而防止任何與Windows DSCP到UP對映行為相關的問題。

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
- 101110.. 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到DSCP對映

分析從實驗室設定取得的加密空中傳輸(OTA)捕獲，以驗證上游QoS配置。

OTA捕獲顯示使用者優先順序(UP)值為5 (影片) 的資料包。雖然OTA捕獲顯示UP 5，但加密資料包中的DSCP值仍為46。

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

```

> Frame 5643: 1442 bytes on wire (11536 bits), 1442 bytes captured (11536 bits) on interface en0, id 0
> Ethernet II, Src: Cisco_a7:1a:7f (34:1b:2d:a7:1a:7f), Dst: Apple_f0:82:d4 (bc:d0:74:f0:82:d4)
> Internet Protocol Version 4, Src: 10.105.60.198, Dst: 10.233.7.212
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AiroPeek/OmniPeek encapsulated IEEE 802.11
> 802.11 radio information
  > IEEE 802.11 QoS Data, Flags: .p....TC
    Type/Subtype: QoS Data (0x0028)
    > Frame Control Field: 0x8841
      .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)]
      ..... 000 = 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在上游方向設定OTA

然後，分析AP上行鏈路埠上的資料包捕獲，確保資料包從AP移動到WLC時保留DSCP值。

- 外部CAPWAP層上的DSCP值保持在46。
- 在CAPWAP隧道中，DSCP值也保持在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)
```

上行方向的AP PpLink捕獲

封包從交換器到達時，WLC會進行擷取。

- 資料包到達WLC時，外部CAPWAP層的DSCP值為46。
- 在CAPWAP隧道中，DSCP值保持在46。

No.	Time	SA	RA	Source	Destination	Protocol	DSCP	Priority	Length	Info
516	10:53:22.989939			10.185.68.158	10.185.68.198	CAPWAP-Data	EF PHB		1582	CAPWAP-Data (Fragment ID: ...)
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
> 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: 10.185.68.158, Dst: 10.185.68.198
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: 258
Protocol: UDP (17)
Header Checksum: 0x35d3 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.185.68.158
Destination Address: 10.185.68.198
> 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)]
.... .... 00 .... = QoS bit 4: Bits 8-15 of QoS Control field are TXOP Duration Requested
.... .... 00 .... = Ack Policy: Normal Ack (0x0)
.... .... 00 .... = 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顯示來自AP的資料包

資料包在WLC上發生髮夾轉彎後，會將其傳送回上行鏈路交換機，目的地為有線PC。WLC轉發DSCP值為46的資料包。

No.	Time	SA	RA	Source	Destination	Protocol	DSCP	Priority	Length	Info
528	10:53:23.040939			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
> 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顯示傳送到有線PC的資料包

最後，分析有線PC上行鏈路上的資料包捕獲，確保資料包從WLC到達時保留DSCP值。

No.	Time	SA	RA	Source	Destination	Protocol	DSCP	Priority	Length	Info
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...

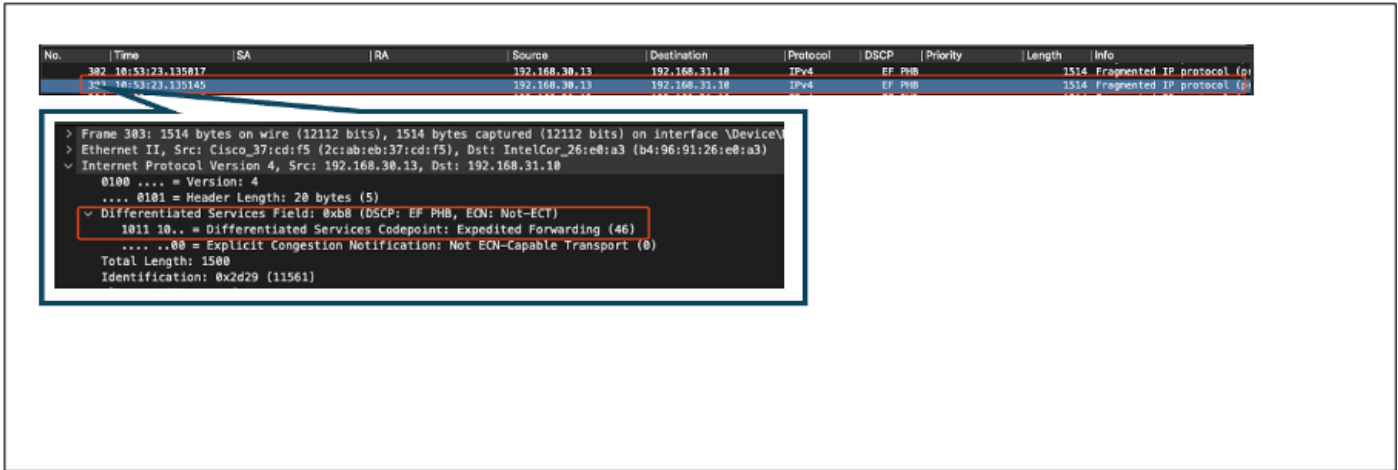
```

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

```

上行方向的有線PC上行鏈路交換機捕獲

在最後階段，分析有線PC收到的資料包，以確保資料包到達DSCP值為46的有線PC。



有線PC捕獲-上行方向

上游QoS測試已成功驗證從無線PC流向有線PC的流量的QoS配置。DSCP值46在整個傳輸路徑中保持一致可以確認QoS策略已正確應用和實施。

疑難排解

語音、影片和其他即時應用程式對網路效能問題尤為敏感，服務品質(QoS)的任何下降都可能產生顯著而有害的影響。當QoS資料包使用較低的DSCP值重新標籤時，對語音和影片的影響可能很大。

對語音的影響：

- 延遲增加：語音通訊要求低延遲，以確保通話自然流暢。較低的DSCP值會導致語音資料包延遲，從而導致會話明顯延遲。
- 抖動：資料包到達時間的變化（抖動）可能會中斷語音資料包的順利傳輸。這可能會導致音效波動或混音，使喇叭難以聽懂。
- 丟包：語音資料包對丟包高度敏感。即使少量資料包丟失也會導致丟失單詞或音節，從而導致通話品質差和誤會。
- 回聲和失真：延遲和抖動增加會導致回聲和音訊失真，進一步降低語音呼叫的品質。

對影片的影響：

- 延遲增加：影片通訊需要低延遲來維持音訊和影片流之間的同步。延遲增加會導致延遲，從而難以進行即時互動。
- 抖動：抖動會導致影片幀以無序或不規則的間隔到達，從而導致影片體驗抖動或抖動。
- 封包遺失：遺失的封包可能會導致遺失影格，進而造成視訊凍結或顯示假影。
- 降低視訊品質：降低DSCP值可能導致影片流的頻寬分配減少，從而導致解析度降低和視訊品質下降。這可能會使在影片中難以看到重要的詳細資訊。

方案1：中間交換機重寫DSCP標籤

在此故障排除方案中，研究了中間交換機在流量到達WLC時重寫DSCP標籤對流量的影響。要複製此配置，交換機配置為在有線PC上行鏈路介面上將DSCP 46標籤重寫為CS1。

資料包使用DSCP 46標籤從有線PC傳送。

```
> 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)
```

有線PC傳送帶有DSCP 46標籤的資料包

資料包到達WLC時的DSCP值為CS1 (DSCP 8)。從DSCP 46更改為DSCP 8會顯著降低資料包的優先順序。

```
> 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)
```

顯示CS1標籤的WLC EPC

在此步驟中，會分析WLC轉送到AP的封包。

- 外部CAPWAP報頭帶有CS1 (DSCP 8)標籤。
- 內部CAPWAP報頭還標籤有CS1 (DSCP 8)。
- 使用者優先順序(UP)值設定為BK (後台)。

```
> 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)]
  .... .... 00.. = EOSP: Service period
  .... .... 00.. = Ack Policy: Normal Ack (0x0)
  .... .... 0... = Payload Type: MSDU
  > 0000 0000 .... = QAP PS Buffer State: 0x00
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > 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

在CAPWAP流量中顯示CS1標籤的WLC EPC

資料包使用DSCP值CS1 (DSCP 8)到達無線PC。

```
> 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
```

顯示CS1標籤的無線PC捕獲

此場景演示了中間交換機上的錯誤配置如何會破壞QoS配置，從而導致高優先順序流量的效能降低

。由於DSCP重寫，最初標籤為高優先順序的語音資料包將被視為低優先順序流量。此場景強調了確保中間網路裝置正確保留QoS標籤以維持高優先順序流量所需服務品質的重要性。

方案2：AP鏈路交換機重寫DSCP標籤

在此場景中，研究連線到AP的中間交換機重寫DSCP標籤對流量的影響。

- 連線到AP的交換機被配置為在AP上行鏈路介面上將DSCP 46標籤重寫為不同的值CS1。
- 資料包使用DSCP標籤46從有線PC傳送。這可以確認在源位置使用DSCP 46正確標籤流量。

```
> 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)
  > 000 = Flags: 0x0
```

顯示DSCP 46的無線PC捕獲

封包從交換器到達時，WLC會進行擷取。

資料包到達WLC時，外部CAPWAP報頭DSCP值為CS1 (DSCP 且內部DSCP值為46。出現這種情況是因為中間交換機無法看到封裝在CAPWAP隧道內的流量。

WLC信任CAPWAP隧道內的DSCP標籤，並將流量轉發到內部DSCP標籤為46的有線PC。

```
> 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
```

顯示CAPWAP DSCP值的WLC EPC

資料包到達有線PC時的DSCP值為46。確認WLC正確轉發具有原始DSCP值46的資料包，同時保留高優先順序標籤。

```
> 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
```

有線PC接收了DSCP 46的資料包

雖然WLC轉發了DSCP標籤為46的流量，但必須瞭解的是，由於外部DSCP標籤被重寫為CS1 (DSCP 8)，因此從AP到WLC的流量被視為低優先順序。

在AP和WLC之間可以有多个交換機，如果為流量分配低優先順序，則流量可能會延遲到達WLC。這可能導致延遲增加、抖動和潛在的資料包丟失，從而降低語音等高優先順序流量的服務品質。

疑難排解提示

1. 驗證初始DSCP標籤：在源（例如，有線PC）捕獲資料包，以確保流量正確標籤為預期的DSCP值。
2. 檢查中間裝置配置：檢視所有中間交換機和路由器的配置，確保它們不會無意中重寫DSCP值。
3. 在關鍵點捕獲流量：
 1. 中間交換機之前和之後。
 2. 在WLC上。
 3. 位於目的地（例如，無線PC）。
4. 模擬流量場景：使用流量發生器或網路模擬工具建立不同型別的流量，並觀察無線網路如何處理QoS。
5. 請參閱9800最佳實踐文檔：檢視有關配置QoS和DSCP標籤的9800最佳實踐文檔。

組態驗證

<#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
```

結論

在整個網路中保持一致的QoS配置對於確保高優先順序流量（如語音和影片）獲得適當的服務和效能水準至關重要。必須定期驗證QoS配置，以確保所有網路裝置都符合預期的QoS策略。此驗證有助於辨識並糾正任何可能損害網路效能的錯誤配置或偏差。

參考資料

- [Cisco Catalyst 9800系列無線控制器的瞭解和故障排除](#)
- [Cisco Catalyst 9800系列配置最佳實踐](#)
- [Cisco Catalyst 9800系列無線控制器軟體配置指南, Cisco IOS® XE都柏林17.12.x](#)
- [無線區域網路語音\(VoWLAN\)疑難排解指南](#)
- [在Windows電腦上啟用DSCP QoS標籤](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。