

# 9800 WLC에서 무선 QoS 검증 및 문제 해결 구성

## 목차

---

[소개](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[설정](#)

[QoS 정책 대상](#)

[Auto QoS](#)

[자동 QoS CLI 컨피그레이션](#)

[모듈형 QoS CLI](#)

[MQS CLI 컨피그레이션](#)

[급속 QoS](#)

[급속 QoS CLI 컨피그레이션](#)

[패킷 캡처로 엔드 투 엔드 QoS 검증](#)

[네트워크 다이어그램](#)

[실습 구성 요소 및 패킷 캡처 포인트](#)

[테스트 시나리오 1: 다운스트림 QoS 검증](#)

[테스트 시나리오 2: 업스트림 QoS 검증](#)

[문제 해결](#)

[시나리오 1: 중간 스위치가 DSCP 마킹을 재작성합니다.](#)

[시나리오 2: AP 링크 스위치가 DSCP 마킹을 재작성합니다.](#)

[문제 해결 팁](#)

[컨피그레이션 확인](#)

[결론](#)

[참조](#)

---

## 소개

이 문서에서는 9800 WLC(Wireless LAN Controller)에서 무선 QoS(Quality of Service)를 구성, 검증 및 트러블슈팅하는 방법에 대해 설명합니다.

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- WLC: 17.12.03을 실행하는 C9800-40-K9
- 액세스 포인트(AP): C9120-AX-D
- 스위치: 17.03.05를 실행하는 C9300-48P
- 유선 및 무선 클라이언트: Windows 10

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

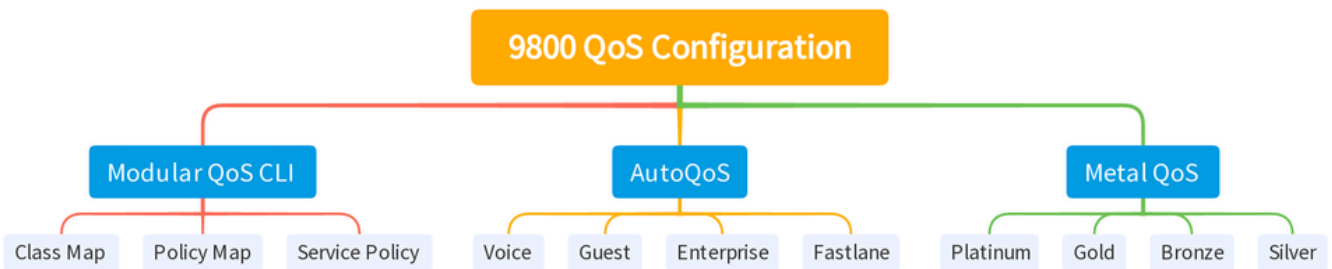
무선 QoS는 핵심 애플리케이션이 최적의 성능에 필요한 대역폭과 낮은 레이턴시를 수신하도록 보장하는 데 필수적입니다. 이 문서에서는 Cisco 무선 네트워크에서 QoS를 구성, 검증 및 트러블슈팅하는 데 필요한 포괄적인 가이드를 제공합니다.

이 문서에서는 독자가 무선 및 유선 QoS 원칙에 대해 기본적으로 이해하고 있다고 가정합니다. 또한 독자들이 Cisco WLC 및 AP를 구성 및 관리하는 데 능숙할 것으로 예상됩니다.

## 설정

이 섹션에서는 9800 무선 컨트롤러의 QoS 컨피그레이션에 대해 살펴봅니다. 이러한 컨피그레이션을 활용하면 중요한 애플리케이션에서 필요한 대역폭과 낮은 레이턴시를 수신하도록 보장하여 전체적인 네트워크 성능을 최적화할 수 있습니다.

9800 WLC QoS 컨피그레이션을 크게 세 가지 범주로 나눌 수 있습니다.



9800 WLC QOS 컨피그레이션 요약

이 문서는 다음 섹션에서 각 섹션을 하나씩 살펴봅니다.

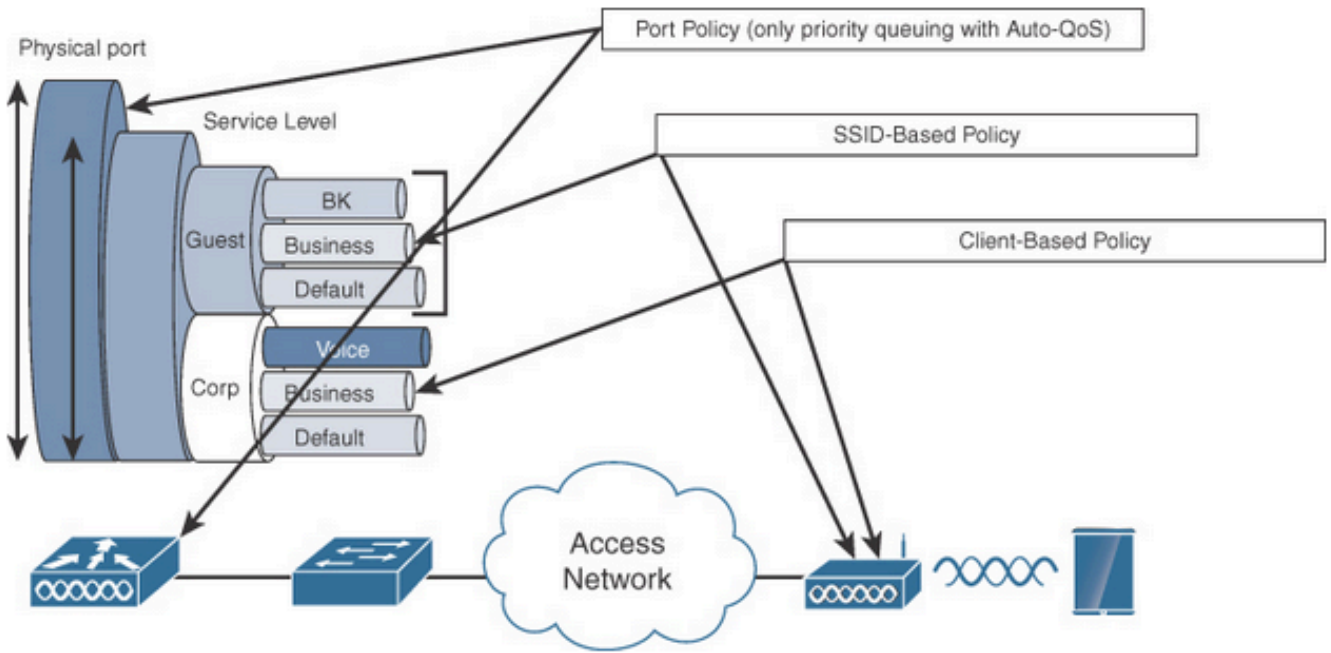
---

참고: 이 문서에서는 로컬 모드의 AP를 중심으로 다룹니다. Flexconnect 모드의 AP는 논의되지 않습니다.

---

## QoS 정책 대상

정책 대상은 QoS 정책을 적용할 수 있는 컨피그레이션 구성입니다. Catalyst 9800에서 QoS 구현은 모듈식이며 유연합니다. 사용자는 SSID, 클라이언트 및 포트 레벨의 세 가지 다른 타겟에서 정책을 구성할 수 있습니다.



QoS 정책 대상

SSID 정책은 SSID당 AP별로 적용할 수 있습니다. SSID에서 정책 및 마킹 정책을 구성할 수 있습니다.

클라이언트 정책은 인그레스(ingress) 및 이그레스(egress) 방향으로 적용할 수 있습니다. 클라이언트에 대한 정책 및 마킹 정책을 구성할 수 있습니다. AAA 재정의도 지원됩니다.

포트 기반 QoS 정책은 물리적 또는 논리적 포트에서 적용할 수 있습니다.

Auto QoS

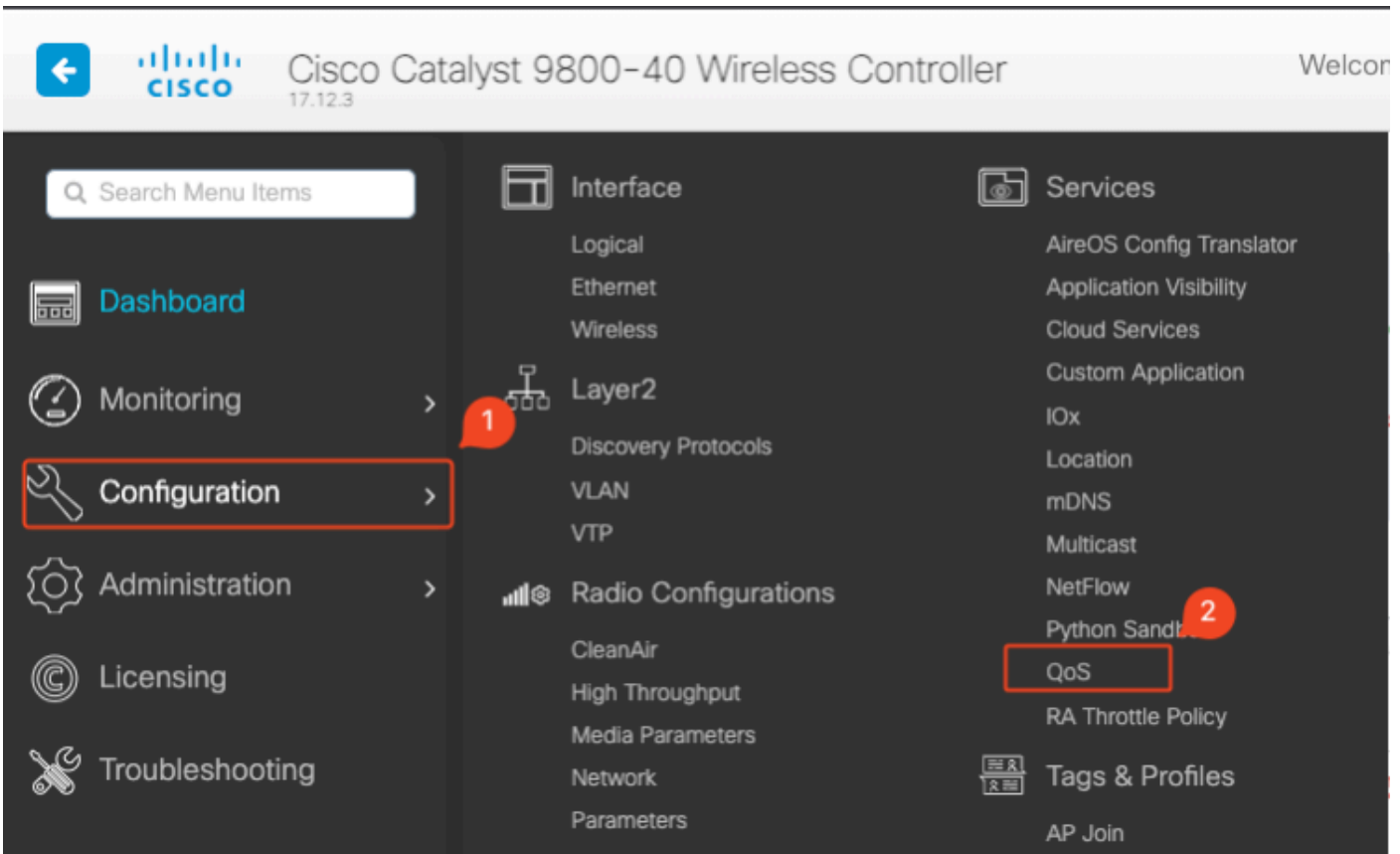
Wireless Auto QoS는 무선 QoS 기능의 구축을 자동화합니다. 여기에는 서로 다른 트래픽 흐름의 우선 순위를 지정하기 위해 관리자가 추가로 수정할 수 있는 사전 정의된 프로필 집합이 있습니다. Auto-QoS는 트래픽을 매칭하고 매칭된 각 패킷을 QoS 그룹에 할당합니다. 그러면 출력 정책 맵에서 특정 QoS 그룹을 우선순위 큐를 비롯한 특정 큐에 넣을 수 있습니다.

모드로 들어갑니다	클라이언트 인그레스	클라이언트 이그레스	BSSID 인그레스	BSSID 이그레스	포트 인그레스	포트 이그레스	라디오
음성	해당 없음	해당 없음	Platinum-up	백금	해당 없음	AutoQos 4.0-wlan-Port-Output-Policy	ACM 켜기
게스트	해당	해당	AutoQos-4.0-wlan-	AutoQos-4.0-wlan-	해당	AutoQos 4.0-	

	없음	없음	GT-SSID-Input-Policy	GT-SSID-Output-Policy	없음	wlan-Port-Output-Policy	
패스트 레인	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음	AutoQos 4.0-wlan-Port-Output-Policy	edca 매개 변수 fastlane
엔터프라이즈 avc	해당 없음	해당 없음	AutoQos-4.0-wlan-ET-SSID-Input-AVC-Policy	AutoQos-4.0-wlan-ET-SSID-Output-Policy	해당 없음	AutoQos 4.0-wlan-Port-Output-Policy	

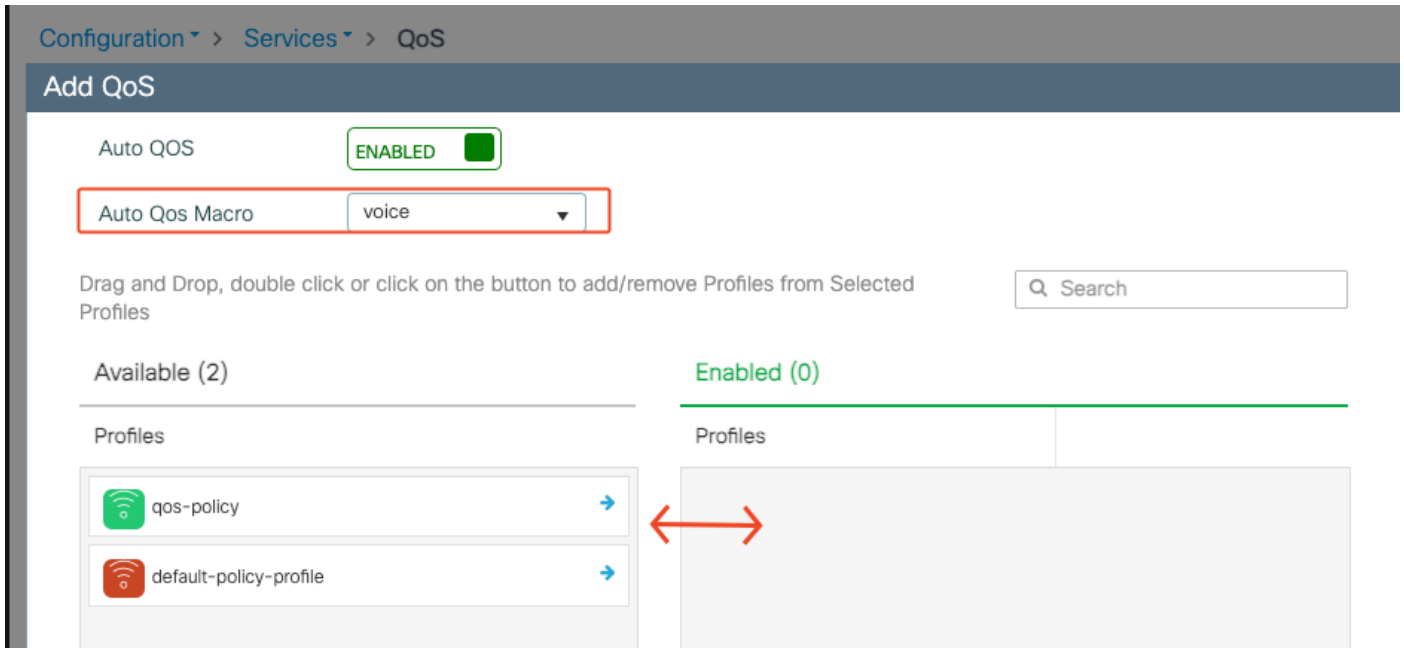
이 표에서는 자동 QoS 프로파일이 적용될 때 발생하는 컨피그레이션 변경 사항을 보여 줍니다.

Auto QoS를 구성하려면 Configuration(컨피그레이션) > QoS로 이동합니다



QoS 워크플로

Add(추가)를 클릭하고 Auto QoS를 enabled(활성화됨)로 설정합니다. 목록에서 적절한 Auto QoS 매크로를 선택합니다. 이 예에서는 음성 트래픽의 우선 순위를 지정하는 음성 매크로가 사용됩니다



AutoQoS 음성 매핑

매크로가 활성화되면 정책에 연결해야 하는 정책을 선택합니다.

## 자동 QoS CLI 컨피그레이션

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

이제 자동 QoS가 활성화되었으므로 변경 사항을 확인할 수 있습니다. 이 섹션에는 음성에 대한 컨피그레이션 변경 사항이 나열됩니다.

```
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
```

## 모듈형 QoS CLI

MQC를 사용하면 트래픽 클래스를 정의하고, 트래픽 정책(정책 맵)을 생성하고, 트래픽 정책을 인터페이스에 연결할 수 있습니다. 트래픽 정책에는 트래픽 클래스에 적용되는 QoS 기능이 포함되어 있습니다.

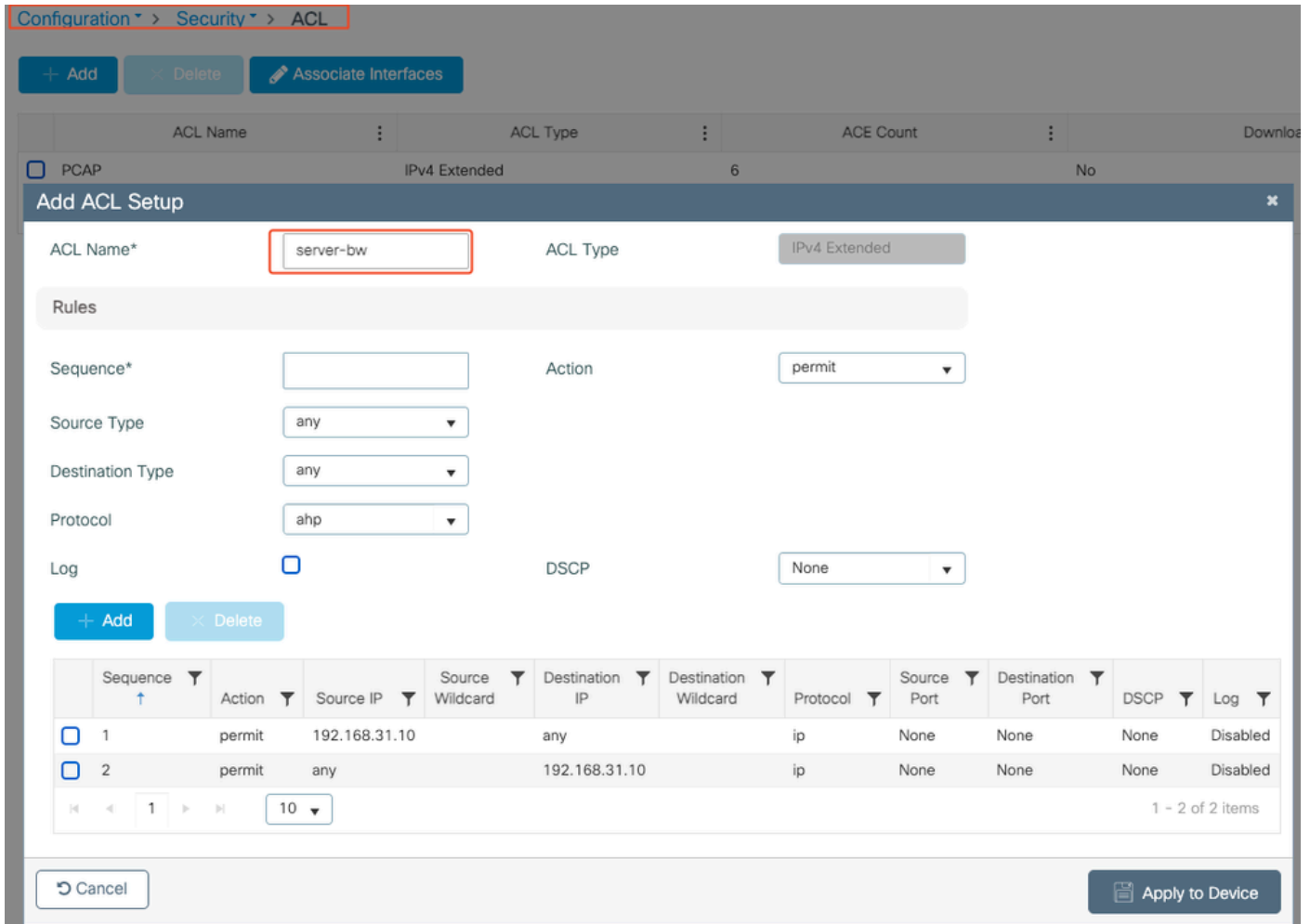


MQS CLI 워크플로

이 예에서는 ACL(Access Control List)을 사용하여 트래픽을 분류하고 대역폭 제한을 적용하는 방법을 보여 줍니다.

관리할 특정 트래픽을 식별하고 분류하기 위해 ACL을 생성합니다. 이는 IP 주소, 프로토콜, 포트 등의 기준에 따라 트래픽과 매칭하는 규칙을 정의하여 수행할 수 있습니다.

Configuration(컨피그레이션) > Security(보안) > ACL로 이동하고 ACL을 추가합니다.



#### ACL 컨피그레이션

ACL을 사용하여 트래픽이 분류되면 이 트래픽에 할당된 대역폭의 양을 제어하도록 대역폭 제한을 구성합니다.

Configuration(컨피그레이션) > Services(서비스) > QoS 및 QoS policy(QoS 정책)로 이동합니다. ACL을 정책 내에 연결하고 kbps 단위로 경찰을 적용합니다.

아래로 스크롤하여 QoS를 적용할 정책 프로필을 선택합니다. SSID 또는 클라이언트 모두에 대해 인그레스/이그레스 방향으로 정책을 선택할 수 있습니다.



### Add QoS

Auto QoS  DISABLED

Policy Name\*

Description

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

+ Add Class-Maps

× Delete

AVC/User Defined

Match  Any  All

Match Type

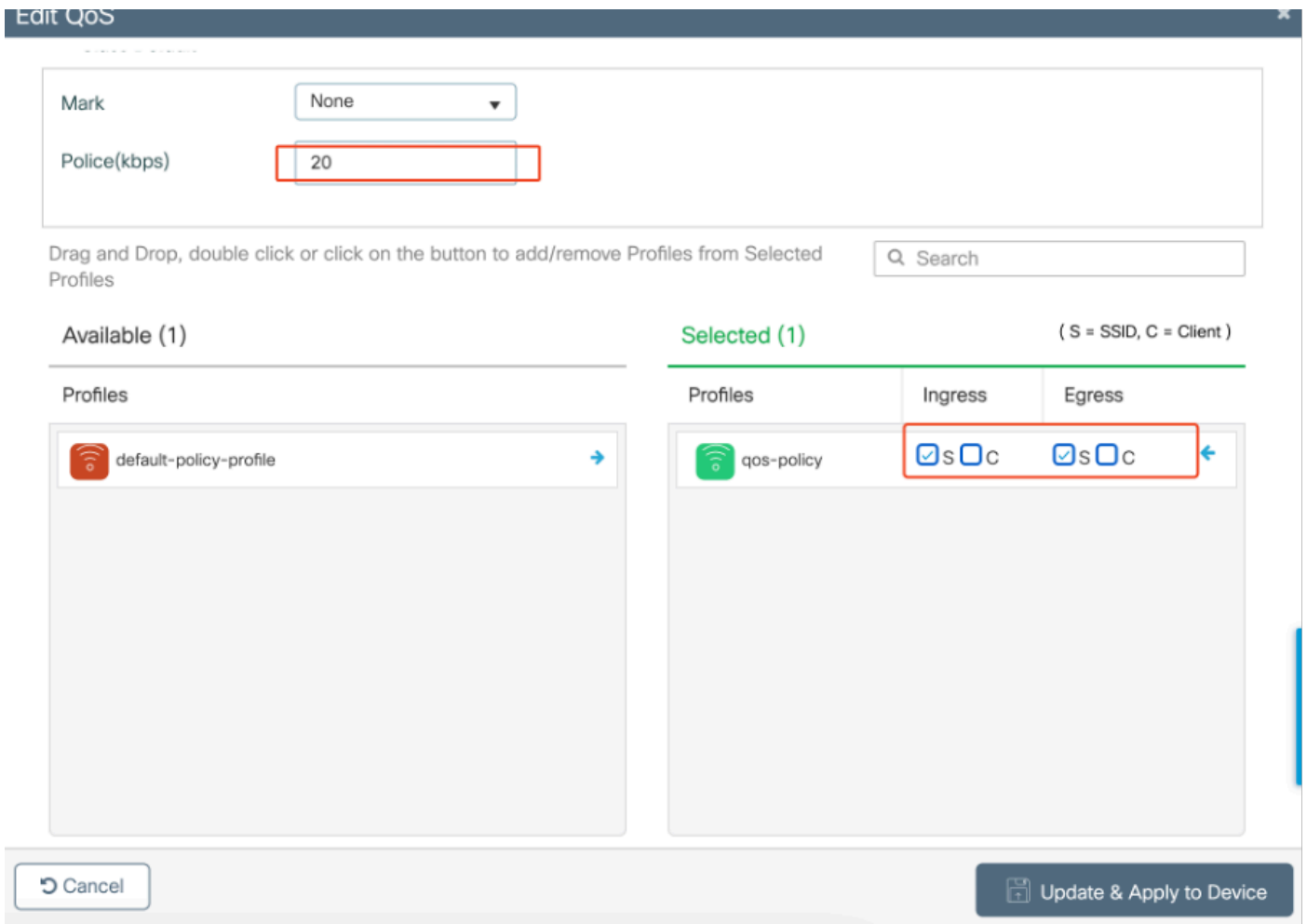
Match Value\*

Mark Type

Drop

Police(kbps)

MQS 정책



MQS 프로필

## MQS CLI 컨피그레이션

```

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

```

## 금속 QoS

이러한 QoS 프로파일의 주된 목적은 무선 네트워크에서 허용되는 최대 DSCP(Differentiated Services Code Point) 값을 제한하여 802.11 UP(User Priority) 값을 제어하는 것입니다.

Cisco 9800 WLC(Wireless LAN Controller)에서 금속 QoS 프로파일은 미리 정의되어 있으며 구성할 수 없습니다. 그러나 QoS 정책을 시행하기 위해 이러한 프로파일을 특정 SSID 또는 클라이언트에 적용할 수 있습니다.

사용 가능한 4가지 금속 QoS 프로파일 있습니다.

Qos 프로파일	최대 DSCP
브론즈	8
실버	0
골드	34
플래티넘	46

Cisco 9800 WLC에서 금속 QoS를 구성하려면

Configuration(컨피그레이션) > Policy(정책) > QoS & AVC로 이동합니다.

- 원하는 금속 QoS 프로파일(Platinum, Gold, Silver 또는 Bronze)을 선택합니다.
- 선택한 프로파일을 대상 SSID 또는 클라이언트에 적용합니다.

⚠ 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**

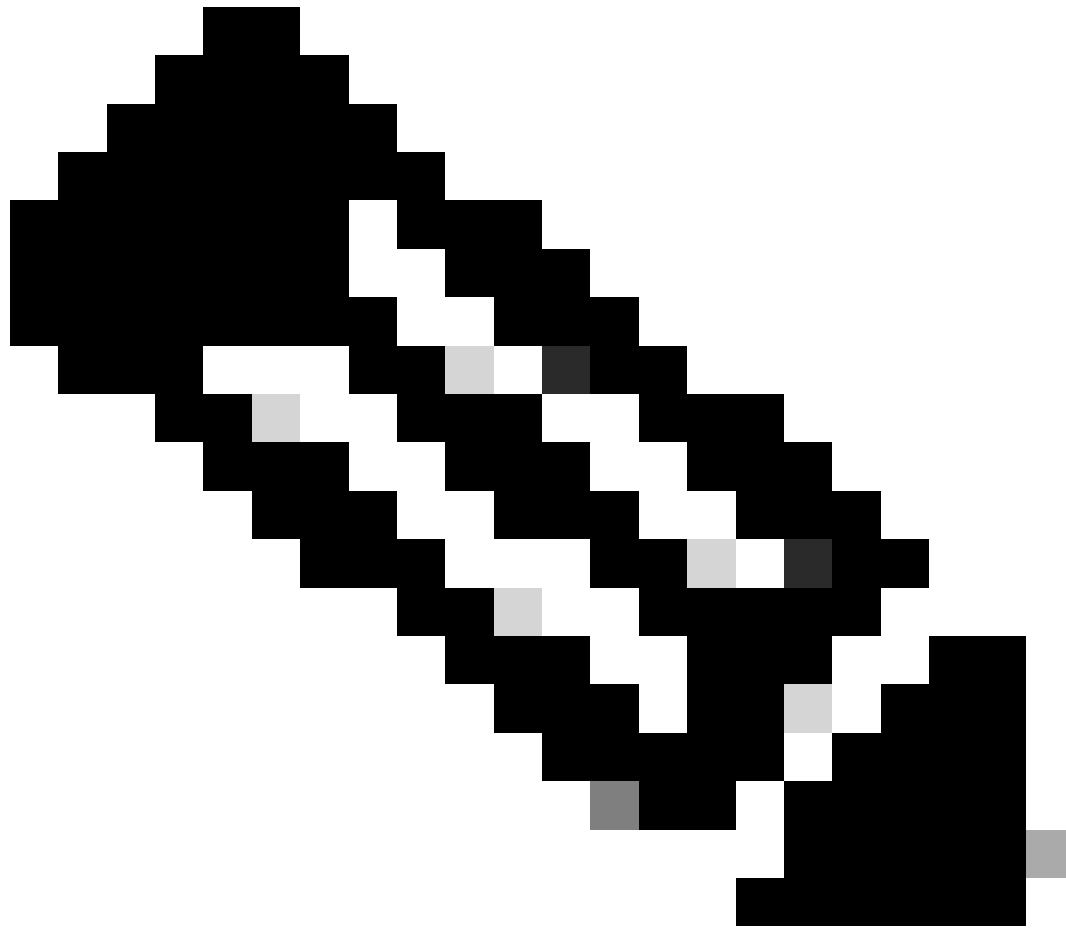
Egress Search or Select

Ingress Search or Select

금속 QoS 프로파일

### 금속 QoS CLI 컨피그레이션

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



참고: 사용자별 및 SSID 대역폭 계약은 Metal QoS가 아닌 QoS 정책을 통해 구성할 수 있습니다. 9800에서 일치하지 않는 트래픽은 기본 클래스로 이동합니다.

---

---

참고: GUI에서는 SSID당 Metal QoS만 설정할 수 있습니다. CLI에서는 클라이언트 대상에  
서 구성할 수도 있습니다.

---

## 패킷 캡처로 엔드 투 엔드 QoS 검증

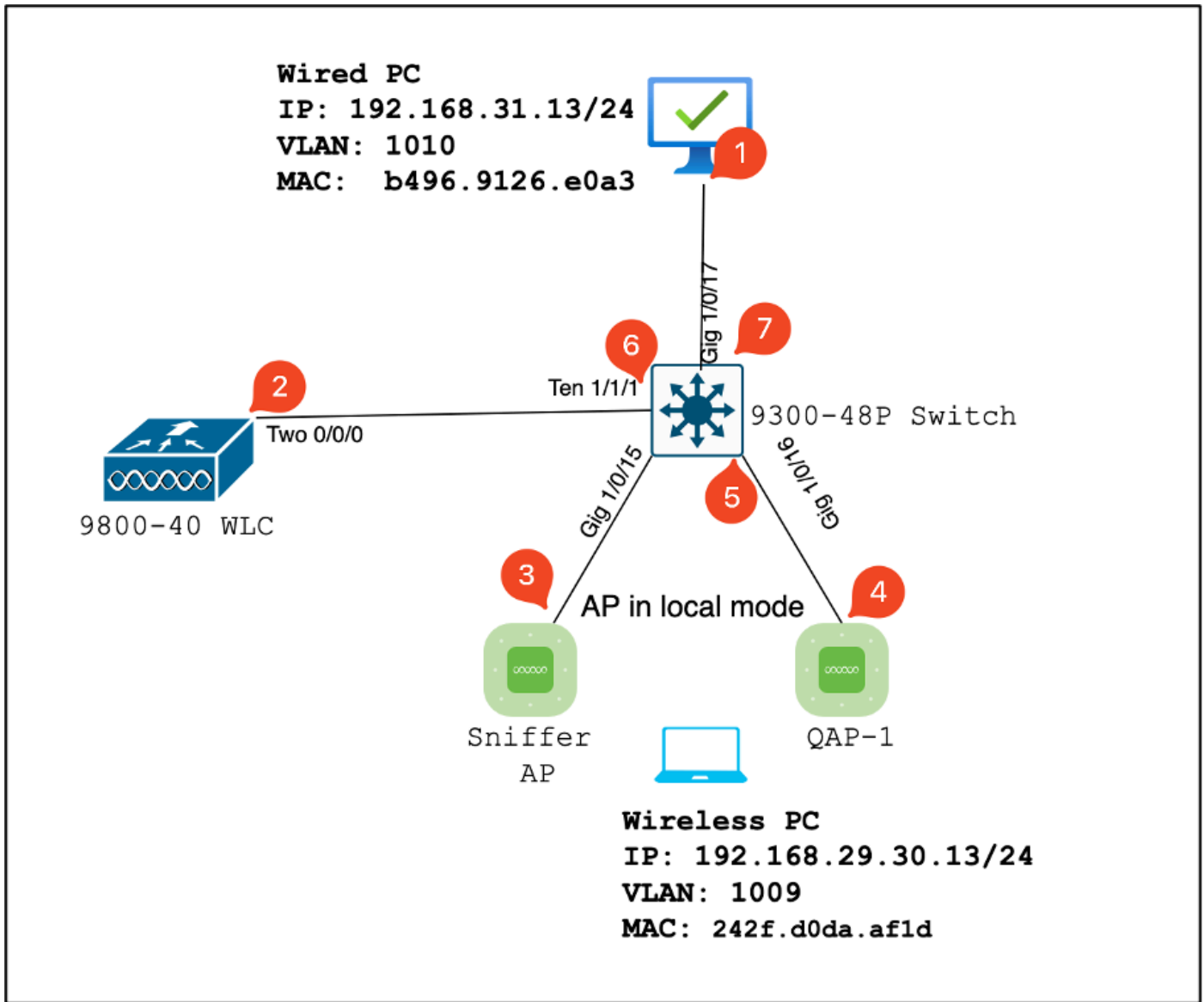
이제 QoS 컨피그레이션이 완료되었으므로 QoS 패킷을 검토하고 QoS 정책이 처음부터 끝까지 올바르게 작동하는지 검증해야 합니다. 이는 패킷 캡처 및 분석을 통해 달성할 수 있습니다.

QoS 컨피그레이션을 복제하고 검증하기 위해 소규모 랩 환경이 사용됩니다. 이 실습에는 다음 구성 요소가 포함됩니다.

- WLC
- AP
- OTA를 가져갈 스니퍼 AP
- 유선 PC
- 스위치

이 모든 구성 요소는 실습 환경 내에서 동일한 스위치에 연결됩니다. 이 다이어그램에서 강조 표시된 숫자는 패킷 캡처가 트래픽 흐름을 모니터링하고 분석할 수 있는 지점을 나타냅니다.

### 네트워크 다이어그램



LAB 토폴로지

### 실습 구성 요소 및 패킷 캡처 포인트

WLC:

- 무선 네트워크에 대한 QoS 정책 및 컨피그레이션을 관리합니다.
- 패킷 캡처 포인트: WLC, AP 및 스위치 간의 트래픽을 캡처합니다.

AP:

- 클라이언트에 무선 연결을 제공하고 QoS 정책을 적용합니다.
- 패킷 캡처 포인트: AP와 스위치 간의 트래픽을 캡처합니다.

### 스니퍼 AP:

- 무선 트래픽을 캡처하기 위한 전용 디바이스 역할을 합니다.
- 패킷 캡처 포인트: AP와 무선 클라이언트 간의 무선 트래픽을 캡처합니다.

### 유선 PC:

- 스위치에 연결되어 유선 트래픽을 시뮬레이션하고 엔드 투 엔드 QoS를 검증합니다.
- 패킷 캡처 포인트: 유선 링크를 통해 전송 및 수신된 QoS 패킷을 캡처합니다.

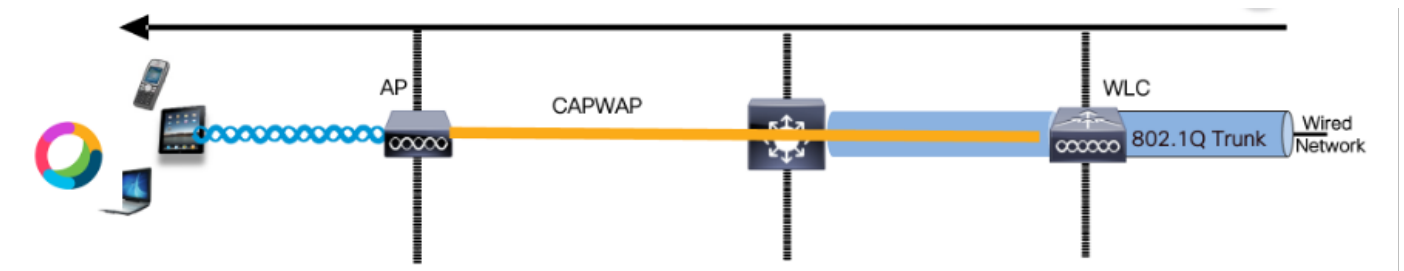
### 무선 PC:

- 무선 트래픽을 시뮬레이션하고 엔드 투 엔드 QoS를 검증하기 위해 WLAN에 연결되었습니다.
- 패킷 캡처 포인트: 무선 링크를 통해 전송 및 수신된 QoS 패킷을 캡처합니다.

### 스위치:

- 모든 랩 구성 요소를 상호 연결하고 트래픽 흐름을 원활하게 하는 중앙 디바이스입니다.
- 패킷 캡처 포인트: 다양한 스위치 포트에서 트래픽을 캡처하여 적절한 QoS 시행을 검증합니다.

논리적으로 LAB 토폴로지는 이렇게 그릴 수 있습니다.



논리적 LAB 토폴로지

QoS 컨피그레이션을 테스트하고 검증하기 위해 iPerf를 사용하여 클라이언트와 서버 간 트래픽을 생성합니다. 이 명령은 QoS 테스트의 방향에 따라 서버 및 클라이언트 역할이 상호 변경되는 iPerf 통신을 용이하게 하는 데 사용됩니다.

### 테스트 시나리오 1: 다운스트림 QoS 검증

다운스트림 QoS 컨피그레이션을 검증하기 위한 목적입니다. 이 설정에는 유선 PC가 DSCP 46으로 패킷을 무선 PC로 전송하는 작업이 포함됩니다.

WLC(Wireless LAN Controller)는 다운스트림 및 업스트림 방향 모두에 대해 메달 "플래티넘 QoS" 정책으로 구성됩니다.

### 테스트 설정:

- 트래픽 흐름:

출처: 유선 PC



대상: 무선 PC

트래픽 유형: DSCP가 있는 UDP 패킷 46

- WLC의 QoS 정책 구성:

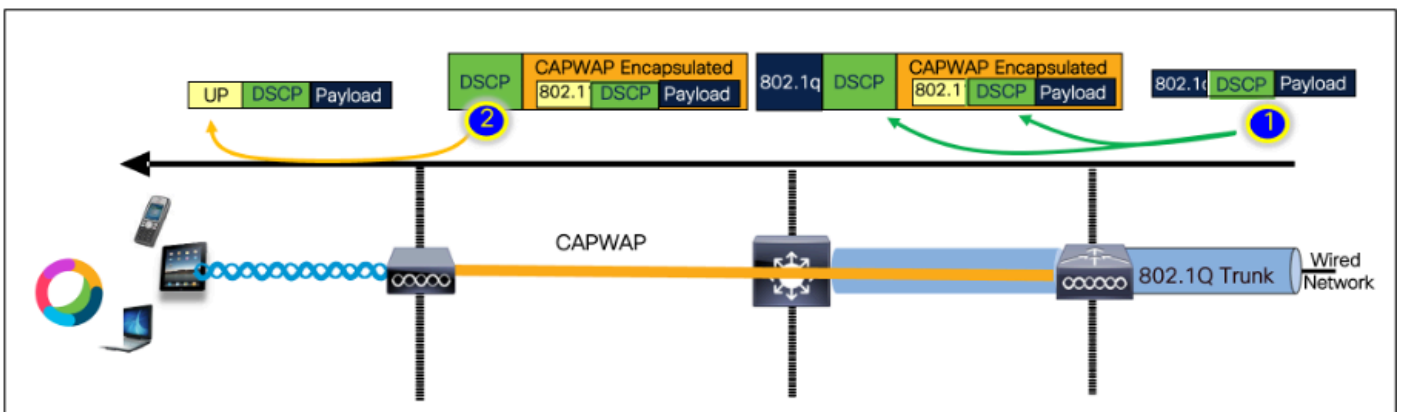
QoS 프로파일: 금속 QoS - 플래티넘 QoS

방향: 다운스트림 및 업스트림 모두

- 금속 QoS 컨피그레이션 명령:

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

### 논리적 토폴로지 및 다운스트림 방향의 DSCP 대화



### DSCP 대화 포인트

유선 PC에서 가져온 패킷 캡처. 그러면 유선 PC가 UDP 패킷을 지정된 목적지 IP 192.168.10.13에 올바른 DSCP 마킹을 46으로 보내는 것을 확인합니다.

```
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-3F5F-4837-BEC3-2A26715EDCA3}, id 0  
> Ethernet II, Src: IntelCor_26:e8:a3 (04:06:01:26:e8:a3), Dst: Cisco_37:cd:fs (2c:ab:eb:37:cd:fs)  
> Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13  
  8190 ... = Version: 4  
  ... = 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)
```

### 유선 PC 캡처 - 다운스트림 방향

다음으로 유선 PC에 연결된 업링크 스위치에서 캡처한 패킷을 살펴보자. 스위치는 DSCP 태그를 신뢰하며 DSCP 값은 46으로 변경되지 않습니다.

참고: Catalyst 9000 Series의 스위치 포트는 기본적으로 신뢰할 수 있는 상태로 설정됩니다.

The image displays a network traffic capture analysis. The top part shows a list of captured packets with the following details:

Packet No.	Time	Source IP	Destination IP	Protocol	Priority	Length	Fragmented
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	08:19:24.605918	192.168.31.10	192.168.30.13	IPv4	EF PHB	1514	Fragmented IP protocol
1008	08:19:24.605918	192.168.31.10	192.168.30.13	IPv4	EF PHB	1514	Fragmented IP protocol

The packet at 1006 is highlighted with a red box. A callout box provides a detailed view of this packet's header:

```
> Frame 1006: 834 bytes on wire (6672 bits), 834 bytes captured (6672 bits) on interface \Device\NPF_{4083E30A-3F5F-4837-BEC3-2A26715EDCA}, id 0
> Ethernet II, Src: IntelCor_26:e8:a3 (04:96:91:26:e8:a3), Dst: Cisco_37:cd:f5 (2c:a8:eb:37:cd:f5)
> Internet Protocol Version 4, Src: 192.168.31.10, Dst: 192.168.30.13
  8100 .... = Version: 4
  .... 8101 = 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)
```

유선 PC 업링크 인터페이스 캡처

EPC를 사용하여 가져온 WLC의 패킷 캡처를 조사하면 패킷이 업링크 스위치에서 동일한 DSCP 태그 46으로 도착합니다. 이렇게 하면 패킷이 WLC에 도달할 때 DSCP 마킹이 보존됩니다.

```

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-2AC20715EDCA}, id 0
> Ethernet II, Src: IntelCor_25:c8:a3 (04:95:91:25:c8:a3), 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 다운스트림 방향

WLC가 CAPWAP 터널 내의 AP로 패킷을 전송할 때 WLC가 해당 컨피그레이션을 기반으로 DSCP를 수정할 수 있는 중요한 교집합입니다. 명확성을 위해 번호가 매겨진 포인트로 강조 표시된 패킷 캡처를 살펴보겠습니다.

- CAPWAP 외부 레이어: CAPWAP 터널의 외부 레이어는 DSCP 태그를 스위치 끝에서 받은 값인 46으로 표시합니다.
- 802.11 UP Value Inside CAPWAP: CAPWAP 터널 WLC 내에서는 DSCP 46을 음성 트래픽에 해당하는 802.11 UP(User Priority) 6에 매핑합니다.
- CAPWAP 내 DSCP 값: Cisco 9800 WLC는 트러스트 DSCP 모델과 함께 작동하므로 CAPWAP 터널 내 DSCP 값은 외부 DSCP 레이어와 동일하게 46으로 유지됩니다.

```

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      10.105.60.198      10.105.60.158      CAPWAP-Data      EF PHB      1478 CAPWAP-Data (Fragment)
2738 08:19:24.716958      192.168.31.10      192.168.30.13      IPv4      EF PHB      164 Fragmented IP protocol

```

```

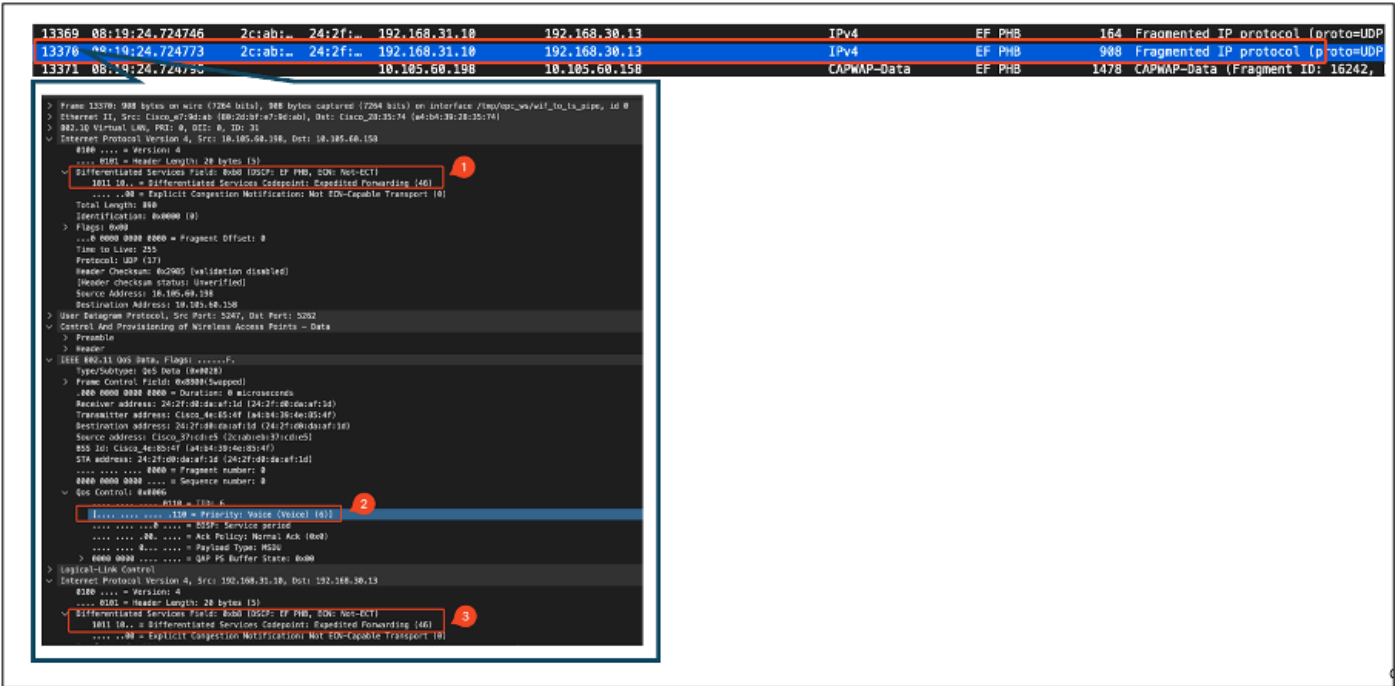
> Frame 2736: 988 bytes on wire (7264 bits), 988 bytes captured (7264 bits)
> Ethernet II, Src: Cisco_c7:9d:a8 (88:2d:3f:fe:79:d8), Dst: Cisco_28:35:74 (a4:b4:39:28:35:74)
> 802.11 Virtual LAN, PRI: 0, DEI: 0, ID: 31
  > Internet Protocol Version 4, Src: 10.105.60.198, Dst: 10.105.60.158
    0100 ... = Version: 4
    ... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 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: 890
    Identification: 0x0000 (0)
  > Flags: 0x00
  ... 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: 0xb800 (Swapped)
    0000 0000 0000 = Duration: 0 microseconds
    Receiver address: 24:2f:d8:d8:af:1d (24:2f:d8:d8:af:1d)
    Transmitter address: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
    Destination address: 24:2f:d8:d8:af:1d (24:2f:d8:d8:af:1d)
    Source address: Cisco_37:cd:e5 (2c:ab:cb:37:cd:e5)
    BSS Id: Cisco_4e:85:4f (a4:b4:39:4e:85:4f)
    STA address: 24:2f:d8:d8:af:1d (24:2f:d8:d8:af:1d)
    .... 0000 = Fragment number: 0
    0000 0000 0000 ... = Sequence number: 0
  > QoS Control: 0x0006
    .... 0110 = TID: 6
    [.... 0110 = Priority: Voice (Voice) (6)]
    .... 0000 = BOSP: 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: 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 표시

그런 다음 AP 업링크 스위치 포트에서 동일한 패킷을 확인합니다.

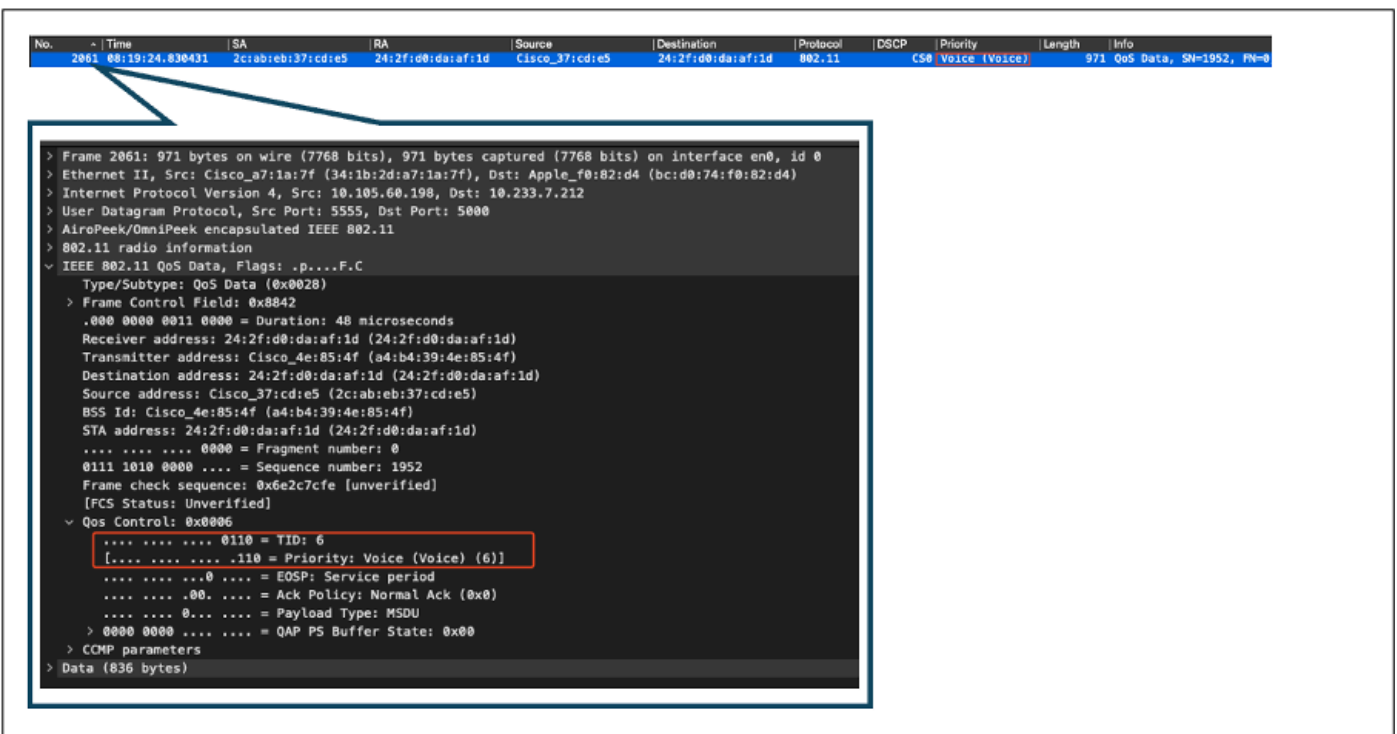
외부 CAPWAP 레이어의 DSCP 값은 46으로 유지됩니다. 설명을 위해 내부 CAPWAP 트래픽이 강조 표시되어 태깅을 표시합니다.



### AP 업링크 스위치 인터페이스 캡처

AP가 패킷을 수신하면 패킷을 공중을 통해 전송합니다. UP(User Priority) 태깅을 확인하기 위해 스니퍼 AP로 촬영한 OTA(Over-the-Air) 캡처가 사용됩니다.

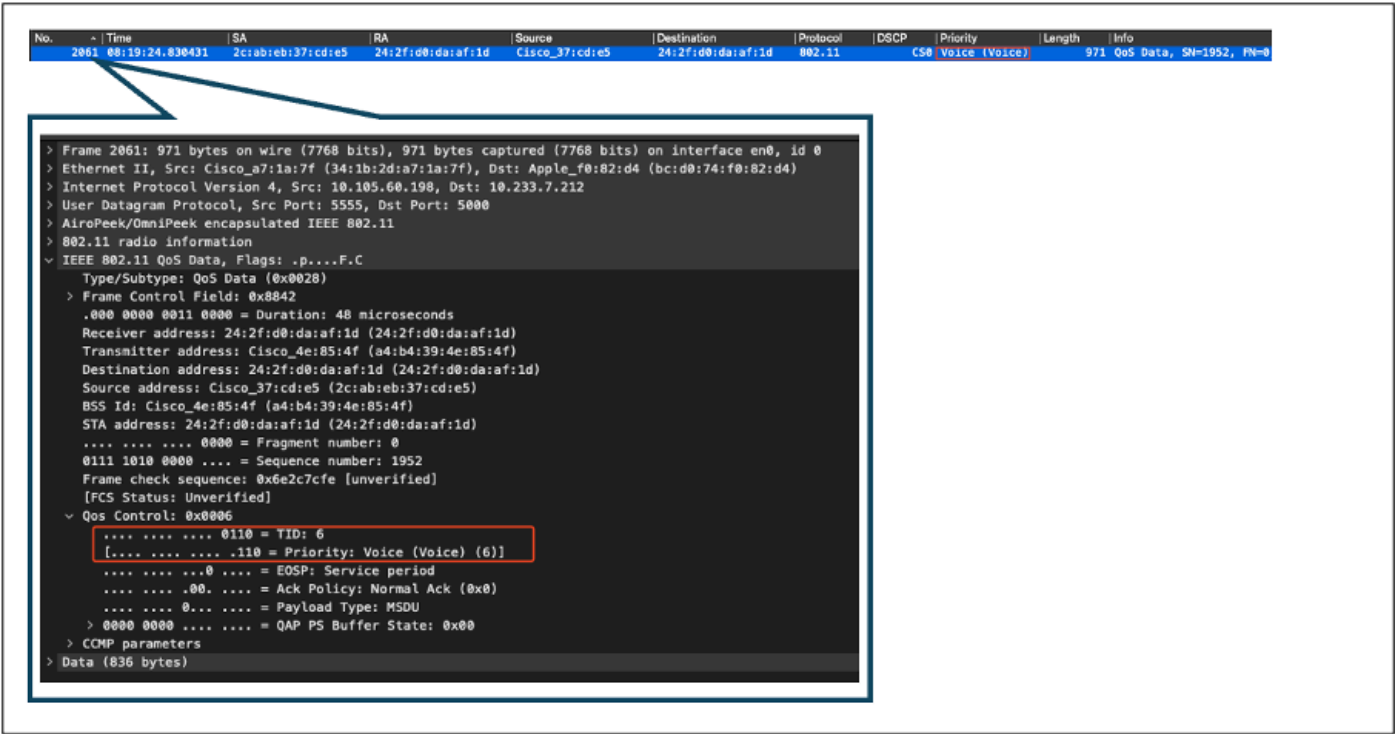
AP가 UP 값 6으로 프레임을 전달했습니다. 그러면 AP가 DSCP 값을 음성 트래픽에 해당하는 적절한 802.11 UP 값(6)에 올바르게 매핑합니다.



### AP에서 클라이언트로 OTA 캡처

마지막 단계에서 무선 PC에서 패킷을 수신했습니다. 무선 PC는 DSCP 값이 46인 프레임을 수신합니다.

이는 유선 PC부터 무선 PC까지 전체 전송경로에 걸쳐 DSCP 마킹이 보존됨을 나타낸다. 일관된 DSCP 값 46은 QoS 정책이 다운스트림 방향으로 올바르게 적용되고 유지되는지 확인합니다.



```
No. 2061 | Time 00:19:24.830431 | SA 2c:ab:eb:37:cd:e5 | RA 24:2f:d0:da:af:1d | Source Cisco_37:cd:e5 | Destination 24:2f:d0:da:af:1d | Protocol 802.11 | DSCP CS0 | Priority Voice (Voice) | Length 971 | Info QoS Data, SI=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: 10.105.60.190, 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)]
      .... .. 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)
```

무선 PC 캡처

### 테스트 시나리오 2: 업스트림 QoS 검증

이 테스트 시나리오에서는 업스트림 QoS 컨피그레이션을 검증하는 것이 목적입니다. 무선 PC가 유선 PC에 DSCP 46이 포함된 UDP 패킷을 전송하는 과정이 수행됩니다. WLC는 업스트림 및 다운스트림 방향 모두에 대해 메탈 "플래티넘 QoS" 정책으로 구성됩니다.

- 트래픽 흐름:

출처: 무선 PC

대상: 유선 PC

트래픽 유형: DSCP가 46인 UDP 패킷

- WLC의 QoS 정책 구성:

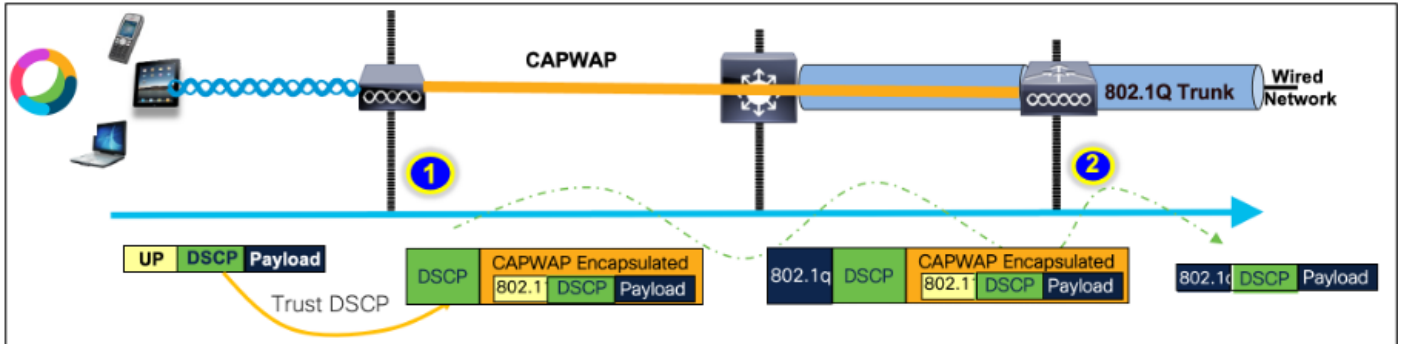
QoS 프로파일: 플래티넘 QoS

방향: 업스트림 및 다운스트림 모두

- 금속 QoS 컨피그레이션 명령:

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

업스트림 방향의 논리적 토폴로지 및 DSCP 변환:



논리적 토폴로지 및 DSCP 변환 - 업스트림

무선 PC에서 유선 PC로 전송된 패킷입니다. 이 캡처는 무선 PC에서 수행됩니다.

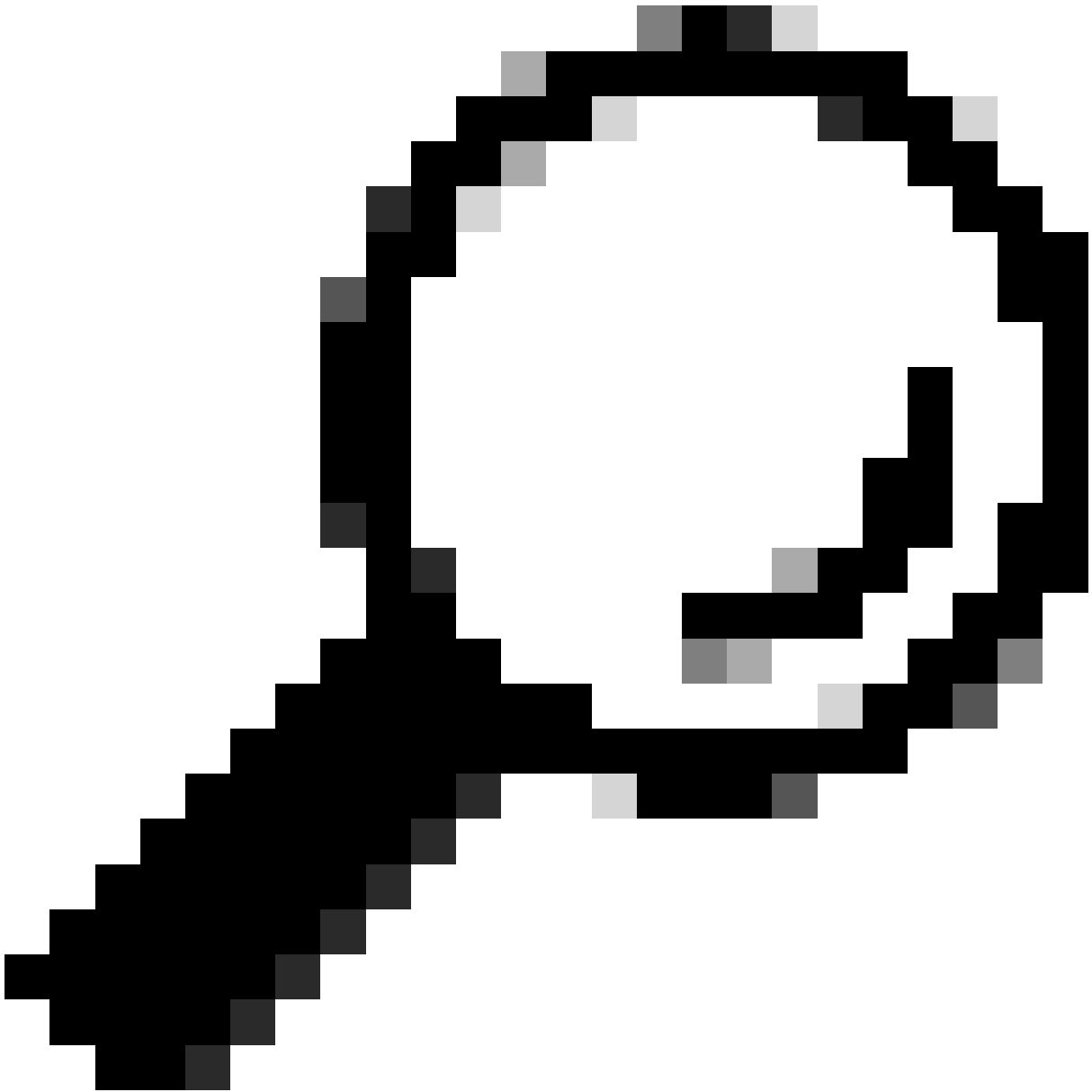
무선 PC는 DSCP 46으로 UDP 패킷을 전송합니다.

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

```
> Frame 241: 834 bytes on wire (6672 bits), 834 bytes captured (6672 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: 24:2f:d0:da:af:1d (24:2f:d0:da:af:1d), Dst: Cisco_37:cd:e5 (2c:ciab: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 Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    ... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 820
  Identification: 0x2d25 (11557)
```

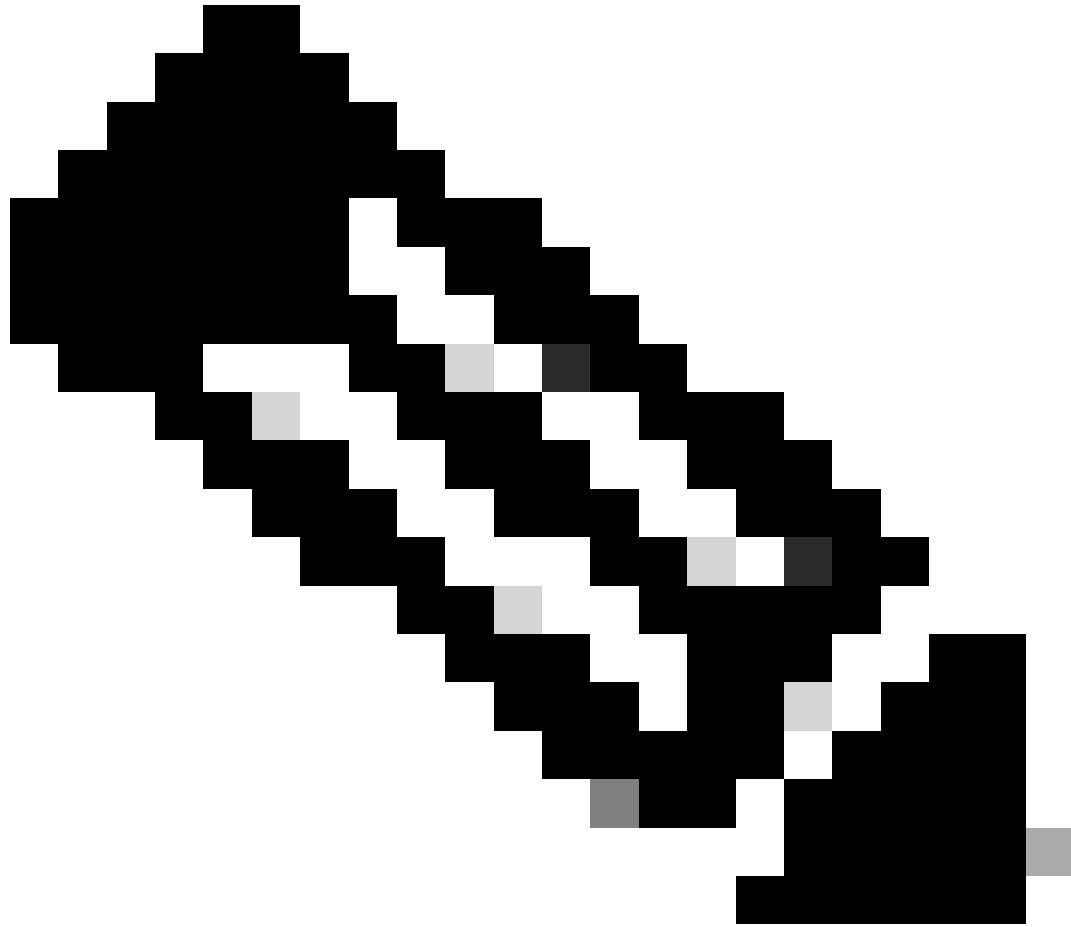
업스트림 방향의 무선 PC 캡처

다음으로 클라이언트에서 AP로의 OTA 캡처에 대해 알아보겠습니다.



팁: Windows 무선 PC를 사용하여 DSCP 46으로 패킷을 보낼 때 Windows는 DSCP 46을 사용자 우선 순위(UP) 값 5(비디오)에 매핑합니다. 따라서 OTA 캡처는 패킷을 비디오 트래픽(UP 5)으로 표시합니다. 그러나 패킷을 해독하면 DSCP 값은 46으로 유지됩니다.

---



참고: 버전 17.4부터 Cisco 9800 WLC의 기본 동작은 AP 조인 프로파일의 DSCP 값을 신뢰하는 것입니다. 이렇게 하면 DSCP 값 46이 WLC에서 보존되고 신뢰되므로 Windows DSCP to UP 매핑 동작과 관련된 문제가 발생하지 않습니다.

---



QoS Control Field: 0000000000000101

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

802.2 Logical Link Control (LLC) Header

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

IP Header - Internet Protocol Datagram

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

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

Windows UP DSCP 매핑

랩 설정에서 가져온 암호화된 OTA(Over-the-Air) 캡처를 분석하여 업스트림 QoS 컨피그레이션을 검증합니다.

OTA 캡처는 UP(User Priority) 값이 5(비디오)인 패킷을 표시합니다. OTA 캡처에 UP 5가 표시되지만 암호화된 패킷 내부의 DSCP 값은 46으로 유지됩니다.

No.	Time	SA	RA	Source	Destination	Protocol	DSCP	Priority	Length	Info
5643	10:53:22.982358	24:2f:d0:da:af:1d	a4:b4:39:4e:85:4f	24:2f:d0:da:af:1d	Cisco_37:cd:e5	802.11	C50 Video (Video)	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)]
      .... .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)
  
```

업스트림 방향의 LAB 설정 OTA

그런 다음 AP 업링크 포트의 패킷 캡처를 분석하여 패킷이 AP에서 WLC로 이동할 때 DSCP 값이 유지되도록 합니다.

- 외부 CAPWAP 레이어의 DSCP 값은 46으로 유지됩니다.
- CAPWAP 터널 내에서도 DSCP 값은 46으로 유지됩니다.

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)
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)
  
```

업스트림 방향의 AP PpLink 캡처

패킷이 스위치에서 도착하면 WLC에서 캡처가 수행됩니다.

- 패킷은 외부 CAPWAP 레이어의 DSCP 값이 46인 WLC에 도착합니다.
- CAPWAP 터널 내에서 DSCP 값은 46으로 유지됩니다.

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: 1)
517	10:53:22.989939	24:2f:d0:da:af:1d	a4:b4:39:4e:85:40	192.168.30.13	192.168.31.10	IPv4	EF PHB	Video (Video)	148	Fragmented IP protocol (p)

```

> Frame 517: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on 0
> Ethernet II, Src: Cisco_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
[.... .... 101 = 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)

```

AP에서 오는 패킷을 보여주는 WLC EPC

패킷이 WLC에서 헤어핀 회전을 하면 유선 PC를 목적지로 하는 업링크 스위치로 다시 전송됩니다. WLC는 DSCP 값이 46인 패킷을 전달합니다.

No.	Time	SA	RA	Source	Destination	Protocol	DSCP	Priority	Length	Info
528	10:53:23.000000			192.168.30.13	192.168.31.10	UDP	EF PHB		838	52121 → 5201 Len=8192

```

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

```

유선 PC로 전송된 패킷을 표시하는 WLC EPC

마지막으로 유선 PC 업링크에서 패킷 캡처를 분석하여 패킷이 WLC에서 도착할 때 DSCP 값이 유지되도록 합니다.

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)

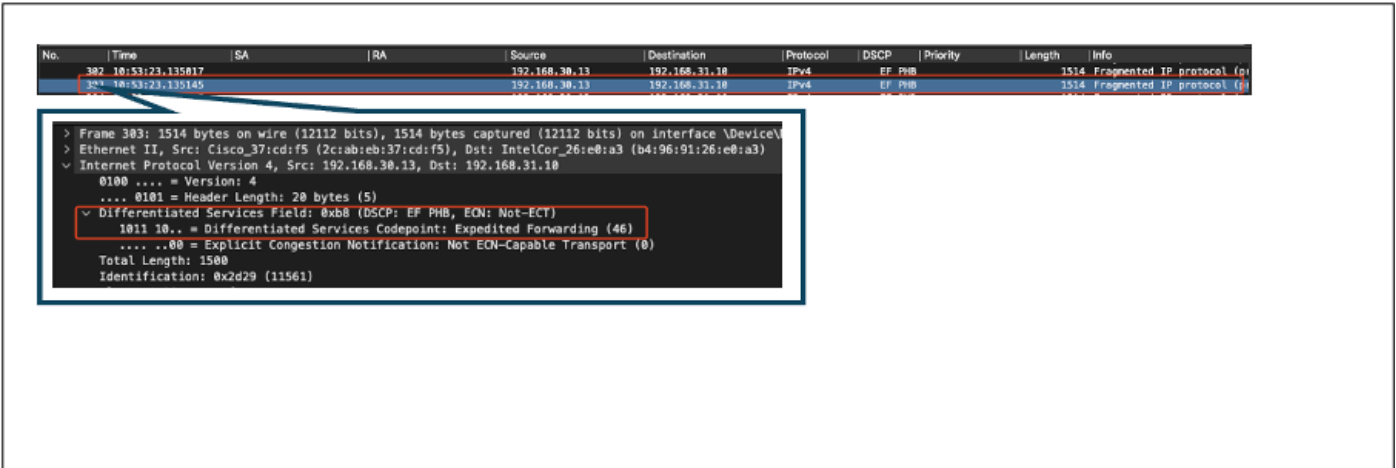
```

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

```

업스트림 방향의 유선 PC 업링크 스위치 캡처

최종 단계에서 유선 PC가 수신한 패킷을 분석하여 유선 PC에 DSCP 값 46으로 패킷이 도착하는지 확인합니다.



유선 PC 캡처 - 업스트림 방향

업스트림 QoS 테스트에서는 무선 PC에서 유선 PC로 이동하는 트래픽에 대한 QoS 구성을 검증했습니다. 전체 전송 경로에서 DSCP 값 46을 일관되게 유지하면 QoS 정책이 올바르게 적용되고 적용되었음을 확인할 수 있습니다.

## 문제 해결

음성, 비디오 및 기타 실시간 애플리케이션은 네트워크 성능 문제에 특히 민감하며 QoS(Quality of Service) 저하는 눈에 띄고 해로운 영향을 미칠 수 있습니다. QoS 패킷이 더 낮은 DSCP 값으로 표시되면 음성 및 비디오에 미치는 영향이 클 수 있습니다.

음성에 미치는 영향:

- 향상된 지연 시간: 음성 커뮤니케이션을 위해서는 낮은 지연 시간이 필요하므로 자연스러운 대화가 보장됩니다. DSCP 값이 낮으면 음성 패킷이 지연되어 대화에 눈에 띄는 지연이 발생할 수 있습니다.
- 지터: 패킷 도착 시간의 가변성(지터)은 음성 패킷의 원활한 전달을 방해할 수 있습니다. 이는 변질되거나 왜곡된 음성으로 이어질 수 있어, 화자를 이해하기 어렵게 만듭니다.
- 패킷 손실: 음성 패킷은 패킷 손실에 매우 민감합니다. 소량의 패킷 손실이라도 단어나 음절이 누락되어 통화 품질이 저하되고 오해가 발생할 수 있습니다.
- 에코 및 왜곡: 레이턴시와 지터가 증가하면 에코 및 오디오 왜곡이 발생하여 음성 통화의 품질이 더욱 저하될 수 있습니다.

비디오에 미치는 영향:

- 레이턴시 증가: 비디오 통신에서는 오디오와 비디오 스트림 간의 동기화를 유지하기 위해 짧은 레이턴시가 필요합니다. 레이턴시가 증가하면 지연이 발생하여 실시간 상호 작용이 어려워질 수 있습니다.
- 지터: 지터로 인해 비디오 프레임이 순서를 벗어나거나 불규칙한 간격으로 도착하여 흔들리거나 비틀거리는 비디오 환경이 발생할 수 있습니다.
- 패킷 손실: 패킷이 손실되면 프레임이 누락될 수 있으며, 이로 인해 비디오가 아티팩트를 고정하거나 표시할 수 있습니다.

- 비디오 품질 감소: DSCP 값이 낮으면 비디오 스트림에 대한 대역폭 할당이 줄어 해상도가 낮아지고 비디오 품질이 저하될 수 있습니다. 이로 인해 비디오에서 중요한 세부 사항을 보기 어렵게 될 수 있습니다.

### 시나리오 1: 중간 스위치가 DSCP 마킹을 재작성합니다.

이 트러블슈팅 시나리오에서는 DSCP 마킹을 재작성하는 중간 스위치가 WLC에 도달할 때 트래픽에 미치는 영향을 조사합니다. 이를 복제하기 위해, 스위치는 유선 PC 업링크 인터페이스에서 CS1에 대한 DSCP 46 마킹을 재작성하도록 구성된다.

패킷은 유선 PC에서 DSCP 46 태그와 함께 전송됩니다.

```

> 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)
  
```

DSCP 46 태그가 있는 유선 PC 전송 패킷

패킷은 DSCP 값이 CS1(DSCP 8)인 WLC에 도착합니다. DSCP 46에서 DSCP 8로 변경하면 패킷의 우선순위가 크게 낮아집니다.

```

> 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, CS1 표시

이 단계에서는 WLC가 AP에 전달한 패킷을 분석합니다.

- 외부 CAPWAP 헤더에는 CS1(DSCP 8)로 태그가 지정됩니다.
- 내부 CAPWAP 헤더에도 CS1(DSCP 8)로 태그가 지정됩니다.
- User Priority (UP)(사용자 우선순위(UP)) 값은 BK (Background)(BK(백그라운드))로 설정됩니다.

```

> 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)

```

CAPWAP 트래픽에 CS1 태그를 표시하는 WLC EPC

패킷은 DSCP 값이 CS1(DSCP 8)인 무선 PC에 도착합니다.

```

> 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

```

CS1 마킹을 표시하는 무선 PC 캡처

이 시나리오에서는 중간 스위치의 컨피그레이션 오류가 QoS 컨피그레이션을 중단하여 우선 순위

가 높은 트래픽의 성능을 저하시키는 방법을 보여줍니다. 초기에 높은 우선 순위로 표시된 음성 패킷은 DSCP 재작성으로 인해 낮은 우선 순위의 트래픽으로 처리되었습니다. 이 시나리오는 우선 순위가 높은 트래픽에 대해 원하는 QoS(Quality of Service)를 유지하기 위해 중간 네트워크 디바이스가 QoS 표시를 올바르게 보존해야 한다는 중요성을 강조합니다.

## 시나리오 2: AP 링크 스위치가 DSCP 마킹을 재작성합니다.

이 시나리오에서는 DSCP 마킹을 다시 쓰는 AP에 연결된 중간 스위치가 트래픽에 미치는 영향을 조사합니다.

- AP에 연결된 스위치는 DSCP 46 마킹을 AP 업링크 인터페이스의 다른 값 CS1으로 재작성하도록 구성됩니다.
- 패킷은 유선 PC에서 DSCP 태그 46으로 전송됩니다. 그러면 트래픽이 소스에서 DSCP 46으로 올바르게 표시되는지 확인합니다.

```
> 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)
  > 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: 0xcd67 (52583)
    > 0000 ... = Flags: 0x0
```

무선 PC 캡처, DSCP 표시 46

패킷이 스위치에서 도착하면 WLC에서 캡처가 수행됩니다.

패킷은 외부 CAPWAP 헤더 DSCP 값이 CS1(DSCP)이고 내부 DSCP 값이 46 인 WLC에 도착합니다. 중간 스위치에서 CAPWAP 터널 내에 캡슐화된 트래픽을 볼 수 없기 때문에 이러한 현상이 발생합니다.

WLC는 CAPWAP 터널 내의 DSCP 태그를 신뢰하고 내부 DSCP 태그가 46인 유선 PC에 트래픽을 전달합니다.

```

> 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 CAPWAP DSCP 값 표시

패킷이 유선 PC에 도착하며 DSCP 값은 46입니다. WLC가 원래 DSCP 값인 46으로 패킷을 올바르게 전달하여 높은 우선 순위 마킹을 유지하는지 확인합니다.

```

> 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

```



WLC에서 DSCP 태그가 46인 트래픽을 전달했지만, 외부 DSCP 태그가 CS1(DSCP 8)에 다시 기록되므로 AP에서 WLC로의 트래픽이 낮은 우선 순위로 처리되었음을 이해하는 것이 중요합니다.

AP와 WLC 사이에 여러 개의 스위치가 있을 수 있으며, 트래픽에 낮은 우선 순위를 부여하면 WLC에 늦게 도착할 수 있습니다. 이로 인해 지연 시간, 지터 및 잠재적 패킷 손실이 증가할 수 있으며, 이는 음성과 같은 우선 순위가 높은 트래픽의 서비스 품질을 저하시킬 수 있습니다.

## 문제 해결 팁

1. 초기 DSCP 마킹 확인: 소스(예: 유선 PC)에서 패킷을 캡처하여 트래픽이 의도한 DSCP 값으로 올바르게 표시되었는지 확인합니다.
2. Intermediate Device Configurations(중간 디바이스 컨피그레이션 확인): 모든 중간 스위치 및 라우터의 컨피그레이션을 검토하여 실수로 DSCP 값을 재작성하지 않도록 합니다.
3. 핵심 지점에서 트래픽 캡처:
  1. 중간 스위치 전후에.
  2. WLC에서.
  3. 대상(예: 무선 PC)에서
4. 트래픽 시나리오 시뮬레이션: 트래픽 생성기 또는 네트워크 시뮬레이션 툴을 사용하여 다양한 유형의 트래픽을 생성하고 QoS가 무선 네트워크에서 처리되는 방식을 관찰합니다.
5. 9800 모범 사례 문서 참조: QoS 및 DSCP 표시 구성에 대한 9800 모범 사례 문서를 검토하십시오.

## 컨피그레이션 확인

<#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
```

## 결론

음성 및 비디오와 같은 우선 순위가 높은 트래픽이 적절한 수준의 서비스 및 성능을 제공받도록 하려면 네트워크 전체에서 일관된 QoS 구성을 유지하는 것이 중요합니다. 모든 네트워크 디바이스가

의도된 QoS 정책을 준수하는지 확인하기 위해 QoS 컨피그레이션을 정기적으로 검증하는 것이 중요합니다. 이러한 검증을 통해 네트워크 성능을 저하시킬 수 있는 잘못된 컨피그레이션 또는 편차를 식별하고 수정할 수 있습니다.

## 참조

- [Cisco Catalyst 9800 Series Wireless Controller 이해 및 문제 해결](#)
- [Cisco Catalyst 9800 Series 구성 모범 사례](#)
- [Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS® XE Dublin 17.12.x](#)
- [VoWLAN\(Voice Over Wireless LAN\) 문제 해결 가이드](#)
- [Windows 컴퓨터에서 DSCP QoS 태깅 사용](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.