在9800 WLC上配置无线QoS的验证和故障排除

目录

简介

本文档介绍在9800无线LAN控制器(WLC)上配置、验证无线服务质量(QoS)并对其进行故障排除的方法。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- WLC：运行17.12.03的C9800-40-K9
- 无线接入点(AP)：C9120-AX-D
- 交换机：运行17.03.05的C9300-48P
- 有线和无线客户端：Windows 10

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

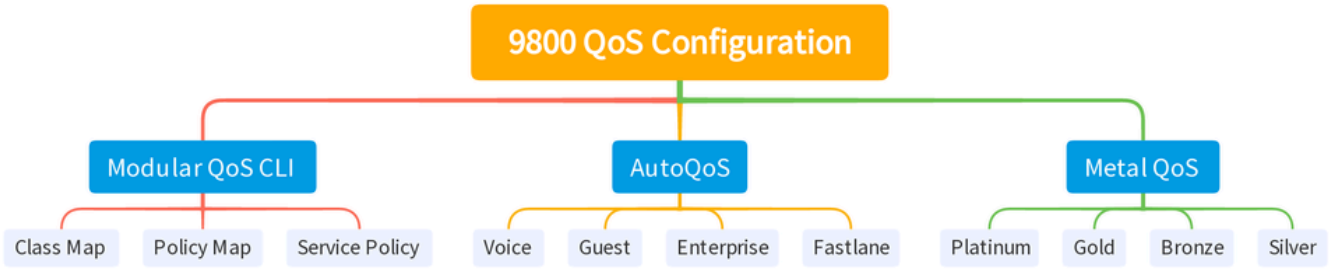
无线QoS对于确保关键应用获得最佳性能所需的必要带宽和低延迟至关重要。本文档提供在Cisco无线网络上配置、验证和排除QoS故障的全面指南。

本文假设读者对无线和有线QoS原则有基本的了解。此外，读者应该能够熟练地配置和管理Cisco WLC和AP。

配置

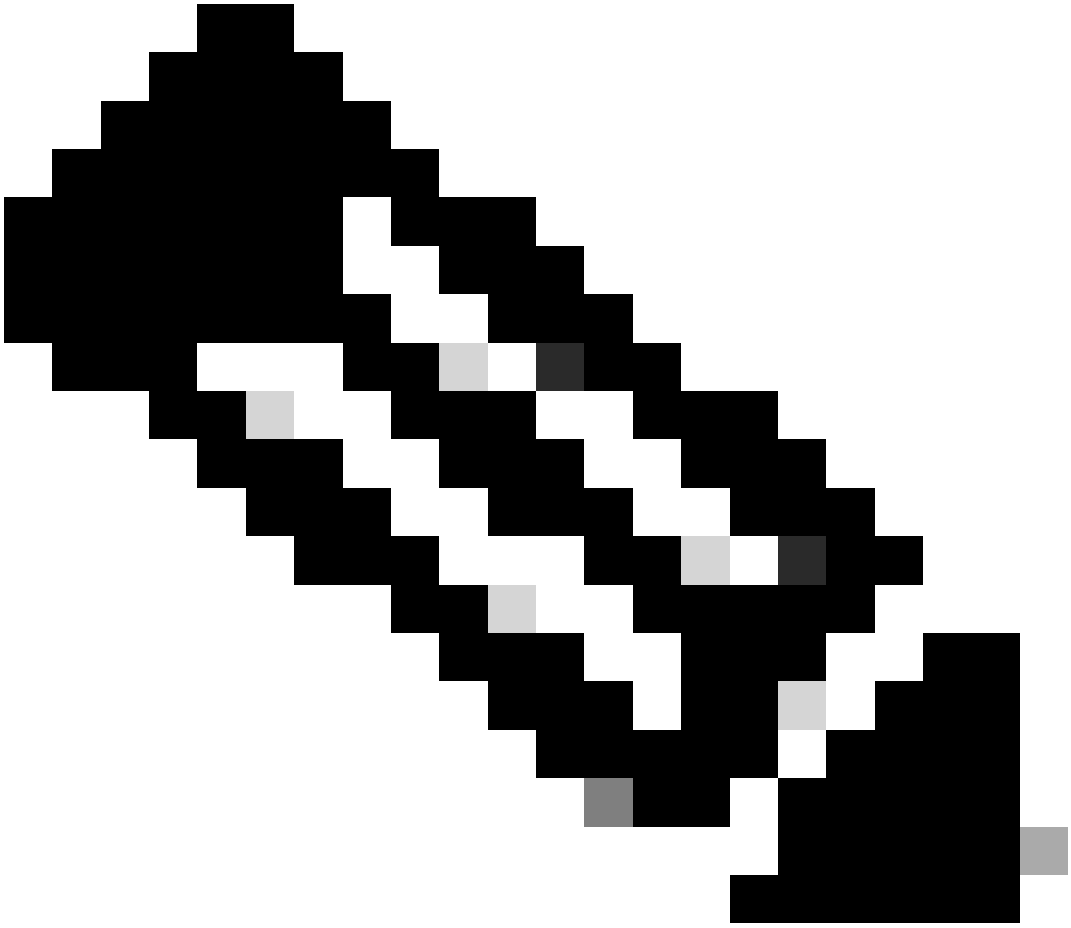
本部分将深入探讨9800无线控制器上的QoS配置。利用这些配置，您可以确保关键应用获得必要的带宽和低延迟，从而优化整体网络性能。

可以将9800 WLC QoS配置主要分为三个不同的类别。



9800 WLC QOS配置摘要

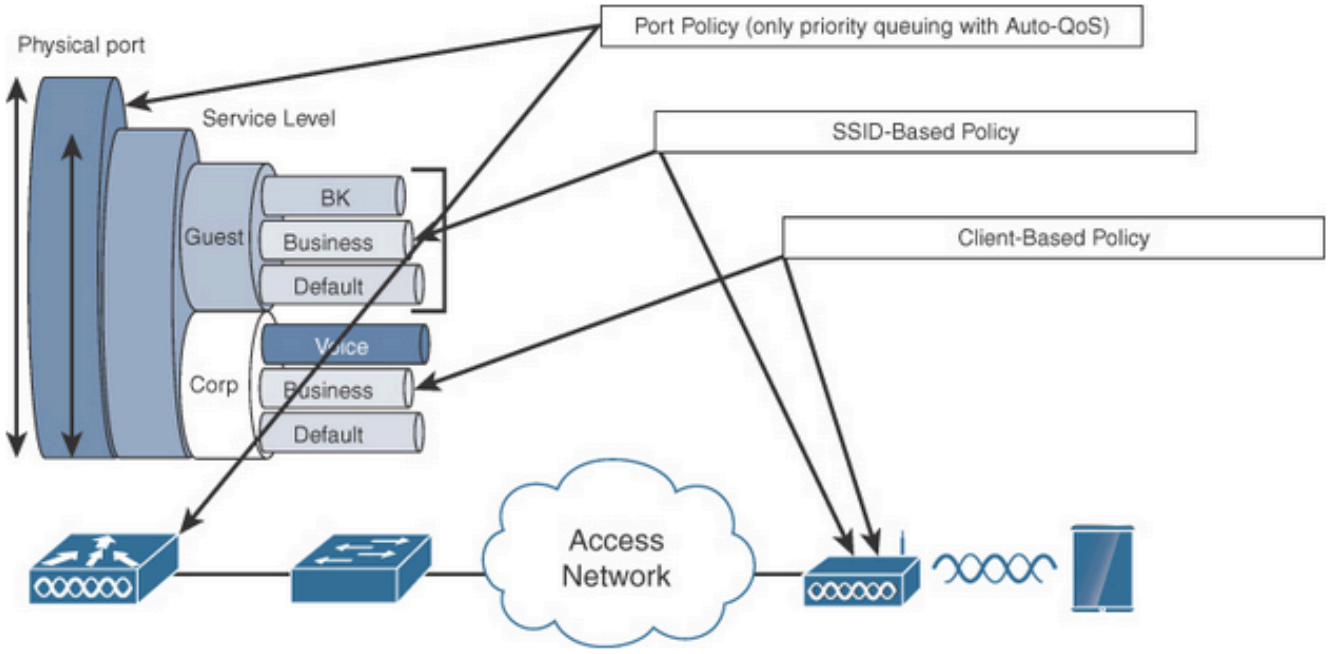
本文档将在后续章节中逐一介绍每个章节。



注意：本文重点介绍本地模式下的AP。不讨论Flexconnect模式下的AP。

QoS策略目标

策略目标是可以应用QoS策略的配置结构。Catalyst 9800上的QoS实施是模块化和灵活的。用户可以决定在三个不同的目标上配置策略：SSID、客户端和端口级别。



QoS策略目标

SSID策略适用于每个SSID的每个AP。您可以在SSID上配置策略和标记策略。

客户端策略适用于入口和出口方向。您可以在客户端上配置策略和标记策略。还支持AAA覆盖。

基于端口的QoS策略可应用于物理或逻辑端口。

自动Qos

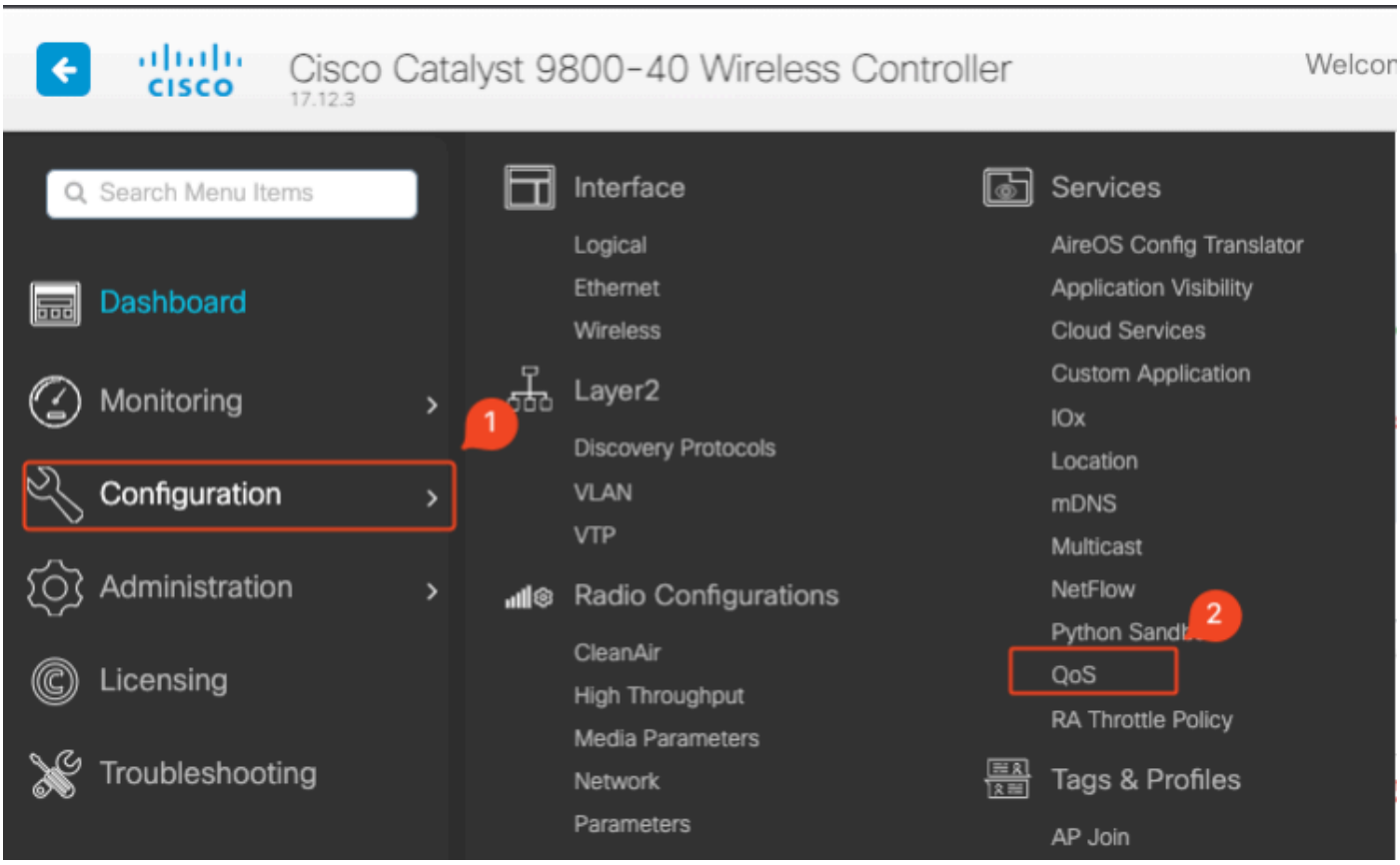
无线自动QoS可自动部署无线QoS功能。它有一组预定义的配置文件，管理员可以进一步修改这些配置文件以区分不同流量的优先级。自动QoS匹配流量并将每个匹配的数据包分配到QoS组。这允许输出策略映射将特定QoS组放入特定队列，包括优先级队列。

模式	客户端入口	客户端出口	入口BSSID	出口BSSID	入口端口	出口端口	无线电
语音	不适用	不适用	Platinum-up	白金级	不适用	AutoQos-4.0-wlan-Port-Output-Policy	ACM打开
访客	不适用	不适用	AutoQos-4.0-wlan-GT-SSID-Input-Policy	AutoQos-4.0-wlan-GT-SSID-Output-Policy	不适用	AutoQos-4.0-wlan-Port-Output-Policy	
Fastlane	不适	不适	不适用	不适用	不适	AutoQos-4.0-	edca-

	用	用			用	wlan-Port-Output-Policy	parameters fastlane
企业AVC	不适用	不适用	AutoQos-4.0-wlan-ET-SSID-Input-AVC-Policy	AutoQos-4.0-wlan-ET-SSID-Output-Policy	不适用	AutoQos-4.0-wlan-Port-Output-Policy	

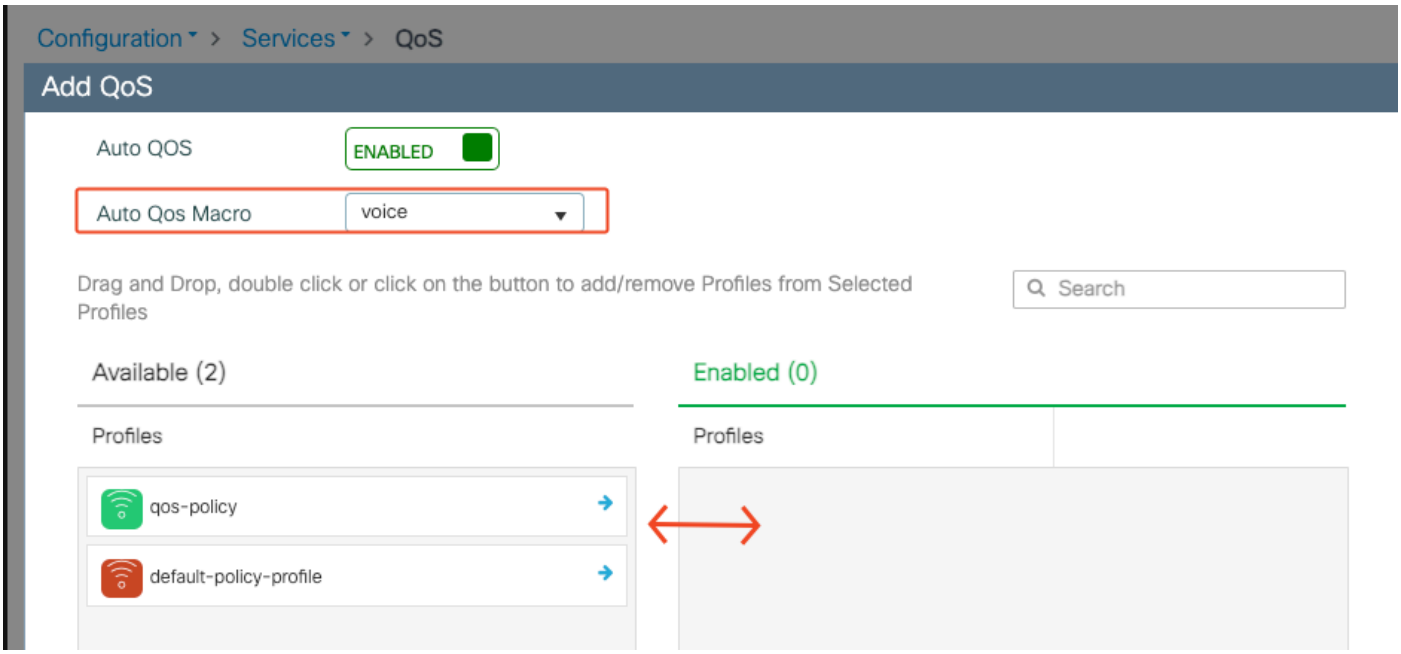
此表描述了应用自动QoS配置文件时发生的配置更改。

要配置自动QoS，请导航到配置> QoS



QoS工作流程

单击Add并将Auto QoS设置为enabled。从列表中选择相应的自动QoS宏。在本示例中，使用Voice宏指定语音流量的优先级。



AutoQoS语音映射

启用宏后，选择需要附加到策略的策略。

自动QoS CLI配置

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

启用自动QoS后，您可以看到发生的更改。本部分列出了语音的配置更改。

```
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
```

模块化QoS CLI

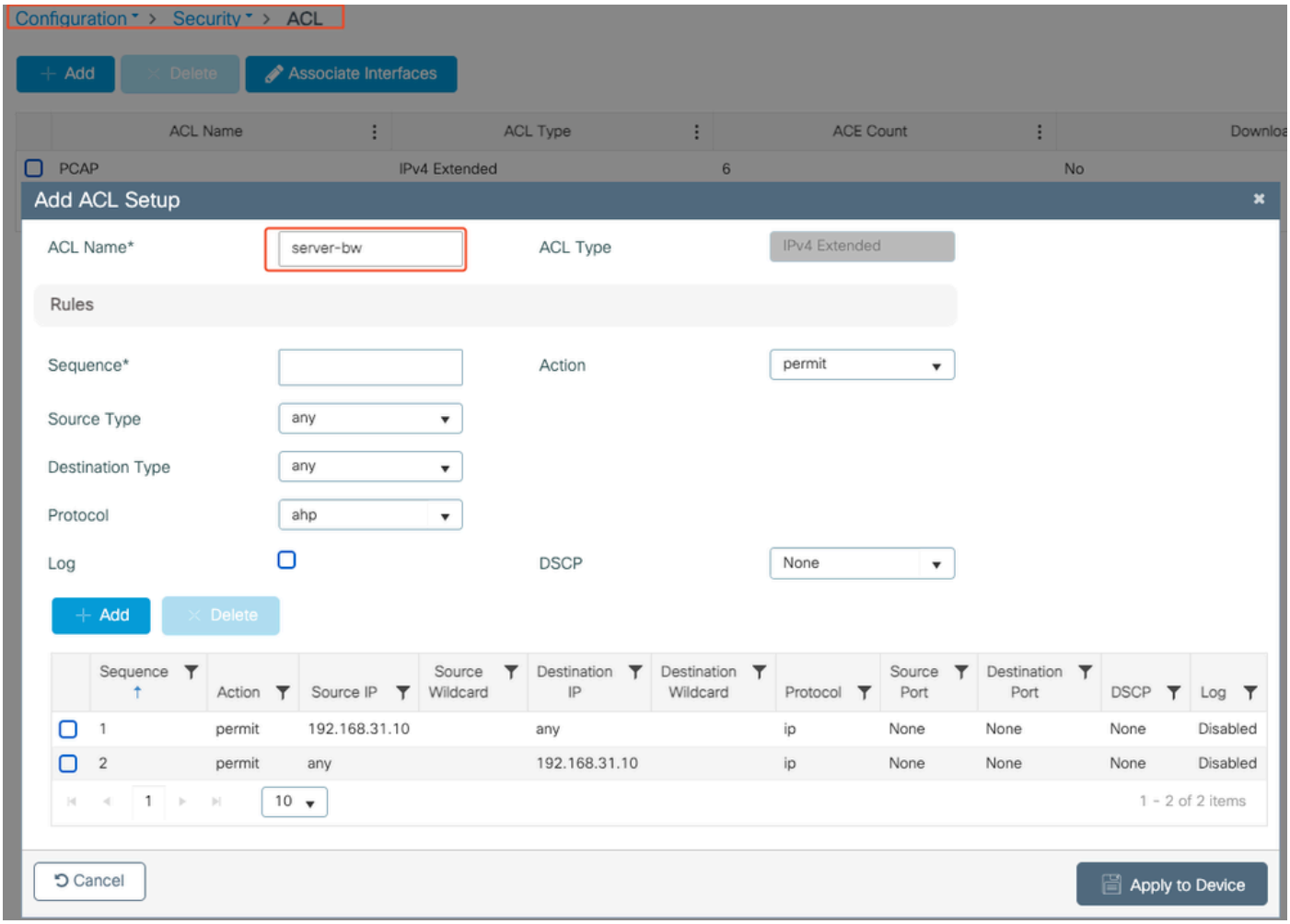
MQC允许您定义流量类，创建流量策略（策略映射），并将流量策略附加到接口。流量策略包含应用于流量类的QoS功能。

MQS CLI工作流程

本示例演示如何使用访问控制列表(ACL)对流量进行分类并应用带宽限制。

创建ACL以识别和分类要管理的特定流量。这可以通过定义根据IP地址、协议或端口等条件匹配流量的规则来实现。

导航到Configuration > Security > ACL，然后添加ACL。

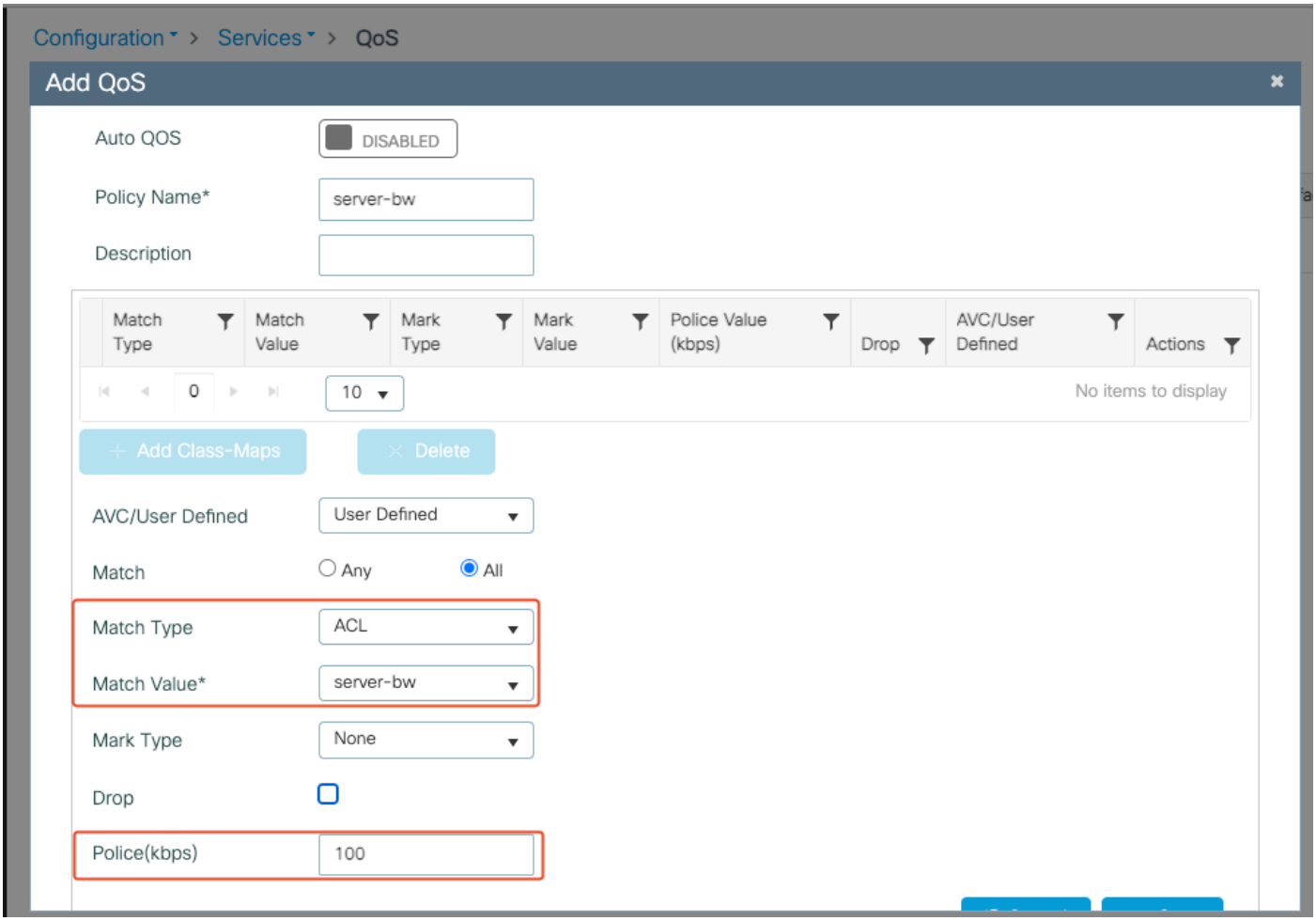


ACL 配置

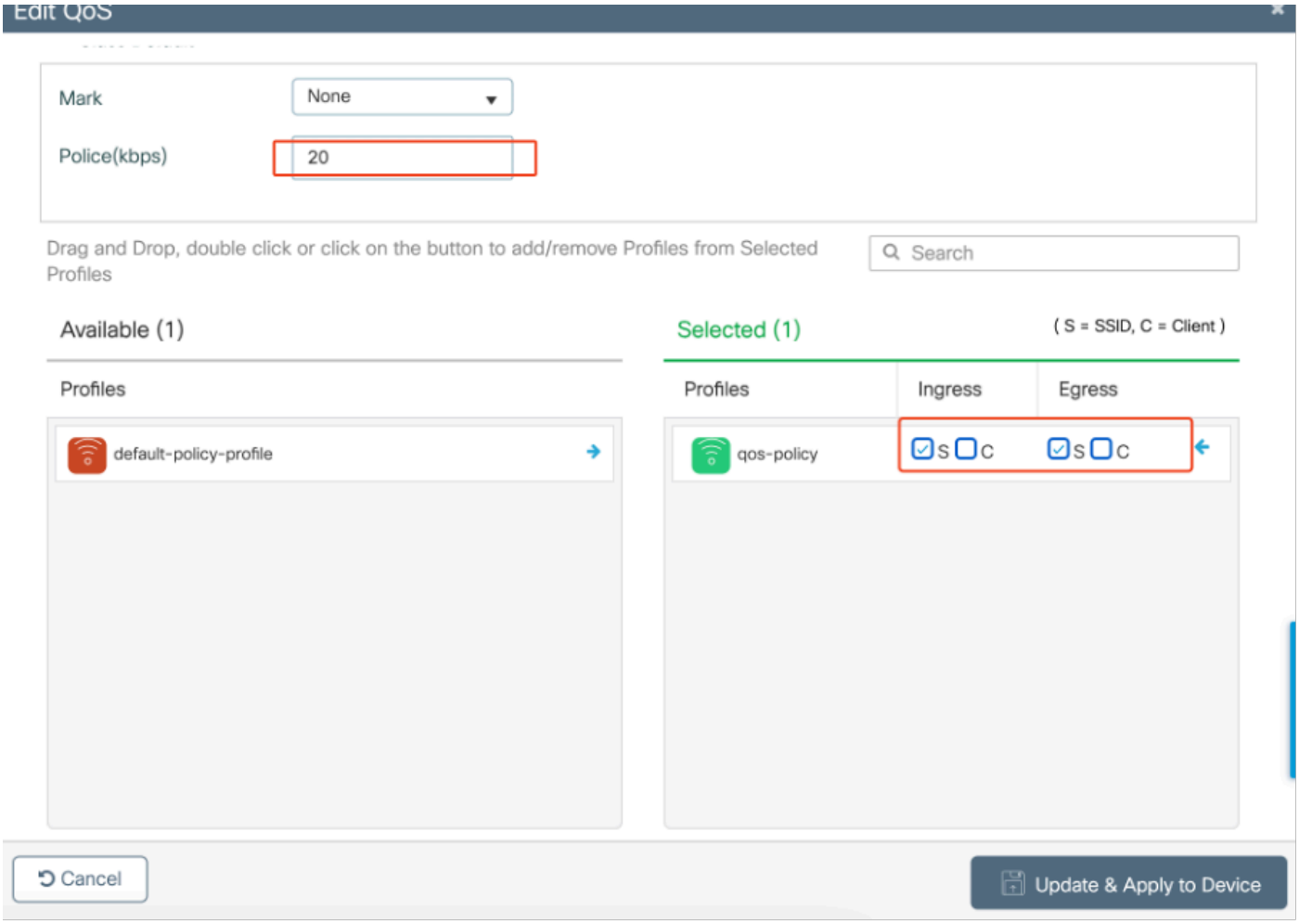
使用ACL对流量分类后，请配置带宽限制来控制分配给该流量的带宽量。

导航到配置>服务> QoS和QoS策略。将ACL附加到策略内，然后以kbps为单位应用策略。

向下滚动并选择应用QoS的策略配置文件。您可以为SSID或客户端选择入口/出口方向的策略。



MQS策略



MQS配置文件

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
```

金属Qos

这些QoS配置文件的主要目的是限制无线网络上允许的最大差分服务代码点(DSCP)值，从而控制802.11用户优先级(UP)值。

在Cisco 9800无线局域网控制器(WLC)中，金属QoS配置文件是预定义的，不可配置。但是，您可以将这些配置文件应用到特定SSID或客户端以实施QoS策略。

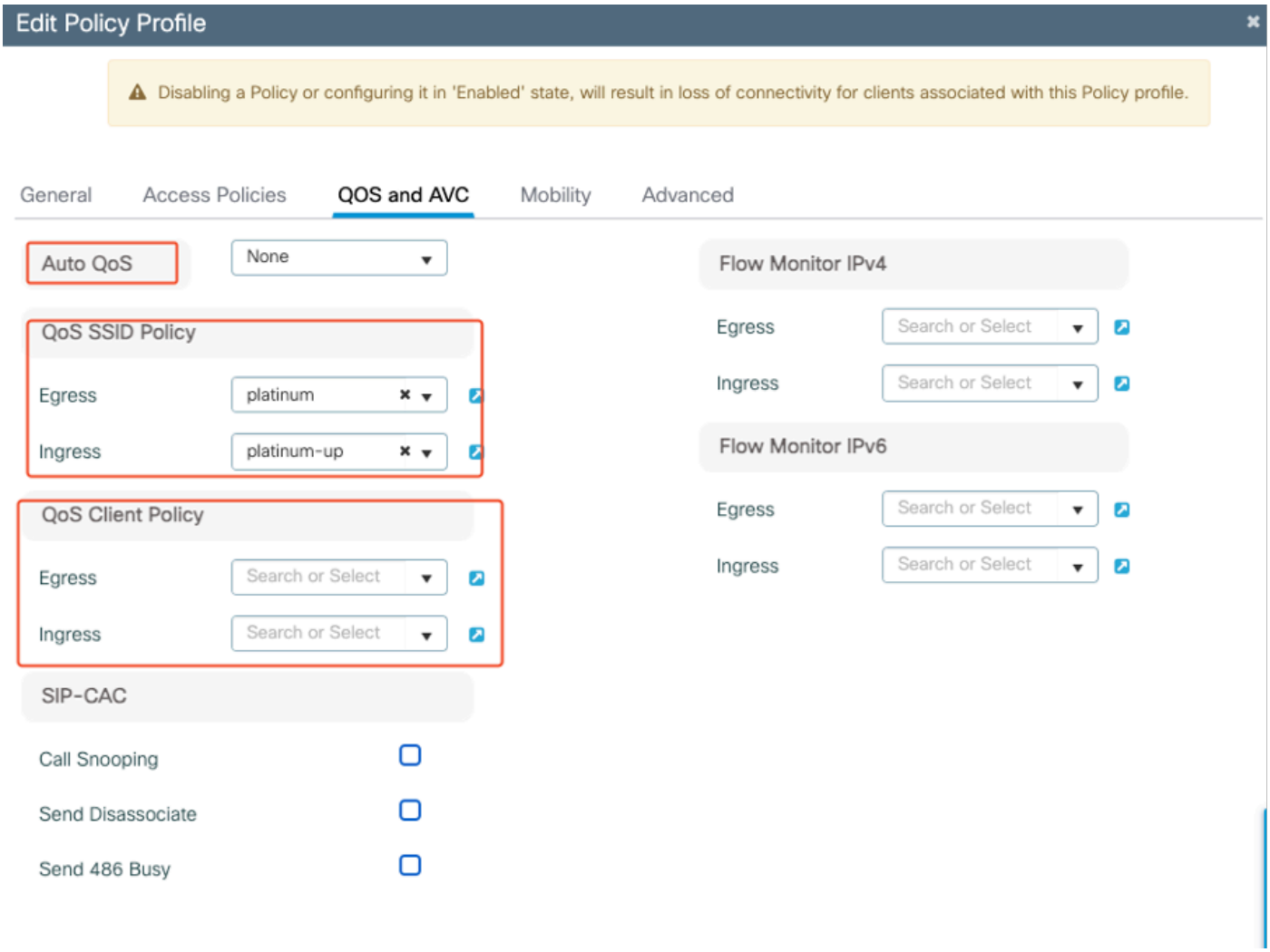
有四个可用的金属QoS配置文件：

Qos配置文件	最大DSCP
铜级	8
银牌	0
金牌	34
白金级	46

要在Cisco 9800 WLC上配置金属QoS，请执行以下操作：

导航到配置>策略> QoS & AVC。

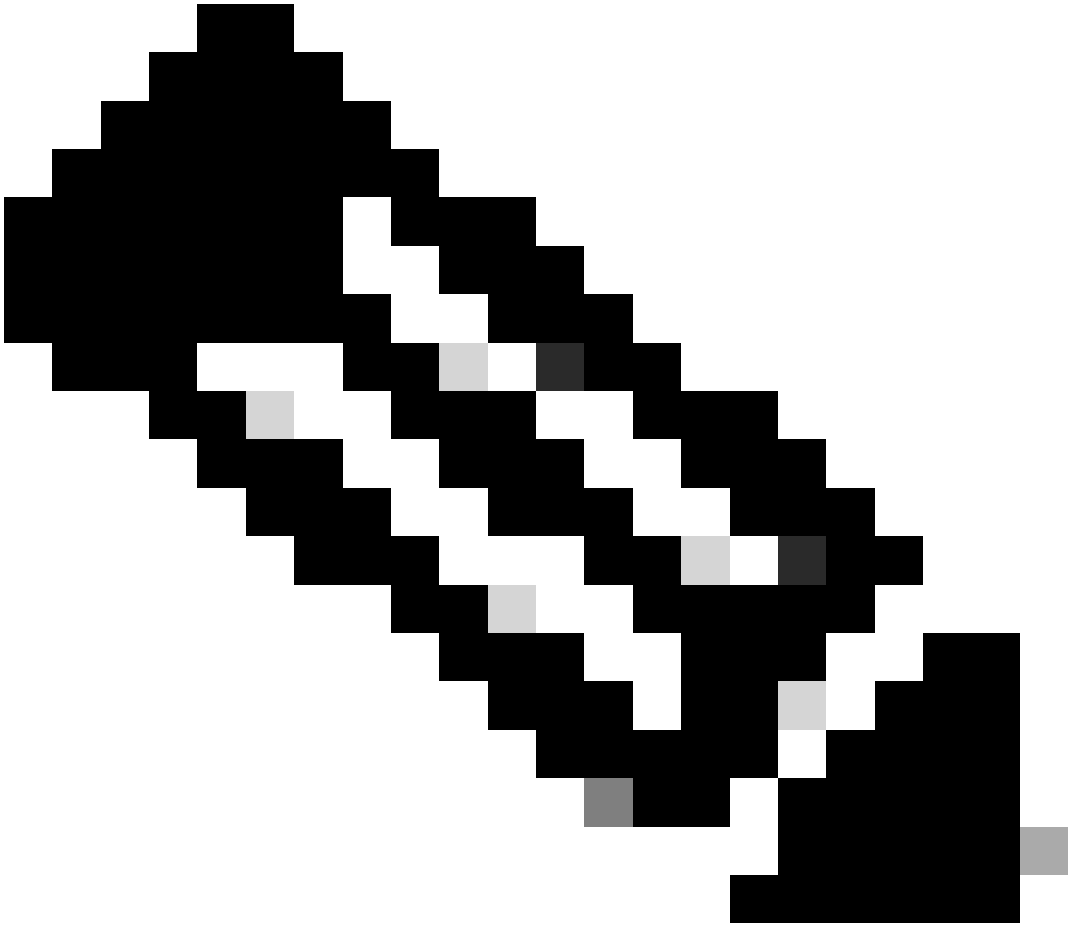
- 选择所需的金属QoS配置文件（白金级、金级、银级或铜级）。
- 将所选配置文件应用到目标SSID或客户端。



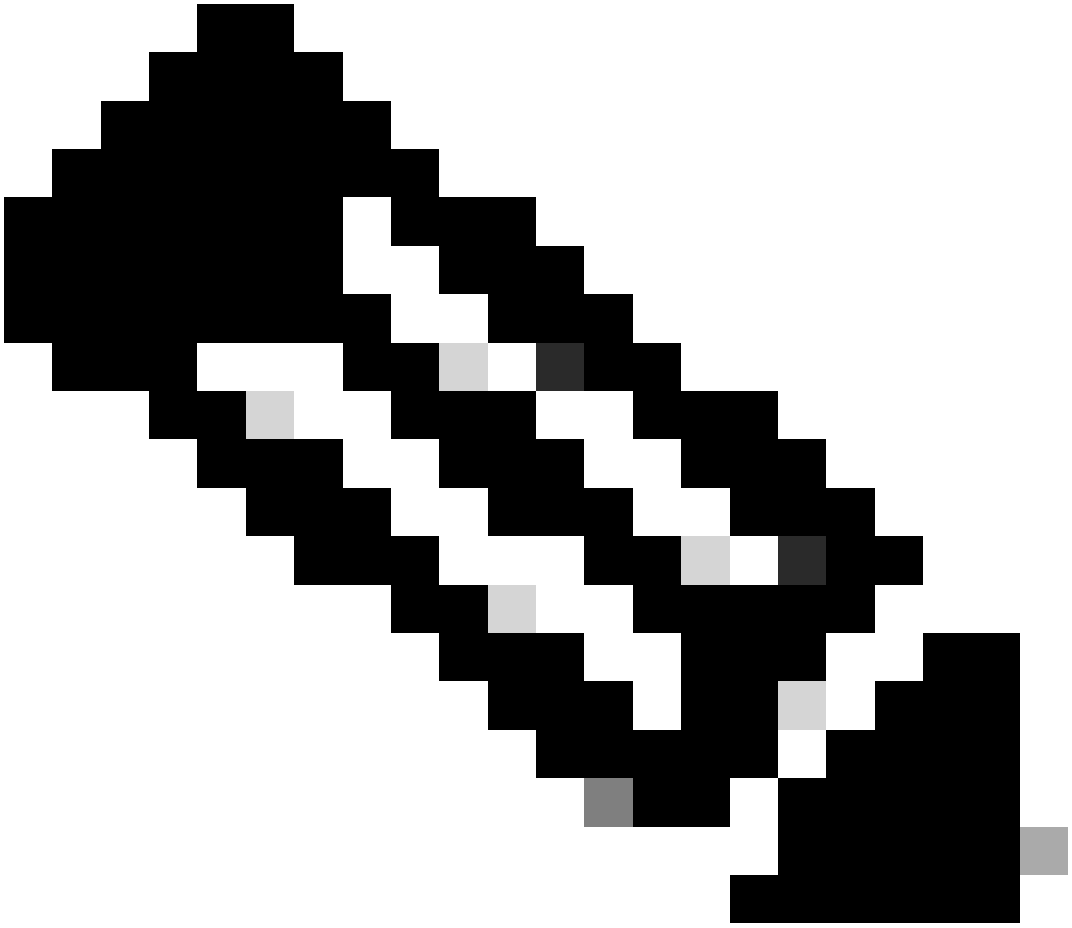
金属QoS配置文件

金属QoS CLI配置

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



注意：每个用户和SSID带宽合同可以通过QoS策略进行配置，而不是直接在金属QoS上进行配置。在9800中，不匹配的流量进入默认类别。



注意：在GUI中，您只能设置每个SSID的金属QoS。在CLI中，您也可以在客户端目标上对其进行配置。

通过数据包捕获验证端到端QoS

现在，QoS配置已完成，必须检查QoS数据包，并验证QoS策略是否从端到端正常运行。这可以通过数据包捕获和分析来实现。

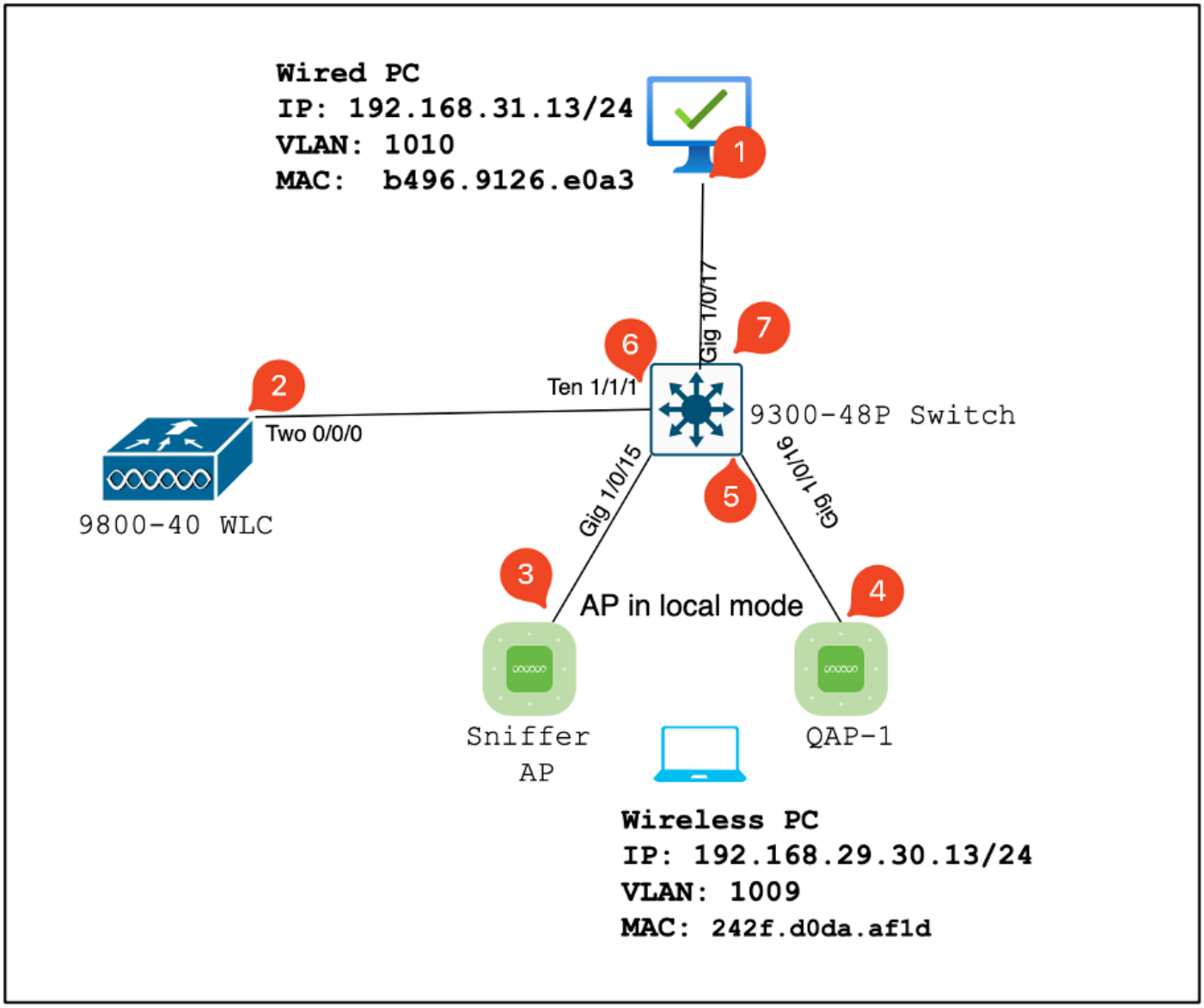
要复制和验证QoS配置，需要使用小型实验环境。本实验包括以下组件：

- WLC
- 无线接入点
- 嗅探器AP将采用OTA
- 有线 PC
- 交换机

所有这些组件都连接到实验环境中的同一台交换机。此图中突出显示的数字表示启用数据包捕获以

监控和分析流量的点。

网络图



实验室拓扑结构

实验组件和数据包捕获点

WLC：

- 管理无线网络的QoS策略和配置。
- 数据包捕获点：捕获WLC、AP和交换机之间的流量。

无线接入点：

- 为客户端提供无线连接并实施QoS策略。
- 数据包捕获点：捕获AP与交换机之间的流量。

嗅探器AP：

- 用作捕获无线流量的专用设备。
- 数据包捕获点：捕获AP与无线客户端之间的无线流量。

有线 PC:

- 连接到交换机来模拟有线流量和验证端到端QoS。
- 数据包捕获点：捕获通过有线链路传输和收到的QoS数据包。

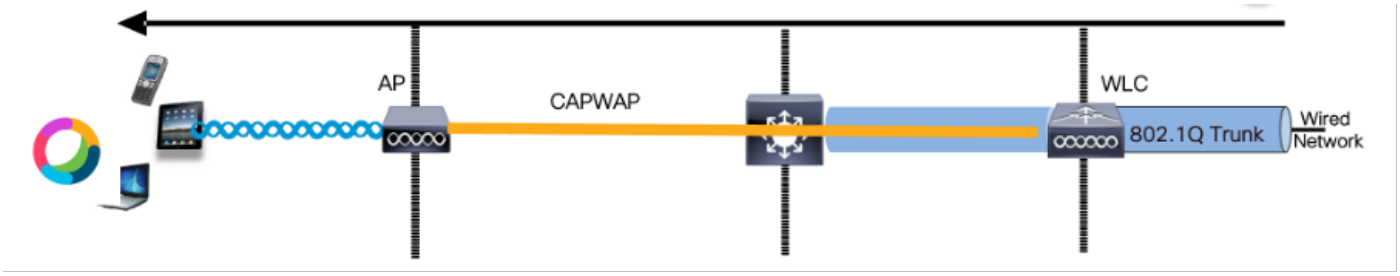
无线 PC:

- 连接到WLAN来模拟无线流量和验证端到端QoS。
- 数据包捕获点：通过无线链路捕获传输和收到的QoS数据包。

交换机：

- 连接所有实验组件和促进流量的中心设备。
- 数据包捕获点：捕获各种交换机端口的流量以验证正确的QoS实施。

从逻辑上讲，LAB拓扑可以这样绘制。



实验逻辑拓扑

为了测试和验证QoS配置，iPerf用于生成客户端和服务器之间的流量。这些命令用于促进iPerf通信，服务器和客户端的角色根据QoS测试方向进行互换。

测试场景1：下行QoS验证

目的是验证下行QoS配置。设置涉及有线PC使用DSCP 46向无线PC发送数据包。
无线局域网控制器(WLC)配置了下行和上行方向的金属“白金级QoS”策略。

测试设置：

- 通信流:

  来源：有线PC

  目的地：无线PC

  流量类型：DSCP为46的UDP数据包

- WLC上的QoS策略配置：

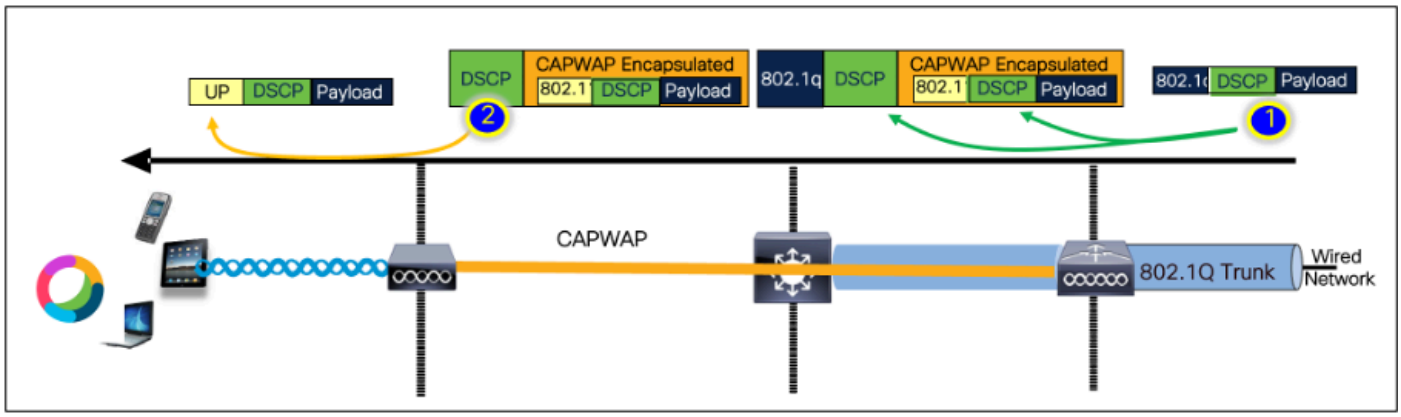
  QoS配置文件：金属QoS -白金级QoS

方向：下游和上游

- 金属QoS配置命令：

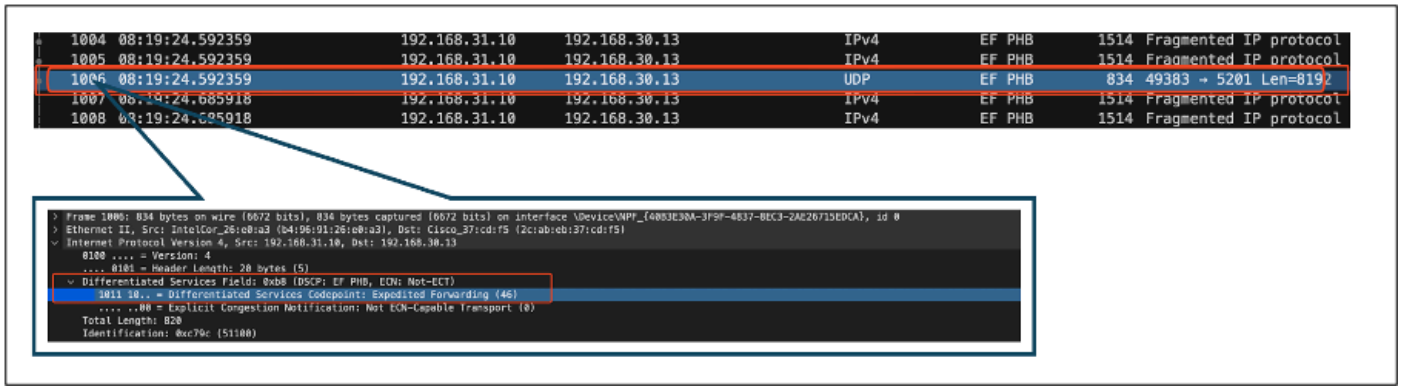
```
wireless profile policy qos-policy
service-policy input platinum-up
service-policy output platinum
```

下游方向的逻辑拓扑和DSCP会话。



DSCP对话点

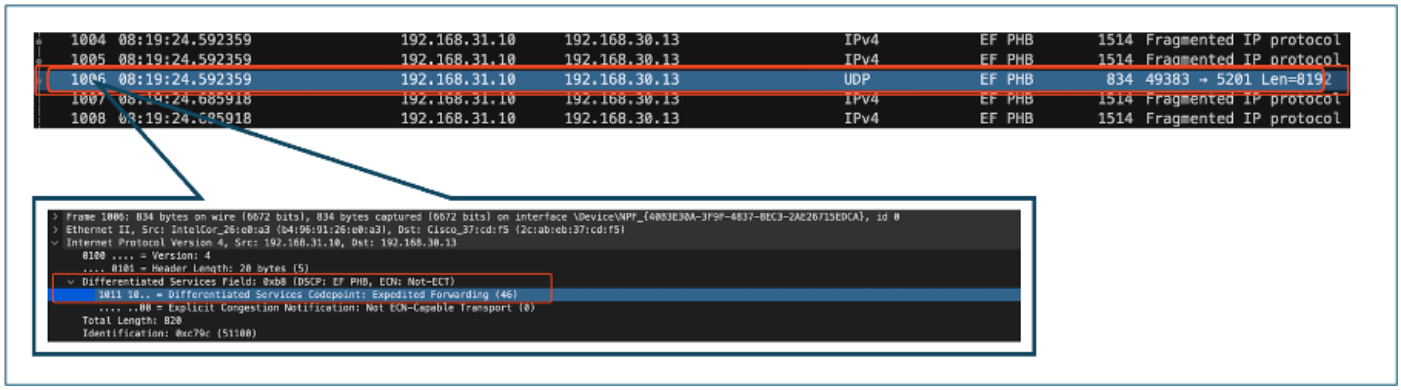
有线PC上的数据包捕获。这确认有线PC正在将UDP数据包发送到具有正确DSCP标记46的指定目标IP 192.168.10.13。



有线PC捕获-下行方向

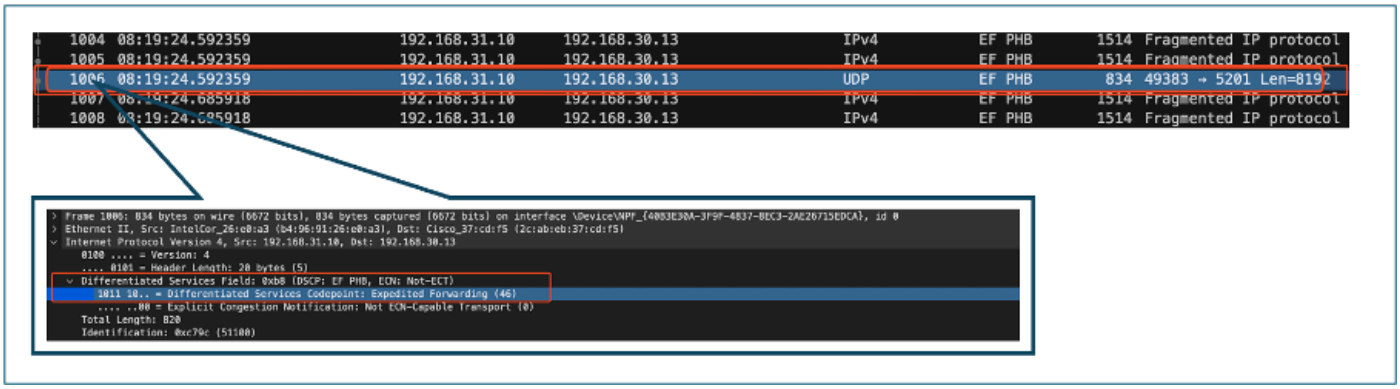
接下来，让我们研究一下在连接到有线PC的上行链路交换机上捕获的数据包。交换机信任DSCP标记，并且DSCP值保持在46不变。

注意：Catalyst 9000系列上的交换机端口默认为受信任状态。



有线PC上行链路接口捕获

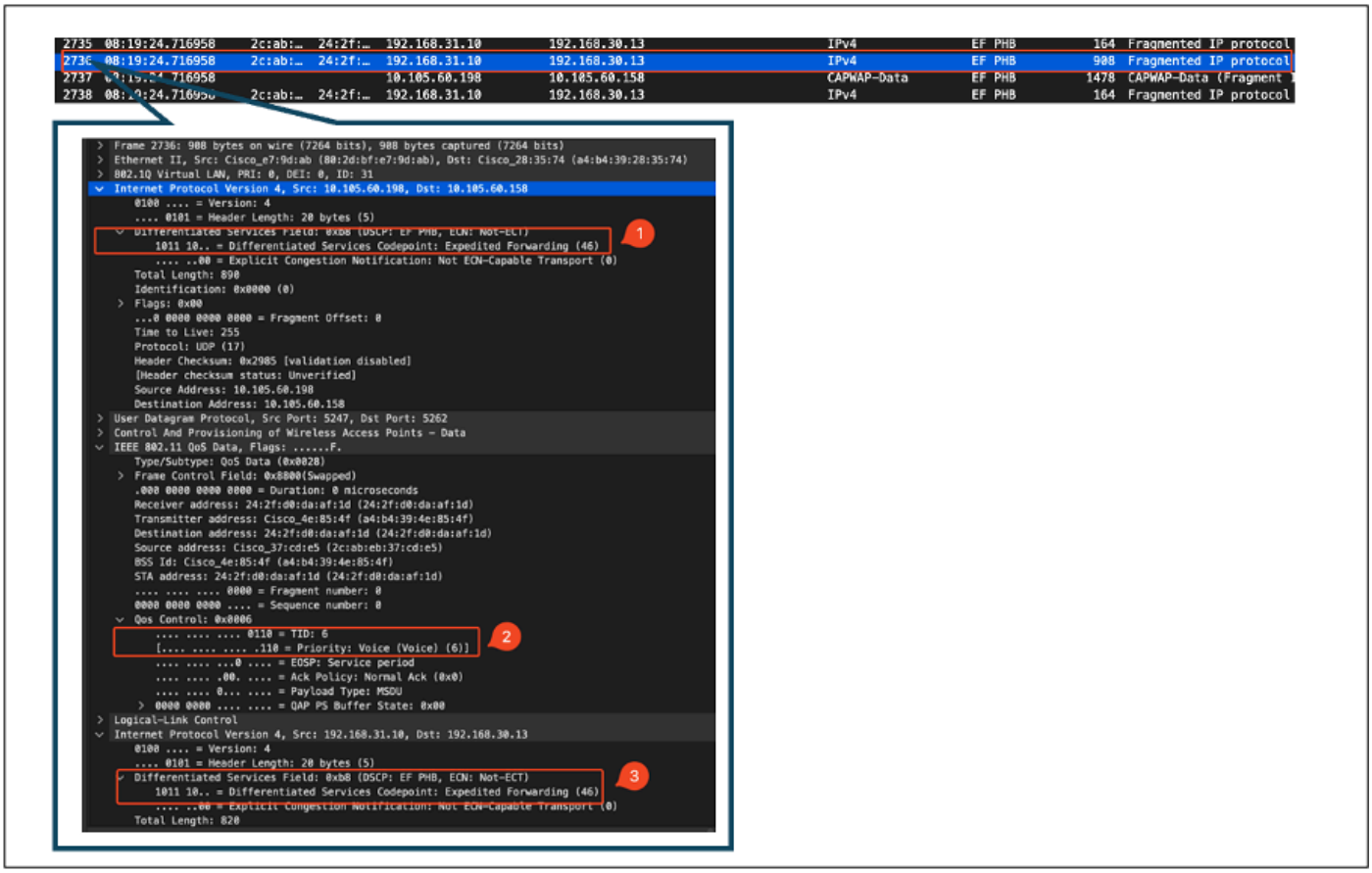
在检查使用EPC捕获的WLC上的数据包后，数据包从上行链路交换机以相同的DSCP标记46到达。这可以确认数据包到达WLC时保留了DSCP标记。



WLC EPC下行方向

当WLC将数据包发送到CAPWAP隧道内的AP时，它是WLC可以根据其配置修改DSCP的关键交叉点。让我们来分解数据包捕获，为清楚起见，它以编号点突出显示：

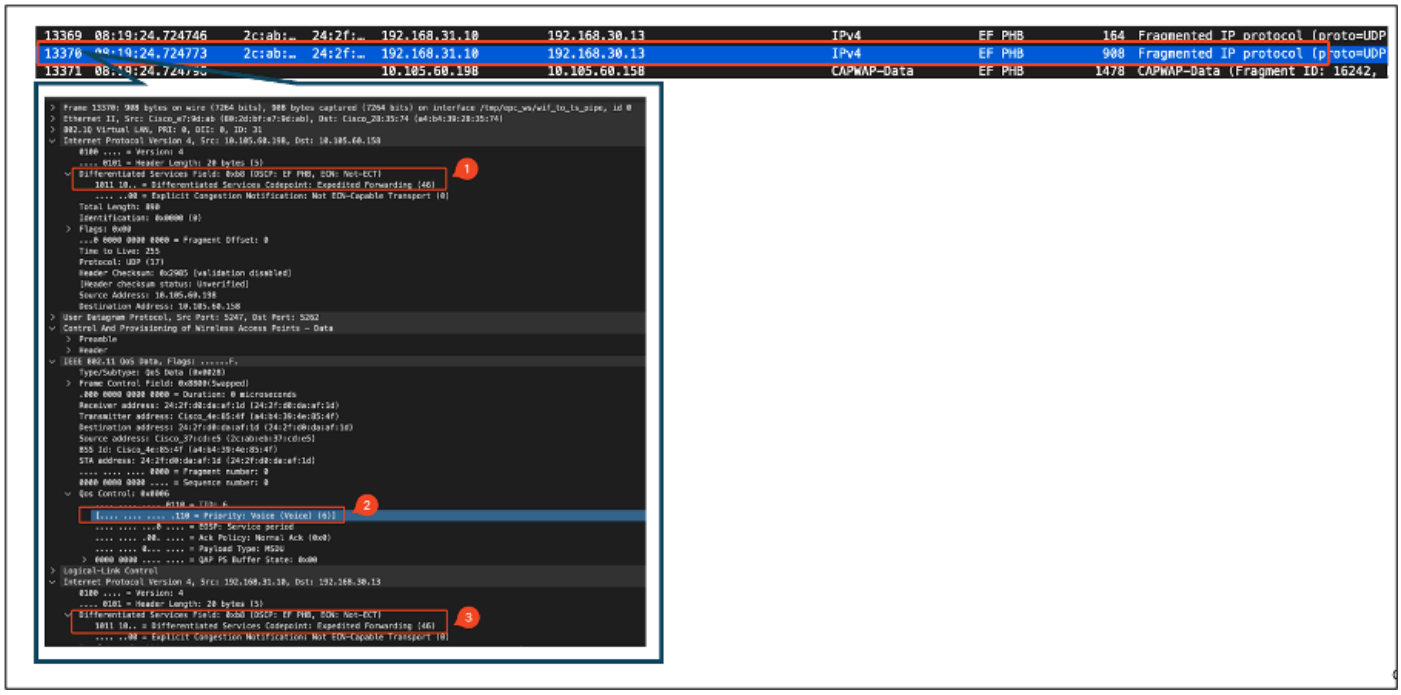
- CAPWAP外层： CAPWAP隧道的外层将DSCP标记显示为46，这是从交换机端接收的值。
- CAPWAP内部的802.11 UP值：CAPWAP隧道WLC将DSCP 46映射为对应于语音流量的802.11用户优先级(UP) 6。
- CAPWAP内部的DSCP值：Cisco 9800 WLC使用信任DSCP模型运行，因此CAPWAP隧道内部的DSCP值保持在与外部DSCP层相同的46。



CAPWAP DSCP标记

接下来，在AP上行链路交换机端口上检查同一个数据包。

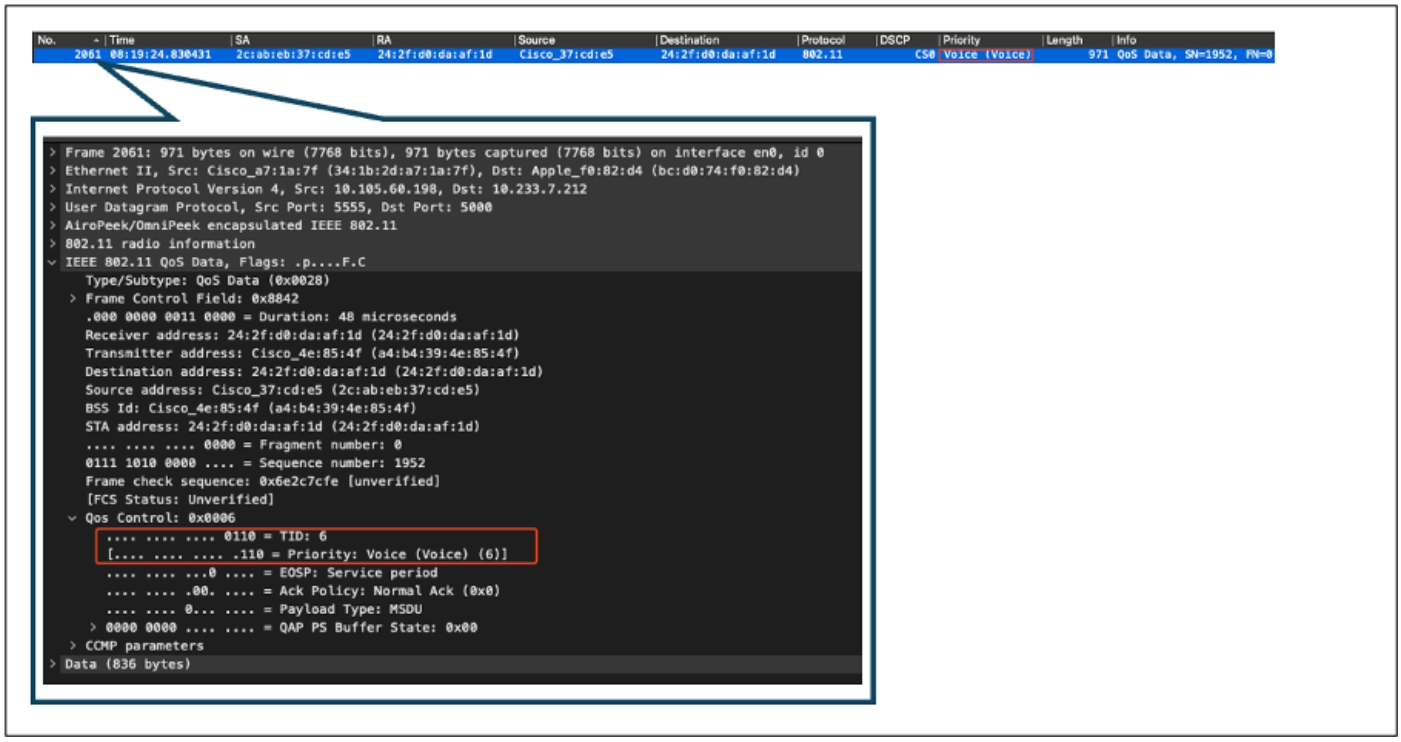
外部CAPWAP层上的DSCP值保持在46。为了说明目的，内部CAPWAP流量突出显示，以显示标记。



AP上行链路交换机接口捕获

一旦AP收到数据包，它就会通过空中传输数据包。为了验证用户优先级(UP)标记，使用通过嗅探器AP进行的空中(OTA)捕获。

AP已转发了UP值为6的帧。这确认AP将DSCP值正确映射到与语音流量对应的适当802.11 UP值(6)。

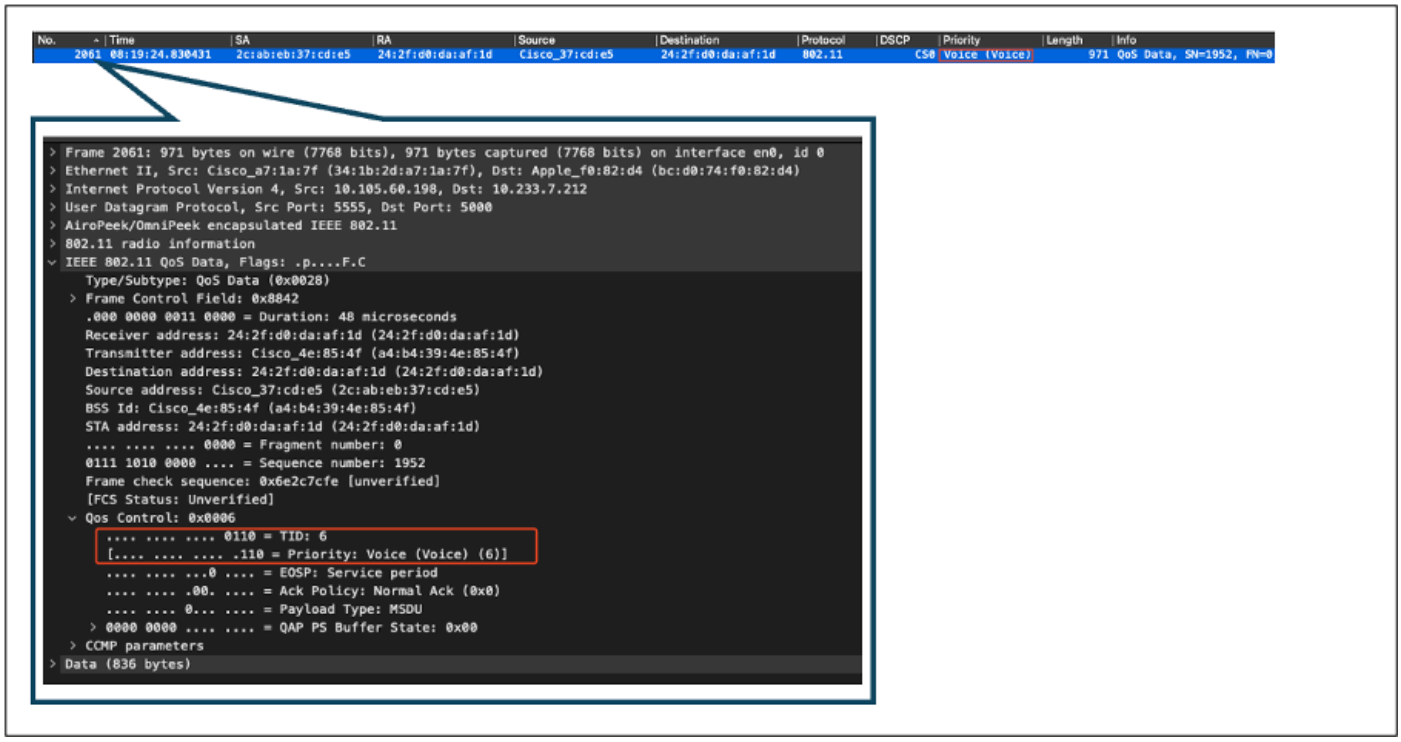


从AP到客户端的OTA捕获

在最后阶段，无线PC接收的数据包。无线PC收到DSCP值为46的帧。

这表示从有线PC到无线PC的整个传输路径中都保留了DSCP标记。一致的DSCP值46证实QoS策略

在下游方向被正确应用和维护。



无线PC捕获

测试场景2：上行QoS验证

在此测试场景中，目的是验证上行QoS配置。设置涉及无线PC使用DSCP 46向有线PC发送UDP数据包。WLC配置了上行和下行方向的金属“白金级QoS”策略。

- 通信流:

来源：无线PC

目的：有线PC

流量类型：DSCP为46的UDP数据包

- WLC上的QoS策略配置：

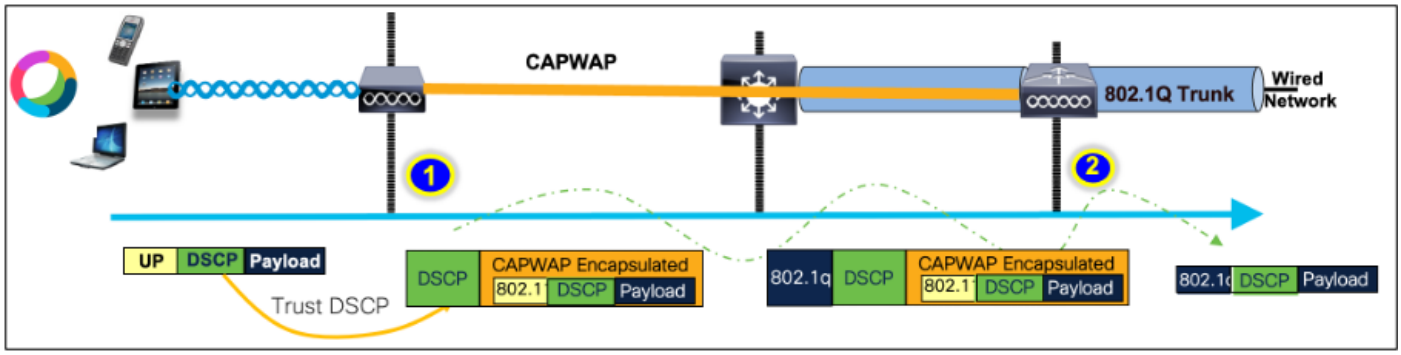
QoS配置文件：白金级QoS

方向：上行和下行

- 金属QoS配置命令：

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

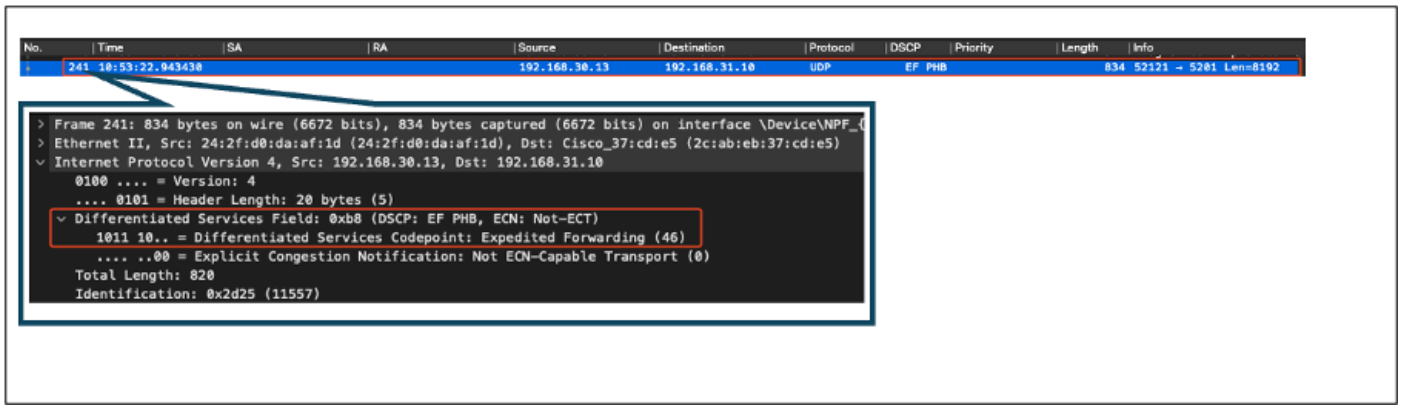
上行方向的逻辑拓扑和DSCP转换：



逻辑拓扑和DSCP转换-上行

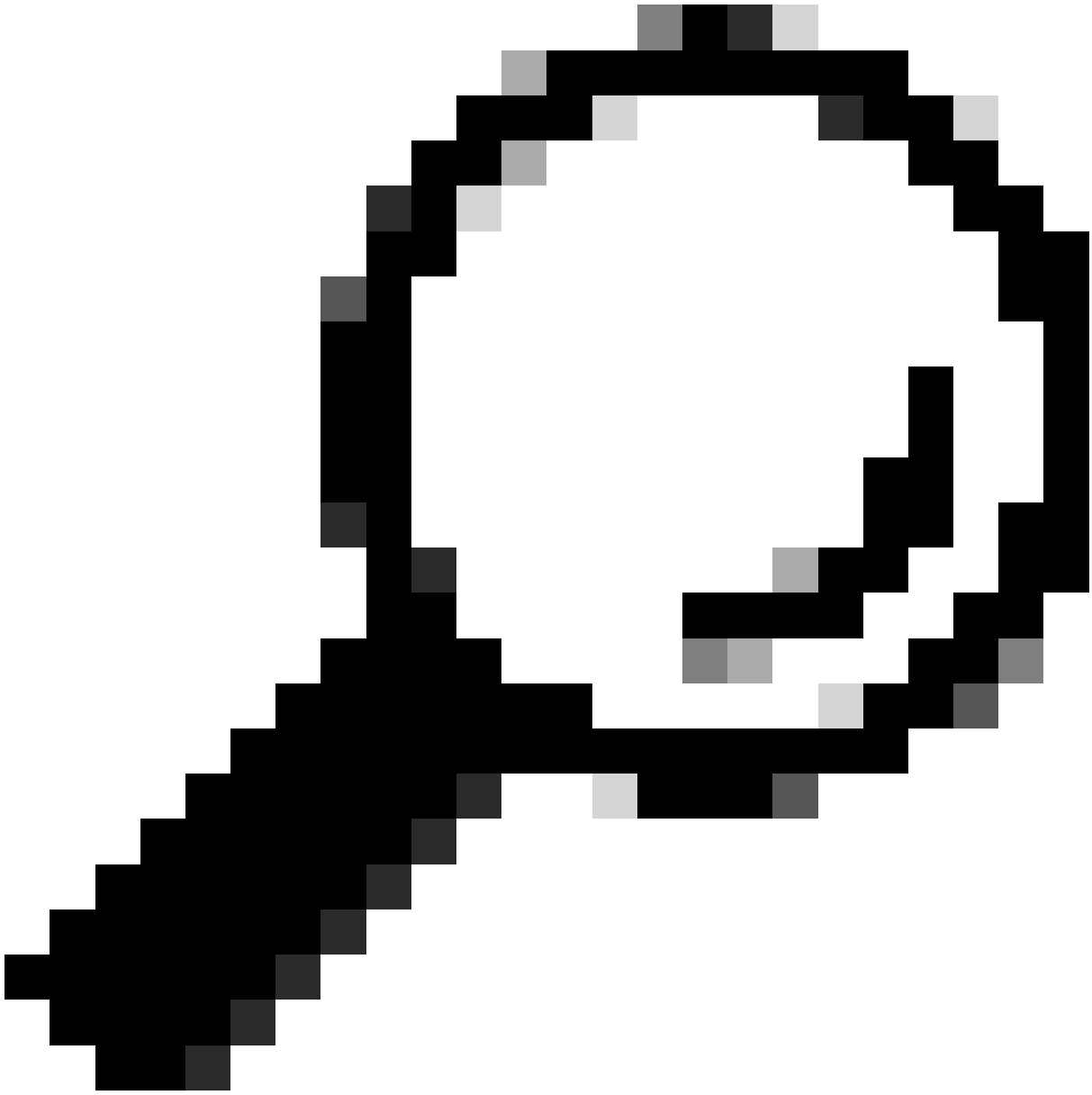
从无线PC发送到有线PC的数据包。此捕获是在无线PC上捕获的。

无线PC使用DSCP 46发送UDP数据包。

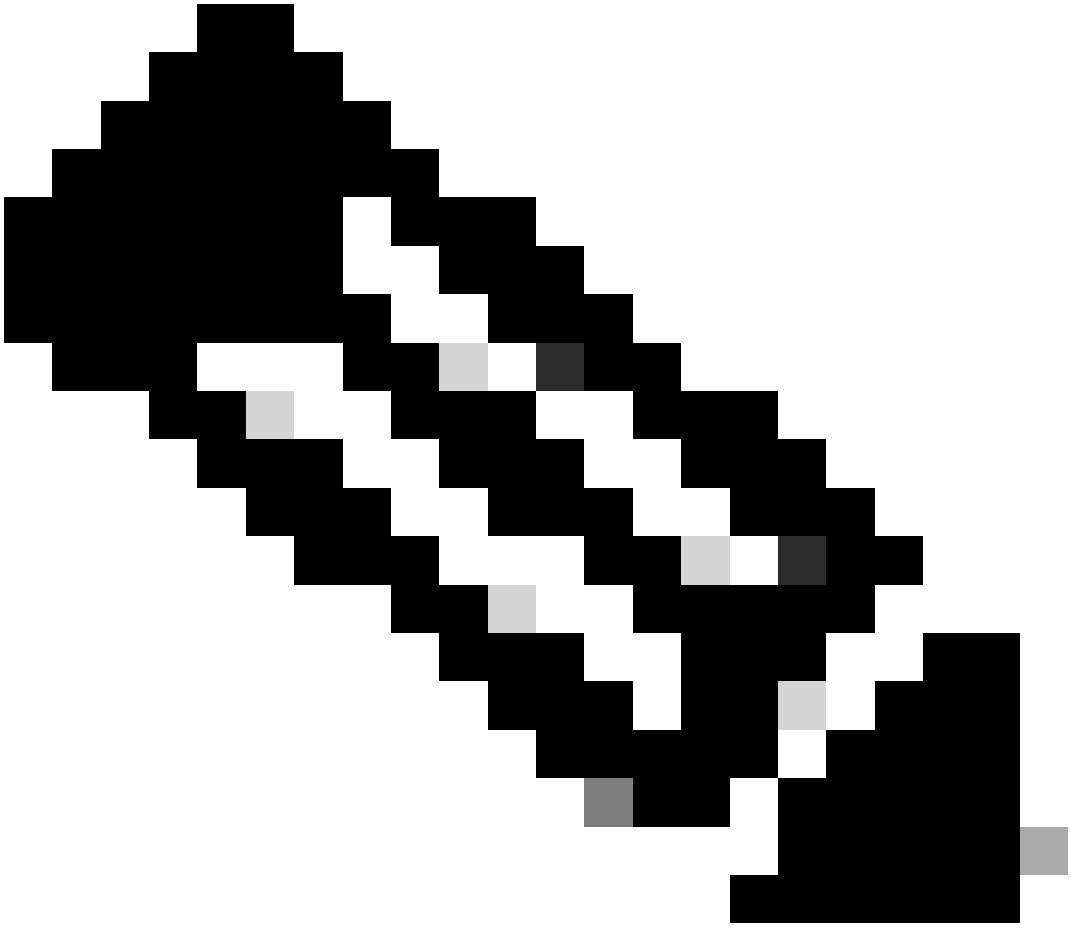


上行方向的无线PC捕获

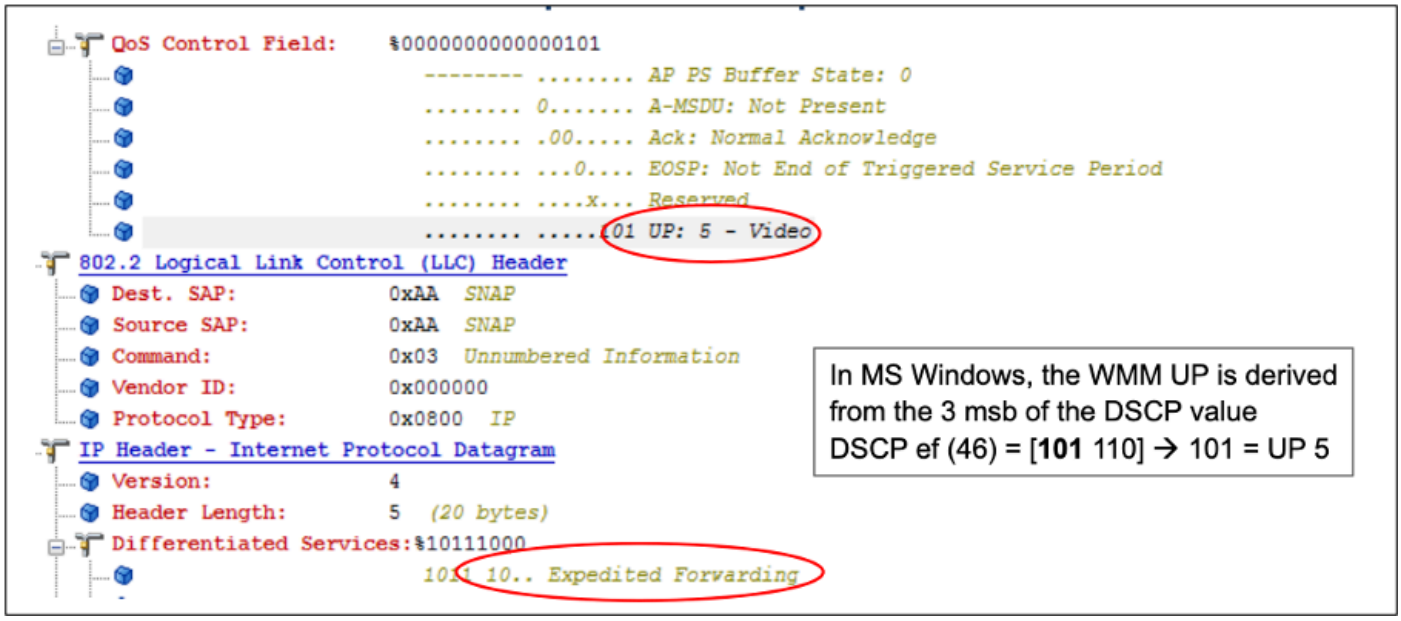
接下来，让我们了解从客户端到AP的OTA捕获。



提示：使用Windows无线PC发送DSCP 46的数据包时，Windows会将DSCP 46映射到用户优先级(UP)值为5（视频）。因此，OTA捕获将数据包显示为视频流量(UP 5)。但是，如果解密数据包，则DSCP值保持在46。



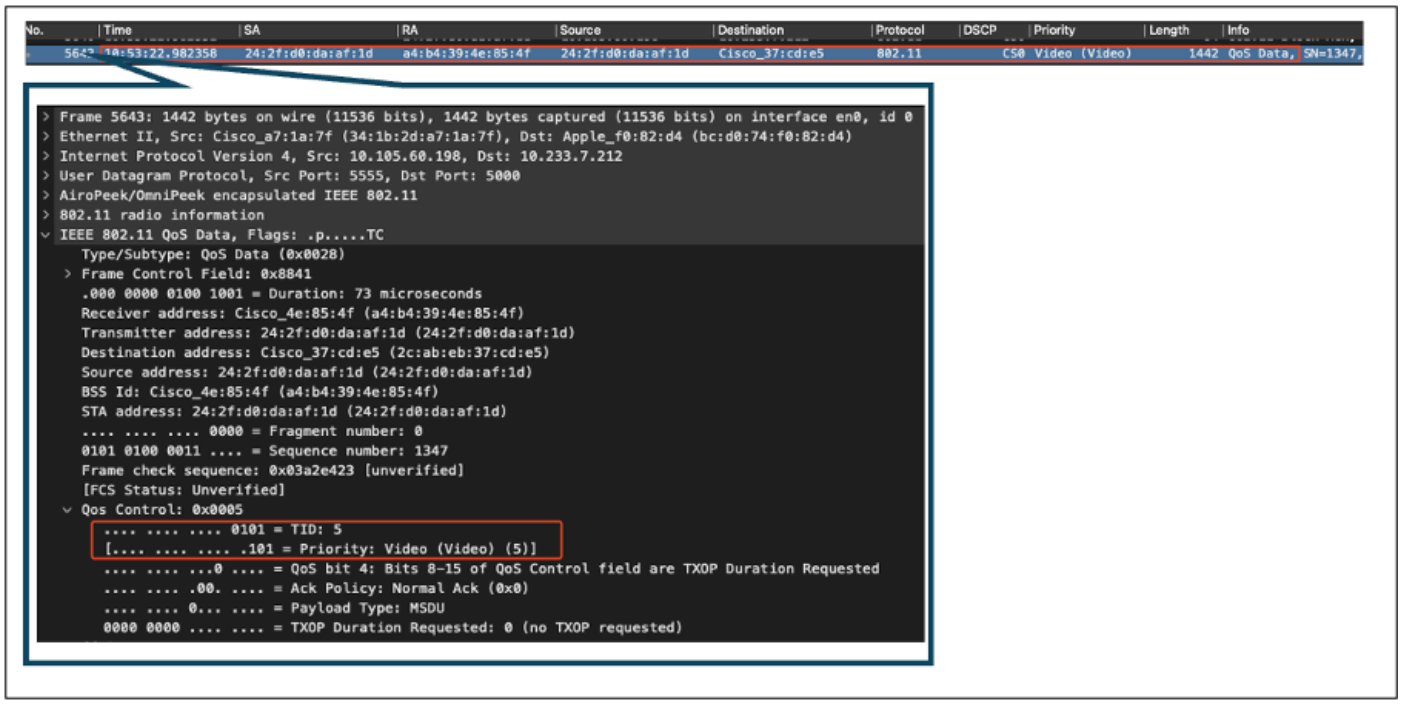
注意：从版本17.4开始，Cisco 9800 WLC的默认行为是信任AP加入配置文件中的DSCP值。这可以确保WLC保留并信任DSCP值46，从而防止任何与Windows DSCP到UP映射行为相关的问题。



Windows UP到DSCP的映射

对从实验室设置获取的加密无线传输(OTA)捕获进行分析，以验证上行QoS配置。

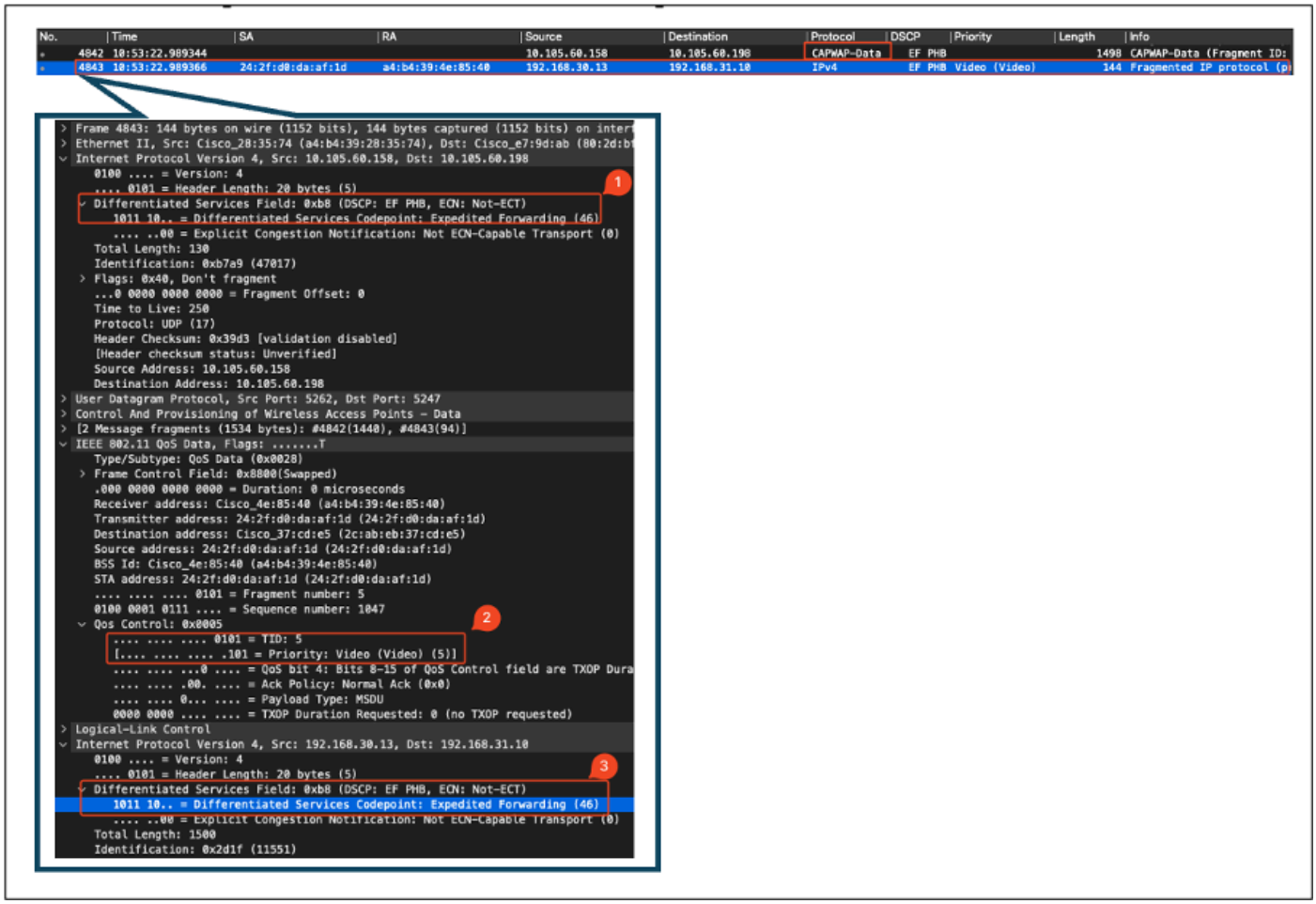
OTA捕获显示用户优先级(UP)值为5（视频）的数据包。虽然OTA捕获显示UP 5，但加密数据包中的DSCP值仍为46。



LAB在上游方向设置OTA

接下来，分析AP上行链路端口上的数据包捕获，确保数据包从AP移动到WLC时保留DSCP值。

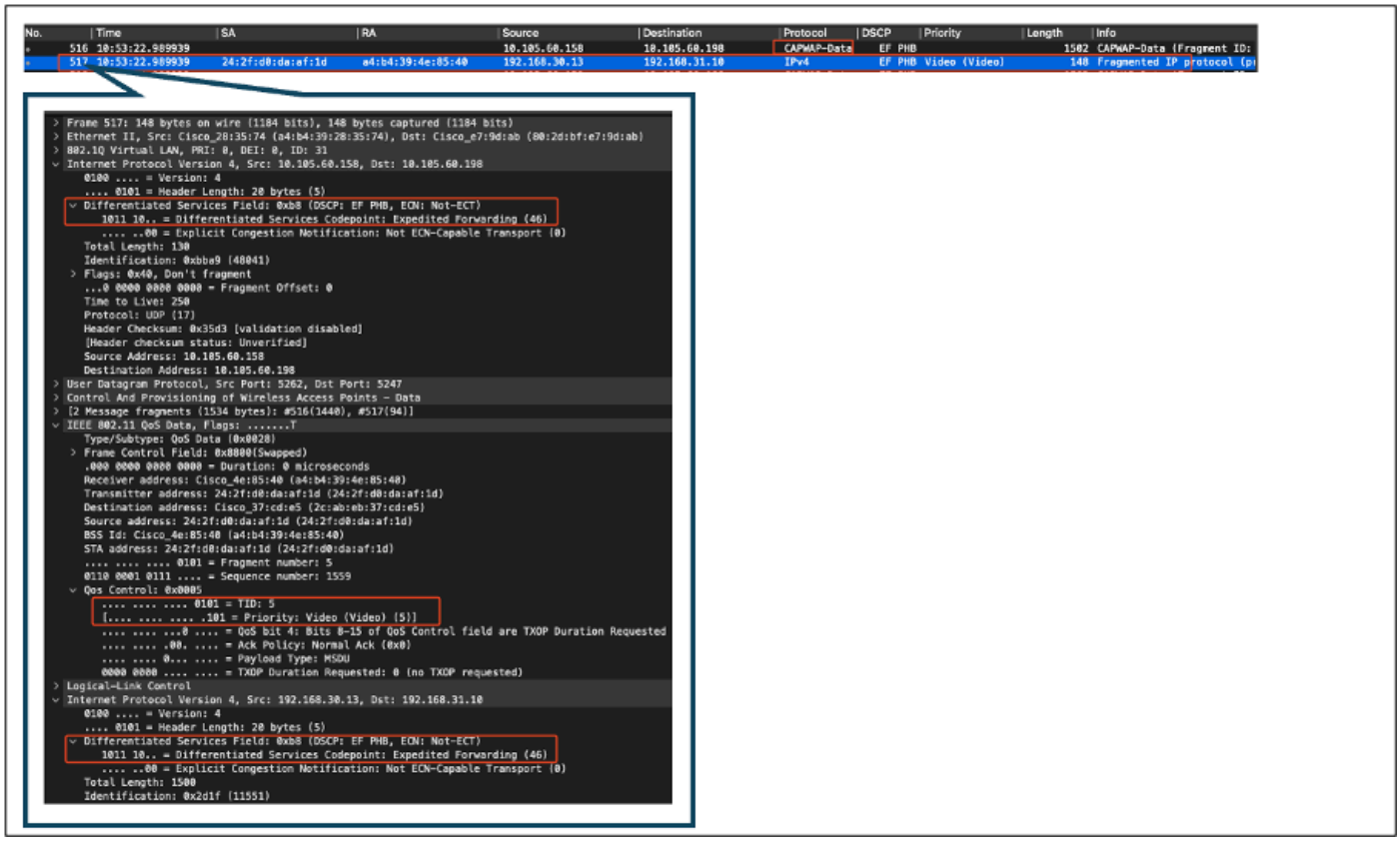
- 外部CAPWAP层上的DSCP值保持在46。
- 在CAPWAP隧道内，DSCP值也保持在46。



上行方向的AP Pplink捕获

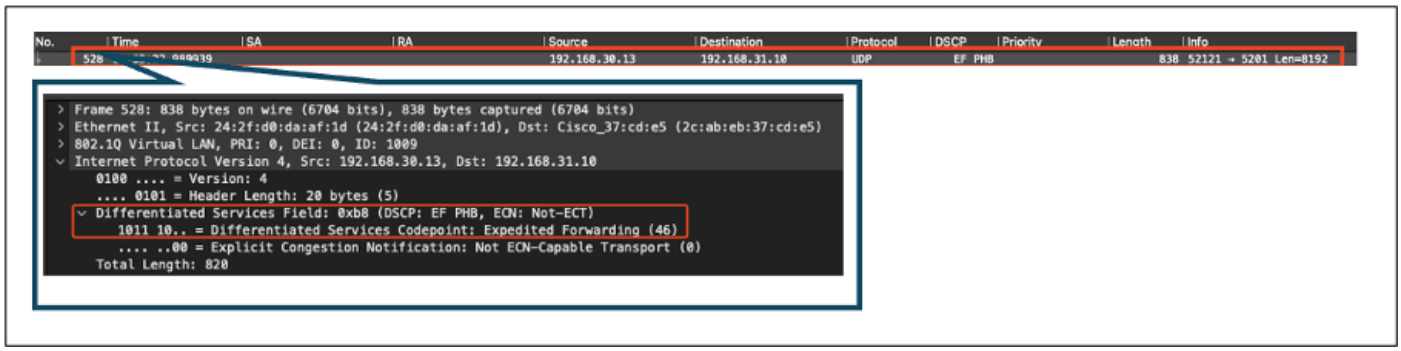
当数据包从交换机到达时，捕获在WLC上。

- 数据包到达外部CAPWAP层上的DSCP值为46的WLC。
- 在CAPWAP隧道内，DSCP值保持在46。



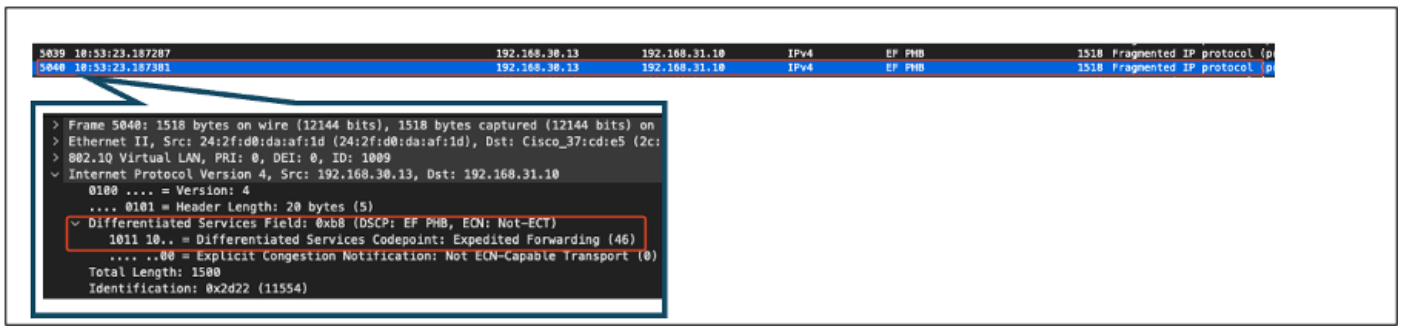
显示来自AP的数据包的WLC EPC

当数据包在WLC上发生发夹转弯后，它将被发送回上行链路交换机，目标为有线PC。WLC转发DSCP值为46的数据包。



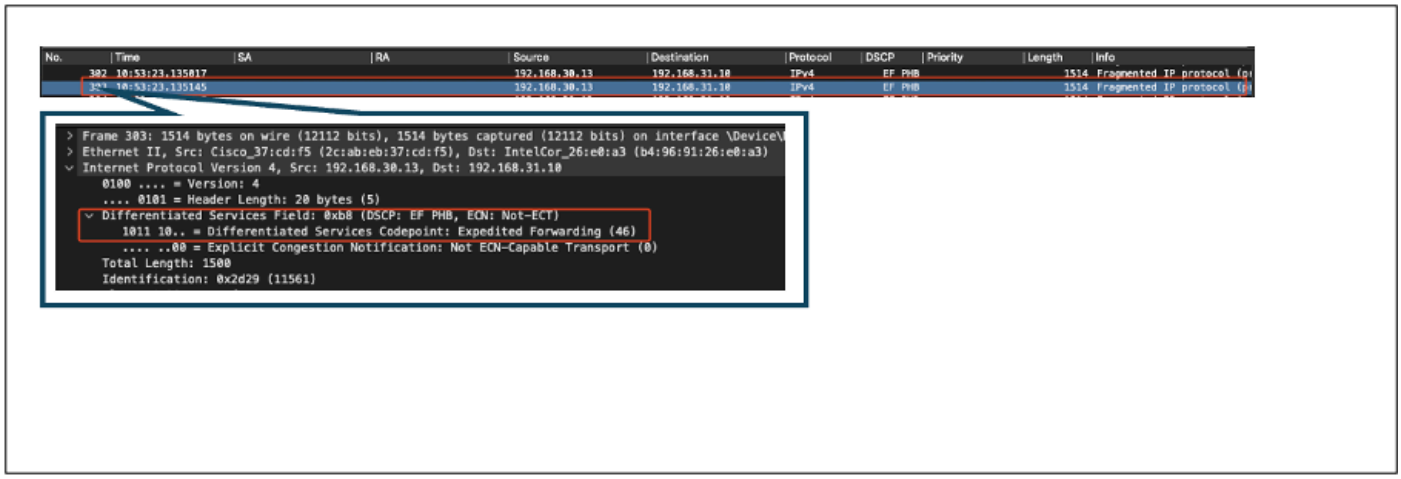
显示发送到有线PC的数据包的WLC EPC

最后，分析有线PC上行链路上的数据包捕获，确保数据包从WLC到达时保留DSCP值。



上行方向有线PC上行链路交换机捕获

在最后阶段，分析有线PC收到的数据包，确保数据包到达DSCP值为46的有线PC。



有线PC捕获-上行方向

上行QoS测试成功验证了从无线PC流向有线PC的流量的QoS配置。在整个传输路径中将DSCP值一致保留为46可确认QoS策略已正确应用和实施。

故障排除

语音、视频和其他实时应用对网络性能问题尤其敏感，服务质量(QoS)的任何降低都可能产生显著的不利影响。使用较低的DSCP值重新标记QoS数据包时，对语音和视频的影响可能很大。

对语音的影响：

- 延迟增加：语音通信要求低延迟，以确保对话自然、流畅。较低的DSCP值可能导致语音数据包延迟，导致明显的会话延迟。
- 抖动：数据包到达时间变化（抖动）可能会中断语音数据包的顺利传输。这会导致音频不稳定或损坏，从而难以理解扬声器。
- 丢包：语音数据包对丢包非常敏感。即使少量数据包丢失也会导致单词或音节丢失，从而导致通话质量下降和误解。
- 回声和失真：延迟和抖动增加可能导致回声和音频失真，进一步降低语音呼叫的质量。

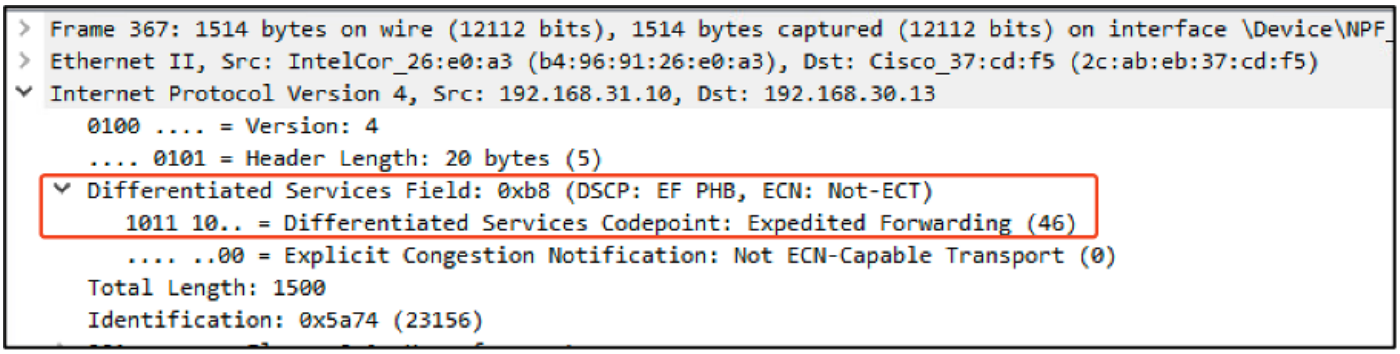
对视频的影响：

- 延迟增加：视频通信需要低延迟以保持音频和视频流之间的同步。延迟增加会导致延迟，从而难以进行实时交互。
- 抖动：抖动可能导致视频帧不按顺序或以不规则的间隔到达，从而导致视频体验抖动或断断续续。
- 丢包：丢包可能导致帧丢失，从而导致视频冻结或显示人为因素。
- 视频质量降低：DSCP值降低可能导致视频流的带宽分配减少，从而导致分辨率降低和视频质量变差。这样在视频中很难看到重要的细节。

场景1：中间交换机重写DSCP标记

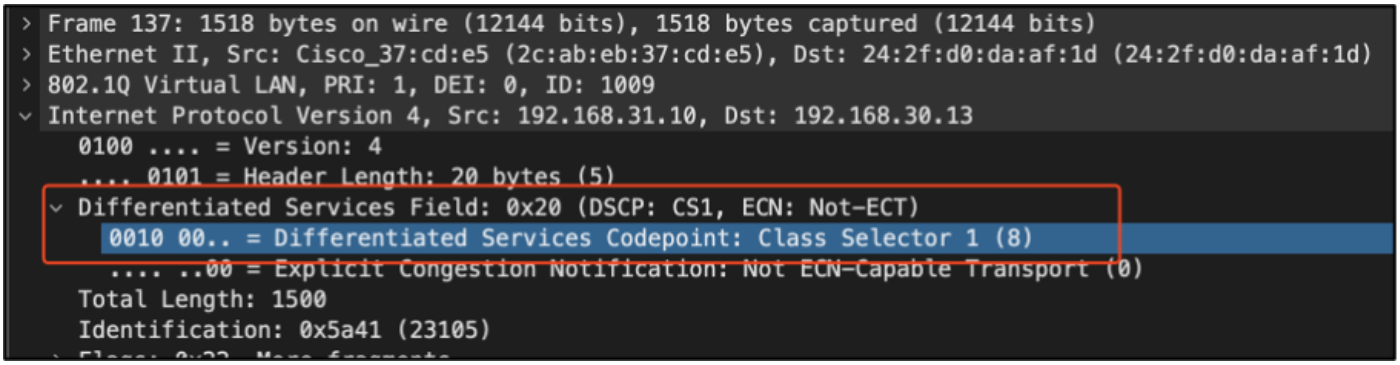
在此故障排除方案中，研究了中间交换机在流量到达WLC时重写DSCP标记对流量的影响。要复制此信息，交换机配置为在有线PC上行链路接口上将DSCP 46标记重写为CS1。

数据包从带DSCP 46标记的有线PC发送。



带DSCP 46标记的有线PC发送数据包

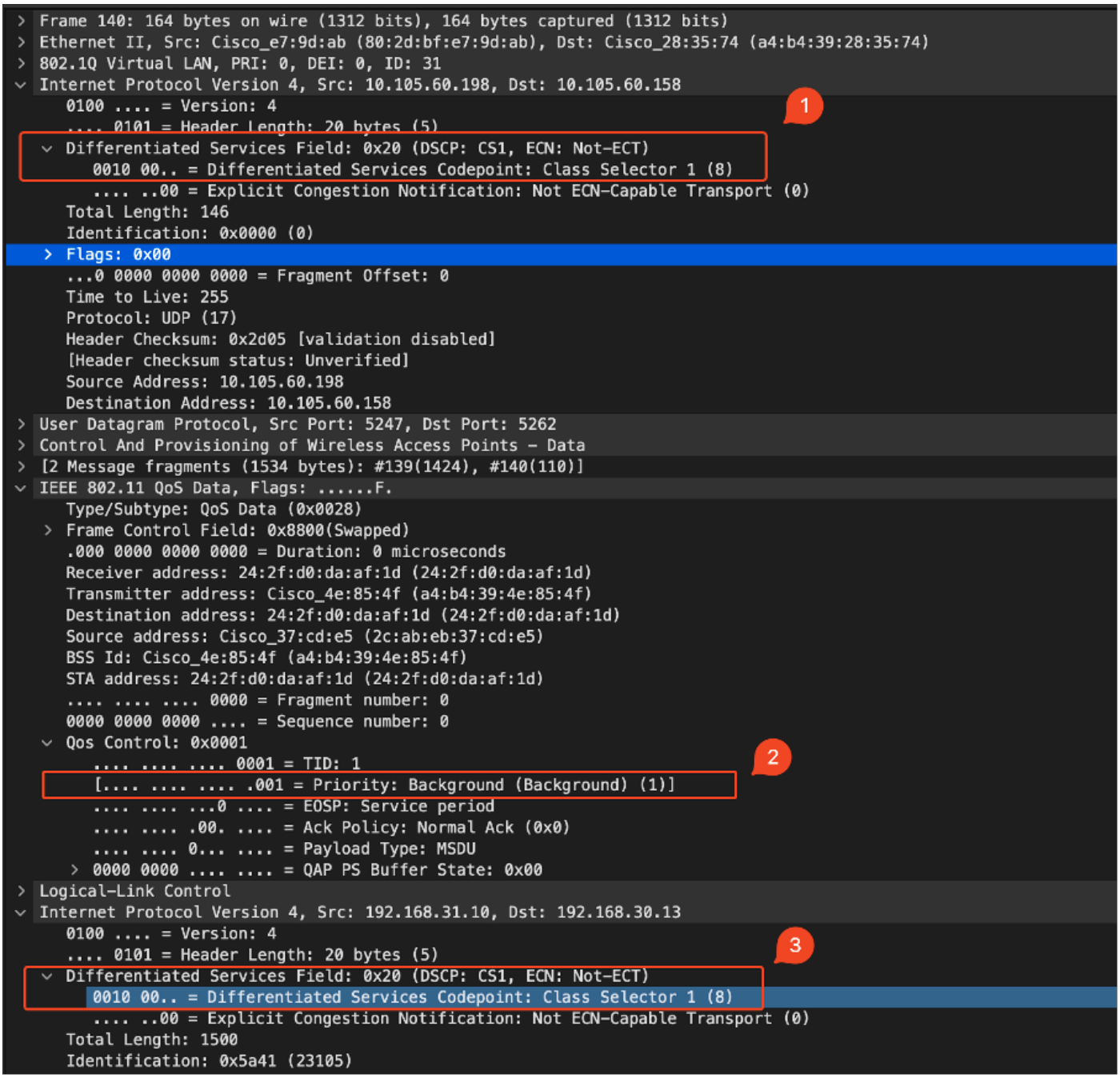
数据包到达WLC时，其DSCP值为CS1 (DSCP 8)。从DSCP 46更改为DSCP 8会显著降低数据包的优先级。



显示CS1标记的WLC EPC

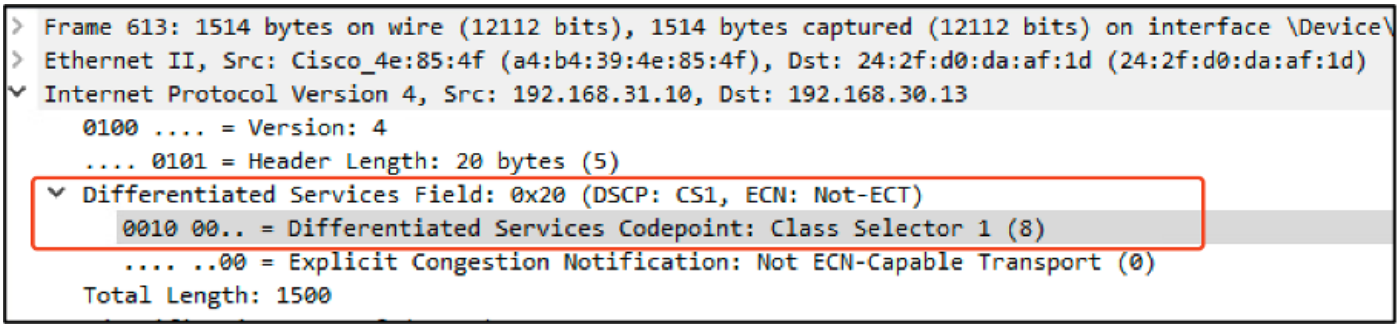
在此步骤中，将分析WLC转发到AP的数据包。

- 外部CAPWAP报头使用CS1 (DSCP 8)进行标记。
- 内部CAPWAP报头也使用CS1 (DSCP 8)进行标记。
- 用户优先级(UP)值设置为BK（后台）。



显示CAPWAP流量中的CS1标记的WLC EPC

数据包使用DSCP值CS1 (DSCP 8)到达无线PC。



显示CS1标记的无线PC捕获

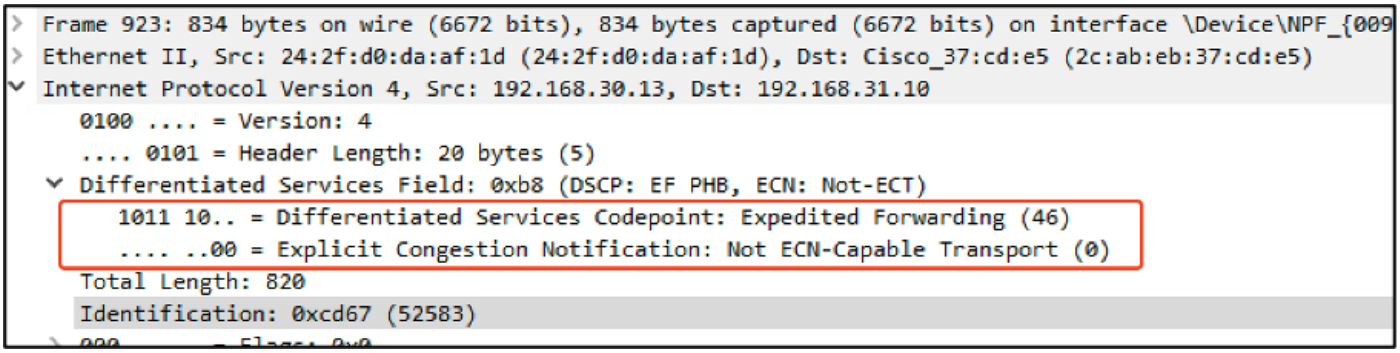
此场景演示了中间交换机上的配置错误如何破坏QoS配置，从而导致高优先级流量的性能下降。由

于DSCP重写，最初标记为高优先级的语音数据包被视为低优先级流量。此场景强调了确保中间网络设备正确保留QoS标记以保持高优先级流量所需服务质量的重要性。

场景2：AP链路交换机重写DSCP标记

在此场景中，调查连接到AP的中间交换机重写DSCP标记对流量的影响。

- 连接到AP的交换机配置为在AP上行链路接口上将DSCP 46标记重写为不同的值CS1。
- 数据包从有线PC发送，DSCP标记为46。这确认在源位置使用DSCP 46正确标记了流量。

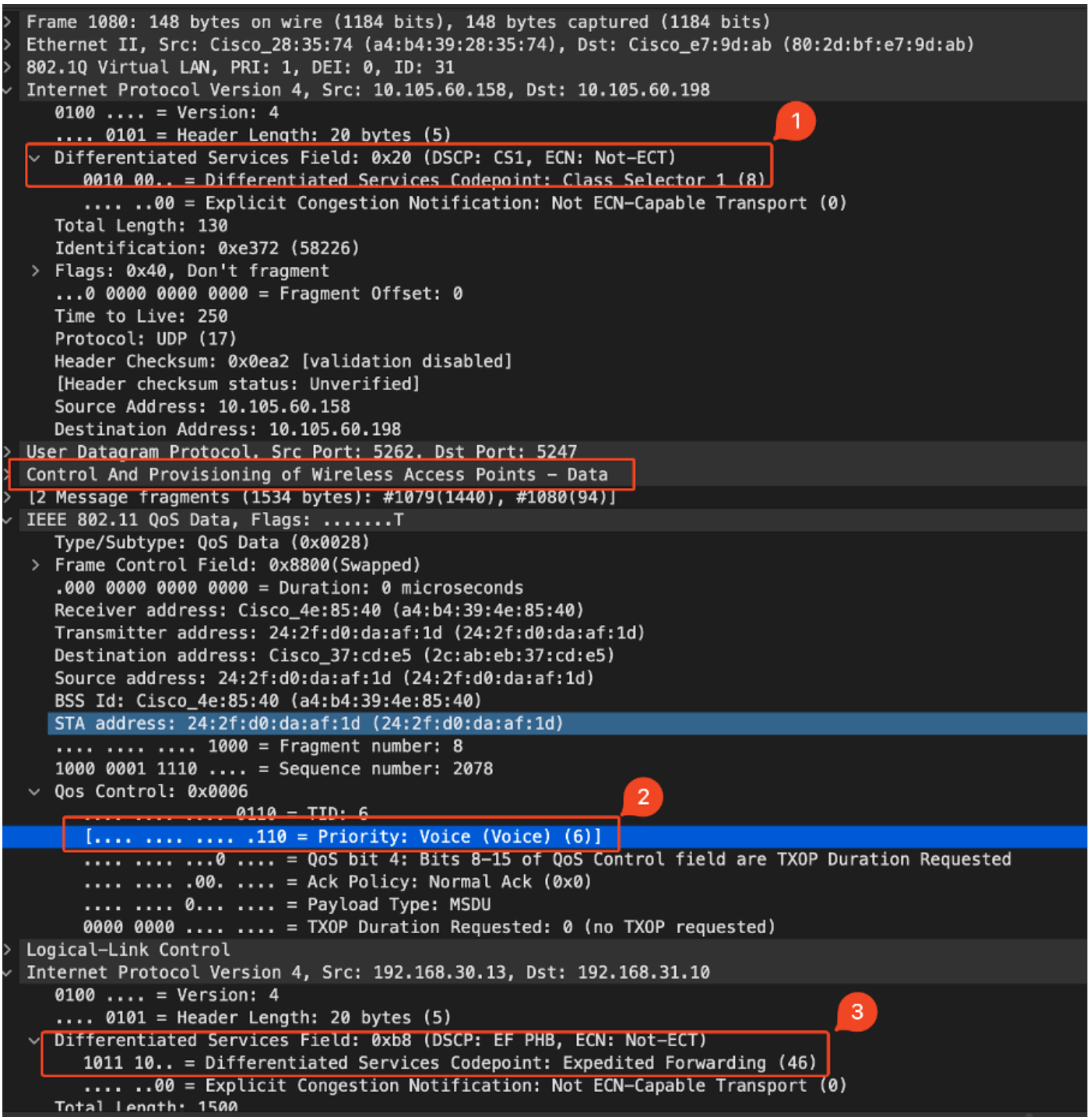


显示DSCP 46的无线PC捕获

当数据包从交换机到达时，捕获在WLC上。

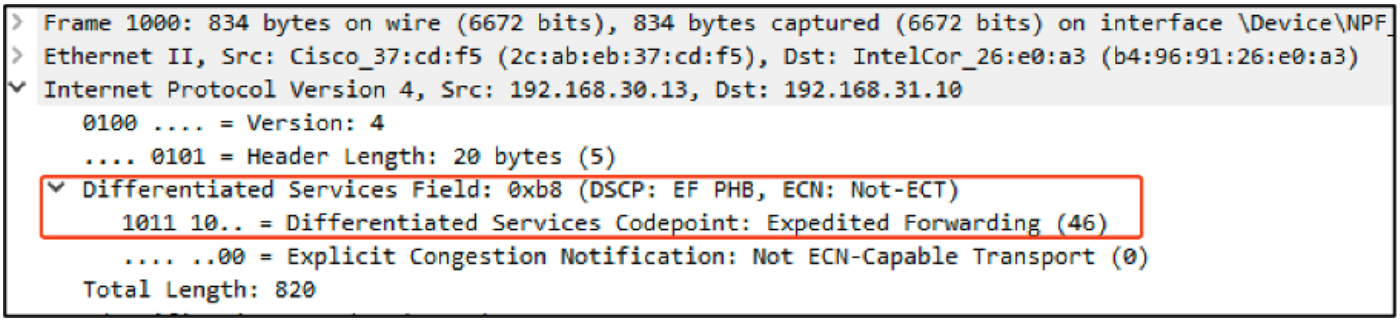
数据包到达WLC时，外部CAPWAP报头DSCP值为CS1(DSCP 和内部DSCP值为46)。发生这种情况是因为中间交换机无法看到封装在CAPWAP隧道内的流量。

WLC信任CAPWAP隧道内的DSCP标记，并将流量转发到具有内部DSCP标记46的有线PC。



显示CAPWAP DSCP值的WLC EPC

数据包到达有线PC时的DSCP值为46。确认WLC正确转发原始DSCP值为46的数据包，同时保留高优先级标记。



虽然WLC使用DSCP标记46转发流量，但必须了解从AP到WLC的流量被视为低优先级，因为外部DSCP标记被重写到CS1 (DSCP 8)。

在AP和WLC之间可以有多个交换机，并且如果为流量分配较低的优先级，那么它可能会延迟到达WLC。这会导致延迟、抖动和潜在的数据包丢失增加，从而降低语音等高优先级流量的服务质量。

故障排除提示

1. 验证初始DSCP标记：在源位置（例如有线PC）捕获数据包，以确保流量已正确标记为预期的DSCP值。
2. 检查中间设备配置：检查所有中间交换机和路由器的配置，确保它们不会无意中重写DSCP值。
3. 在关键点捕获流量：
    1. 中间交换机前后。
    2. 在WLC上。
    3. 在目的地址（例如，无线PC）。
4. 模拟流量场景：使用流量生成器或网络模拟工具创建不同类型的流量，并观察无线网络如何处理QoS。
5. 请参阅9800最佳做法文档：查看有关配置QoS和DSCP标记的9800最佳做法文档。

配置验证

<#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
```

结论

在整个网络中保持一致的QoS配置对于确保高优先级流量（如语音和视频）获得适当的服务和性能水平至关重要。定期验证QoS配置以确保所有网络设备都符合预期的QoS策略至关重要。此验证有助于确定并纠正任何可能影响网络性能的错误配置或偏差。

参考

- 了解Cisco Catalyst 9800系列无线控制器并进行故障排除
- Cisco Catalyst 9800系列配置最佳实践
- Cisco Catalyst 9800系列无线控制器软件配置指南，Cisco IOS® XE都柏林17.12.x
- 无线局域网语音(VoWLAN)故障排除指南
- 在Windows计算机上启用DSCP QoS标记

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。