融合接入控制器和轻量AP上的QoS配置示例

目录

简介

本文档介绍如何在具有轻量接入点(LAP)的思科融合接入网络中配置QoS，以及如何使用Cisco Catalyst 3850交换机或Cisco 5760无线LAN控制器(WLC)。

先决条件

要求

Cisco 建议您了解以下主题：

- 有关如何配置LAP和思科融合接入控制器的基本知识
- 关于如何在有线网络中配置基本路由和 QoS 的知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行Cisco IOS的Cisco Catalyst 3850交换机?XE软件版本3.2.2(SE)
- 运行Cisco IOS XE软件版本3.2.2(SE)的Cisco 5760无线局域网控制器
- 思科3600系列轻量接入点

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

QoS 是指网络向一系列用户或应用提供对其他用户或应用有损害的更好或特别服务的能力。

借助QoS，可以跨LAN(包括无线LAN(WLAN)和WAN)更高效地管理带宽。QoS通过以下服务提供增强的可靠网络服务：

- 支持重要用户和应用指定的专用带宽.
- 控制实时流量所需的抖动和延迟。
- 管理并将网络拥塞减至最低.
- 形成网络流量，以便使流量流畅。
- 设置网络流量优先级.

在过去，WLAN 主要用于传输低带宽、数据应用流量。随着WLAN扩展到垂直（如零售、金融和教育）和企业环境，WLAN现在被用于与时间敏感的多媒体应用一起传输高带宽数据应用。此要求导致了无线 QoS 的必要性。

IEEE 802.11标准委员会内的IEEE 802.11e工作组已完成标准定义，Wi-Fi联盟已创建Wi-Fi多媒体(WMM)认证，但802.11e标准的采用仍然有限。大多数设备都通过WMM认证，因为802.11n和802.11ac认证需要WMM认证。许多无线设备不会为发送到数据链路层的数据包分配不同的QoS级别，因此这些设备发送大部分流量时没有QoS标记，也没有相对优先级。但是，大多数802.11无线局域网语音(VoWLAN)IP电话确实会标记其语音流量并确定其优先级。本文档重点介绍VoWLAN IP电话的QoS配置以及标记其语音流量的支持视频的wi-fi设备。

注意：不执行内部标记的设备的QoS配置不在本文档的范围内。

802.11e修正版定义了八个用户优先级(UP)级别，将二乘二分为四个QoS级别（访问类别）：

- 白金级/语音（UP 7和6） — 确保无线语音的高质量服务。
- 金牌/视频（UP 5和4） — 支持高质量视频应用。
- 银牌/尽力服务（UP 3和0） — 支持客户端的正常带宽。这是默认设置。
- 铜级/后台（UP 2和1） — 为访客服务提供最低带宽。

白金常用于VoIP客户端，黄金用于视频客户端。本文档提供了一个配置示例，说明如何在控制器上配置QoS并与为VoWLAN和视频客户端配置了QoS的有线网络通信。

L3 QoS数据包标记增强功能

思科融合接入控制器支持WLC和LAP发送的数据包的第3层(L3)IP差分服务代码点(DSCP)标记。此功能增强了接入点(AP)使用此L3信息的方式，以确保数据包从AP接收到无线客户端的正确空中优先级。

在使用Catalyst 3850交换机作为无线控制器的融合接入WLAN架构中，AP直接连接到交换机。在使用5760控制器的融合接入WLAN架构中，WLAN数据通过无线接入点控制和调配(CAPWAP)协议在AP和WLC之间隧道传输。为了在此隧道中保持原始QoS分类，封装数据包的QoS设置必须正确映射到外部隧道数据包的第2层(L2)(802.1p)和第3层(IP DSCP)字段。

为VoWLAN和视频配置QoS时，可以为无线客户端配置特定QoS策略，为WLAN配置特定策略，或同时配置两者。您还可以使用特定于连接AP的端口的配置来补充设置，特别是使用Catalyst 3850交换机。此配置示例重点介绍无线客户端、WLAN和AP端口的QoS配置。VoWLAN和视频应用的QoS配置的主要目标是：

- 识别上游和下游的语音和视频流量（流量分类和标记）。
- 将语音和视频流量标记为语音优先级： 802.11e UP 6、802.1p 5、DSCP 46（用于语音）。802.11e UP 5,DSCP 34，用于视频。
- 为语音流量、语音信令和视频流量分配带宽。

使用MQC配置无线网络以实现QoS

在配置QoS之前，必须配置Catalyst 3850交换机或Cisco 5760 WLC的无线控制器模块(WCM)功能，以执行基本操作，并将LAP注册到WCM。本文档假设WCM已配置为基本操作，并且LAP已注册到WCM。

融合接入解决方案使用模块化QoS(MQC)命令行界面(CLI)。 有关在Catalyst 3850交换机上的QoS配置中使用MQC的更多信息，请参阅《QoS配置指南， Cisco IOS XE版本3SE（Catalyst 3850交换机）》。

在融合接入控制器上配置带MQC的QoS依赖于四个要素：

- **类映射用**于识别所关注的流量。类映射可以使用各种技术（如现有QoS标记、访问列表或VLAN）来识别所关注的流量。
- **策略映射**用于确定应将哪些QoS设置应用于所关注的流量。策略映射呼叫类映射并将各种QoS设置（如特定标记、优先级、带宽分配等）应用到每个类。
- **服务策略**用于将策略映射应用于网络的战略点。在融合接入解决方案中，服务策略可应用于用户、服务集标识符(SSID)、AP无线电和端口。端口、SSID和客户端策略可由用户配置。无线电策略由无线控制模块控制。当流量从交换机或控制器流向无线客户端时，端口、SSID、客户端和无线电的无线QoS策略会在下游方向应用。
- **表映射用**于检查传入的QoS标记和确定传出的QoS标记。表映射位于应用于SSID的策略映射中。表映射可用于保留（复制）或更改标记。表映射也可用于创建有线和无线标记之间的映射。有线标记使用DSCP(L3 QoS)或802.1p(L2 QoS)。 无线标记使用用户优先级(UP)。 表映射通常用于确定每个感兴趣的UP应使用哪个DSCP标记，以及每个感兴趣的DSCP值应使用什么UP。表映射是融合接入QoS的基础，因为DSCP和UP值之间没有直接转换。

但是，DSCP到UP表映射也允许复*制指*令。在这种情况下，融合接入解决方案使用思科语音、视频和集成数据架构(AVVID)映射表来确定DSCP到UP或UP到DSCP的转换：

标签索引	密钥字段	传入值	外部DSCP	CoS	UP

0	不。	未勾选	0	0	0
1-10	DSCP	0-7	0-7	0	0
11-18	DSCP	8-15	8-15	1	2
19-26	DSCP	16-23	16-23	2	3
27-34	DSCP	24-31	24-31	3	4
35-46	DSCP	32-39	32-39	4	5
47-48	DSCP	40-47	40-47	5	6
49-63	DSCP	48-55	48-55	6	7
64	DSCP	56-63	56-63	7	7
65	CoS	0	0	0	0
66	CoS	1	8	1	2
67	CoS	2	16	2	3
68	CoS	3	24	3	4
69	CoS	4	32	4	5
70	CoS	5	40	5	6
71	CoS	6	48	6	7
72	CoS	7	56	7	7
73	UP	0	0	0	0
74	UP	1	8	1	1
75	UP	2	16	1	2
76	UP	3	24	2	3
77	UP	4	34	3	4
78	UP	5	34	4	5
79	UP	6	46	5	6
80	UP	7	46	7	7

默认硬编码策略

融合接入控制器启用可应用于WLAN的硬编码QoS策略配置文件。这些配置文件应用思科统一无线网络(CUWN)控制器管理员熟悉的金属策略（白金、金等）。如果您的目标不是创建为语音流量分配特定带宽的策略，而只是为了确保语音流量接收正确的QoS标记，您可以使用硬编码策略。硬编码策略可以应用于WLAN，并且在上游和下游方向上可能不同。

> **注意：**
>
> 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。
>
> 命令输出解释程序工具（仅限注册用户）支持某些 **show 命令。**使用输出解释器工具来查看 show 命令输出的分析。

白金

语音硬编码策略称为白金。无法更改名称。

以下是白金级QoS级别的下行策略：

```
Policy-map platinum
Class class-default
 set dscp dscp table plat-dscp2dscp
```

```
 set wlan user-priority dscp table plat-dscp2up
Table-map plat-dscp2dscp
   from 45 to 45
   from 46 to 46
   from 47 to 47
   default copy
Table-map plat-dscp2up
   from 34 to 4
   from 46 to 6
   default copy
```

这是白金级QoS级别的上游策略：

```
Policy-map platinum-up
   Class class-default
     set dscp wlan user-priority table plat-up2dscp

Table-map plat-up2dscp
   from 4 to 34
   from 5 to 34
   from 6 to 46
   from 7 to 8
   default copy
```

金牌

视频的硬编码策略称为gold。无法更改名称。

以下是黄金QoS级别的下游策略：

```
Policy Map gold
   Class class-default
     set dscp dscp table gold-dscp2dscp
     set wlan user-priority dscp table gold-dscp2u
Table Map gold-dscp2dscp
   from 45 to 34
   from 46 to 34
   from 47 to 34
   default copy

Table Map gold-dscp2up
   from 45 to 4
   from 46 to 4
   from 47 to 4
   default copy
```

以下是黄金QoS级别的上游策略：

```
Policy Map gold-up
   Class class-default
     set dscp wlan user-priority table gold-up2dscp

Table Map gold-up2dscp
   from 6 to 34
   from 7 to 34
   default copy
```

银牌

用于尽力而为的硬编码策略称为银牌。无法更改名称。

以下是银级QoS级别的下行策略：

```
Policy Map silver
   Class class-default
     set dscp dscp table silver-dscp2dscp
     set wlan user-priority dscp table silver-dscp2up

Table Map silver-dscp2dscp
   from 34 to 0
   from 45 to 0
   from 46 to 0
   from 47 to 0
   default copy
Table Map silver-dscp2up
   from 34 to 0
   from 45 to 0
   from 46 to 0
   from 47 to 0
   default copy
```

这是银级QoS级别的上游策略：

```
Policy Map silver-up
   Class class-default
     set dscp wlan user-priority table silver-up2dscp
Table Map silver-up2dscp
   from 4 to 0
   from 5 to 0
   from 6 to 0
   from 7 to 0
   default copy
```

铜级

后台流量的硬编码策略称为铜级。无法更改名称。

这是铜级QoS级别的下游策略：

```
Policy Map bronze
   Class class-default
     set dscp dscp table bronze-dscp2dscp
 set wlan user-priority dscp table bronze-dscp2up

Table Map bronze-dscp2dscp
   from 0 to 8
   from 34 to 8
   from 45 to 8
   from 46 to 8
   from 47 to 8
   default copy

Table Map bronze-dscp2up
   from 0 to 1
   from 34 to 1
   from 45 to 1
   from 46 to 1
```

```
   from 47 to 1
   default copy
```

这是铜级QoS级别的上游策略：

```
Policy Map bronze-up
   Class class-default
     set dscp wlan user-priority table bronze-up2dscp
Table Map bronze-up2dscp
   from 0 to 8
   from 1 to 8
   from 4 to 8
   from 5 to 8
   from 6 to 8
   from 7 to 8
   default copy
```

确定哪个表映射最符合给定SSID的目标流量后，即可将匹配策略应用到WLAN。在本示例中，一个策略应用于下游方向（从AP到无线客户端的输出），一个策略应用于上游方向（从无线客户端通过AP到控制器的输入）：

```
3850#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
3850(config)#wlan test1
3850(config-wlan)#service-policy output platinum
3850(config-wlan)#service-policy input platinum-up
3850(config-wlan)#end
3850#
```

检查WLAN配置以验证将哪个策略应用于WLAN:

```
3850#show wlan name test1
WLAN Profile Name     : test1
===============================================
Identifier                                    : 1
Network Name (SSID)                           : test1
Status                                        : Disabled
Broadcast SSID                                : Enabled
Maximum number of Associated Clients          : 0
AAA Policy Override                           : Disabled
Network Admission Control
 NAC-State                                   : Disabled
Number of Active Clients                      : 0
Exclusionlist Timeout                         : 60
Session Timeout                               : 1800 seconds
CHD per WLAN                                  : Enabled
Webauth DHCP exclusion                        : Disabled
Interface                                     : default
Interface Status                              : Up
Multicast Interface                           : Unconfigured
WLAN IPv4 ACL                                 : unconfigured
WLAN IPv6 ACL                                 : unconfigured
DHCP Server                                   : Default
DHCP Address Assignment Required              : Disabled
DHCP Option 82                                : Disabled
DHCP Option 82 Format                         : ap-mac
DHCP Option 82 Ascii Mode                     : Disabled
DHCP Option 82 Rid Mode                       : Disabled
QoS Service Policy - Input
 Policy Name                                 : platinum-up
 Policy State                                : Validation Pending
```

```
QoS Service Policy - Output
 Policy Name                                : platinum
 Policy State                               : Validation Pending
QoS Client Service Policy
 Input  Policy Name                         : unknown
 Output Policy Name                         : unknown
WMM                                          : Allowed
Channel Scan Defer Priority:
 Priority (default)                         : 4
 Priority (default)                         : 5
 Priority (default)                         : 6
Scan Defer Time (msecs)                      : 100
Media Stream Multicast-direct                : Disabled
CCX - AironetIe Support                      : Enabled
CCX - Gratuitous ProbeResponse (GPR)         : Disabled
CCX - Diagnostics Channel Capability         : Disabled
Dot11-Phone Mode (7920)                      : Invalid
Wired Protocol                               : None
Peer-to-Peer Blocking Action                 : Disabled
Radio Policy                                 : All
DTIM period for 802.11a radio                : 1
DTIM period for 802.11b radio                : 1
Local EAP Authentication                     : Disabled
Mac Filter Authorization list name           : Disabled
Accounting list name                         : Disabled
802.1x authentication list name              : Disabled
Security
   802.11 Authentication                     : Open System
   Static WEP Keys                           : Disabled
   802.1X                                    : Disabled
   Wi-Fi Protected Access (WPA/WPA2)         : Enabled
       WPA (SSN IE)                          : Disabled
       WPA2 (RSN IE)                         : Enabled
           TKIP Cipher                       : Disabled
           AES Cipher                        : Enabled
       Auth Key Management
           802.1x                            : Enabled
           PSK                               : Disabled
           CCKM                              : Disabled
   CKIP                                      : Disabled
   IP Security                               : Disabled
   IP Security Passthru                      : Disabled
   L2TP                                      : Disabled
   Web Based Authentication                  : Disabled
   Conditional Web Redirect                  : Disabled
   Splash-Page Web Redirect                  : Disabled
   Auto Anchor                               : Disabled
   Sticky Anchoring                          : Enabled
   Cranite Passthru                          : Disabled
   Fortress Passthru                         : Disabled
   PPTP                                      : Disabled
   Infrastructure MFP protection             : Enabled
   Client MFP                                : Optional
   Webauth On-mac-filter Failure             : Disabled
   Webauth Authentication List Name          : Disabled
   Webauth Parameter Map                     : Disabled
   Tkip MIC Countermeasure Hold-down Timer   : 60
Call Snooping                                : Disabled
Passive Client                               : Disabled
Non Cisco WGB                                : Disabled
Band Select                                  : Disabled
Load Balancing                               : Disabled
IP Source Guard                              : Disabled
```

手动配置

硬编码策略应用默认QoS标记，但不应用带宽分配。硬编码策略还假定流量已标记。在复杂环境中，您可能希望使用策略组合以正确识别和标记语音和视频流量，在下游和上游方向设置带宽分配，以及使用呼叫准入控制以限制从无线小区发起的呼叫数。

注意：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

步骤 1：语音流量的识别和标记

第一步是识别语音和视频流量。语音流量可分为两类：

- 语音流，它承载通信的音频部分。
- 语音信令，用于传送语音终端之间交换的统计信息。

语音流通常使用实时传输协议(RTP)和用户数据报协议(UDP)目的端口，范围为16384 - 32767。这是范围；实际端口通常较窄，具体取决于实施。

有多种语音信令协议。此配置示例使用Jabber。Jabber将以下TCP端口用于连接和目录：

- TCP 80(HTTP)
- 143（Internet邮件访问协议[IMAP]）
- 443 (HTTPS)
- 993(IMAP)，用于Cisco Unified MeetingPlace或Cisco WebEx等服务，用于会议；Cisco Unity或Cisco Unity Connection用于语音邮件功能
- TCP 389/636（轻量级目录访问协议[LDAP]服务器，用于联系人搜索）
- FTP(1080)
- 用于从对等设备或从服务器传输文件（如配置文件）的TFTP(UDP 69)

这些服务可能不需要特定优先级。

Jabber使用会话初始协议(SIP)（UDP/TCP 5060和5061）进行语音信令。

视频流量使用不同的端口和协议，这取决于您的实施。此配置示例使用Tandberg PrecisionHD 720p摄像头进行视频会议。Tandberg PrecisionHD 720p摄像头可使用多个编解码器；消耗的带宽取决于选择的编解码器：

- C20、C40和C60编解码器使用H.323/SIP，在点对点连接中消耗的速度最高可达6 Mbps。
- C90编解码器使用这些相同的协议，在多站点通信中最高可消耗10 Mbps。

H.323的TANDBERG实施通常使用UDP 970来传输视频，使用UDP 971来传输视频信令，使用UDP 972来传输音频，使用UDP 973来传输音频信令。Tandberg摄像头还使用其他端口，例如：

- UDP 161
- UDP 962（简单网络管理协议[SNMP]）
- TCP 963(netlog)、TCP 964(FTP)
- TCP 965（虚拟网络计算[VNC]）
- UDP 974（会话通告协议[SAP]）

这些附加端口可能不需要特定优先级。

识别流量的常用方法是创建针对所关注流量的类映射。每个类映射都可以指向一个访问列表，该列表针对使用语音和视频端口的任何流量：

```
ip access-list extended JabberVOIP
permit udp any any range 16384 32767
ip access-list extended JabberSIGNALING
permit tcp any any range 5060 5061
permit udp any any range 5060 5061
ip access-list extended H323Videostream
permit udp any any eq 970
ip access-list extended H323Audiostream
permit udp any any eq 972
ip access-list extended H323VideoSignaling
permit udp any any eq 971
ip access-list extended H323AudioSignaling
permit udp any any eq 973
```

然后，您可以为每种流量类型创建一个类映射；每个类映射指向相关访问列表：

```
class-map RTPaudio
match access-group name JabberVOIP
match access-group name H323Audiostream
class-map H323realtimevideo
match access-group name H323Videostream
class-map signaling
match access-group name JabberSIGNALING
match access-group name H323VideoSignaling
match access-group name H323AudioSignaling
```

通过类映射识别语音流量和视频流量后，请确保正确标记流量。这可以通过表映射在WLAN级别完成，也可以通过客户端策略映射完成。

表映射检查传入流量的QoS标记，并确定传出QoS标记应是什么。因此，当传入流量已经具有QoS标记时，表映射非常有用。表映射在SSID级别专用。

相反，策略映射可以针对由类映射识别的流量，并且更适合潜在的无标记感兴趣的流量。此配置示例假设来自有线端的流量在进入Catalyst 3850交换机或Cisco 5760 WLC之前已正确标记。如果情况不是这样，您可以使用策略映射并在SSID级别将其作为客户端策略应用。由于来自无线客户端的流量可能尚未标记，因此您需要正确标记语音和视频流量：

- 应使用DSCP 46（加速转发[EF]）标记实时语音。
- 视频应标记为DSCP 34（保证转发类41 [AF41]）。
- 语音和视频的信令应标记为DSCP 24（类选择器服务值3 [CS3]）。

要应用这些标记，请创建一个策略映射，该映射调用这些类中的每个类，并标记等效流量：

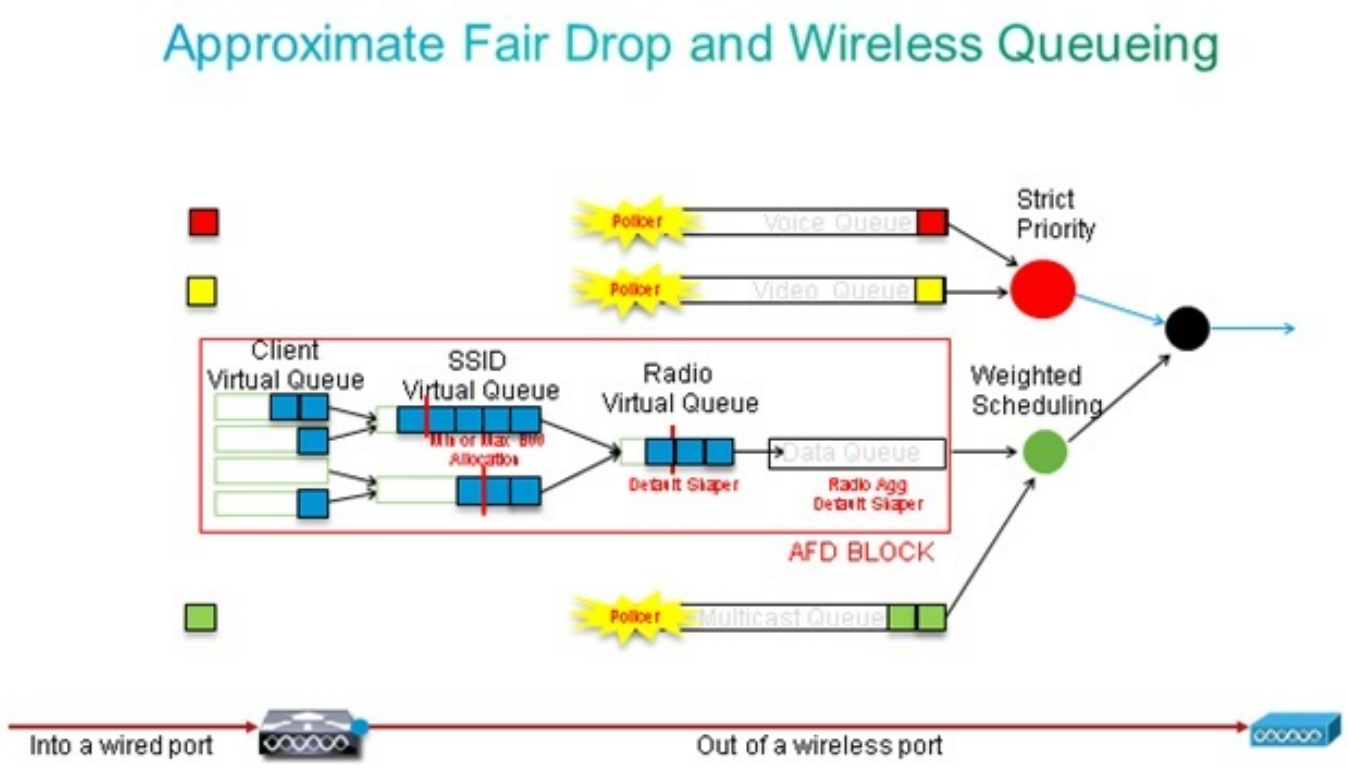
```
policy-map taggingPolicy
 class RTPaudio
 set dscp ef

 class H323realtimevideo
 set dscp af41

 class signaling
 set dscp cs3
```

步骤 2：端口级带宽和优先级管理

下一步是确定进出AP的端口的QoS策略。此步骤主要适用于Catalyst 3850交换机。如果您的配置是在Cisco 5760控制器上完成的，则此步骤不是必需的。Catalyst 3850端口承载进出无线客户端和AP的语音和视频流量。此情景中的QoS配置符合两个要求：

1. **分配带宽**。您可能想确定为每种流量类型分配多少带宽。此带宽分配也可在SSID级别完成。设置端口带宽分配，以优化每个为目标SSID提供服务的AP可以接收多少带宽。必须为目标AP上的所有SSID设置此带宽。此简化配置示例假设只有一个SSID和一个AP，因此语音和视频的端口带宽分配与SSID级别语音和视频的全局带宽分配相同。每种流量类型分配6 Mbps，并受到管制，因此不会超出此分配的带宽。

2. **确定流量的优先**级。端口有四个队列。前两个队列按优先顺序排列，并为实时流量（通常是语音和视频）保留。第四个队列保留用于非实时组播流量，第三个队列包含所有其他流量。使用融合接入队列逻辑，每个客户端的流量都分配到虚拟队列，在虚拟队列中可以配置QoS。客户端QoS策略的结果会注入到SSID虚拟队列中，也可以在其中配置QoS。由于给定AP无线电上可以存在多个SSID，因此AP无线电上存在的每个SSID的结果会注入AP无线电虚拟队列，其中流量根据无线电容量进行整形。在这些阶段中的任意阶段，可以使用称为近似公平丢弃(AFD)的QoS机制来延迟或丢弃流量。 然后，此策略的结果将发送到AP端口（称为无线端口），其中优先级分配给前两个队列（高达可配置的带宽量），然后按本段前面所述发送到第三和第四个队列。



此配置示例使用priority level命令将语音放入第一优先级队列，并将视频放入第二优先级**队列**中。其余流量将分配其余端口带宽。

请注意，不能使用基于访问控制列表(ACL)的目标流量的类映射。 在端口级别应用的策略可以基于类映射来针对流量，但这些类映射应以通过其QoS值标识的流量为目标。根据ACL确定流量并在客户端SSID级别正确标记此流量后，在端口级别对同一流量执行第二次深度检查将是冗余的。当流量到达通向AP的端口时，它已正确标记。

在本示例中，您重复使用为SSID策略创建的常规类映射，并直接将语音RTP流量和视频实时流量作为目标：

```
Class-map allvoice
match dscp ef
Class-map videoandsignaling
Match dscp af41
match dscp cs3
```

确定感兴趣的流量后，可以决定应用哪项策略。当检测到AP时，默认策略（称为parent_port）将自动应用于每个端口。您不应更改此默认值，其设置为：

```
policy-map parent_port
class class-default
shape average 1000000000
service-policy port_child_policy
```

由于默认parent_port策略调用port_child_policy，因此一个选项是编辑port_child_policy。（您不应更改其名称）。 此子策略确定每个队列中应传输的流量以及应分配多少带宽。第一个队列具有最高优先级，第二个队列具有第二高优先级，依此类推。这两个队列保留用于实时流量。第四个队列用于非实时组播流量。第三个队列包含所有其他流量。

在本示例中，您决定将语音流量分配到第一个队列，将视频流量分配到第二个队列，并将带宽分配到每个队列和所有其他流量：

```
Policy-map port_child_policy
Class allvoice
 Priority level 1
 police rate percent 10
 conform-action transmit
 exceed-action drop
class videoandsignaling
 priority level 2
 police rate percent 20
 conform-action transmit
 exceed-action drop
class non-client-nrt-class
 bandwidth remaining ratio 7
class class-default
 bandwidth remaining ratio 63
```

在此策略中，与“语音”和“视频和信令”类关联的优先级语句允许您将该流量分配到相关优先级队列。但是，请注意，策略速率百分比语句仅适用于组播流量，而不适用于单播流量。

您无需在端口级别应用此策略，因为一旦检测到AP，该策略就会自动应用。

步骤 3：SSID级别的带宽和优先级管理

下一步是在SSID级别处理QoS策略。此步骤适用于Catalyst 3850交换机和5760控制器。此配置假设语音和视频流量通过使用类映射和访问列表进行识别并正确标记。但是，某些未被访问列表锁定的传入流量可能不显示其QoS标记。在这种情况下，您可以决定是否应使用默认值标记此流量，还是保留未标记流量。类映射已标记但未针对的流量也采用相同逻辑。在表映射中使用*default copy*语句，以确保未标记的流量保持未标记状态，并且标记的流量保持标记且未重新标记。

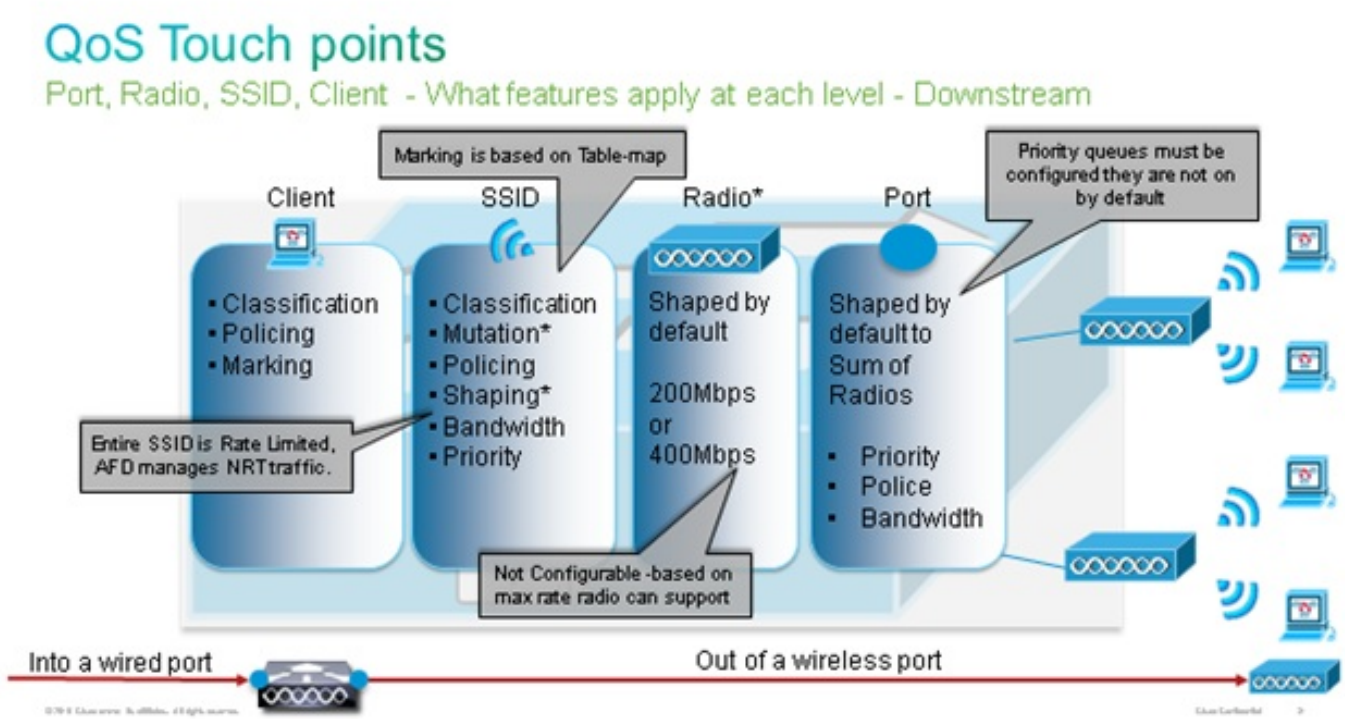
表映射决定传出DSCP值，但也用于创建802.11帧以决定帧UP值。

在本示例中，显示语音QoS级别(DSCP 46)的传入流量维护其DSCP值，并且该值映射到等效的802.11标记(UP 6)。 显示视频QoS级别(DSCP 34)的传入流量维护其DSCP值，该值映射到等效的

802.11标记(UP 5)。 同样，标有DSCP 24的流量可能是语音信令；DSCP值应保持并转换为802.11 UP 3:

```
Table-map dscp2dscp
Default copy
Table-map dscp2up
Map from 46 to 6
Map from 24 to 3
Map from 34 to 5
Default copy
```

标记也可以在传入的有线端口级别完成。此图显示了流量从有线传输到无线时可以采取哪些QoS操作：



此配置示例重点介绍QoS配置的无线方面，并标记无线客户端级别的流量。标记部分完成后，您需要分配带宽；此处，6 Mbps的带宽分配给语音流量。（虽然这是语音的总带宽分配，但每个呼叫的消耗会更少，例如128 kbps。）此带宽使用**police**命令进行分配，以保留带宽并丢弃超量流量。

视频流量也分配了6 Mbps并受到管制。此配置示例假设只有一个视频流。

视频和语音流量的信令部分也需要分配带宽。有两种可能的策略。

- 使用**shape average**命令，该命令允许缓冲和稍后发送超出的流量。这种逻辑对于语音或视频流本身并不有效，因为这些流需要一致的延迟和抖动；但是，它对于信令而言可能非常有效，因为信令可以稍微延迟而不影响呼叫质量。在融合接入解决方案中，shape命令不接受所谓的“桶配置”，即确定可缓冲超过分配带宽的流量。因此，必须添加第二个命令**queue-buffers ratio 0**，以指定桶大小为0。如果在其余流量中包含信令并使用shape命令，则在高拥塞时可能会丢弃信令流量。这反过来可能导致呼叫被丢弃，因为任一端都确定不再进行通信。
- 为避免呼叫被丢弃的风险，您可以将信令包括在一个优先级队列中。此配置示例之前将优先级队列定义为语音和视频，现在将信令添加到视频队列。

策略对语音流使用呼叫准入控制(CAC)。CAC以无线流量为目标并匹配特定UP（在本配置示例中为

UP 6和7）。然后，CAC确定此流量应使用的最大带宽量。在您管制语音流量的配置中，应为CAC分配分配给语音的总带宽量的子集。例如，如果语音被管制为6 Mbps，则CAC不能超过6 Mbps。CAC在集成到主下游策略映射（称为父策略）的策略映射（称为子策略）中配置。CAC是通过admit cac wmm-tspec**命令引入的，后跟目标UP和分配给目标流量的带宽。**

每个呼叫不会消耗分配给语音的所有带宽。例如，每个呼叫每路消耗64 kbps，这将导致128 kbps的有效双向带宽消耗。速率指令确定每个呼叫带宽消耗，而策略语句确定分配给语音流量的总带宽。如果蜂窝内发生的所有呼叫都使用接近最大允许带宽，则从蜂窝内发起并导致消耗的带宽超过允许语音的最大带宽的任何新呼叫都将被拒绝。您可以通过在频段级别配置CAC来微调此过程，如步骤4所述：CAC的呼叫限制。

因此，您需要配置包含CAC说明并集成到主下游策略的子策略。上游策略映射中未配置CAC。CAC确实适用于从信元发起的语音呼叫，但是，由于CAC是对这些呼叫的响应，因此CAC仅设置在下游策略映射中。上游策略映射将不同。不能使用之前创建的类映射，因为这些类映射基于ACL的目标流量。注入到SSID策略的流量已经通过客户端策略，因此您不应再次对数据包执行深度检查。相反，使用由客户端策略产生的QoS标记来目标流量。

如果决定不将信令保留在默认类中，则还需要确定信令的优先级。

在本例中，信令和视频处于同一类别，并且为该类别分配了更多带宽以适应信令部分；6 Mbps分配给视频流量（一个Tandberg摄像头点对点流），1 Mbps分配给所有语音呼叫和视频流量的信令：

```
Class-map allvoice
match dscp ef
Class-map videoandsignaling
Match dscp af41
Match dscp cs3
```

下游子策略为：

```
Policy-map SSIDout_child_policy
class allvoice
priority level 1
police 6000000
admit cac wmm-tspec
rate 128
wlan-up 6 7
class videoandsignaling
priority level 2
police 1000000
```

下游父策略为：

```
policy-map SSIDout
class class-default
set dscp dscp table dscp2dscp
set wlan user-priority dscp table dscp2up
shape average 30000000
queue-buffers ratio 0
service-policy SSIDout_child_policy
```

上游流量是来自无线客户端的流量，在流量从有线端口发出或发送到另一个SSID之前发送到WCM。在这两种情况下，都可以配置策略映射来定义分配给每种流量类型的带宽。策略可能会因流量是从有线端口发送出去还是发送到另一个SSID而异。

在上游方向，您主要关心的是确定优先级，而不是带宽。换句话说，您的上游策略映射不会为每种

流量类型分配带宽。由于流量已经位于AP，并且已经越过半双工无线空间形成的瓶颈，因此您的目标是将此流量引入Catalyst 3850交换机或Cisco 5760 WLC的控制器功能以进行进一步处理。在AP级别收集流量时，您可以决定是否应信任潜在的现有QoS标记，以便确定发送到控制器的流量的优先级。在本例中，可以信任现有DSCP值：

```
Policy-map SSIDin
Class class-default
set dscp dscp table dscp2dscp
```

创建策略后，将策略映射应用到WLAN。在本例中，连接到WLAN的任何设备都应支持WMM，因此需要WMM。

```
wlan test1
wmm require
service-policy client input taggingPolicy
service-policy input SSIDin
service-policy output SSIDout
```

步骤 4：CAC的呼叫限制

最后一步是根据您的具体情况定制CAC。在步骤3中介绍的CAC配置中：在SSID级别的带宽和优先级管理中，AP会丢弃任何超出分配带宽的语音数据包。

为避免带宽最大值。您还需要配置WCM以识别已拨呼叫和将导致带宽超出的呼叫。某些电话支持WMM流量规范(TSPEC)，并通知无线基础设施预计会消耗的带宽。然后，WCM可以在发出呼叫之前拒绝该呼叫。

某些SIP电话不支持TSPEC，但WCM和AP可以设置为识别发送到SIP端口的呼叫发起数据包，并且可以使用此信息来确定SIP呼叫即将发出。由于SIP电话未指定呼叫将消耗的带宽，因此管理员必须根据编解码器、采样时间等确定预期带宽。

CAC计算每个AP级别的消耗带宽。CAC可设置为在计算中仅使用客户端带宽消耗（静态CAC），也可以考虑同一信道上的相邻AP和设备（基于负载的CAC）。 思科建议您将静态CAC用于SIP电话，将基于负载的CAC用于TSPEC电话。

最后，请注意，CAC是按频段激活的。

在本示例中，电话会使用SIP而不是TSPEC发起会话，每个呼叫对每个流方向使用64 kbps，启用静态CAC时禁用基于负载的CAC，并且每个AP带宽的最大75%分配给语音流量：

```
ap dot11 5ghz shutdown
ap dot11 5ghz cac voice acm
no ap dot11 5ghz cac voice load-based
ap dot11 5ghz cac voice max-bandwidth 75
ap dot11 5ghz cac voice sip bandwidth 64
no ap dot11 5ghz shutdown
```

您可以对2.4 GHz频段重复相同的配置：

```
ap dot11 24ghz shutdown
ap dot11 24ghz cac voice acm
no ap dot11 24ghz cac voice load-based
ap dot11 24ghz cac voice max-bandwidth 75
```

```
ap dot11 24ghz cac voice sip bandwidth 64
no ap dot11 24ghz shutdown
```

对每个频段应用CAC后，您还需要在WLAN级别应用SIP CAC。此过程使AP能够检查无线客户端流量的第4层(L4)信息，以识别发送到UDP 5060的表示SIP呼叫尝试的查询。TSPEC在802.11级运行，由AP本地检测。SIP电话不使用TSPEC，因此AP必须执行更深入的数据包检测以识别SIP流量。由于您不希望AP对所有SSID执行此检测，因此您需要确定哪些SSID预期SIP流量。然后，您可以在这些SSID上启用呼叫监听以查找语音呼叫。您还可以确定如果SIP呼叫必须被拒绝时要执行的操作 — 取消关联SIP客户端或发送SIP忙消息。

在本例中，呼叫监听已启用，如果SIP呼叫必须被拒绝，则会发送忙消息。添加第3步中的QoS策略：SSID级别的带宽和优先级管理，这是示例WLAN的SSID配置：

```
wlan test1
wmm require
service-policy client input taggingPolicy
service-policy input SSIDin
service-policy output SSIDout
call-snoop
sip-cac send-486busy
```

验证

使用这些命令以确认您的QoS配置工作正常。

> **注意：**
>
> 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。
>
> 命令输出解释程序工具（仅限注册用户）支持某些 **show 命令。**使用输出解释器工具来查看 show 命令输出的分析。

show class-map

此命令显示在平台上配置的类映射：

```
3850#show class-map
 Class Map match-any H323realtimeaudio (id 6)
  Match access-group name H323Audiostream
Class Map match-any H323realtimevideo (id 7)
  Match access-group name H323Videostream
Class Map match-any allvideo (id 10)
  Match   dscp af41 (34)
Class Map match-any jabberaudiosignaling (id 11)
  Match access-group name JabberSIGNALING
Class Map match-any allvoice (id 12)
  Match   dscp ef (46)
Class Map match-any RTPaudio (id 19)
  Match access-group name JabberVOIP
  Match access-group name H323Audiostream
Class Map match-any class-default (id 0)
  Match any
Class Map match-any jabberRTPaudio (id 14)
```

```
  Match access-group name JabberVOIP
Class Map match-any non-client-nrt-class (id 1)
  Match non-client-nrt
Class Map match-any H323audiosignaling (id 17)
  Match access-group name H323AudioSignaling
Class Map match-any H323videosignaling (id 18)
  Match access-group name H323VideoSignaling
Class Map match-any signaling (id 20)
  Match access-group name JabberSIGNALING
  Match access-group name H323VideoSignaling
  Match access-group name H323AudioSignaling
```

show policy-map

此命令显示平台上配置的策略映射：

```
3850 #show policy-map
show policy-map
 Policy Map port_child_policy
   Class non-client-nrt-class
     bandwidth remaining ratio 7
   Class allvoice
     priority level 1
    police rate percent 10
      conform-action transmit
      exceed-action drop
   Class allvideo
     priority level 2
    police rate percent 20
      conform-action transmit
      exceed-action drop
   Class class-default
     bandwidth remaining ratio 63
 Policy Map SSIDin
   Class class-default
     set dscp dscp table dscp2dscp
 Policy Map SSIDout_child_policy
   Class allvoice
     priority level 1
    police cir 6000000 bc 187500
      conform-action transmit
      exceed-action drop
     admit cac wmm-tspec
       rate 6000 (kbps)
       wlan-up 6
   Class allvideo
     priority level 2
    police cir 6000000 bc 187500
      conform-action transmit
      exceed-action drop
     admit cac wmm-tspec
       rate 6000 (kbps)
       wlan-up 4 5
 Policy Map taggingPolicy
   Class RTPaudio
     set dscp ef
   Class H323realtimevideo
     set dscp af41
   Class signaling
     set dscp cs3
 Policy Map SSIDout
```

```
   Class class-default
     set dscp dscp table dscp2dscp
     set wlan user-priority dscp table dscp2up
     shape average 30000000 (bits/sec)
     queue-buffers ratio 0
     service-policy SSIDout_child_policy
 Policy Map parent_port
   Class class-default
     shape average 1000000000 (bits/sec) op
```

show wlan

此命令显示WLAN配置和服务策略参数：

```
3850# show wlan name test1 | include Policy
AAA Policy Override                              : Disabled
QoS Service Policy - Input
 Policy Name                                    : SSIDin
 Policy State                                   : Validated
QoS Service Policy - Output
 Policy Name                                    : SSIDout
 Policy State                                   : Validated
QoS Client Service Policy
 Input  Policy Name                             : taggingPolicy
 Output Policy Name                             : taggingPolicy
Radio Policy                                     : All
```

show policy-map interface

此命令显示为特定接口安装的策略映射：

```
3850#show policy-map interface wireless ssid name test1

Remote SSID test1 iifid: 0x01023F4000000033.0x00F2E98000000003.0x00C2EB000000001F
 Service-policy input: SSIDin
   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp dscp table dscp2dscp

Remote SSID test1 iifid: 0x01023F4000000033.0x00C8384000000004.0x00D0D08000000021

 Service-policy input: SSIDin

   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp dscp table dscp2dscp

SSID test1 iifid: 0x01023F4000000033.0x00F2E98000000003.0x00EC3E800000001E

 Service-policy input: SSIDin

   Class-map: class-default (match-any)
```

```
    Match: any
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
      dscp dscp table dscp2dscp

 Service-policy output: SSIDout

   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp dscp table dscp2dscp
       wlan user-priority dscp table dscp2up
     shape (average) cir 30000000, bc 120000, be 120000
     target shape rate 30000000
     queue-buffers ratio 0

     Service-policy : SSIDout_child_policy

       Class-map: allvoice (match-any)
         Match:  dscp ef (46)
           0 packets, 0 bytes
           30 second rate 0 bps
         Priority: Strict,

         Priority Level: 1
         police:
             cir 6000000 bps, bc 187500 bytes
           conformed 0 bytes; actions:
             transmit
           exceeded 0 bytes; actions:
             drop
           conformed 0000 bps, exceed 0000 bps
         cac wmm-tspec rate 6000 kbps

       Class-map: allvideo (match-any)
         Match:  dscp af41 (34)
           0 packets, 0 bytes
           30 second rate 0 bps
         Priority: Strict,

         Priority Level: 2
         police:
             cir 6000000 bps, bc 187500 bytes
           conformed 0 bytes; actions:
             transmit
           exceeded 0 bytes; actions:
             drop
           conformed 0000 bps, exceed 0000 bps
         cac wmm-tspec rate 6000 kbps

       Class-map: class-default (match-any)
         Match: any
           0 packets, 0 bytes
           30 second rate 0 bps

SSID test1 iifid: 0x01023F4000000033.0x00C8384000000004.0x00DB568000000020

 Service-policy input: SSIDin

   Class-map: class-default (match-any)
     Match: any
```

```
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp dscp table dscp2dscp

 Service-policy output: SSIDout

   Class-map: class-default (match-any)
     Match: any
       0 packets, 0 bytes
       30 second rate 0 bps
     QoS Set
       dscp dscp table dscp2dscp
       wlan user-priority dscp table dscp2up
     shape (average) cir 30000000, bc 120000, be 120000
     target shape rate 30000000
     queue-buffers ratio 0

     Service-policy : SSIDout_child_policy

       Class-map: allvoice (match-any)
         Match:  dscp ef (46)
           0 packets, 0 bytes
           30 second rate 0 bps
         Priority: Strict,

         Priority Level: 1
         police:
             cir 6000000 bps, bc 187500 bytes
           conformed 0 bytes; actions:
             transmit
           exceeded 0 bytes; actions:
             drop
           conformed 0000 bps, exceed 0000 bps
         cac wmm-tspec rate 6000 kbps

       Class-map: allvideo (match-any)
         Match:  dscp af41 (34)
           0 packets, 0 bytes
           30 second rate 0 bps
         Priority: Strict,

         Priority Level: 2
         police:
             cir 6000000 bps, bc 187500 bytes
           conformed 0 bytes; actions:
             transmit
           exceeded 0 bytes; actions:
             drop
           conformed 0000 bps, exceed 0000 bps
         cac wmm-tspec rate 6000 kbps

       Class-map: class-default (match-any)
         Match: any
           0 packets, 0 bytes
           30 second rate 0 bps

3850#show policy-map interface wireless client
Client 8853.2EDC.68EC iifid:
0x01023F4000000033.0x00F2E98000000003.0x00EC3E800000001E.0x00E0D04000000022

 Service-policy input: taggingPolicy

   Class-map: RTPaudio (match-any)
```

```
    Match: access-group name JabberVOIP
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: access-group name H323Audiostream
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
      dscp ef

  Class-map: H323realtimevideo (match-any)
    Match: access-group name H323Videostream
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
      dscp af41

  Class-map: signaling (match-any)
    Match: access-group name JabberSIGNALING
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: access-group name H323VideoSignaling
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: access-group name H323AudioSignaling
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
      dscp cs3
  Class-map: class-default (match-any)
    Match: any
      0 packets, 0 bytes
      30 second rate 0 bps

Service-policy output: taggingPolicy

  Class-map: RTPaudio (match-any)
    Match: access-group name JabberVOIP
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: access-group name H323Audiostream
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
      dscp ef

  Class-map: H323realtimevideo (match-any)
    Match: access-group name H323Videostream
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
      dscp af41

  Class-map: signaling (match-any)
    Match: access-group name JabberSIGNALING
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: access-group name H323VideoSignaling
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: access-group name H323AudioSignaling
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
      dscp cs3
```

```
  Class-map: class-default (match-any)
    Match: any
      0 packets, 0 bytes
      30 second rate 0 bps
```

show platform qos policies

此命令显示为端口、AP无线电、SSID和客户端安装的QoS策略。请注意，您可以验证但无法更改无线电策略：

```
3850#show platform qos policies PORT
Loc Interface          IIF-ID             Dir Policy           State
--- ------------------ ------------------ --- ---------------- --------------
L:0 Gi1/0/20           0x01023f4000000033 OUT defportangn      INSTALLED IN HW
L:0 Gi1/0/20           0x01023f4000000033 OUT port_child_policyINSTALLED IN HW

3850#show platform qos policies RADIO
Loc Interface          IIF-ID             Dir Policy           State
--- ------------------ ------------------ --- ---------------------------------
L:0 R56356842871193604 0x00c8384000000004 OUT def-11an         INSTALLED IN HW
L:0 R68373680329064451 0x00f2e98000000003 OUT def-11gn         INSTALLED IN HW
3850#show platform qos policies SSID
Loc Interface          IIF-ID             Dir Policy           State
--- ------------------ ------------------ --- ---------------------------------
L:0 S70706569125298203 0x00fb33400000001b OUT SSIDout_child_policyINSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 OUT SSIDout_child_policyINSTALLED IN HW
L:0 S70706569125298203 0x00fb33400000001b OUT SSIDout          INSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 OUT SSIDout          INSTALLED IN HW
L:0 S70706569125298203 0x00fb33400000001b IN  SSIDin           INSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 IN  SSIDin           INSTALLED IN HW

3850#show platform qos policies CLIENT
Loc Interface          IIF-ID             Dir Policy           State
--- ------------------ ------------------ --- ---------------- --------------
L:0 8853.2edc.68ec     0x00e0d04000000022 IN  taggingPolicy    NOT INSTALLED IN HW
L:0 8853.2edc.68ec     0x00e0d04000000022 OUT taggingPolicy    NOT INSTALLED IN HW
```

show wireless client mac-address <mac> service-policy

此命令显示在客户端级别应用的策略映射：

```
3850#show wireless client mac-address 8853.2EDC.68EC service-policy output
Wireless Client QoS Service Policy
Policy Name  : taggingPolicy
Policy State : Installed
3850#sh wireless client mac-address 8853.2EDC.68EC service-policy in
3850#sh wireless client mac-address 8853.2EDC.68EC service-policy input
Wireless Client QoS Service Policy
Policy Name  : taggingPolicy
Policy State : Installed
```

故障排除

目前没有针对此配置的故障排除信息。