在聚合的访问控制器和轻量级AP配置示例的QoS

目录

简介

本文描述如何配置在思科聚合的访问网络的QoS用轻量级接入点(拉普)和用思科Catalyst 3850交换机或思科5760无线局域网控制器(WLC)。

先决条件

要求

Cisco 建议您了解以下主题：

- 基础知识如何配置拉普和思科聚合访问控制器
- 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：

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

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。

使用QoS，带宽可以在LAN间效率更高管理，包括无线LAN (WLAN)和WAN。QoS提供增强版和可靠的网络网络服务这些服务：

- 支持关键用户和应用程序的专用带宽。
- 控制由实时数据流要求的抖动和延迟。
- 管理并且最小化网络拥塞。
- 整形网络流量为了使光滑流量流。
- 设置网络流量优先权。

在过去，WLAN 主要用于传输低带宽、数据应用流量。使用WLAN扩展到垂直(例如零售、金融和教育)和企业环境里， WLAN当前用于与时间敏感的一道传输高带宽数据应用，多媒体应用。此要求导致了无线 QoS 的必要性。

在IEEE 802.11标准委员会内的IEEE 802.11e工作组完成标准的定义，并且wi-fi联盟创建wi-fi多媒体(WMM)证明，但是802.11e标准的采用仍然被限制。因为WMM证明为802.11n和802.11ac证明，是需要的多数设备是WMM经过认证。许多无线设备不指定不同的QoS级别到发送的数据包到数据链路层，因此那些设备最发送他们的流量没有QoS标记和没有相对优先级。然而，多数802.11无线局域网语音(VoWLAN) IP电话标记并且指定优先级他们的语音流量。本文着重在VoWLAN IP电话的QoS配置和标记他们的语音流量的支持视频wi-fi设备。

> **注意**：在本文的范围之外，不执行内部标记的设备的QoS配置是。

802.11e附录定义了八个用户优先级()级别，分组两由两到四个QoS级别(访问类别) ：

- 白金服务/voice (7和6) -保证服务高质量语音的在无线。
- 金牌服务/视频(5和4) -支持优质视频应用程序。
- 西尔弗/尽力(3和0) -支持正常带宽客户端的。这是默认设置。
- 铜牌服务/背景(2和1) -为访客服务提供低带宽。

白金服务为VoIP客户端和金牌服务是常用的视频客户端的。本文提供说明如何配置在控制器的QoS和通信与有线网络配置与VoWLAN和视频客户端的QoS的配置示例。

L3 QoS数据包标记增强

思科由WLCs和拉普聚合访问控制器支持第3层(L3) IP差分服务代码点标记发送的数据包。此功能提高接入点(AP)如何使用此L3信息为了保证数据包接收从AP的正确通过空气优先级给无线客户端。

在使用Catalyst 3850交换机作为无线控制器的聚合的访问WLAN体系结构里， AP连接直接地到交换机。在使用5760个控制器的聚合的访问WLAN体系结构里， WLAN数据被建立隧道在AP和无线接入点(CAPWAP)协议之间WLC通过控制和供应。为了维护在此通道间的原始QoS分类，必须适当地映射封装的数据数据包的QoS设置到外面隧道信息包的Layer2 (L2) (802.1p)和L3 (IP DSCP)字段。

当您配置VoWLAN和视频的时QoS，您能配置无线客户端的QoS策略特定和策略特定到WLAN或者两个。您能也补全与配置特别的设置到连接AP的端口，特别是用Catalyst 3850交换机。此配置示例着重无线客户端、WLAN和端口的QoS配置对AP。QoS配置的主要目标VoWLAN和视频应用的是：

- 认可语音和视频流量(数据流分类和标记)，两上行和下行。
- 用语音优先级优先级别标记语音和视频流量： 802.11e向上6， 802.1p 5，语音的DSCP 46。802.11e向上5，视频的DSCP 34。
- 分配语音流量、语音信令和视频流量的带宽。

配置QoS的无线网络与MQC

在您配置QoS前，您必须配置Catalyst 3850交换机或思科5760 WLC的无线控制器模块(WCM)功能基本操作的和注册拉普到WCM。本文假设， WCM为基本操作配置，并且拉普注册对WCM。

聚合的接入解决方案使用模块化QoS (MQC)命令行界面(CLI)。参考的QoS配置指南，关于使用的Cisco IOS XE版本3SE (Catalyst 3850交换机) MQC的更多信息在QoS配置方面在Catalyst 3850交换机。

QoS的配置与MQC的在聚合的访问控制器依靠四个元素：

- **类映射**用于为了认可流量利益。类映射能使用多种技术(例如存在QoS标记、访问列表或者VLAN)为了识别流量利益。
- **策略映射**用于为了确定应该应用什么QoS设置到流量利益。策略映射呼叫类映射和应用多种QoS设置(例如特定标记、优先级，带宽分配，等等)对每类。
- **服务策略**用于为了适用于策略映射您的网络有战略意义的点。在聚合的接入解决方案，服务策略可以应用到用户、服务集标识符(Ssid)， AP无线电和端口。波尔特、SSID和客户端策略可以由用户配置。无线电策略是由无线控制模块控制的。当流量从交换机或控制器流到无线客户端时，端口、SSID、客户端和无线电的无线QoS策略在下行方向应用。
- **表映射**用于为了检查流入QoS标记和决定流出的QoS标记。表映射在策略映射被安置应用对Ssid。表映射可以用于为了保持(复制)或更改标记。表映射可能也用于为了创建有线的和无线标记之间的一映射。有线的标记使用DSCP (L3 QoS)或802.1p (L2 QoS)。无线标记使用用户优先级()。表映射是常用的确定应该用于应该用于什么DSCP标记其中每一利益，并且什么每个DSCP值利益。因为没有在DSCP和上值之间的直接转换表映射是基本的对聚合的访问QoS。

然而，对上表映射的DSCP也允许*复制*说明。在那种情况下，聚合的接入解决方案使用思科体系结构语音、视频和集成数据(AVVID)映射表为了确定DSCP到上或至DSCP转换：

标签索引	密钥字段	流入值	外面DSCP	Cos	
0	N.A.	不已勾选	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		0	0	0	0
74		1	8	1	1
75		2	16	1	2
76		3	24	2	3
77		4	34	3	4
78		5	34	4	5
79		6	46	5	6
80		7	46	7	7

默认硬编码的策略

聚合的访问控制器出发可以应用到WLAN的硬编码的QoS策略配置文件。这些配置文件运用跟熟悉Cisco Unified无线网络的金属策略(白金，金牌服务，等等) (CUWN)控制器的管理员。如果您的目标不将创建分配特定带宽到语音流量的策略，但是保证语音流量接收适当的QoS标记，您能使用硬编码的策略。硬编码的策略应用到WLAN，并且可以是不同的在上行和下行方向。

> 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。请使用Output Interpreter Tool为了查看show命令输出分析。

白金服务

语音的硬编码的策略呼叫白金。名称不可能更改。

这是白金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
```

这是白金服务QoS级别的上游政策：

```
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
```

金牌服务

视频的硬编码的策略呼叫金牌服务。名称不可能更改。

这是金QoS级别的下行策略：

```
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
```

这是金QoS级别的上游政策：

```
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
```

西尔弗

尽力的硬编码的策略呼叫银色。名称不可能更改。

这是银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QoS级别的上游政策：

```
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
```

铜牌服务

后台流量的硬编码的策略呼叫古铜色。名称不可能更改。

这是铜牌服务QoS级别的下行策略：

```
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
```

这是铜牌服务QoS级别的上游政策：

```
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
```

一旦决定了最佳哪的表映射匹配一给的SSID的目标流量，您能运用匹配的策略到您的WLAN。在本例中，一项策略在下行方向(输出应用，从AP到无线客户端)，并且一项策略在上行方向(输入应用，从无线客户端，通过AP，对控制器)：

```
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配置为了验证哪项策略应用对您的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
```

手工配置

硬编码的策略应用默认QoS标记，但是不应用带宽分配。硬编码的策略也假设，您的流量已经被标记。在复杂环境，您可以要使用策略的组合为了认可和标记语音和视频流量适当地，设置在下行和上行方向的带宽分配和使用呼叫接纳控制为了限制从无线信元发起的呼叫数量。

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：语音流量识别和标记

第一步将认可语音和视频流量。语音流量可以分类到两个类别：

- 语音流，运载通信的音频部分。
- 语音信令，传播统计信息交换在语音终端之间。

语音流通常使用实时传输协议(RTP)和用户数据报协议(UDP)目的地端口在16384 - 32767范围内。这是范围;实际端口通常是更加缩小的并且取决于实施。

有几份语音信令协议。此配置示例使用Jabber。Jabber使用这些TCP端口连接和目录：

- TCP 80 (HTTP)
- 143 (互联网消息访问协议[IMAP])
- 443 (HTTPS)
- 993 (IMAP)服务的例如Cisco Unified MeetingPlace或思科WebEx会议的和Cisco Unity或者Cisco Unity Connection语音邮件功能的
- TCP 389/636 (轻量级目录访问协议联系方式搜索的[LDAP]服务器)
- FTP (1080)
- TFTP (UDP 69)文件传输的(例如配置文件)从对等体或从服务器

这些服务可能不需要一特定优先级。

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

视频流量使用取决于您的实施的不同的端口和协议。此配置示例使用一Tandberg PrecisionHD 720p摄像头视频会议。Tandberg PrecisionHD 720p摄像头能使用几个编码;使用的带宽取决于选择的编码：

- C20、C40和C60编码使用H.323/SIP，并且能消耗至在点对点连接的6 Mbps。
- C90编码使用这些同样协议，并且能消耗至在多站点通信的10 Mbps。

H.323的Tandberg实施典型地使用视频信号的UDP 970视频流，放出的音频UDP 971，音频信号的UDP 972和UDP 973。Tandberg摄像头也使用其他端口，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])

这些另外的端口可能不需要一特定优先级。

识别流量的普通方法是创建瞄准流量利益的类映射。每类映射能指向access-list该目标使用语音和视频端口的所有流量：

```
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
```
您能然后创建每种流量类型的一类映射;每类映射指向相关access-list ：

```
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
```
一旦语音流量和视频流量通过类映射识别，请保证流量适当地被标记。这执行在WLAN级通过表映射，并且可能通过客户端策略映射也执行。

表映射检查流入的数据流QoS标记并且确定什么流出的QoS标记应该是。因此，当流入的数据流已经有QoS标记时，表映射是有用的。表映射完全使用在SSID级别。

相反，策略映射能瞄准类映射识别的流量并且是更加好潜在适应未标签的数据流利益。此配置示例假设，从有线的侧的流量适当地已经被标记了，在输入Catalyst 3850交换机或思科5760 WLC前。如果这不是实际情形，您能使用策略映射和应用它在SSID级别作为客户端策略。由于从无线客户端的流量不可以被标记了，您需要适当地标记语音和视频流量：

- 应该标记实时语音用DSCP 46 (加速转发[EF])。
- 视频应该是被标记的DSCP 34 (有保证的转发级41 [AF41])。
- 发信号语音和视频的应该是被标记的DSCP 24 (等级选择器服务值3 [CS3])。

要应用这些标记，请创建呼叫这些类中的每一，并且标记等同的流量的策略映射：

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

 class H323realtimevideo
 set dscp af41

 class signaling
 set dscp cs3
```

步骤 2：带宽和优先级管理在波尔特级别

下一步是确定来来往往对AP的端口的QoS策略。此步骤主要适用于Catalyst 3850交换机。如果您的配置在思科5760控制器被执行，此步骤不是必须。Catalyst 3850端口运载去对或来自无线客户端和AP的语音和视频流量。QoS配置在此上下文匹配两个需求：

1. **分配带宽**。您可以要决定多少带宽为每种流量类型分配。此带宽分配可能也完成在SSID级别。设置端口带宽分配为了完善为目标SSID服务的多少带宽可以由每个AP接收。此带宽必须为在目标AP的所有Ssid设置。此简化的配置示例假设只有一SSID和一个AP，因此语音和视频端口带宽分配是相同的象语音的全局带宽分配和视频在SSID级别。每流量类型是分配的6 Mbps和被管辖，以便此已分配带宽没有被超出。

2. **指定优先级的流量**。端口有四个队列。前两个队列为实时数据流优先安排并且保留-典型语音和视频，分别。第四个队列为非实时组播数据流保留，并且第三个队列包含其他流量。使用聚

合的访问排队逻辑，每个客户端的流量分配到一个虚拟队列， QoS可以配置。客户端QoS策略的结果被注入SSID虚拟队列， QoS可能也配置。因为几Ssid在给的AP无线电能存在，是存在AP无线电每SSID的结果被注入AP无线电虚拟队列，流量被整形根据无线电产能。流量可以延迟或降低在任何这些阶段利用呼叫Approximate Fair丢弃的QoS机制(AFD)。此策略结果在此段然后发送到AP端口(呼叫无线端口)，其中优先级给对前两个队列(至可配置相当数量带宽)，然后对第三个和第四个队列如描述前。

此配置示例放置语音到最优先考虑的事队列和视频在第二个优先级队列通过使用**优先级**命令。分配流量的其余端口带宽的其余。

注意您不能使用瞄准根据访问控制列表(ACL)的流量的类映射。策略应用在端口级别能瞄准根据类映射的流量，但是这些类映射应该瞄准其QoS值识别的流量。一旦识别流量根据ACL和适当地被标记此流量在客户端SSID级别，冗余执行该同样流量的第二深检查在端口级别。当流量到达去AP的端口时，适当地已经被标记。

在本例中，您重新使用为SSID策略创建的一般类映射和直接地瞄准语音RTP流量和视频实时数据流：

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

一旦识别流量利益，您能决定应用的哪项策略。默认策略(呼叫parent_port)在每个端口自动地应用，当AP检测时。您不应该更改此默认，设置：

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

由于默认parent_port策略呼叫port_child_policy，一个选项是编辑port_child_policy。(您不应该更改其名称)。此子策略确定应该分配什么流量在每个队列应该进来，并且多少带宽。第一个队列有最高优先级，第二个队列有第二高优先级，等等。这两个队列为实时数据流保留。第四个队列使用非实时组播数据流。第三个队列包含其他流量。

在本例中，您决定分配语音流量到第一个队列和视频流量到第二个队列和分配带宽到每个队列和到其他流量：

```
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，优先级语句关联对‘语音’和‘videoandsignaling的’类给您分配该流量对相关优先级队列。公告，然而， police rate百分比语句应用只组播，不是单播，流量。

您不需要运用此策略在端口级别，因为自动地应用，当AP检测。

步骤 3：带宽和优先级管理在SSID级别

下一步是照料QoS策略在SSID级别。此步骤适用于对两个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识别和适当地被标记。然而，没有由瞄准access-list的若干流入的数据流可能不显示其QoS标记。在那种情况下，您能决定此流量应该是否用默认值标记或被留下无标记。同样逻辑为类映射已经被标记，但是没瞄准的流量去。请使用*默认复制*语句在表映射为了保证未玷污的流量被留下未玷污，并且标记的数据流保持标记，并且没被重新标明的它。

表映射决定流出的DSCP值，但是也使用创建802.11帧决定帧上值。

在本例中，显示的流入的数据流语音QoS级别(DSCP 46)维护其DSCP值和值被映射对等同802.11标记(6)。显示视频QoS级别的流入的数据流(DSCP 34)维护其DSCP值和值被映射对等同802.11标记(5)。同样地，流量被标记的DSCP 24可能是语音信令;应该维护和翻译DSCP值到802.11 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
```

标记能也完成在流入有线的端口级别。此图显示什么QoS操作可以被采取作为从有线的流量传输到无线：

此配置示例着重QoS配置和标记该流量的无线方面在无线客户端级别。一旦标记部分完成，您需要分配带宽;此处，带宽6 Mbps分配到语音流量运输流量。(当这是语音时全部带宽分配，每呼叫例如将消耗少， 128 Kbps。)此带宽分配**police命令**为了保留带宽和降低过份的流量。

视频流量是也分配的6 Mbps和修正。此配置示例假设，只有一个视频流。

视频和语音流量的发信号的部分也需要是分配的带宽。有两个可能的策略。

- 请使用**形状平均值**命令，允许过份的流量缓冲并且发送以后。因为那些流要求一致延迟和抖动，此逻辑为语音或视频流不是高效;然而，因为发信号可以轻微延迟，不用对呼叫质量的作用它可以是高效为发信号。在聚合的接入解决方案，形状命令不接受什么呼叫“桶配置”，确定超出已分配带宽的多少流量可以缓冲。所以，必须添加第二条命令，**队列缓冲区比率0**，为了指定桶大小是0。如果在流量的其余包括信令并且使用形状命令，信令流量也许在高拥塞时候丢弃。这也许，反过来，导致呼叫丢弃，因为任一个末端确定通信不再发生。
- 要避免呼叫断线风险，您能在其中一个优先级队列中包括信令。此配置示例以前定义优先级队列，语音和视频和当前添加信令到视频队列。

策略使用呼叫接纳控制(CAC)语音流。CAC瞄准无线数据流并且匹配特定(在本例中配置示例， 6和7)。CAC然后确定此流量应该使用的最大带宽量。在您修正语音流量的配置中，应该分配CAC为语音带宽分配的整体相当数量的一子集。例如，如果语音被管辖对6 Mbps， CAC不可以超出6 Mbps。CAC在策略映射配置(呼叫子策略)集成到主要下行策略映射(呼叫父策略)。CAC用**承认cac WMM TSpec**命令介绍，遵从被目标向上和带宽分配到被瞄准的流量。

每呼叫不使用所有带宽分配到语音。例如，每呼叫可能消耗64 Kbps每个方式，导致128 Kbps有效双向带宽消耗。而监控语句确定全部带宽分配到语音流量，速率说明确定每呼叫带宽消耗。如果在接近最大允许的带宽的信元使用内发生的所有呼叫，其中任一被发起从信元的内部，并且造成已消耗带宽超出为语音允许的最大带宽的新建的呼叫将拒绝。您能通过CAC的配置优化此进程在波段级

别，按照步骤4:说明与CAC的呼叫限制。

所以，您需要配置包含CAC说明，并且集成到主要下行策略的子策略。CAC在上行策略映射没有配置。CAC适用于从信元发起的语音呼叫，但是，因为它是对那些呼叫的一答复， CAC仅设置到下行策略映射。上行策略映射不同的。因为这些类映射瞄准根据ACL的流量您不能使用以前创建的类映射。流量被注入SSID策略已经通过客户端策略，因此您不应该执行在数据包的深检查每第二次。反而，与该QoS的标记的目标流量起因于客户端策略。

如果决定不留下在默认组的信令，您也将需要优先安排信令。

在本例中，信令和视频在同班，并且更多带宽分配到该类为了适应发信号的部分;6 Mbps为视频流量(一个Tandberg摄像头点到点流)分配，并且1 Mbps分配到发信号所有语音呼叫和视频流的：

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

下行子策略是：

```
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
```

下行父策略是：

```
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
```

上行流量是来自无线客户端的流量和发送对WCM，在流量发送在一个有线的端口外面或发送对另一SSID前。在两种情况下，您能配置定义了带宽分配到每种流量类型的策略映射。策略很可能将有所不同基于流量是否发送在一个有线的端口外面或对另一SSID。

在上行方向，您的最关心是决定优先级，不是带宽。换句话说，您的上行策略映射不分配带宽到每种流量类型。由于流量已经在AP和已经交叉了半双工无线空间形成的瓶颈，您的目标是给Catalyst 3850交换机的控制器功能带来此流量或进一步处理的思科5760 WLC。当流量收集在AP级别时，您能决定应该是否委托潜在的现有QoS标记为了优先安排通信流发送对控制器。在本例中，存在DSCP值可以委托：

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

一旦您的策略创建，请应用策略映射对WLAN。在本例中，连接对WLAN的所有设备预计支持WMM，因此WMM要求。

```
wlan test1
wmm require
```

```
service-policy client input taggingPolicy
service-policy input SSIDin
service-policy output SSIDout
```

步骤 4：与CAC的呼叫限制

最后一步是为CAC专门制作您的特殊的例子。在步骤解释的CAC配置中3 ：带宽和优先级管理在SSID级别， AP丢弃超出已分配带宽的所有语音数据包。

为了避免最大带宽。，您也需要配置WCM为了认可发出将造成带宽被超出的呼叫和呼叫。一些电话技术支持WMM流量规格(TSPEC)和通知无线结构带宽设想的呼叫预计消耗。在放置前， WCM能然后拒绝呼叫。

一些SIP电话不支持TSPEC，但是WCM和AP设置认可呼叫开始发送的数据包到SIP端口，并且能使用此信息为了设立将放置SIP呼叫。由于SIP电话不指定将由呼叫消耗的带宽，管理员必须根据编码确定预计带宽，采样时间，等等。

CAC计算已消耗带宽在每个AP级别。CAC在其计算(静态CAC)可以设置使用仅客户端带宽消耗或也假定有相邻的AP和设备在同一个信道(基于负载的CAC)。思科建议您使用静态CAC SIP电话和基于负载的CAC TSPEC电话。

最后，请注意CAC在a激活每个波段基本类型。

在本例中，电话使用SIP而不是TSPEC他们的会话开始，每呼叫用途64 Kbps每个数据流方向，基于负载的CAC禁用，当静态CAC启用时，并且75%每AP最大带宽分配到语音流量：

```
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
```

您能重复2.4 GHz频段的相同的配置：

```
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
```

一旦CAC为每个波段应用，您也需要应用SIP CAC在级的WLAN。此进程使AP检查无线客户端数据流的Layer4 (L4)信息为了识别指示SIP呼叫尝试的查询被发送对UDP 5060。TSPEC运行在802.11级别和由AP本地检测。SIP电话不使用TSPEC，因此AP必须进行更加深刻的包侦测为了识别SIP流量。由于您不希望AP执行在所有Ssid的此检查，您需要确定哪些Ssid期待SIP流量。能然后启用呼叫监听在那些Ssid的您为了寻找语音呼叫。您能也确定什么操作实行，如果SIP呼叫必须拒绝-请取消关联SIP客户端或传送SIP忙碌信息。

在本例中，监听的呼叫启用，并且忙碌信息传送，如果SIP呼叫必须拒绝。增加从步骤3的QoS策略：带宽和优先级管理在SSID级别，这是SSID配置示例WLAN的：

```
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

请使用这些命令为了确认您的QoS配置适当地工作。

> 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。请使用Output Interpreter Tool为了查看show命令输出分析。

show class-map

此命令显示在平台配置的类映射：

```
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

此命令显示在平台配置的策略映射：

```
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
```

显示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

此命令显示为一个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
```

显示平台QoS策略

此命令显示为端口、AP无线电、Ssid和客户端安装的QoS策略。注意您能验证，但是不能更改，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
```

显示无线客户端MAC地址<mac>服务策略

此命令显示策略映射应用在客户端级别：

```
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。