配置限制在有AAA覆盖的Catalyst 9800无线控制器的QoS (BDRL)速率

目录

简介

本文为限制服务质量(QoS)双定向的速率提供配置示例(BDRL)验证、授权和认为的(AAA)覆盖在Catalyst 9800 Series无线控制器。

贡献用费尔南达角唱腔和亚历杭德罗Ramírez G.， Cisco TAC工程师

先决条件

要求

Cisco 建议您了解以下主题：

- Catalyst无线9800配置型号
- AAA用Cisco身份服务引擎(ISE)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 在版本16.12.1s的Cisco Catalyst 9800-CL无线控制器
- 在版本2.2的身份服务引擎

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 9800年WLC平台使用概念和组件和Catalyst 9000平台一样。此部分提供一全局概述这些组件如何工作，并且如何可能他们配置取得不同的结果。

实质上， QoS象这样的递归工作：

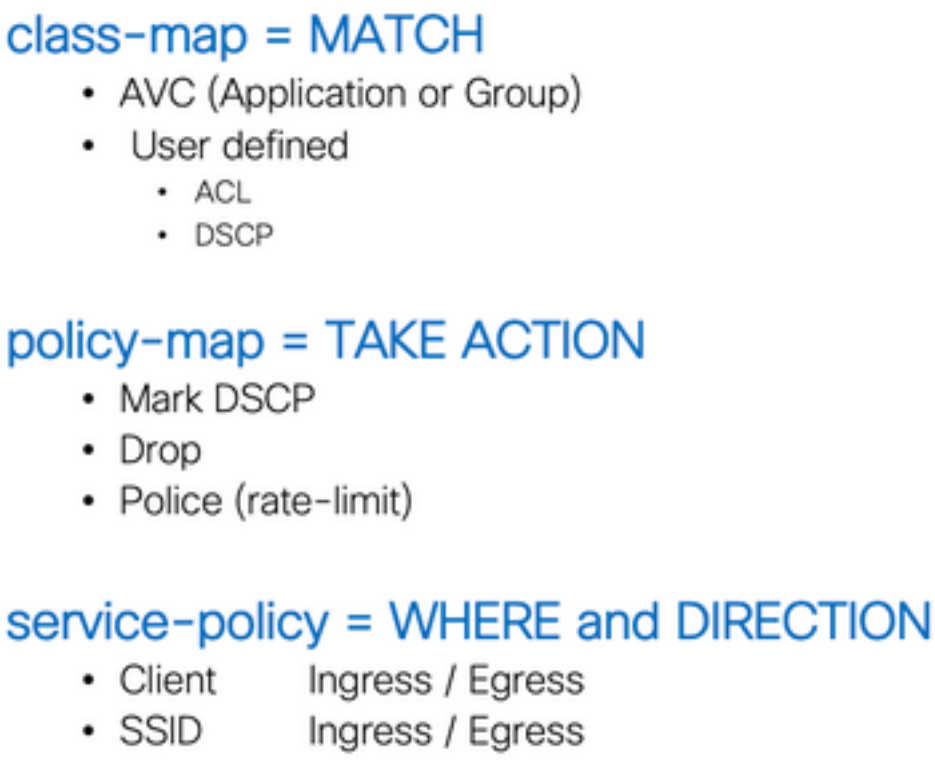
1. 类映射：识别某种流量。类映射能有效利用应用程序可见性和控制(AVC)引擎。并且能定义自定义类映射识别流量匹配访问控制列表(ACL)的用户或差分服务代码点

2. 策略映射：是适用于类映射的策略。
这些策略能指示DSCP、丢弃或者速率限制匹配类映射的流量

4. 服务策略：策略映射在SSID的策略配置文件可以应用或每客户端在某一方向使用service-policy命令。

3. (可选)表映射：他们用于转换标记的一种类型到另一个，例如， Cos到DCSP。

Note: (432);(DSCPCOS)



Note:万一两个或多个策略每个目标是可适用的，在优先级之下选定的根据的策略解决方法：

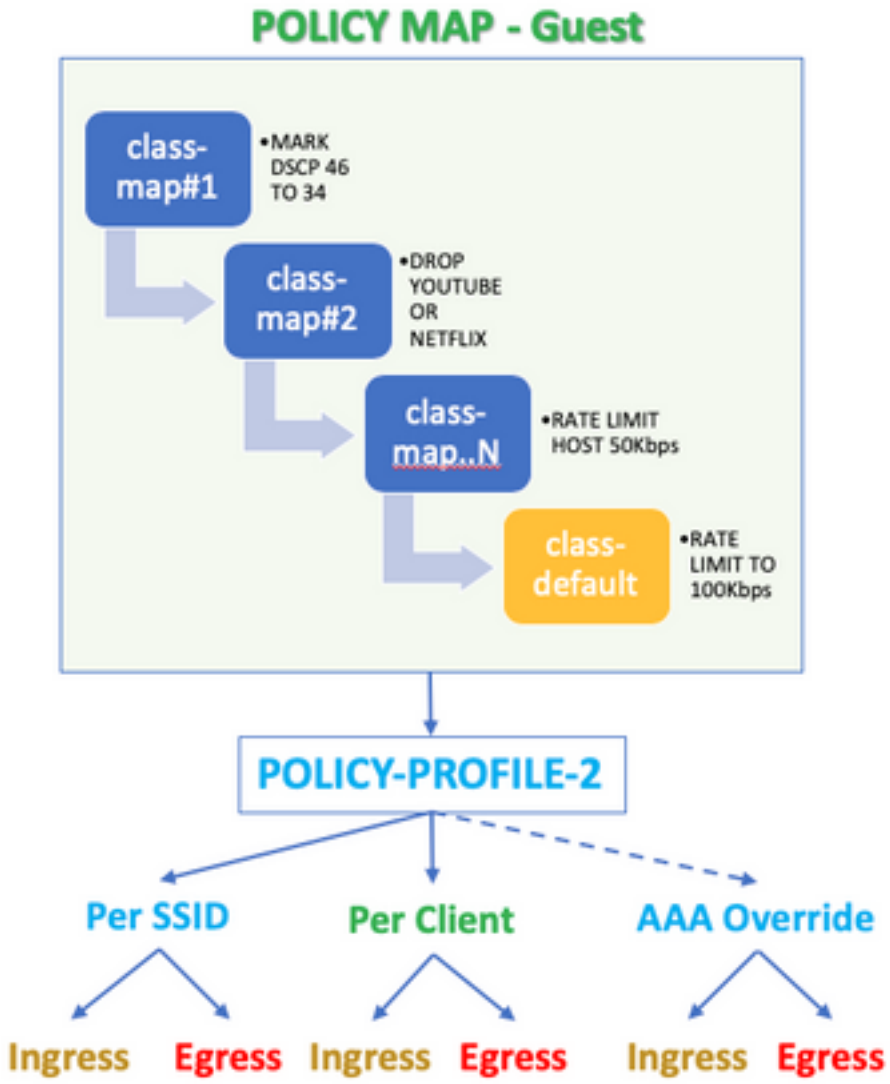
•AAA覆盖(最高)
•本地描出(本地策略)
•已配置的策略
•默认策略(最低)

更多详细信息可以在9800的正式QoS配置指南找到

关于QoS理论的其他信息可以在9000系列QoS配置指南找到

示例：guest和Corp QoS策略

此示例展示解释的QoS组件如何在真实世界方案应用。目的将配置访客的QoS策略那：注释DSCP，丢包Youtube和Netflix视频，速率限制在ACL指定的主机对50Kbps，并且，根本地，速率限制其他流量对100Kbps。

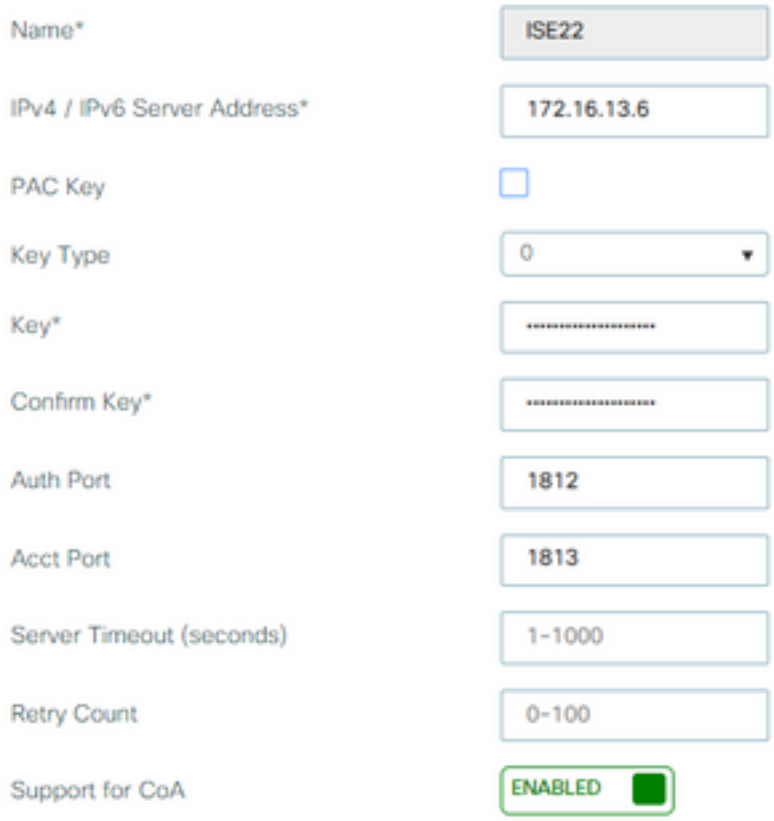


对于示例，应该每在两个方向入口的对该策略的配置文件的SSID和出口应用QoS策略对访客WLAN的链路。

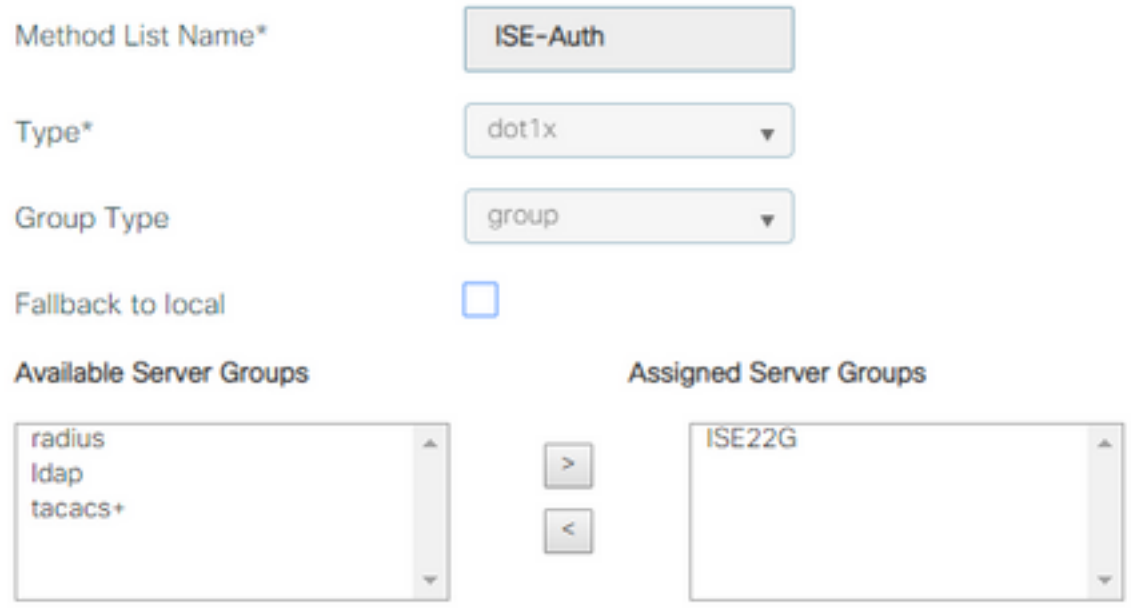
配置

AAA服务器和方法列表

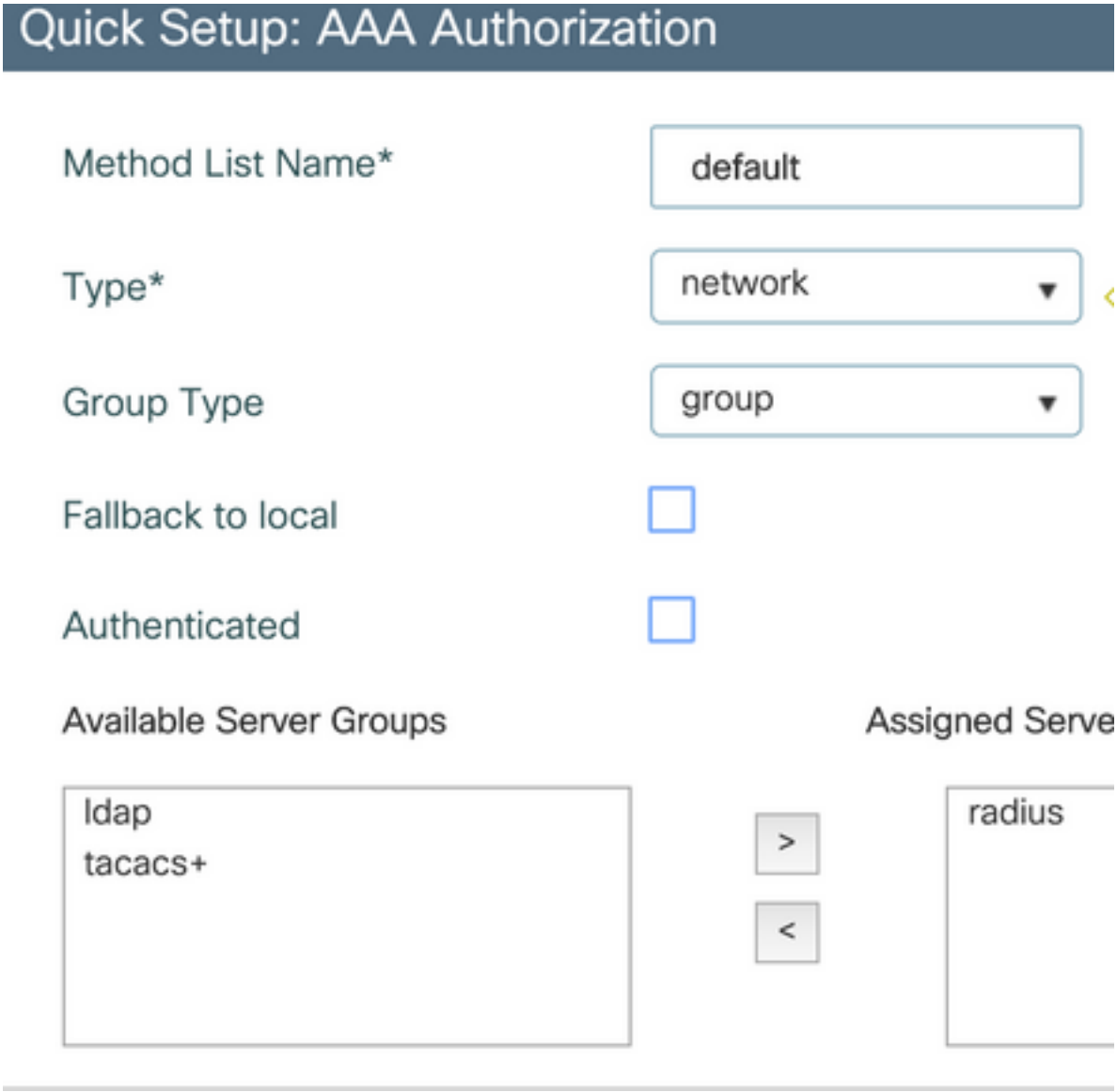
步骤1.导航给**Configuration>安全>AAA >验证>服务器/组**并且选择**+Add。**输入AAA服务器的名称、IP地址和密钥，必须匹配共享机密在**Administration >**在ISE的**网络资源>网络设备下。**



步骤2.导航对**Configuration>安全>AAA >验证>AAA方法列表**并且选择**+Add。**选择从可用服务器组的已分配服务器组。



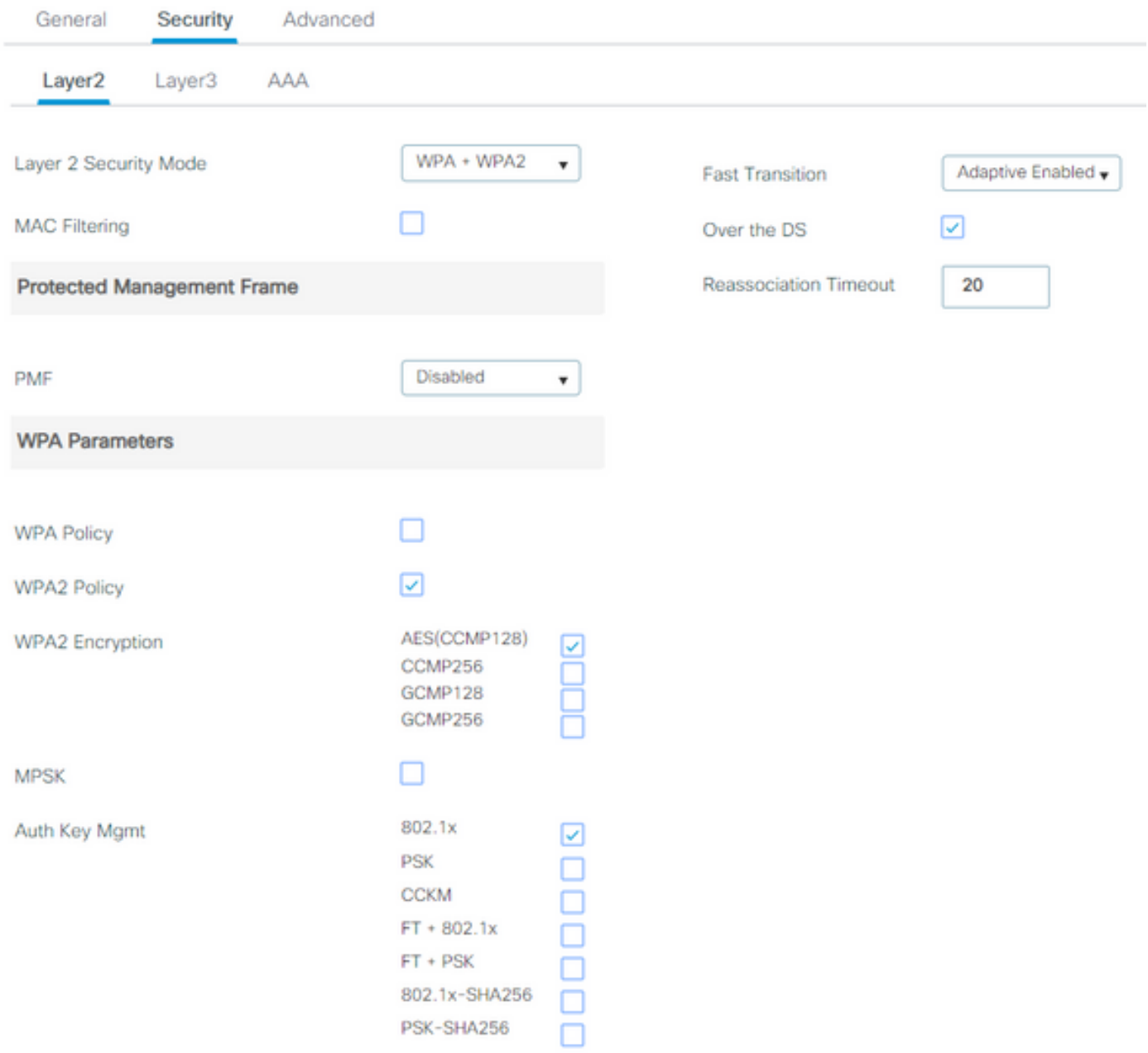
步骤3.导航对**Configuration>安全>AAA >授权>AAA方法列表**并且选择**添加。**选择默认方法和“网络”作为类型。



这要求为了控制器能应用AAA服务器(即此处QoS策略)返回的授权attributres。否则，从RADIUS接收的策略不会应用。

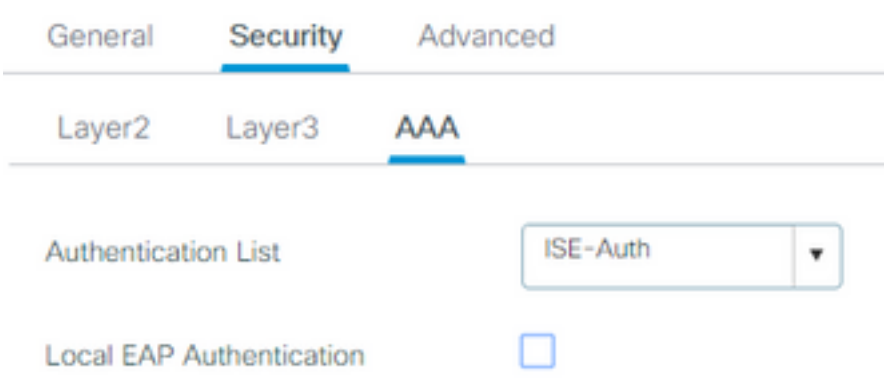
WLAN策略、站点标记和AP标记

步骤1.导航对**Configuration>无线设置>Advanced >开始当前> WLAN配置文件**并且选择**+Add**创建一新的WLAN。配置SSID、配置文件名称、WLAN ID和集状态对已启用。然后，请导航对**安全> Layer2**并且配置Layer2验证参数：



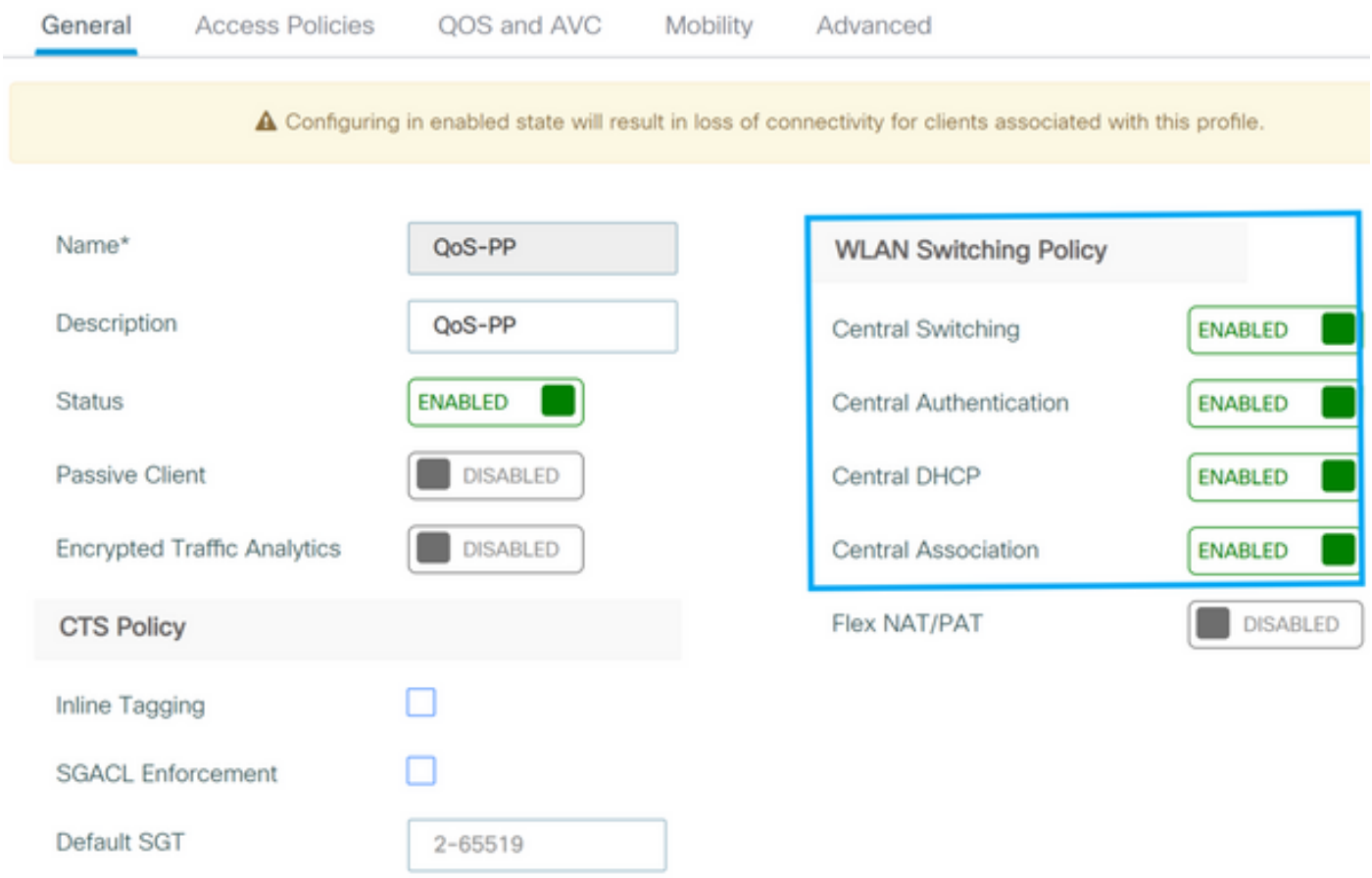
Ssid的安全不必须是802.1x作为QoS的一件必需品，用于此配置示例AAA覆盖。

步骤2.导航对**安全>AAA**并且选择在**认证列表**下拉框的AAA服务器。

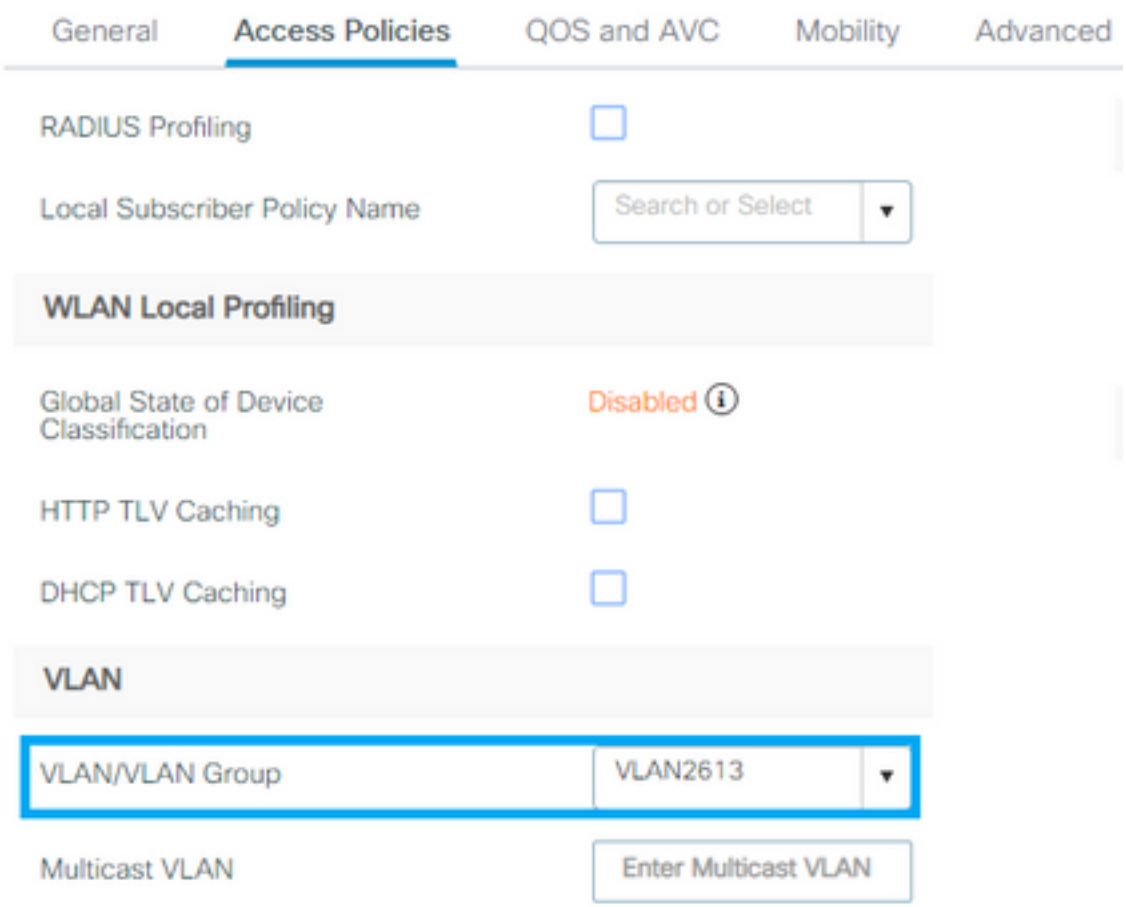


步骤3.选择**策略配置文件**并且选择**+Add。** 配置策略配置文件名称。设置状态如启用;也请启用中央

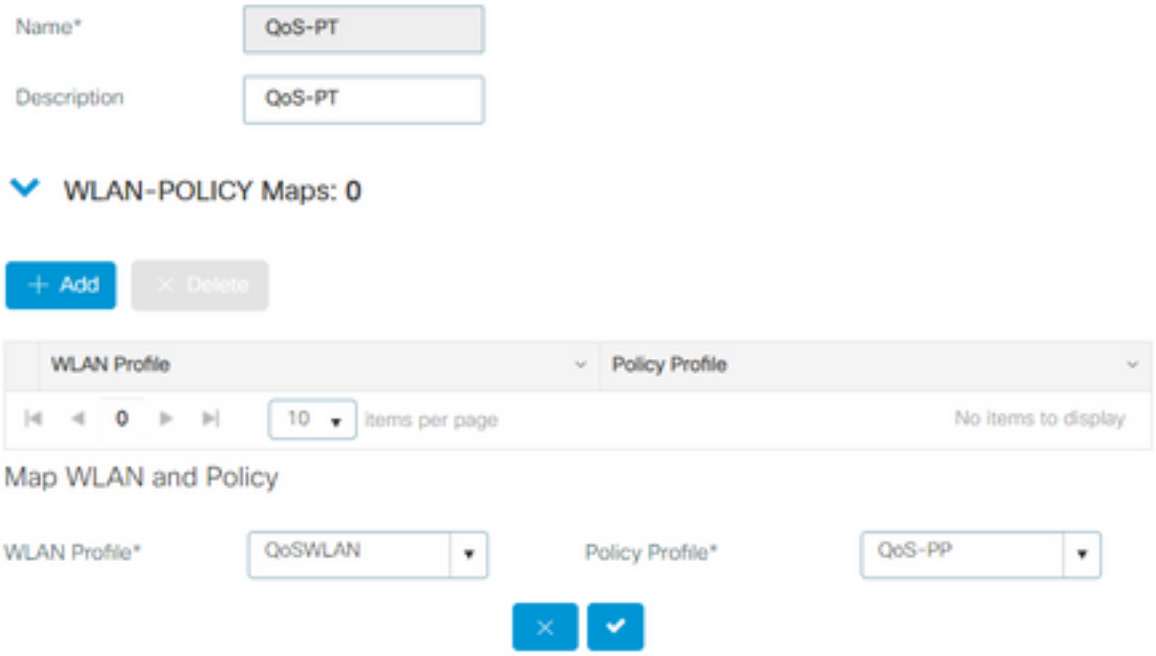
交换、验证、DHCP和关联：



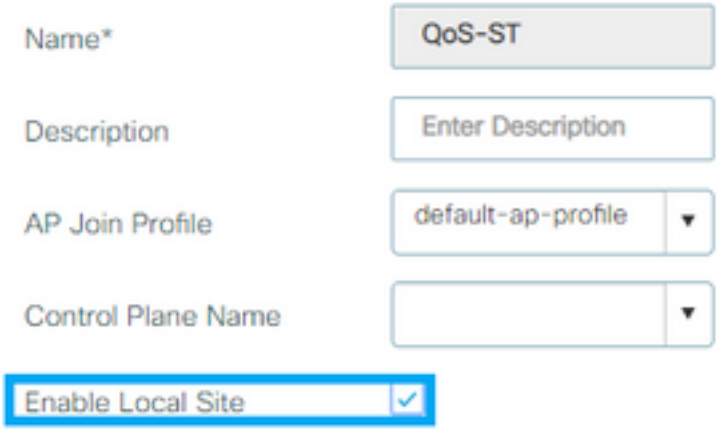
步骤4.导航对**访问策略**并且配置无线客户端将分配对的VLAN，当客户端连接对SSID时：



步骤5.选择**策略标记**并且选择**+Add。**配置策略标记名称。在WLAN**策略地图下，**在**+Add，请**选择**WLAN配置文件，**并且从下拉菜单的**策略配置文件**，选择能将配置的地图的检查。



步骤6.选择**站点标记**并且选择**+Add。**检查**Enable (event)本地站点**方框AP操作在本地传送方式(或留给它uncheked为FlexConnect) ：

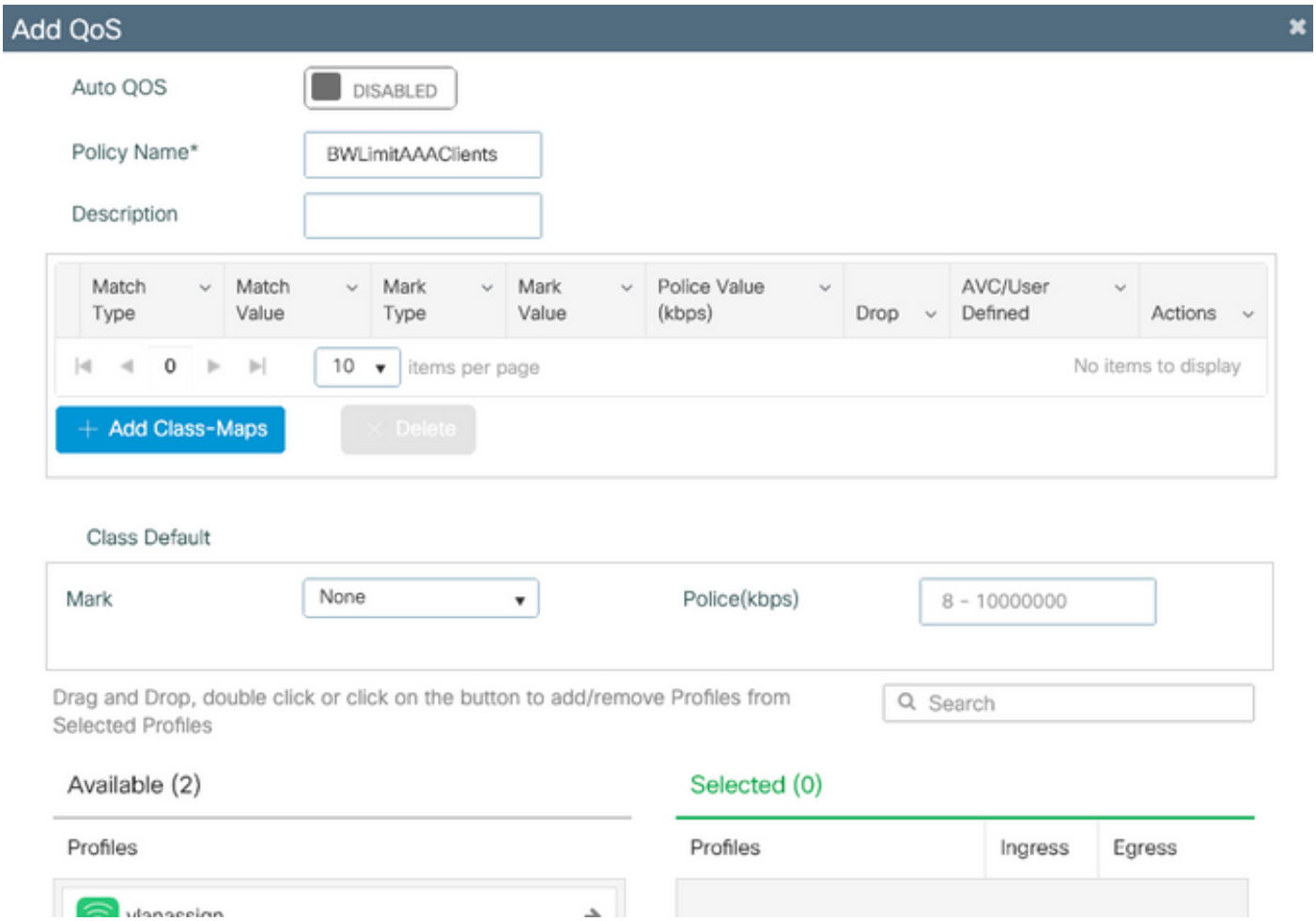


步骤7.选择**标记AP**，选择AP并且添加策略、站点和RF标记：

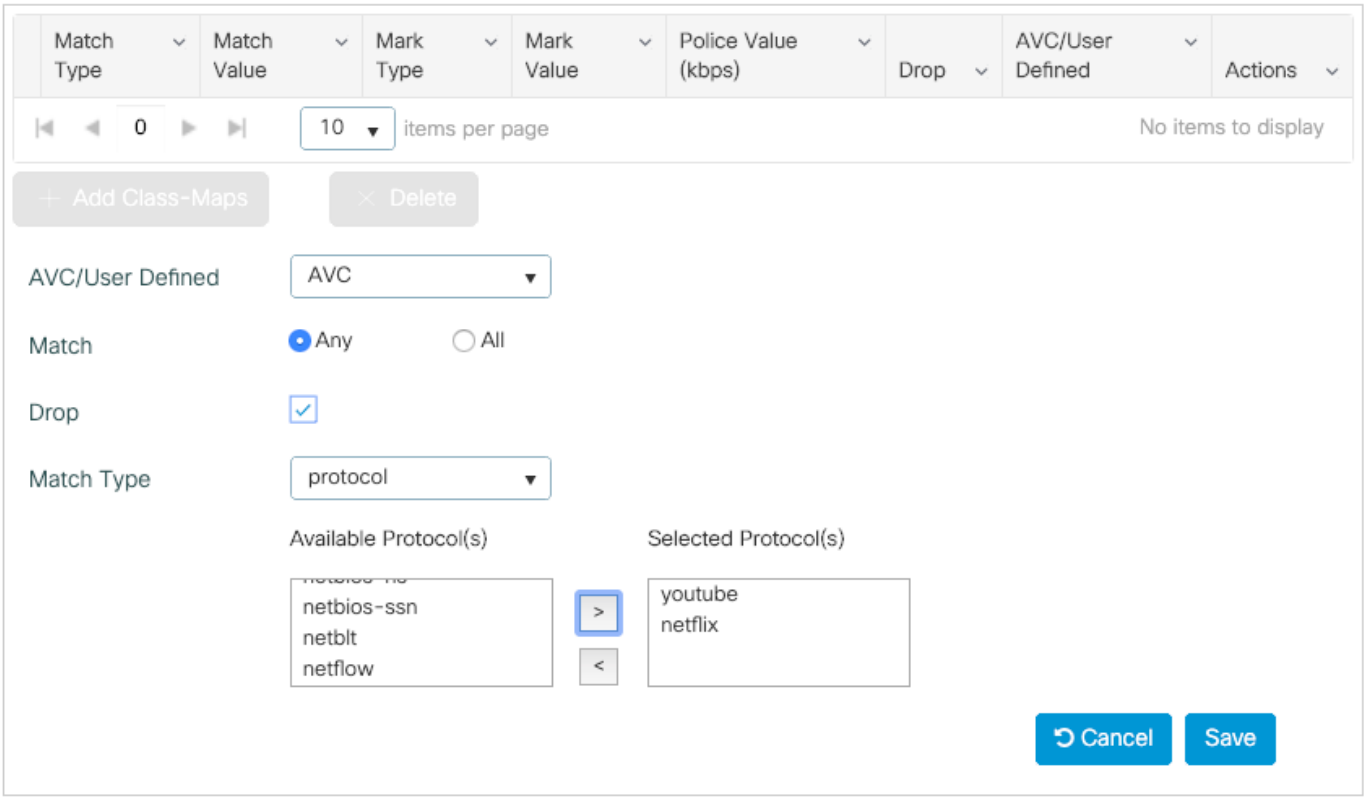
QoS

步骤1.导航对**Configuration> Services> QoS**并且选择**+Add**创建QoS策略。给出它(此示例

：BWLimitAAAClients)。



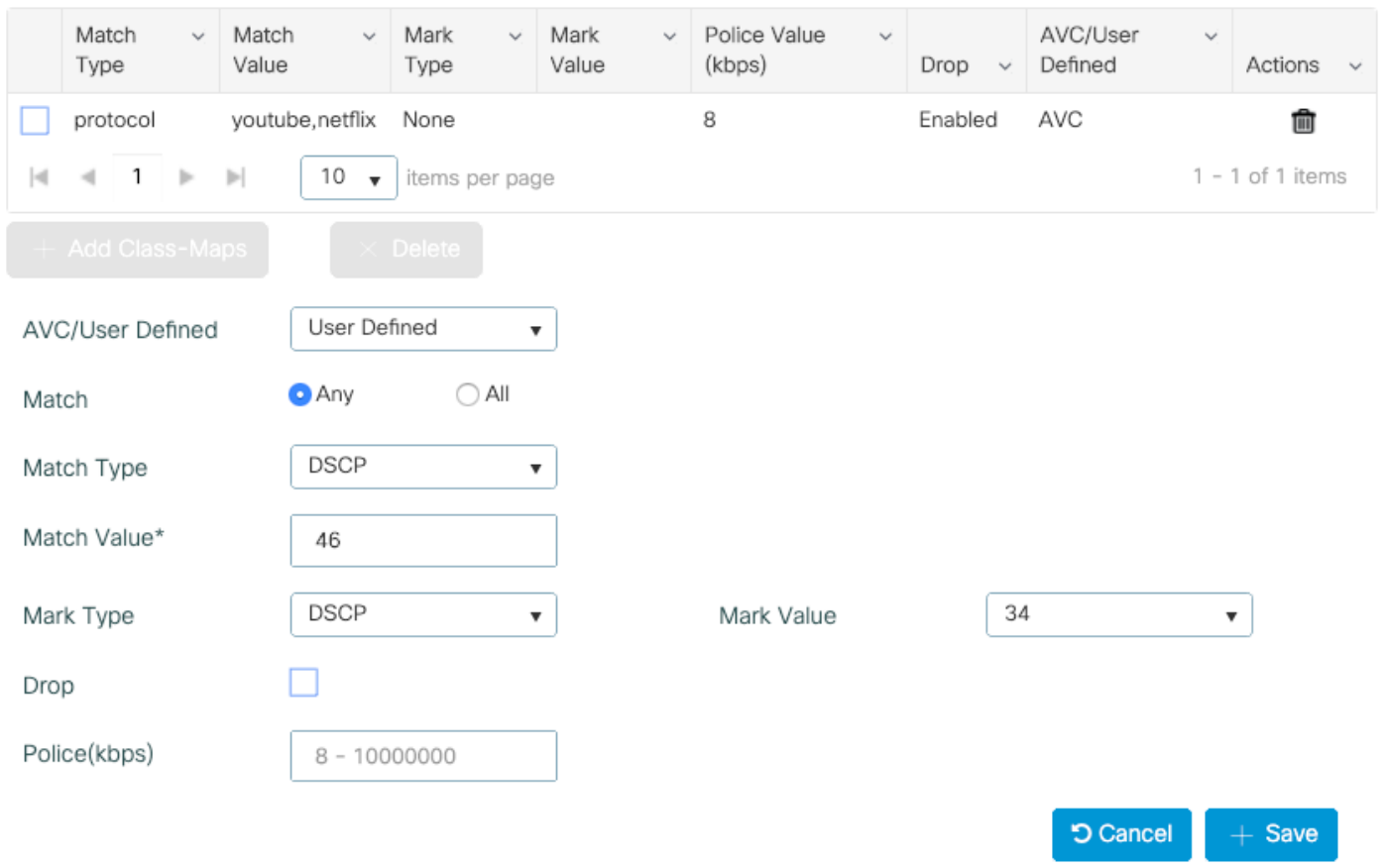
步骤2.添加一个类映射下降Youtube和Netflix。单击**添加类映射**。选择AVC，匹配其中**任一**，**丢弃操作**并且选择两份协议。



命中数**保存。**

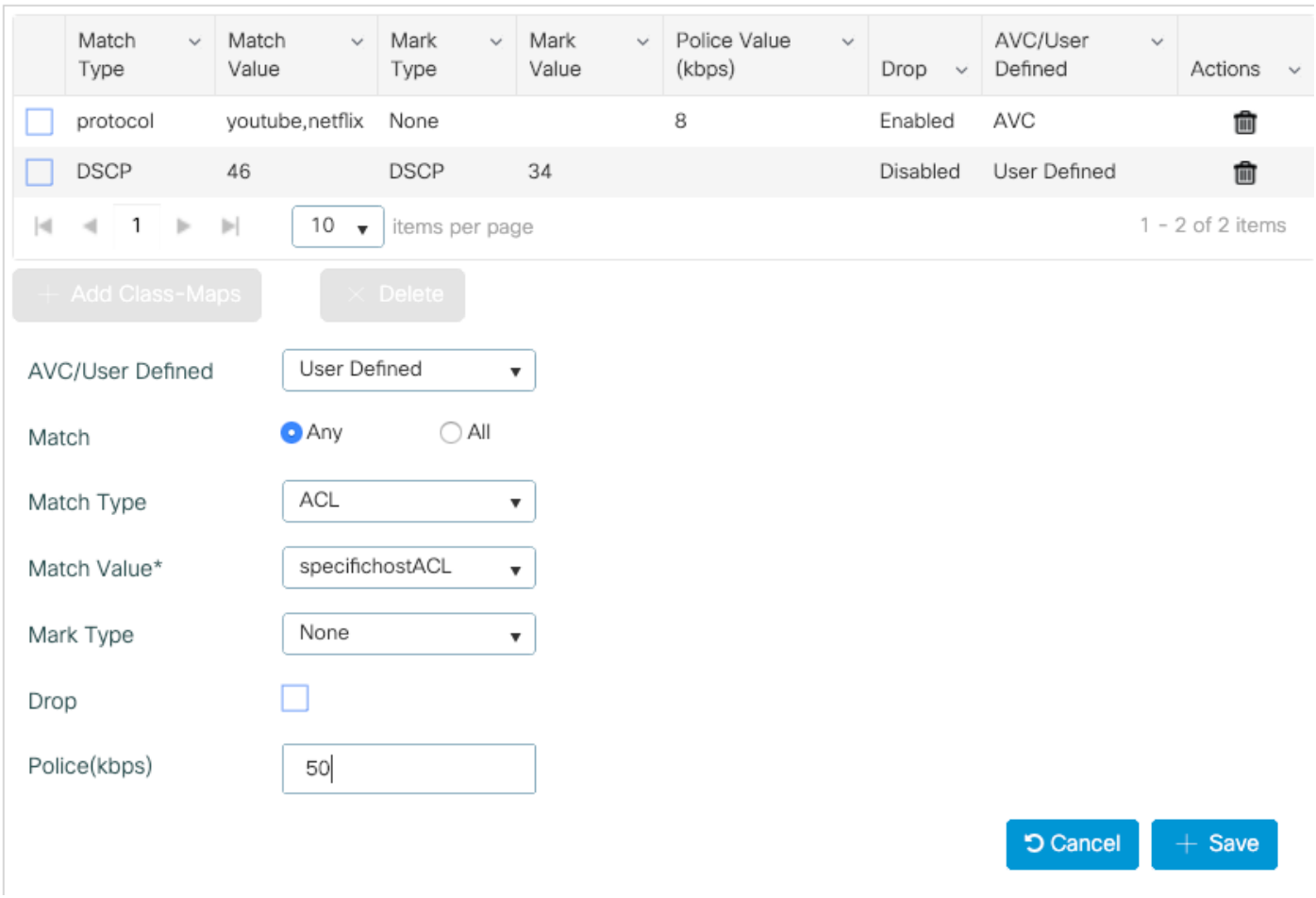
步骤3.添加将重新标明DSCP 46到34的一个类映射。单击**添加类映射**。匹配其中**任一，用户定义**，匹配类型**DSCP**，匹配值**46**，标记类型**DSCP**，标记值**34。**

.。

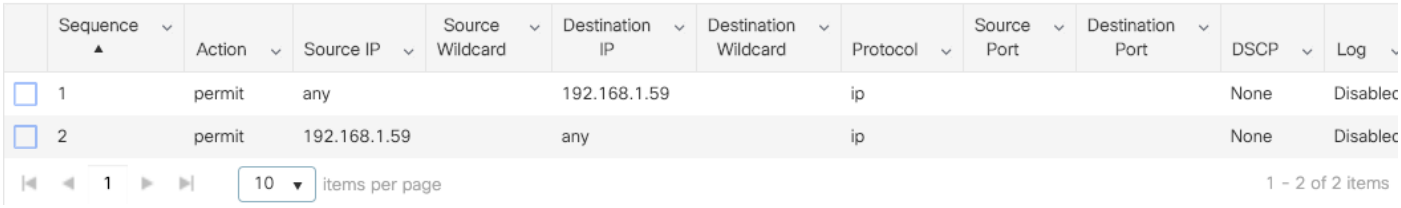


点击**保存。**

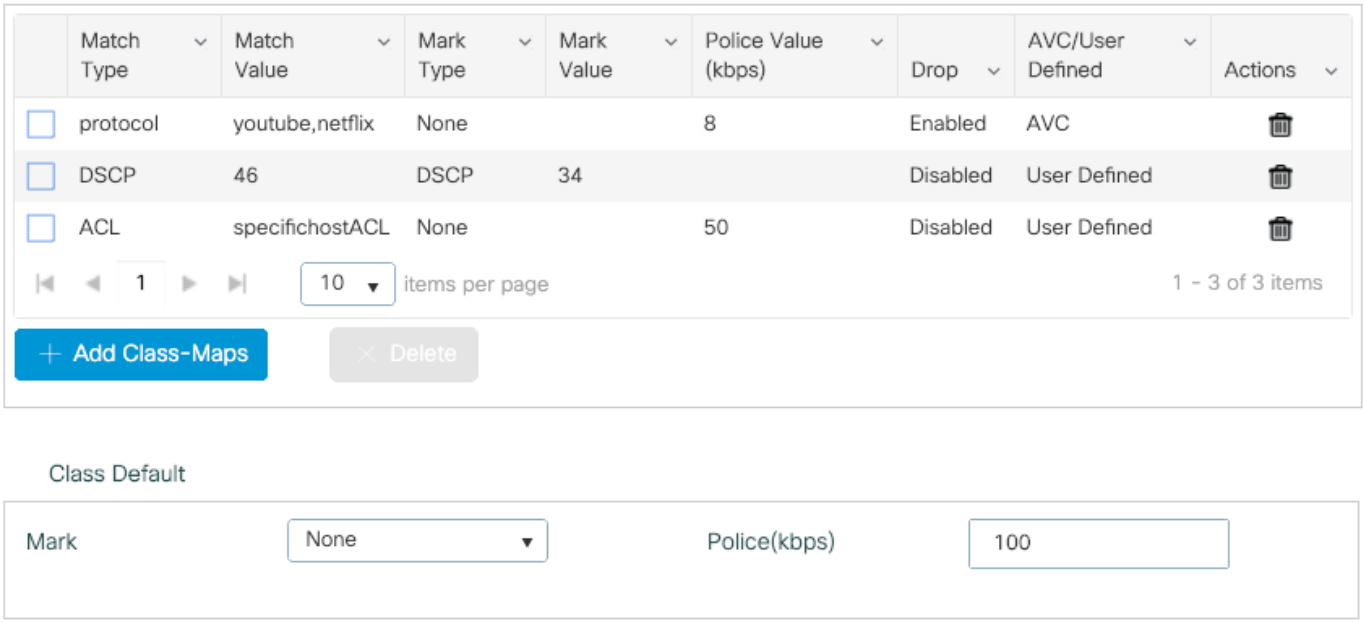
步骤4.为了定义将规定流量到一台特定主机的类映射，您需要创建它的ACL。点击**Add类映射**，选择**用户定义**，匹配其中**任一，**匹配类型**ACL**，选择您的ACL名称(此处**specifichostACL**)，标记类型无并且选择速率限制值。命中数**保存**



对于说明目的，这是我们使用识别一个特定主机流量ACL的示例：



第 5 步：在类映射帧下，请使用默认组设置限制为所有其他流量的速率。这将设置没有由其中一个上面规则瞄准限制在所有客户端的流量的速率。



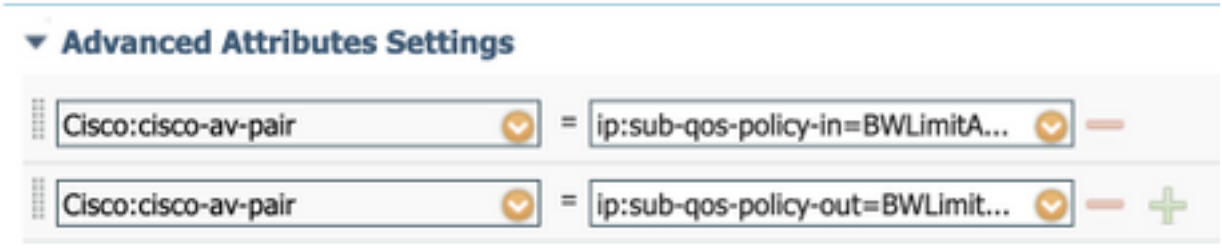
步骤6.点击**Apply到设备**在底部。

CLI等同的配置：

```
policy-map BWLimitAAAclients
 class BWLimitAAAclients1_AVC_UI_CLASS
  police cir 8000
   conform-action drop
   exceed-action drop
 class BWLimitAAAclients1_ADV_UI_CLASS
  set dscp af41
 class BWLimitAAAclients2_ADV_UI_CLASS
  police cir 50000
   conform-action transmit
   exceed-action drop
 class class-default
  police cir 100000
   conform-action transmit
   exceed-action drop


class-map match-all BWLimitAAAclients1_AVC_UI_CLASS
  description BWLimitAAAclients1_AVC_UI_CLASS UI_policy_DO_NOT_CHANGE
 match protocol youtube
 match protocol netflix
class-map match-any BWLimitAAAclients1_ADV_UI_CLASS
  description BWLimitAAAclients1_ADV_UI_CLASS UI_policy_DO_NOT_CHANGE
 match dscp ef
class-map match-all BWLimitAAAclients2_ADV_UI_CLASS
  description BWLimitAAAclients2_ADV_UI_CLASS UI_policy_DO_NOT_CHANGE
 match access-group name specifichostACL
```

> **Note**:在本例中，因为由AAA覆盖，应用**配置文件未**根据QoS策略选择。然而，为了手工运用QoS策略到策略配置文件，请选择希望的配置文件。

Step 2.在ISE，请导航对**策略>Policy元素>结果>授权配置文件**并且选择在**+Add**创建授权配置文件。为了运用QoS策略，请添加他们作为**先进的属性设置**通过Cisco AV对。假设， ISE认证和授权策略配置匹配正确的规则和取得此授权结果。属性是**ip ：sub-qos-policy-in=<policy name>**和**ip ：sub-qos-policy-out=<policyname>**



Note:策略名称区分大小写。确保案件正确!

验证

请使用此部分确认您的配置适当地工作：

在WLC

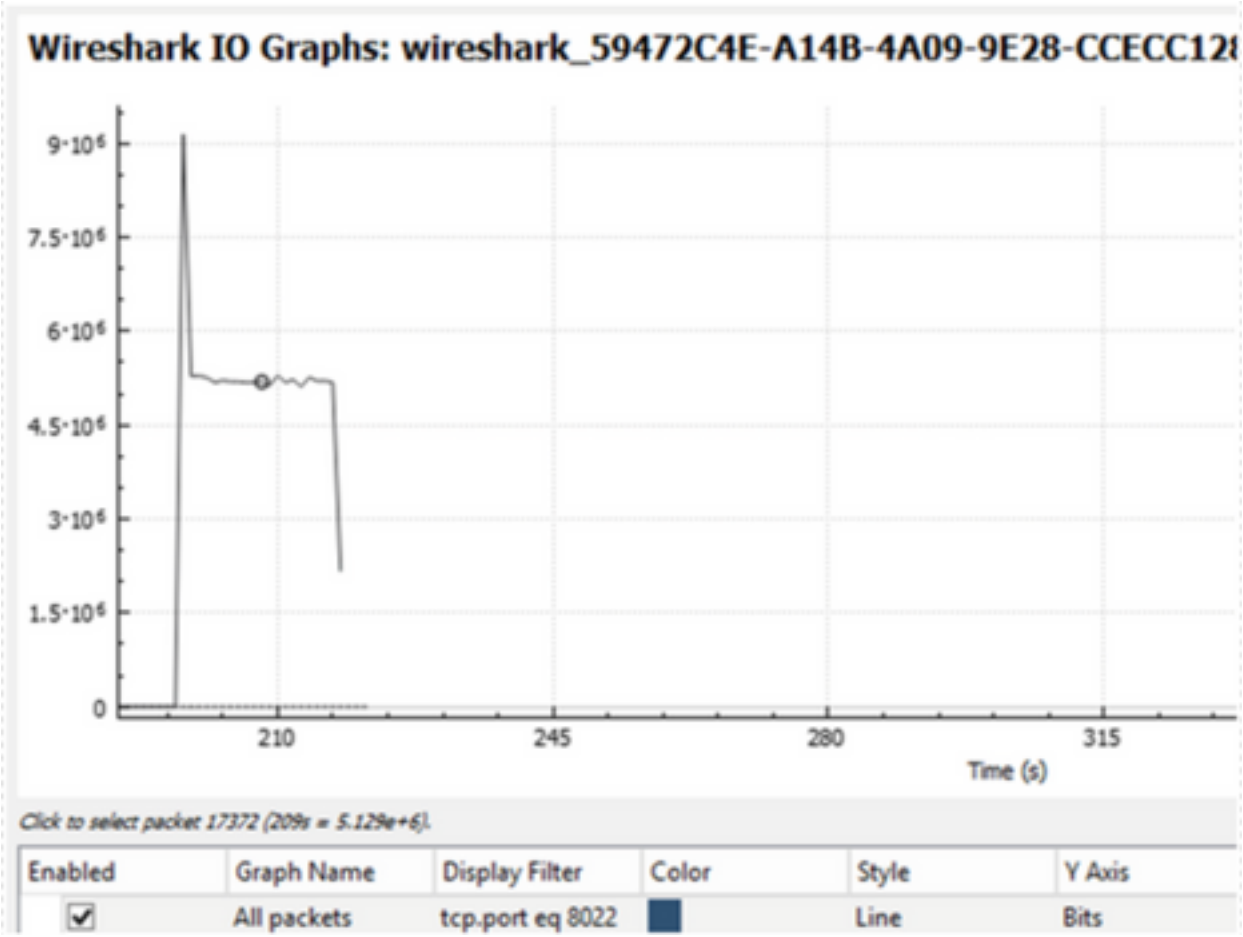
```
# show run wlan
# show run aaa
# show aaa servers
# show ap tag summary
# show ap name <AP-name> tag detail
# show wireless tag policy summary
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
# show policy-map <policy-map name>
# sh policy-map interface wireless ssid/client profile-name <WLAN> radio type <2.4/5GHz> ap name
<name>input/output

# show wireless client mac <client-MAC-address> detail
# show wireless client <client-MAC-address> service-policy input
# show wireless client <client-MAC-address> service-policy output

To verify EDCS parameters :
sh controllers dot11Radio 1 | begin EDCA

9800#show wireless client mac e836.171f.a162 det

Client MAC Address : e836.171f.a162
Client IPv4 Address : 192.168.1.11
Client IPv6 Addresses : fe80::c6e:2ca4:56ea:ffbf
                        2a02:a03f:42c2:8400:187c:4faf:c9f8:ac3c
                        2a02:a03f:42c2:8400:824:e15:6924:ed18
                        fd54:9008:227c:0:1853:9a4:77a2:32ae
                        fd54:9008:227c:0:1507:c911:50cd:2062
Client Username : Nico
```

```
AP MAC Address : 502f.a836.a3e0
AP Name: AP780C-F085-49E6
AP slot : 1
Client State : Associated

(...)

  Local Policies:
  Service Template : wlan_svc_QoS-PP (priority 254)
  VLAN             : 1
  Absolute-Timer   : 1800
  Server Policies:
  Input QOS        : BWLimitAAAClients
  Output QOS       : BWLimitAAAClients
  Resultant Policies:
  VLAN Name         : default
  Input QOS        : BWLimitAAAClients
  Output QOS       : BWLimitAAAClients
  VLAN             : 1
  Absolute-Timer   : 1800
```

在AP

故障排除在AP没有要求，当AP在本地传送方式或在Flexconnect中央交换模式时的SSID， QoS和服务策略由WLC完成。

数据包捕获IO图表分析



故障排除

本部分提供的信息可用于对配置进行故障排除。

步骤1.清除所有已存在的调试情况。

```
# clear platform condition all
```

步骤2.启用有问题的无线客户端的调试。

```
# debug wireless mac <client-MAC-address> {monitor-time <seconds>}
```

步骤3.联络无线客户端对SSID为了再生产问题。

步骤4.，一旦问题被再生产，请终止调试。

```
# no debug wireless mac <client-MAC-address>
```

在测验期间捕获的日志在一个本地文件的WLC存储有名称的：

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

步骤5.为了收集以前生成的文件，您能复制镭trace .log到外部服务器或显示输出直接地在屏幕。用此命令检查RA跟踪文件的名称：

```
# dir bootflash: | inc ra_trace
```

您能复制文件到外部服务器：

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
tftp://a.b.c.d/ra-FILENAME.txt
```

或者请显示内容：

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

步骤6.删除调试条件。

```
# clear platform condition all
```

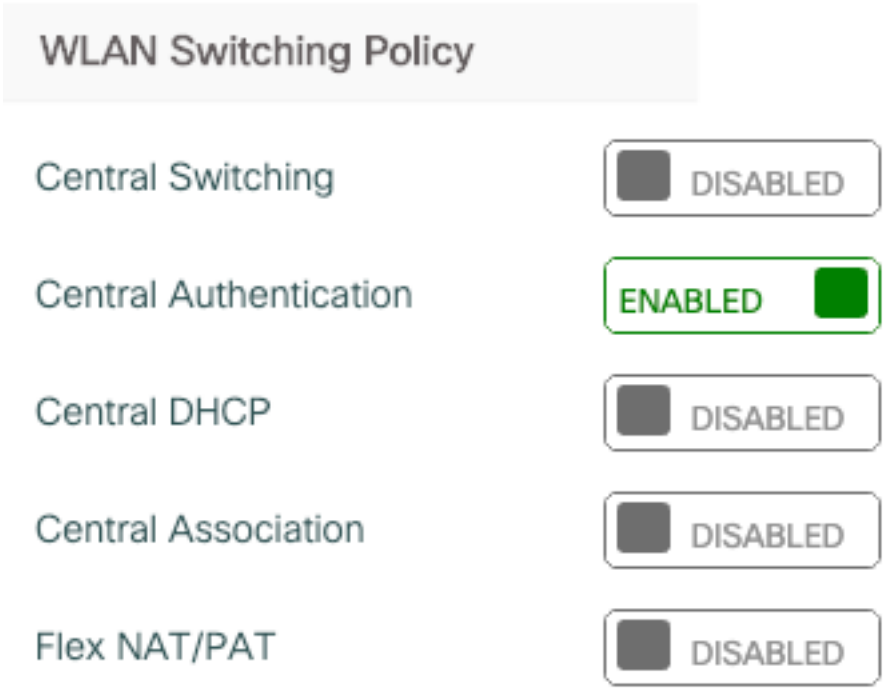
Flexconnect本地交换(或fabric/SDA)方案

在flexconnect本地交换(或结构/SDA的情况下)它是在WLC将运用该所有的QoS策略您定义的AP。

配置

配置正确地是相同的象此条款第一部分有两例外：

1. 策略配置文件设置为本地交换：



2. 站点标记设置不是本地站点：

排除故障Flexconnect/结构

因为AP是应用QoS策略的设备，以下命令可帮助缩小什么应用

显示dot11 qos

show policy-map

显示速率限制客户端

显示速率限制bssid

显示速率限制WLAN

显示flexconnect客户端

```
AP780C-F085-49E6#show dot11 qos
Qos Policy Maps (UPSTREAM)

ratelimit targets:
   Client: A8:DB:03:6F:7A:46

platinum-up targets:
```

```
   VAP: 0 SSID:LAB-DNAS
   VAP: 1 SSID:VlanAssign
   VAP: 2 SSID:LAB-Qos

Qos Stats (UPSTREAM)

total packets:   29279
dropped packets: 0
marked packets:  0
shaped packets:  0
policed packets: 182
copied packets:  0

DSCP TO DOT1P (UPSTREAM)

Default dscp2dot1p Table Value:
[0]->0 [1]->2 [2]->10 [3]->18 [4]->26 [5]->34 [6]->46 [7]->48
Active dscp2dot1p Table Value:
[0]->0 [1]->2 [2]->10 [3]->18 [4]->26 [5]->34 [6]->46 [7]->48

Trust DSCP Upstream : Disabled

Qos Policy Maps (DOWNSTREAM)

ratelimit targets:
   Client: A8:DB:03:6F:7A:46

Qos Stats (DOWNSTREAM)

total packets:   25673
dropped packets: 0
marked packets:  0
shaped packets:  0
policed packets: 150
copied packets:  0

DSCP TO DOT1P (DOWNSTREAM)

Default dscp2dot1p Table Value:
[0]->0 [1]->-1 [2]->1 [3]->-1 [4]->1 [5]->-1 [6]->1 [7]->-1
[8]->-1 [9]->-1 [10]->2 [11]->-1 [12]->2 [13]->-1 [14]->2 [15]->-1
[16]->-1 [17]->-1 [18]->3 [19]->-1 [20]->3 [21]->-1 [22]->3 [23]->-1
[24]->-1 [25]->-1 [26]->4 [27]->-1 [28]->-1 [29]->-1 [30]->-1 [31]->-1
[32]->-1 [33]->-1 [34]->5 [35]->-1 [36]->-1 [37]->-1 [38]->-1 [39]->-1
[40]->-1 [41]->-1 [42]->-1 [43]->-1 [44]->-1 [45]->-1 [46]->6 [47]->-1
[48]->7 [49]->-1 [50]->-1 [51]->-1 [52]->-1 [53]->-1 [54]->-1 [55]->-1
[56]->7 [57]->-1 [58]->-1 [59]->-1 [60]->-1 [61]->-1 [62]->-1 [63]->-1
Active dscp2dot1p Table Value:
[0]->0 [1]->0 [2]->1 [3]->0 [4]->1 [5]->0 [6]->1 [7]->0
[8]->1 [9]->1 [10]->2 [11]->1 [12]->2 [13]->1 [14]->2 [15]->1
[16]->2 [17]->2 [18]->3 [19]->2 [20]->3 [21]->2 [22]->3 [23]->2
[24]->3 [25]->3 [26]->4 [27]->3 [28]->3 [29]->3 [30]->3 [31]->3
[32]->4 [33]->4 [34]->5 [35]->4 [36]->4 [37]->4 [38]->4 [39]->4
[40]->5 [41]->5 [42]->5 [43]->5 [44]->5 [45]->5 [46]->6 [47]->5
[48]->7 [49]->6 [50]->6 [51]->6 [52]->6 [53]->6 [54]->6 [55]->6
[56]->7 [57]->7 [58]->7 [59]->7 [60]->7 [61]->7 [62]->7 [63]->7

Profinet packet recieved from
wired port:
0
wireless port:
?
```

```
AP780C-F085-49E6#show policy-map
2 policymaps
Policy Map BWLimitAAAClients            type:qos client:default
    Class BWLimitAAAClients_AVC_UI_CLASS
      drop

    Class BWLimitAAAClients_ADV_UI_CLASS
      set dscp af41 (34)


    Class class-default
      police rate 5000000 bps (625000Bytes/s)
        conform-action
        exceed-action


Policy Map platinum-up          type:qos client:default
    Class cm-dscp-set1-for-up-4
      set dscp af41 (34)


    Class cm-dscp-set2-for-up-4
      set dscp af41 (34)


    Class cm-dscp-for-up-5
      set dscp af41 (34)


    Class cm-dscp-for-up-6
      set dscp ef (46)


    Class cm-dscp-for-up-7
      set dscp ef (46)


    Class class-default
      no actions


AP780C-F085-49E6#show rate-limit client
Config:
              mac vap rt_rate_out rt_rate_in rt_burst_out rt_burst_in nrt_rate_out nrt_rate_in
nrt_burst_out nrt_burst_in
A8:DB:03:6F:7A:46   2           0          0            0           0            0           0
0            0
Statistics:
            name    up  down
        Unshaped     0     0
  Client RT pass     0     0
 Client NRT pass     0     0
 Client RT drops     0     0
Client NRT drops     0 38621
               9 54922     0
AP780C-F085-49E6#

AP780C-F085-49E6#show flexconnect client
Flexconnect Clients:

              mac radio vap aid state       encr aaa-vlan aaa-acl aaa-ipv6-acl assoc    auth
switching key-method    roam key-progmed handshake-sent wgb SGT
A8:DB:03:6F:7A:46     1   2   1   FWD AES_CCM128     none    none         none Local Central
Local      Other regular          No            Yes  No   0
```

AP780C-F085-49E6#

参考资料

Catalyst 9000 16.12 QoS指南

9800 QoS配置指南

Catalyst 9800配置型号