在具有AAA覆盖的Catalyst 9800无线控制器上配置QoS (BDRL)速率限制

目录

简介

本文档介绍Catalyst 9800系列无线控制器上的双向速率限制(BDRL)的配置示例。

先决条件

要求

Cisco 建议您了解以下主题：

- Catalyst Wireless 9800配置型号
- 使用思科身份服务引擎(ISE)的AAA

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

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

9800 WLC平台中的QoS使用与Catalyst 9000平台相同的概念和组件。

本部分提供有关这些组件如何工作以及如何配置它们以实现不同结果的全局概述。

实质上，QoS递归的工作方式如下：

1. Class-Map：标识特定类型的流量。类映射可以利用应用可视性与可控性(AVC)引擎。

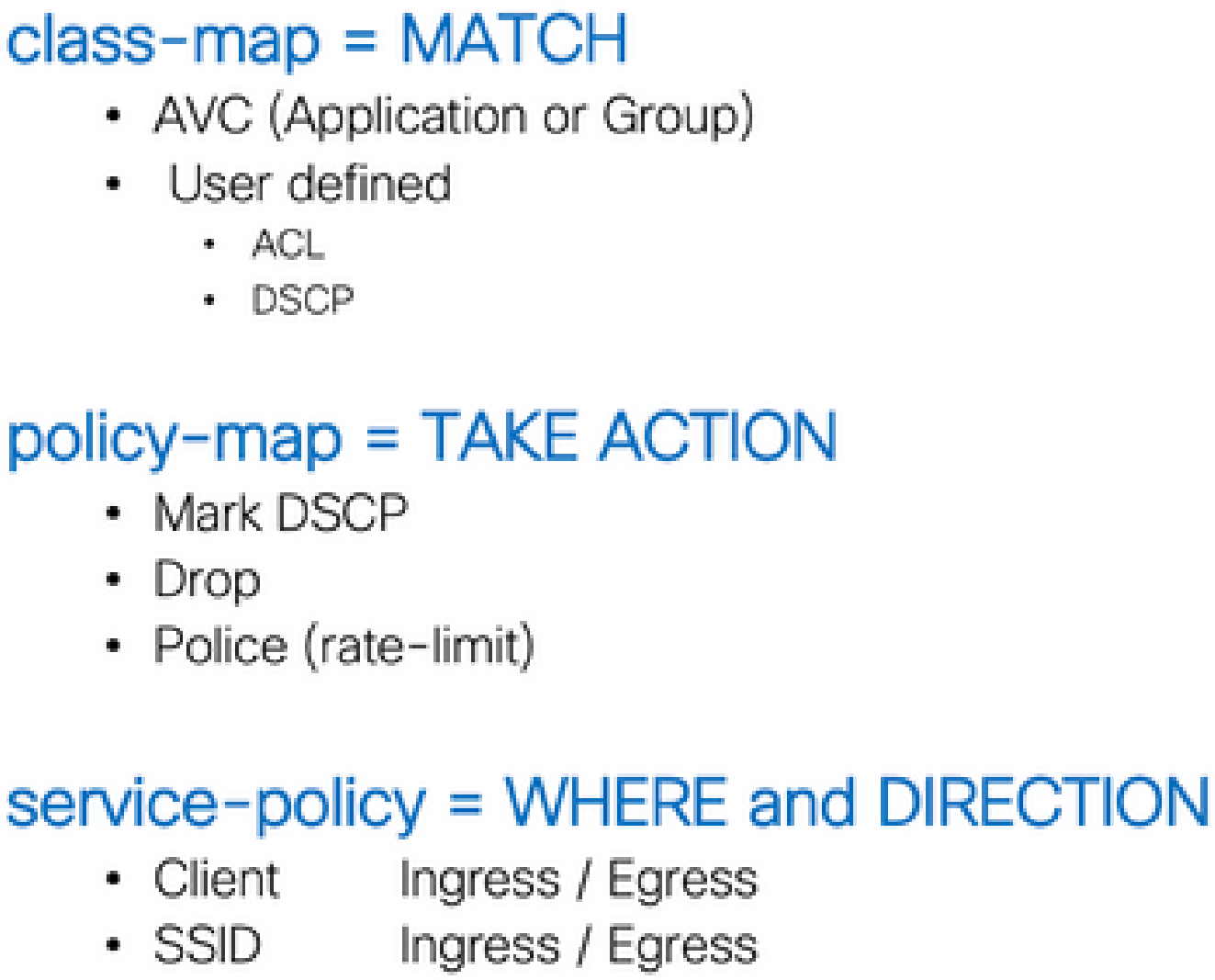
此外，用户可以定义自定义类映射以识别与访问控制列表(ACL)或差分服务代码点(DSCP)匹配的流量

2. 策略映射：是应用于类映射的策略。
这些策略可以标记DSCP、丢弃或速率限制与类映射匹配的流量

4. Service-Policy：使用service-policy命令，可以在特定方向上的SSID的策略配置文件或每客户端上应用策略映射。

3.（可选）表映射：用于将一种标记转换为另一种标记，例如CoS转换为DCSP。

注意：在表映射中，指定要更改的值（4到32）；在策略映射中，指定了技术（COS到DSCP）。



注意：如果每个目标适用两个或多个策略，则根据以下优先级排名选择策略解决方案：

· AAA覆盖（最高）
· 本机分析（本地策略）
· 配置的策略
· 默认策略（最低）

有关详细信息，请参阅9800官方QoS配置指南

有关QoS理论的其他信息，请参阅9000系列QoS配置指南

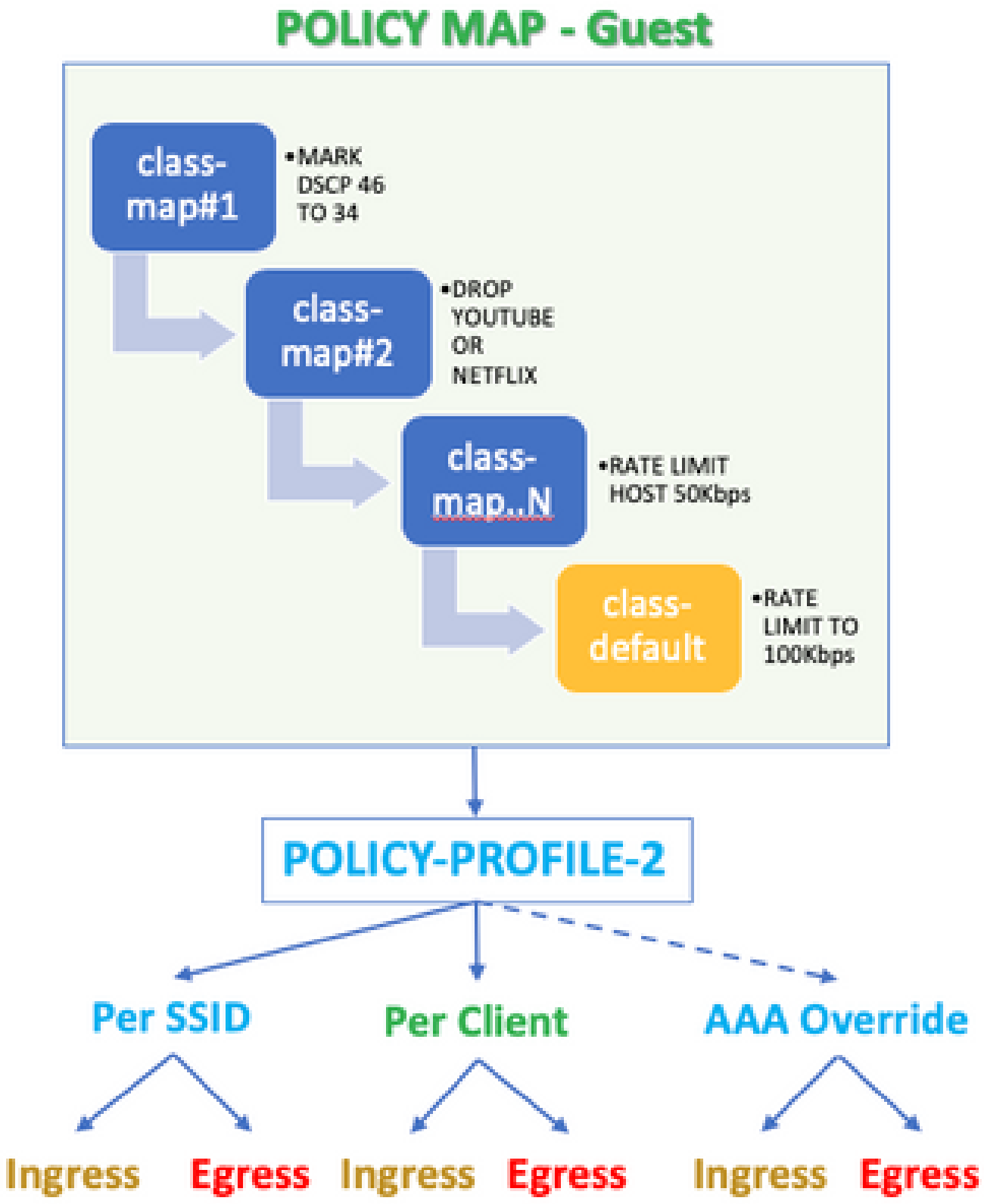
示例：访客和公司QoS策略

此示例演示说明的QoS组件如何应用于实际场景。

目的是为访客配置QoS策略，该策略应：

- 备注DSCP
- 丢弃Youtube和Netflix视频

- ACL中指定的主机的速率限制为50Kbps
- 将所有其他流量速率限制为100Kbps



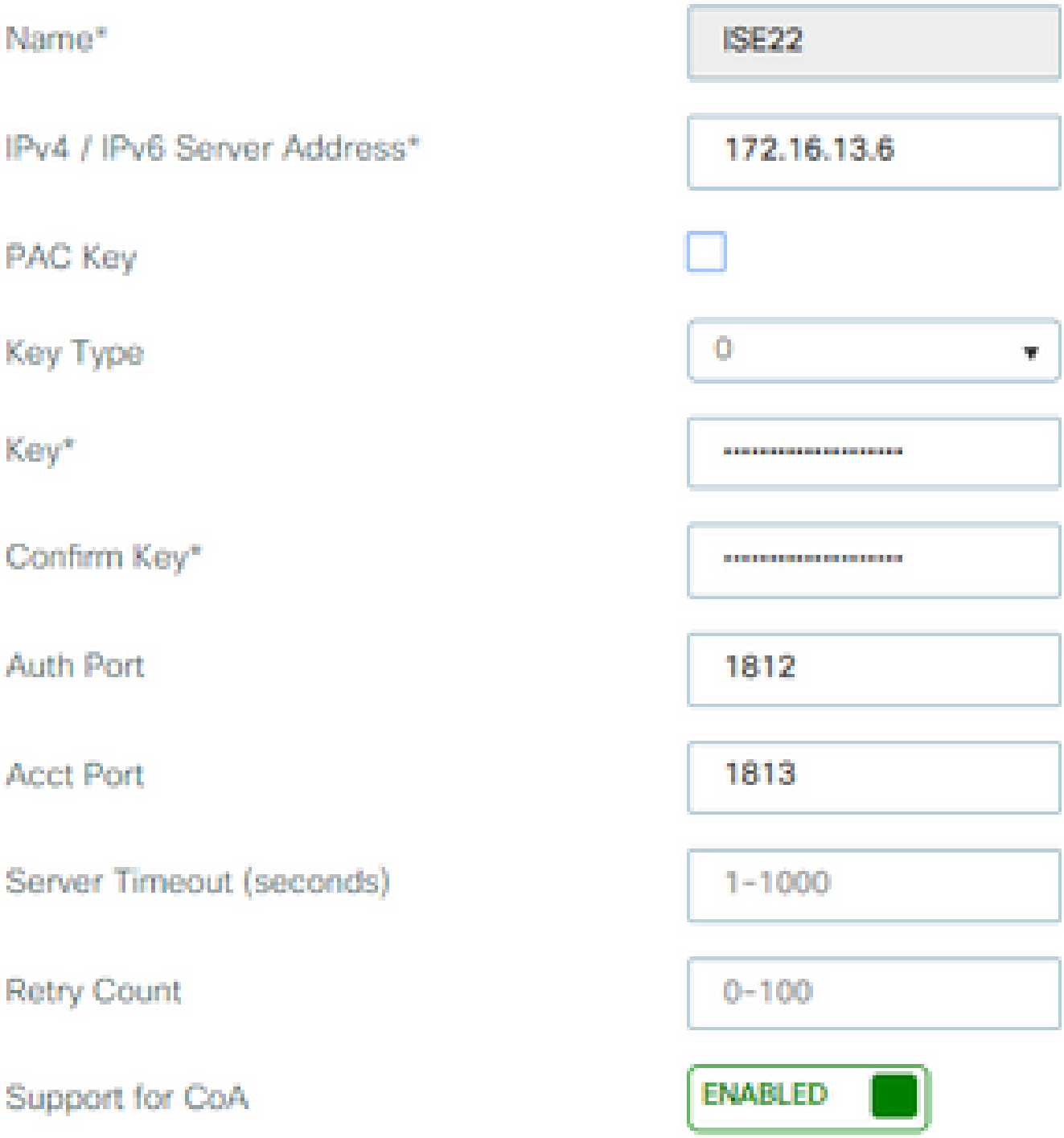
例如，QoS策略必须在每个SSID的入口和出口两个方向应用到链接到访客WLAN的策略配置文件。

配置

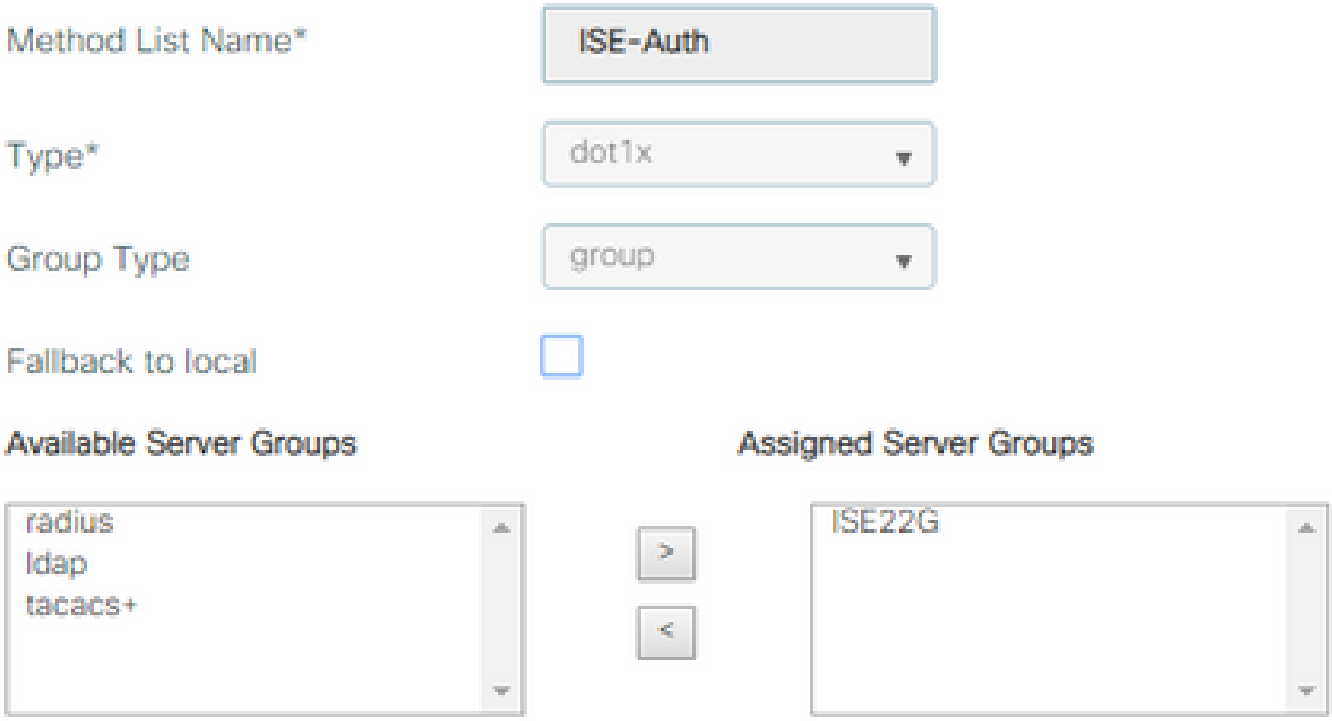
AAA服务器和方法列表

步骤1:导航到Configuration > Security > AAA > Authentication > Servers/Groups，然后选择+Add。

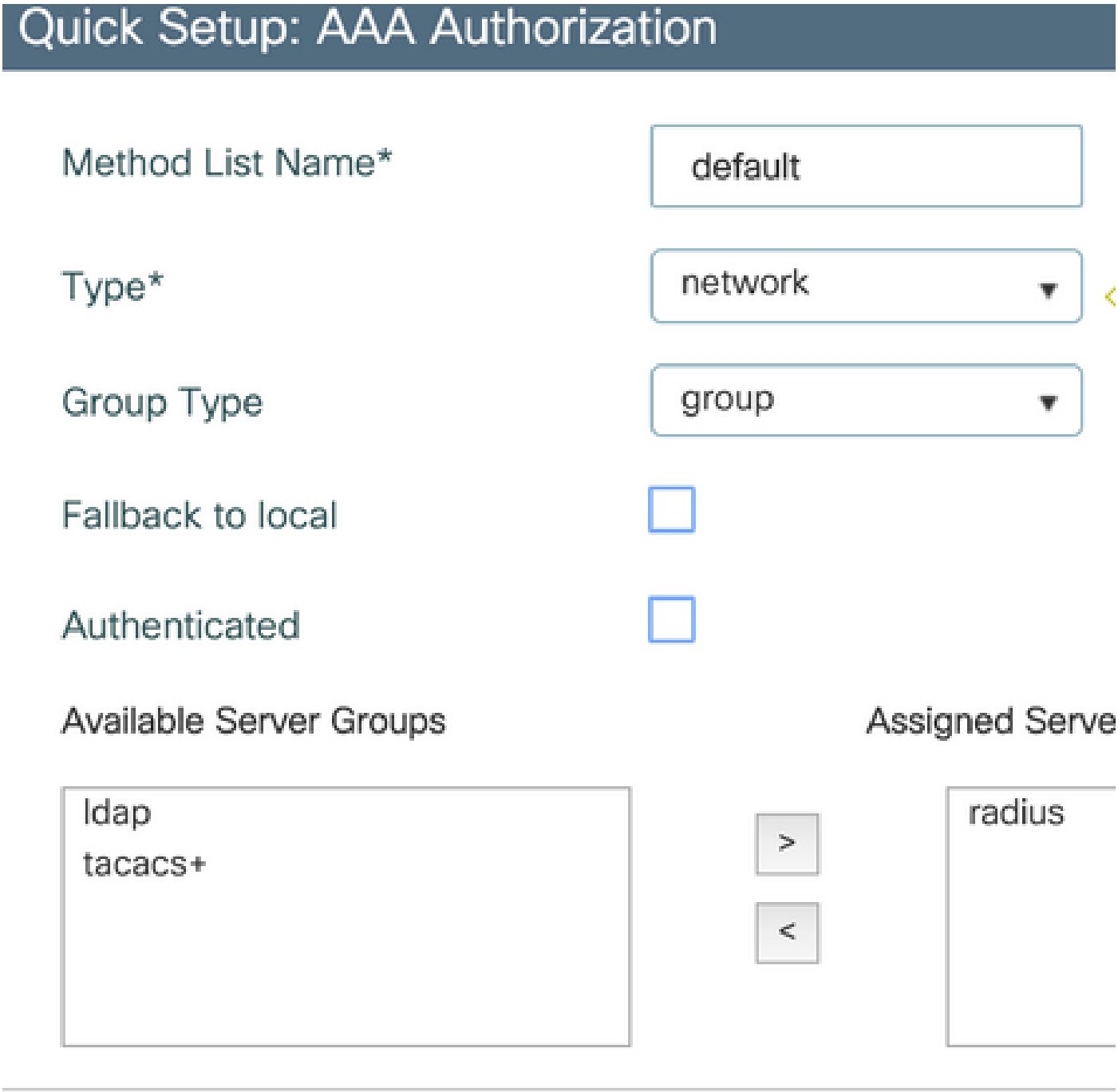
输入AAA服务器名称、IP地址和密钥，这必须与ISE上Administration > Network Resources > Network Devices下的共享密钥匹配。



第二步： 导航到Configuration > Security > AAA > Authentication > AAA Method List，然后选择+Add。从Available Server Groups中选择Assigned Server Groups。



第三步：导航到Configuration > Security > AAA > Authorization > AAA method List，然后选择Add。选择默认方法，然后选择“network”作为类型。

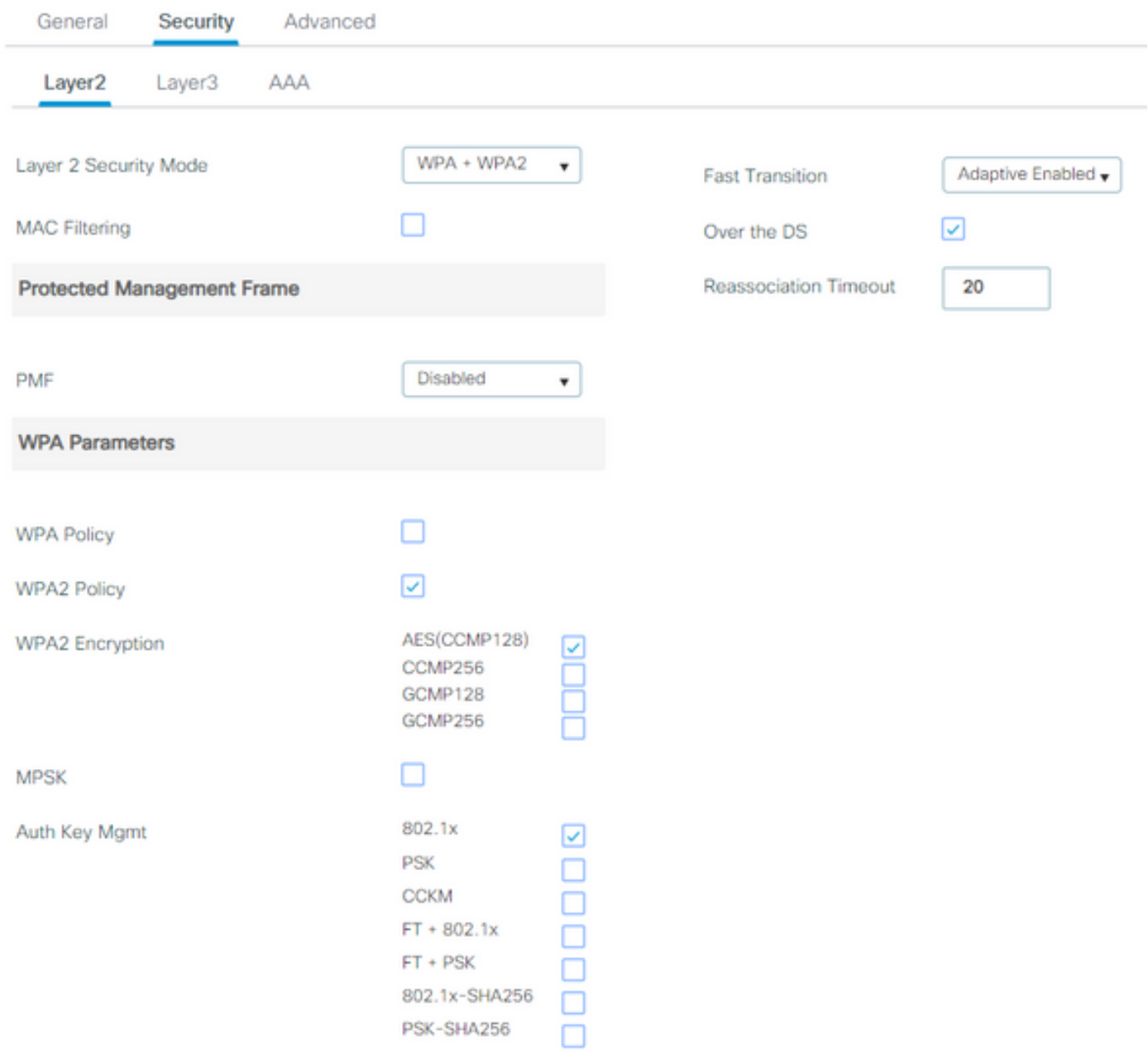


控制器必须应用由AAA服务器返回的授权属性（例如，此处的QoS策略）。否则，不会应用从RADIUS接收的策略。

WLAN策略、站点标签和AP标签

步骤1:导航到配置>无线设置>高级>立即启动> WLAN配置文件，选择+添加创建新的WLAN。配置SSID、配置文件名称、WLAN ID并将状态设置为启用。

然后，导航到Security > Layer 2并配置第2层身份验证参数：

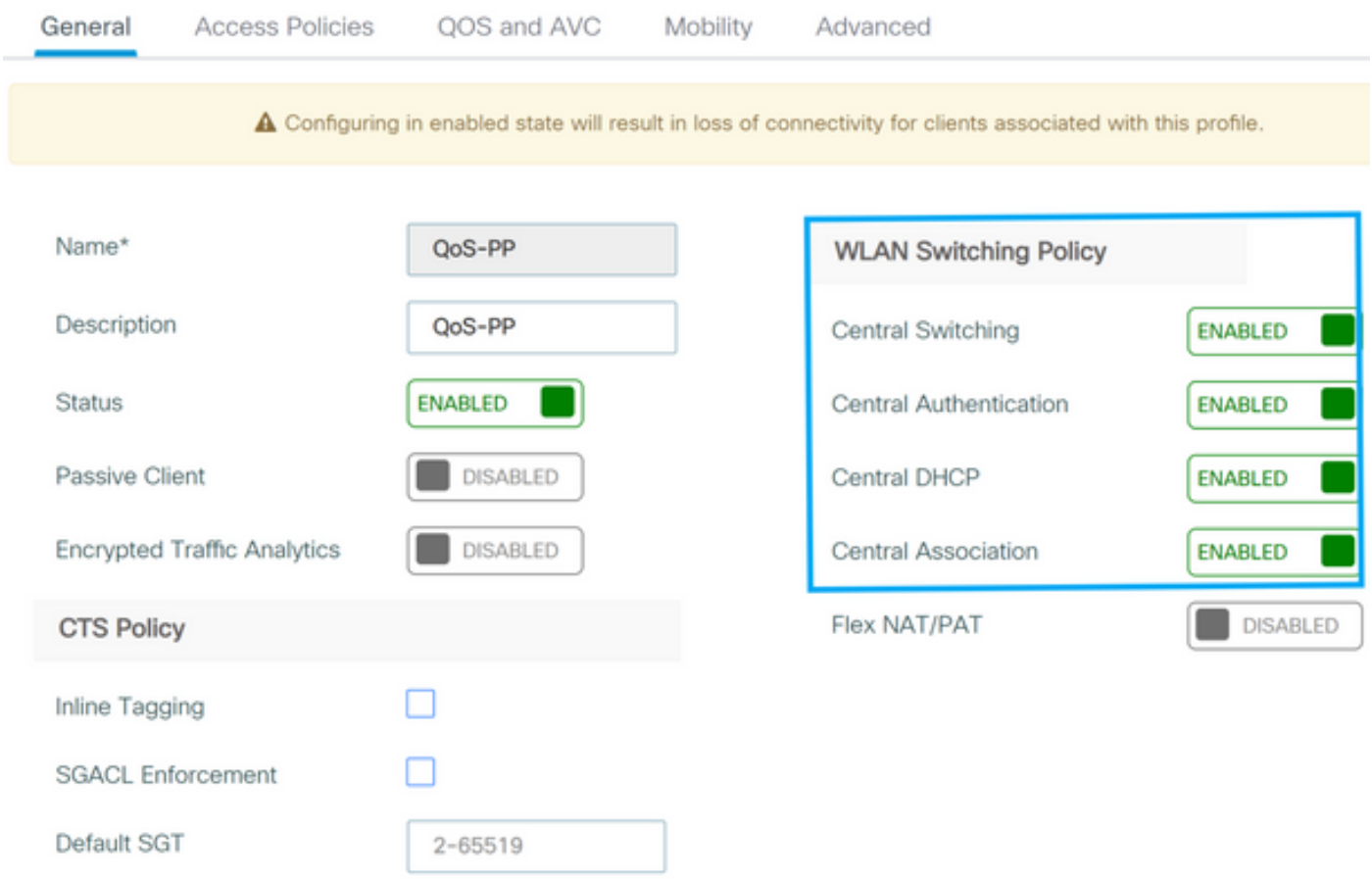


SSID安全性不必是802.1x作为QoS的必要条件，但在本配置示例中仍用于AAA覆盖。

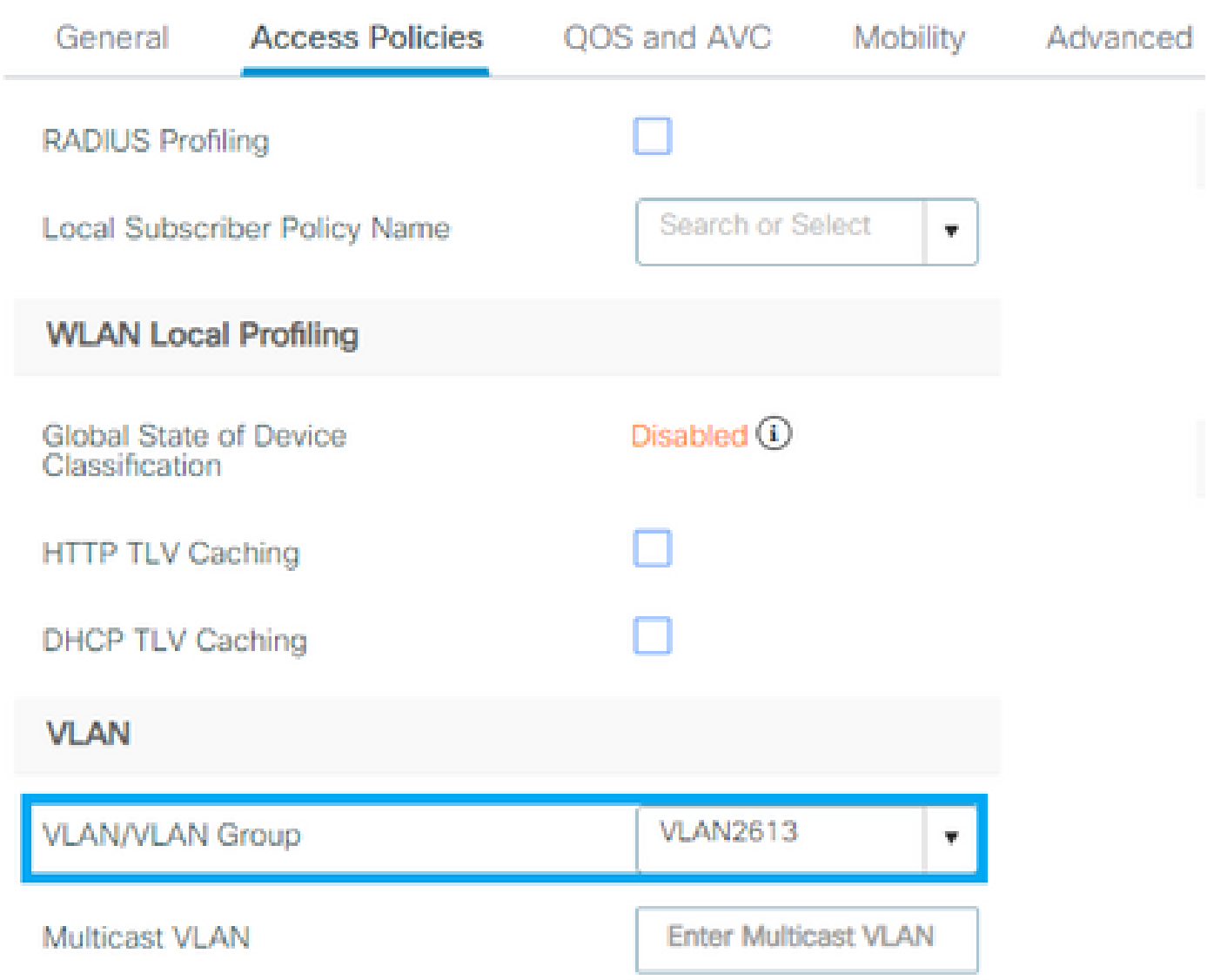
第二步：导航到Security > AAA，然后在Authentication List 下拉框中选择AAA服务器。

第三步：选择Policy Profile 并选择+Add。 配置策略配置文件名称。

将Status（状态）设置为Enabled（启用）；同时启用Central Switching（集中交换）、Authentication（身份验证）、DHCP(DHCP)和Association（关联）：

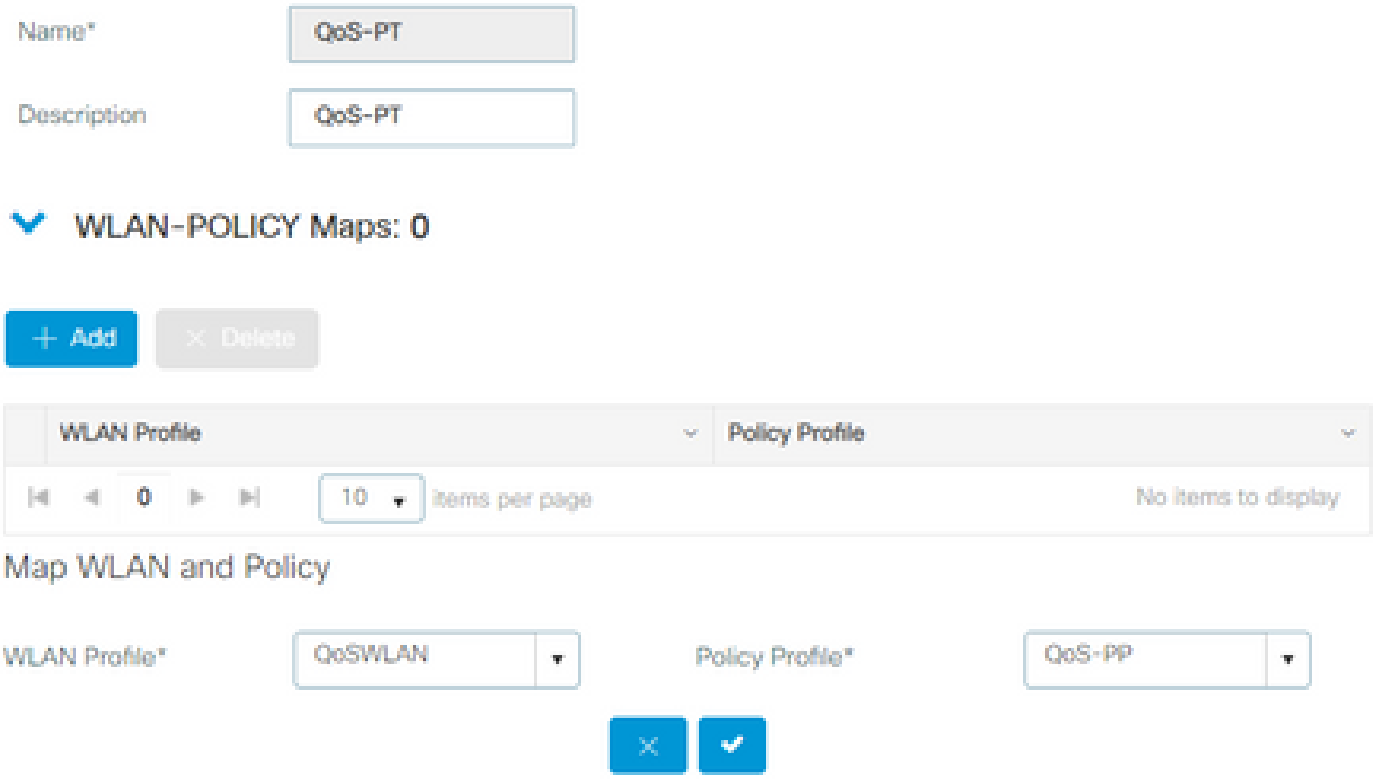


第四步：导航到访问策略，然后配置当客户端连接到SSID时无线客户端所分配的VLAN：

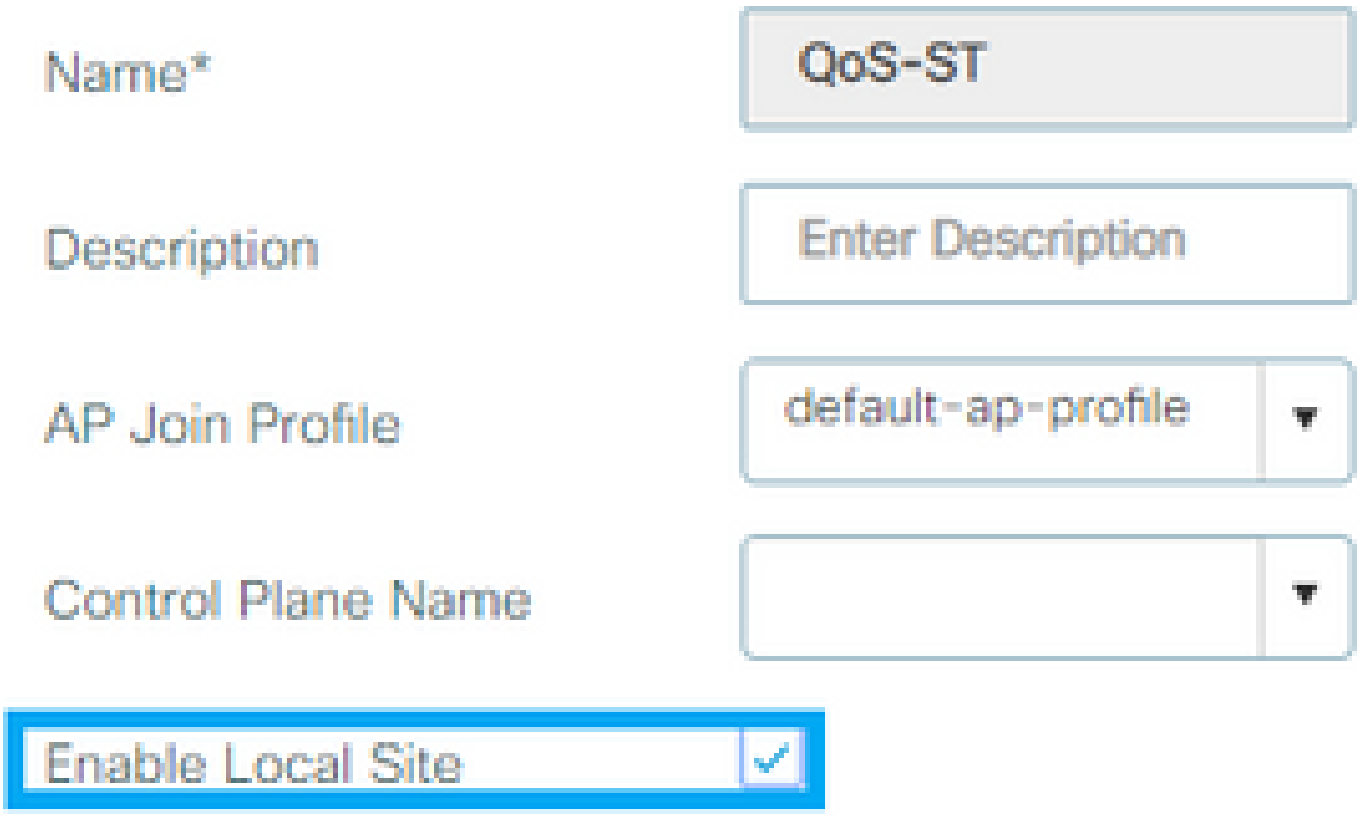


第五步：选择Policy Tag 并选择+Add。配置策略标记名称。

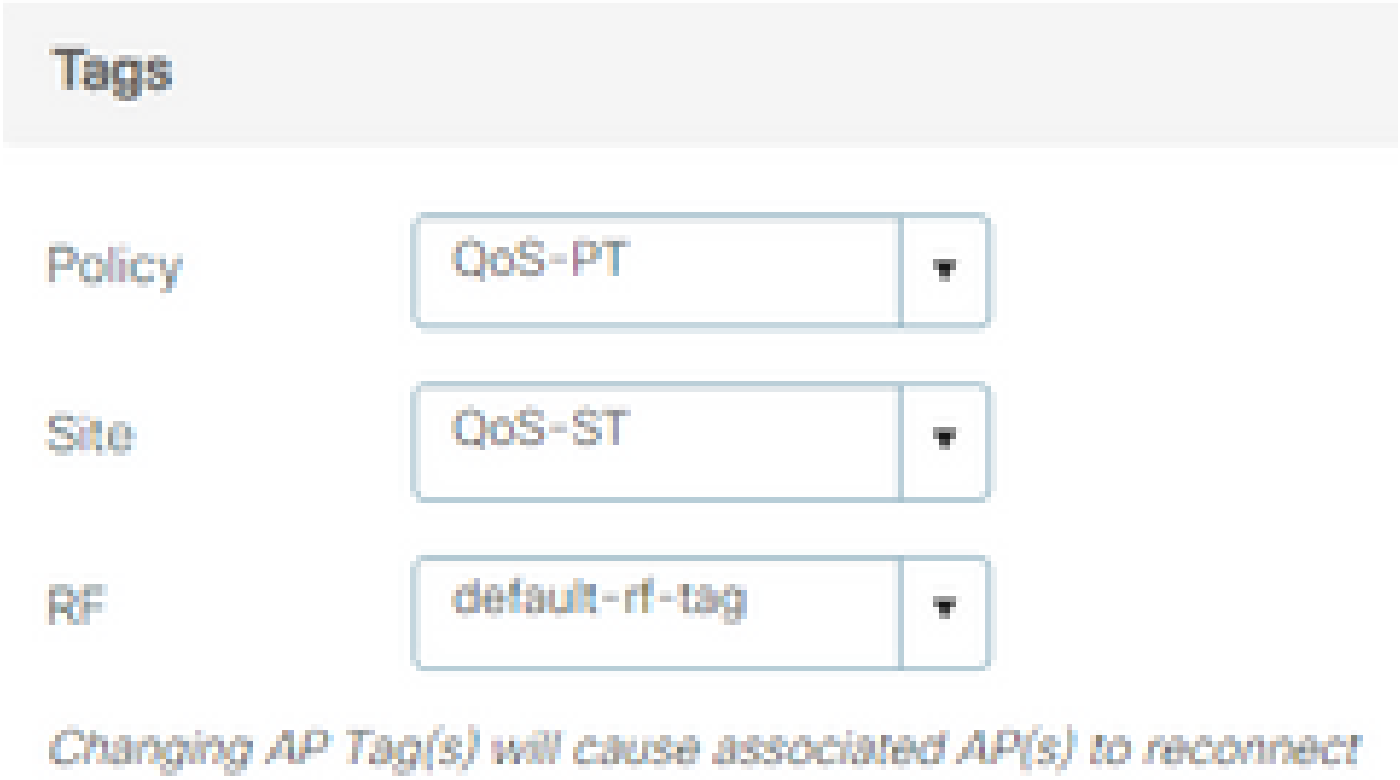
在WLAN-Policy Maps下，在+Add上，从下拉菜单中选择WLAN Profile和Policy Profile，然后选中要配置的映射的复选框。



第六步：选择Site Tag并选择+Add。选中Enable Local Site框，使AP在本地模式下运行（或者对FlexConnect取消选中）：



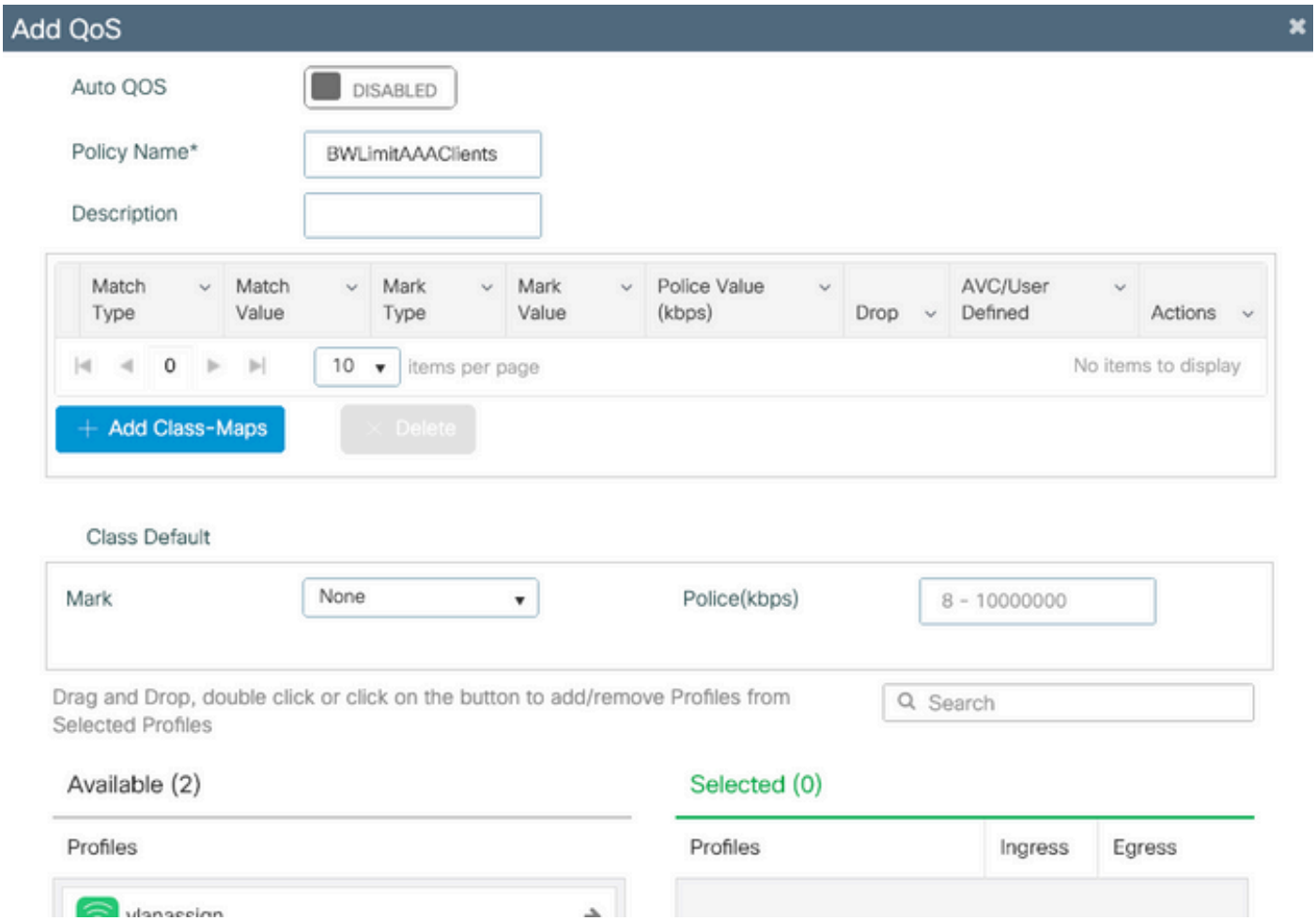
步骤 7.选择Tag APs，选择AP并添加策略、站点和RF标记：



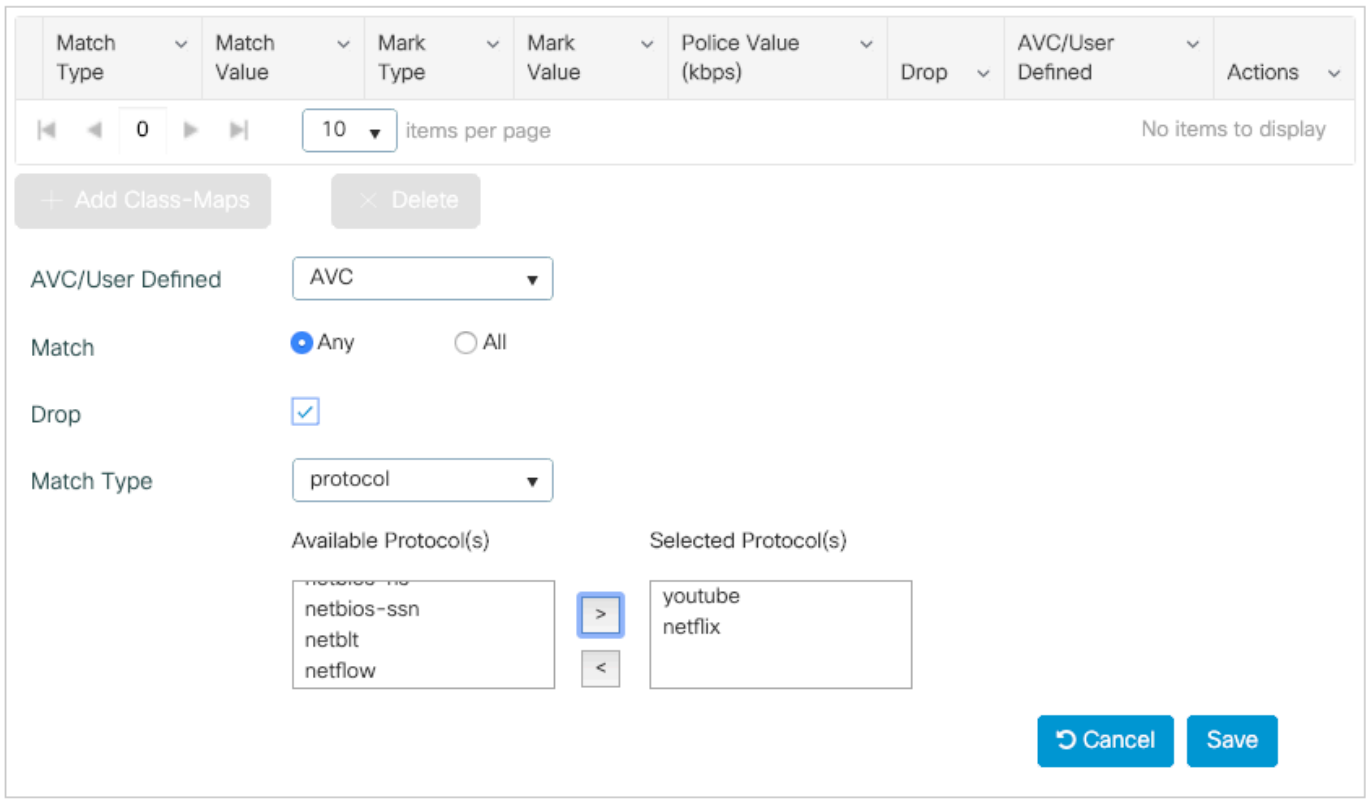
QoS

步骤1:导航到配置>服务> QoS，然后选择+添加创建QoS策略。

将其命名（在本示例中：BWLimitAAAClients）。



第二步：添加一个类映射以删除Youtube和Netflix。单击Add Class-Maps。选择AVC、match any、drop操作并选择两个协议。

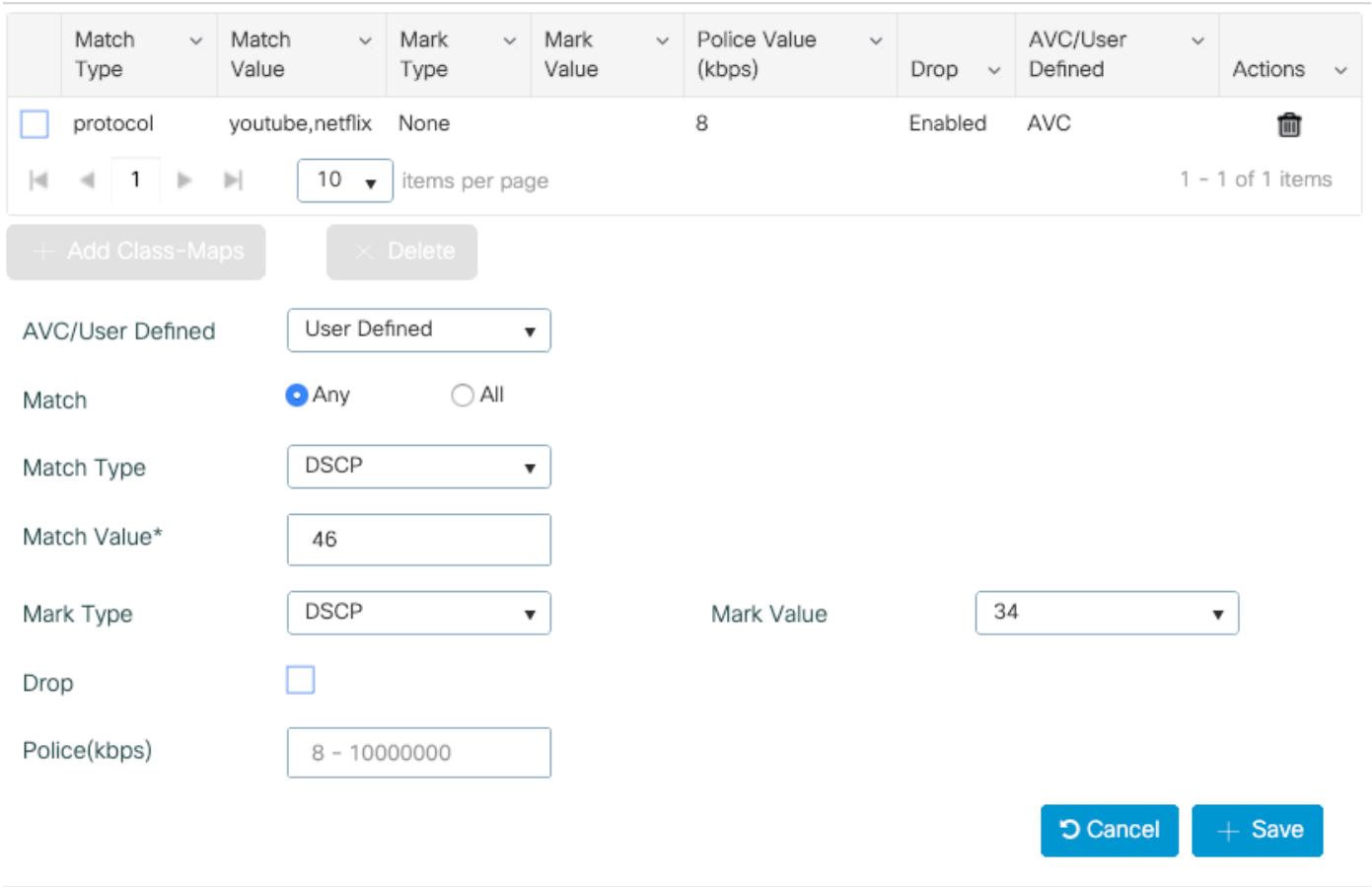


单击Save。

第三步：添加一个将DSCP 46注释为34的类映射。

单击Add Class-Maps。

- Match any，User Defined
- 匹配类型DSCP
- 匹配值46
- 标记类型DSCP
- 标记值34



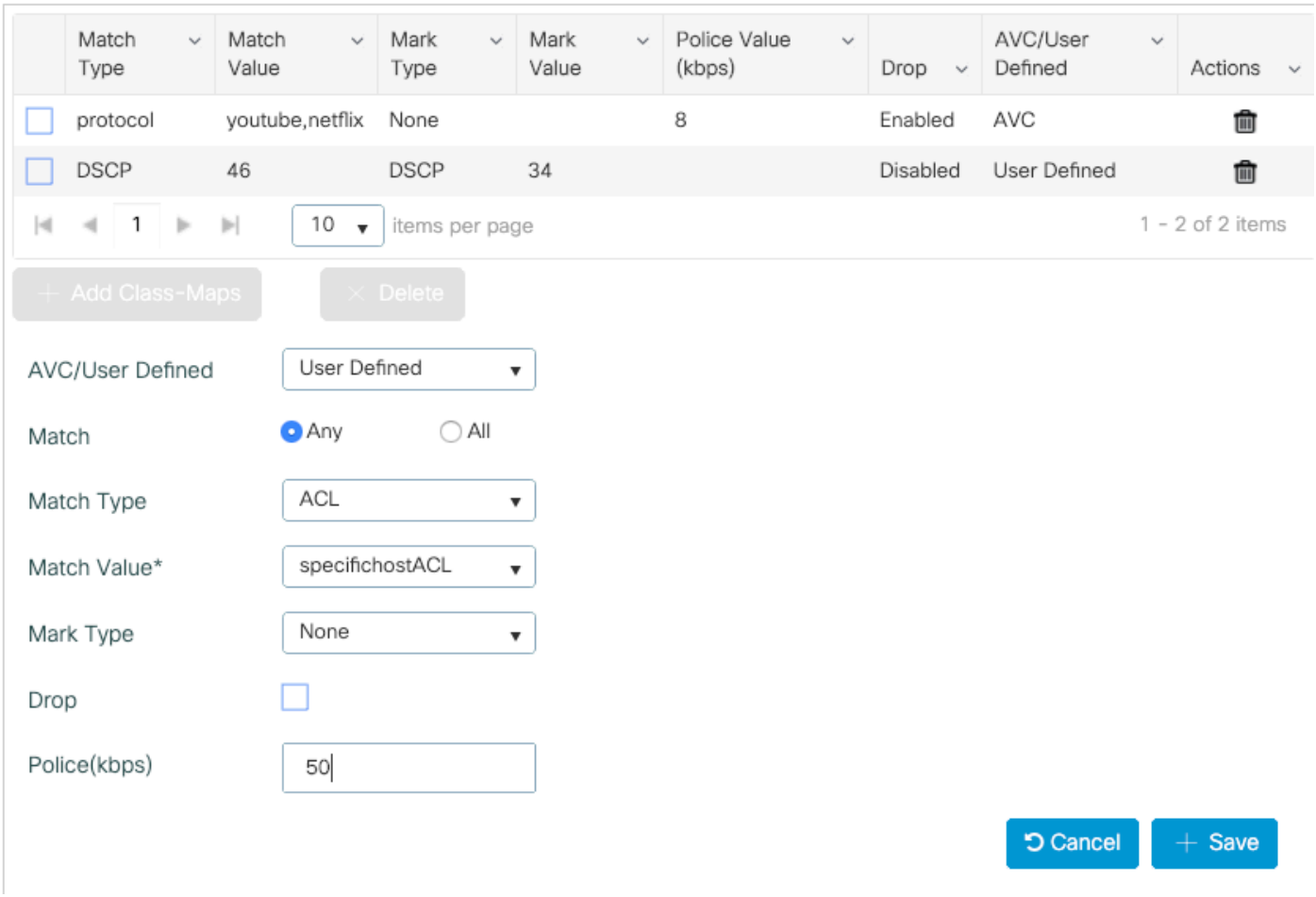
单击Save。

第四步：要定义一个类映射来规定流向特定主机的流量，请为其创建一个ACL。

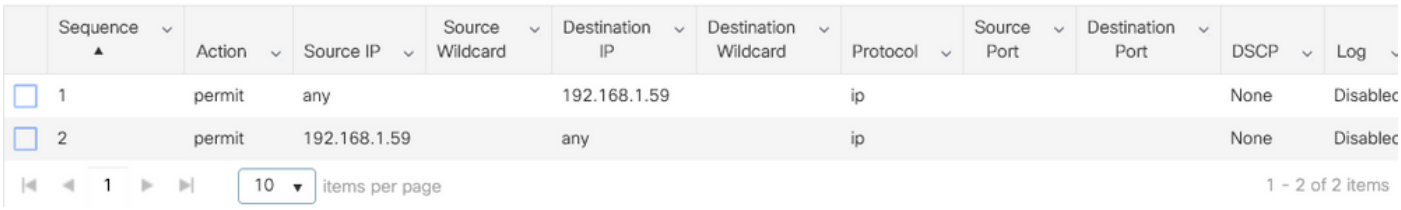
单击Add Class-Maps，

选择User Defined、match any、match type ACL，选择您的ACL名称(此处specifichostACL)，标记type none并选择速率限制值。

Click Save.

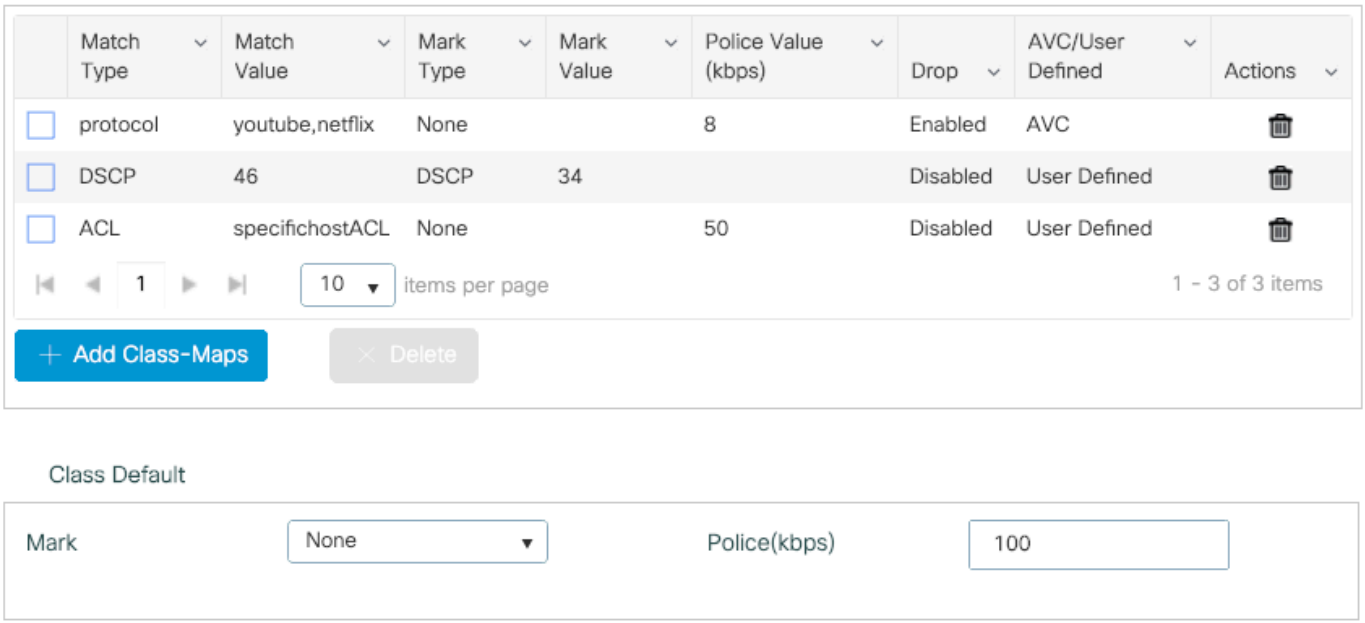


以下是我们用于识别特定主机流量的ACL示例：



第五步：在class maps帧下，使用默认类设置所有其他流量的速率限制。

这会设置上面规则之一未针对的所有客户端流量的速率限制。



第六步：单击底部的Apply to Device。

CLI等效配置：

```
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
```

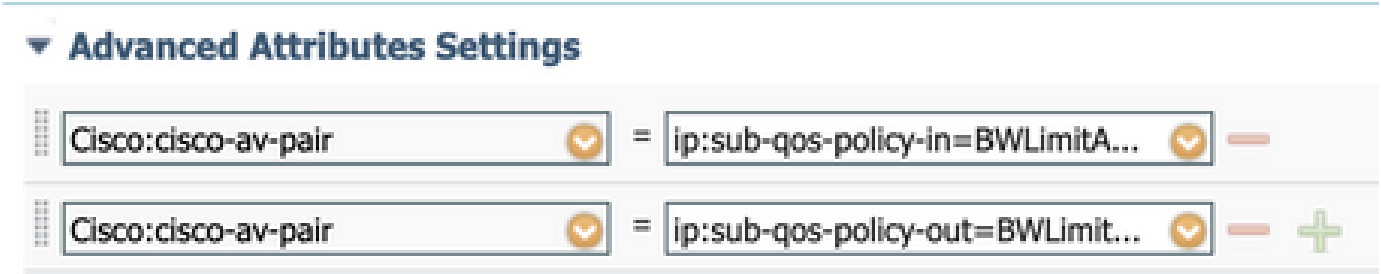
注意：在本示例中，由于配置文件由AAA覆盖应用，因此未在QoS策略下选择。但是，为了将QoS策略手动应用到策略配置文件，请务必选择所需的配置文件。

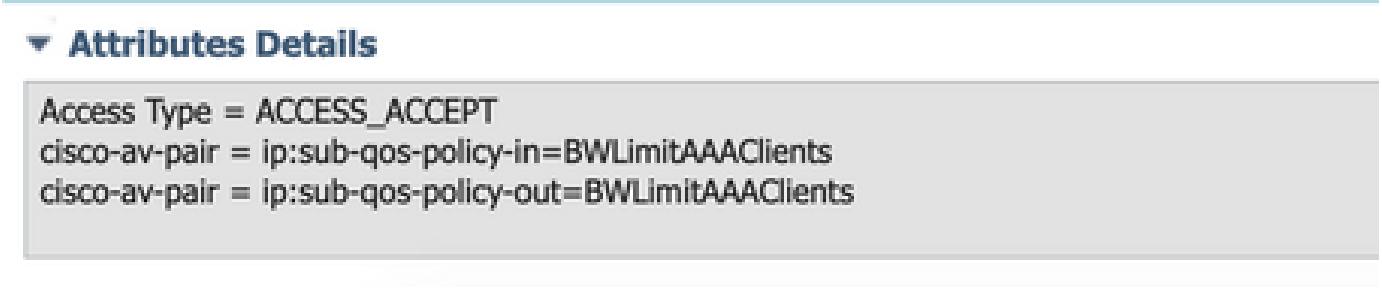
第二步：在ISE上，导航到策略>策略元素>结果>授权配置文件，选择+添加以创建授权配置文件。

要应用QoS策略，请通过Cisco AV对将其添加为高级属性设置。

假设ISE身份验证和授权策略配置为与正确的规则匹配并获得此授权结果。

属性包括ip：sub-qos-policy-in=<policy name>和ip：sub-qos-policy-out=<policyname>





注意：策略名称区分大小写。确保案例正确！

验证

使用本部分可确认您的配置是否工作正常：

在WLC上

```
# 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>

# 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
```

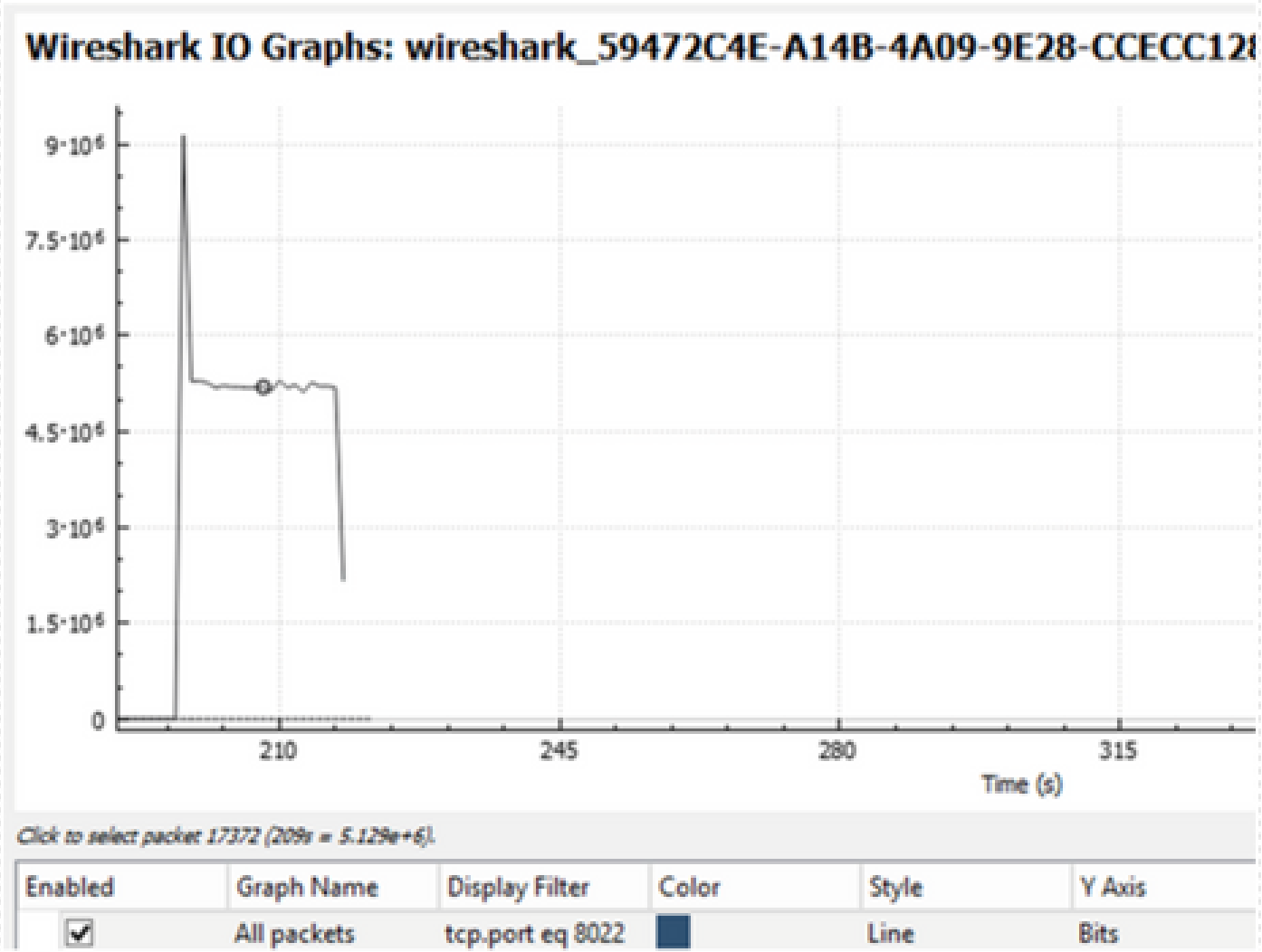
<#root>

```
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上

当AP处于本地模式或SSID处于Flexconnect中心交换模式时，无需对AP进行故障排除，因为QoS和服务策略由WLC完成。

数据包捕获IO图分析



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:清除所有预先存在的调试条件。

```
# clear platform condition all
```

第二步：启用所述无线客户端的调试。

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

第三步：将无线客户端连接到SSID以重现问题。

第四步：重现问题后停止调试。

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

测试期间捕获的日志存储在WLC上的本地文件中，该文件名为：

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

如果使用GUI工作流程生成此跟踪，则保存的文件名为debugTrace_aaaa.bbbb.cccc.txt。

第五步：要收集以前生成的文件，请将ra trace .log复制到外部服务器或直接在屏幕上显示输出。

使用以下命令检查RA跟踪文件的名称：

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

将文件复制到外部服务器：

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.
```

或者，显示内容：

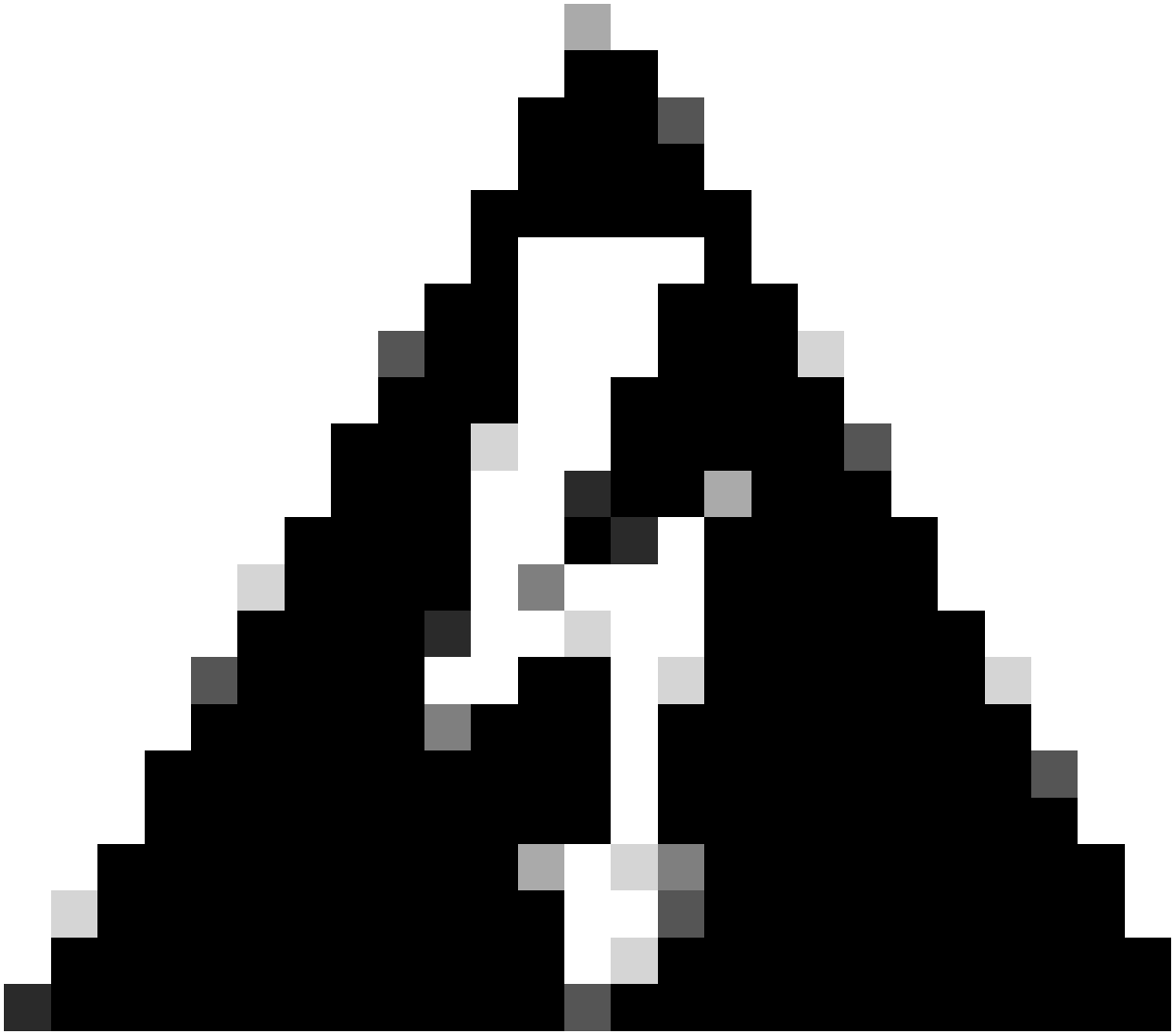
```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

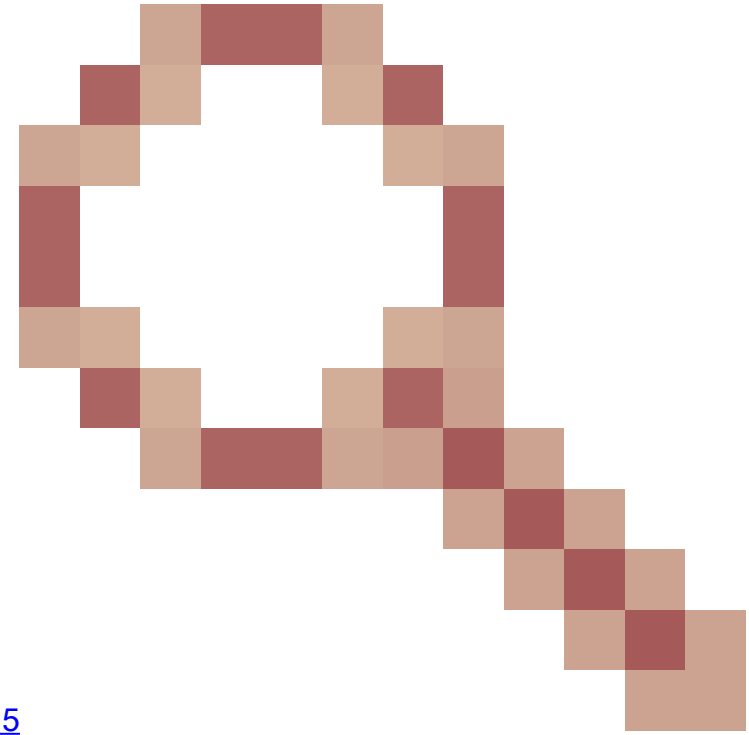
第六步：删除调试条件。

```
# clear platform condition all
```

Flexconnect本地交换（或交换矩阵/SDA）方案

对于flexconnect本地交换（或交换矩阵/SDA），AP将应用您在WLC上定义的所有QoS策略。





警告：由于Cisco Bug ID CSCwh74415

，RADIUS服务器返回的最新QoS策略将应用于连接到同一接入点的所有客户端，从而覆盖所有其他QoS策略。 从17.6.2版本开始，使用AAA覆盖的每客户端速率限制不再正常工作。请参阅漏洞说明，查找修复版本。

在wave2和11ax接入点上，速率限制发生在每流（5元组）级别上，而不是发生在17.6之前的每客户端或每SSID级别上。这适用于Flexconnect/交换矩阵中的无线接入点(EWc-AP)部署中的嵌入式无线控制器。

从17.5开始，可以利用AAA覆盖来推送属性以实现每客户端速率限制。

从17.6开始，802.11ac Wave 2和11ax AP在Flex本地交换配置中支持每客户端双向速率限制。

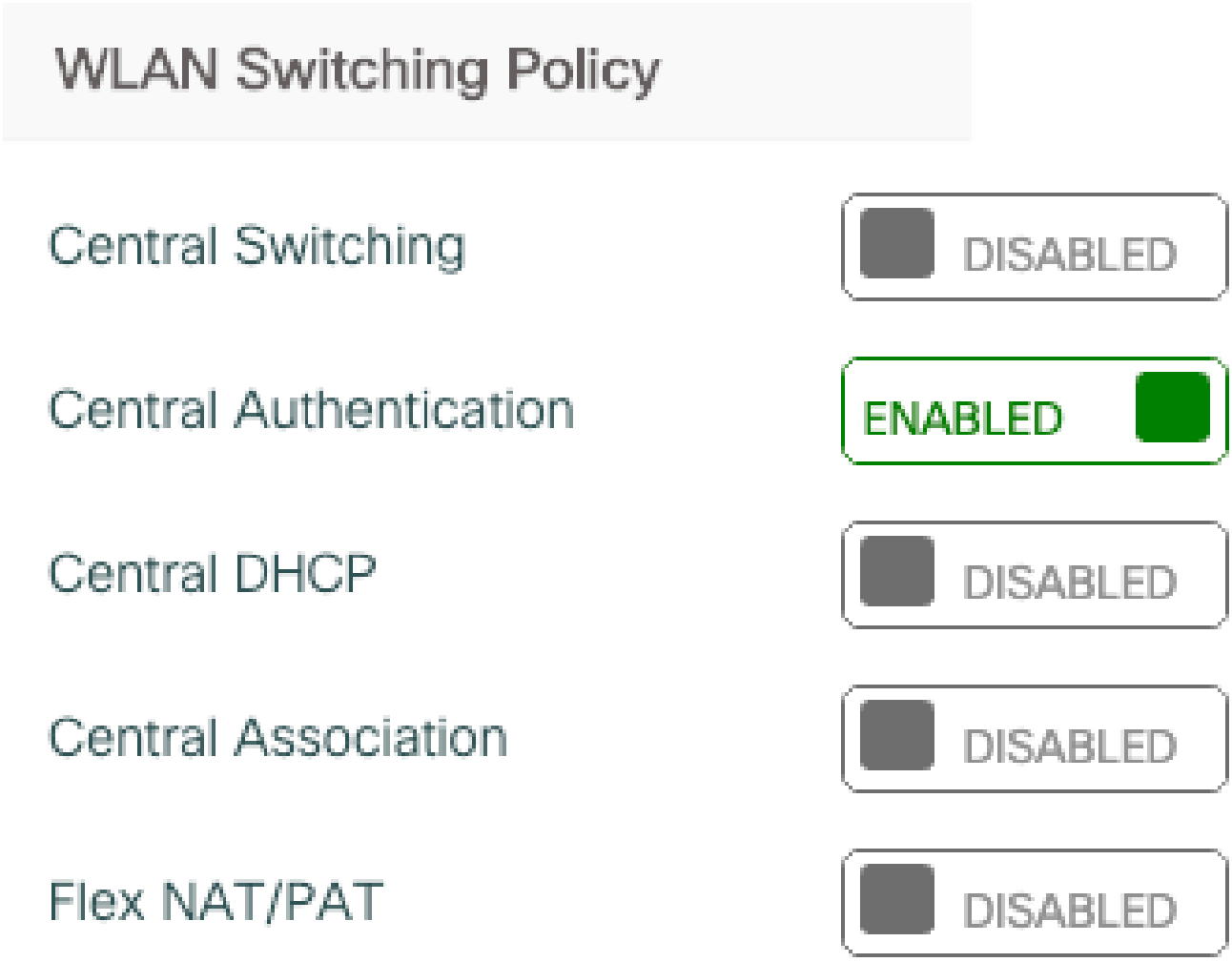
注意：Flex AP不支持QoS策略中存在ACL。它们也不支持BRR（剩余带宽）和策略优先级，后者可通过CLI进行配置但在9800 Web UI中不可用，在9800上不受支持。思科漏洞ID CSCvx81067跟踪QoS策略对Flex AP的支持。

配置

配置与本文第一部分完全相同，但有两个例外：

1. 策略配置文件设置为本地交换。Flex部署要求禁用中央关联，直到班加罗尔17.4版本。

自17.5开始，此字段已硬编码，不可用于用户配置。



2. 站点标签设置为非本地站点

Flexconnect/交换矩阵故障排除

因为AP是应用QoS策略的设备，所以这些命令有助于缩小应用的范围。

show dot11 qos

show policy-map

show rate-limit client

show rate-limit bssid

show rate-limit wlan

show flexconnect client

<#root>

```
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_burs
A8:DB:03:6F:7A:46   2           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
A8:DB:03:6F:7A:46     1   2   1   FWD AES_CCM128     none    none         none Local Central     Local


AP780C-F085-49E6#
```

参考

[Catalyst 9000 16.12 QoS指南]

[9800 QoS配置指南]

[Catalyst 9800配置型号]

[Cisco IOS® XE 17.6发行版本注释]

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）。