Configuración del Límite de Velocidad de QoS (BDRL) en los Controladores Inalámbricos Catalyst 9800 con Anulación AAA

Contenido

Introducción

Este documento describe un ejemplo de configuración para Límite de velocidad bidireccional (BDRL) en los controladores inalámbricos Catalyst serie 9800.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Modelo de configuración de Catalyst Wireless 9800
- AAA con Cisco Identity Service Engine (ISE)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Controlador inalámbrico Cisco Catalyst 9800-CL en la versión 16.12.1s
- Identity Service Engine en la versión 2.2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de

laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

QoS en la plataforma 9800 WLC utiliza los mismos conceptos y componentes que las plataformas Catalyst 9000.

En esta sección se proporciona una descripción general del funcionamiento de estos componentes y de cómo se pueden configurar para obtener diferentes resultados.

Básicamente, la recursividad de QoS funciona de la siguiente manera:

1. Mapa de clase: Identifica cierto tipo de tráfico. Los mapas de clase pueden aprovechar el motor de visibilidad y control de aplicaciones (AVC).

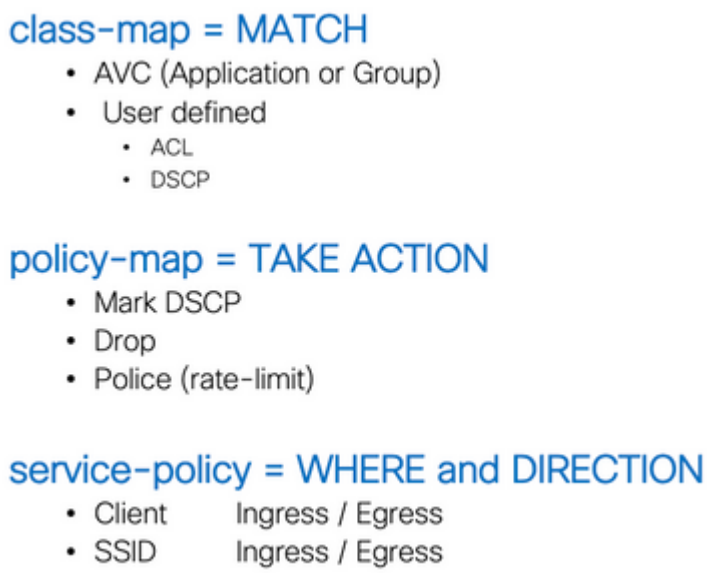
Además, el usuario puede definir mapas de clase personalizados para identificar el tráfico que coincida con una lista de control de acceso (ACL) o un punto de código de servicios diferenciados (DSCP)

2. Policy-Map: son políticas que se aplican a los Class-maps.
Estas políticas pueden marcar DSCP, descartar o limitar la velocidad del tráfico que coincide con el mapa de clase

4. Service-Policy: los Policy-maps se pueden aplicar en el Policy Profile de un SSID o Per-Client en una dirección determinada con el comando service-policy.

3. (Opcional) Table-Map: Se utilizan para convertir un tipo de marca a otro, por ejemplo, CoS a DCSP.

Nota: En el mapa de tabla, especifique los valores que desea cambiar (de 4 a 32); en el mapa de política, se especifica la tecnología (COS a DSCP).



Nota: En caso de que se apliquen dos o más políticas por destino, la resolución de políticas se elige en función de esta clasificación de prioridades:

· Anulación de AAA (más alta)
· Creación de perfiles nativos (políticas locales)
· Política configurada
· Política predeterminada (más baja)

Puede encontrar más detalles en la guía de configuración oficial de QoS para 9800

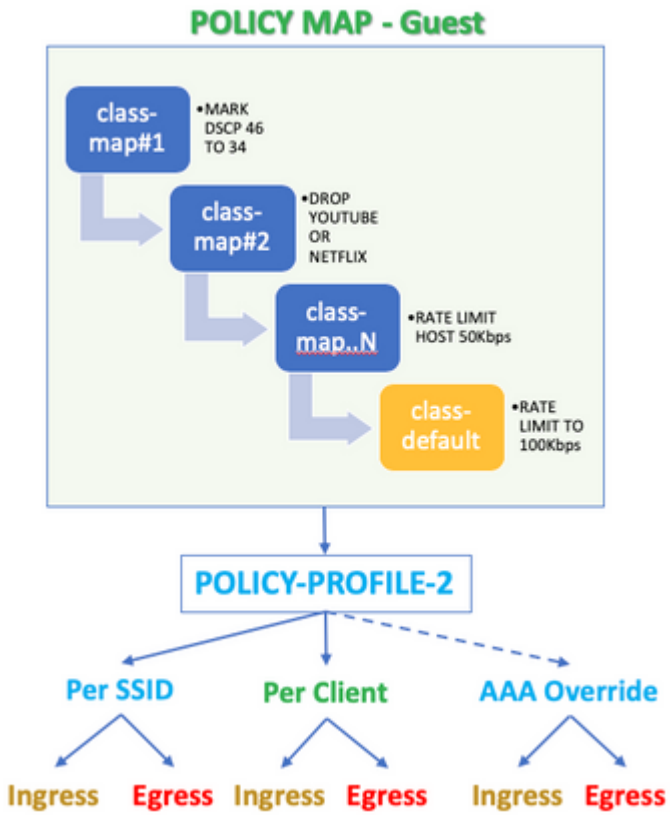
Puede encontrar información adicional sobre la teoría de QoS en la guía de configuración de QoS de la serie 9000

Ejemplo: políticas de QoS de invitado y de empresa

En este ejemplo se muestra cómo se aplican los componentes de QoS explicados en un escenario real.

La intención es configurar una política de QoS para invitado que:

- Observaciones DSCP
- Vídeo de YouTube y Netflix descartado
- Velocidad Limita un host especificado en una ACL a 50 Kbps
- Velocidad Limita el resto del tráfico a 100 Kbps



Por ejemplo, la política de QoS se debe aplicar por SSID en ambas direcciones: Ingreso y Salida al perfil de política que enlaza con la WLAN de invitado.

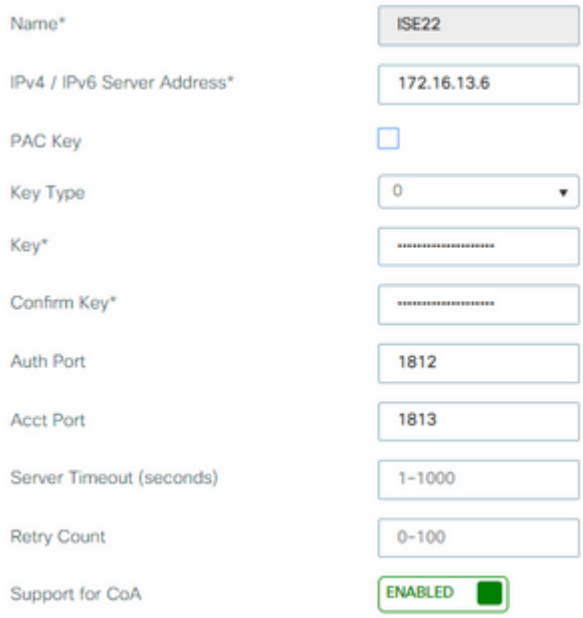
Configurar

Servidor AAA y lista de métodos

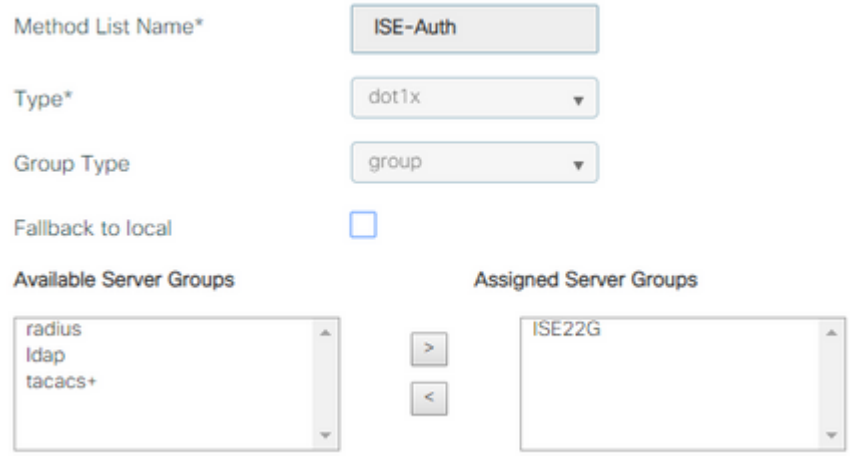
Paso 1. Navegue hasta **Configuration > Security > AAA > Authentication > Servers/Groups** y seleccione

+Add.

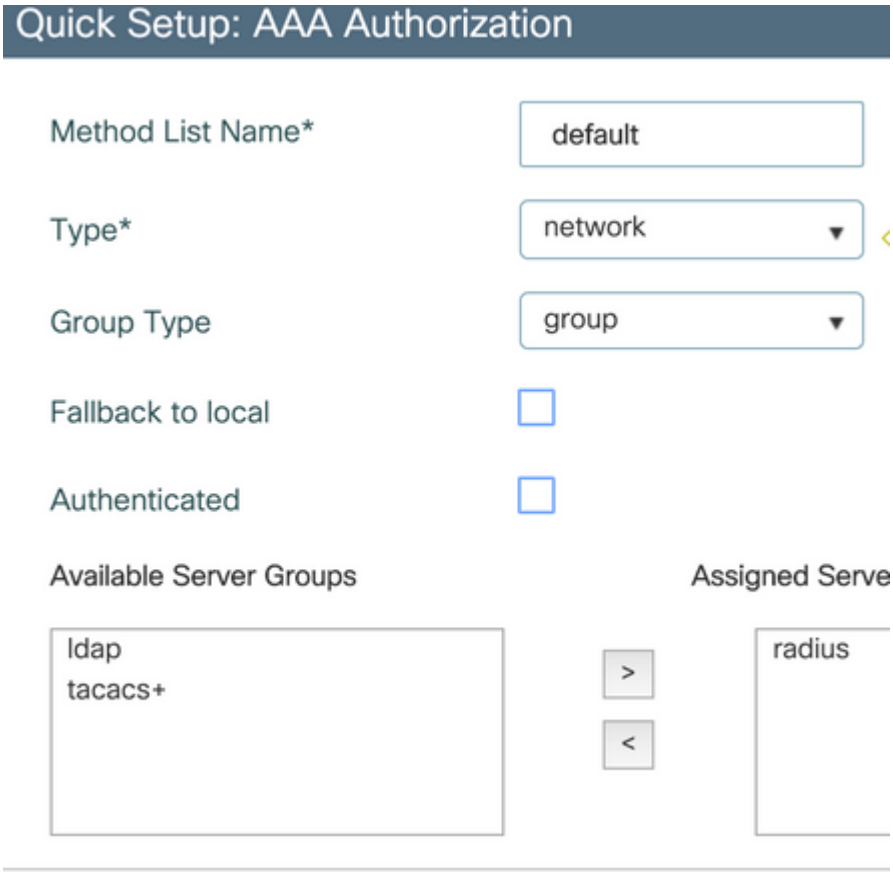
Introduzca el nombre del servidor AAA, la dirección IP y la clave, que deben coincidir con el secreto compartido en **Administration > Network Resources > Network Devices** en ISE.



Paso 2. Vaya a **Configuration > Security > AAA > Authentication > AAA Method List** y seleccione **+Add.** Seleccione los grupos de servidores asignados de Grupos de servidores disponibles.



Paso 3. Vaya a **Configuration > Security > AAA > Authorization > AAA method List** y seleccione **Add.** Elija el método predeterminado y "network" como tipo.

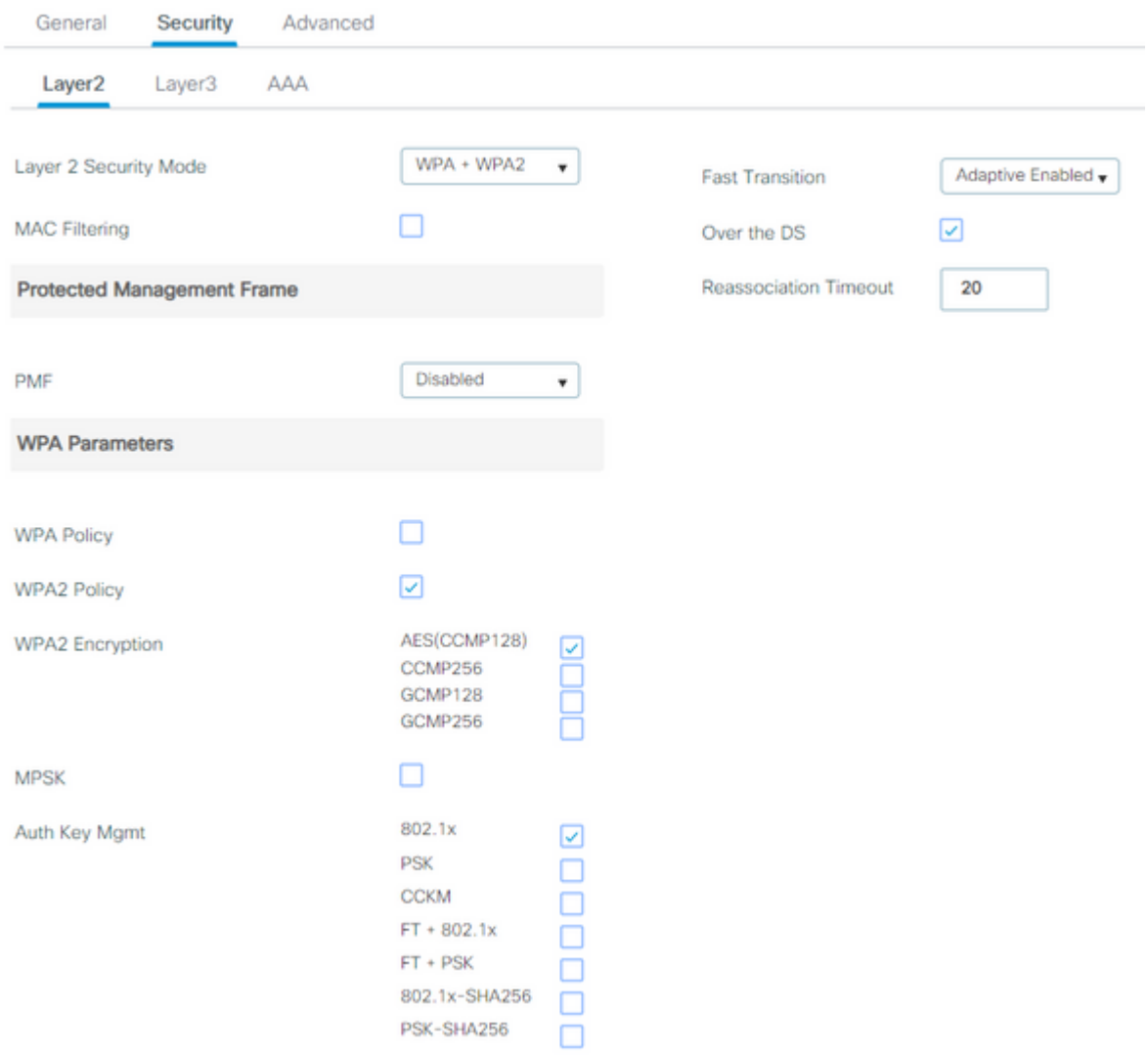


Esto es necesario para que el controlador aplique los atributos de autorización (por ejemplo, la política de QoS aquí) devueltos por el servidor AAA. De lo contrario, la política recibida de RADIUS no se aplica.

Política WLAN, etiqueta del sitio y etiqueta AP

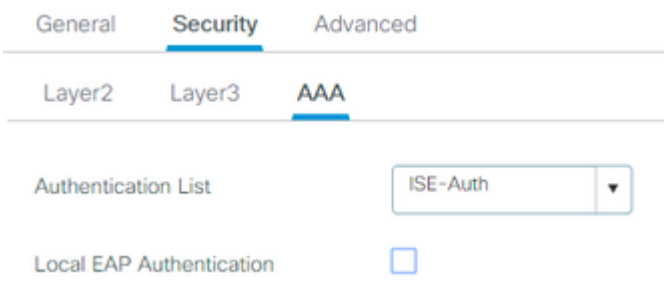
Paso 1. Vaya a **Configuration > Wireless Setup > Advanced > Start Now > WLAN Profile** y seleccione **+Add** para crear una nueva WLAN. Configure el SSID, el nombre de perfil, el ID de WLAN y establezca el estado en activado.

Luego, navegue hasta **Seguridad > Capa 2** y configure los parámetros de autenticación de la Capa 2:



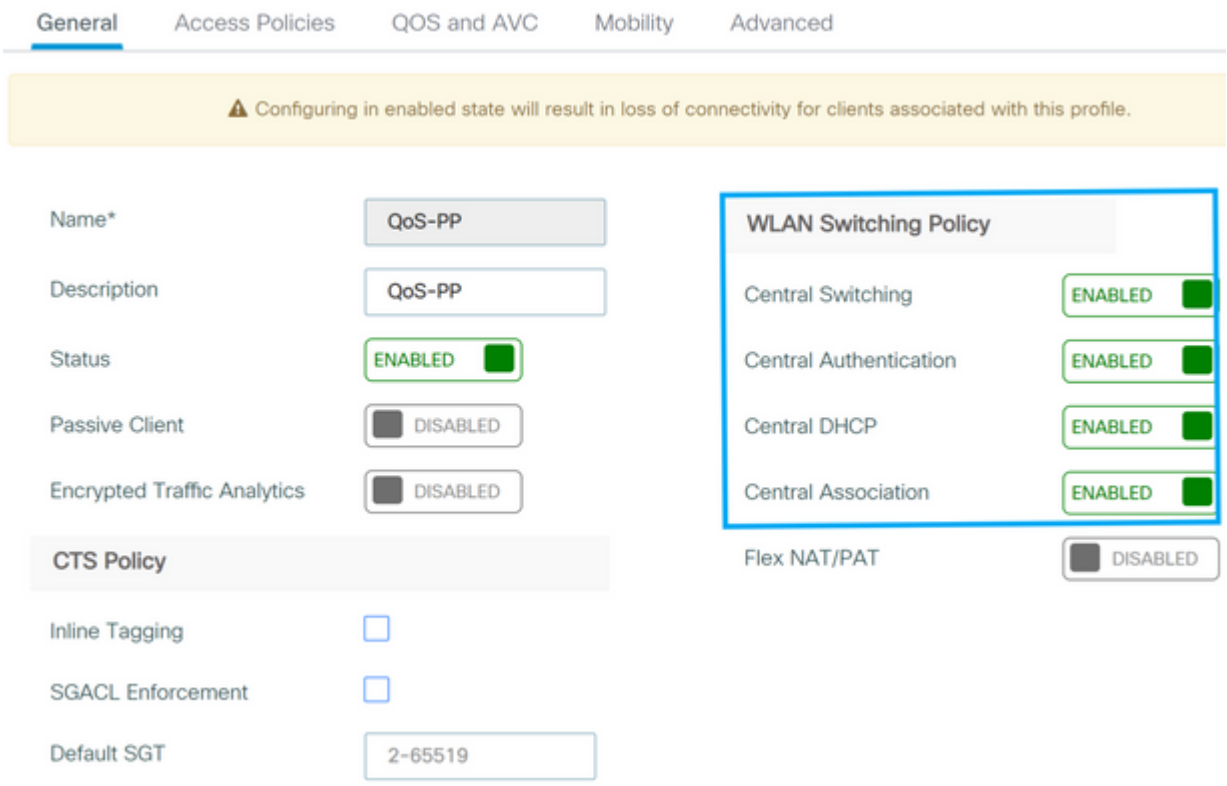
La seguridad SSID no tiene que ser 802.1x como requisito para QoS, pero se utiliza en este ejemplo de configuración para la invalidación de AAA.

Paso 2. Navegue hasta **Security > AAA** y seleccione el servidor AAA en el cuadro desplegable **Authentication List**.

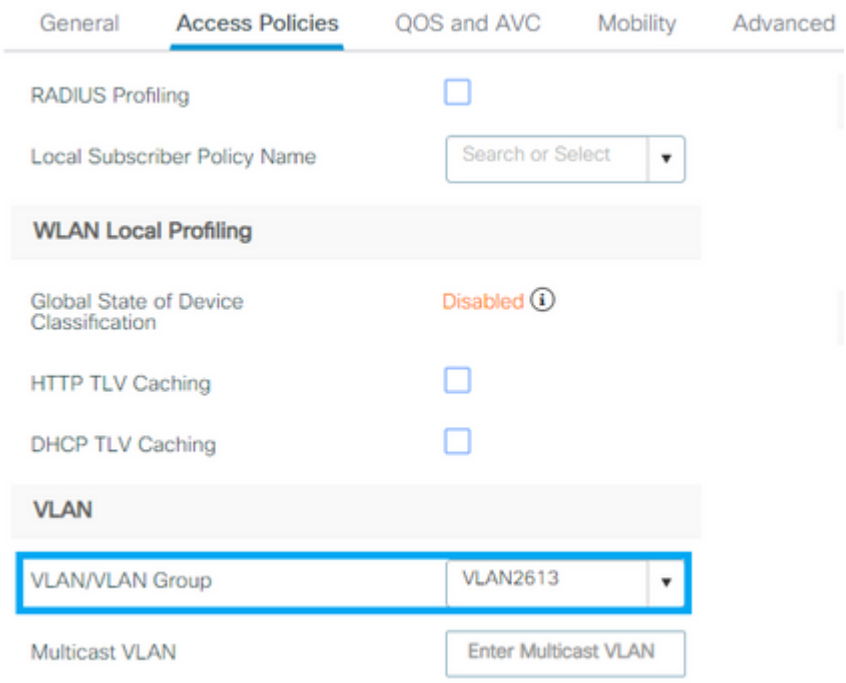


Paso 3. Seleccione **Perfil de política** y seleccione **+Agregar.** Configure el nombre del perfil de política.

Establezca el estado como Activado; también active Conmutación central, Autenticación, DHCP y asociación:

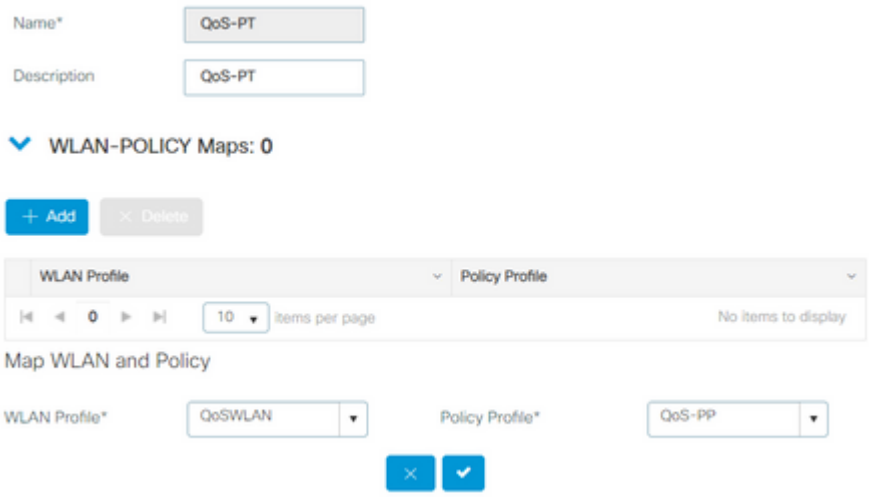


Paso 4. Navegue hasta **Access Policies** y configure la VLAN a la que está asignado el cliente inalámbrico cuando el cliente se conecta al SSID**:**

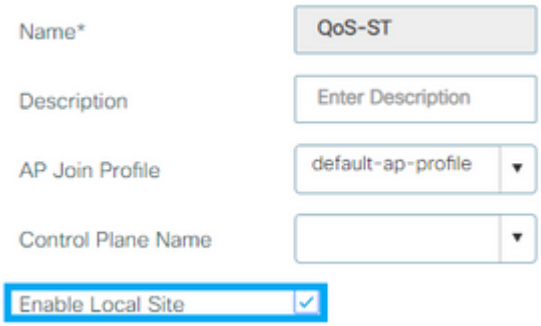


Paso 5. Seleccione **Etiqueta de directiva** y seleccione **+Agregar.** Configure el nombre de la etiqueta de directiva.

En **WLAN-Policy Maps,** en **+Add,** seleccione el **perfil WLAN** y el **perfil de política** en los menús desplegables, seleccione la verificación para que se configure el mapa.



Paso 6. Seleccione **Etiqueta del sitio** y seleccione **+Agregar.** Marque la casilla **Enable Local Site** para que los AP funcionen en el modo local (o déjelo sin marcar para FlexConnect):

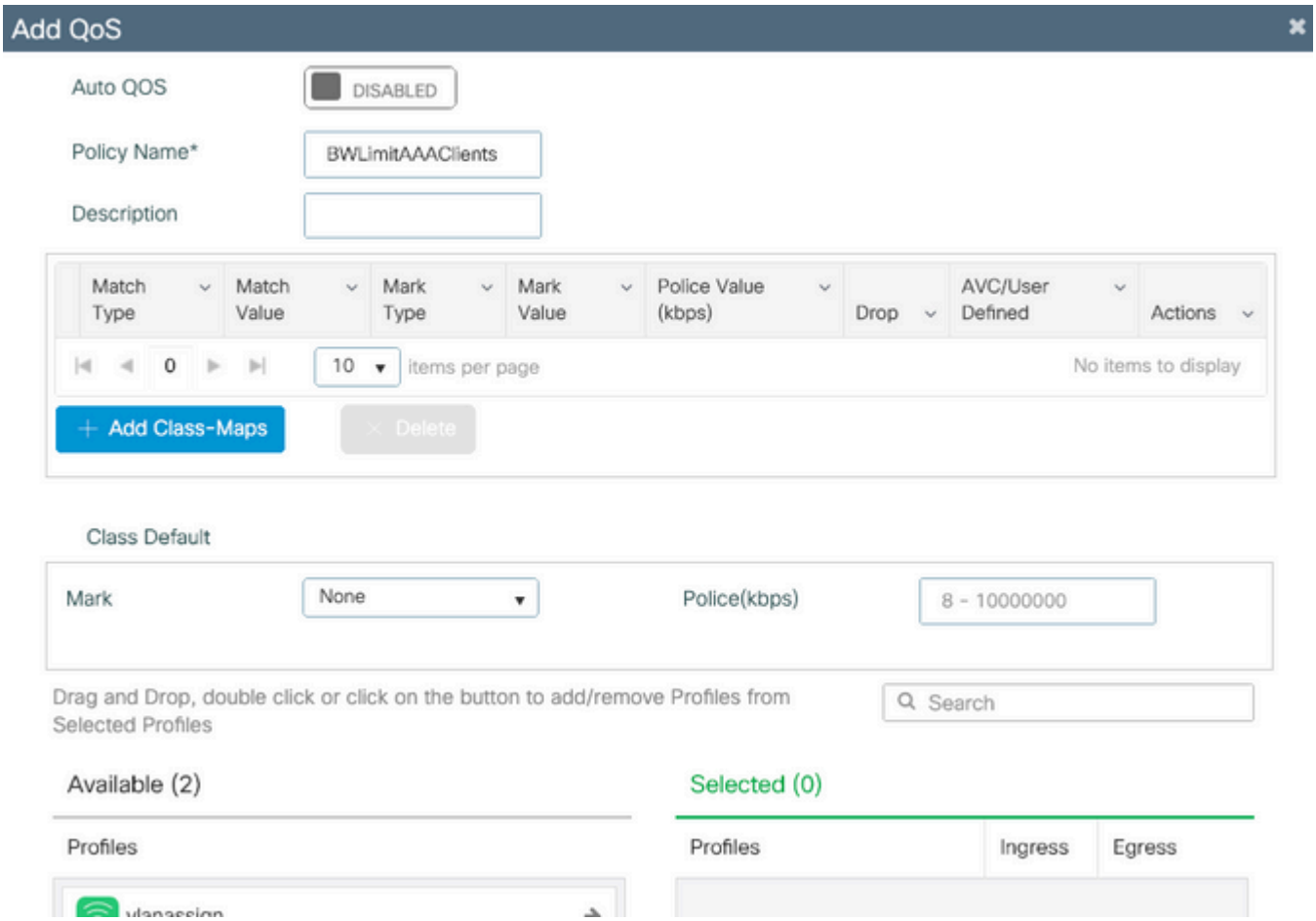


Paso 7. Seleccione **Tag APs**, elija los APs y agregue la etiqueta Policy, Site y RF:

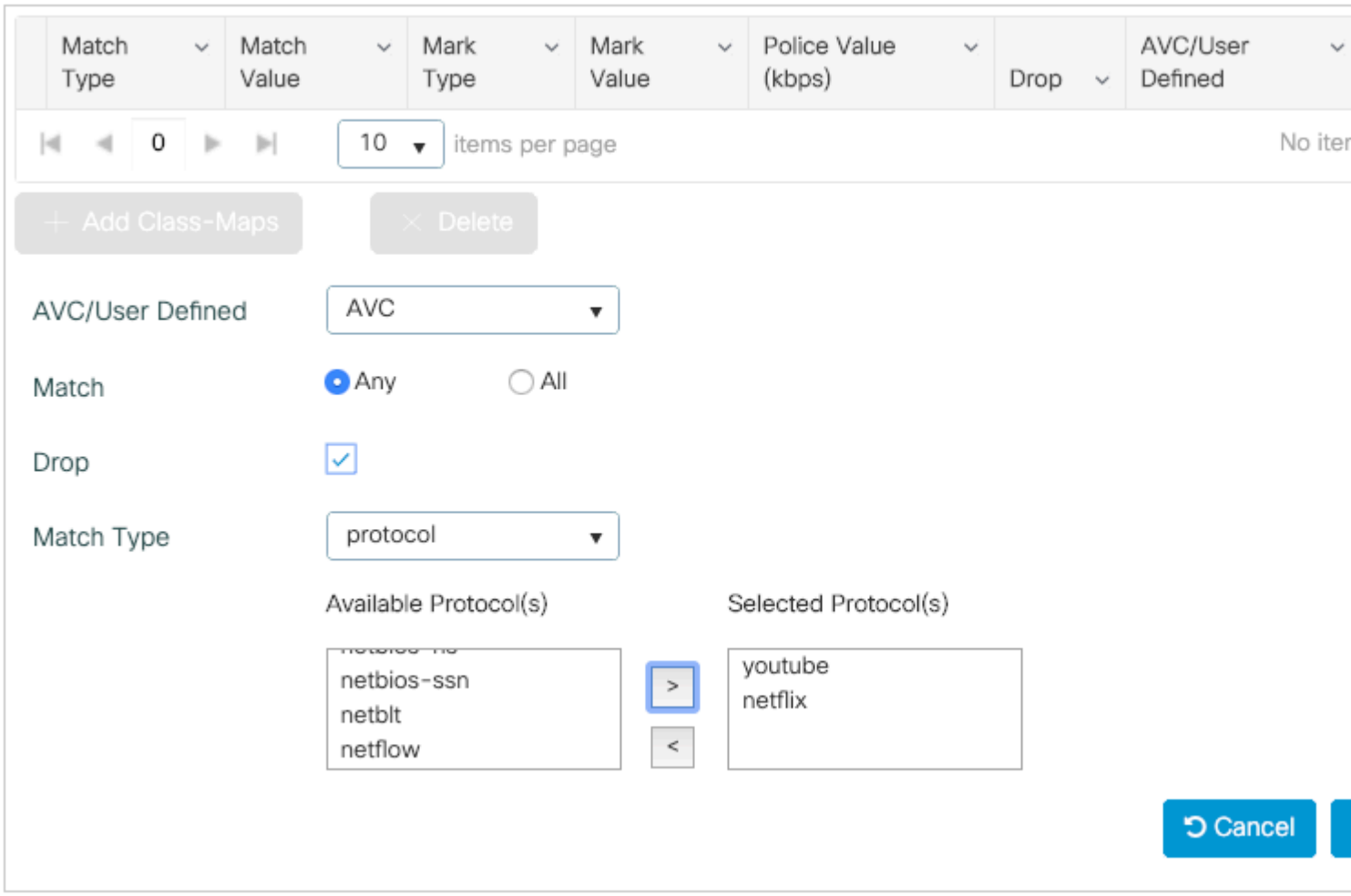
QoS

Paso 1. Navegue hasta **Configuration > Services > QoS** y seleccione **+Add** para crear una política de QoS.

Asígnele un nombre (para este ejemplo: BWLimitAAAClients).



Paso 2. Agregue un mapa de clase para descartar Youtube y Netflix. Haga clic en **Add Class-Maps**. Seleccione **AVC**, match **any**, **drop** action y elija ambos protocolos.



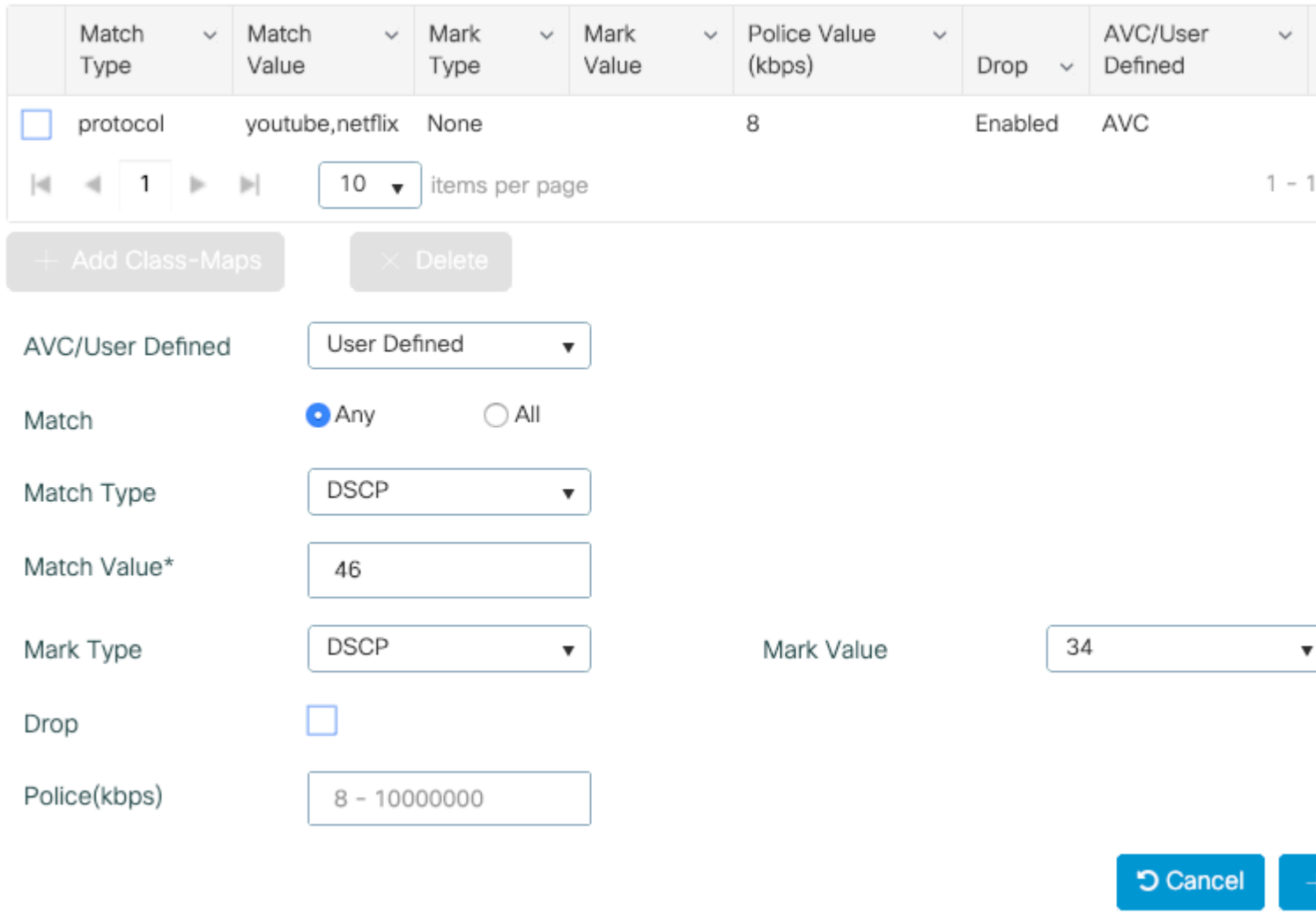
Pulse **Guardar.**

Paso 3. Agregue un mapa de clase que señale DSCP 46 a 34.

Haga clic en **Add Class-Maps**.

- Coincidir con **cualquiera, definido por el usuario**
- Tipo de coincidencia **DSCP**
- Coincidir valor **46**
- Tipo de marca **DSCP**
- Valor de la marca **34**

.



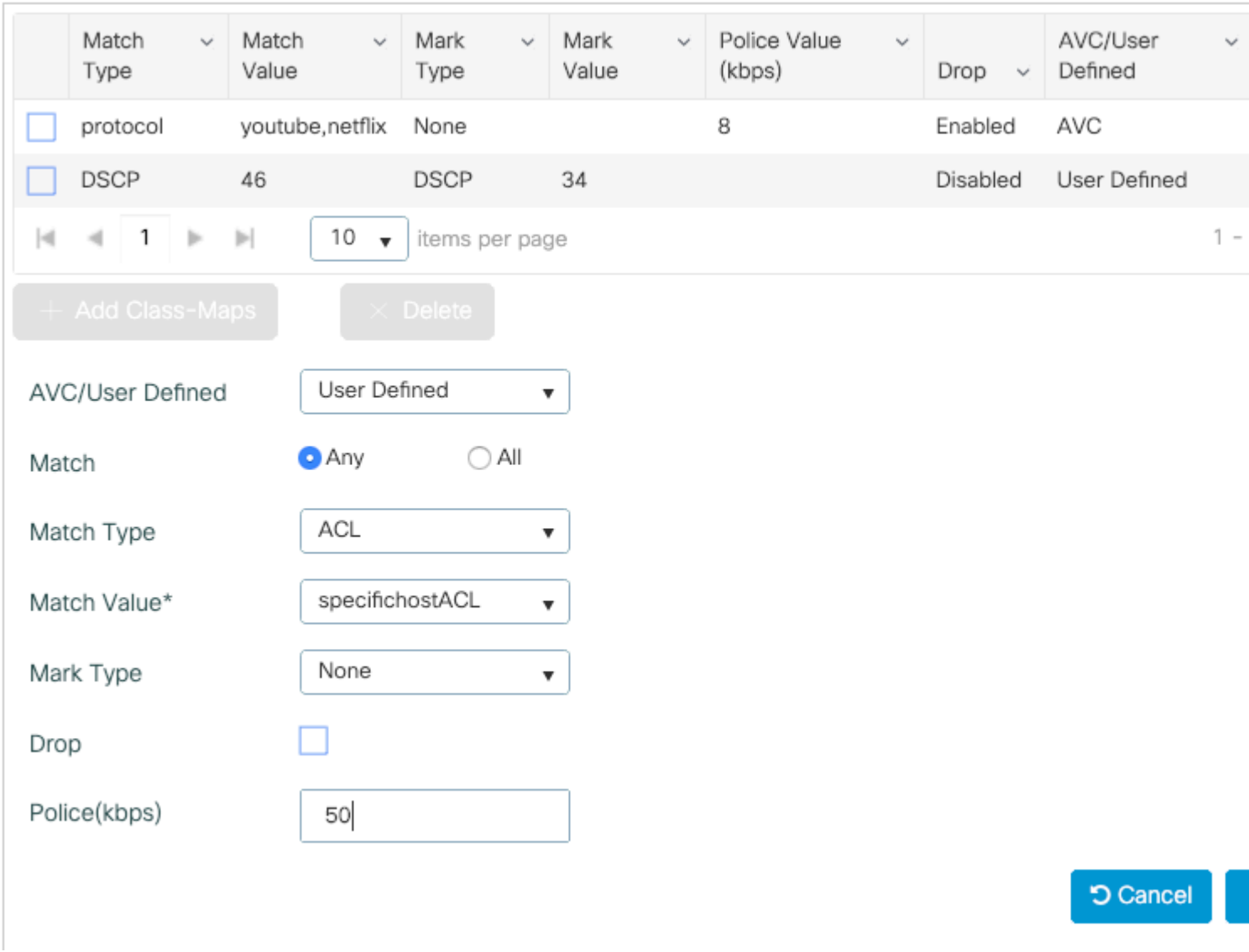
Pulse **Guardar.**

Paso 4. Para definir un mapa de clase que regule el tráfico a un host específico, cree una ACL para él.

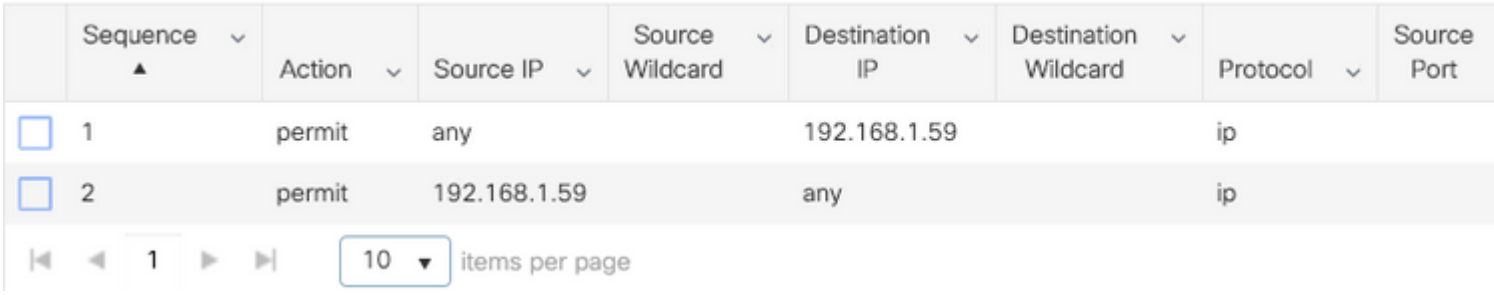
Haga clic en **Add Class-Maps**,

Elija User Defined, match **any,** match type **ACL**, elija su nombre de ACL (aquí **specific hostACL**), marque el tipo none y elija el valor de límite de velocidad.

Click Save.

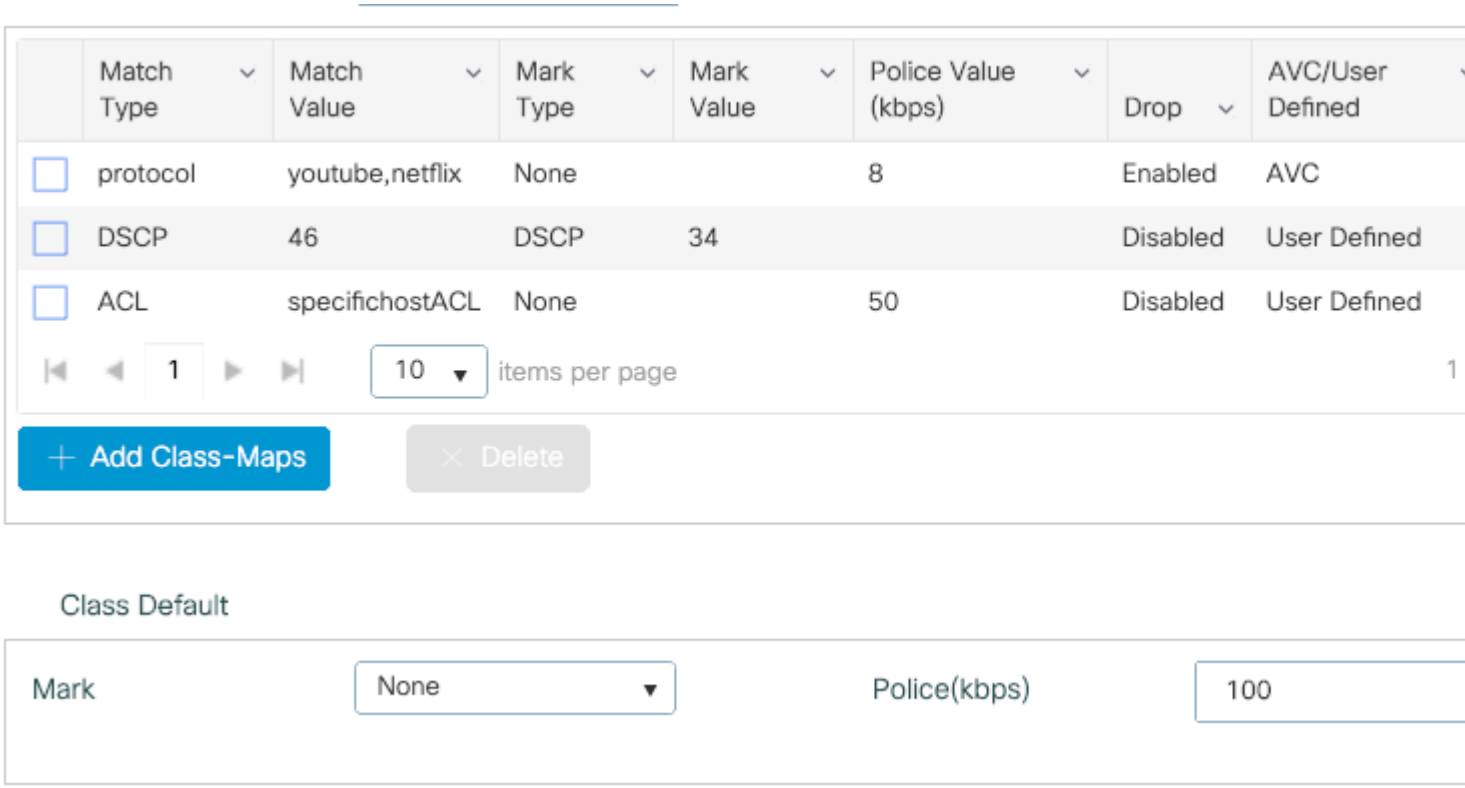


Aquí hay un ejemplo de ACL que utilizamos para identificar un tráfico de host específico :



Paso 5. En la trama de mapas de clase, utilice la clase predeterminada para establecer el límite de velocidad para el resto del tráfico.

Esto establece un límite de velocidad en todo el tráfico del cliente que no es el objetivo de una de las reglas anteriores.



Paso 6. Haga clic en **Apply to Device** en la parte inferior.

Configuración equivalente de CLI:

```
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
```

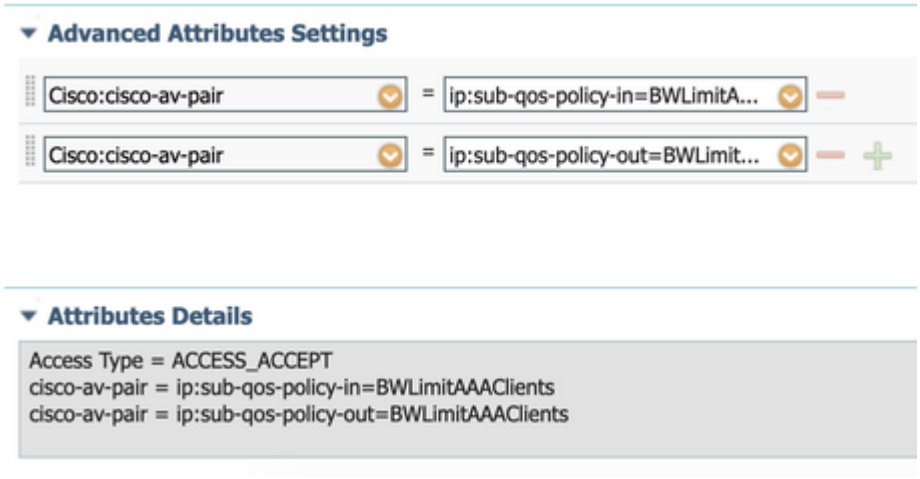
> **Nota**: En este ejemplo, no se seleccionó **Profiles** en la política de QoS, ya que es aplicada por la sustitución de AAA. Sin embargo, para aplicar la política de QoS a un perfil de política manualmente, seleccione los perfiles deseados.

Paso 2. En ISE, navegue hasta **Política > Elementos de política > Resultados > Perfiles de autorización** y seleccione **+Agregar** para crear un perfil de autorización.

Para aplicar la política de QoS, agréguela como **Advanced Attributes Settings** a través de Cisco AV Pairs.

Se supone que las políticas de autenticación y autorización de ISE están configuradas para coincidir con la regla correcta y obtener este resultado de autorización.

Los atributos son **ip:sub-qos-policy-in=<nombre de política>** e **ip:sub-qos-policy-out=<nombre de política>**



> **Nota**: Los nombres de las políticas distinguen entre mayúsculas y minúsculas. Asegúrese de que el caso es correcto.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente:

En el 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>i

# show wireless client mac
```

```
       detail
# show wireless client



       service-policy input
# show wireless client



       service-policy output

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

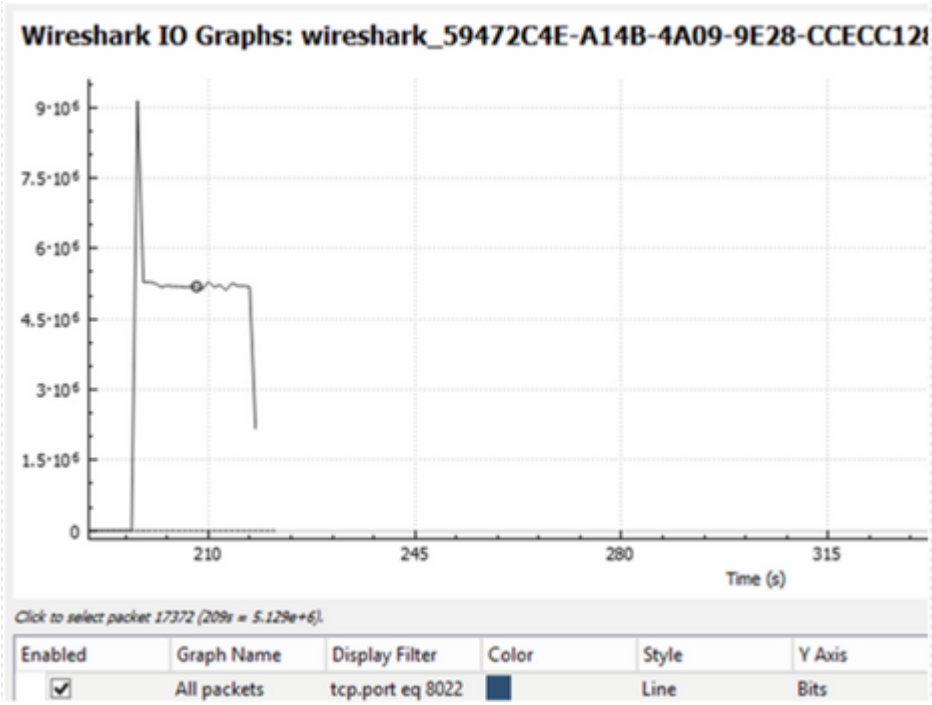
<#root>

```
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
```

En el AP

No se requiere ninguna solución de problemas en el AP cuando el AP está en modo local o el SSID en el modo de conmutación central de Flexconnect como las políticas de QoS y de servicio son hechas por el WLC.

Análisis de gráficos de E/S de capturas de paquetes



Troubleshoot

Esta sección proporciona la información para resolver problemas en su configuración.

Paso 1. Borre todas las condiciones de depuración preexistentes.

```
# clear platform condition all
```

Paso 2. Active la depuración para el cliente inalámbrico en cuestión.

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

Paso 3. Conecte el cliente inalámbrico al SSID para reproducir el problema.

Paso 4. Detenga los debugs una vez que se reproduzca el problema.

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

Los registros capturados durante la prueba se almacenan en el WLC en un archivo local con el nombre:

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Si se utiliza el flujo de trabajo GUI para generar este seguimiento, el nombre de archivo guardado es debugTrace_aaaa.bbbb.cccc.txt.

Paso 5. Para recopilar el archivo generado anteriormente, copie el archivo .log de seguimiento de ra en un servidor externo o muestre el resultado directamente en la pantalla.

Verifique el nombre del archivo de trazas RA con este comando:

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

Copie el archivo en un servidor externo:

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

También puede mostrar el contenido:

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

Paso 6. Elimine las condiciones de depuración.

```
# clear platform condition all
```

Escenario de switching local Flexconnect (o fabric/SDA)

En el caso de la conmutación local flexconnect (o fabric/SDA), es el AP que aplica cualquier política de QoS que haya definido en el WLC.

En los puntos de acceso wave2 y 11ax, el límite de velocidad se produce en un nivel por flujo (5 tuplas) y no por cliente o por SSID antes de 17.6.

Esto se aplica a los puntos de acceso de las implementaciones de Flexconnect/Fabric, controlador inalámbrico integrado en punto de acceso (EWc-AP).

A partir de la versión 17.5, se puede aprovechar la invalidación de AAA para presionar los atributos con el fin de alcanzar el límite de tasa por cliente.

A partir de la versión 17.6, el límite de velocidad bidireccional por cliente se admite en los PA 802.11ac Wave 2 y 11ax en la configuración de switching local Flex.

> **Nota**: los AP Flex no admiten la presencia de ACL en las políticas de QoS. Tampoco son compatibles con BRR (ancho de banda restante) ni con la prioridad de políticas que se pueden configurar a través

---

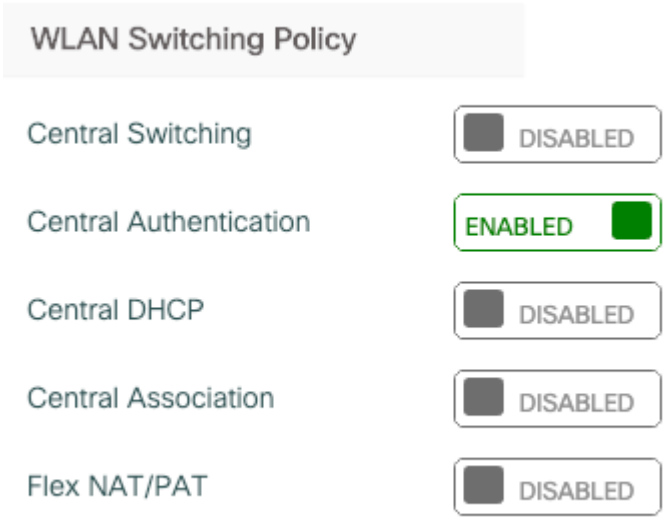
de CLI, pero que no están disponibles en la interfaz de usuario web del 9800 y que no son compatibles con el 9800. El ID de bug de Cisco CSCvx81067 rastrea el soporte de ACL en las políticas de QoS para los AP flexibles.

Configuración

La configuración es exactamente la misma que la de la primera parte de este artículo con dos excepciones :

1. El perfil de política se establece en conmutación local. La implementación de Flex requiere que Central Association esté desactivada hasta la versión 17.4 de Bengaluru.

A partir de la versión 17.5, este campo no está disponible para la configuración del usuario, ya que está codificado.



2. La etiqueta del sitio se establece en no ser sitio local

Solución de problemas de Flexconnect/Fabric

Debido a que el AP es el dispositivo que aplica las políticas de QoS, estos comandos pueden ayudar a restringir lo que se aplica.

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


AP780C-F085-49E6#
```

Referencias

[Guía de QoS de Catalyst 9000 16.12]

[Guía de configuración de QoS 9800]

[Modelo de configuración de Catalyst 9800]

[Notas de la versión de Cisco IOS® XE 17.6]

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).