QoS (BDRL)-snelheidslimiet configureren voor Catalyst 9800 draadloze controllers met AAA-opheffing

Inhoud

Inleiding

Dit document beschrijft een configuratievoorbeeld voor BI Directional Rate Limit (BDRL) op Catalyst 9800 Series draadloze controllers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Catalyst draadloze 9800 configuratiemodel
- AAA met Cisco Identity Service Engine (ISE)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Catalyst 9800-CL draadloze controller op versie 9 16.12.1s
- Identity Service Engine op versie 2.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle

apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

QoS in 9800 WLC-platform maakt gebruik van dezelfde concepten en componenten als Catalyst 9000-platforms.

In dit gedeelte wordt een globaal overzicht gegeven van hoe deze componenten werken en hoe ze kunnen worden geconfigureerd om verschillende resultaten te bereiken.

In essentie werkt QoS-recursie als volgt:

1. Klasse-Map: identificeert een bepaald type verkeer. Class-maps kunnen gebruikmaken van de Application Visibility and Control (AVC) engine.

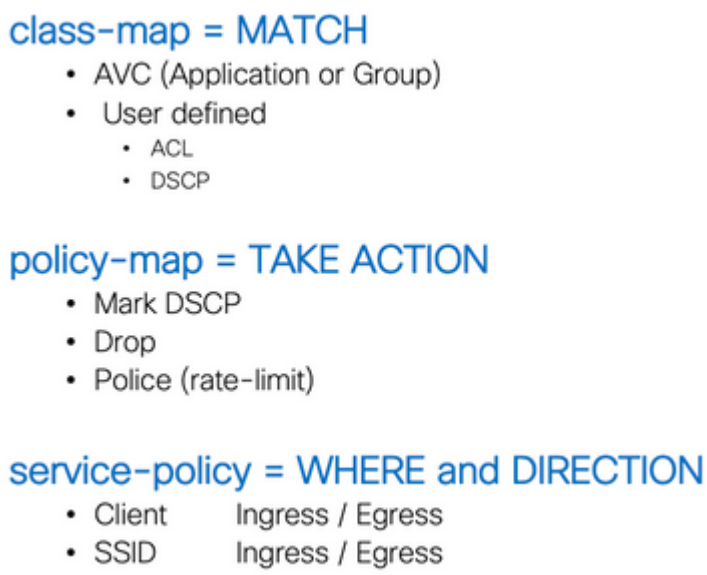
De gebruiker kan ook aangepaste klasse-kaarten definiëren om verkeer te identificeren dat overeenkomt met een toegangscontrolelijsten (ACL) of een gedifferentieerd servicescodepunt (DSCP)

2. Policy-Map: zijn beleidslijnen die van toepassing zijn op Class-maps.
Dit beleid kan DSCP markeren, of het verkeer beperken dat overeenkomt met de klasse-kaart

4. Service-Policy: Policy-maps kunnen worden toegepast op het Policy Profile van een SSID of Per-Client op een bepaalde richting met de service-policy commando.

3. (facultatief) Table-Map: Ze worden gebruikt om een type van merk naar een ander, bijvoorbeeld CoS naar DCSP om te zetten.

Opmerking: Specificeer in de tabel-kaart de te wijzigen waarden (4 tot 32); in de beleidskaart wordt de technologie gespecificeerd (COS tot DSCP).



Opmerking: Indien twee of meer beleidslijnen per doelstelling van toepassing zijn, wordt de beleidsresolutie gekozen op basis van deze prioriteitsklasse:

· AAA-overschrijding (hoogste)
· Native profiling (lokaal beleid)
· Geconfigureerd beleid
· Standaardbeleid (laagste)

Meer details zijn te vinden in de officiële QoS-configuratiehandleiding voor de 9800

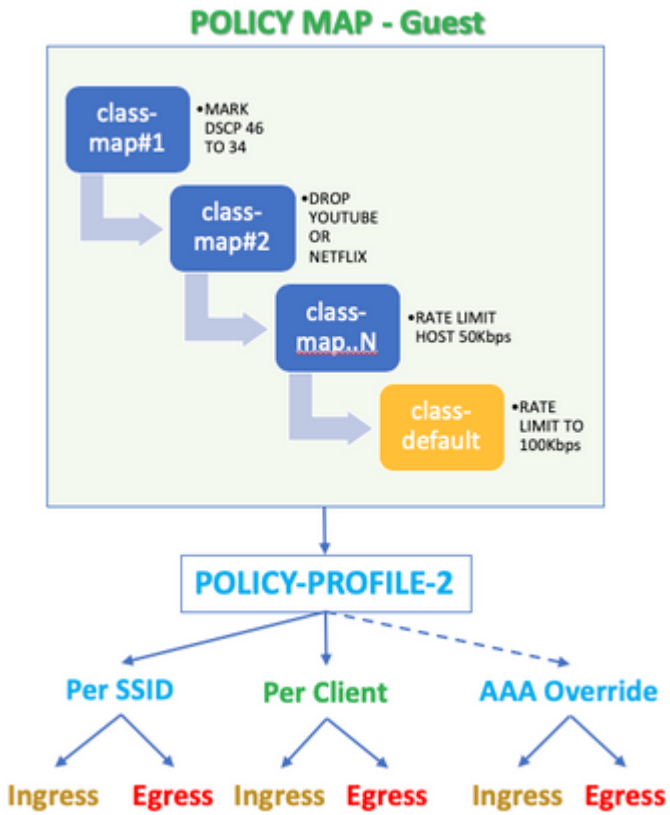
Aanvullende informatie over de QoS-theorie kan worden gevonden in de QoS-configuratiehandleiding van de 9000-serie

Voorbeeld: Guest and Corp QoS-beleid

Dit voorbeeld toont aan hoe de verklaarde componenten QoS in een echt wereldscenario van toepassing zijn.

De bedoeling is om een QoS-beleid voor gasten te configureren dat:

- Opmerkingen DSCP
- Drops YouTube en Netflix video
- Snelheidsbeperkingen voor een host die in een ACL is gespecificeerd, tot 50 Kbps
- Snelheid beperkt al het andere verkeer tot 100 Kbps



Het QoS-beleid moet bijvoorbeeld worden toegepast per SSID in beide richtingen Ingress en uitgaande naar het beleidsprofiel dat koppelt naar het Guest WLAN.

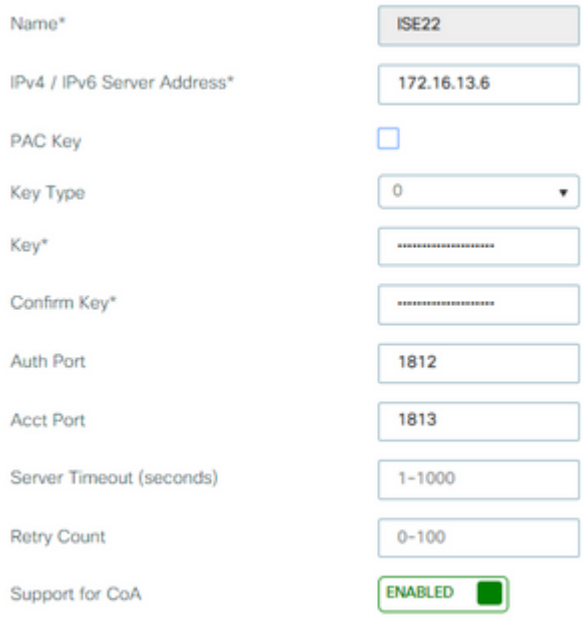
Configureren

AAA-server en methodelijst

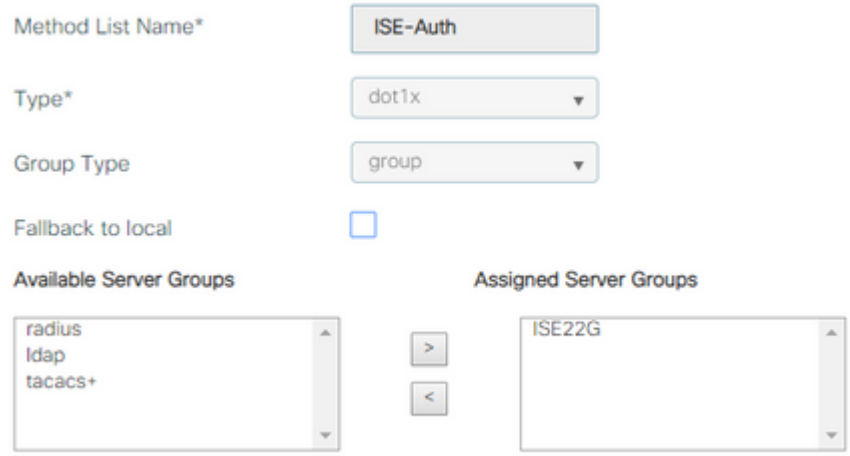
Stap 1. Navigeer naar **Configuratie > Beveiliging > AAA > Verificatie > Servers/groepen** en selecteer

+Add.

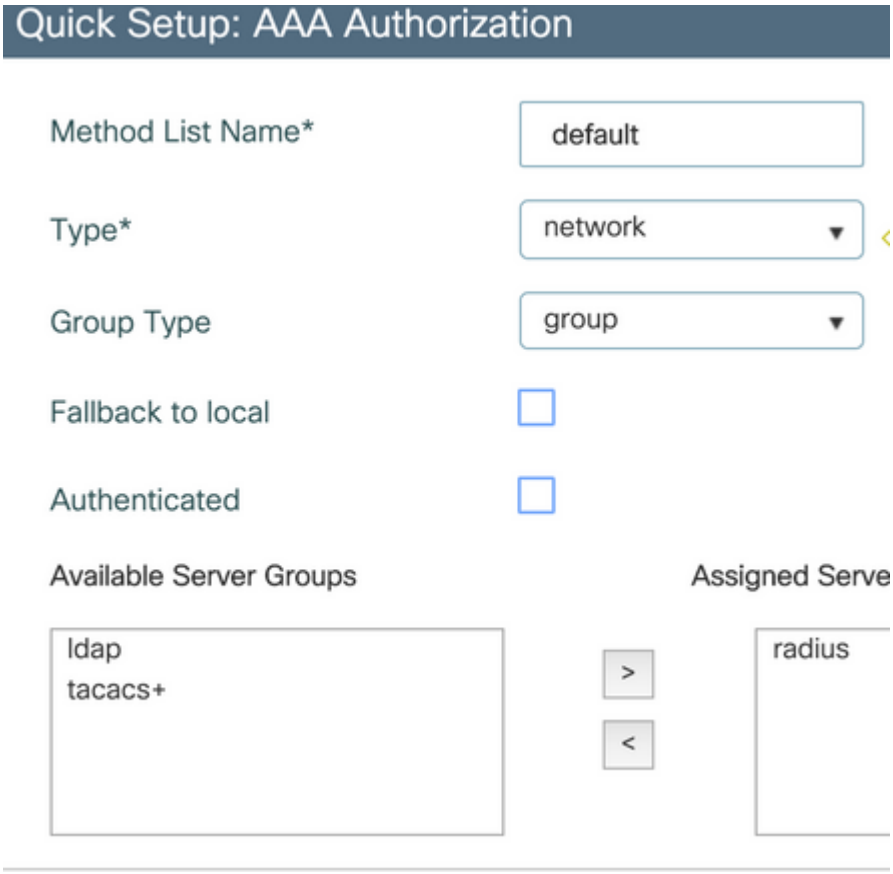
Voer de naam, het IP-adres en de sleutel van de AAA-server in. Deze moeten overeenkomen met het gedeelde geheim onder **Beheer > Netwerkbronnen > Netwerkapparaten** op ISE.



Stap 2. Navigeer naar **Configuratie > Beveiliging > AAA > Verificatie > AAA-methodelijst** en selecteer **+Add.** Selecteer de Toegewezen servergroepen in de lijst met beschikbare servergroepen.



Stap 3. Navigeer naar **Configuratie > Beveiliging > AAA > Autorisatie > AAA-methodelijst** en selecteer **Toevoegen.** Kies de standaardmethode en "netwerk" als type.

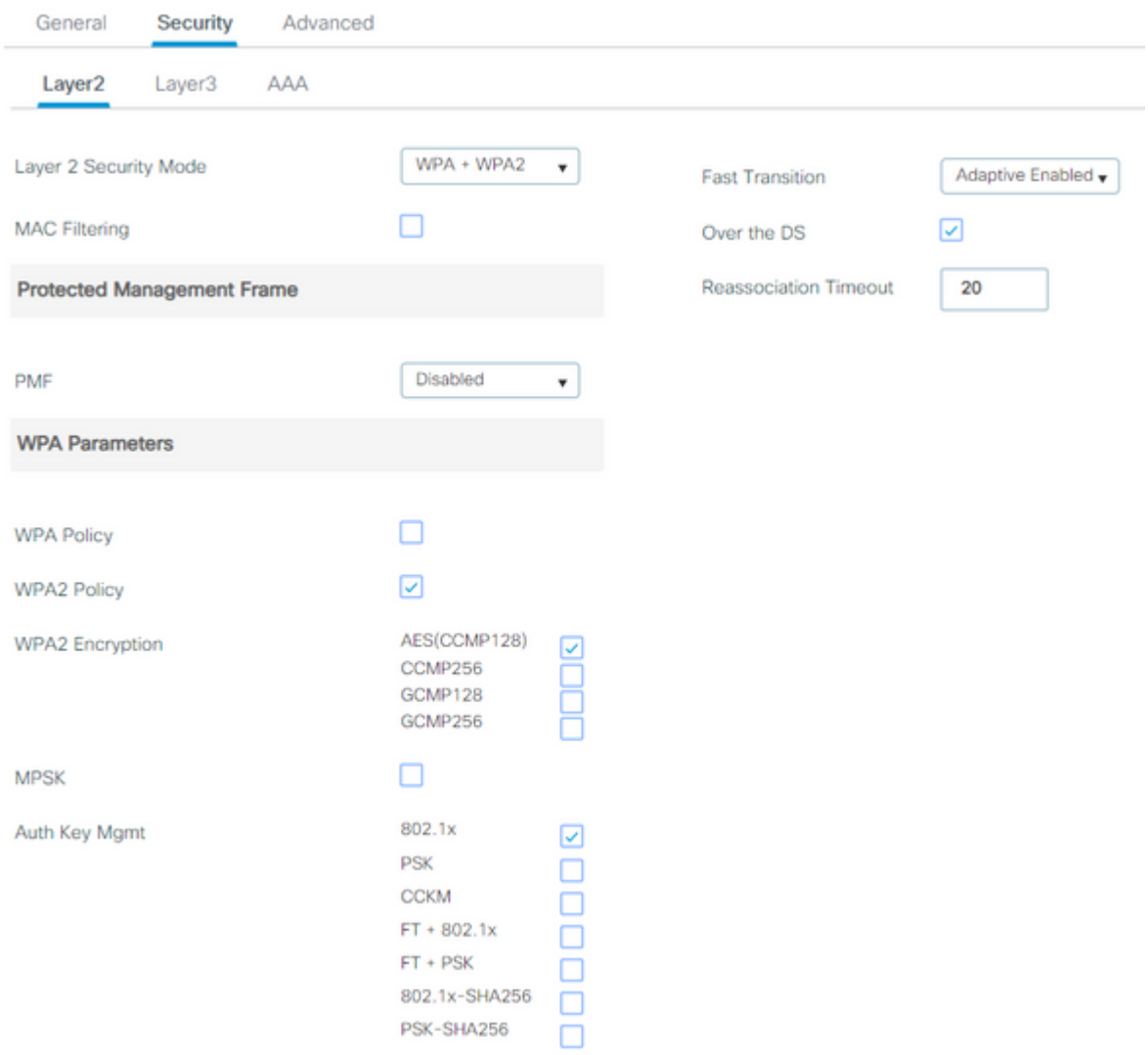


Dit is vereist als de controller de autorisatiekenmerken wil toepassen (bijvoorbeeld het QoS-beleid hier) die door de AAA-server worden teruggestuurd. Anders wordt het beleid dat van RADIUS wordt ontvangen niet toegepast.

WLAN-beleid, sitetag en AP-tag

Stap 1. Ga naar **Configuration > Wireless Setup > Advanced > Start nu > WLAN-profiel** en selecteer **+Add** om een nieuw WLAN te maken. Configureer de SSID, Profielnaam, WLAN-id en stel de status in op ingeschakeld.

Navigeer vervolgens naar **Security > Layer 2** en configureer de Layer 2-verificatieparameters:

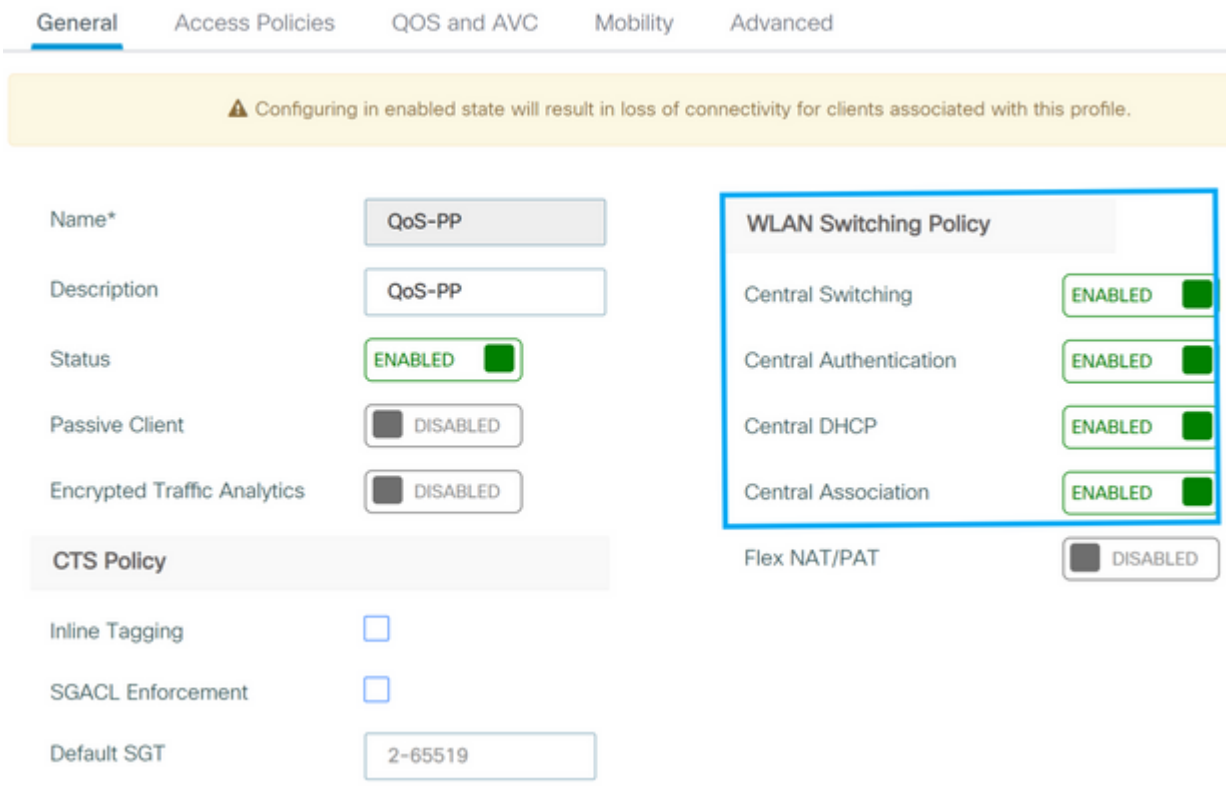


De SSID-beveiliging hoeft niet 802.1x te zijn als vereiste voor QoS, maar wordt in dit configuratievoorbeeld gebruikt voor AAA-override.

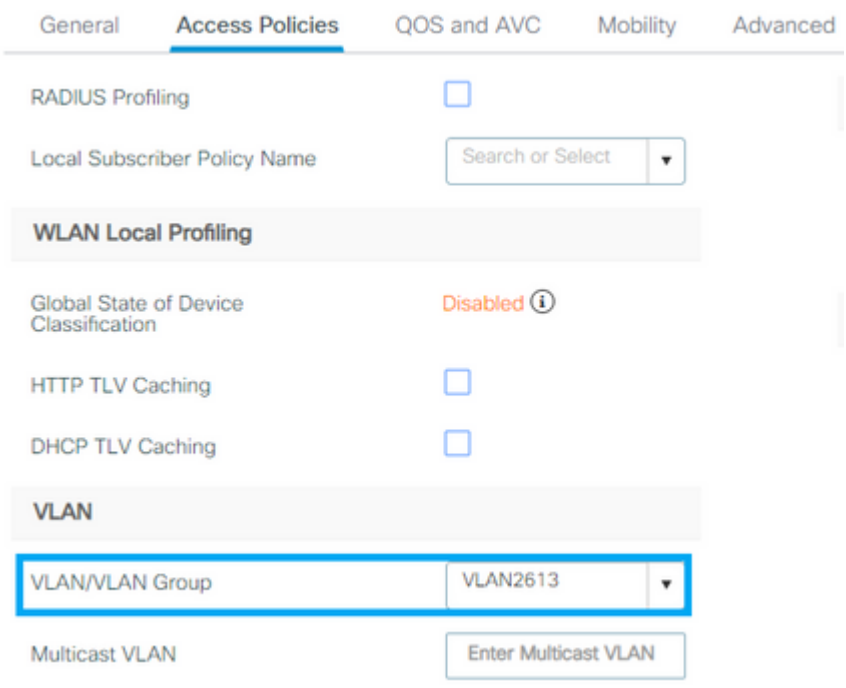
Stap 2. Navigeer naar **Security > AAA** en selecteer de AAA-server in het vervolgkeuzevenster **Verificatielijst**.

Stap 3. Selecteer **Beleidsprofiel** en selecteer **+Add.** Configureer de naam van het beleidsprofiel.

Stel de status in als Ingeschakeld. Schakel ook Centrale switching, verificatie, DHCP en associatie in:

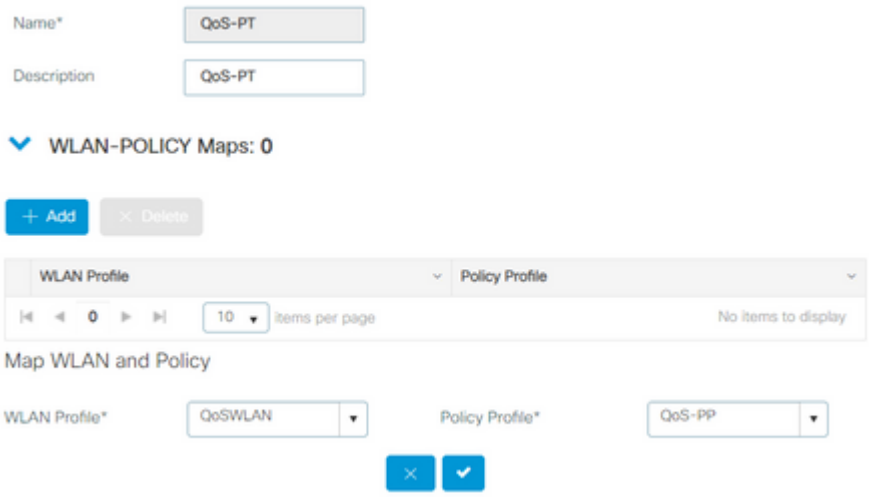


Stap 4. Navigeer naar **Toegangsbeleid** en configureer het VLAN waaraan de draadloze client is toegewezen wanneer de client verbinding maakt met de SSID**:**

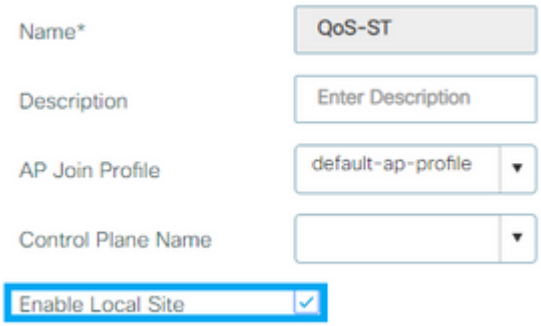


Stap 5. Selecteer **Beleidsmarkering** en selecteer **+Add.** Configureer de naam van de beleidstag.

Selecteer onder **WLAN-beleidskaarten** op **+Add** de optie **WLAN-profiel** en **WLAN-beleidsprofiel** in de uitrolmenu's. Selecteer vervolgens de optie voor het configureren van de kaart.



Stap 6. Selecteer **Site Tag** en selecteer **+Add.** Schakel het vakje **Local Site inschakelen in** als de toegangspunten in Local Mode moeten werken (of als u FlexConnect niet wilt inschakelen)**:**

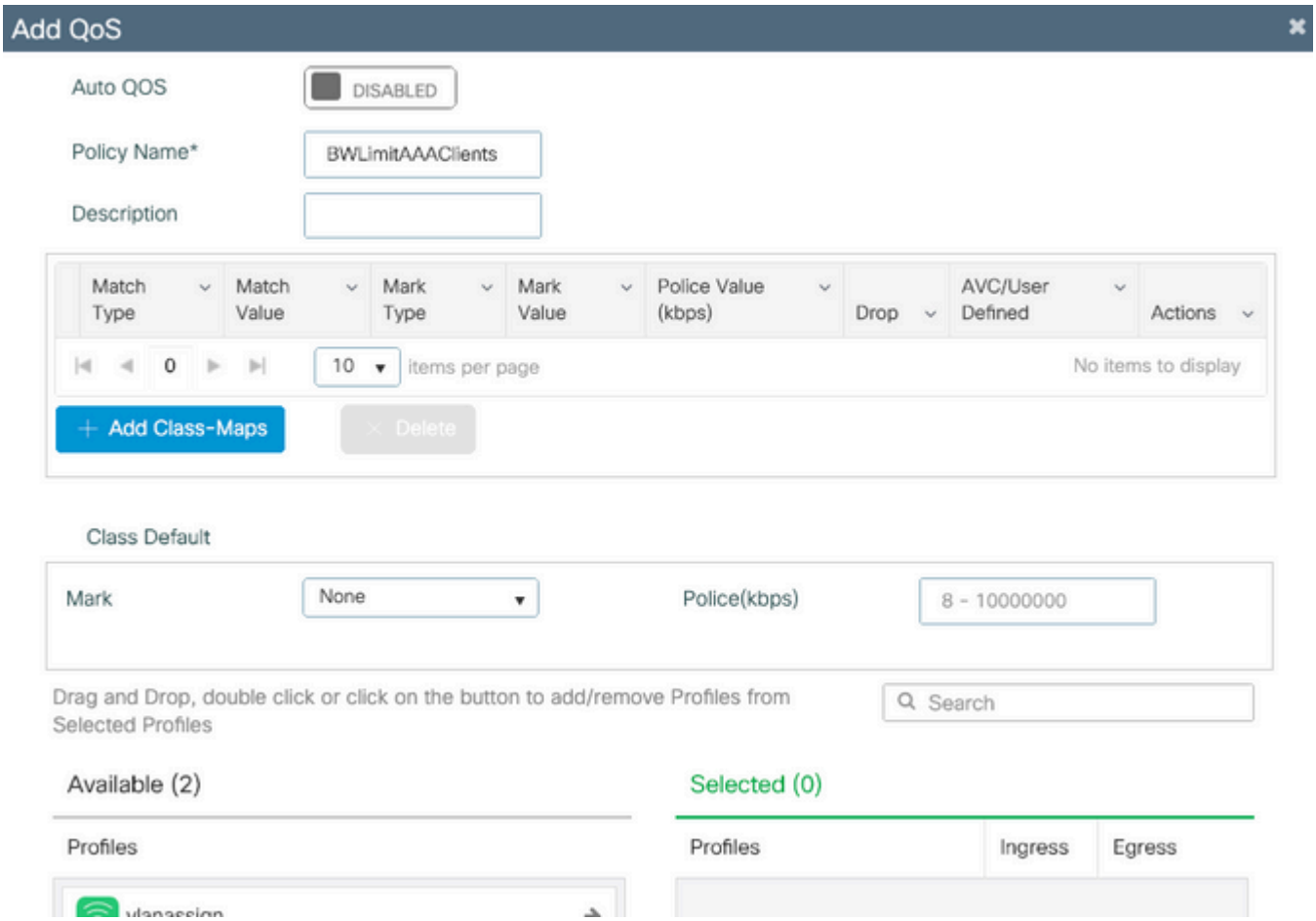


Stap 7. Selecteer **Tag AP's**, kies de AP's en voeg de Policy, Site en RF tag toe:

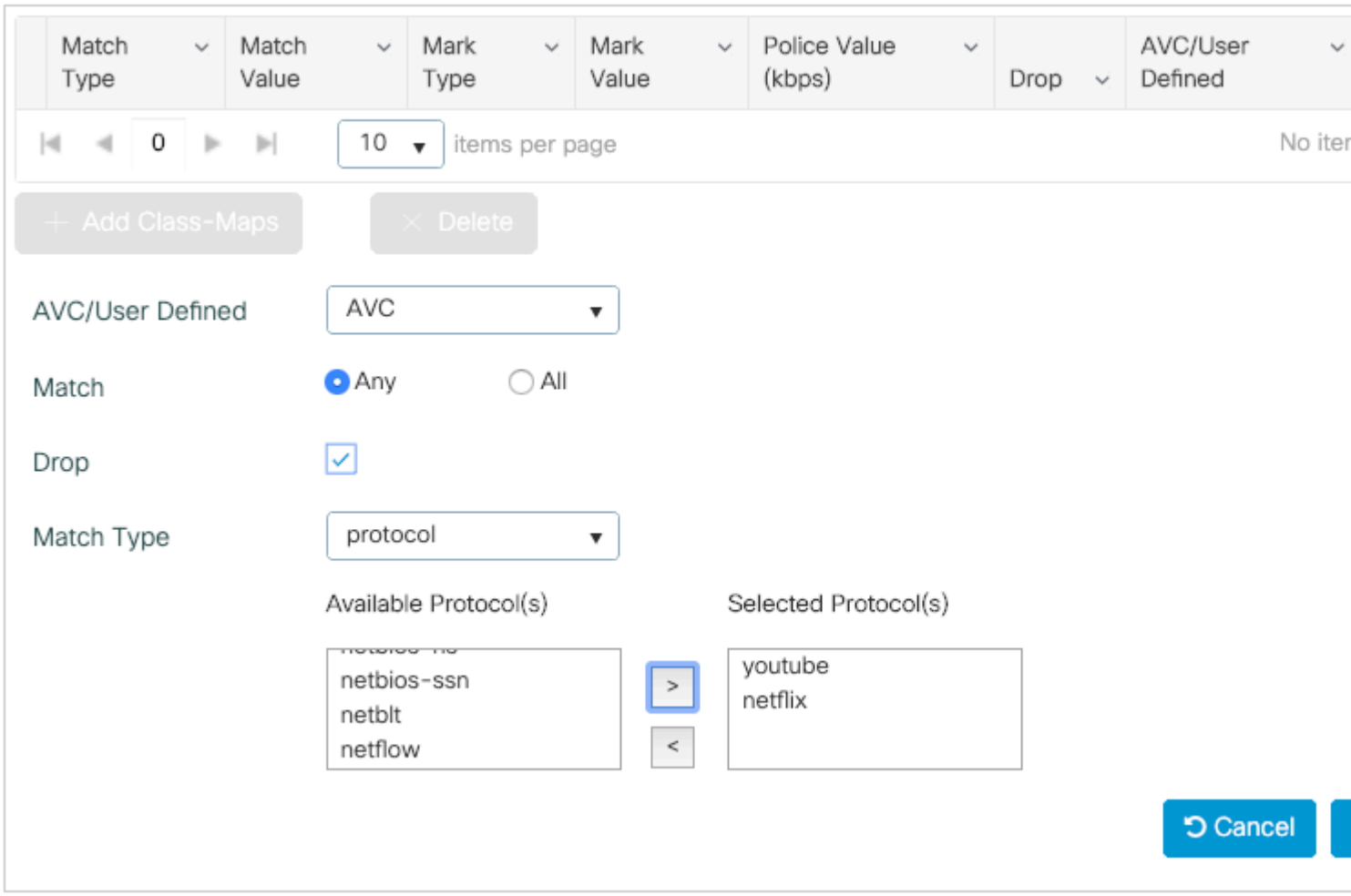
QoS

Stap 1. Navigeer naar **Configuration > Services > QoS** en selecteer **+Add** om een QoS-beleid te maken.

Noem het (bijvoorbeeld: BWLimitAAAClients).



Stap 2. Voeg een klassenkaart toe om Youtube en Netflix te laten vallen. Klik op **Klasse-Maps toevoegen**. Selecteer **AVC**, stem **om het even welke**, **drop**-actie af en kies beide protocollen.



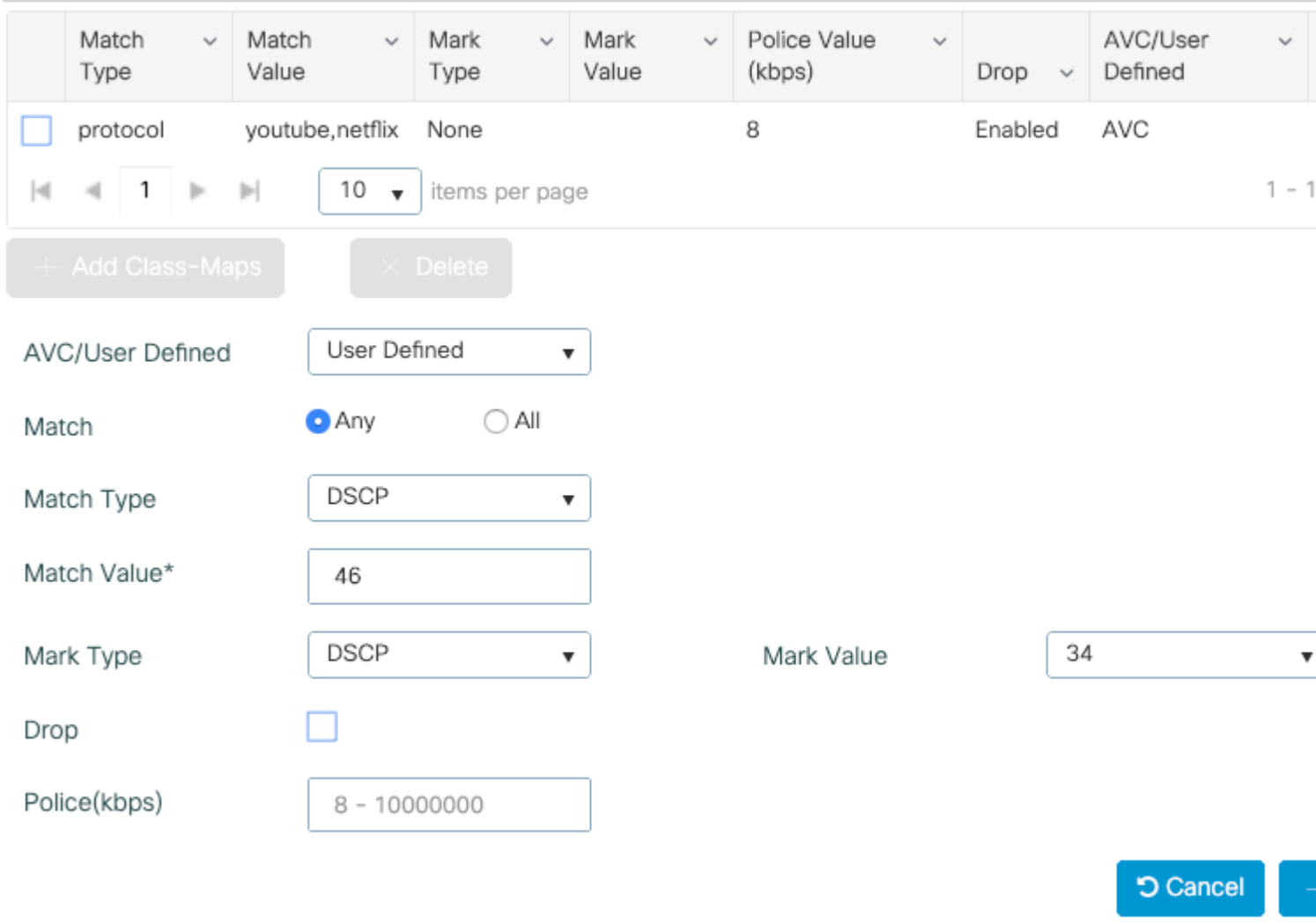
Sla op **Opslaan.**

Stap 3. Voeg een klassenkaart toe die DSCP 46 tot 34 opmerkt.

Klik op **Klasse-kaarten toevoegen**.

- Overeenkomend met **elk gewenst, door gebruiker gedefinieerd**
- **DSCP**-type overeenkomst
- Overeenkomstwaarde **46**
- **DSCP**-type markeren
- Merkwaarde **34**

.



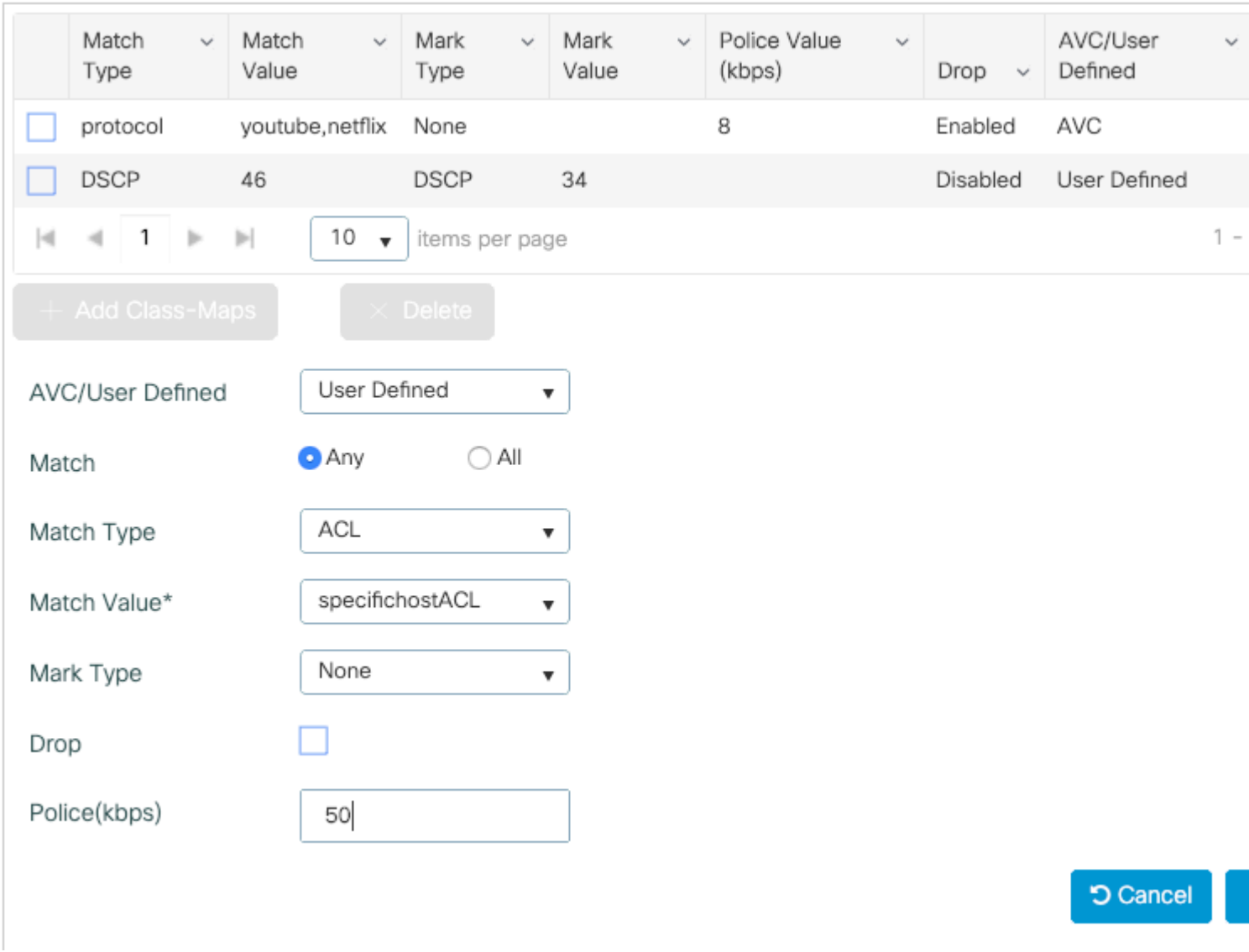
Sla op **Opslaan.**

Stap 4. Om een klassenkaart te bepalen die verkeer aan een specifieke gastheer regelt, creeer ACL voor het.

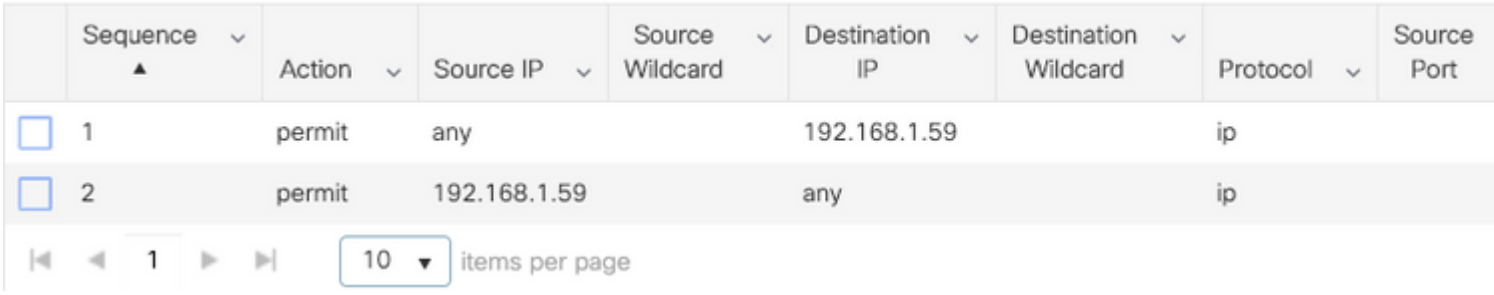
Klik op **Klasse-kaarten toevoegen**.

Kies door gebruiker gedefinieerd, **overeenkomen met een** overeenkomend type **ACL**, kies uw ACL-naam (hier **specifichostACL**), merk type **niets** en kies de snelheidsgrenswaarde.

Klik op Save (Opslaan).

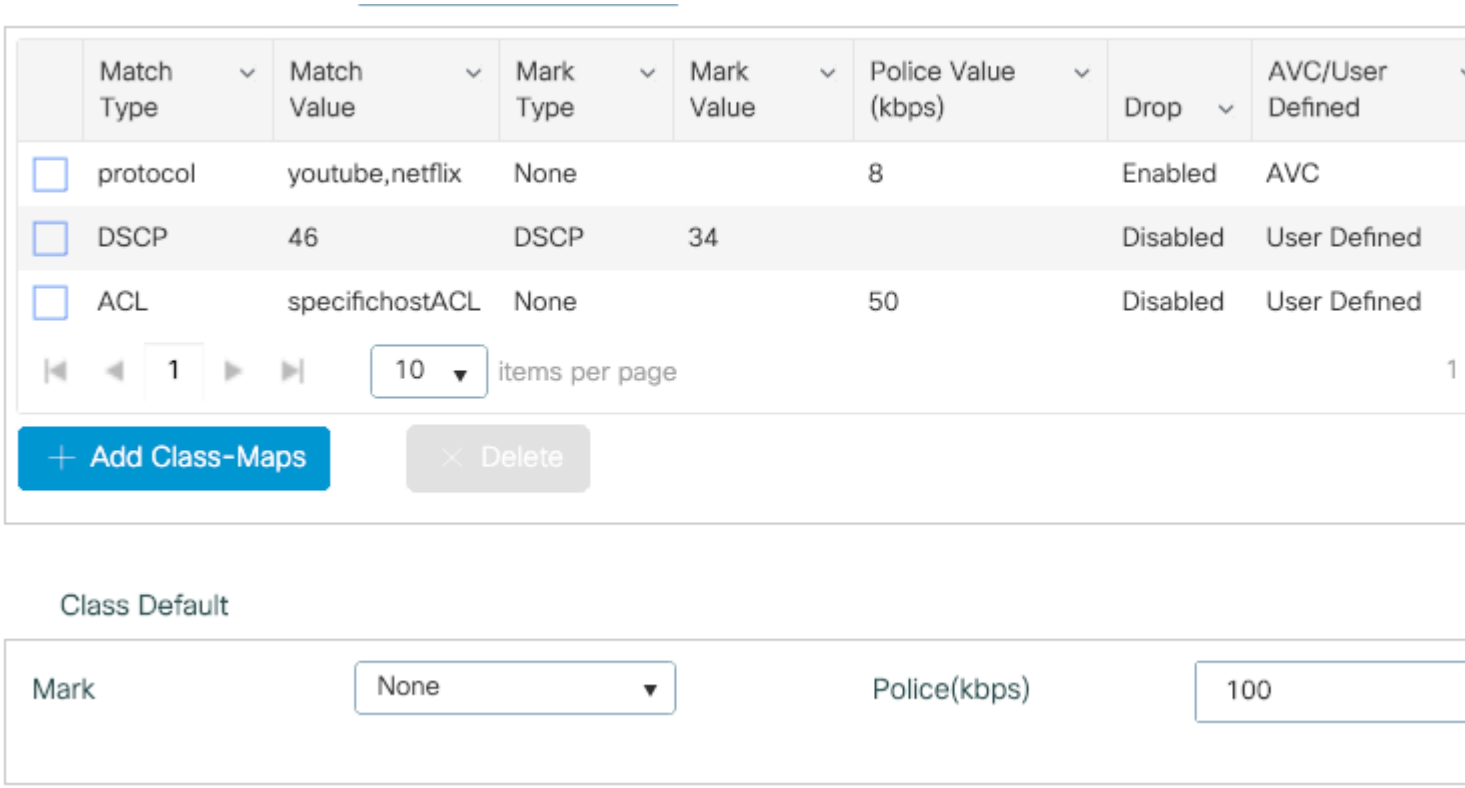


Hier is een voorbeeld van ACL die we gebruiken om een specifiek hostverkeer te identificeren:



Stap 5. Gebruik onder het frame met klassekaarten de standaardklasse om de snelheidslimiet voor al het andere verkeer in te stellen.

Dit stelt een maximumtarief vast voor al het cliëntenverkeer dat niet onder een van de bovenstaande regels valt.



Stap 6. Klik onderaan op **Toepassen op apparaat**.

CLI-equivalente configuratie:

```
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
```

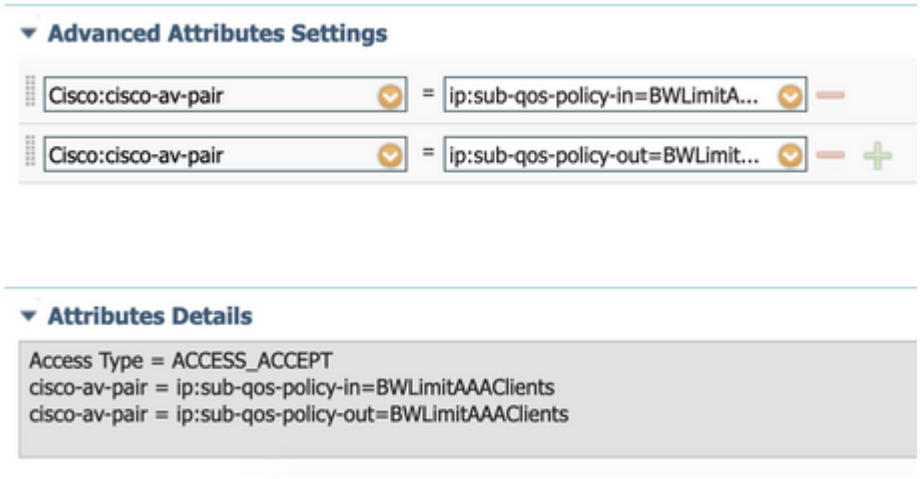
Opmerking: in dit voorbeeld zijn geen **profielen** geselecteerd onder het QoS-beleid, omdat AAA-opheffing wordt toegepast. Als u het QoS-beleid echter handmatig op een beleidsprofiel wilt toepassen, selecteert u de gewenste profielen.

Stap 2. Ga op ISE naar **Policy > Policy Elements > Results > Authorisation Profiles** en selecteer on **+Add** om een autorisatieprofiel te maken.

Als u het QoS-beleid wilt toepassen, voegt u deze toe als **Advanced Attributes Settings** via Cisco AV Paren.

Er wordt aangenomen dat het beleid voor ISE-verificatie en -autorisatie zodanig is geconfigureerd dat het aan de juiste regel voldoet en dit autorisatieresultaat krijgt.

De kenmerken zijn **ip:sub-qos-policy-in=<policy name>** en **ip:sub-qos-policy-out=<policy-name>**



Opmerking: beleidsnamen zijn hoofdlettergevoelig. Controleer of de case juist is!

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt:

Op de 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
```

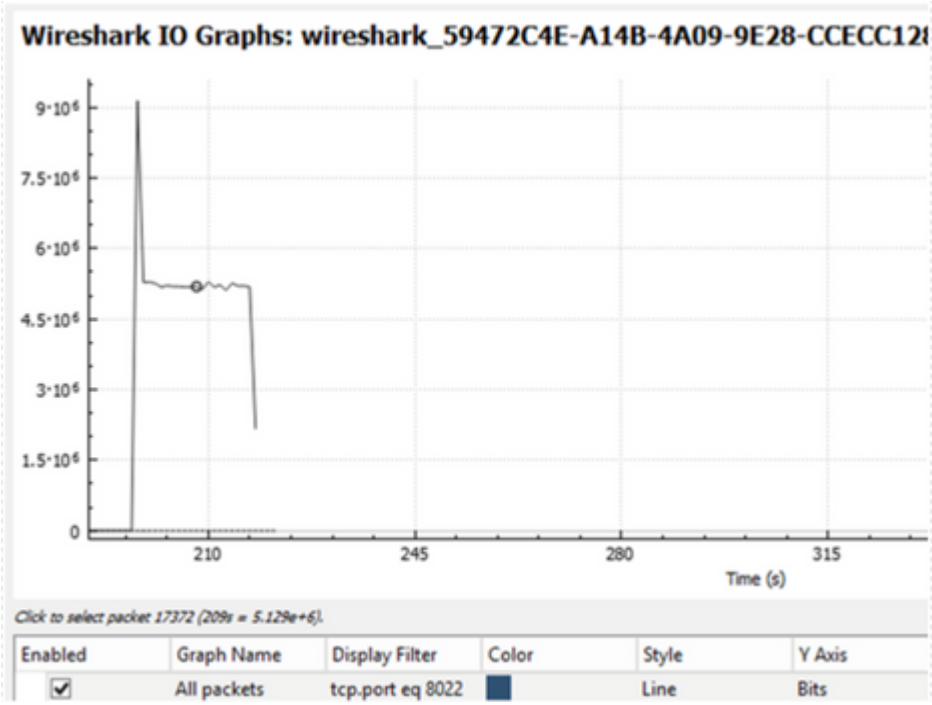
<#root>

```
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
```

Op het toegangspunt

Er is geen probleemoplossing vereist op het toegangspunt wanneer het toegangspunt zich in de lokale modus bevindt of wanneer het toegangspunt zich in de modus Flexconnect Central Switching bevindt omdat het QoS- en servicebeleid door de WLC wordt uitgevoerd.

PacketCapture IOS-grafieanalyse



Problemen oplossen

Deze sectie verschaft informatie om problemen met uw configuratie op te lossen.

Stap 1. Schakel alle bestaande debug-voorwaarden uit.

```
# clear platform condition all
```

Stap 2. Schakel de debug voor de draadloze client in kwestie in.

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

Stap 3. Sluit de draadloze client aan op de SSID om het probleem te reproduceren.

Stap 4. Stop de debugs zodra de kwestie wordt gereproduceerd.

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

De logbestanden die tijdens de test worden opgenomen, worden in de WLC opgeslagen in een lokaal bestand met de naam:

ra_trace_MAC_aabbcccc_HMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Als de GUI-workflow wordt gebruikt om deze overtrek te genereren, is de opgeslagen bestandsnaam debugTrace_aaaa.bbbb.ccc.txt.

Stap 5. Als u het eerder gegenereerde bestand wilt verzamelen, kopieert u het spoor .log naar een externe server of geeft u de uitvoer rechtstreeks op het scherm weer.

Controleer de naam van het RA traces bestand met deze opdracht:

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

Kopieert het bestand naar een externe server:

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

U kunt ook de inhoud weergeven:

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

Stap 6. Verwijder de debug-voorwaarden.

```
# clear platform condition all
```

Flexconnect lokale switching (of fabric/SDA)-scenario

In het geval van flexconnect lokale switching (of stof / SDA), is het de AP die elk QoS-beleid toepast dat u hebt gedefinieerd op de WLC.

Op Wave2 en 11ax access points vindt snelheidsbeperking plaats op een per-flow (5 tuple) niveau en niet per client of per SSID voor 17.6.

Dit is van toepassing op AP in Flexconnect/Fabric, Ingesloten draadloze controller op access point (EWc-AP) implementaties.

Vanaf 17.5 kan AAA-overschrijding worden ingezet om de kenmerken zodanig te duwen dat de snelheidslimiet per client wordt bereikt.

Vanaf 17.6 wordt de bidirectionele snelheidslimiet per client ondersteund op 802.11ac Wave 2 en 11ax APâ€™s in Flex lokale switchconfiguratie.

> **Opmerking**: Flex APâ€™s ondersteunen de aanwezigheid van ACLâ€™s in QoS-beleid niet. Ze ondersteunen ook geen BRR (bandbreedte blijft) en beleidsprioriteit die configureerbaar zijn via de

---

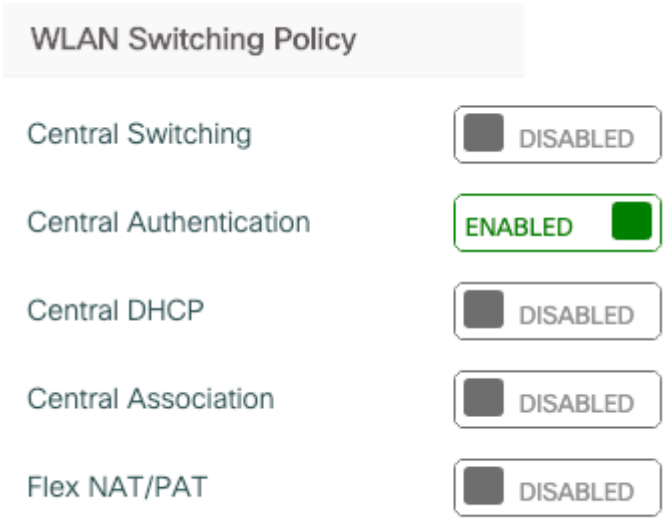
CLI maar niet beschikbaar zijn in de 9800 web UI en niet ondersteund worden op 9800. Cisco bug-id CSCvx81067 houdt de ondersteuning van ACLâ€™s in QoS-beleid voor flex APâ€™s bij.

Configuratie

De configuratie is precies hetzelfde als het eerste deel van dit artikel, met twee uitzonderingen:

1. Het beleidsprofiel is ingesteld op lokale switching. Flex-implementatie vereist dat Central Association wordt uitgeschakeld tot Bengaluru 17.4 release.

Vanaf 17.5 is dit veld niet beschikbaar voor gebruikersconfiguratie omdat het hardcodeerd is.



2. Het sitetag is ingesteld op niet-lokale site

Probleemoplossing voor Flexconnect/Fabric

Omdat het toegangspunt het apparaat is dat het QoS-beleid toepast, kunnen deze opdrachten helpen te versmallen wat wordt toegepast.

toon dot11 qos

beleidsanalyse tonen

client voor snelheidsbeperking weergeven

Bssid met snelheidsbeperking weergeven

show rate-limit WLAN

laten zien 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#
```

Referenties

[Catalyst 9000 16.12 QoS handleiding]

[De 9800 QoS-configuratiehandleiding]

[Catalyst 9800 configuratiemodel]

[Opmerkingen bij Cisco IOS® XE 17.6 release]

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.