Configurazione del limite di velocità QoS (BDRL) sui controller wireless Catalyst 9800 con override AAA

Sommario

Introduzione

Questo documento descrive un esempio di configurazione per Bi Directional Rate Limit (BDRL) sui controller wireless Catalyst serie 9800.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Catalyst Wireless 9800 modello di configurazione
- AAA con Cisco Identity Service Engine (ISE)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Catalyst 9800-CL Wireless Controller sulla versione 16.12.1s
- Identity Service Engine sulla versione 2.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

QoS nella piattaforma 9800 WLC utilizza gli stessi concetti e componenti delle piattaforme Catalyst 9000.

In questa sezione viene fornita una panoramica globale del funzionamento di questi componenti e di come è possibile configurarli per ottenere risultati diversi.

In sostanza, la ricorsione del QoS funziona così:

1. Class-Map: identifica un determinato tipo di traffico. Le mappe di classe possono utilizzare il motore AVC (Application Visibility and Control).

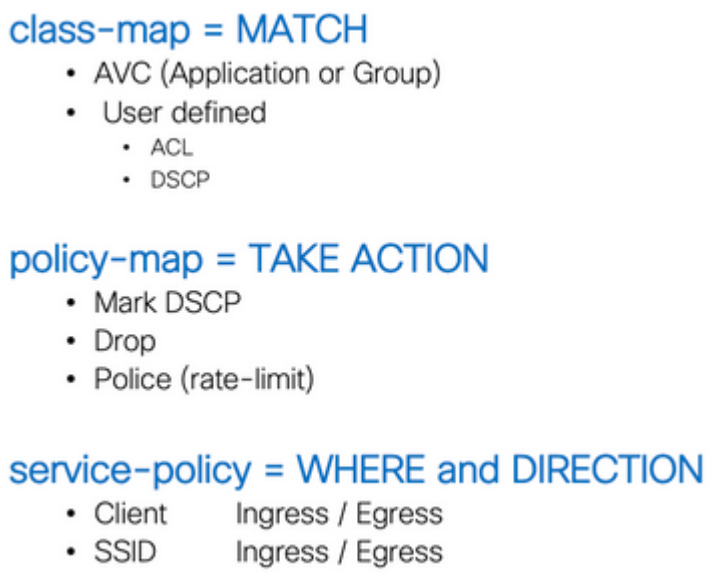
L'utente può inoltre definire mappe di classi personalizzate per identificare il traffico che corrisponde a un Access Control Lists (ACL) o a un Differentiated Services Code Point (DSCP)

2. Policy-Map: criteri che si applicano alle mappe di classi.
Questi criteri possono contrassegnare DSCP, eliminare o limitare il traffico che corrisponde alla mappa classi

4. Service-Policy: le mappe dei criteri possono essere applicate al profilo dei criteri di un SSID o per client in una determinata direzione con il comando service-policy.

3. (Facoltativo) Mapping tabella: vengono utilizzati per convertire un tipo di contrassegno in un altro, ad esempio CoS in DCSP.

Nota: nella mappa-tabella, specificare i valori da modificare (da 4 a 32); nella mappa-criteri, la tecnologia è specificata (da COS a DSCP).



Nota: nel caso in cui siano applicabili due o più criteri per oggetto, la risoluzione dei criteri viene scelta in base alla seguente classificazione di priorità:

· Override AAA (massimo)
· Profiling nativo (criteri locali)
· Criteri configurati
· Criterio predefinito (minimo)

Per maggiori dettagli, consultare la guida ufficiale alla configurazione QoS per 9800

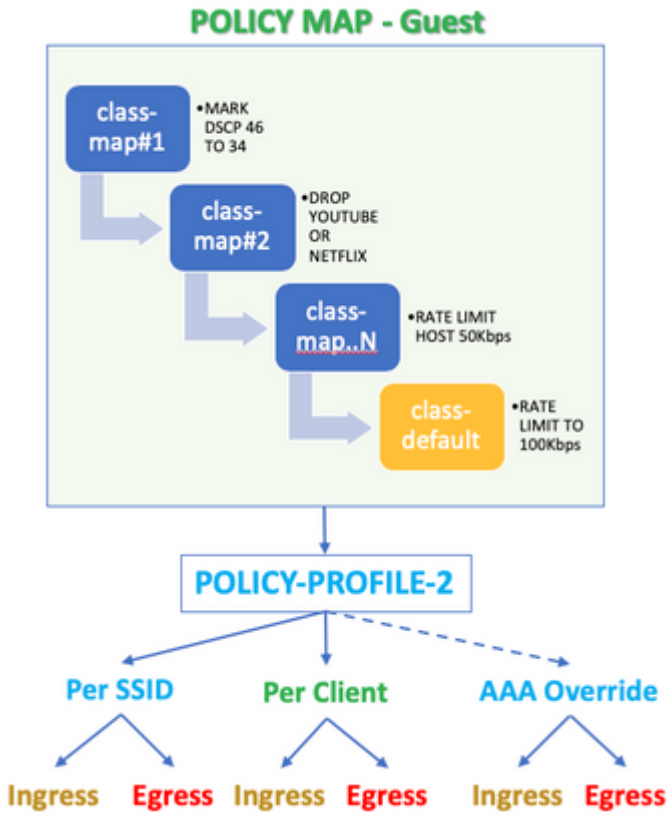
Ulteriori informazioni sulla teoria QoS sono disponibili nella guida alla configurazione QoS della serie 9000

Esempio: criteri QoS guest e aziendali

Nell'esempio viene mostrato come i componenti QoS spiegati si applicano in uno scenario reale.

L'obiettivo è configurare un criterio QoS per i guest che:

- Note DSCP
- Getta video su Youtube e Netflix
- Limita la velocità a 50 Kbps di un host specificato in un ACL
- Velocità Limita tutto il resto del traffico a 100 Kbps



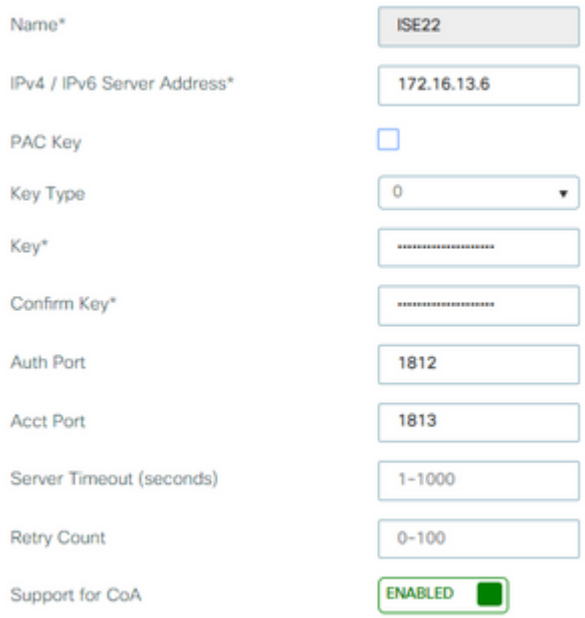
Ad esempio, il criterio QoS deve essere applicato per SSID in entrambe le direzioni: In entrata e In uscita verso il profilo del criterio che si collega alla WLAN guest.

Configurazione

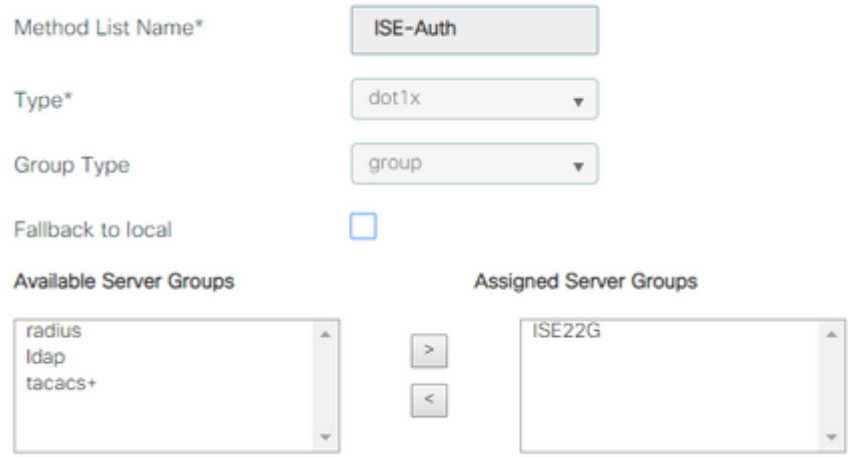
Server AAA ed elenco metodi

Passaggio 1. Passare a **Configurazione > Sicurezza > AAA > Autenticazione > Server/Gruppi** e selezionare **+Aggiungi.**

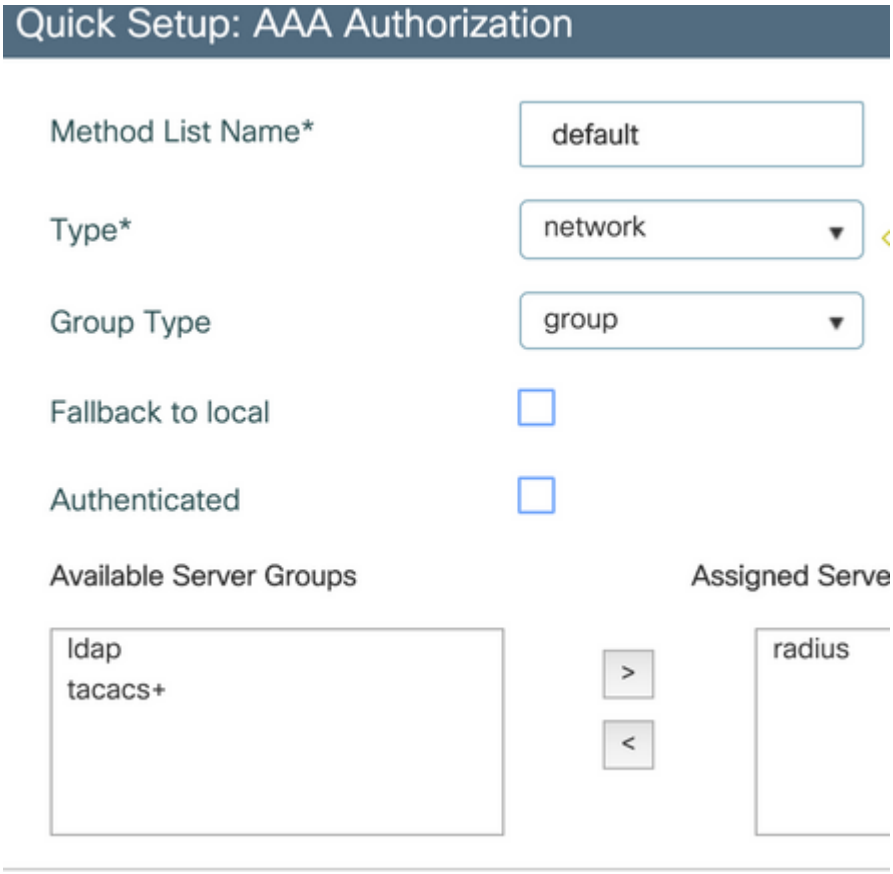
Immettere il nome del server AAA, l'indirizzo IP e la chiave che devono corrispondere al segreto condiviso in **Amministrazione > Risorse di rete > Dispositivi di rete** su ISE.



Passaggio 2. Selezionare **Configurazione > Sicurezza > AAA > Autenticazione > Elenco metodi AAA** e selezionare **+Aggiungi.** Selezionare i gruppi di server assegnati da Gruppi di server disponibili.



Passaggio 3. Selezionare **Configurazione > Sicurezza > AAA > Autorizzazione > Elenco metodi AAA** e selezionare **Aggiungi.** Selezionate il metodo di default e "network" come tipo.

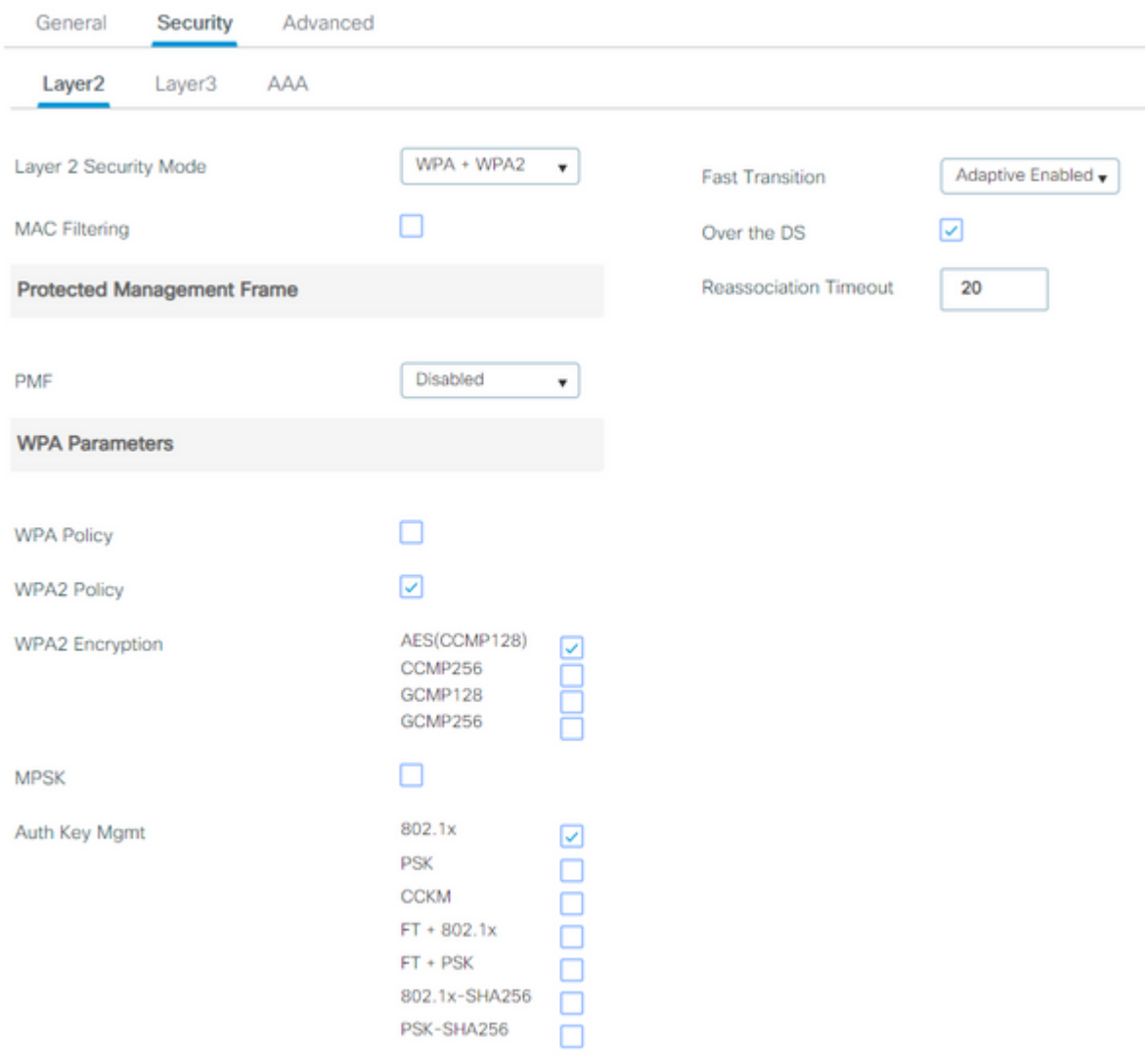


Questa operazione è necessaria per consentire al controller di applicare gli attributi di autorizzazione (ad esempio, il criterio QoS qui) restituiti dal server AAA. In caso contrario, il criterio ricevuto da RADIUS non verrà applicato.

Criteri WLAN, tag del sito e tag AP

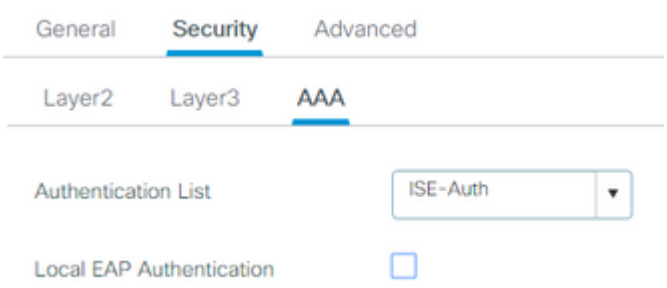
Passaggio 1. Selezionare **Configuration > Wireless Setup > Advanced > Start Now > WLAN Profile** (Configurazione > Configurazione wireless > Avanzate > Avvia ora > Profilo WLAN), quindi selezionare **+Add** (Aggiungi) per creare una nuova WLAN. Configurare SSID, Nome profilo, ID WLAN e impostare lo stato su Abilitato.

Quindi, selezionare **Sicurezza > Layer 2** e configurare i parametri di autenticazione di Layer 2:



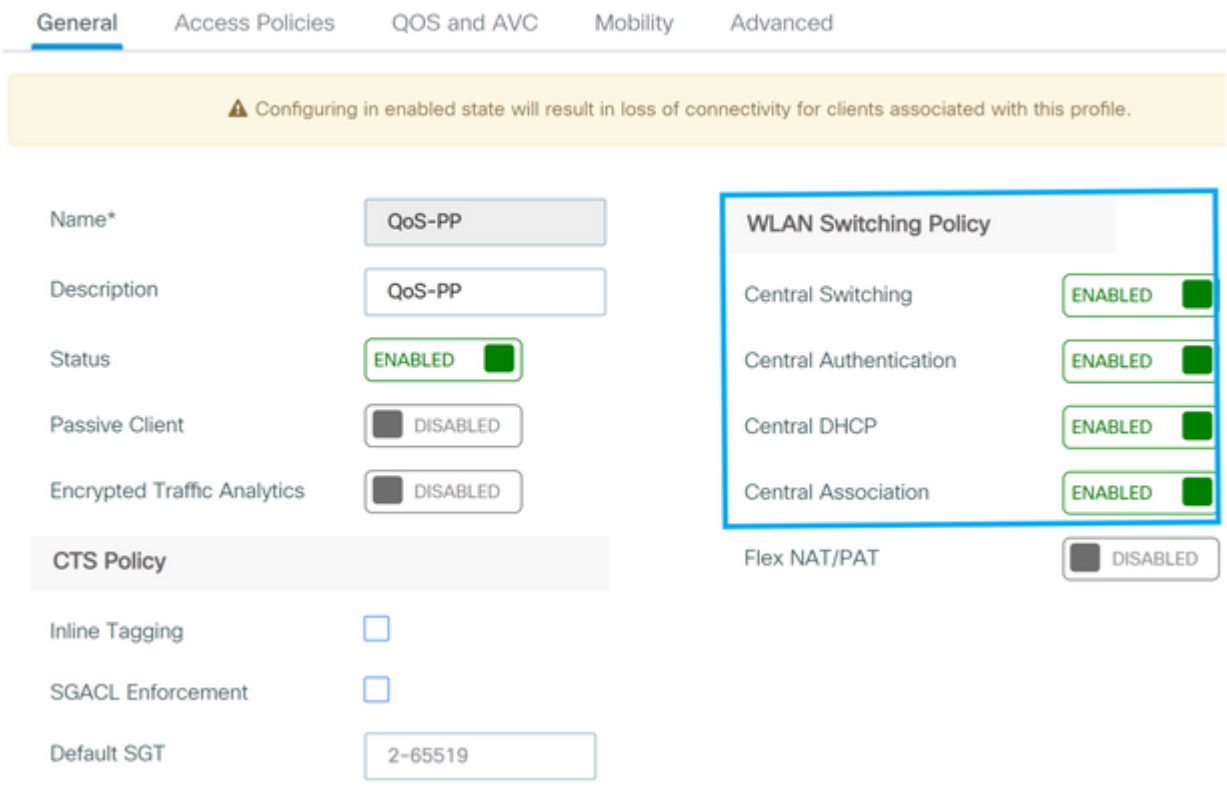
La sicurezza SSID non deve essere necessariamente 802.1x come requisito per QoS, ma viene utilizzata in questo esempio di configurazione per l'override di AAA.

Passaggio 2. Passare a **Sicurezza > AAA** e selezionare il server AAA nella casella di riepilogo a discesa **Authentication List** (Elenco autenticazione).

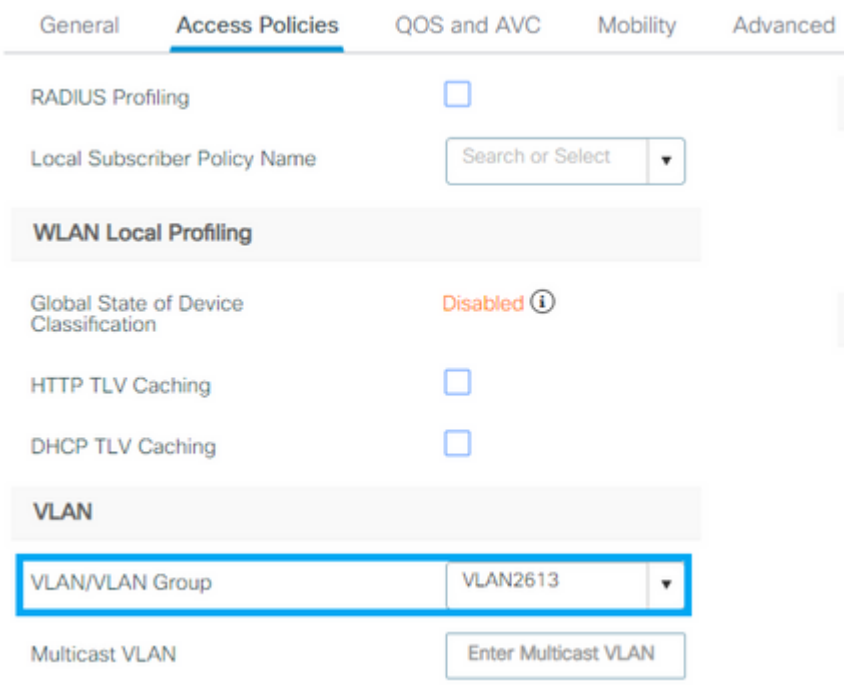


Passaggio 3. Selezionare **Policy Profile** (Profilo criterio), quindi selezionare **+Add (Aggiungi).** Configurare il nome del profilo dei criteri.

Impostare lo stato su Abilitato. Abilitare anche la commutazione centrale, l'autenticazione, DHCP e l'associazione:

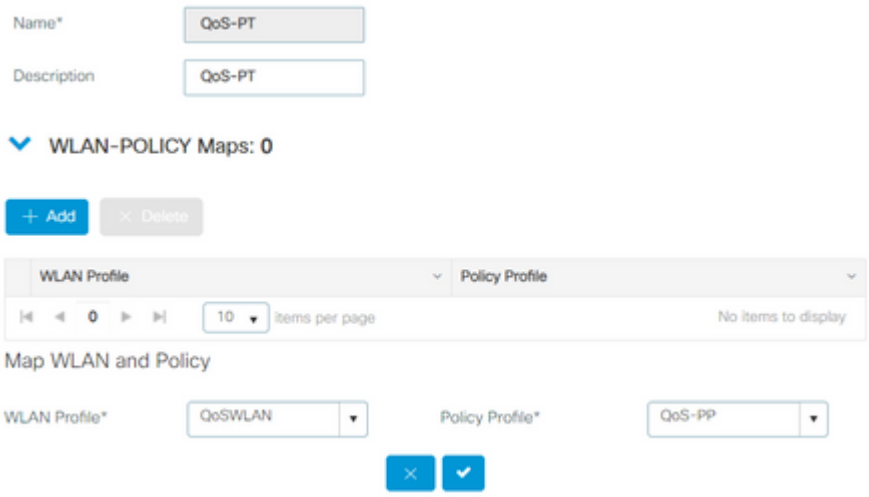


Passaggio 4. Passare a **Criteri di accesso** e configurare la VLAN a cui è assegnato il client wireless quando questo si connette all'SSID**:**

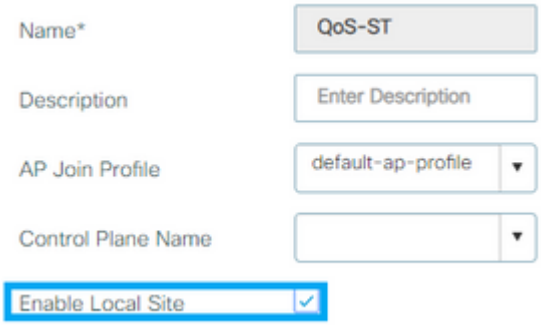


Passaggio 5. Selezionare **Tag criteri** e selezionare **+Aggiungi.** Configurare il nome del tag dei criteri.

In **WLAN-Policy Maps,** su **+Add,** selezionare **WLAN Profile** e **Policy Profile** dai menu a discesa, quindi selezionare il controllo per la mappa da configurare.



Passaggio 6. Selezionare **Site Tag (Tag sito)** e selezionare **+Add (Aggiungi).** Selezionare la casella **Abilita sito locale** per fare in modo che gli access point funzionino in modalità locale (o lasciarla deselezionata per FlexConnect)**:**

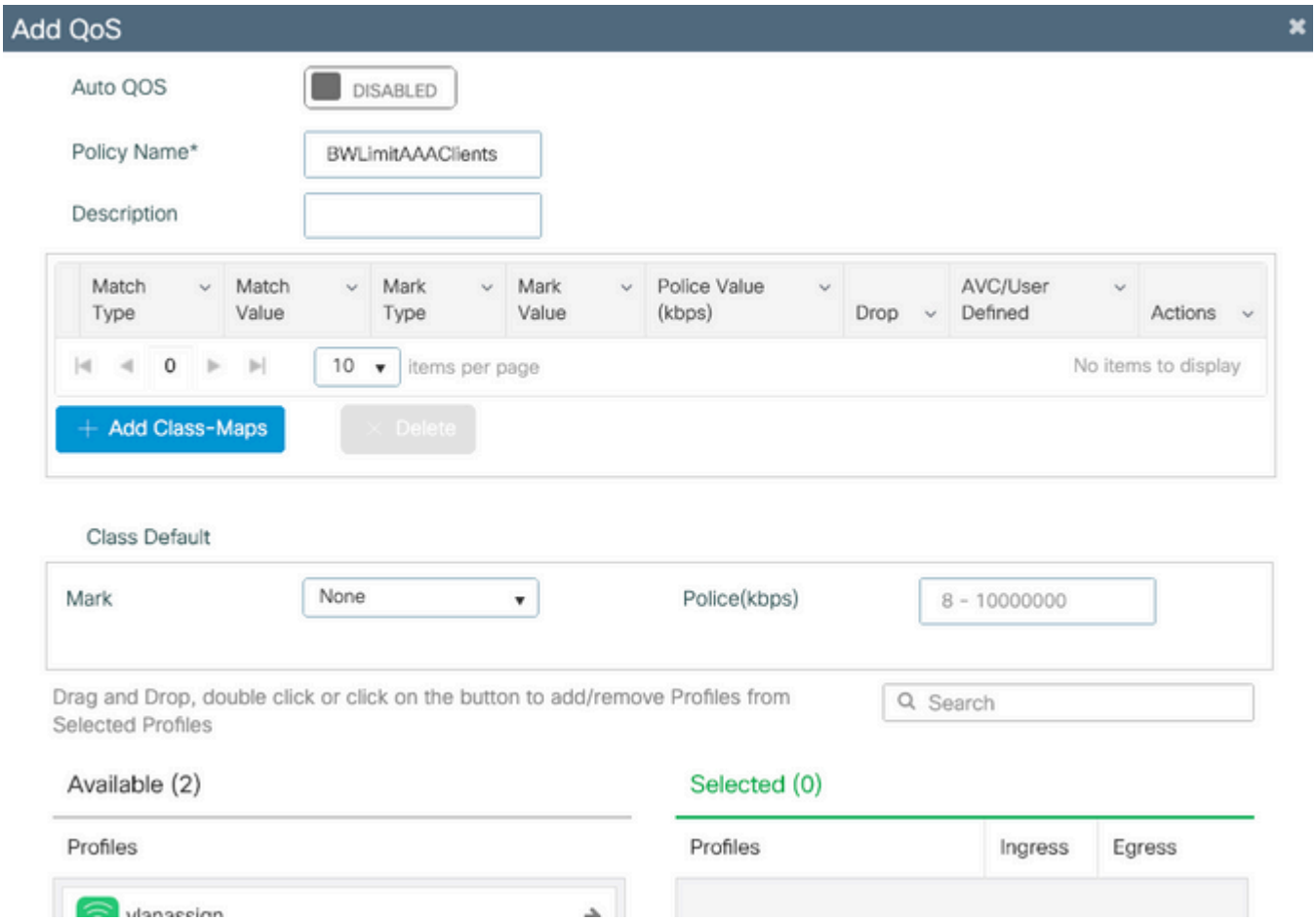


Passaggio 7. Selezionare **Tag AP**, scegliere gli AP e aggiungere il tag Policy, Site e RF:

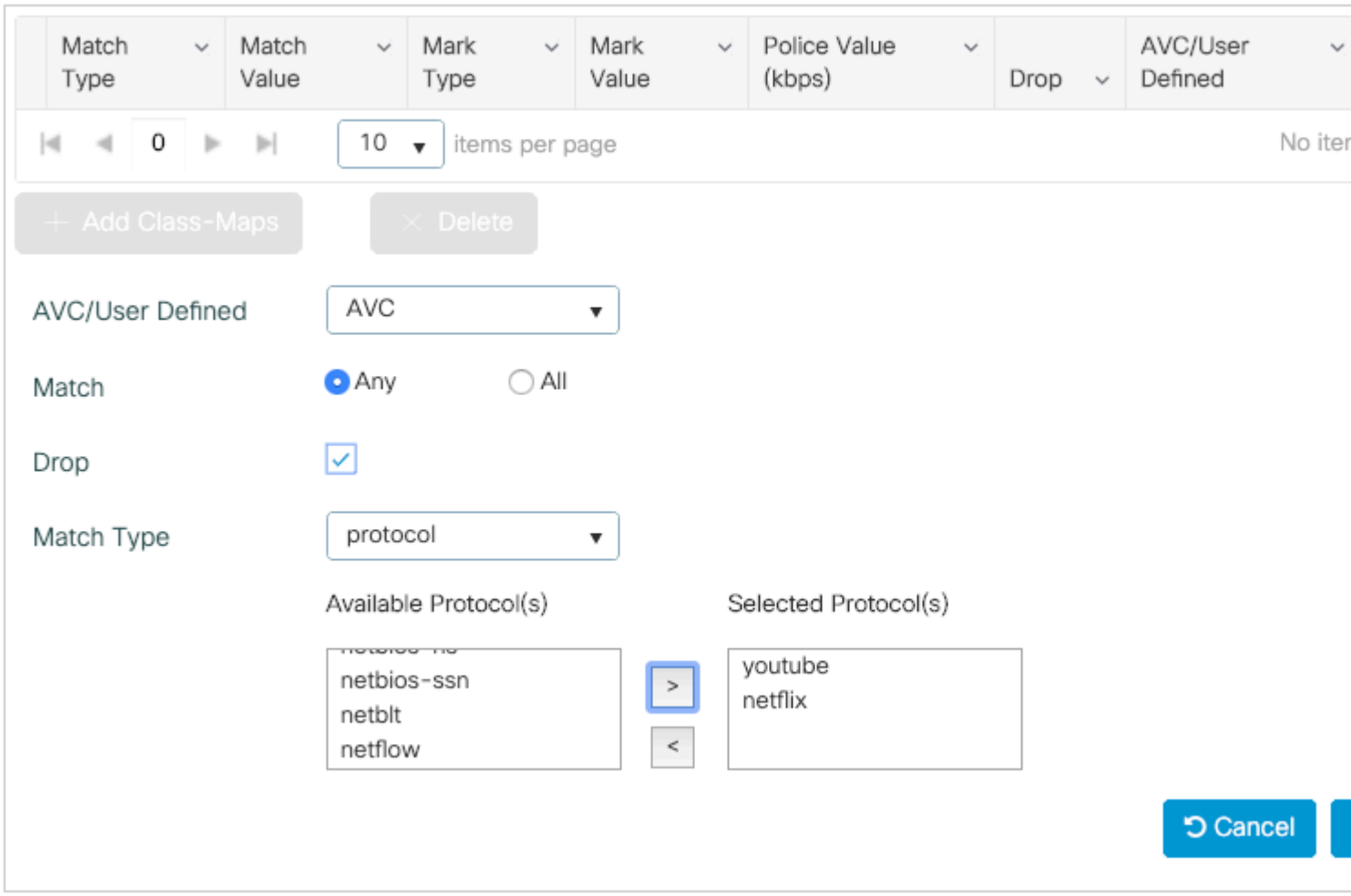
QoS

Passaggio 1. Selezionare **Configurazione > Servizi > QoS** e selezionare **+Aggiungi** per creare un criterio QoS.

Assegnare un nome al client (ad esempio: BWLimitAAClients).



Passaggio 2. Aggiungere una mappa delle classi per eliminare Youtube e Netflix. Fare clic su **Add Class-Maps**. Selezionare **AVC**, match **any**, **drop** action e scegliere entrambi i protocolli.



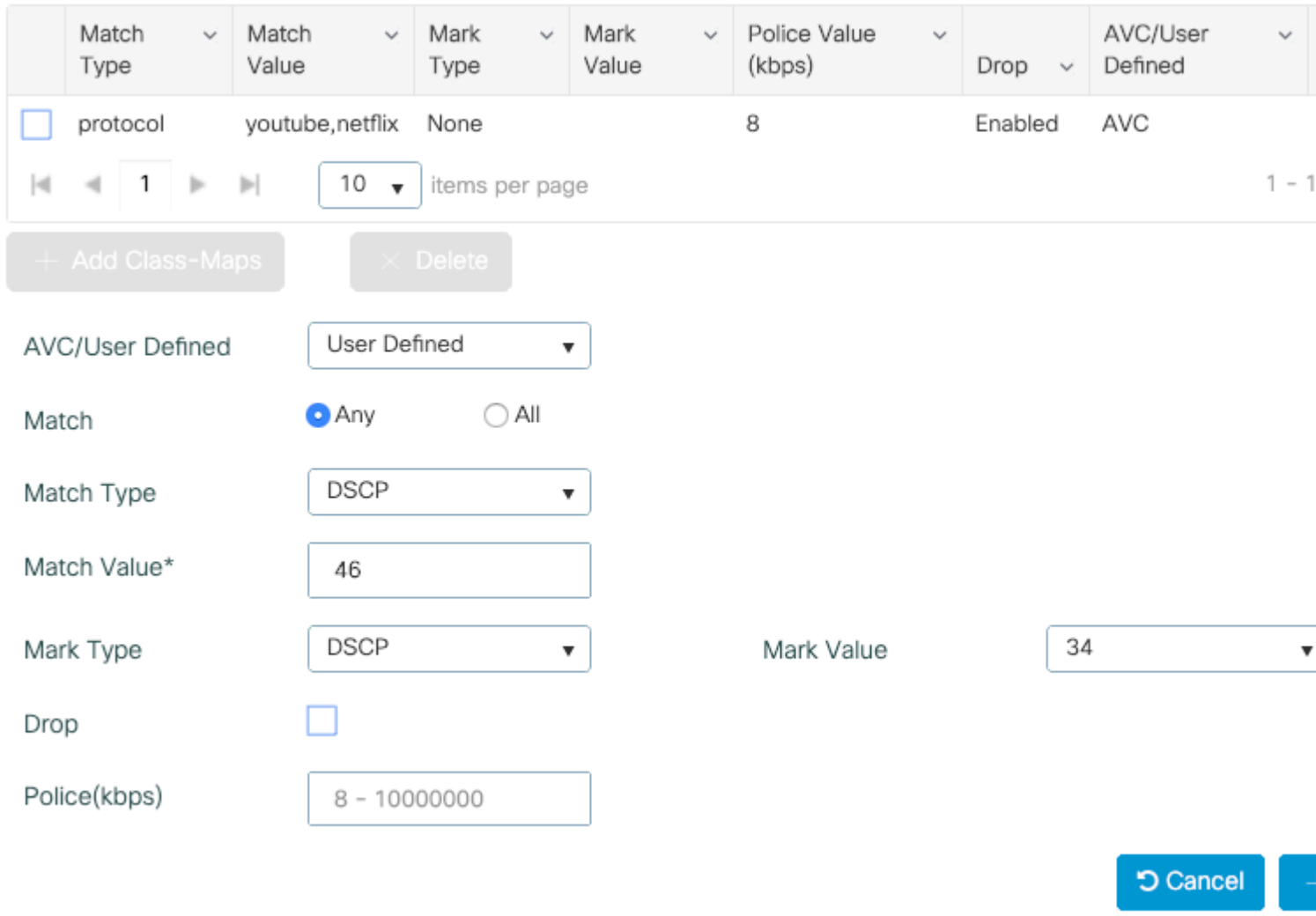
Premere **Salva.**

Passaggio 3. Aggiungere una mappa delle classi con i commenti da DSCP 46 a 34.

Fare clic su **Aggiungi mapping classi**.

- Corrispondenza **qualsiasi, definita dall'utente**
- **DSCP** tipo corrispondente
- Corrispondenza valore **46**
- Tipo contrassegno **DSCP**
- Valore contrassegno **34**

.



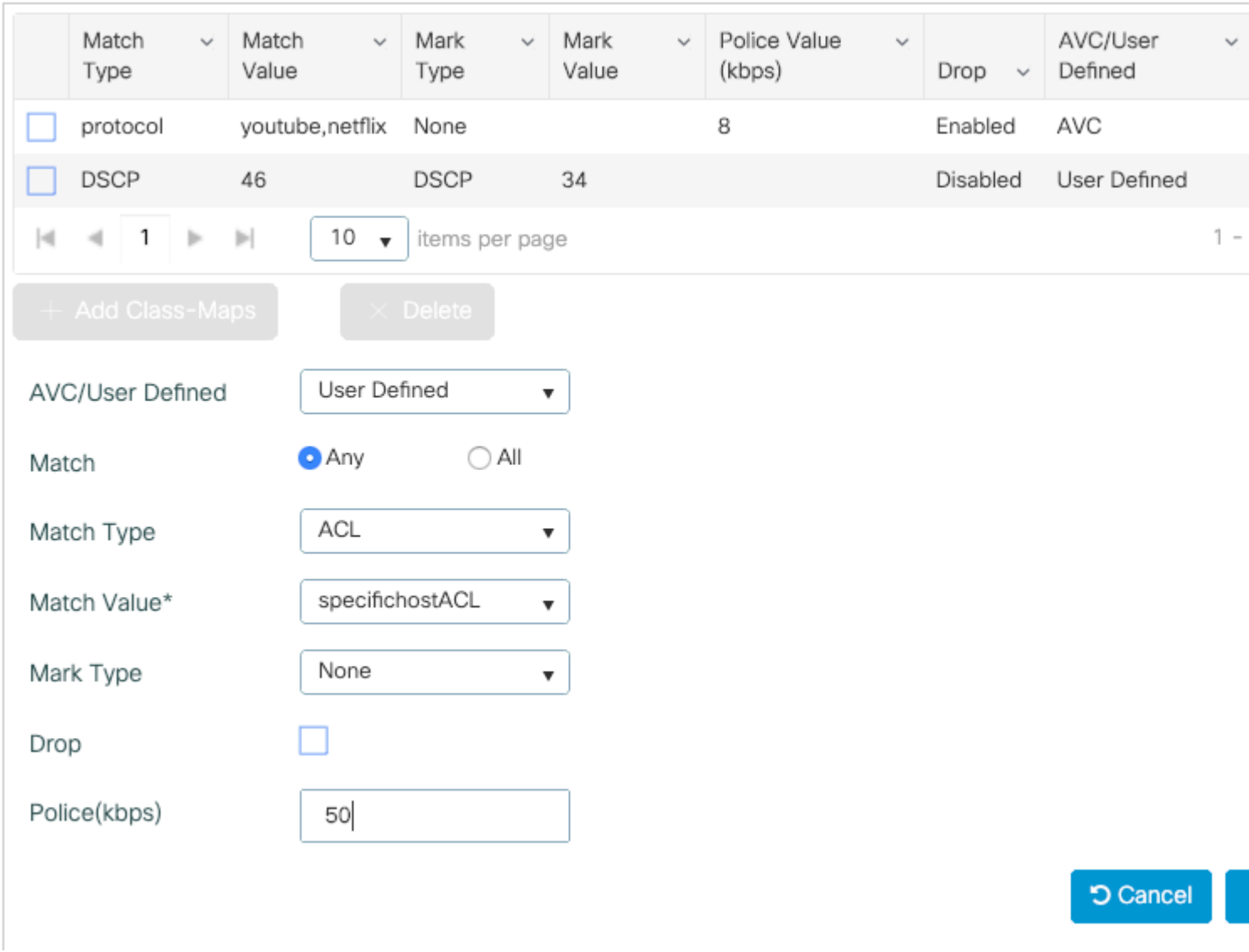
Premere **Salva.**

Passaggio 4. Per definire una mappa di classe che regola il traffico verso un host specifico, creare un ACL per tale host.

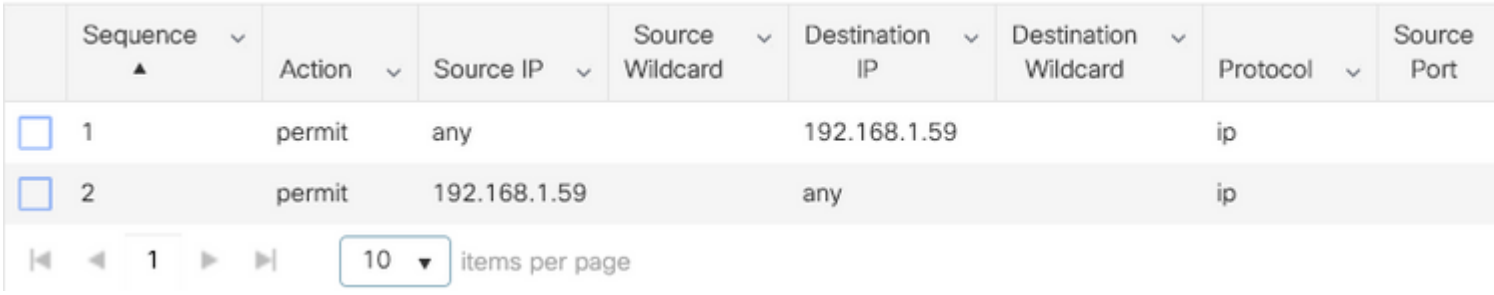
Fare clic su **Add Class-Maps**,

Selezionare Definito dall'utente, Corrispondi a **qualsiasi,** Corrispondi al tipo di **ACL**, scegliere il nome dell'ACL (qui **specifichostACL**), contrassegnare il tipo **none** e scegliere il valore di limite della velocità.

Fare clic su **Salva.**

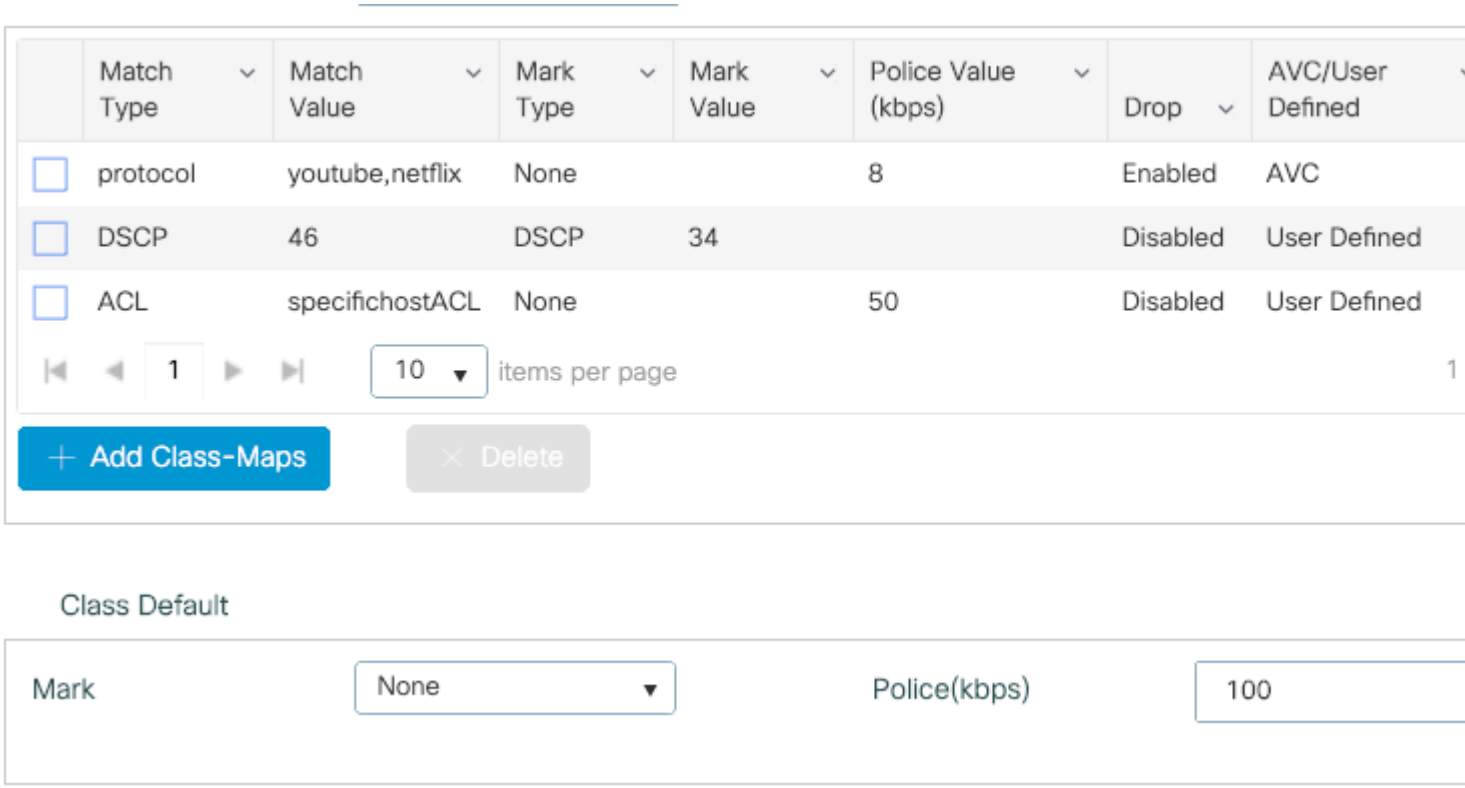


Di seguito è riportato un esempio di ACL che viene usato per identificare un traffico host specifico:



Passaggio 5. Sotto il frame delle mappe di classe, utilizzare la classe predefinita per impostare il limite di velocità per tutto il resto del traffico.

In questo modo viene impostato un limite di velocità per tutto il traffico client non interessato da una delle regole sopra indicate.



Passaggio 6. Fare clic su **Apply to Device (Applica** alla **periferica)** in basso.

Configurazione equivalente da 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
```

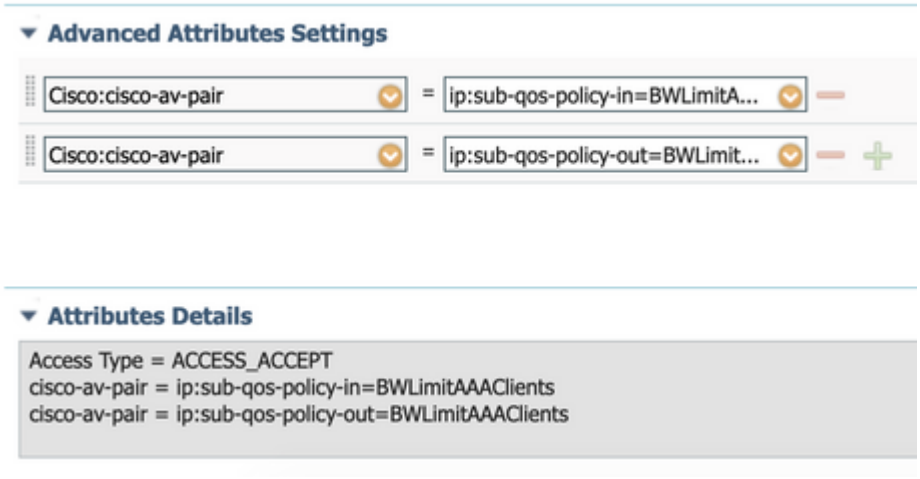
> **Nota**: in questo esempio, non è stato selezionato alcun **profilo** nei criteri QoS, poiché questi vengono applicati dalla sostituzione AAA. Tuttavia, per applicare manualmente il criterio QoS a un profilo criterio, selezionare i profili desiderati.

Passaggio 2. Su ISE, selezionare **Policy > Policy Elements > Results > Authorization Profiles** e selezionare **+Add** per creare un profilo di autorizzazione.

Per applicare il criterio QoS, aggiungerli come **Impostazioni attributi avanzati** tramite le coppie Cisco AV.

Si presume che i criteri di autenticazione e autorizzazione ISE siano configurati in modo da corrispondere alla regola corretta e ottenere questo risultato dell'autorizzazione.

Gli attributi sono **ip:sub-qos-policy-in=<nome criterio>** e **ip:sub-qos-policy-out=<nome criterio>**



> **Nota**: per i nomi dei criteri viene fatta distinzione tra maiuscole e minuscole. Assicurati che il caso sia corretto!

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione:

Sul 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
```

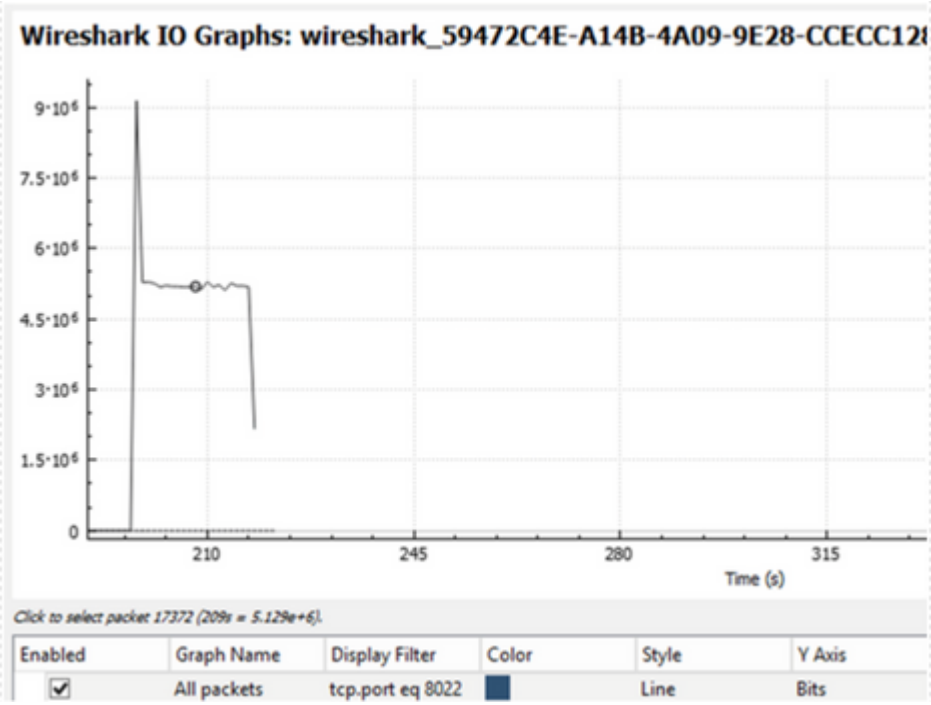
<#root>

```
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
```

Sull'AP

Non è richiesta alcuna risoluzione dei problemi sull'access point quando l'access point è in modalità locale o sull'SSID in modalità di switching centrale Flexconnect, in quanto le policy QoS e dei servizi sono applicate dal WLC.

Il pacchetto acquisisce l'analisi del grafico IO



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Passaggio 1. Cancella tutte le condizioni di debug preesistenti.

```
# clear platform condition all
```

Passaggio 2. Abilitare il debug per il client wireless in questione.

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

Passaggio 3. Collegare il client wireless all'SSID per riprodurre il problema.

Passaggio 4. Interrompere i debug una volta riprodotto il problema.

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

I log acquisiti durante il test vengono archiviati sul WLC in un file locale con il nome:

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Se per generare questa traccia viene utilizzato il flusso di lavoro GUI, il nome file salvato è debugTrace_aaaa.bbbb.cccc.txt.

Passaggio 5. Per raccogliere il file generato in precedenza, copiare il file di traccia ra .log in un server esterno o visualizzare l'output direttamente sullo schermo.

Controllare il nome del file di tracce dell'Autorità registrazione con questo comando:

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

Copiare il file su un server esterno:

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

In alternativa, visualizzare il contenuto:

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

Passaggio 6. Rimuovere le condizioni di debug.

```
# clear platform condition all
```

Scenario di switching locale Flexconnect (o fabric/SDA)

In caso di switching locale flexconnect (o fabric / SDA), è l'AP che applica i criteri QoS definiti sul WLC.

Sugli access point wave2 e 11ax, il limite di velocità si verifica a livello di flusso (5 tuple) e non per client o per SSID prima della 17,6.

Ciò è valido per i punti di accesso nelle implementazioni Flexconnect/Fabric, Embedded Wireless Controller on Access Point (EWc-AP).

A partire dalla versione 17.5, l'override AAA può essere utilizzato per spingere gli attributi e raggiungere il limite di tasso per client.

A partire dalla versione 17.6, il limite di velocità bidirezionale per client è supportato sugli access point 802.11ac Wave 2 e 11ax in configurazione di switching locale Flex.

> **Nota**: i Flex AP non supportano la presenza di ACL nei criteri QoS. Inoltre, non supportano la BRR (larghezza di banda rimanente) e la priorità dei criteri configurabili tramite la CLI ma non disponibili nell'interfaccia utente Web 9800 e non supportate su 9800. L'ID bug Cisco CSCvx81067 tiene traccia

---

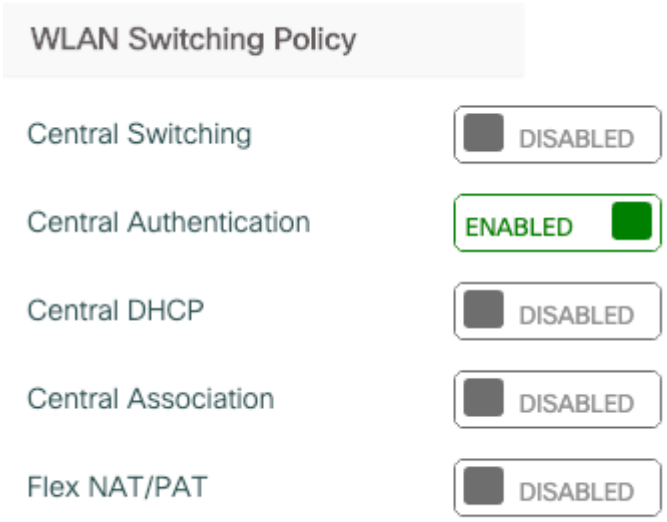
del supporto degli ACL nei criteri QoS per i Flex AP.

Configurazione

La configurazione è esattamente la stessa della prima parte di questo articolo, con due eccezioni:

1. Il profilo dei criteri è impostato su commutazione locale. La distribuzione Flex richiede la disabilitazione dell'associazione centrale fino alla versione Bengaluru 17.4.

A partire dalla versione 17.5, questo campo non è disponibile per la configurazione utente in quanto è hardcoded.



2. Il tag del sito non è impostato come sito locale

Risoluzione dei problemi relativi a Flexconnect/Fabric

Poiché l'access point è il dispositivo che applica i criteri QoS, questi comandi possono aiutare a limitare il campo di applicazione.

show dot11 qos

show policy-map

show rate-limit client

show rate-limit bssid

show rate-limit wlan

mostra client flexconnect

<#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#
```

Riferimenti

[Guida QoS di Catalyst 9000 16.12]

[Guida alla configurazione QoS 9800]

[Catalyst 9800 modello di configurazione]

[Note sulla release di Cisco IOS® XE 17.6]

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).