Policing QoS sugli switch Catalyst serie 6500/6000

Sommario

Introduzione

Il policy QoS su una rete determina se il traffico di rete è all'interno di un profilo specificato (contratto). In questo modo, il traffico fuori profilo potrebbe scendere o essere contrassegnato su un altro valore DSCP (Differentiated Services Code Point) per applicare un livello di servizio contratto. (DSCP è una misura del livello QoS del frame.)

Non confondere il traffic policing con il traffic shaping. Entrambi garantiscono che il traffico rimanga all'interno del profilo (contratto). Quando si controlla il traffico, non è necessario memorizzare i pacchetti fuori profilo. Non influisce pertanto sul ritardo di trasmissione. Il traffico viene interrotto o contrassegnato con un livello QoS inferiore (markdown DSCP). Al contrario, con il traffic shaping, è possibile bloccare il traffico fuori profilo e ridurre i picchi di traffico. Ciò influisce sulla variazione di ritardo e ritardo. È possibile applicare il traffic shaping solo su un'interfaccia in uscita. È possibile applicare il policy sia alle interfacce in entrata che a quelle in uscita.

La Policy Feature Card (PFC) e la PFC2 dello switch Catalyst 6500/6000 supportano solo la funzione Ingress Policing. Il PFC3 supporta sia il controllo in entrata che in uscita. Il traffic shaping è supportato solo su alcuni moduli WAN per gli switch Catalyst serie 6500/7600, ad esempio i moduli OSM (Optical Services Module) e FlexWAN. Per ulteriori informazioni, consultare le note di configurazione del modulo router Cisco serie 7600

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Parametri di Policing QoS

Per impostare il controllo, è necessario definire i controlli e applicarli alle porte (QoS basato su porta) o alle VLAN (QoS basato su VLAN). Ogni policer definisce un nome, un tipo, una frequenza, una frammentazione e le azioni per il traffico all'interno e all'esterno del profilo. I policer sul Supervisor Engine II supportano anche i parametri relativi alle tariffe in eccesso. Esistono due tipi di policer: microflusso e aggregato.

- **Microflusso**: il traffico di polizia per ciascuna porta/VLAN applicata separatamente, in base al flusso.
- **Aggregazione**: il traffico di polizia su tutte le porte/VLAN applicate.

Ciascun policer può essere applicato a più porte o VLAN. Il flusso viene definito utilizzando i seguenti parametri:

- source IP address
- indirizzo IP di destinazione
- Protocollo di layer 4 (ad esempio UDP [User Datagram Protocol])
- numero porta di origine
- numero porta di destinazione

Èpossibile affermare che i pacchetti che corrispondono a un particolare set di parametri definiti appartengono allo stesso flusso. (Questo è essenzialmente lo stesso concetto di flusso utilizzato dalla commutazione NetFlow).

Ad esempio, se si configura un policer di microflusso per limitare il traffico TFTP a 1 Mbps sulla VLAN 1 e sulla VLAN 3, viene autorizzato 1 Mbps per ciascun flusso sulla VLAN 1 e 1 Mbps per ciascun flusso sulla VLAN 3. In altre parole, se ci sono tre flussi sulla VLAN 1 e quattro flussi sulla VLAN 3, il policer di microflusso consente ognuno di questi flussi a 1 Mbps. Se si configura un policer aggregato, il traffico TFTP viene limitato a 1 Mbps per tutti i flussi combinati sulla VLAN 1 e sulla VLAN 3.

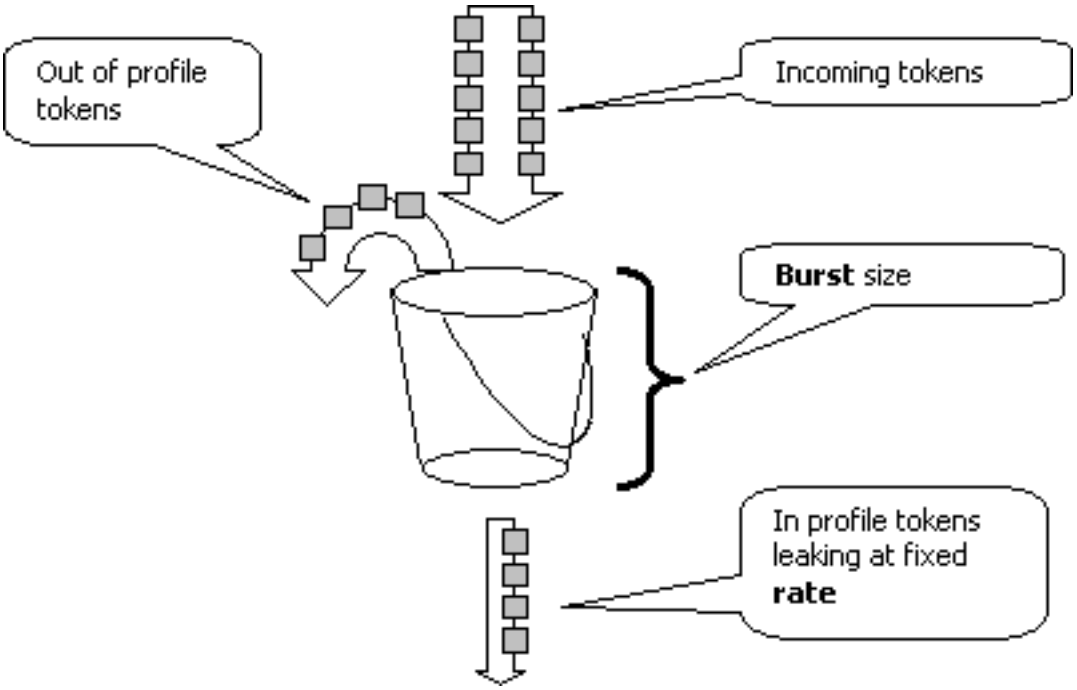
Se si applicano i criteri di aggregazione e di microflusso, QoS esegue sempre l'azione più grave specificata dai criteri. Ad esempio, se un policer specifica di rilasciare il pacchetto, mentre un altro specifica di contrassegnare il pacchetto, il pacchetto viene scartato.

Per impostazione predefinita, i criteri di microflusso funzionano solo con il traffico indirizzato (livello 3 [L3]). Per controllare anche il traffico con bridging (Layer 2 [L2]), è necessario abilitare il monitoraggio del microflusso con bridging. Sul Supervisor Engine II, è necessario abilitare il controllo del microflusso tramite bridging anche per il controllo del microflusso L3.

Il monitoraggio riconosce il protocollo. Tutto il traffico è diviso in tre tipi:

- IP
- IPX (Internetwork Packet Exchange)
- Other (Altro)

Il monitoraggio è implementato sugli switch Catalyst 6500/6000 secondo il concetto di un "bucket di perdite". I token corrispondenti ai pacchetti del traffico in entrata vengono inseriti in un bucket. Ogni token rappresenta un bit, quindi un pacchetto di grandi dimensioni è rappresentato da più token rispetto a un pacchetto di piccole dimensioni. A intervalli regolari, un numero definito di token vengono rimossi dal bucket e inviati durante il loro percorso. Se nel bucket non è presente alcun spazio per i pacchetti in entrata, i pacchetti vengono considerati fuori profilo. Vengono eliminate o contrassegnate in base all'azione di monitoraggio configurata.



Nota: il traffico non viene memorizzato nel buffer, come potrebbe apparire nell'immagine precedente. Il traffico effettivo non attraversa affatto il bucket, il bucket viene utilizzato solo per decidere se il pacchetto è all'interno o all'esterno del profilo.

Calcola parametri

Il funzionamento del bucket di token è controllato da diversi parametri, come mostrato di seguito:

- **Frequenza**: definisce il numero di token da rimuovere a ogni intervallo. Questo imposta di fatto il tasso di sorveglianza. Tutto il traffico al di sotto della velocità è considerato di profilo.
- **Intervallo**: definisce la frequenza con cui i token vengono rimossi dal bucket. L'intervallo è fissato a 0,00025 secondi, quindi i token vengono rimossi dal bucket 4.000 volte al secondo. Impossibile modificare l'intervallo.
- **Burst** - Definisce il numero massimo di token che il bucket può contenere contemporaneamente. Per mantenere la velocità di traffico specificata, la frammentazione non deve essere inferiore alla velocità moltiplicata per l'intervallo. Un'altra considerazione è che il pacchetto di dimensioni massime deve essere contenuto nel bucket.

Per determinare il parametro di frammentazione, utilizzare la seguente equazione:

- Burst = (Velocità [bps]) * 0,00025 [sec/intervallo]) *o* (dimensioni massime del pacchetto [bit]), a seconda di quale è maggiore.

Ad esempio, se si desidera calcolare il valore minimo di burst necessario per sostenere una velocità di 1 Mbps su una rete Ethernet, la velocità viene definita come 1 Mbps e la dimensione massima del pacchetto Ethernet è 1518 byte. L'equazione è:

- Burst = (1.000.000 bps * 0,00025) *o* (1518 byte * 8 bit/byte) = 250 *o* 12144.

Il risultato più grande è 12144, arrotondato a 13 kbps.

Nota: nel software Cisco IOS®, la velocità di policing è definita in bit al secondo (bps), a differenza dei kbps nel sistema operativo Catalyst (CatOS). Anche nel software Cisco IOS, la velocità di burst è definita in byte, a differenza dei kilobit in CatOS.

Nota: a causa della granularità dei criteri hardware, la velocità e la frammentazione esatte vengono arrotondate al valore supportato più vicino. Accertarsi che il valore di burst non sia inferiore al pacchetto di dimensioni massime. In caso contrario, tutti i pacchetti più grandi delle dimensioni della frammentazione vengono scartati.

Ad esempio, se si tenta di impostare la frammentazione su 1518 nel software Cisco IOS, viene arrotondata a 1000. In questo modo, tutti i frame più grandi di 1000 byte vengono scartati. La soluzione è configurare burst su 2000.

Quando si configura la velocità di burst, tenere presente che alcuni protocolli (ad esempio il protocollo TCP) implementano un meccanismo di controllo del flusso che reagisce alla perdita di pacchetti. Ad esempio, il protocollo TCP riduce della metà il tempo di attesa per ciascun pacchetto perso. Di conseguenza, se sottoposto a policy a una determinata frequenza, l'utilizzo effettivo del collegamento è inferiore alla frequenza configurata. È possibile aumentare la frammentazione per ottenere un utilizzo migliore. Un buon inizio per questo tipo di traffico è raddoppiare le dimensioni dello burst. (nell'esempio, le dimensioni della frammentazione vengono aumentate da 13 kbps a 26 kbps). Quindi, monitorare le prestazioni e apportare ulteriori regolazioni se necessario.

Per lo stesso motivo, non è consigliabile eseguire il benchmark dell'operazione del policer utilizzando il traffico orientato alla connessione. Questo generalmente mostra prestazioni inferiori a quelle consentite dal policer.

Azioni della polizia

Come accennato nell'Introduzione, il policer può fare una di due cose per proteggere un pacchetto fuori profilo:

- elimina il pacchetto (il parametro `drop` nella configurazione)
- contrassegnare il pacchetto con un DSCP inferiore (parametro `policed-dscp` nella configurazione)

Per contrassegnare il pacchetto, è necessario modificare la mappa DSCP controllata. Per impostazione predefinita, il DSCP controllato è impostato in modo che il pacchetto venga contrassegnato sullo stesso DSCP (non si verifica alcun contrassegno).

Nota: se i pacchetti "out-of-profile" (fuori profilo) sono contrassegnati per il livello inferiore su un DSCP mappato su una coda di output diversa da quella del DSCP originale, è possibile che alcuni pacchetti vengano inviati fuori ordine. Per questo motivo, se l'ordine dei pacchetti è importante, si consiglia di contrassegnare i pacchetti fuori profilo con un DSCP mappato alla stessa coda di

output dei pacchetti nel profilo.

Sul Supervisor Engine II, che supporta il tasso in eccesso, sono possibili due trigger:

- Quando il traffico supera la velocità normale
- Quando il traffico supera la velocità in eccesso

Un esempio di applicazione delle tariffe in eccesso consiste nel contrassegnare i pacchetti che superano le tariffe normali e nel contrassegnare quelli che superano le tariffe in eccesso.

Funzionalità di monitoraggio supportate da Catalyst 6500/6000

Come accennato nell'introduzione, il PFC1 sul Supervisor Engine 1a e il PFC2 sul Supervisor Engine 2 supportano solo il controllo in entrata (interfaccia in entrata). Il PFC3 sul Supervisor Engine 720 supporta il controllo in entrata e in uscita (interfaccia in uscita).

Catalyst 6500/6000 supporta fino a 63 policer di microflusso e fino a 1023 policer aggregati.

Supervisor Engine 1a supporta il monitoraggio in entrata, a partire dalla versione 5.3(1) di CatOS e dal software Cisco IOS versione 12.0(7)XE.

Nota: per il controllo con Supervisor Engine 1a è necessaria una scheda secondaria PFC o PFC2.

Supervisor Engine 2 supporta le policy in entrata, a partire dalla versione 6.1(1) di CatOS e dal software Cisco IOS versione 12.1(5c)EX. Supervisor Engine II supporta il parametro di controllo della velocità in eccesso.

Le configurazioni con DFC (Distributed Forwarding Card) supportano solo il monitoraggio basato sulle porte. Inoltre, il policer aggregato conta il traffico solo per motore di inoltro, non per sistema. DFC e PFC sono entrambi motori di inoltro; se un modulo (scheda di linea) non dispone di un DFC, utilizza un PFC come motore di inoltro.

Aggiornamento delle funzionalità di monitoraggio per Supervisor Engine 720

Nota: se non si ha dimestichezza con il monitoraggio QoS di Catalyst 6500/6000, leggere le sezioni Parametri e funzionalità di monitoraggio QoS supportate da Catalyst 6500/6000 di questo documento.

Supervisor Engine 720 ha introdotto queste nuove funzionalità di policy QoS:

- **Polizia in uscita**. Supervisor 720 supporta il controllo degli ingressi su una porta o interfaccia VLAN. Supporta il controllo in uscita su una porta o su un'interfaccia con routing L3 (nel caso del software di sistema Cisco IOS). A prescindere dalla modalità QoS della porta (QoS basato sulla porta o QoS basato sulla VLAN), a tutte le porte della VLAN viene applicato un policy all'uscita. Policy di microflusso non supportata in uscita. Configurazioni di esempio sono fornite nella sezione Configurazione e monitoraggio del monitoraggio dei criteri nel software CatOS e nella sezione Configurazione e monitoraggio dei criteri nel software Cisco IOS di questo documento.
- **Policy di microflusso per utente**. Il Supervisor 720 supporta un miglioramento al controllo del

microflusso noto come controllo del microflusso per utente. Questa funzione è supportata solo con il software di sistema Cisco IOS. Consente di fornire una determinata larghezza di banda per ogni utente (per indirizzo IP) dietro determinate interfacce. A tale scopo, è necessario specificare una maschera di flusso all'interno dei criteri del servizio. La maschera di flusso definisce quali informazioni vengono utilizzate per distinguere i flussi. Ad esempio, se si specifica una maschera di flusso di sola origine, tutto il traffico proveniente da un indirizzo IP viene considerato come un unico flusso. Questa tecnica consente di controllare il traffico per utente su alcune interfacce (in cui è stato configurato il criterio di servizio corrispondente); sulle altre interfacce, si continua a usare la maschera di flusso predefinita. È possibile avere fino a due diverse maschere di flusso QoS attive nel sistema in un dato momento. È possibile associare una sola classe a una maschera di flusso. Una regola può avere fino a due diverse maschere di flusso.

Un altro importante cambiamento nel controllo del Supervisor Engine 720 è che può contare il traffico per la lunghezza L2 del frame. Questa opzione è diversa da Supervisor Engine 2 e Supervisor Engine 1, che contano i frame IP e IPX per la lunghezza L3. In alcune applicazioni, la lunghezza L2 e L3 potrebbe non essere coerente. Un esempio è rappresentato da un piccolo pacchetto L3 all'interno di un frame L2 di grandi dimensioni. In questo caso, Supervisor Engine 720 potrebbe visualizzare una velocità del traffico controllata leggermente diversa rispetto a Supervisor Engine 1 e Supervisor Engine 2.

Configurazione e monitoraggio delle policy nel software CatOS

La configurazione della policy per CatOS è costituita da tre passi principali:

1. Definire un policer: la normale velocità di traffico, la velocità in eccesso (se applicabile), la frammentazione e l'azione di policy.
2. Creare un ACL QoS per selezionare il traffico da indirizzare alla polizia e collegare un policer a questo ACL.
3. Applicare l'ACL QoS alle porte o alle VLAN necessarie.

Nell'esempio viene mostrato come bloccare tutto il traffico sulla porta UDP 111 sulla porta 2/8.

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 drop !--- This defines a
policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip
udp_qos_port dscp 0 aggregate udp_1mbps udp any any eq
111 !--- This creates QoS ACL to select traffic and
attaches !--- the policer to the QoS ACL. commit qos acl
all !--- This compiles the QoS ACL. set qos acl map
udp_qos_port 2/8 !--- This maps the QoS ACL to the
switch port.
```

L'esempio successivo è lo stesso. tuttavia, nell'esempio riportato, il policer viene collegato a una VLAN. La porta 2/8 appartiene alla VLAN 20.

Nota: è necessario modificare la porta QoS nella modalità `basata su vlan`. A tale scopo, usare il comando **set port qos**.

Questo policer valuta il traffico da tutte le porte della VLAN configurata per la QoS basata sulla VLAN:

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 drop !--- This defines a
policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip
udp_qos_vlan dscp 0 aggregate udp_1mbps udp any any eq
111 !--- This creates the QoS ACL to select traffic and
attaches !--- the policer to QoS ACL. commit qos acl all
!--- This compiles the QoS ACL. set port qos 2/8 vlan-
based !--- This configures the port for VLAN-based QoS.
set qos acl map udp_qos_vlan 20 !--- This maps QoS ACL
to VLAN 20.
```

Quindi, invece di eliminare i pacchetti fuori profilo con DSCP 32, contrassegnarli con un DSCP di 0 (sforzo massimo).

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 policed-dscp !--- This
defines a policer. For the calculation of rate and
burst, !--- refer to Calculate Parameters. set qos acl
ip udp_qos_md trust-ipprec aggregate udp_1mbps udp any
any eq 111 dscp-field 32 !--- Note: The above command
should be on one line. !--- This creates the QoS ACL to
select traffic and attaches !--- the policer to the QoS
ACL.

commit qos acl all
!--- This compiles the QoS ACL. set qos policed-dscp-map
32:0 !--- This modifies the policed DSCP map to mark
down DSCP 32 to DSCP 0. set port qos 2/8 vlan-based !---
This configures the port for VLAN-based QoS. set qos acl
map udp_qos_md 20 !--- This maps the QoS ACL to VLAN 20.
```

Nell'esempio viene mostrata la configurazione del controllo delle uscite solo per Supervisor Engine 720. Mostra come controllare tutto il traffico IP in uscita sulla VLAN da 3 a 10 Mbps aggregata.

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
egress_10mbps rate 10000 burst 20 drop !--- This defines
a policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip egress_pol
trust-ipprec aggregate egress_10mbps ip any any !---
This creates the QoS ACL to select traffic and attaches
!--- the policer to the QoS ACL. commit qos acl all !---
This compiles the QoS ACL. set qos acl map egress_pol 3
output !--- This maps the QoS ACL to VLAN 3 in the
output direction.
```

Utilizzare **show qos maps runtime policed-dscp-map** per visualizzare la mappa DSCP con criteri corrente.

Usa **show qos policer runtime {*policer_name* | all}** per verificare i parametri del policer. È anche possibile vedere l'ACL QoS a cui è collegato il policer.

Nota: con Supervisor Engine 1 e 1a, non è possibile avere statistiche di controllo per singoli policer aggregati. Per visualizzare le statistiche dei criteri per sistema, utilizzare questo comando:

```
Cat6k> (enable) show qos statistics l3stats
Packets dropped due to policing: 1222086
IP packets with ToS changed: 27424
IP packets with CoS changed: 3220
Non-IP packets with CoS changed: 0
```

Per controllare le statistiche di controllo del microflusso, utilizzare questo comando:

```
Cat6k> (enable) show mls entry qos short
Destination-IP  Source-IP Port  DstPrt SrcPrt Uptime  Age
--------------- --------------- ----- ------ ------ -------- --------

IP bridged entries:
239.77.77.77 192.168.10.200UDP   63 6300:22:02 00:00:00
Stat-Pkts : 165360
Stat-Bytes : 7606560
Excd-Pkts : 492240
Stat-Bkts : 1660
239.3.3.3192.168.11.200UDP  888 77700:05:38 00:00:00
Stat-Pkts : 42372
Stat-Bytes : 1949112
Excd-Pkts : 126128
Stat-Bkts : 1628

Only out of the profile MLS entries are displayed
Cat6k> (enable)
```

Con Supervisor Engine II, è possibile visualizzare le statistiche di controllo aggregate per singolo policer con il comando **show qos statistics aggregate-policer**.

In questo esempio, un generatore di traffico è collegato alla porta 2/8 e invia 17 Mbps di traffico UDP con la porta di destinazione 11. Poiché si prevede che il policer scarichi 16/17 del traffico, 1 Mbps dovrebbe passare attraverso:

```
Cat6k> (enable) show qos statistics aggregate-policer udp_1mbps
QoS aggregate-policer statistics:
Aggregate policerAllowed packet Packets exceed Packets exceed
                count        normal rate       excess rate
------------------------------ -------------- -------------- --------------
udp_1mbps58243997321089732108

Cat6k> (enable) show qos statistics aggregate-policer udp_1mbps
QoS aggregate-policer statistics:
Aggregate policerAllowed packet Packets exceed Packets exceed
                count        normal rate       excess rate
------------------------------ -------------- -------------- --------------
udp_1mbps58250497331989733198
```

Nota: si noti che i pacchetti consentiti sono aumentati di 65 e quelli in eccesso di 1090. Ciò significa che il policer ha scartato 1090 pacchetti e ne ha autorizzati il passaggio a 65. È possibile

calcolare 65 / (1090 + 65) = 0,056, o all'incirca 1/17. Di conseguenza, il policer funziona correttamente.

Configurazione e monitoraggio delle policy nel software Cisco IOS

La configurazione del policing nel software Cisco IOS prevede i seguenti passaggi:

1. Definire un policer.
2. Creare un ACL per selezionare il traffico da sorvegliare.
3. Definire una mappa delle classi per selezionare il traffico con precedenza ACL e/o DSCP/IP.
4. Definire un criterio del servizio che utilizza la classe e applicare il policer a una classe specificata.
5. Applicare i criteri del servizio a una porta o a una VLAN.

Considerare lo stesso esempio fornito nella sezione Configurazione e monitoraggio del controllo del software CatOS, ma ora con il software Cisco IOS. Nell'esempio, un generatore di traffico è collegato alla porta 2/8. Invia 17 Mbps di traffico UDP con la porta di destinazione 11:

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. mls qos aggregate-policer
udp_1mbps 1000000 2000 conform-action transmit exceed-
action drop !--- Note: The above command should be on
one line. !--- This defines a policer. For the
calculation of rate and burst, !--- refer to Calculate
Parameters. !--- Note: The burst is 2000 instead of
1518, due to hardware granularity.

access-list 111 permit udp any any eq 111
!--- This defines the ACL to select traffic. class-map
match-all udp_qos match access-group 111 !--- This
defines the traffic class to police. policy-map
udp_policy class udp_qos police aggregate udp_1mbps !---
This defines the QoS policy that attaches the policer to
the traffic class. interface GigabitEthernet2/8
switchport service-policy input udp_policy !--- This
applies the QoS policy to an interface.
```

Nel software Cisco IOS sono disponibili due tipi di criteri di aggregazione: **denominato** e **per interfaccia**. Il policer aggregato denominato regola il traffico combinato da tutte le interfacce a cui viene applicato. Questo è il tipo utilizzato nell'esempio precedente. Il traffico dei criteri per interfaccia viene impostato separatamente su ogni interfaccia in entrata a cui viene applicato. Nella configurazione della mappa dei criteri è definito un policer per interfaccia. Si consideri questo esempio, in cui è presente un policer di aggregazione per interfaccia:

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 111 permit udp any
any eq 111 !--- This defines the ACL to select traffic.
class-map match-all udp_qos match access-group 111 !---
This defines the traffic class to police. policy-map
udp_policy class udp_qos !--- This defines the QoS
```

```
policy that attaches the policer to the traffic class.
police 1000000 2000 2000 conform-action transmit exceed-
action drop !--- This creates a per-interface aggregate
!--- policer and applies it to the traffic class.
interface GigabitEthernet2/8 switchport service-policy
input udp_policy !--- This applies the QoS policy to an
interface.
```

I criteri di microflusso vengono definiti all'interno della configurazione della mappa dei criteri, così come i criteri aggregati per interfaccia. Nell'esempio seguente, per ogni flusso dall'host 192.168.2.2 alla VLAN 2, viene eseguito il policy a 100 kbps. Tutto il traffico proveniente da 192.168.2.2 viene sorvegliato fino a 500 kbps aggregati. La VLAN 2 include le interfacce fa4/11 e fa4/12:

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 1 permit 192.168.2.2
!--- This defines the access list to select traffic from
host 192.168.2.2. class-map match-all host_2_2 match
access-group 1 !--- This defines the traffic class to
police. policy-map host class host_2_2 !--- This defines
the QoS policy. police flow 100000 2000 conform-action
transmit exceed-action drop !--- This defines a
microflow policer. For the calculation of rate and !---
burst, refer to Calculate Parameters. police 500000 2000
2000 conform-action transmit exceed-action drop !---
This defines the aggregate policer to limit !--- traffic
from the host to 500 kbps aggregate. interface fa4/11
mls qos vlan-based interface fa4/12 mls qos vlan-based
!--- This configures interfaces in VLAN 2 for VLAN-based
QoS. interface vlan 2 service-policy input host !---
This applies the QoS policy to VLAN 2.
```

L'esempio seguente mostra una configurazione per il controllo in uscita per Supervisor Engine 720. Stabilisce il controllo di tutto il traffico in uscita sull'interfaccia Gigabit Ethernet da 8/6 a 100 kbps:

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 111 permit ip any any
!--- This defines the ACL to select traffic. All IP
traffic is subject to policing. class-map match-all
cl_out match access-group 111 !--- This defines the
traffic class to police. policy-map pol_out class cl_out
police 100000 3000 3000 conform-action transmit exceed-
action drop !--- This creates a policer and attaches it
to the traffic class. interface GigabitEthernet8/6 ip
address 3.3.3.3 255.255.255.0 service-policy output
pol_out !--- This attaches the policy to an interface.
```

L'esempio seguente mostra una configurazione per il monitoraggio per utente per Supervisor Engine 720. Il traffico proveniente dagli utenti dietro la porta 1/1 verso Internet viene monitorato a 1 Mbps per utente. Il traffico proveniente da Internet e diretto agli utenti è controllato a 5 Mbps per utente:

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 111 permit ip any any
!--- This defines the ACL to select user traffic. class-
map match-all cl_out match access-group 111 !--- This
defines the traffic class for policing. policy-map
pol_out class cl_out police flow mask src-only 1000000
32000 conform-act transmit exceed-act drop
!--- Only the source IP address is considered for flow
creation !--- on interfaces with this policy attached.
interface gigabit 1/1 !--- 1/1 is the uplink toward the
users. service-policy input pol_out !--- Traffic comes
in from users, so the policy is attached !--- in the
input direction. class-map match-all cl_in match access-
group 111 policy-map pol_in class cl_in police flow mask
dest-only 5000000 32000 conform-act transmit exceed-act
drop
!--- Only the destination IP address is considered for
flow creation !--- on interfaces with this policy
attached. interface gigabit 1/2 !--- 1/2 is the uplink
to the Internet. service-policy input pol_in
```

Per monitorare il controllo, è possibile utilizzare i seguenti comandi:

```
bratan# show mls qos
QoS is enabled globally
Microflow policing is enabled globally
QoS global counters:
Total packets: 10779
IP shortcut packets: 0
Packets dropped by policing: 2110223
IP packets with TOS changed by policing: 0
IP packets with COS changed by policing: 0
Non-IP packets with COS changed by policing: 0

bratan# show mls qos ip gigabitethernet 2/8
[In] Policy map is udp_policy [Out] Default.
QoS Summary [IP]: (* - shared aggregates, Mod - switch module)

Int   Mod Dir Class-map DSCP AgId Trust FlId AgForward-Pk AgPoliced-Pk
--------------------------------------------------------------------------------
Gi2/8 1   In  udp_qos   0    1*   No0 127451  2129602


bratan# show mls qos ip gigabitethernet 2/8
[In] Policy map is udp_policy [Out] Default.
QoS Summary [IP]: (* - shared aggregates, Mod - switch module)

Int   Mod Dir Class-map DSCP AgId Trust FlId AgForward-Pk AgPoliced-Pk
--------------------------------------------------------------------------------
Gi2/8 1   In  udp_qos   0    1*   No0 127755  2134670
```

Nota: i pacchetti consentiti sono aumentati di 304 e quelli in eccesso di 5068. Ciò significa che il policer ha scartato 5068 pacchetti e ne ha autorizzati il passaggio a 304. Data la velocità di input di 17 Mbps, il policer deve superare 1/17 del traffico. Se si confrontano i pacchetti ignorati e inoltrati, si osserverà che è stato così: 304 / (304 + 5068) = 0,057, o all'incirca 1/17. È possibile una qualche piccola variazione a causa della granularità del controllo hardware.

Per le statistiche di controllo del microflusso, utilizzare il comando **show mls ip detail**:

```
Orion# show mls ip detail
IP Destination IP Source        Protocol L4 Ports     Vlan Xtag L3-protocol
--------------+---------------+--------+-------------+----+----+-----------+
192.168.3.33192.168.2.2udp555 / 5550   1ip
192.168.3.3192.168.2.2udp63 / 630   1ip

[IN/OUT] Ports Encapsulation RW-Vlan RW-MACSourceRW-MACDestinationBytes
--------------+-------------+-------+--------------+-----------------+------------+
Fa4/11 - ----ARPA3    0030.7137.1000  0000.3333.3333314548
Fa4/11 - ----ARPA3    0030.7137.1000  0000.2222.2222314824

Packets     Age   Last SeenQoS      Police Count ThresholdLeak
------------+-----+---------+-----------+------------+---------+-----------+
6838     36   18:50:090x80  34619762*2^5 3*2^0
6844     36   18:50:090x80  34669562*2^5 3*2^0

Drop Bucket  Use-Tbl Use-Enable
----+-------+-------+----------+
YES   1968     NONO
YES   1937     NONO
```

Nota: il campo `Conteggio poliziotti` mostra il numero di pacchetti controllati per flusso.

Informazioni correlate

- Configurazione di QoS
- Qualità del servizio sugli switch Catalyst serie 6000
- Supporto dei prodotti LAN
- Supporto della tecnologia di switching LAN
- Documentazione e supporto tecnico – Cisco Systems