Informazioni sul Policing e il contrassegno QoS su Catalyst 3550

Sommario

Introduzione

La funzione di controllo determina se il livello di traffico rientra nel profilo o nel contratto specificato e consente di eliminare il traffico esterno al profilo o di contrassegnarlo con un valore DSCP (Differential Services Code Point) diverso. In questo modo viene applicato un livello di servizio contratto.

DSCP è una misura del livello QoS (Quality of Service) del pacchetto. Oltre al DSCP, vengono usate anche la precedenza IP e la classe di servizio (CoS) per trasmettere il livello QoS del pacchetto.

La sorveglianza non deve essere confusa con il traffic shaping, anche se entrambi assicurano che il traffico rimanga all'interno del profilo o del contratto.

Il policing non effettua il buffer del traffico, quindi non influisce sul ritardo di trasmissione. Anziché archiviare pacchetti fuori profilo, il policing li scarta o li contrassegna con livelli QoS diversi (markdown DSCP).

Il traffic shaping memorizza il traffico fuori profilo e attenua i picchi di traffico, ma influisce sulla variazione di ritardo e ritardo. La forma può essere applicata solo all'interfaccia in uscita, mentre il controllo può essere applicato sia all'interfaccia in entrata che a quella in uscita.

Catalyst 3550 supporta il policing sia per le direzioni in entrata che in uscita. Traffic shaping non supportato.

Il contrassegno modifica il livello QoS del pacchetto in base a un criterio.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

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.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Versioni hardware e software

Il Policing e il contrassegno su Catalyst 3550 sono supportati su tutte le versioni del software. La guida alla configurazione più recente è elencata qui. Fare riferimento a questa documentazione per tutte le funzionalità supportate.

- Configurazione di QoS

Parametri di monitoraggio e contrassegno QoS

Per impostare il policy, è necessario definire le mappe dei criteri QoS e applicarle alle porte. Questo processo è noto anche come QoS basato su porta.

Nota: QoS basato su VLAN non supportato da Catalyst 3550.

Il policer è definito dai parametri di velocità e burst, nonché dall'azione per il traffico fuori profilo.

Sono supportati i due tipi di policer seguenti:

- Aggregazione
- Individuale

Il policer aggregato agisce sul traffico tra tutte le istanze in cui è applicato. Il singolo policer agisce separatamente sul traffico attraverso ogni istanza in cui viene applicato.

Nota: sullo switch Catalyst 3550, il policer aggregato può essere applicato solo a classi diverse dello stesso criterio. Il policing aggregato tra più interfacce o criteri non è supportato.

Ad esempio, applicare il policer aggregato per limitare a 1 Mbps il traffico delle classi customer1 e

customer2 nella stessa mappa dei criteri. Tale policer consente 1 Mbps di traffico nella classe customer1 e customer2 insieme. Se si applica il singolo policer, il policer limita il traffico per la classe customer1 a 1 Mbps e per la classe customer2 a 1 Mbps. Pertanto, ogni istanza del policer è separata.

Nella tabella viene riepilogata l'azione QoS sul pacchetto quando viene gestita dalle policy in entrata e in uscita:

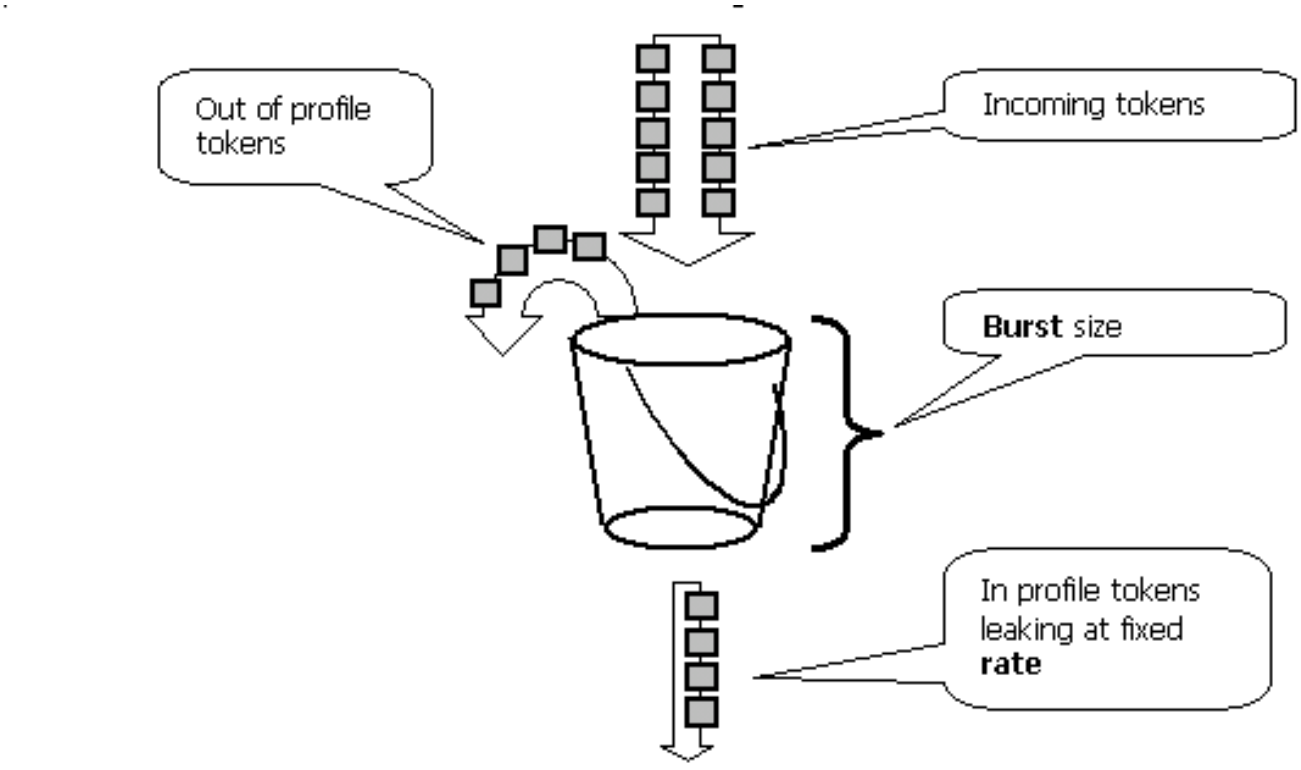
	Ingress policy			
Egress policy	**Transmit**	**Drop**	**Markdown$_i$**	**Mark$_i$**
Transmit	Transmit	Drop	Markdown$_i$	Mark$_i$
Drop	Drop	Drop	Drop	Drop
Markdown$_e$	Markdown$_e$	Drop	Markdown$_i$ then Markdown$_e$	Mark$_i$ then Markdown$_e$

Nota: è possibile contrassegnare e contrassegnare all'interno della stessa classe di traffico della stessa policy. In questo caso, tutto il traffico per la classe specifica viene contrassegnato per primo. Le policy e il markdown si verificano sul traffico già contrassegnato.

Il controllo QoS di Catalyst 3550 è conforme a questo concetto di bucket di perdite:

Il numero di token proporzionali alle dimensioni del pacchetto del traffico in entrata vengono inseriti in un token bucket; il numero di token è uguale alle dimensioni del pacchetto. A intervalli regolari, un numero definito di token derivati dalla velocità configurata viene rimosso dal bucket. Se nel bucket non è presente alcun spazio per ospitare un pacchetto in arrivo, il pacchetto viene considerato fuori profilo e viene scartato o contrassegnato in base all'azione di policy configurata.

Questo concetto viene illustrato nell'esempio seguente:



Nota: il traffico non viene memorizzato nel buffer nel periodo fisso come può apparire in questo esempio. il traffico effettivo non passa affatto attraverso il periodo fisso; il periodo fisso viene usato solo per decidere se il pacchetto è nel profilo o fuori dal profilo.

Nota: l'implementazione hardware della policy può variare, ma dal punto di vista funzionale è ancora conforme a questo modello.

Questi parametri controllano il funzionamento del policing:

- **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 nel profilo. Le velocità supportate vanno da 8 Kbps a 2 Gbps e aumentano di 8 Kbps.
- **Intervallo**: definisce la frequenza con cui i token vengono rimossi dal bucket. L'intervallo è fissato a 0,125 millisecondi (o 8000 volte al secondo). Impossibile modificare l'intervallo.
- **Burst**: definisce la quantità massima di token che il bucket può contenere in qualsiasi momento. I burst supportati vanno da 8000 byte a 2000000 byte e aumentano di 64 byte.

Nota: sebbene le stringhe della Guida della riga di comando mostrino un ampio intervallo di valori, l'opzione rate-bps non può superare la velocità della porta configurata e l'opzione burst-byte non può superare i 2000000 byte. Se si immette un valore maggiore, lo switch rifiuta la mappa dei criteri quando viene collegata a un'interfaccia.

Per mantenere la velocità di traffico specificata, la frammentazione non deve essere inferiore alla somma di questa equazione:

```
Burstmin (bits) = Rate (bps) / 8000 (1/sec)
```

Ad esempio, calcolare il valore di burst minimo per mantenere una velocità di 1 Mbps. La velocità è definita come 1000 Kbps, quindi la frammentazione minima necessaria è la somma di questa equazione:

```
1000 (Kbps) / 8000 (1/sec) =125 (bits)
```

La dimensione minima della frammentazione supportata è di 8000 byte, un valore superiore alla frammentazione minima calcolata.

Nota: a causa della granularità dei criteri hardware, la velocità e la frammentazione esatte vengono arrotondate al valore supportato più vicino.

Quando si configura la velocità di burst, è necessario tenere presente che alcuni protocolli implementano meccanismi che reagiscono alla perdita di pacchetti. Ad esempio, il protocollo TCP (Transmission Control Protocol) riduce della metà la finestra di ogni pacchetto perso. Questo causa un effetto "saw tooth" nel traffico TCP quando il protocollo TCP tenta di accelerare alla velocità della linea e viene limitato dal policer. Se si calcola la velocità media del traffico a dente di sega, questa velocità è molto più bassa di quella controllata. Tuttavia, è possibile aumentare la frammentazione per ottenere un utilizzo migliore. Si consiglia di impostare la frammentazione su un valore pari al doppio della quantità di traffico inviata con la velocità desiderata durante il tempo di andata e ritorno (TCP RTT). Se RTT non è noto, è possibile raddoppiare il valore del parametro burst.

Per lo stesso motivo, non è consigliabile eseguire il benchmark del funzionamento del policer in base al traffico orientato alla connessione. In questo scenario vengono generalmente visualizzate prestazioni inferiori a quelle consentite dal policer.

Il traffico senza connessione può anche reagire in modo diverso alle policy. Ad esempio, il Network File System (NFS) utilizza blocchi che possono essere costituiti da più pacchetti UDP (User Datagram Protocol). Un pacchetto scartato può causare la ritrasmissione di molti pacchetti,

persino dell'intero blocco.

In questo esempio viene calcolata la frammentazione per una sessione TCP con una velocità di controllo di 64 Kbps e, considerato che il valore di TCP/RTT è 0,05 secondi:

```
<burst> = 2*  *  = 2 * 0.05 [sec] * 64000/8 [bytes/sec] = 800    [bytes]
```

Nell'esempio, `<burst>` è per una sessione TCP. Ridimensionare questa cifra per calcolare la media del numero previsto di sessioni che attraversano il policer.

Nota: questo è solo un esempio e in ogni caso è necessario valutare i requisiti e il comportamento del traffico e delle applicazioni rispetto alle risorse disponibili per scegliere i parametri di policy.

L'azione di controllo può consistere nell'eliminare il pacchetto o nel modificare il DSCP del pacchetto (markdown). Per marcare il pacchetto, è necessario modificare una mappa DSCP con criteri. Una mappa DSCP predefinita con criteri contrassegna il pacchetto sullo stesso DSCP. Pertanto, non si verifica alcun markdown.

I pacchetti possono essere inviati fuori ordine quando un pacchetto fuori profilo viene contrassegnato per il livello inferiore in un DSCP mappato in una coda di output diversa da quella del DSCP originale. Se l'ordine dei pacchetti è importante, contrassegnare i pacchetti fuori profilo con il DSCP mappato alla stessa coda di output dei pacchetti nel profilo.

Funzioni di monitoraggio e contrassegno supportate da Catalyst 3550

Questa tabella fornisce un riepilogo delle funzionalità di monitoraggio e contrassegno supportate dallo switch Catalyst 3550, suddivise per direzione:

	Direction	
Feature	Ingress	Egress
Individual policers	Yes, totally 128 for GE and 8 for FE including ingress aggregate policers	Yes, totally 8 including egress aggregate policers
Aggregate policers	Yes, totally 128 for GE and 8 for FE including ingress individual policers	Yes, totally 8 including egress individual policers
Marking	Yes	No
Policer Markdown	Yes	Yes
Match with ACL	Yes	**No**
Match DSCP	Yes	**Yes**
Match IP precedence	Yes	No
Match COS	Yes, for non-IP traffic	No
Trust DSCP	Yes	No
Trust COS	Yes	No
Trust IP precedence	Yes	No

Èsupportata un'istruzione match per mappa di classe. Di seguito sono riportate le istruzioni di corrispondenza valide per i criteri in ingresso:

- match access-group
- corrispondenza ip dscp
- corrispondenza ip precedence

Nota: sullo switch Catalyst 3550, il comando **match interface** non è supportato e in una class-map è consentito un solo comando match. Pertanto, è difficile classificare tutto il traffico che arriva attraverso un'interfaccia e sorvegliare tutto il traffico con un solo policer. Vedere Come classificare tutto il traffico di interfaccia con un singolo policer in questo documento.

Questa è l'istruzione match valida per il criterio di uscita:

- corrispondenza ip dscp

Di seguito sono riportate le azioni valide per i criteri in ingresso:

- polizia
- set ip dscp (contrassegno)
- imposta precedenza ip (contrassegno)
- trust dscp
- trust ip-precedence
- cc trust

Nella tabella seguente viene illustrata la matrice dei criteri QoS in entrata supportati:

Trust I/F	Match DSCP[1]	Match ACL	Trust Class[2]	Set DSCP[3]	Police	Result
						Traffic is assigned default QOS level of the port (0 by default)
√						QOS level of incoming traffic is preserved, according to what is trusted
	√		√		√	IP Traffic is matched by DSCP and then trusted then policed, excess traffic dropped or marked down
	√		√			IP Traffic is matched by DSCP/IP precedence and its QOS level is preserved
	√			√		IP Traffic is matched by DSCP/IP precedence then marked
	√			√	√	IP Traffic is matched by DSCP/IP precedence then marked then policed
		√	√		√	Traffic is matched by access list, QOS level of the matched traffic is preserved, then traffic is policed
		√	√			Traffic is matched by access list and its QOS level is preserved according to what is trusted
		√		√	√	Traffic is matched by access list then marked and then policed
		√		√		Traffic is matched by ACL then marked with specified DSCP/IP precedence
		MAC ACL w/COS	√			Match non-IP traffic by MAC EtherType and COS and preserve QOS level
		MAC ACL w/COS	√		√	Match non-IP IP traffic by MAC EtherType and COS and preserve QOS level then police
		MAC ACL w/COS		√		Match non-IP IP traffic by MAC EtherType and COS then mark matched traffic
		MAC ACL W/COS		√	√	Match non-IP IP traffic by MAC EtherType and COS then mark and then police

1. Questa opzione copre anche la precedenza IP della corrispondenza.
2. Questa opzione riguarda l'attendibilità di CoS, IP precedence e DSCP.
3. Questa opzione consente inoltre di impostare la precedenza IP.

Azione criterio valida per il criterio di uscita:

- polizia

Nella tabella viene mostrata la matrice dei criteri QoS in uscita supportati:

Match DSCP	Police	Result
		Traffic is sent out with COS and IP precedence according to QOS maps and internal DSCP after ingress QOS processing
√	√	Traffic is matched by DSCP and policed

Il contrassegno permette di modificare il livello QoS del pacchetto in base alla classificazione o all'applicazione di policy. La classificazione suddivide il traffico in diverse classi per l'elaborazione QoS in base ai criteri definiti.

L'elaborazione QoS si basa sul DSCP interno; misura del livello QoS del pacchetto. Il DSCP interno viene derivato in base alla configurazione di trust. Il sistema supporta l'attendibilità di CoS, DSCP, IP precedence e interfacce non attendibili. Trust specifica il campo da cui deriva il DSCP interno per ogni pacchetto, nel modo seguente:

- Quando si considera attendibile il CoS, il livello QoS viene derivato dall'intestazione Layer 2 (L2) dell'ISL (Inter-Switch Link Protocol) o dal pacchetto incapsulato 802.1Q.
- Quando si considera attendibile la precedenza DSCP o IP, il sistema deriva il livello QoS dal campo DSCP o IP precedence del pacchetto di conseguenza.

Affidare il CoS ha senso solo sulle interfacce trunking e affidarsi al DSCP (o IP precedence) ha senso solo per i pacchetti IP.

Quando un'interfaccia non è considerata attendibile, il DSCP interno viene derivato dal CoS predefinito configurabile per l'interfaccia corrispondente. Questo è lo stato predefinito quando QoS è abilitato. Se non è configurato alcun CoS predefinito, il valore predefinito è zero.

Una volta determinato, il DSCP interno può essere modificato mediante contrassegno e applicazione di policy oppure conservato.

Dopo che il pacchetto è stato sottoposto a elaborazione QoS, i relativi campi del livello QoS (all'interno del campo IP/DSCP per IP e all'interno dell'intestazione ISL/802.1Q, se presente) vengono aggiornati dal DSCP interno. Ci sono queste mappe QoS speciali che hanno a che fare con la polizia:

- **DSCP-to-Policed DSCP**: utilizzato per derivare il DSCP sottoposto a policy quando si esegue il markdown del pacchetto.
- **DSCP-to-CoS**: utilizzato per derivare il livello CoS dal DSCP interno e aggiornare l'intestazione ISL/802.1Q del pacchetto in uscita.
- **CoS-to-DSCP**: utilizzato per derivare il DSCP interno dal CoS in ingresso (intestazione ISL/802.1Q) quando l'interfaccia è in modalità CoS trust.

Ecco alcune importanti considerazioni specifiche dell'implementazione:

- I criteri del servizio in entrata non possono essere associati all'interfaccia quando questa è configurata per considerare attendibili le metriche QoS, ad esempio CoS/DSCP o IP Precence. Per ottenere una corrispondenza con la precedenza DSCP/IP e con la polizia in entrata, è necessario configurare l'attendibilità per la classe specifica all'interno del criterio e non sull'interfaccia. Per contrassegnare in base alla precedenza DSCP/IP, non è necessario configurare alcun trust.

- Solo il traffico IPv4 senza opzioni IP e l'incapsulamento Ethernet II Advanced Research Projects Agency (ARPA) sono considerati traffico IP dal punto di vista hardware e QoS. Tutto il resto del traffico viene considerato non IP, incluso IP con opzioni quali IP incapsulato SNAP (Sub Network Access Protocol) e IPv6.
- Per i pacchetti non IP, l'unico metodo di classificazione è "match access group", in quanto non è possibile stabilire una corrispondenza con DSCP per il traffico non IP. A tal fine viene utilizzato un elenco degli accessi (ACL) per il controllo degli accessi ai supporti (MAC); è possibile creare una corrispondenza tra i pacchetti in base all'indirizzo MAC di origine, all'indirizzo MAC di destinazione e a EtherType. Non è possibile far corrispondere il traffico IP con l'ACL MAC, poiché lo switch fa una distinzione tra traffico IP e non IP.

Configurazione e monitoraggio del monitoraggio dei criteri

Questi passaggi sono necessari per configurare il monitoraggio in Cisco IOS:

1. Definire un policer (per i policer aggregati)
2. Definire i criteri per selezionare il traffico per il policing
3. Definire una mappa di classe per selezionare il traffico utilizzando criteri definiti
4. Definire un criterio di servizio utilizzando una classe e applicando un policer alla classe specificata
5. Applicare una policy sui servizi a una porta

Sono supportati i due tipi di policer seguenti:

- Aggregazione denominata
- Individuale

Il policer aggregato denominato regola il traffico combinato da tutte le classi all'interno dello stesso criterio alla posizione in cui viene applicato. Il policing aggregato tra diverse interfacce non è supportato.

Nota: il policer aggregato non può essere applicato a più di un criterio. In caso affermativo, viene visualizzato questo messaggio di errore:

```
QoS: Cannot allocate policer for policy map <policy name>
```

Considerate questo esempio:

Alla porta Gigabit Ethernet0/3 è collegato un generatore di traffico che invia circa 17 Mbps di traffico UDP con la porta di destinazione 111. È inoltre presente il traffico TCP dalla porta 20. Si desidera che questi due flussi di traffico vengano controllati fino a 1 Mbps e che il traffico eccessivo venga interrotto. Nell'esempio viene mostrato come eseguire questa operazione:

```
!--- Globally enables QoS. mls qos !--- Defines the QoS policer, sets the burst !--- to 16000
for better TCP performance. mls qos aggregate-policer pol_1mbps 1000000 16000 exceed-action drop
!--- Defines the ACLs to select traffic. access-list 123 permit udp any any eq 111
access-list 145 permit tcp any eq 20 any
!--- Defines the traffic classes to be policed. class-map match-all cl_udp111 match access-group
123
class-map match-all cl_tcp20
  match access-group 145
```

```
!--- Defines the QoS policy, and attaches !--- the policer to the traffic classes. policy-map
po_test
  class cl_udp111
    police aggregate pol_1mbps
  class cl_tcp20
    police aggregate pol_1mbps
!--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport switchport
access vlan 2 service-policy input po_test
!
```

Nel primo esempio viene utilizzato il policer aggregato denominato. Il singolo policer, a differenza del policer indicato, regola il traffico separatamente su ciascuna classe in cui viene applicato. Il singolo policer viene definito nella configurazione della mappa dei criteri. Nell'esempio, due classi di traffico sono sorvegliate da due singoli agenti di polizia; cl_udp111 viene controllato a 1 Mbps per ogni burst da 8 K e cl_tcp20 a 512 Kbps per ogni burst da 32 K:

```
!--- Globally enables QoS. mls qos !--- Defines the ACLs to select traffic. access-list 123
permit udp any any eq 111
access-list 145 permit tcp any eq 20 any
!--- Defines the traffic classes to be policed. class-map match-all cl_udp111
  match access-group 123
class-map match-all cl_tcp20
  match access-group 145
!--- Defines QoS policy, and creates and attaches !--- the policers to the traffic classes.
policy-map po_test2
  class cl_udp111
    police 1000000 8000 exceed-action drop
  class cl_tcp20
    police 512000 32000 exceed-action drop
!--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport switchport
access vlan 2 service-policy input po_test2
```

Questo comando è usato per monitorare l'operazione di applicazione del policy:

```
cat3550#show mls qos interface g0/3 statistics
GigabitEthernet0/3
Ingress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
Others: 267718     0          267717     0          0
Egress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
Others: 590877        n/a        n/a      266303     0

WRED drop counts:
  qid  thresh1    thresh2   FreeQ
   1 : 0          0         1024
   2 : 0          0         1024
   3 : 0          0         8
   4 : 0          0         1024
```

Nota: per impostazione predefinita non sono disponibili statistiche per DSCP. Catalyst 3550 supporta una raccolta di statistiche per interfaccia e per direzione per un massimo di otto valori DSCP diversi. Questa opzione viene configurata quando si esegue il comando **mls qos monitor**. Per monitorare le statistiche per i DSCP 8, 16, 24 e 32, è necessario usare questo comando **per interfaccia**:

```
cat3550(config-if)#mls qos monitor dscp 8 16 24 32
```

Nota: il comando **mls qos monitor dscp 8 16 24 32** modifica l'output del comando **show mls qos int g0/3 statistics** in questo modo:

```
cat3550#show mls qos interface g0/3 statistics
GigabitEthernet0/3
Ingress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
    8 : 0          0          675053785  0          0
    16: 1811748    0          0          0          0         ? per DSCP statistics
    24: 1227820404 15241073   0          0          0
    32: 0          0          539337294  0          0
Others: 1658208    0          1658208    0          0
Egress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
    8 : 675425886     n/a        n/a       0          0
    16: 0             n/a        n/a       0          0         ? per DSCP statistics
    24: 15239542      n/a        n/a       0          0
    32: 539289117     n/a        n/a       536486430  0
Others: 1983055       n/a        n/a       1649446    0

WRED drop counts:
  qid  thresh1    thresh2   FreeQ
   1 : 0          0         1024
   2 : 0          0         1024
   3 : 0          0         6
   4 : 0          0         1024
```

Questa è una descrizione dei campi nell'esempio:

- **In entrata**: visualizza il numero di pacchetti in arrivo da ciascuna direzione.
- **NO_change**: visualizza il numero di pacchetti considerati attendibili (ad esempio, il livello QoS non modificato).
- **Classificato**: visualizza il numero di pacchetti assegnati al DSCP interno dopo la classificazione.
- **Policed**—mostra quanti pacchetti sono stati contrassegnati dal policing; DSCP visualizzato prima del markdown.
- **Ignorato**: visualizza il numero di pacchetti ignorati dal policing

Tenere presenti le seguenti considerazioni specifiche dell'implementazione:

- Se quando si usa il comando **mls qos monitor** sono configurati otto valori DSCP, il contatore degli altri valori rilevato quando si usa il comando **show mls qos int statistics** potrebbe visualizzare informazioni inadeguate.
- Non è disponibile alcun comando specifico per verificare la velocità del traffico offerto o in uscita per policer.
- Poiché i contatori vengono recuperati dall'hardware in sequenza, è possibile che la loro somma non sia corretta. Ad esempio, la quantità di pacchetti controllati, classificati o scartati può essere leggermente diversa dal numero di pacchetti in arrivo.

Configurazione e monitoraggio del contrassegno

Questi passaggi sono necessari per configurare il contrassegno:

1. Definire i criteri per la classificazione del traffico
2. Definire le classi di traffico da classificare con i criteri definiti in precedenza
3. Creare una mappa dei criteri che associa azioni di contrassegno e azioni di controllo alle classi definite
4. Configurare le interfacce corrispondenti in modalità attendibile
5. Applicare il mapping dei criteri a un'interfaccia

Nell'esempio, il traffico IP in arrivo sull'host 192.168.192.168 deve essere contrassegnato con IP precedence 6 e controllato fino a 1 Mbps; il traffico in eccesso deve essere contrassegnato con IP precedence 2:

```
!--- Globally enables QoS. mls qos !--- Defines the ACLs to select traffic. access-list 167
permit ip any host 192.168.192.168
!--- Defines the traffic class. class-map match-all cl_2host
  match access-group 167
!--- Defines QoS policy, and creates and attaches !--- the policers to the traffic classes.
policy-map po_test3
  class cl_2host
!--- Marks all the class traffic with the IP precedence 6. set ip precedence 6
!--- Polices down to 1 Mbps and marks down according to the QoS map. police 1000000 8000 exceed-
action policed-dscp-transmit
!--- Modifies the policed DSCP QoS map, so the !--- traffic is marked down from IP precedence 6
to 2. !--- In terms of DSCP, this is from 48 to 16 (DSCP=IPprec x8). mls qos map policed-dscp 48
to 16 !--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport
switchport access vlan 2 service-policy input po_test3
```

Per monitorare il contrassegno, viene emesso lo stesso comando **show mls qos interface statistics**. Output di esempio e implicazioni sono documentati nella sezione di questo documento.

Come classificare tutto il traffico di interfaccia con un singolo policer

Sul Catalyst 3550, il comando **match interface** non è supportato e per ciascuna class-map è consentito un solo comando match. Inoltre, lo switch Catalyst 3550 non consente al traffico IP di essere associato agli ACL MAC. Pertanto, il traffico IP e non IP deve essere classificato con due mappe di classe separate. Questo rende difficile classificare tutto il traffico che arriva in un'interfaccia e controllare tutto il traffico con un singolo policer. La configurazione di esempio consente di eseguire questa operazione. In questa configurazione, il traffico IP e non IP viene abbinato a due diverse mappe di classe. Tuttavia, ciascuno utilizza un policer comune per entrambi i tipi di traffico.

```
access-list 100 permit ip any any

class-map ip
match access-group 100
!--- This class-map classifies all IP traffic. mac access-list extended non-ip-acl
permit any any

class-map non-ip
match access-group name non-ip-acl
!--- Class-map classifies all non-IP traffic only. mls qos aggregate-policer all-traffic 8000
8000 exceed-action drop
!--- This command configures a common policer that is applied for both IP and non-IP traffic.
policy-map police-all-traffic
class non-ip
```

```
police aggregate all-traffic
class ip
police aggregate all-traffic

interface gigabitEthernet 0/7
service-policy input police-all-traffic
!--- This command applies the policy map to the physical interface.
```

Informazioni correlate

- Configurazione di QoS su Catalyst 3550
- Pagine di supporto Quality of Service
- Pagina di supporto dello switching LAN
- Pagine di supporto dei prodotti LAN
- Documentazione e supporto tecnico – Cisco Systems