Policing e contrassegno QOS con i Supervisor Engine basato su Catalyst 4000/4500 IOS

Sommario

Introduzione

La funzione Policing determina se il livello di traffico è all'interno del profilo specificato (contratto). La funzione di monitoraggio consente di eliminare il traffico fuori profilo o di contrassegnare il traffico con un valore DSCP (Differential Services Code Point) diverso per applicare il livello di servizio stipulato. DSCP è una misura del livello QoS (Quality of Service) del pacchetto. Oltre al DSCP, la precedenza IP e la classe di servizio (CoS) vengono usate per trasmettere il livello QoS del pacchetto.

Non confondere la sorveglianza con il traffic shaping, anche se entrambi garantiscono che il traffico rimanga all'interno del profilo (contratto). Il Policing non effettua il buffer del traffico, quindi il ritardo della trasmissione non viene influenzato. Anziché archiviare pacchetti fuori profilo, il policing li scarta o li contrassegna con un livello QoS diverso (DSCP contrassegna per il basso). 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 su un'interfaccia in uscita, mentre il policing può essere applicato sia su interfacce in entrata che in uscita.

Catalyst 4000/4500 con Supervisor Engine 3, 4 e 2+ (SE3, SE4, SE2+ d'ora in poi in questo documento) supporta il policing nelle direzioni in entrata e in uscita. Anche il Traffic Shaping è supportato, ma questo documento tratta solo di policy e contrassegni. Il contrassegno è un processo di modifica del livello QoS di un pacchetto in base a una policy.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

Parametri di monitoraggio e contrassegno QoS

Il policing viene configurato definendo le mappe dei criteri QoS e applicandole alle porte (QoS basato su porta) o alle VLAN (QoS basato su VLAN). Il policer è definito dai parametri di velocità e burst, nonché dalle azioni per il traffico nel profilo e fuori profilo.

Sono supportati due tipi di criteri: aggregati e per interfaccia. Ciascun policer può essere applicato a più porte o VLAN.

Il policer aggregato agisce sul traffico su tutte le porte/VLAN applicate. Ad esempio, si applica il policer aggregato per limitare il traffico TFTP (Trivial File Transfer Protocol) a 1 Mbps sulle VLAN 1 e 3. Questo policer consentirà 1 Mbps di traffico TFTP sulle VLAN 1 e 3 insieme. Se si applica un policer per interfaccia, il traffico TFTP sulle VLAN 1 e 3 verrà limitato a 1 Mbps ciascuna.

Nota: se a un pacchetto viene applicata la policy in entrata e in uscita, viene presa la decisione più grave. In altre parole, se il policer in entrata specifica di rilasciare il pacchetto e il policer in uscita specifica di contrassegnare il pacchetto come non attivo, il pacchetto verrà scartato. La tabella 1 riepiloga l'azione QoS sul pacchetto quando viene gestito dalle policy in entrata e in uscita.

Tabella 1. Azione QoS in base alle 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$_e$	Markdown$_e$
Mark$_e$	Mark$_e$	Drop	Mark$_e$	Mark$_e$

L'hardware Catalyst 4000 SE3, SE4, SE2+ QoS è implementato in modo che il contrassegno reale del pacchetto si verifichi dopo l'agente di controllo dell'uscita. Ciò significa che anche se il criterio in entrata segnala il pacchetto (da parte del policer mark down o del normal marking), il criterio in uscita vedrà comunque i pacchetti contrassegnati con il livello QoS originale. La policy in uscita vedrà il pacchetto come se non fosse stato contrassegnato dalla policy in entrata. Ciò significa quanto segue:

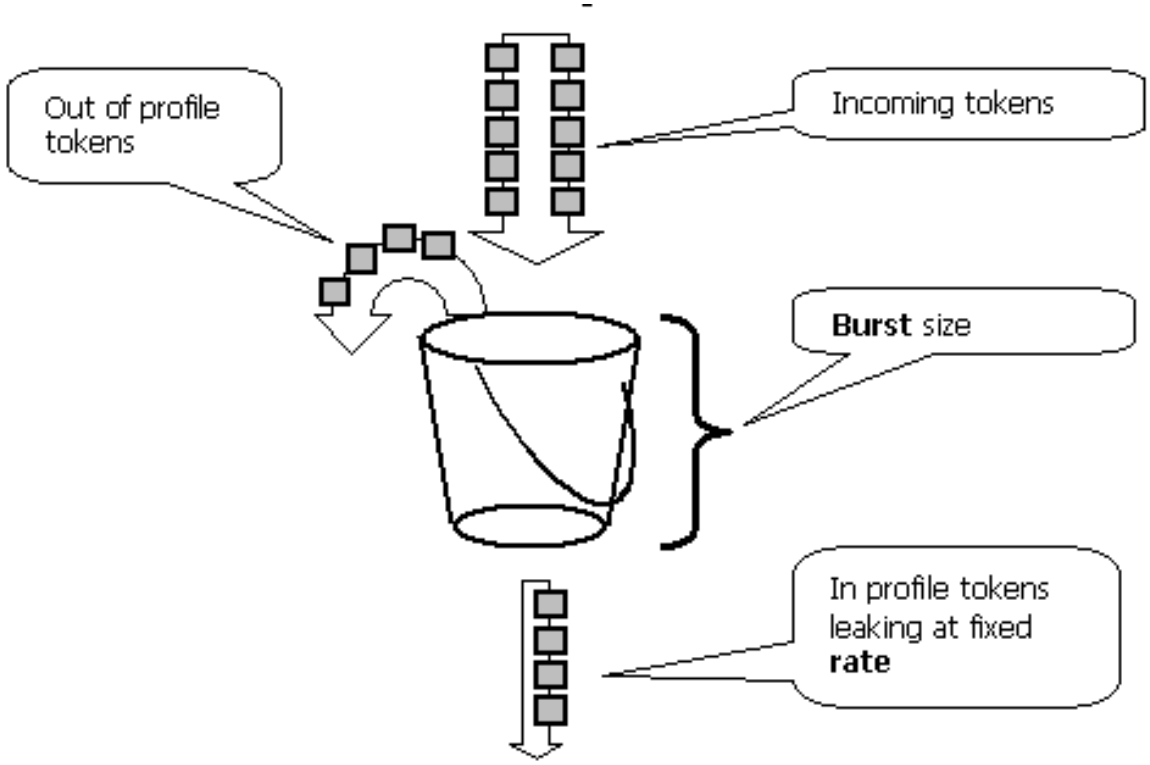
- Il contrassegno di uscita ha la precedenza sul contrassegno di entrata.
- I criteri di uscita non possono corrispondere ai nuovi livelli QoS modificati dal contrassegno di entrata.

Altre importanti implicazioni sono le seguenti:

- Non è possibile contrassegnare all'interno della stessa classe di traffico all'interno dello stesso criterio.
- I criteri aggregati sono per direzione. In altre parole, se un policer aggregato viene applicato

sia in entrata che in uscita, saranno presenti due policer aggregati, uno in entrata e uno in uscita.
- Quando un policer aggregato viene applicato all'interno del criterio alle VLAN e all'interfaccia fisica, in effetti saranno presenti due policer aggregati, uno per le interfacce VLAN e l'altro per le interfacce fisiche. Al momento, non è possibile controllare le interfacce VLAN e le interfacce fisiche insieme su un aggregato.

Il Policing in Catalyst 4000 SE3, SE4, SE2+ è conforme al concetto di bucket di perdite, come illustrato nel modello seguente. I token corrispondenti ai pacchetti del traffico in entrata vengono inseriti in un bucket (numero di token = dimensioni del pacchetto). A intervalli regolari, un numero definito di token (derivato 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 quindi scartato o contrassegnato, in base all'azione di policy configurata.



Notare che il traffico non viene memorizzato nel buffer, come potrebbe sembrare dal modello riportato sopra. Il traffico effettivo non scorre attraverso il secchio. Il periodo fisso viene utilizzato solo per decidere se il pacchetto è all'interno o all'esterno del profilo.

Si noti che l'implementazione hardware esatta del policing potrebbe essere diversa, dal punto di vista funzionale è conforme al modello precedente.

I seguenti parametri controllano il funzionamento del policing:

- Rate definisce il numero di token rimossi 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 fisso a 16 nanosecondi (16 sec *10-9). Impossibile modificare l'intervallo.
- Burst definisce la quantità massima di token che il bucket può contenere in qualsiasi momento.

Per le differenze nella frammentazione tra Catalyst 6000 e Catalyst 4000 e Catalyst 4000/4500 IOS, fare riferimento alla sezione Confronto delle policy e del contrassegno sui Supervisor Engine

basati su Catalyst 6000 e Catalyst 4000 SE3, SE4, SE2+.

Il policer assicura che se si esamina un qualsiasi periodo di tempo (da zero all'infinito), il policer non consentirà mai più di

```
<rate> * <period> + <burst-bytes> + <1 packet> bytes
```

di traffico attraverso l'agente di polizia durante tale periodo.

L'hardware Catalyst 4000 SE3, SE4, SE2+ QoS ha una certa granularità per la gestione delle policy. A seconda del tasso configurato, la deviazione massima dal tasso è pari all'1,5% del tasso.

Quando si configura la velocità di burst, è necessario tenere presente che alcuni protocolli (ad esempio il protocollo TCP) implementano meccanismi di controllo del flusso che reagiscono alla perdita di pacchetti. Ad esempio, il protocollo TCP riduce la finestra della metà per ciascun pacchetto perso. Quando sottoposto a policy a una determinata frequenza, l'utilizzo effettivo del collegamento sarà inferiore alla frequenza configurata. È possibile aumentare la frammentazione per ottenere un migliore utilizzo. Per ottenere un traffico di questo tipo, è consigliabile impostare lo burst in modo che equivalga al doppio della quantità di traffico inviato con la velocità desiderata durante il Round-Trip Time (RTT). Per lo stesso motivo, non è consigliabile eseguire il benchmark del funzionamento del policer in base al traffico orientato alla connessione, in quanto in genere le prestazioni risultano inferiori a quelle consentite dal policer.

Nota: anche il traffico senza connessione potrebbe reagire in modo diverso al monitoraggio. Ad esempio, il Network File System (NFS) utilizza blocchi che possono essere costituiti da più pacchetti UDP (User Datagram Protocol). Un pacchetto scartato potrebbe causare la ritrasmissione di molti pacchetti (intero blocco).

Ad esempio, di seguito viene riportato un calcolo della frammentazione per una sessione TCP, con una velocità di controllo di 64 Kbps e una velocità TCP RTT di 0,05 secondi:

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

Nota: <burst> è per una sessione TCP, quindi deve essere scalato in modo da calcolare la media del numero di sessioni previste che passano attraverso il policer. Poiché si tratta solo di un esempio, 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 controllo.

L'azione di controllo consiste nell'eliminare il pacchetto (drop) o nel modificare il DSCP del pacchetto (mark down). Per contrassegnare il pacchetto, è necessario modificare la mappa DSCP sottoposta a policy. Il DSCP controllato predefinito contrassegna il pacchetto sullo stesso DSCP, ovvero non si verifica alcun contrassegno.

Nota: i pacchetti potrebbero non essere ordinati quando un pacchetto non profilo viene contrassegnato da un DSCP a una coda di output diversa da quella del DSCP originale. Per questo motivo, se è importante ordinare i pacchetti, si consiglia di contrassegnare i pacchetti fuori profilo con DSCP mappato alla stessa coda di output dei pacchetti nel profilo.

Funzioni di policy e contrassegno supportate dai Supervisor Engine basato su Catalyst 4000/4500 IOS

Il monitoraggio in entrata (interfaccia in entrata) e in uscita (interfaccia in uscita) è supportato su

Catalyst 4000 SE3, SE4, SE2+. Lo switch supporta 1024 policy in entrata e 1024 in uscita. Due policer in entrata e due in uscita vengono utilizzati dal sistema per il comportamento predefinito di nessun policing.

Notare che quando il policer aggregato viene applicato all'interno del criterio a una VLAN e a un'interfaccia fisica, viene utilizzata una voce del policer hardware aggiuntiva. Al momento, non è possibile controllare le interfacce VLAN e le interfacce fisiche insieme su un aggregato. Questa condizione potrebbe essere modificata nelle versioni future del software.

Tutte le versioni software includono il supporto per il controllo. Catalyst 4000 supporta fino a 8 istruzioni match valide per classe e fino a 8 classi per mappa dei criteri. Le istruzioni di corrispondenza valide sono le seguenti:

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

Nota: per i pacchetti non IP V4, l'istruzione **match ip dscp** è l'unico modo di classificazione, a condizione che i pacchetti arrivino alle porte trunking che considerano attendibile il CoS. Non essere fuorviato dalla parola chiave ip nel comando **match ip dscp**, in quanto la corrispondenza del DSCP interno riguarda tutti i pacchetti, non solo l'IP. Quando una porta è configurata per considerare attendibile il CoS, questo viene estratto dal frame L2 (con tag 802.1Q o ISL) e convertito in DSCP interno utilizzando una mappa QoS da CoS a DSCP. Questo valore DSCP interno può quindi essere trovato nel criterio utilizzando **match ip dscp**.

Le azioni valide per i criteri sono le seguenti:

- polizia
- set ip dscp
- imposta precedenza ip
- trust dscp
- cc trust

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 a criteri definiti. Per ottenere una corrispondenza con IP Precence o DSCP, l'interfaccia in ingresso corrispondente deve essere impostata sulla modalità trusted. Lo switch supporta l'attendibilità di CoS, DSCP e interfacce non attendibili. Trust specifica il campo da cui verrà derivato il livello QoS del pacchetto.

Quando si considera attendibile il CoS, il livello QoS viene derivato dall'intestazione L2 del pacchetto ISL o incapsulato 802.1Q. Quando si considera attendibile DSCP, lo switch deriva il livello QoS dal campo DSCP del pacchetto. L'impostazione di un trust CoS ha significato solo sulle interfacce trunking e l'impostazione di un trust DSCP è valida solo per i pacchetti IP V4.

Quando un'interfaccia non è attendibile (questo è lo stato predefinito quando QoS è abilitato), il DSCP interno verrà derivato dal CoS o dal DSCP predefinito configurabile per l'interfaccia corrispondente. Se non è configurato alcun CoS o DSCP predefinito, il valore predefinito sarà zero (0). Una volta determinato il livello QoS originale del pacchetto, questo viene mappato nel DSCP interno. Il DSCP interno può essere mantenuto o modificato mediante contrassegno o applicazione di policy.

Dopo che il pacchetto è stato sottoposto a elaborazione QoS, i campi del livello QoS (all'interno

del campo IP DSCP per IP e all'interno dell'intestazione ISL/802.1Q, se presente) verranno aggiornati dal DSCP interno.

Sono disponibili mappe speciali utilizzate per convertire le metriche QoS attendibili del pacchetto nel DSCP interno e viceversa. Queste mappe sono le seguenti:

- da DSCP a DSCP controllato; usato per derivare il DSCP sottoposto a policy quando si contrassegna il pacchetto.
- Da DSCP a CoS: utilizzato per derivare il livello CoS dal DSCP interno per aggiornare l'intestazione ISL/802.1Q del pacchetto in uscita.
- CoS su DSCP: utilizzato per derivare il DSCP interno dal CoS in ingresso (intestazione ISL/802.1Q) quando l'interfaccia è in modalità CoS trust.

Si noti che quando un'interfaccia è in modalità CoS trust, il CoS in uscita sarà sempre lo stesso del CoS in ingresso. Questa funzionalità è specifica dell'implementazione QoS in Catalyst 4000 SE3, SE4, SE2+.

Configurazione e monitoraggio dei criteri

La configurazione del policing in IOS prevede i passi riportati di seguito.

1. Definizione di un policer.
2. Definizione dei criteri per selezionare il traffico per il policing.
3. Definizione dei criteri del servizio mediante la classe e applicazione di un policer a una classe specificata.
4. Applicazione di una policy sui servizi a una porta o a una VLAN.

Si consideri l'esempio seguente. Alla porta 5/14 è collegato un generatore di traffico che invia circa 17 Mbps di traffico UDP con una destinazione della porta 111. Si desidera che il traffico venga controllato fino a 1 Mbps e che il traffico eccessivo venga interrotto.

```
! enable qos
qos
! define policer, for rate and burst values, see 'policing parameters
qos aggregate-policer pol_1mbps 1mbps 1000 conform-action transmit
exceed-action
drop
! define ACL to select traffic
access-list 111 permit udp any any eq 111
! define traffic class to be policed
class-map match-all cl_test
match access-group 111
! define QoS policy, attach policer to traffic class
policy-map po_test
class cl_test
police aggregate pol_1mbps
! apply QoS policy to an interface
interface FastEthernet5/14
switchport access vlan 2
! switch qos to vlan-based mode on this port
qos vlan-based
! apply QoS policy to an interface
interface Vlan 2
service-policy output po_test
!
```

Notare che quando una porta è in modalità QoS basata su VLAN, ma non vengono applicati criteri del servizio alla VLAN corrispondente, lo switch seguirà gli eventuali criteri del servizio applicati a una porta fisica. Ciò consente una maggiore flessibilità nel combinare QoS basata su porta e VLAN.

Sono supportati due tipi di criteri: aggregato denominato e per interfaccia. Un policer aggregato denominato controllerà il traffico combinato da tutte le interfacce a cui viene applicato. Nell'esempio precedente viene utilizzato un policer denominato. A differenza di un policer specifico, un policer per interfaccia consente di controllare il traffico separatamente su ogni interfaccia a cui viene applicato. Nella configurazione della mappa dei criteri è definito un policer per interfaccia. Considerare l'esempio seguente con un policer di aggregazione per interfaccia:

```
! enable qos
qos
! define traffic class to be policed
class-map match-all cl_test2
match ip precedence 3 4
! define QoS policy, attach policer to traffic class
policy-map po_test2
class cl_test2
! per-interface policer is defined inside the policy map
police 512k 1000 conform-action transmit exceed-action drop
interface FastEthernet5/14
switchport
! set port to trust DSCP - need this to be able to match to incoming IP precedence
qos trust dscp
! switch to port-based qos mode
no qos vlan-based
! apply QoS policy to an interface
service-policy input po_test2
```

Il comando seguente viene utilizzato per monitorare l'operazione di applicazione dei criteri:

```
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400026 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166067574 bytes Exceed: 5268602114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400138 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166088574 bytes Exceed: 5268693114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
```

Il contatore vicino a class-map sta contando il numero di pacchetti corrispondenti alla classe corrispondente.

Tenere presenti le seguenti considerazioni specifiche sull'implementazione:

- Il contatore di pacchetti per classe non è per interfaccia. In altre parole, vengono conteggiati tutti i pacchetti che corrispondono alla classe tra tutte le interfacce in cui questa classe viene applicata nei criteri del servizio.
- I criteri non gestiscono i contatori dei pacchetti. Sono supportati solo i contatori dei byte.
- Non è disponibile alcun comando specifico per verificare la velocità del traffico offerto o in uscita per policer.
- I contatori vengono aggiornati periodicamente. Se si esegue ripetutamente il comando precedente in rapida successione, è possibile che i contatori vengano ancora visualizzati in un determinato momento.

Configurazione e monitoraggio del contrassegno

La configurazione del contrassegno prevede i passi riportati di seguito.

1. Definire i criteri per classificare il traffico: elenco degli accessi, DSCP, precedenza IP e così via.
2. Definire le classi di traffico da classificare utilizzando i criteri definiti in precedenza.
3. Creare una mappa dei criteri allegando azioni contrassegno e/o azioni di controllo alle classi definite.
4. Configurazione della modalità di trust sulle interfacce corrispondenti.
5. Applicare la mappa dei criteri a un'interfaccia.

Si consideri l'esempio seguente in cui si desidera che il traffico in entrata con IP precedence 3 arrivi all'host 192.168.196.3, UDP port 777 mappato all'IP precedence 6. Tutto il resto del traffico IP precedence 3 viene controllato fino a 1 Mbps e il traffico in eccesso deve essere contrassegnato fino all'IP precedence 2.

```
! enable QoS globally
qos
! define ACL to select UDP traffic to 192.168.196.3 port 777
ip access-list extended acl_test4
permit udp any host 192.168.196.3 eq 777
! define class of traffic using ACL and ip precedence matching
class-map match-all cl_test10
match ip precedence 3
match access-group name acl_test4
! all the remaining ip precedence 3 traffic will match this class
class-map match-all cl_test11
match ip precedence 3
! define policy with above classes
policy-map po_test10
class cl_test10
! mark traffic belonging to class with ip precedence 6
set ip precedence 6
class cl_test11
! police and mark down all other ip precedence 3 traffic
police 1 mbps 1000 exceed-action policed-dscp-transmit
!
! adjust DSCP to policed DSCP map so to map DSCP 24 to DSCP 16
```

```
qos map dscp policed 24 to dscp 16
!
interface FastEthernet5/14
! set interface to trust IP DSCP
qos trust dscp
! apply policy to interface
service-policy input po_test10
!
```

Il comando **sh policy interface** viene usato per monitorare il contrassegno. L'output di esempio e le relative implicazioni sono documentati nella configurazione di policing sopra riportata.

Confronto delle funzionalità di policy e contrassegno sui Supervisor Engine basato su Catalyst 6000 e Catalyst 4000/4500 IOS

Feature	Catalyst6000	Catalyst4000 SE3
Egress QoS policies	Not supported by Supervisor 1A and Superviso r2 hardware.	Supported.
Burst policing parameter calculation	Burst should be at least the same size as maximum frame supposed to pass via policer and no less then rate/interval, with the interval being 250 microseconds	No such restriction.
QoS policing L2 & L3	By default, microflow policing is only enabled for L3 on the sup1a and is not enabled at all for Supervisor 2. A CLI command is available to enable it for L2 on sup1a and L2 & L3 for sup2. Aggregate policing for sup1a & Supervisor 2 is enabled by default for L2 & L3.	Always.
Egress CoS	Always derived from internal DSCP using DSCP to CoS QoS map.	If the ingress port is in trust CoS mode, the egress CoS will be the same as the ingress CoS. Otherwise, it will be derived from the internal DSCP.
Microflow policing	Supported.	Not supported.
QoS behavior when port is in VLAN-based QoS mode, but no policy is applied to the VLAN.	No policy applied.	Fallback to port-based QoS. Will apply policy attached to port.

Informazioni correlate

- Descrizione e configurazione di QoS
- Supporto tecnico – Cisco Systems