Informazioni sui contatori pacchetti nell'output del comando show interface rate con Committed Access Rate (CAR)

Sommario

Introduzione

Committed Access Rate (CAR) è una funzione di limitazione della velocità che può essere utilizzata per fornire servizi di classificazione e monitoraggio. L'ACL può essere usato per classificare i pacchetti in base a certi criteri, come l'indirizzo IP e i valori delle porte che usano gli elenchi degli accessi. È possibile definire l'azione per i pacchetti conformi al valore limite di velocità e che superano tale valore. Per ulteriori informazioni su come configurare CAR, fare riferimento a Configurazione della velocità di accesso vincolata.

Questo documento spiega perché l'output del comando **show interface x/x rate-limit** mostra un valore in bps `diverso da zero superato` quando il valore in bps `conforme` è inferiore al valore CIR (Committed Information Rate) configurato.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni

nei suggerimenti tecnici.

Informazioni sull'output del comando show interface rate

L'output di questo comando consente di visualizzare le velocità in eccesso diverse da zero in tre condizioni:

- I valori burst sono impostati su un valore troppo basso per consentire una velocità effettiva sufficiente. Ad esempio, vedere l'ID bug Cisco CSCdw42923 (solo utenti registrati).
- Problema risolto con doppio accounting nel software Cisco IOS®
- Bug software in Cisco IOS

Osservare l'output di esempio di un'interfaccia di accesso virtuale. In questa configurazione, il protocollo RADIUS viene usato per assegnare un limite di velocità all'interfaccia di accesso virtuale creata in modo dinamico.

```
AV Pair from Radius
Cisco-AVPair = "lcp:interface-config#1=rate-limit input 256000 7500 7500
conform-action continue
exceed-action drop",
Cisco-AVPair = "lcp:interface-config#2=rate-limit output 512000 7500 7500
conform-action continue
exceed-action drop",
```

Usare il comando show interface x rate-limit per monitorare le prestazioni del Cisco legacy policer, CAR. In questo esempio, l'output di questo comando fornisce suggerimenti sul motivo per cui sono presenti bps diversi da zero. Il valore di burst corrente è 7392 byte, mentre il valore di burst vincolato (Bc), indicato dal valore limite, è impostato su 7500 byte.

```
router#show interfaces virtual-access 26 rate-limit
Virtual-Access26 Cable Customers
  Input
    matches: all traffic
      params:  256000 bps, 7500 limit, 7500 extended limit
      conformed 2248 packets, 257557 bytes; action: continue
      exceeded 35 packets, 22392 bytes; action: drop
      last packet: 156ms ago, current burst: 0 bytes
      last cleared 00:02:49 ago, conformed 12000 bps, exceeded 1000 bps
  Output
    matches: all traffic
      params:  512000 bps, 7500 limit, 7500 extended limit
      conformed 3338 packets, 4115194 bytes; action: continue
      exceeded 565 packets, 797648 bytes; action: drop
      last packet: 188ms ago, current burst: 7392 bytes
      last cleared 00:02:49 ago, conformed 194000 bps, exceeded 37000 bps
```

Quando si configura CAR o un policer più recente di Cisco, con il policing basato su classi, è necessario configurare valori burst sufficientemente alti per garantire il throughput previsto e assicurare che il policer scarti i pacchetti solo per punire la congestione a breve termine.

Quando si selezionano i valori di frammentazione, è importante tenere conto degli aumenti transitori delle dimensioni della coda. Non si può semplicemente presumere che i pacchetti arrivino e partano contemporaneamente. Inoltre, non si può presumere che la coda passi da vuota a un pacchetto e che rimanga in un unico pacchetto in base a un orario di arrivo coerente di uno dei due pacchetti. Se il traffico tipico è piuttosto burst, i valori di burst devono essere

proporzionalmente grandi in modo da mantenere l'utilizzo del collegamento a un livello accettabile. Una dimensione di burst troppo bassa o una soglia minima troppo bassa possono determinare un utilizzo del collegamento inaccettabilmente basso.

Un burst può essere definito semplicemente come una serie di frame back-to-back di dimensioni MTU, ad esempio frame di 1500 byte che hanno origine su una rete Ethernet. Quando una frammentazione di tali frame arriva a un'interfaccia di output, può sopraffare i buffer di output e superare la profondità configurata del bucket di token in un momento istantaneo. Con l'uso di un sistema di controllo dei token, un policer prende una decisione binaria se un pacchetto in arrivo è conforme, supera o viola i valori di controllo configurati. Con il traffico bursty, come ad esempio un flusso FTP, la velocità di arrivo istantaneo di questi pacchetti può superare i valori burst configurati e portare a cadute CAR.

Inoltre, la velocità effettiva complessiva in periodi di congestione varia con il tipo di traffico valutato dal policer. Mentre il traffico TCP risponde alla congestione, gli altri flussi no. Esempi di flussi che non rispondono includono i pacchetti basati su UDP e ICMP.

Il protocollo TCP si basa su un riconoscimento positivo con ritrasmissione. Il protocollo TCP utilizza una finestra scorrevole come parte del proprio meccanismo di riconoscimento positivo. I protocolli a finestra scorrevole utilizzano meglio la larghezza di banda della rete in quanto consentono al mittente di trasmettere più pacchetti prima di attendere una conferma. Ad esempio, in un protocollo a finestra scorrevole con una dimensione di finestra pari a 8, al mittente è consentito trasmettere 8 pacchetti prima di ricevere una conferma. Se si aumentano le dimensioni della finestra, il tempo di inattività della rete viene in gran parte eliminato. Un protocollo a finestra scorrevole ottimizzato mantiene la rete completamente saturata dai pacchetti e mantiene un elevato throughput.

Poiché gli endpoint non conoscono lo stato di congestione specifico della rete, il protocollo TCP è progettato per rispondere alla congestione nella rete riducendo le velocità di trasmissione in caso di congestione. In particolare, utilizza due tecniche:

Tecnica	Descrizione
Riduzione moltiplicativa della prevenzione delle congestioni	In caso di perdita di un segmento (l'equivalente di un pacchetto al TCP), dimezzare la finestra di congestione. La finestra di congestione è un secondo valore o finestra che viene utilizzata per limitare il numero di pacchetti che un mittente può trasmettere nella rete prima di attendere una conferma.
Avvio del ripristino lento	Quando si avvia il traffico su una nuova connessione o si aumenta il traffico dopo un periodo di congestione, avviare la finestra di congestione alle dimensioni di un singolo segmento e aumentare la finestra di congestione di un segmento ogni volta che arriva una conferma. Il protocollo TCP inizializza la finestra di congestione su 1, invia un segmento iniziale e attende. All'arrivo della conferma, la finestra di

	congestione aumenta a 2, invia due segmenti e attende. Per ulteriori informazioni, vedere la RFC 2001 .

I pacchetti possono andare persi o essere distrutti quando gli errori di trasmissione interferiscono con i dati, quando l'hardware della rete si guasta o quando le reti diventano troppo sovraccariche per gestire il carico presentato. Il protocollo TCP presume che la perdita di pacchetti o i pacchetti che non vengono riconosciuti entro l'intervallo di tempo a causa di un ritardo estremo indichino una congestione della rete.

Il sistema di misurazione token bucket di un policer viene richiamato all'arrivo di ogni pacchetto. In particolare, il tasso conformato e il tasso in eccesso vengono calcolati in base a questa semplice formula:

```
(conformed bits since last clear counter)/(time in seconds elapsed since last clear counter)
```

Poiché la formula calcola le velocità in un periodo dall'ultima volta in cui i contatori sono stati azzerati, Cisco consiglia di cancellare i contatori per monitorare la velocità corrente. Se i contatori non vengono azzerati, la velocità della formula precedente indica che l'output del comando **show** visualizza una media calcolata su un periodo potenzialmente molto lungo e che i valori potrebbero non essere significativi nella determinazione della velocità corrente.

Il throughput medio deve corrispondere alla velocità delle informazioni di cui è stato eseguito il commit (CIR, Committed Information Rate) in un periodo di tempo. Le dimensioni burst consentono di impostare la durata massima della frammentazione in un determinato momento. Se il traffico non è presente o è inferiore al valore CIR del traffico e il bucket di token non viene riempito, una frammentazione molto grande è comunque limitata a una dimensione particolare calcolata in base alla normale frammentazione e alla frammentazione estesa.

La velocità di caduta è il risultato di questo meccanismo

1. Annotare l'ora corrente.
2. Aggiornare il bucket di token con il numero di token accumulati in modo continuo dall'ultimo arrivo di un pacchetto.
3. Il numero totale di token accumulati non può superare il valore maxtokens. Elimina token in eccesso.
4. Verifica la conformità del pacchetto.

La limitazione della velocità può essere ottenuta anche con Policing. Questa è una configurazione di esempio per limitare la velocità sull'interfaccia Ethernet che usa il policy basato su classi.

```
class-map match-all rtp1
   match ip rtp 2000 10
!
   policy-map p3b
   class rtp1
   police 200000 6250 6250 conform-action transmit exceed-action drop violate-action    drop
policy-map p2
   class rtp1
   police 250000 7750 7750 conform-action transmit exceed-action drop violate-action    drop
   !
interface Ethernet3/0
   service-policy output p3b
   service-policy input p2
```

In questo output di esempio del comando show policy-map interface vengono illustrati i valori calcolati e sincronizzati correttamente per la velocità offerta e la velocità di rilascio, nonché per le velocità conformate e superiori a bps.

```
router#show policy-map interface ethernet 3/0
  Ethernet3/0

   Service-policy input: p2

     Class-map: rtp1 (match-all)
       88325 packets, 11040625 bytes
       30 second offered rate 400000 bps, drop rate 150000 bps
       Match: ip rtp 2000 10
       police:
         250000 bps, 7750 limit, 7750 extended limit
         conformed 55204 packets, 6900500 bytes; action: transmit
         exceeded 33122 packets, 4140250 bytes; action: drop
         conformed 250000 bps, exceed 150000 bps violate 0 bps

       Service-policy : p3b

         Class-map: rtp1 (match-all)
           88325 packets, 11040625 bytes
           30 second offered rate 400000 bps, drop rate 50000 bps
           Match: ip rtp 2000 10
           police:
             200000 bps, 6250 limit, 6250 extended limit
             conformed 44163 packets, 5520375 bytes; action: transmit
             exceeded 11041 packets, 1380125 bytes; action: drop
             conformed 200000 bps, exceed 50000 bps violate 0 bps

         Class-map: class-default (match-any)
           0 packets, 0 bytes
           30 second offered rate 0 bps, drop rate 0 bps
           Match: any
```

Problemi noti dei contatori di controllo basati su classi e CAR

In questa tabella vengono elencati i problemi risolti con i contatori visualizzati nei comandi **show policy-map** o **show interface rate-limit**. Gli utenti registrati che hanno effettuato l'accesso possono visualizzare le informazioni sul bug in Bug Search Tool.

Sintomo	ID bug risolti e soluzioni
Contatori di rilascio inferiori al previsto	• ID bug Cisco CSCdv41231 (solo utenti registrati)Quando un criterio di servizio gerarchico di input utilizza il comando **Police** ai livelli padre e figlio, il policer può eliminare un numero di pacchetti inferiore a quello previsto poiché il policer di livello padre deve essere congestionato prima di rilasciare i pacchetti. Questo è un esempio di tale politica: `policy-map child` `class dscp1` `police cir 100000 bc 3000 conform-action transmit exceed-action drop`

	`` ! policy-map parent class rtp1 police cir 250000 bc 7750 conform- action transmit exceed-action drop service-policy child ``` Per ovviare al problema, creare criteri separati e applicarne uno in entrata e uno in uscita, in modo da evitare la configurazione di criteri gerarchici.
Raddoppiare la velocità prevista di caduta e throughput	• ID bug Cisco CSCds23924 (solo utenti registrati)Cisco Express Forwarding (CEF) definisce un meccanismo di commutazione IOS che inoltra i pacchetti dall'interfaccia di input a quella di output. Prima delle modifiche implementate da questo ID bug, i meccanismi CEF e QoS configurati, ad esempio CAR o il policy basato su classi, incrementavano i contatori dei pacchetti. Il risultato è la cosiddetta doppia contabilizzazione e pacchetti conformati gonfiati e valori di perdita in eccesso. • ID bug Cisco CSCdr40598 (solo utenti registrati)Su Cisco serie 12000, quando l'auto di uscita è abilitata e la scheda di linea in entrata è il motore 2, i contatori di uscita in uscita vengono raddoppiati. Questo doppio accounting deriva dalla modalità di gestione dei contatori di output. • ID bug Cisco CSCdv84259 (solo utenti registrati)Se si abilita globalmente il comando **ip cef distributed** su un router Cisco serie 7500, viene visualizzata un'interfaccia di scheda VIP (non-Versatile Interface Processor) con il comando **ip route-cache distributed** abilitato per impostazione predefinita. I non VIP non supportano CEF distribuiti e un effetto collaterale raro di questo comando visualizzato nei non VIP è il doppio accounting.
Nessuna caduta o percentuale di caduta pari a zero	In generale, quando si applicano funzionalità QoS basate su classi, il primo passaggio nella risoluzione dei problemi consiste nel garantire il corretto funzionamento del meccanismo di classificazione QoS. In altre parole, assicurarsi che i pacchetti specificati nelle istruzioni match nella mappa di classe corrispondano alle classi corrette. ``` router#show policy-map interface ATM4/0.1 ```

	Service-policy input: drop-inbound-http-hacks (1061) Class-map: http-hacks (match-any) (1063/2) 149 packets, 18663 bytes 5 minute offered rate 2000 bps, drop rate 0 bps Match: protocol http url "*cmd.exe*" (1067) 145 packets, 18313 bytes 5 minute rate 2000 bps Match: protocol http url "*.ida*" (1071) 0 packets, 0 bytes 5 minute rate 0 bps Match: protocol http url "*root.exe*" (1075) 4 packets, 350 bytes 5 minute rate 0 bps Match: protocol http url "*readme.eml*" (1079) 0 packets, 0 bytes 5 minute rate 0 bps police: 1000000 bps, 31250 limit, 31250 extended limit conformed 0 packets, 0 bytes; action: drop exceeded 0 packets, 0 bytes; action: drop violated 0 packets, 0 bytes; action: drop conformed 0 bps, exceed 0 bps violate 0 bps • ID bug Cisco CSCds3478 (solo utenti registrati)La classificazione ha esito negativo quando è abilitato CEF e non DCEF e a un PVC ATM è collegato un criterio di input. Nel software Cisco IOS versione 12.1T, la classificazione dell'output non ha esito positivo se è abilitato CEF, non DCEF, e un criterio di output è associato a un PVC ATM.
Frequenza di rilascio anomala o incoerente	• ID bug Cisco CSCdw50583 (solo utenti registrati)La velocità di rilascio visualizzata nella mappa di classe non corrisponde alle velocità di rilascio indicate dall'azione della polizia. In questo output di esempio, la velocità di rilascio per la classe è di 745000 bps, mentre la velocità di rilascio indicata dall'azione della polizia è di 1072000 bps. router#**show policy-map interface** Serial3/0.1: DLCI 13 - Service-policy output: out Class-map: c2 (match-all) 172483 packets, 91760956 bytes 30 second offered rate 1384000 bps, drop rate 745000 bps Match: ip precedence 0 police:

	384000 bps, 1500 limit, 1500 extended limit conformed 38903 packets, 20696396 bytes; action: transmit exceeded 133580 packets, 71064560 bytes; action: drop conformed 311000 bps, exceed 1072000 bps violate 0 bps

Informazioni correlate

- Configurazione della velocità di accesso impegnata
- Sorveglianza con CAR
- Uso di CAR durante gli attacchi DOS
- Pagina di supporto per la tecnologia QoS
- Pagina di supporto per i protocolli di routing IP
- Pagina di supporto per il routing IP
- Documentazione e supporto tecnico – Cisco Systems