Het begrip van de tellers van het Packet in de uitvoer van het showinterfacetarief met Committed Access Rate (CAR)

Inhoud

Inleiding

Committed Access Rate (CAR) is een snelheidsbeperkende functie die kan worden gebruikt om classificatiediensten en diensten voor toezicht te verlenen. De CAR kan worden gebruikt om pakketten te classificeren op basis van bepaalde criteria, zoals IP adres en poortwaarden die toegangslijsten gebruiken. De actie voor pakketten die aan de snelheidsgrenswaarde voldoen en de waarde overschrijden kan worden gedefinieerd. Raadpleeg het Committed Access Rate voor meer informatie over het configureren van de CAR.

Dit document legt uit waarom de uitvoer van de opdracht **Show interface x/x rate-limit"** toont een `niet-nul overtroffen bps` waarde wanneer de `conform bps` waarde minder is dan het geconfigureerde toegewezen informatiesnelheid (CIR).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor

meer informatie over documentconventies.

De uitvoer van het showinterfacesnelheids begrijpen

Er zijn drie voorwaarden waarin u overschrijding van de niet-nul-waarden in de uitvoer van deze opdracht kunt zien:

- De barstwaarden worden te laag ingesteld om een voldoende doorvoersnelheid te bereiken. Zie Cisco bug-ID CSCdw42923 (alleen geregistreerde klanten) bijvoorbeeld.
- Opgeloste probleem met dubbele accounting in Cisco IOS® software
- Softwarebug in Cisco IOS

Bekijk de voorbeelduitvoer van een virtuele-toegangsinterface. In deze configuratie wordt RADIUS gebruikt om een snelheidsgrens toe te kennen aan de dynamisch gemaakte virtuele toegangsinterface.

```
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",
```

Gebruik de opdracht Show interface x rate-limit (interface x rate-limiet) om de prestaties van de Cisco legacy-agent, CAR, te controleren. In dit voorbeeld, verstrekt de output van deze opdracht punten om waarom er een niet-nul overschreden bps is. De huidige waarde is 7392 bytes, terwijl de geëngageerde waarde (Bc), die door de grenswaarde wordt aangegeven, is ingesteld op 7500 bytes.

```
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
```

Wanneer u CAR of een nieuwere politieagent van Cisco, op klasse gebaseerde controle vormt, moet u voldoende hoge burstwaarden configureren om de verwachte doorvoersnelheid te verzekeren en om te verzekeren dat de politieagent pakketten slechts laat vallen om korte termijncongestie te bestraffen.

Wanneer u barstwaarden selecteert, is het belangrijk om voorbijgaande verhogingen in de rijgrootte aan te passen. U kunt niet eenvoudigweg aannemen dat pakketten tegelijk arriveren en vertrekken. U kunt ook niet aannemen dat de rij van leeg in één pakket verandert en dat de rij op

één pakket blijft gebaseerd op een consistente aankomsttijd in/uit. Als het typische verkeer vrij zwaar is, moeten de barstwaarden dienovereenkomstig groot zijn om het gebruik van de verbinding op een aanvaardbaar hoog niveau te kunnen handhaven. Een te lage barstgrootte, of een te lage minimumdrempel, kan leiden tot een onaanvaardbaar laag gebruik van een link.

Een uitbarsting kan eenvoudig worden gedefinieerd als een reeks back-to-back frames met een groot aantal MTU's, zoals 1500 byte-frames die op een Ethernet-netwerk gegenereerd zijn. Wanneer een barst van dergelijke frames op een uitvoer-interface aankomt, kan deze de uitvoerbuffers overweldigen en de geconfigureerde diepte van de token-emmer op een moment in de tijd overschrijden. Met het gebruik van een symbolisch metersysteem, neemt een politieagent een binaire beslissing over of een aankomend pakket de geconfigureerde politiwaarden conformeert, overschrijdt of schendt. Met bursty verkeer, zoals een FTP stream, kan het huidige aankomstpercentage van deze pakketten de ingestelde barstwaarden overschrijden en tot CAR-druppels leiden.

Bovendien varieert de totale doorvoersnelheid in tijden van congestie met het type verkeer dat door de politieagent wordt beoordeeld. Terwijl het TCP verkeer op congestie reageert, zijn andere stromen niet. Voorbeelden van niet-responsieve stromen zijn op UDP gebaseerde en op ICMP gebaseerde pakketten.

TCP is gebaseerd op positieve erkenning met hertransmissie. TCP gebruikt een glijvenster als deel van zijn positieve erkenningsmechanisme. De delen van het venster gebruiken netwerkbandbreedte beter omdat zij de afzender toestaan om vele pakketten te verzenden alvorens zij op een ontvangstbevestiging wachten. In een protocol van een venster dat op een venstergrootte van 8 lijkt, is de afzender toegestaan 8 pakketten te verzenden voordat deze een ontvangstbevestiging ontvangt. Als u de venstergrootte verhoogt, wordt de netwerkstationstijd grotendeels geëlimineerd. Een goed afgestemd protocol op het schuifvenster houdt het netwerk volledig verzadigd met pakketten en handhaaft een hoge doorvoersnelheid.

Aangezien endpoints de specifieke congestiestatus van het netwerk niet kennen, wordt TCP als een protocol ontworpen om op congestie in het netwerk te reageren door de transmissietarieven te verlagen wanneer congestie optreedt. Er zijn twee technieken:

techniek	Beschrijving
Meervoudige vermindering van congestie vermijding	Na het verlies van een segment (de equivalent van een pakket aan TCP), verlaagt u het congestievenster met de helft. Het venster voor congestie is een tweede waarde of venster dat wordt gebruikt om het aantal pakketten te beperken dat een afzender in het netwerk kan verzenden voordat het op een erkenning wacht.
Langzame start	Wanneer u verkeer op een nieuwe verbinding start of het verkeer vergroot na een periode van congestie, start het venster op de grootte van één segment en vergroot het venster op de congestie met één segment telkens wanneer een ontvangstbevestiging arriveert. TCP initialiseert het congestievenster aan 1, verstuurt een eerste segment en wacht. Wanneer de ontvangstbevestiging arriveert, verhoogt deze het congestievenster naar 2,

	stuurt twee segmenten en wacht. Zie voor meer informatie RFC 2001 .

Packets kunnen verloren of vernietigd worden wanneer transmissiefouten gegevens verstoren, wanneer de netwerkhardware faalt of wanneer netwerken te zwaar geladen worden om de aangeboden lading aan te passen. TCP veronderstelt dat verloren pakketten, of pakketten die niet binnen het getimed interval wegens extreem vertraging worden erkend, congestie in het netwerk aangeven.

Op elke pakketaankomst wordt het symbolische emmer-systeem van een politieagent ingeroepen. Met name het conformiteitspercentage en het overschrijdingspercentage worden berekend op basis van deze eenvoudige formule:

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

Aangezien de formule rentetarieven berekent over een periode van de laatste keer dat de tellers werden goedgekeurd, adviseert Cisco om de tellers te ontruimen om het huidige tarief te controleren. Als de tellers niet worden geklaard, betekent het vorige formule tarief feitelijk dat de opdrachtoutput van de **show** een gemiddelde weergeeft dat over een potentieel zeer lange periode is berekend, en de waarden mogelijk niet betekenisvol zijn in de bepaling van het huidige tarief.

De gemiddelde doorvoersnelheid moet overeenkomen met het geconfigureerde geëngageerde informatietarief (CIR) over een periode. De barstgrootte maakt een maximale barsttijd op een bepaald tijdstip mogelijk. Indien er geen verkeer is of minder dan de waarde van de CIR en de penning niet vult, is een zeer grote uitbarsting nog beperkt tot een bepaalde omvang, berekend op basis van normale uitbarsting en uitgestelde uitbarsting.

De daling is het gevolg van dit mechanisme

1. Let op de huidige tijd.
2. Update de pennenemmer met het aantal penningen dat zich sinds de laatste keer dat een pakje arriveert continu heeft verzameld.
3. Het totale aantal opgestapelde penningen kan de maxtokens-waarde niet overschrijden. Dek teveel penningen.
4. Controleer op overeenstemming van het pakket.

Snelheidsbeperking kan ook worden bereikt door toezicht uit te oefenen. Dit is een voorbeeldconfiguratie om snelheidsbeperking op de Ethernet interface te bieden die op klasse gebaseerd toezicht gebruikt.

```
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
```

Deze steekproefuitvoer van de **show policy-map interface** opdracht illustreert correct berekende en gesynchroniseerde waarden voor aangeboden tarief en dalingssnelheid evenals conformeerde en overschrijdt bps tarieven.

```
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
```

Bekende problemen met CAR- en Class Based Policing Counters

Deze tabel toont opgeloste problemen met de tellers die in de **show beleid-kaart** worden weergegeven of **toont** opdrachten **van de interfacetariumlimiet**. Geregistreerde klanten die inlogd zijn, kunnen de bug informatie in de zoekfunctie voor bugs bekijken.

Symptoom	Opgeloste Bug-id's en -werelden
Minder dan verwachte valtellers	• Cisco bug-id CSCdv41231 (alleen geregistreerde klanten)Wanneer een hiërarchisch servicebeleid van de **politie** gebruikmaakt van de ouder- en kinderstand, kan de politieagent minder dan het verwachte aantal pakketten neerzetten aangezien de op het ouderniveau actieve politieagent moet worden gestopt voordat de pakketten worden weggegooid. Dit is een voorbeeld van zo'n beleid: `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 Als een tijdelijke oplossing moet u afzonderlijk beleid maken en één op inkomende en één op uitgaande toepassen om de configuratie van een hiërarchisch beleid te vermijden.
Verwacht tempo van druppels en doorvoer snelheid verdubbelen	• Cisco bug-id CSCds23924 (alleen geregistreerde klanten)Cisco Express Forwarding (CEF) definieert een IOS-switching mechanisme dat pakketten converteert van invoer naar uitvoerinterface. Voorafgaand aan de veranderingen die van deze bug-ID zijn geïmplementeerd, hebben zowel CEF als geconfigureerde QoS-mechanismen zoals CAR of op klasse gebaseerde controle de pakkettellers verhoogd. Het resultaat is een zogeheten dubbele accounting en opgeblazen conformiteitspakketten en overmatige waarde. • Cisco bug-id CSCdr40598 (alleen geregistreerde klanten)Op de Cisco 12000-serie, wanneer de uitvoer van CAR is ingeschakeld en de ingang van de lijnkaart Engine 2 is, worden de uitgang van de tellers verdubbeld. Deze dubbele boekhouding vloeit voort uit de manier waarop outputtelaars worden behandeld. • Cisco bug-id CSCdv84259 (alleen geregistreerde klanten)Als u de **ip** cef **gedistribueerde** opdracht op een Cisco 7500 Series router globaal toelaat, verschijnt een niet-veelzijdige interface van de interfacekaart (VIP) met het **ip route-cache gedistribueerde** opdracht die standaard wordt ingeschakeld. Niet-VIP's ondersteunen gedistribueerde CEF niet, en een zeldzaam neveneffect van deze opdracht op niet-VIP's is dubbele accounting.
Geen druppels	In het algemeen, wanneer u op klasse gebaseerde QoS functies toepast, is de eerste

of een nul druppels nelheid	stap in het oplossen van problemen om te verzekeren dat het QoS classificatiemechanisme goed werkt. Met andere woorden, zorg dat de pakketten die in de overeenkomende verklaringen in uw class-map worden gespecificeerd de juiste klassen aanslaan.
	`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`
	• Cisco bug-id CSCds3478 (alleen geregistreerde klanten)De classificatie faalt als CEF, en niet DCEF, is ingeschakeld en een invoerbeleid is gekoppeld aan een ATM PVC. In Cisco IOS-softwarerelease 12.1T mislukt de uitvoerclassificatie als CEF en niet DCEF ingeschakeld zijn en er een uitvoerbeleid aan een ATM PVC is gekoppeld.

Anomalo og of inconseq uent dalingsp ercentag	• Cisco bug-id CSCdw50583 (alleen geregistreerde klanten)De daling die in de class-map wordt weergegeven, komt niet overeen met de daling die in het politieoptreden wordt aangegeven. In dit

e	voorbeeld is de output van het neerwaartse cijfer voor de klas 745000 bps, terwijl het neerwaartse cijfer dat bij politieoptreden wordt getoond 1072000 bps is.
	`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`

Gerelateerde informatie

- Committed Access Rate instellen
- Toezicht met CAR
- CAR gebruiken tijdens DOS-aanvallen
- QoS-pagina voor technologieondersteuning
- Ondersteuningspagina voor IP-routeringsprotocollen
- Ondersteuningspagina voor IP-routing
- Technische ondersteuning en documentatie – Cisco Systems