O Que São Contadores de Pacotes na Saída do Comando show interface rate com CAR (Taxa de Acesso Comprometida)

Contents

Introduction

A taxa de acesso consolidada (CAR) é um recurso de limitação de taxa que pode ser usado para proporcionar serviços de classificação e controle. A CAR pode ser usada para classificar os pacotes com base em determinados critérios, tais como endereço IP e valores das portas que usam listas de acesso. A medida a ser tomada para pacotes que estão em conformidade com o valor de limite de taxa e excedem o valor pode ser definida. Consulte Configurando Taxa de Acesso Consolidada para obter mais informações sobre como configurar a CAR.

Este documento explica por que a saída do comando **show interface x/x rate-limit** mostra um valor de `bps excedido não zero` quando o valor `de bps conformado` é menor que a taxa de informação comprometida (CIR) configurada.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre

convenções de documentos.

Compreendendo a saída do comando show interface rate

Há três condições nas quais você pode ver taxas excedidas diferentes de zero na saída deste comando:

- Os valores de intermitência são definidos como muito baixos para permitir uma taxa de transferência suficiente. Por exemplo, consulte o bug da Cisco ID CSCdw42923 (somente clientes registrados).
- Problema resolvido com dupla contabilização no software Cisco IOS®
- Bug de software no Cisco IOS

Observe o exemplo de saída de uma interface de acesso virtual. Nesta configuração, o RADIUS é usado para atribuir um limite de taxa à interface de acesso virtual criada dinamicamente.

```
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",
```

Use o comando show interface x rate-limit para monitorar o desempenho do Cisco Legacy policer, CAR. Neste exemplo, a saída desse comando fornece dicas sobre por que há um bps excedido de diferente de zero. O valor de intermitência atual é 7392 bytes, enquanto o valor de intermitência comprometida (Bc), indicado pelo valor limite, é definido como 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
```

Ao configurar o CAR ou um vigilante mais recente da Cisco, a vigilância baseada em classe, você deve configurar valores de intermitência suficientemente altos para garantir o throughput esperado e para garantir que o vigilante descarte pacotes somente para punir o congestionamento de curto prazo.

Quando você seleciona valores de intermitência, é importante acomodar aumentos transitórios no tamanho da fila. Você não pode simplesmente supor que os pacotes chegam e partem ao mesmo tempo. Você também não pode supor que a fila muda de vazia para um pacote e que a fila permanece em um pacote com base em uma hora de chegada consistente de entrada/saída. Se

o tráfego típico estiver razoavelmente intermitente, os valores de intermitência precisarão ser correspondentemente grandes para permitir que a utilização do link seja mantida em um nível aceitavelmente alto. Um tamanho de intermitência muito baixo, ou um limite mínimo muito baixo, pode resultar em uma utilização de link inaceitavelmente baixa.

Uma intermitência pode ser definida simplesmente como uma série de quadros de tamanho MTU back-to-back, como quadros de 1.500 bytes originados em uma rede Ethernet. Quando uma intermitência desses quadros chega a uma interface de saída, ela pode sobrecarregar os buffers de saída e exceder a profundidade configurada do token bucket em um momento instantâneo. Com o uso de um sistema de medição de token, um vigilante toma uma decisão binária sobre se um pacote de chegada está em conformidade, excede ou viola os valores de vigilância configurados. Com o tráfego em surtos, como um fluxo FTP, a taxa de chegada instantânea desses pacotes pode exceder os valores de intermitência configurados e levar a quedas de CAR.

Além disso, o throughput geral em tempos de congestionamento varia com o tipo de tráfego que é avaliado pelo vigilante. Embora o tráfego TCP seja responsivo ao congestionamento, outros fluxos não são. Exemplos de fluxos não responsivos incluem pacotes baseados em UDP e baseados em ICMP.

O TCP é baseado em reconhecimento positivo com retransmissão. O TCP usa uma janela móvel como parte de seu mecanismo de confirmação positiva. Os protocolos de janelas móveis usam melhor a largura de banda da rede porque permitem que o remetente transmita vários pacotes antes de esperar por uma confirmação. Por exemplo, em um protocolo de janela móvel com tamanho de janela 8, o remetente tem permissão para transmitir 8 pacotes antes de receber uma confirmação. Se você aumentar o tamanho da janela, o tempo ocioso da rede será eliminado em grande parte. Um protocolo de janela móvel bem ajustado mantém a rede completamente saturada com pacotes e mantém um alto throughput.

Como os endpoints não sabem o status de congestionamento específico da rede, o TCP como um protocolo é projetado para reagir ao congestionamento na rede pela redução de suas taxas de transmissão quando ocorre congestionamento. Especificamente, usa duas técnicas:

Técnica	Descrição
Prevenção de aumento de congestionamento multiaplicativo.	Após a perda de um segmento (o equivalente de um pacote ao TCP), reduza a janela de congestionamento pela metade. A janela de congestionamento é um segundo valor ou janela que é usado para limitar o número de pacotes que um remetente pode transmitir para a rede antes de esperar por uma confirmação.
Recuperação de início lento	Quando você iniciar o tráfego em uma nova conexão ou aumentar o tráfego após um período de congestionamento, inicie a janela de congestionamento no tamanho de um único segmento e aumente a janela de congestionamento em um segmento cada vez que uma confirmação chegar. O TCP inicializa a janela de congestionamento para 1, envia um segmento inicial e espera. Quando a confirmação chega, aumenta a janela de congestionamento para 2, envia

	dois segmentos e espera. Para obter mais detalhes, consulte RFC 2001 .

Os pacotes podem ser perdidos ou destruídos quando erros de transmissão interferem nos dados, quando o hardware da rede falha ou quando as redes se tornam muito carregadas para acomodar a carga apresentada. O TCP supõe que pacotes perdidos, ou pacotes que falham em ser confirmados dentro do intervalo temporizado devido a um atraso extremo, indicam congestionamento na rede.

O sistema de medição de token-bucket de um vigilante é chamado em cada chegada de pacote. Especificamente, a taxa de conformação e a taxa de excedência são calculadas com base nesta fórmula simples:

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

Como a fórmula calcula as taxas em um período desde a última vez em que os contadores foram zerados, a Cisco recomenda limpar os contadores para monitorar a taxa atual. Se os contadores não forem zerados, a taxa de fórmula anterior efetivamente significa que a saída do comando **show** exibe uma média calculada em um período potencialmente muito longo, e os valores possivelmente não são significativos na determinação da taxa atual.

O throughput médio deve corresponder à taxa de informação comprometida (CIR) configurada durante um período. Os tamanhos de intermitência permitem uma duração máxima de intermitência em um determinado momento. Se não houver tráfego ou menos do que o valor do tráfego da CIR e o token bucket não for preenchido, uma intermitência muito grande ainda será limitada a um tamanho específico calculado com base na intermitência normal e na intermitência estendida.

A taxa de queda resulta desse mecanismo

1. Observe o tempo atual.
2. Atualize o token bucket com o número de tokens que foram acumulados continuamente desde a última vez que um pacote chegou.
3. O número total de tokens acumulados não pode exceder o valor máximo. Descartar tokens em excesso.
4. Verifique a conformação de pacotes.

A limitação de taxa também pode ser alcançada com o policiamento. Esta é uma configuração de exemplo para fornecer limitação de taxa na interface Ethernet que usa vigilância baseada em classe.

```
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
```

Este exemplo de saída do comando show policy-map interface ilustra os valores corretamente calculados e sincronizados para a taxa oferecida e a taxa de queda, bem como as taxas de bps conformadas e excedidas.

```
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
```

Problemas conhecidos com CAR e contadores de vigilância baseados em classe

Esta tabela lista os problemas resolvidos com os contadores exibidos nos comandos **show policy-map** ou **show interface rate-limit**. Os clientes registrados que estão conectados podem exibir as informações de bug na Bug Search Tool.

Sintoma	IDs de bug e alternativas resolvidas

Contadores de queda inferiores ao esperado	• ID de bug da Cisco CSCdv41231 (somente clientes registrados)Quando uma política de serviço hierárquico de entrada usa o comando **police** nos níveis pai e filho, o vigilante pode descartar menos do que o número esperado de pacotes, já que o vigilante de nível pai deve estar congestionado antes de descartar os pacotes. Este é um exemplo dessa política:
	`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 Como solução alternativa, crie políticas separadas e aplique uma na entrada e outra na saída para evitar a configuração de uma política hierárquica.
Dobre a taxa esperada de quedas e throughput.	• ID de bug da Cisco CSCds23924 (somente clientes registrados)O Cisco Express Forwarding (CEF) define um mecanismo de switching do IOS que encaminha pacotes de entrada para a interface de saída. Antes das alterações implementadas a partir dessa ID de bug, o CEF e os mecanismos de QoS configurados, como CAR ou vigilância baseada em classe, incrementavam os contadores de pacote. O resultado é a chamada contabilidade dupla, pacotes conformados inflados e valores de queda em excesso. • ID de bug da Cisco CSCdr40598 (somente clientes registrados)Na série Cisco 12000, quando o CAR de saída é ativado e a placa de linha de entrada é Engine 2, os contadores de saída de saída são duplicados. Essa contabilidade dupla resulta de como os contadores de saída são tratados. • ID de bug da Cisco CSCdv84259 (somente clientes registrados)Se você habilitar globalmente o comando **ip cef distribute** em um roteador da série Cisco 7500, uma interface de placa VIP (processador de interface não versátil) será exibida com o comando **ip route-cache distribution** habilitado por padrão. Não-VIPs não suportam CEF distribuído, e um efeito colateral raro desse comando que aparece em não-VIPs é a contabilidade dupla.
Nenhuma queda ou uma taxa de queda	Em geral, quando você aplica recursos de QoS baseados em classe, a primeira etapa na solução de problemas é garantir que o mecanismo de classificação de QoS funcione corretamente. Em outras palavras, certifique-se de que os pacotes especificados nas instruções de correspondência em seu mapa de classe atinjam as classes corretas.

<table>
<tr>
<td>em zero</td>
<td>
<pre>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</pre>

ID de bug da Cisco CSCds34478 (somente clientes registrados)A classificação falha quando o CEF, e não o DCEF, é ativado e uma política de entrada é anexada a um ATM PVC. No Cisco IOS Software Release 12.1T, a classificação de saída falha quando o CEF, e não o DCEF, está ativado e uma política de saída é anexada a um ATM PVC.

</td>
</tr>
<tr>
<td>Taxa de queda anômala ou inconsistente</td>
<td>

ID de bug da Cisco CSCdw50583 (somente clientes registrados)A taxa de queda exibida no mapa de classes não corresponde às taxas de queda indicadas pela ação policial. Neste exemplo de saída, a taxa de queda para a classe é de 745000 bps, enquanto a taxa de queda mostrada pela ação policial é de 1072000 bps.
<pre>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</pre>

</td>
</tr>
</table>

	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

Informações Relacionadas

- Configurando Taxa de Acesso Comprometida
- Vigilância com CAR
- Usando CAR durante ataques de DOS
- Página de suporte à tecnologia QoS
- Página de suporte aos protocolos de roteamento IP
- Página de Suporte do IP Routing
- Suporte Técnico e Documentação - Cisco Systems