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

Índice

Introdução

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 porque a saída do **comando show interface x/x rate-limit** mostra um valor `excedido diferente de zero bps` quando o valor `conformado bps` é menos do que a taxa de informação comprometida configurada (CIR).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Convenções

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 circunstâncias em que você pode ver que diferente de zero excedido avalia na saída deste comando:

- Os valores de intermitência são ajustados demasiado baixos para reservar uma suficiente taxa de throughput. Por exemplo, veja a identificação de bug Cisco CSCdw42923 (clientes registrados somente) no Bug Toolkit, ligado da página das ferramentas e utilitário (clientes registrados somente).**Nota:** Você deve ser um usuário registrado e entrado a fim usar o Bug Toolkit.
- Questão solucionada com contabilidade dupla no software de Cisco IOS®
- Bug de Software no Cisco IOS

Olhe as saídas de exemplo de uma interface de acesso virtual. Nesta configuração, o RAIO é usado a fim atribuir um limite de taxa à interface de acesso virtual dinamicamente criada.

```
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 a fim monitorar o desempenho do vigilante do legado Cisco, CAR. Neste exemplo, a saída deste comando fornece sugestões a respeito de porque há uns bps excedidos diferente de zero. O valor de intermitência atual é 7392 bytes, quando o valor do (Bc) do committed burst, indicado pelo valor-limite, for ajustado a 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
```

Quando você configura o CAR ou um vigilante mais novo de Cisco, class-based policing, você deve configurar suficientemente valores de alta intermitência a fim assegurar esperou a taxa de transferência e a fim assegurar-se de que os pacotes de quedas de policer para punir somente a congestão a curto prazo.

Quando você seleciona valores de intermitência, é importante acomodar aumentos transientes no tamanho da fila. Você não pode simplesmente supor que os pacotes chegam e partem ao mesmo tempo. Você igualmente não pode supor que a fila muda de vazio a um pacote e que a fila permanece em um pacote baseado em um um tempo de chegada consistente in/one para fora. Se o tráfego típico é razoavelmente intermitência, a seguir os valores de intermitência precisam de ser correspondentemente grandes a fim permitir que a utilização do enlace esteja mantida aceitavelmente em um nível alto. Um tamanho de intermitência que seja demasiado baixo, ou um limiar mínimo que seja demasiado baixo, podem conduzir à utilização do enlace inaceitavelmente baixa.

Uma explosão pode ser definida simplesmente enquanto uma série de lado a lado, quadros do

tamanho MTU, tais como os quadros 1500-byte que originam em uma rede Ethernet. Quando uma explosão de tais quadros chega em uma interface de saída, pode oprimir os bufferes de saída e exceder a profundidade configurada do Token Bucket em um momento instantâneo a tempo. Com o uso de um sistema de medição simbólico, um vigilante faz uma decisão binária sobre se um pacote chegando se conforma, se excede, ou se viola os valores de policiamento configurados. Com tráfego intermitente, tal como um córrego FTP, a taxa de chegada instantânea destes pacotes pode exceder os valores da intermitência configurada e conduzi-los às gotas CAR.

Além, o throughput geral em período da congestão varia com o tipo de tráfego que é avaliado pelo vigilante. Quando o tráfego TCP for responsivo à congestão, outros fluxos não são. Os exemplos de fluxos NON-responsivos incluem pacotes UDP-baseados e ICMP-baseados.

O TCP é baseado no reconhecimento positivo com retransmissão. O TCP usa um indicador de deslizamento como parte de seu mecanismo do reconhecimento positivo. Largura de banda de rede do uso dos protocolos de janela de rolagem melhor porque permitem que o remetente transmita pacotes múltiplos antes que esperarem um reconhecimento. Por exemplo, em um protocolo de janela de rolagem com um tamanho de janela de 8, o remetente está permitido para transmitir 8 pacotes antes que receba um reconhecimento. Se você aumenta o tamanho de janela, o tempo ocioso da rede está eliminado pela maior parte. Um protocolo de janela de rolagem bem-ajustado mantém a rede saturada completamente com os pacotes e mantém o throughput elevado.

Desde que os valores-limite não conhecem o status de congestionamento específico da rede, o TCP como um protocolo está projetado reage à congestão na rede pela redução suas taxas de transmissão quando a congestão ocorre. Especificamente, usa duas técnicas:

Técnica	Descrição
Prevenção de aumento de congestionamento multiaplicativo.	Em cima da 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 indicador que sejam usados para limitar o número de pacotes que um remetente pode transmitir na rede antes que espere um reconhecimento.
Recuperação de início lento	Quando você começa o tráfego em uma nova conexão ou aumenta o tráfego após um período de congestionamento, ligue a janela de congestionamento no tamanho de um único segmento e aumente a janela de congestionamento por um segmento cada vez que um reconhecimento chega. O TCP inicializa a janela de congestionamento a 1, envia um segmento inicial, e espera. Quando o reconhecimento chega, aumenta a janela de congestionamento a 2, envia dois segmentos, e espera. Para mais detalhes, veja o RFC 2001 .

Os pacotes podem ser perdidos ou destruído quando os erros de transmissão interferem com os dados, quando o hardware de rede falha, ou quando as redes se tornam carregadas demasiado

pesadamente para acomodar a carga apresentada. O TCP supõe que os pacotes perdidos, ou os pacotes que não reconhecem dentro do intervalo programado devido ao atraso extremo, indicam a congestão na rede.

O sistema de medição do token bucket de um vigilante é invocado em cada chegada de pacote. Especificamente, a taxa conformada e excede a taxa é calculada com base nesta fórmula simples:

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

Desde que a fórmula calcula taxas durante um período da última vez que os contadores estiveram cancelados, Cisco recomenda cancelar os contadores a fim monitorar a taxa atual. Se os contadores não são cancelados, a seguir a taxa da fórmula anterior significa eficazmente que o **show command output (resultado do comando show)** indica uma média calculada durante potencialmente muito um período longo, e os valores não são possivelmente significativos na determinação da taxa atual.

A taxa de transferência média deve combinar a taxa de informação comprometida configurada (CIR) durante um período de tempo. Os tamanhos de intermitência permitem uma duração da lintermitência máxima em um dado momento. Se há um sem tráfego ou menos do que o valor do CIR do tráfego e do Token Bucket não enche, uma explosão muito grande está limitada ainda a um tamanho particular calculado com base na explosão e na intermitência extendida do normal.

Os resultados da taxa da gota deste mecanismo

1. Observe o tempo atual.
2. Atualize o Token Bucket com o número de tokens que acumularam continuamente desde a última vez onde um pacote chegou.
3. O número total de tokens acumulados não pode exceder o valor dos maxtokens. Tokens do excesso da gota.
4. Verifique a conformação de pacotes.

A taxa limite pode igualmente ser conseguida com policiamento. Esta é uma configuração de exemplo a fim fornecer a taxa limite na interface Ethernet que usa o policiamento baseado 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 calculado corretamente e os valores sincronizados para a taxa oferecida e a gota avaliam assim como conformaram-se e excedem taxas 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
```

Problemas conhecidos com CAR e contadores de vigilância baseado em classe

Esta tabela alista questões solucionadas com os contadores indicados nos **comandos show policy-map or show interface rate-limit**. Os clientes registrados que são entrados podem ver a informação do bug no Bug Toolkit, ligado da página das ferramentas e utilitário (clientes registrados somente).

Sintoma	Erro resolved ID e ações alternativas

Abaixe do que contadores de queda previstos	• Identificação de bug Cisco CSCdv41231 (clientes registrados somente)
	Quando uma política de serviços hierárquica da entrada usa o **comando police** a níveis do pai e da criança, o vigilante pode deixar cair menos do que o número esperado de pacotes desde que o vigilante do pai-nível deve ser congestionado antes que deixe cair os pacotes. Este é um exemplo de tal 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 uma ação alternativa, crie políticas separadas e aplique um em de entrada e um em de partida a fim evitar a configuração de uma política hierárquica.

Dobre a taxa esperada de quedas e throughput.	• Identificação de bug Cisco CSCds23924 (clientes registrados somente) O Cisco Express Forwarding (CEF) define um mecanismo do IOS switching que para a frente pacotes da entrada à interface de saída. Antes das mudanças executadas deste Bug ID, o CEF e os mecanismos de QoS configurados tais como o CAR ou o class-based policing incrementaram os contadores de pacote de informação. O resultado é contabilidade dupla assim chamada e valores conformados inflados do pacote e os adicionais da gota. • Identificação de bug Cisco CSCdr40598 (clientes registrados somente) No Cisco 12000 Series, quando a saída CAR é permitida e a placa de linha do ingresso é Engine 2, os contadores de emissor da saída são dobrados. Esta contabilidade dupla resulta de

	como os contadores de emissor são segurados. • Identificação de bug Cisco CSCdv84259 (clientes registrados somente) Se você permite globalmente o **comando ip cef distributed em um** Cisco 7500 Series Router, uma relação NON-versátil do cartão do processador de interface (VIP) aparece com o **comando ip route-cache distributed** permitido à revelia. Os NON-VIP não apoiam o CEF distribuído, e um efeito colateral raro deste comando que aparece em NON-VIP é contabilidade dupla.
Nenhuma queda ou uma taxa de queda em zero	Geralmente, quando você aplica características de QoS classe-baseadas, a primeira etapa no Troubleshooting é assegurar-se de que o mecanismo da classificação de QoS trabalhe corretamente. Ou seja assegure-se de que os pacotes especificados nas instruções compatível em seu mapa de classe batam as classes corretas. `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` • Identificação de bug Cisco CSCds34478 (clientes registrados somente) A classificação falha quando o CEF, e não o DCEF, são permitidos e uma política de entrada está anexada a um ATM PVC. No Cisco IOS Software Release 12.1T, a classificação de emissor falha quando o CEF, e não o DCEF, são permitidos e uma política emissora está anexada a um ATM PVC.
Taxa anômala ou incompatível da gota	• Identificação de bug Cisco CSCdw50583 (clientes registrados somente) A taxa da gota indicada no mapa de classe não combina as taxas da gota indicadas pela ação policial. Nestas saídas de exemplo, a taxa da gota para a classe é 745000 bps, quando a taxa da gota mostrada pela ação policial for 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

Informações Relacionadas

- Configurando Taxa de Acesso Comprometida
- Policiamento com CAR
- Usando CAR durante ataques de DOS
- Página de suporte da tecnologia de QoS
- Página de suporte dos protocolos roteados de IP
- Página de Suporte do IP Routing
- Suporte Técnico e Documentação - Cisco Systems