Introducción a los Contadores de paquetes en el resultado del comando show interface rate con Velocidad de acceso comprometida (CAR)

Contenido

Introducción

Committed Access Rate (CAR) es una función de limitación de la tarifa que se puede utilizar para proporcionar servicios de Clasificación y Regulación. CAR se puede utilizar para clasificar paquetes en función de ciertos criterios, tales como dirección IP y los valores de puerto que utilizan listas de acceso. Se puede definir la acción para los paquetes que se ajustan al valor del límite de velocidad y los que exceden el valor. Consulte Configuración de la velocidad de acceso comprometida para obtener más información sobre cómo configurar CAR.

Este documento explica por qué la salida del comando **show interface x/x rate-limit** muestra un valor `non-zero overded bps` cuando el valor de `conformado bps` es menor que la velocidad de información comprometida (CIR) configurada.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Comprensión de la salida del comando show interface rate

Hay tres condiciones en las que puede ver tasas excedidas no nulas en el resultado de este comando:

- Los valores de ráfaga se establecen demasiado bajos para permitir una velocidad de rendimiento suficiente. Por ejemplo, vea Cisco bug ID CSCdw42923 (sólo clientes registrados).
- Problema resuelto con contabilidad doble en el software Cisco IOS®
- bug de software en Cisco IOS

Observe el ejemplo de resultado de una interfaz de acceso virtual. En esta configuración, RADIUS se utiliza para asignar un límite de velocidad a la interfaz de acceso virtual creada dinámicamente.

```
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",
```

Utilice el comando show interface x rate-limit para monitorear el rendimiento del regulador de tráfico heredado de Cisco, CAR. En este ejemplo, el resultado de este comando proporciona sugerencias sobre por qué hay un bps excedido distinto de cero. El valor de ráfaga actual es 7392 bytes, mientras que el valor de ráfaga comprometida (Bc), indicado por el valor límite, se establece en 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
```

Cuando configura CAR o un regulador más nuevo de Cisco, la regulación basada en clase, debe configurar valores de ráfaga suficientemente altos para asegurar el rendimiento esperado y para asegurarse de que el regulador descarte paquetes solamente para castigar la congestión a corto plazo.

Cuando selecciona valores de ráfaga, es importante dar cabida a aumentos transitorios en el tamaño de la cola. No puede asumir simplemente que los paquetes llegan y salen al mismo

tiempo. Tampoco puede asumir que la cola cambia de vacío a un paquete y que la cola permanece en un paquete basado en un tiempo de llegada uno adentro/uno afuera consistente. Si el tráfico típico está bastante agitado, los valores de ráfaga deben ser proporcionalmente grandes para permitir que la utilización del link se mantenga en un nivel aceptablemente alto. Un tamaño de ráfaga demasiado bajo, o un umbral mínimo demasiado bajo, puede resultar en una utilización de links inaceptablemente baja.

Una ráfaga se puede definir simplemente como una serie de tramas adosadas de tamaño MTU, como tramas de 1500 bytes que se originan en una red Ethernet. Cuando una ráfaga de tales tramas llega a una interfaz de salida, puede saturar las memorias intermedias de salida y exceder la profundidad configurada de la cubeta con ficha en un momento instantáneo en el tiempo. Con el uso de un sistema de medición de tokens, un regulador toma una decisión binaria sobre si un paquete que llega cumple, excede o viola los valores de regulación de tráfico configurados. Con el tráfico en ráfaga, como un flujo FTP, la velocidad de llegada instantánea de estos paquetes puede exceder los valores de ráfaga configurados y conducir a descartes de CAR.

Además, el rendimiento total en tiempos de congestión varía según el tipo de tráfico que evalúa el regulador. Mientras que el tráfico TCP responde a la congestión, otros flujos no lo son. Algunos ejemplos de flujos que no responden incluyen paquetes basados en UDP e ICMP.

TCP se basa en un reconocimiento positivo con retransmisión. TCP utiliza una ventana deslizante como parte de su mecanismo de reconocimiento positivo. Los protocolos de ventana deslizante utilizan mejor el ancho de banda de la red porque permiten al remitente transmitir varios paquetes antes de esperar a que se acuse de recibo. Por ejemplo, en un protocolo de ventana deslizante con un tamaño de ventana de 8, se permite al remitente transmitir 8 paquetes antes de recibir una confirmación. Si aumenta el tamaño de la ventana, el tiempo de inactividad de la red se elimina en gran medida. Un protocolo de ventana deslizante bien adaptado mantiene la red completamente saturada con paquetes y mantiene un alto rendimiento.

Dado que los terminales no conocen el estado de congestión específico de la red, el TCP como protocolo está diseñado reacciona ante la congestión en la red mediante la reducción de sus tasas de transmisión cuando se produce la congestión. Específicamente, utiliza dos técnicas:

Técnica	Descripción
Prevención de congestión de disminución multiplicativa.	Al perder un segmento (el equivalente de un paquete a TCP), reduzca la ventana de congestión a la mitad. La ventana de congestión es un segundo valor o ventana que se utiliza para limitar el número de paquetes que un remitente puede transmitir a la red antes de esperar a un reconocimiento.
Recuperación de arranque lento	Cuando inicia el tráfico en una nueva conexión o aumenta el tráfico después de un período de congestión, inicie la ventana de congestión al tamaño de un solo segmento y aumente la ventana de congestión en un segmento cada vez que llega un reconocimiento. TCP inicializa la ventana de congestión en 1, envía un segmento inicial y espera. Cuando llega el reconocimiento, aumenta la ventana de

	congestión a 2, envía dos segmentos y espera. Para obtener más detalles, vea RFC 2001 .

Los paquetes se pueden perder o destruir cuando los errores de transmisión interfieren con los datos, cuando falla el hardware de la red o cuando las redes se sobrecargan demasiado para acomodar la carga presentada. TCP asume que los paquetes perdidos, o los paquetes que no se reconocen dentro del intervalo de tiempo debido a un retraso extremo, indican congestión en la red.

El sistema de medición de cubeta con ficha de un regulador se invoca en cada llegada de paquetes. Específicamente, la tasa conformada y la tasa de excedente se calculan en base a esta simple fórmula:

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

Puesto que la fórmula calcula las tasas durante un período desde la última vez que se borraron los contadores, Cisco recomienda borrar los contadores para monitorear la velocidad actual. Si los contadores no se borran, entonces la velocidad de fórmula anterior significa efectivamente que el resultado del comando **show** muestra un promedio calculado durante un período potencialmente muy largo, y los valores posiblemente no son significativos en la determinación de la velocidad actual.

El rendimiento promedio debe coincidir con la velocidad de información comprometida (CIR) configurada durante un período de tiempo. Los tamaños de ráfaga permiten una duración máxima de ráfaga en un momento dado. Si no hay tráfico o es inferior al valor de tráfico de la CIR y la cubeta con ficha no se llena, una ráfaga muy grande se sigue limitando a un tamaño particular calculado sobre la base de ráfaga normal y ráfaga extendida.

La tasa de caída se obtiene de este mecanismo

1. Tenga en cuenta la hora actual.
2. Actualice la cubeta con fichas con el número de tokens que se han acumulado continuamente desde la última vez que llegó un paquete.
3. El número total de tokens acumulados no puede exceder el valor maxtokens. Suelte los tokens sobrantes.
4. Verifique la conformidad de los paquetes.

La limitación de velocidad también se puede lograr con la regulación de tráfico. Ésta es una configuración de ejemplo para proporcionar limitación de velocidad en la interfaz Ethernet que utiliza regulación basada en clase.

```
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 ejemplo de salida del comando show policy-map interface ilustra valores correctamente calculados y sincronizados para la velocidad y velocidad de descarte ofrecidas, así como las tasas de bps conformadas y superiores.

```
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 Conocidos de CAR y Contadores de Regulación Basada en Clases

Esta tabla enumera los problemas resueltos con los contadores mostrados en los comandos **show policy-map** o **show interface rate-limit**. Los clientes registrados que han iniciado sesión pueden ver la información de error en la Herramienta de búsqueda de errores.

Síntoma	Errores de ID y soluciones resueltos

Contadores de caídas inferiores a los esperados	• Id. de error de Cisco CSCdv41231 (sólo clientes registrados)Cuando una política de servicio jerárquica de entrada utiliza el comando **police** en los niveles primario y secundario, el regulador puede descartar menos de la cantidad esperada de paquetes, ya que el regulador de nivel primario debe estar congestionado antes de descartar los paquetes. Este es un ejemplo 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 solución alternativa, cree políticas separadas y aplique una en el entrante y otra en el saliente para evitar la configuración de una política jerárquica.
Doble el índice esperado de caídas y de rendimiento	• Id. de bug Cisco CSCds23924 (sólo clientes registrados)Cisco Express Forwarding (CEF) define un mecanismo de switching de IOS que reenvía los paquetes de la interfaz de entrada a la de salida. Antes de los cambios implementados a partir de este ID de bug, los mecanismos CEF y QoS configurados como CAR o la regulación basada en clase incrementaban los contadores de paquetes. El resultado es la llamada contabilidad doble y paquetes conformados inflados y valores de descarte excesivos. • Id. de bug Cisco CSCdr40598 (sólo clientes registrados)En la serie Cisco 12000, cuando se habilita la CAR de salida y la tarjeta de línea de ingreso es el Motor 2, los contadores de salida se duplican. Esta doble contabilidad se debe a cómo se gestionan los contadores de resultados. • Id. de error de Cisco CSCdv84259 (sólo clientes registrados)Si habilita globalmente el comando **ip cef distributed** en un Cisco 7500 Series Router, aparece una interfaz de tarjeta de Procesador de interfaz no versátil (VIP) con el comando **ip route-cache distributed** habilitado de forma predeterminada. Los que no son VIP no soportan CEF distribuido, y un efecto secundario raro de este comando que aparece en los que no son VIP es la contabilidad doble.
Ausencia de caídas o velocidad de caída cero	En general, cuando aplica funciones de QoS basadas en clase, el primer paso en la solución de problemas es asegurarse de que el mecanismo de clasificación de QoS funcione correctamente. En otras palabras, asegúrese de que los paquetes especificados en las sentencias match en su mapa de clase lleguen a las clases correctas. 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. de bug Cisco CSCds34478 (sólo clientes registrados)La clasificación falla cuando CEF, y no DCEF, está habilitado y una política de entrada está conectada a un PVC ATM. En Cisco IOS Software Release 12.1T, la clasificación de salida falla cuando CEF, y no DCEF, está habilitado y una política de salida está conectada a un ATM PVC.
Tasa de caída anómala o incoherente	• Id. de error de Cisco CSCdw50583 (sólo clientes registrados)La velocidad de caída mostrada en el mapa de clase no coincide con las tasas de caída indicadas por la acción de la policía. En este resultado de ejemplo, la velocidad de caída para la clase es 745000 bps, mientras que la velocidad de caída mostrada por la acción de regulación es 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
```

Información Relacionada

- Configuración de la velocidad de acceso comprometida
- Vigilancia con CAR
- Uso de CAR durante ataques de DOS
- Página de soporte de tecnología de QoS
- Página de Soporte de IP Routed Protocols
- Página de Soporte de IP Routing
- Soporte Técnico y Documentación - Cisco Systems