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 porqué la salida del **comando show interface x/x rate-limit** muestra un valor `excedido no-cero BPS` cuando el valor `conformado BPS` es menos que la Velocidad de información comprometida (CIR) configurada.

prerrequisitos

Requisitos

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 cuales usted puede ver que no-cero excedida valora en la salida de este comando:

- Los valores de ráfaga se fijan demasiado bajos para permitir un suficiente índice de rendimiento de procesamiento. Por ejemplo, vea el Id. de bug Cisco CSCdw42923 (clientes registrados solamente) en el Bug Toolkit, conectado de la página de las Herramientas y utilidades (clientes registrados solamente).**Nota:** Usted debe ser usuario registrado y abierto una sesión para utilizar el Bug Toolkit.
- Problema resuelto con la Contabilidad doble en el software de Cisco IOS®
- Bug de software en el Cisco IOS

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

```
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 funcionamiento del policer del legado de Cisco, CAR. En este ejemplo, la salida de este comando proporciona las indirectas en cuanto a porqué hay BPS excedidos no-cero. El valor de ráfaga actual es 7392 bytes, mientras que el valor de (Bc) del committed burst, indicado por el valor límite, se fija 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
```

Cuando usted configura el CAR o un policer más nuevo de Cisco, class-based policing, usted debe configurar suficientemente los valores altos de ráfaga para asegurar contaba con la producción y para asegurarse de que el policer cae los paquetes para castigar solamente la congestión a corto plazo.

Cuando usted selecciona los valores de ráfaga, es importante acomodar los aumentos transitorios en el tamaño de la cola. Usted no puede asumir simplemente que los paquetes llegan y salen al mismo tiempo. Usted también no puede asumir que la cola cambia de vacío a un paquete y que la cola permanece en un paquete basado en una una hora de llegada constante in/one hacia fuera. Si el tráfico típico es bastante bursty, después los valores de ráfaga necesitan ser correspondientemente grandes para permitir que la utilización del vínculo sea mantenida en aceptable un nivel elevado. Un tamaño de ráfaga que es demasiado bajo, o un umbral mínimo que es demasiado bajo, puede dar lugar a la utilización del vínculo inaceptable baja.

Una explosión se puede definir simplemente mientras que una serie de bastidores continuos,

MTU clasificados, tales como tramas 1500-byte que originen en una red Ethernet. Cuando una explosión de tales bastidores llega una interfaz de salida, puede abrumar los búferes de salida y exceder la profundidad configurada del token bucket en un momento instantáneo a tiempo. Con el uso de un sistema de medición simbólico, un policer toma una decisión binaria sobre si un paquete de llegada conforma, excede, o viola los valores de vigilancia configurados. Con el tráfico congestionado, tal como una secuencia FTP, la velocidad de llegada instantánea de estos paquetes puede exceder los valores de la ráfaga configurado y llevar a los descensos CAR.

Además, el rendimiento de procesamiento general en tiempos de la congestión varía con el tipo de tráfico que es evaluado por el policer. Mientras que tráfico TCP es responsivo a la congestión, otros flujos no son. Los ejemplos de los flujos no sensibles incluyen los paquetes basados en UDP y basados en ICMP.

El TCP se basa en el reconocimiento positivo con la retransmisión. El TCP utiliza una ventana de desplazamiento como parte de su mecanismo del reconocimiento positivo. Ancho de banda de la red del uso de los Sliding Window Protocol mejor porque permiten que el remitente transmita los paquetes múltiples antes de que esperen un acuse de recibo. Por ejemplo, en un Sliding Window Protocol con un tamaño de la ventana de 8, el remitente se permite para transmitir 8 paquetes antes de que reciba un acuse de recibo. Si usted aumenta el tamaño de la ventana, el tiempo de inactividad de la red se elimina en gran parte. Un Sliding Window Protocol bien-ajustado mantiene la red saturada totalmente con los paquetes y mantiene el alto rendimiento.

Puesto que los puntos finales no conocen al estado de congestión específico de la red, el TCP como protocolo se diseña reacciona a la congestión en la red por la reducción sus velocidades de transmisión cuando ocurre la congestión. Específicamente, utiliza dos técnicas:

Técnica	Descripción
Prevención de congestión de disminución multiplicativa.	Sobre la pérdida de un segmento (el equivalente de un paquete al TCP), reduzca la ventana de congestión por la mitad. La ventana de congestión es un segundo valor o ventana que se utilizan para limitar el número de paquetes que un remitente pueda transmitir en la red antes de que espere un acuse de recibo.
Recuperación de arranque lento	Cuando usted comienza el tráfico en una nueva conexión o aumenta el tráfico después de un período de congestión, encienda la ventana de congestión en el tamaño de un solo segmento y aumente la ventana de congestión en un segmento cada vez que llega un acuse de recibo. El TCP inicializa la ventana de congestión a 1, envía un segmento inicial, y espera. Cuando llega el acuse de recibo, aumenta la ventana de congestión a 2, envía dos segmentos, y espera. Para más detalles, vea el RFC 2001 .

Los paquetes pueden ser perdidos o ser destruidos cuando los errores de transmisión interfieren con los datos, cuando el hardware de red falla, o cuando las redes se cargan demasiado pesadamente para acomodar la carga presentada. El TCP asume que los paquetes perdidos, o

los paquetes que no pueden ser reconocidos dentro del intervalo temporizado debido al retardo extremo, indican la congestión en la red.

El sistema de medición de la cubeta con ficha de un policer se invoca en cada llegada de paquete. Específicamente, la tarifa conformada y excede la tarifa se calcula sobre la base de esta fórmula simple:

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

Puesto que la fórmula calcula las tarifas durante un período a partir de la última vez que los contadores fueron borrados, Cisco recomienda borrar los contadores para monitorear la velocidad actual. Si los contadores no se borran, después la tarifa de la fórmula anterior significa con eficacia que la **salida del comando show** visualiza una media calculada durante potencialmente mismo un período prolongado, y los valores no son posiblemente significativos en la determinación de la velocidad actual.

La producción media debe hacer juego la Velocidad de información comprometida (CIR) configurada durante un período de tiempo. Los tamaños de ráfaga permiten una duración de la ráfaga máxima en un momento dado. Si no hay tráfico o menos que el valor CIR del tráfico y del token bucket no llena, una explosión muy grande todavía se limita a un tamaño determinado calculado sobre la base de la explosión normal y de la ráfaga ampliada.

Los resultados de la tarifa del descenso de este mecanismo

1. Tenga en cuenta la hora actual.
2. Ponga al día el token bucket con el número de tokens que han acumulado continuamente desde la última vez que llegó un paquete.
3. El número total de Token acumulados no puede exceder el valor de los maxtokens. Tokens del exceso del descenso.
4. Verifique la conformidad de los paquetes.

La limitación de la tarifa se puede también alcanzar con el policing. Esto es una configuración de muestra para proporcionar la limitación de la tarifa en la interfaz de Ethernet que utiliza el policing basado 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
```

Esta salida de muestra del [comando show policy-map interface](#) ilustra calculado correctamente y los valores sincronizados para la velocidad ofrecida y el descenso valoran así como conformaron y exceden las tarifas 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 Conocidos de CAR y Contadores de Regulación Basada en Clases

Esta tabla enumera los Problemas resueltos con los contadores visualizados en los **comandos show policy-map or show interface rate-limit**. Los clientes registrados se abren una sesión que pueden ver la información de bug en el Bug Toolkit, conectado de la página de las Herramientas y utilidades (clientes registrados solamente).

Síntoma	ID de bug resueltos y soluciones alternativas

Baje que los contadores de caídas previstos	• Id. de bug Cisco CSCdv41231 (clientes registrados solamente)
	Cuando una política de servicio jerárquica de la entrada utiliza el **comando police** en los niveles del padre y del niño, el policer puede caer menos que el número esperado de paquetes puesto que el policer del padre-nivel debe ser congestionado antes de que caiga los paquetes. Éste es un ejemplo de tal directiva:
	`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 las políticas diferenciados y aplique uno en entrante y uno en saliente para evitar la configuración de una política de jerarquía.

Doble el índice esperado de caídas y de rendimiento	• Id. de bug Cisco CSCds23924 (clientes registrados solamente) El Cisco Express Forwarding (CEF) define un mecanismo del IOS Switching que adelante los paquetes de la entrada a la interfaz de salida. Antes de los cambios implementados de este ID de bug, el CEF y los mecanismos de Calidad de servicio (QoS) configurados tales como CAR o el class-based policing incrementaron a los contadores de paquetes. El resultado es supuesta Contabilidad doble y de valores conformados inflados del paquete y exceso del descenso. • Id. de bug Cisco CSCdr40598 (clientes registrados solamente) En las Cisco 12000 Series, cuando se habilita la salida CAR y el linecard del ingreso es motor 2, doblan a los contadores de salida de la salida.

	Esta Contabilidad doble resulta de cómo manejan a los contadores de salida. • Id. de bug Cisco CSCdv84259 (clientes registrados solamente) Si usted global habilita el **comando ip cef distributed** en un Cisco 7500 Series Router, una interfaz NON-versátil del indicador luminoso LED amarillo de la placa muestra gravedad menor del procesador de interfaz (VIP) aparece con el **comando ip route-cache distributed** habilitado por abandono. Los NON-VIP no soportan el CEF distribuido, y a efecto colateral poco común de este comando que aparezca en los NON-VIP es Contabilidad doble.
Ausencia de caídas o velocidad de caída cero	Generalmente cuando usted aplica las características basadas en la clase de QoS, el primer paso en el troubleshooting es asegurarse de que el mecanismo de la clasificación de QoS trabaja correctamente. Es decir asegúrese de que los paquetes especificados en las declaraciones de coincidencia en su clase-mapa golpeen 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 (clientes registrados solamente) La clasificación falla cuando se habilita el CEF, y no el DCEF, y una política de entrada se asocia a una atmósfera PVC. En el Cisco IOS Software Release 12.1T, la clasificación de resultados falla cuando se habilita el CEF, y no el DCEF, y una política de resultado se asocia a una atmósfera PVC.
Tarifa anómala o contraria del descenso	• Id. de bug Cisco CSCdw50583 (clientes registrados solamente) La tarifa del descenso visualizada en el clase-mapa no hace juego las tarifas del descenso indicadas por la acción policial. En esta salida de ejemplo, la tarifa del descenso para la clase es 745000 BPS, mientras que la tarifa del descenso mostrada por la acción policial 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
- Policing con el CAR
- Uso de CAR durante ataques de DOS
- Página de soporte de la tecnología de calidad de servicio
- Página de Soporte de IP Routed Protocols
- Página de Soporte de IP Routing
- Soporte Técnico y Documentación - Cisco Systems