Preguntas frecuentes - Caídas de salida en los switches Catalyst de Cisco serie 9000

Introducción

Este documento proporciona respuestas a preguntas comunes sobre caídas de salida en los switches Catalyst de Cisco serie 9000.

Prerequisites

Requirements

Cisco recomienda que tenga una comprensión fundamental de los conceptos de switching, incluidas las configuraciones de almacenamiento en búfer de la interfaz y de calidad de servicio (QoS).

Componentes Utilizados

Este documento se aplica a todos los switches Catalyst de Cisco serie 9000 y no se limita a versiones específicas de hardware o software.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Las caídas de salida ocurren cuando se agota un búfer de salida de interfaz, lo que resulta en la pérdida de paquetes y el rendimiento de red degradado. Entre las causas habituales se incluyen la congestión de la red, las microrráfagas de tráfico, los errores de configuración o las limitaciones de hardware. Este documento de preguntas frecuentes responde a preguntas comunes sobre caídas de salida en los switches Catalyst de Cisco serie 9000. Proporciona orientación para identificar las causas principales, metodologías de solución de problemas y prácticas

recomendadas para restaurar la eficacia y la fiabilidad de la red.

P. ¿Qué son las caídas de salida?

R. Las caídas de salida en los switches Cisco Catalyst 9000 se refieren al número de paquetes que se descartan y no se transmiten fuera de una interfaz, aunque los paquetes hayan sido procesados por el dispositivo. Esto ocurre cuando la cola de salida de la interfaz se llena. La interfaz del switch tiene memorias intermedias de hardware que almacenan temporalmente los paquetes antes de que se transmitan o reenvíen fuera del puerto. Cuando la velocidad del tráfico saliente excede la velocidad a la que el hardware puede transmitirlo, las memorias intermedias se llenan y cualquier paquete adicional que llegue a la cola se descarta.

P. ¿Qué comando se puede utilizar para verificar caídas de salida?

R. Utilice el comando show interfaces <interface> y busque el contador de caídas de salida totales, que indica el número de paquetes caídos en la cola de salida de esa interfaz.

Ejemplo:

<#root>

```
GigabitEthernet1/0/1 is up, line protocol is up (connected)
  Input queue: 0/2000/0/0 (size/max/drops/flushes);

Total output drops: 3089


  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
```

P. ¿Cuáles son las causas comunes de las caídas de salida?

R. Las caídas de salida en los switches Catalyst 9000 generalmente ocurren cuando los paquetes se descartan antes de la transmisión debido a diversos problemas de congestión o configuración. Las causas comunes incluyen:

- Microráfagas de tráfico: Picos repentinos y de alta intensidad en el tráfico que se producen durante milisegundos. Dado que las herramientas de supervisión de red estándar (como

SNMP) sondean a intervalos de 1 o 5 minutos, estas ráfagas suelen ser invisibles para el software de gestión, pero son suficientes para agotar los búferes de salida del hardware.
- Sobresuscripción: Cuando el ancho de banda agregado del tráfico entrante excede significativamente la capacidad de la interfaz saliente, la congestión es inevitable. Esto es habitual en situaciones en las que varios puertos de alta velocidad (por ejemplo, 10 G) envían tráfico a un único puerto de menor velocidad (por ejemplo, 1 G).
- Restricciones de búfer: Cada interfaz tiene una cantidad finita de espacio de búfer de hardware. Cuando la cola de salida alcanza su capacidad máxima debido a la congestión sostenida, el switch realiza el 'descarte de cola', donde todos los paquetes entrantes subsiguientes se descartan hasta que el espacio esté disponible.
- Error de configuración de calidad de servicio (QoS): Las políticas de QoS configuradas incorrectamente (en concreto, la regulación agresiva o el modelado restrictivo) pueden provocar caídas. Si se configura una política para limitar el tráfico por debajo de la capacidad real del link, los paquetes que excedan ese umbral serán descartados incluso si el link físico no está congestionado.
- Discordancias de velocidad y dúplex: Aunque es menos común con la negociación automática moderna, una discordancia entre el puerto del switch y el dispositivo conectado puede conducir a una transmisión ineficiente, mayores colisiones (en semidúplex) y la subsiguiente saturación de la cola.
- Control de flujo (IEEE 802.3x): Si el control de flujo está habilitado, se le puede indicar al switch que detenga la transmisión por parte del dispositivo receptor. Si las tramas de pausa son frecuentes, la salida de las memorias intermedias del switch puede llenarse, lo que provoca caídas mientras el switch espera para reanudar la transmisión.
- Desequilibrio de Port-Channel: Si el tráfico en un EtherChannel/Port-Channel no se distribuye uniformemente a través de los links miembro, una interfaz puede congestionarse mientras que otras permanecen infrautilizadas.

P. ¿Qué son las microrráfagas?

R. Las microrráfagas son picos de tráfico de alta intensidad y corta duración que se producen en microsegundos o milisegundos. Causan caídas de salida al agotar instantáneamente las memorias intermedias del hardware de salida en los switches Catalyst 9000. Dado que las herramientas de supervisión estándar realizan el tráfico medio a intervalos más largos, estas ráfagas a menudo permanecen invisibles. Esto resulta en la pérdida de paquetes incluso cuando la utilización promedio de una interfaz parece estar dentro de la capacidad. En consecuencia, estos picos transitorios son una causa principal de congestión en entornos de red de alta velocidad.

P. ¿Las caídas de salida son siempre un problema?

R. No, las caídas de salida pueden ocurrir durante ráfagas de tráfico cortas incluso en redes saludables. Los switches modernos utilizan colas basadas en búfer y pueden producirse caídas

ocasionales sin afectar a las aplicaciones. Las caídas suelen ser problemáticas cuando:

- Las caídas aumentan continuamente
- Las aplicaciones experimentan latencia o pérdida de paquetes
- Aumento de retransmisiones TCP
- Las aplicaciones en tiempo real (VoIP/vídeo) se ven afectadas

P. ¿Por qué se producen caídas de salida incluso cuando la interfaz no se utiliza completamente?

R. Las caídas de salida pueden ocurrir incluso cuando la utilización de la interfaz está muy por debajo del ancho de banda máximo del link (por ejemplo, por debajo de 1000 MBPS en una interfaz Gigabit). Esto sucede porque el tráfico de red no se transmite en un flujo perfectamente fluido y continuo. En una situación ideal, cada bit se transmite uniformemente a través del link y todos los dispositivos envían tráfico a intervalos sincronizados con precisión. Sin embargo, en las redes reales, los dispositivos transmiten el tráfico siempre que lo necesitan. Como resultado, varios paquetes pueden llegar al switch al mismo tiempo y deben transmitirse a través de la misma interfaz de salida. Para manejar esta situación, los switches utilizan memorias intermedias de hardware en cada interfaz. Estas memorias intermedias almacenan temporalmente los paquetes que llegan simultáneamente para que puedan transmitirse secuencialmente a través del link. Si el volumen de paquetes que llegan a la interfaz en un momento determinado excede la capacidad de memoria intermedia disponible, el switch no puede almacenarlos todos. Cuando esto ocurre, los paquetes excedentes se descartan, lo que resulta en caídas de salida.

Esta es la razón por la que es posible observar caídas de salida incluso cuando el uso medio del ancho de banda es relativamente bajo (por ejemplo, 300 MBPS en una interfaz de 1 GBPS). La utilización media puede parecer baja, pero las ráfagas cortas de tráfico pueden exceder momentáneamente la capacidad de la interfaz para transmitir paquetes o exceder la capacidad de memoria intermedia disponible.

También es importante tener en cuenta que los valores de utilización de la interfaz que se muestran a través de las herramientas de monitoreo SNMP o el comando show interface se basan en las mediciones de tráfico promedias en intervalos tales como 30 segundos o 5 minutos. Estos promedios no reflejan picos de tráfico muy cortos que pueden ocurrir en milisegundos.

P. ¿Cómo puedo controlar las caídas de salida sin aumentar la velocidad del link?

R. Puede administrar y reducir las caídas de salida en switches Catalyst 9000 a través de varias técnicas sin actualizar la velocidad del link físico:

- Aumentar el multiplicador de SoftMax (mitigación rápida): para aumentar el número de búferes que una cola puede solicitar del conjunto de búferes compartidos, puede ajustar el umbral de SoftMax mediante el comando de configuración global qos queue-softmax-multiplier <100-1200>. El valor predeterminado es 100. Si se establece este valor en 1200, la capacidad de la cola para absorber microrráfagas se multiplica por 12 en comparación con la configuración predeterminada.

  Este comando aumenta los umbrales de cola de puerto para que la cola pueda consumir unidades de buffer adicionales del conjunto de buffer compartido cuando sea necesario. Esto se utiliza comúnmente como una técnica de mitigación rápida para reducir las caídas de salida causadas por las ráfagas de tráfico. Sin embargo, debido a que los buffers son recursos compartidos, la configuración asume que las microráfagas no ocurren simultáneamente en todos los puertos.

Modificación de búfer por cola (ajuste de política de QoS): si el multiplicador de SoftMax no es suficiente, la asignación de búfer se puede ajustar en el nivel de cola mediante mapas de política de QoS. Esto permite a los administradores asignar más espacio de búfer a clases de tráfico específicas, modificar los ratios de búfer de cola y configurar colas de prioridad para el tráfico crítico. Este enfoque es útil cuando tipos de tráfico específicos requieren recursos de búfer dedicados o cuando los perfiles de tráfico varían significativamente.

Ejemplo:

```
policy-map QOS-POLICY
 class VOICE
  priority level 1
  queue-buffers ratio 50
 class class-default
  queue-buffers ratio 50
```

- Implementación de calidad de servicio (QoS): Ayuda a controlar las caídas de paquetes priorizando el tráfico de red crítico durante los períodos de congestión. Permite a las redes dar prioridad al tráfico sensible a la latencia, como el de voz y vídeo, proteger el tráfico del plano de control y garantizar que los datos importantes se transmiten antes que el tráfico de menor prioridad. Los mecanismos de QoS típicos incluyen la clasificación del tráfico, la priorización de las colas, la asignación del búfer de las colas y la gestión de la congestión. Al aplicar estas técnicas, la red puede garantizar que el tráfico menos importante se interrumpa primero, lo que ayuda a proteger las aplicaciones vitales para la empresa y a mantener el rendimiento general de la red.

- Modelado de tráfico: configure el modelado de salida en la interfaz para suavizar las ráfagas de tráfico. Al limitar la velocidad de transmisión ligeramente por debajo de la velocidad de línea física, se fuerza el almacenamiento en búfer del tráfico y su envío a una velocidad constante y predecible. Esto evita el comportamiento de caída de cola causado por microrráfagas repentinas de alta velocidad.

Ejemplo:

```
policy-map SHAPE-POLICY
 class class-default
  shape average
```

- Optimizar la distribución de la carga (equilibrio de canal de puerto): En una configuración de EtherChannel o Port-Channel, el hashing desigual puede causar que los links de miembros específicos se congestionen mientras que otros permanecen infrautilizados. Al optimizar los algoritmos de balanceo de carga, se asegura de que el tráfico se distribuya uniformemente a través de todos los links miembro, lo que evita la congestión en las interfaces individuales y mitiga las caídas de salida.

Ejemplo:

```
port-channel load-balance src-dst-ip
```

P. ¿Cuál es la solución definitiva para caídas de salida?

R. Las soluciones más efectivas para eliminar las caídas de salida son:

- Aumentar la velocidad de la línea de interfaz: actualice la velocidad de la interfaz para proporcionar un mayor ancho de banda de salida y reducir la sobresuscripción. Por ejemplo, pase de una interfaz 1G a una interfaz 10G si está disponible en el switch.
- Usar agrupación de puertos (EtherChannel): agregue varios enlaces físicos en un único enlace lógico mediante la agrupación de puertos, siempre que el dispositivo conectado admita esta función. Esto aumenta el ancho de banda general y ayuda a distribuir la carga de tráfico.
- Actualización de hardware cuando sea necesario: si no hay disponible una interfaz de mayor velocidad en el switch y el dispositivo conectado no admite la agrupación de puertos, considere la posibilidad de actualizar la plataforma de hardware a una con mayor capacidad

o búferes más grandes.

P. ¿Cómo se pueden verificar las estadísticas de cola en una interfaz?

R. Para los switches Catalyst 9000, las estadísticas detalladas de la cola de hardware se pueden verificar usando el comando show platform hardware fed active qos queue stats interface <port>. Este comando proporciona estadísticas detalladas que incluyen el uso del búfer, los recuentos de cola y los contadores de caídas por cola en la interfaz especificada, lo que ayuda a supervisar el rendimiento de la cola e identificar la congestión o las caídas de paquetes.

Ejemplo:

<#root>

show platform hardware fed switch active qos queue stats interface Gig 1/0/1

```
DATA Port:0 Enqueue Counters
-------------------------------------------------------------------------------------------
Q Buffers          Enqueue-TH0          Enqueue-TH1          Enqueue-TH2             Qpolicer
  (Count)              (Bytes)              (Bytes)              (Bytes)              (Bytes)
- ------- -------------------- -------------------- -------------------- --------------------
0       0                    0                    0

384251797

                  0
1       0                    0                    0

488393930284

                  0
...
DATA Port:0 Drop Counters
-------------------------------------------------------------------------------------------
Q             Drop-TH0             Drop-TH1             Drop-TH2             SBufDrop
               (Bytes)              (Bytes)              (Bytes)              (Bytes)
- -------------------- -------------------- -------------------- -------------------- ----------
0                    0                    0                    0                    0
1                    0                    0

192308101

                  0                    0                    0
...
```

P. ¿Cómo confirmar si QoS está causando caídas de salida?

R. Para verificar si QoS es responsable de caídas de salida, verifique las estadísticas de política de QoS usando el comando show policy-map interface <interface> y los contadores de cola. Si los contadores de caídas aumentan bajo una clase específica de QoS, las caídas pueden ser causadas por los límites de cola o la regulación de tráfico de QoS. Si es posible, durante una ventana de mantenimiento, elimine temporalmente la política de QoS de la interfaz usando el comando no service-policy output <policy-name> y monitoree si continúan las caídas de salida. Si las caídas se detienen después de eliminar la política, es probable que la configuración de QoS esté contribuyendo a las caídas.

Ejemplo:

<#root>

```
sh policy-map interface gigabitEthernet 1/0/1


GigabitEthernet1/0/1
Service-policy output: TEST
Class-map: class-default (match-any)
0 packets
Match: any
Queueing

(total drops) 587230


(bytes output) 834545
...
```

P. ¿Se pueden producir caídas de salida en interfaces de alta velocidad como 10G o 40G?

R. Sí, incluso las interfaces de alta velocidad como 10G o 40G pueden experimentar caídas de salida cuando varios flujos de alta velocidad convergen en un único puerto, lo que provoca que los búferes de la interfaz se vean saturados. Además, las microrráfagas (ráfagas cortas de tráfico que exceden el ancho de banda de la interfaz) pueden agotar rápidamente los búferes de los puertos y provocar caídas de paquetes.

P. ¿Pueden las caídas de salida ser causadas por fallas de hardware?

R. Las caídas de salida generalmente no son causadas por fallas de hardware. Suelen ser el resultado de la congestión del tráfico, donde los búferes de la interfaz se desbordan debido a las altas velocidades de tráfico o las microrráfagas. Pueden producirse caídas relacionadas con el hardware, pero normalmente están vinculadas a condiciones de error específicas, que son poco frecuentes en comparación con las caídas relacionadas con la congestión. Por lo tanto, las caídas de salida se asocian principalmente con condiciones de tráfico de red en lugar de fallas de hardware. La supervisión de los errores de interfaz, como los errores FCS/CRC, puede ayudar a identificar los problemas de hardware si existen, pero estos son distintos de las caídas de salida causadas por la congestión.

P. ¿Pueden los errores de software causar caídas de salida?

R. Las caídas de salida causadas por defectos de software son muy raras y en su mayoría son cosméticas, y no afectan sustancialmente al tráfico. La mayoría de las caídas de salida se deben principalmente a la congestión del tráfico y al agotamiento del búfer.

P. ¿El ECMP o el balanceo de carga pueden reducir la congestión?

R. Sí, el routing de múltiples rutas de igual coste (ECMP) y el equilibrio de carga reducen la congestión distribuyendo el tráfico de forma uniforme entre varias rutas de igual coste a un destino. Este enfoque aumenta la utilización del ancho de banda e impide que cualquier ruta individual se convierta en un cuello de botella.

P. ¿Las caídas de salida afectan el tráfico UDP de manera diferente que TCP?

R. Sí, las caídas de salida afectan al tráfico UDP de manera diferente que a TCP porque UDP es un protocolo sin conexión que no retransmite los paquetes perdidos, por lo que cualquier pérdida de paquetes afecta directamente a aplicaciones como voz o vídeo, que dependen de la entrega oportuna. Por el contrario, TCP incluye mecanismos de retransmisión que intentan recuperar los paquetes perdidos, mitigando el impacto de las caídas. Por lo tanto, las caídas de salida pueden causar una degradación más notable en las aplicaciones en tiempo real basadas en UDP, ya que los paquetes perdidos no se recuperan y pueden conducir a problemas de calidad.

P. ¿Cuál es la diferencia entre las caídas de entrada y las caídas de salida?

R. Las caídas de entrada en las interfaces ocurren típicamente cuando las colas de entrada se desbordan y no pueden procesar los paquetes lo suficientemente rápido, causando el descarte selectivo de paquetes basado en el algoritmo de colocación en cola. Las caídas de salida ocurren cuando los paquetes se descartan mientras se abandona una interfaz debido a la congestión en la cola de salida o al agotamiento del búfer. Las caídas de entrada están relacionadas con los límites de procesamiento de ingreso, mientras que las caídas de salida son causadas principalmente por la congestión de egreso y el desbordamiento de buffer. Estas caídas pueden verse influidas por factores como las ráfagas de tráfico, las limitaciones de la plataforma y las configuraciones de calidad del servicio (QoS) que administran la congestión y la asignación de búfer.

P. ¿Pueden los trabajos de respaldo grandes causar caídas de salida?

R. Sí, los trabajos de copia de seguridad de gran tamaño, como las copias de seguridad de datos, la replicación o las transferencias masivas, suelen generar tráfico en ráfagas que puede saturar los búferes de interfaz, lo que provoca caídas de salida. Estas ráfagas pueden causar una congestión temporal en la interfaz de salida, especialmente cuando el ancho de banda saliente es menor que la velocidad del tráfico entrante o cuando varios flujos de alta velocidad convergen en un solo puerto.

P. ¿Cómo puedo identificar si las ráfagas de tráfico están causando caídas de salida?

R. Para confirmar caídas de salida causadas por ráfagas de tráfico, puede utilizar una sesión SPAN combinada con Wireshark para capturar y analizar el tráfico de salida en la interfaz afectada mientras se producen caídas de salida. Observe estos pasos para verificar las caídas de salida accionadas por las ráfagas de tráfico.

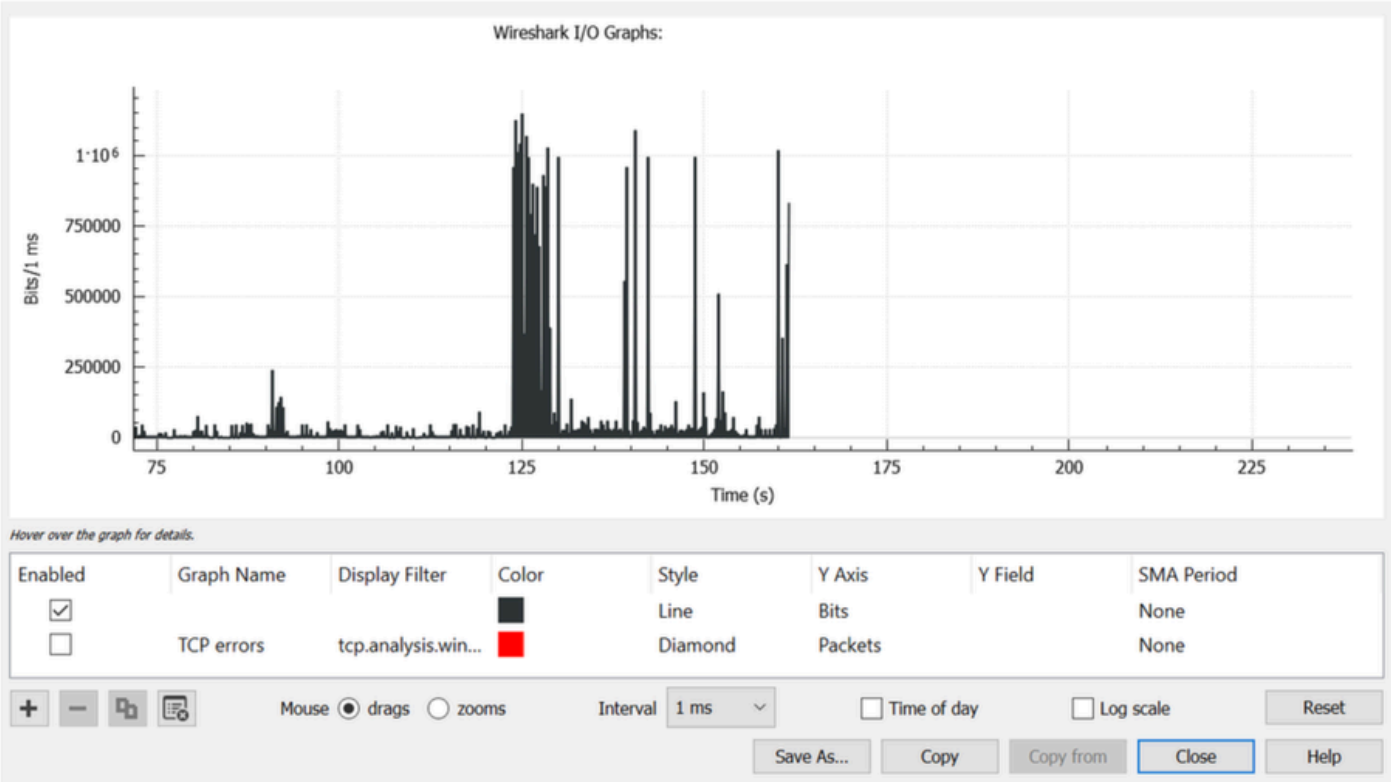
- Conecte un ordenador portátil con Wireshark instalado a un puerto no utilizado del switch.
- Configure SPAN en el switch para reflejar el tráfico de salida de la interfaz que experimenta caídas de salida en el puerto donde está conectado el portátil.

```
monitor session 1 source interface

      Tx

monitor session 1 destination interface
```

```
Replace

      with the interface where output drops are seen for the source.

Replace

      with the interface connected to the laptop for the destination.
```

- Inicie la captura de SPAN en el switch mientras las caídas de salida aumentan de forma activa para garantizar que se capture el tráfico relevante.
- Abra el archivo de captura en Wireshark y, a continuación, vaya a Statistics > I/O Graph.
- Cambie el intervalo de 1 segundo predeterminado a 1 milisegundo (1 ms).
- Haga clic en Restablecer para actualizar el gráfico con el nuevo intervalo.
- El gráfico mostrará el tráfico en bits por milisegundo.

Busque picos de tráfico que superen la velocidad de reenvío de la interfaz en una escala de milisegundos (por ejemplo, 1.000.000 bits/ms para una interfaz de 1 GBPS). Cuando el tráfico supera esta velocidad de reenvío, el switch almacena en el búfer los paquetes, lo que puede causar congestión y caídas de salida. Identifique las ráfagas de tráfico (microrráfagas) observando los picos seguidos de períodos de tráfico bajo o sin tráfico. En Wireshark, al hacer clic en un pico, se seleccionan los paquetes correspondientes, lo que permite un análisis más detallado del tráfico que desencadenó las caídas. La siguiente imagen muestra el gráfico de E/S actualizado para una interfaz que experimentó caídas de salida.



Consideraciones importantes

- Asegúrese de que los puertos de origen y destino de SPAN tengan las mismas velocidades o velocidades compatibles para evitar la introducción de caídas adicionales.
- Capture el tráfico mientras las caídas de salida aumentan de forma activa para capturar las ráfagas relevantes.
- No se recomienda la captura de paquetes integrada (EPC) para este fin, ya que limita las tasas de captura y puede perder ráfagas.

Conceptos erróneos comunes sobre caídas de salida

Concepto erróneo: Cualquier caída de salida significa que la red no funciona correctamente.

Realidad: Un pequeño número de caídas de salida es normal en redes de alta velocidad debido a microrráfagas o picos de tráfico cortos.

Concepto erróneo: Si la utilización de la interfaz es baja, no deben producirse caídas.

Realidad: La utilización se mide como un promedio en el tiempo. Las microrráfagas pueden exceder temporalmente el ancho de banda de la interfaz, causando caídas incluso cuando el uso promedio es bajo.

Concepto erróneo: Las caídas de salida significan que el hardware del switch es defectuoso.

Realidad: Las caídas de salida suelen ser causadas por congestión de tráfico o tráfico en ráfagas, no por problemas de hardware.

Concepto erróneo: El aumento de la asignación de búfer evitará todas las caídas.

Realidad: Los búferes sólo absorben ráfagas temporales. La congestión persistente seguirá dando lugar a caídas de paquetes.

Concepto erróneo: Solo las interfaces 1G experimentan caídas de salida.

Realidad: Las caídas pueden producirse en interfaces de 10 G, 25 G, 40 G o de mayor velocidad cuando las ráfagas de tráfico superan el ancho de banda o la capacidad de búfer disponibles.

Concepto erróneo: QoS debe eliminar todas las caídas y evitar la pérdida de paquetes.

Realidad: QoS da prioridad al tráfico importante, pero puede descartar de forma intencionada el tráfico de menor prioridad durante la congestión.

Concepto erróneo: Cualquier caída de salida causará un impacto en el usuario.

Realidad: Muchas aplicaciones utilizan retransmisión TCP, que puede recuperarse de caídas de paquetes ocasionales sin un impacto notable.

Concepto erróneo: Las caídas solo ocurren cuando las interfaces alcanzan una utilización del 100%.

Realidad: Las caídas pueden ocurrir durante ráfagas cortas de tráfico, incluso si la utilización media sigue siendo baja.

Concepto erróneo: La configuración de QoS es siempre la causa de las caídas.

Realidad: La mayoría de las caídas se deben a patrones de tráfico o sobresuscripción, no a políticas de QoS.

Concepto erróneo: Una red saludable nunca debe tener caídas de salida.

Realidad: En entornos de switching de alto rendimiento, se esperan caídas ocasionales y son

normales.

Guías de resolución de problemas

- Solución de problemas de caídas de salida en los switches Catalyst 9000
- Comprensión de la Asignación del Buffer de Cola en los Catalyst 9000 Switches
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).