Resolución de problemas de latencia de red y caídas de paquetes en switches Catalyst 9000

Contenido

Introducción

Este documento describe una metodología detallada para resolver problemas de latencia de red y pérdida de paquetes en los switches Catalyst de Cisco serie 9000.

Prerequisites

Requirements

Cisco recomienda tener un conocimiento fundamental de los conceptos de red, incluidos TCP/IP, VLAN y protocolos de árbol de extensión (STP). El conocimiento de los switches Catalyst de Cisco serie 9000 y la CLI de Cisco IOS® XE es fundamental. También es necesario estar familiarizado con las herramientas de supervisión de red y los privilegios de acceso para la configuración y el diagnóstico.

Componentes Utilizados

La información de este documento se basa en los switches Cisco Catalyst 9000 con todas las versiones. Este documento no se limita a ninguna versión específica de software o hardware.

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

Este documento está diseñado para ingenieros y administradores de red, y proporciona orientación para identificar, aislar y resolver estos problemas de manera eficiente en entornos de red empresariales. La latencia de red y la pérdida de paquetes pueden afectar negativamente al rendimiento y la fiabilidad en los entornos empresariales. Estos problemas a menudo son el resultado de la congestión de la red, la configuración incorrecta o factores ambientales. Los switches Catalyst de Cisco serie 9000 se han diseñado para ofrecer un alto rendimiento y resistencia. Este documento proporciona pasos de troubleshooting enfocados para ayudar a los profesionales de la red a identificar y resolver los problemas de latencia y caída de paquetes usando estos switches.

Comprensión de la latencia de red y pérdidas de paquetes

Latencia de red

La latencia de red es la medida del retraso experimentado cuando los datos atraviesan una red

desde el origen hasta el destino. Generalmente, la latencia se expresa como Tiempo de ida y vuelta (RTT), el tiempo que tarda un paquete en viajar desde el origen al destino y de regreso.

La latencia se mide normalmente en milisegundos (ms).

Impacto: La alta latencia puede degradar el rendimiento de las aplicaciones, especialmente en protocolos como TCP, que se basan en reconocimientos oportunos para enviar datos de manera eficiente.

Descartes de paquetes

Las pérdidas de paquetes se producen cuando los dispositivos de red no pueden reenviar paquetes a su destino previsto, a menudo debido a congestión, desbordamientos de búfer, configuraciones erróneas o hardware defectuoso. Las caídas de paquetes se miden normalmente como un porcentaje de paquetes perdidos durante un intervalo específico.

Impacto: las caídas de paquetes reducen el rendimiento, provocan retransmisiones y pueden afectar a la fiabilidad de las aplicaciones.

Parámetros de latencia esperados

Tipo de red	RTT típico
Misma VLAN (capa de acceso)	< 1 ms
Núcleo de campus transversal	1 - 5 ms
WAN de metro	5 - 30 ms
Internet/WAN	30 - 150 ms

Nota: La distancia geográfica entre los saltos de red puede aumentar el RTT y contribuir a una mayor latencia.

Medición de latencia de red

Empiece por conocer a fondo su red y su topología. Cuando su red está diseñada con variables deterministas y una imprevisibilidad mínima, el proceso de identificación y resolución de problemas de latencia y descarte de paquetes se vuelve significativamente más sencillo.

Normalmente, se utilizan dos herramientas principales para medir la latencia de red.

Ping

Devuelve como resultado si un destino es alcanzable junto con estadísticas sobre la pérdida de paquetes y RTT. Tan pronto como identifique los saltos problemáticos, puede intentar hacer ping entre ellos directamente y registrar los dispositivos para encontrar el problema.

<#root>

Switch#ping 8.8.8.8

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!.!!.
```

Success rate is 60 percent (3/5),

round-trip min/avg/max = 12/

15

/22 ms

<===== 2 dropped out of 5 packets, Average RTT 15 ms

Traceroute

Traceroute muestra todos los saltos en la trayectoria de ruteo desde el origen al destino junto con los resultados de RTT para cada salto. Por ejemplo, un traceroute puede mostrar en qué parte de la red (qué salto en la ruta de routing) existe o se inicia el retraso. Este ejemplo se muestra en el siguiente resultado de traceroute.

<#root>

Switch#traceroute 8.8.8.8

```
Type escape sequence to abort.
Tracing the route to 8.8.8.8

1 2 ms 2 ms 2 ms   [10.10.10.10]
2 2 ms 1 ms 1 ms   [20.20.20.20]
```

3 7 ms 45 ms 40 ms [30.30.30.30]

<===== High latency at this hop

```
4 7 ms 3 ms 1 ms   [40.40.40.40]

Note: The IP addresses shown for each hop are provided for demonstration purposes only.
```

Este resultado indica un retraso probable en el salto 3, como lo demuestra un aumento significativo en el RTT entre el salto 2 y el salto 3. La diferencia de tiempo relativamente pequeña entre el salto 3 y el salto 4 sugiere que el problema se localiza en el segmento entre 20.20.20.20 y 30.30.30.30.

Causas comunes de latencia y caídas de paquetes

Problemas de la capa 1 (capa física)

Los problemas de Capa 1 son una fuente común de latencia de red y caídas de paquetes. Es importante verificar estos aspectos en la capa física:

- Verifique que las configuraciones de dúplex y velocidad estén correctamente configuradas en todas las interfaces.
- Verifique las interfaces para CRC, los errores de entrada, que pueden indicar problemas de capa física.
- Los cables de red, las conexiones de fibra, los módulos SFP o los puertos de switch defectuosos también pueden causar retrasos y caídas de paquetes.

<#root>

```
Switch#show interface gi1/0/1

GigabitEthernet1/0/1 is up, line protocol is up
  Hardware is Gigabit Ethernet, address is 70b3.171d.c101
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,

Full-duplex, 1000Mb/s,

 media type is 10/100/1000BaseTX
  ...
  5 minute input rate 2000 bits/sec, 5 packets/sec
  5 minute output rate 3000 bits/sec, 8 packets/sec
     250000 packets input, 22000000 bytes, 0 no buffer
     Received 300 broadcasts (200 multicasts)
     0 runts, 0 giants, 0 throttles

85 input errors, 85 CRC,

 0 frame, 0 overrun, 0 ignored

<===== Input errors and CRC

     0 watchdog, 0 multicast, 0 pause input
```

```
  ...
     260000 packets output, 23000000 bytes, 0 underruns
     5 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
```

```
Switch# show interfaces counters errors

Port        Align-Err  FCS-Err    Xmit-Err  Rcv-Err  UnderSize  OutDiscards
Gi1/0/1     0          0          0         0        0          0

Gi1/0/2     0          0          0         0        0          0
...
```

Caídas de salida

Las caídas de salida ocurren cuando una cola de transmisión de una interfaz de switch está llena y no puede reenviar paquetes adicionales. Esto puede provocar un aumento de la latencia a medida que los paquetes esperan en la cola, y también puede provocar caídas de paquetes si la cola se desborda, lo que afecta al rendimiento de las aplicaciones y a la fiabilidad de la red.

<#root>

```
Switch#show interface gi1/0/1

GigabitEthernet1/0/1 is up, line protocol is up
  Hardware is Gigabit Ethernet, address is 70b3.171d.c101
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
  Full-duplex, 1000Mb/s, media type is 10/100/1000BaseTX
...
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 2d00h
  Input queue: 0/2000/0/0 (size/max/drops/flushes)
; Total output drops: 4216760900

  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 389946000 bits/sec, 84175 packets/sec
  5 minute output rate 694899000 bits/sec, 106507 packets/sec
     7885666654 packets input, 4677291827948 bytes, 0 no buffer
...
```

El contador Total output drops muestra un gran número de paquetes descartados, lo que indica congestión o desbordamiento de cola en esta interfaz. Esto puede aumentar la latencia y la

pérdida de paquetes, lo que afecta al rendimiento de la red y de las aplicaciones.

Estabilidad de STP

La inestabilidad de STP puede contribuir significativamente a la latencia de red y a las caídas de paquetes. En una red estable, los cambios de topología deben ser mínimos. Los frecuentes cambios de topología pueden indicar problemas subyacentes y pueden interrumpir las operaciones de reenvío normales.

Consideraciones clave para minimizar la latencia relacionada con STP:

Cambios de topología (TCN): Los cambios excesivos en la topología STP pueden dar lugar a un vaciado frecuente de la dirección MAC de la tabla del switch (CAM), lo que provoca un aumento del tráfico de difusión y la latencia a medida que los switches inundan los paquetes de unidifusión desconocidos hasta que la tabla se rellena de nuevo.

Configuración del puerto perimetral: Asegúrese de que todos los puertos de borde estén configurados con PortFast. La habilitación de PortFast evita que se generen notificaciones de cambio de topología (TCN) STP cuando los clientes o servidores se conectan o desconectan, lo que reduce la antigüedad innecesaria de la tabla CAM y mejora la estabilidad.

Planificación del puente raíz: Planifique y asigne manualmente el puente raíz STP y las prioridades para mantener una topología de red predecible y minimizar los cambios innecesarios en la topología.

Cuando se produce un cambio de topología (como los estados de transición de un puerto), el switch envía una TCN BPDU hacia el puente raíz. Luego, el puente raíz propaga las BPDU de TCN a todos los switches, lo que les pide que acorten el tiempo de vencimiento de sus direcciones MAC del valor predeterminado (300 segundos) al valor de Retraso de reenvío (generalmente 15 segundos). Esto hace que las entradas inactivas recientes se vacíen, lo que provoca más unidifusión desconocida y un aumento de la inundación en toda la red.

<#root>

```
Switch#show spanning-tree detail | include ieee|from|occur|is exec


VLAN0705 is executing the ieee compatible Spanning Tree protocol

Number of topology changes 6233

last change occurred 00:00:03 ago

     <===== Topology Changes



from GigabitEthernet1/0/25                                  <===== From Gi1/0/25
```

MAC Flapping/Layer 2 Loops

Los loops de Capa 2/Inestabilidad de MAC causan latencia de red y caídas de paquetes al actualizar continuamente la tabla de direcciones MAC con la misma MAC de origen en diferentes puertos. Este cambio constante interrumpe el reenvío del tráfico, lo que provoca interrupciones y pérdida de paquetes. Los loops de Capa 2 empeoran el problema al causar que los paquetes de broadcast circulen sin fin, desencadenando más inestabilidad MAC y degradando aún más el rendimiento de la red. La implementación de protocolos de prevención de loops como STP es esencial para mantener un funcionamiento estable de la red y evitar estos problemas.

Para configurar la notificación de movimiento de MAC, utilice el comando mac address-table notification mac-move en el modo de configuración global.

<#root>

Mac Flapping logs:

```
%MAC_MOVE-SW1-4-NOTIF: Host 8c45.0021.0b17 in vlan 152 is flapping between port Po2 and port Po
%MAC_MOVE-SW1-4-NOTIF: Host 8c45.0021.0b17 in vlan 152 is flapping between port Po2 and port Po
%MAC_MOVE-SW1-4-NOTIF: Host 8c45.0021.0b17 in vlan 152 is flapping between port Po1 and port Po
%MAC_MOVE-SW1-4-NOTIF: Host b0f1.ec27.69ea in vlan 154 is flapping between port Po9 and port Po
```

Control de Flujo

Cuando se habilita el control de flujo y un búfer de recepción de un puerto de switch se acerca a la capacidad, el switch envía tramas de pausa para detener temporalmente el tráfico entrante. Este proceso puede aumentar la latencia a medida que la transmisión de datos se detiene intermitentemente. Por el contrario, si el control de flujo no está habilitado o los dispositivos ascendentes no cumplen las tramas de pausa, el tráfico entrante puede exceder la capacidad del búfer, lo que resulta en desbordamientos del búfer y caídas de paquetes.

El control de flujo debe configurarse cuidadosamente, teniendo en cuenta las capacidades de todos los dispositivos en la ruta de tráfico. Un uso inadecuado o una configuración incorrecta pueden provocar un aumento de la latencia y el descarte de paquetes, lo que repercute negativamente en el rendimiento de las aplicaciones.

<#root>

Switch#show interfaces gigabitEthernet 1/0/1

```
GigabitEthernet1/0/1 is up, line protocol is up (connected)
□
```

input flow-control is on,

```
 output flow-control is unsupported
```

<===== Input Flow Control is ON

```
Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 6530
5 minute input rate 8000 bits/sec, 8 packets/sec
5 minute output rate 0 bits/sec, 0 packets/s
0 watchdog, 5014620 multicast,
1989 pause input
<===== Pause Input


0 unknown protocol drops 0 babbles, 0 late collision,
0 deferred 0 lost carrier, 0 no carrier, 0 pause output


Switch#show controllers ethernet-controller gigabitEthernet 1/0/1


Transmit        GigabitEthernet1/0/1     Receive
0 MacUnderrun frames                0 MacOverrun frames
0 Pause frames
1878 Pause frames              <===== Pause frames in RX
```

Utilización de la CPU

Un uso elevado de la CPU puede provocar una mayor latencia de red y caídas de paquetes. Cuando la CPU está muy cargada, el switch no puede procesar el tráfico del plano de control, las actualizaciones de routing ni las funciones de gestión de manera eficiente. Esto puede retrasar el reenvío de paquetes, causar tiempos de espera para protocolos como ARP o Spanning Tree, y dar lugar a paquetes perdidos, especialmente para el tráfico que requiere la intervención de la CPU.


```
Switch#show processes cpu sorted
CPU utilization for five seconds:
95%/8%;
 one minute: 92%; five minutes: 90%
<===== CPU utilization 93%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
 439     3560284      554004       6426 54.81% 55.37% 48.39%   0 SISF Main Thread


 438     2325444      675817       3440 22.67% 28.17% 27.15%   0


SISF Switcher Th
 104      548861       84846       6468 10.76%  8.17%  7.51%   0 Crimson flush tr
```

```
 119      104155      671081        155  1.21%  1.27%  1.26%   0 IOSXE-RP Punt Se
```

Utilización de memoria

El uso elevado de la memoria puede provocar latencia y caídas de paquetes al sobrecargar los procesos de la CPU y del plano de control. Esta sobrecarga retrasa la gestión de las actualizaciones de routing, las políticas de QoS y la gestión del búfer, lo que provoca una congestión en la canalización de procesamiento de paquetes. En consecuencia, los paquetes se pueden descartar o retrasar. Por lo tanto, la alta utilización de la memoria afecta al rendimiento de la red al reducir la eficacia del switch en la gestión del tráfico.

<#root>

Switch#show platform resources

```
Resource                  Usage                    Max             Warning         Critical
-------------------------------------------------------------------------------------------
Control Processor       25.00%                     100%            90%             95%
  DRAM
```

3656MB(94%)

```
            866MB           90%             95%             W
```

High memory logs:

```
%PLATFORM-4-ELEMENT_WARNING:Switch 2 R0/0: smand:  1/RP/0: Used Memory value 94% exceeds warning
%PLATFORM-4-ELEMENT_WARNING:Switch 2 R0/0: smand:  1/RP/0: Used Memory value 94% exceeds warning
%PLATFORM-4-ELEMENT_WARNING:Switch 2 R0/0: smand:  1/RP/0: Used Memory value 94% exceeds warning
```

Mensajes de Redireccionamiento y de Inalcanzable ICMP

Cuando un paquete llega a una interfaz de Capa 3 y se rutea fuera de la misma interfaz, el switch genera un mensaje de redirección ICMP para informar al origen de un salto siguiente más eficiente en la misma subred. Esto hace que el paquete original atraviese la vLAN dos veces, lo que aumenta el uso del ancho de banda. Además, el paquete de redirección ICMP consume ancho de banda y requiere procesamiento de CPU, lo que puede provocar interrupciones de la CPU y un aumento de la latencia. Si se producen muchas de estas redirecciones, especialmente durante el tráfico intenso, la carga de la CPU puede aumentar significativamente, lo que puede provocar caídas de paquetes.

La generación y el procesamiento frecuentes de mensajes ICMP inalcanzables también pueden aumentar la utilización de la CPU, lo que afecta al rendimiento de la red. Los altos volúmenes de tráfico ICMP inalcanzable consumen recursos de la CPU, lo que puede conducir a la latencia y a la caída de paquetes.

Para mitigar estos efectos, Cisco recomienda inhabilitar los mensajes de ICMP inalcanzable y los redireccionamientos de ICMP en las interfaces virtuales del switch (SVI) y las interfaces de Capa 3 mediante los comandos no ip unreachables y no ip redirects. Esta práctica recomendada reduce la carga de la CPU y mejora la estabilidad de la red.

<#root>

Switch#show ip traffic | in unreachable

```
...
  Rcvd: 194943 format errors, 369707 checksum errors,
3130 redirects,
734412 unreachable

  Sent: 29265 redirects, 14015958 unreachable, 196823 echo, 786959149 echo reply
...
```

Switch#show platform hardware fed active qos queue stats internal cpu policer

```
           CPU Queue Statistics
============================================================================================
                                                (default) (set)     Queue        Queue
QId PlcIdx  Queue Name                 Enabled   Rate     Rate      Drop(Bytes)  Drop(Frames)
--------------------------------------------------------------------------------------------
0    11     DOT1X Auth                  Yes     1000      1000     0            0
1    1      L2 Control                  Yes     2000      2000     0            0
2    14     Forus traffic               Yes     4000      4000     3296567      2336
3    0      ICMP GEN                    Yes     750       750      0            0
4    2      Routing Control             Yes     5500      5500     1085196      12919
5    14     Forus Address resolution    Yes     4000      4000     51723336     760639

6    0      ICMP Redirect               Yes     750       750      8444220485535  6978564145

...
```

Tormentas de tráfico

Una tormenta de tráfico se produce cuando un exceso de paquetes de difusión, multidifusión o unidifusión inunda una LAN, saturando los recursos del switch y degradando el rendimiento de la red.

El control de tormentas de los switches supervisa el tráfico de difusión, multidifusión y unidifusión en las interfaces físicas y lo compara con los umbrales configurados. Cuando el tráfico excede

estos límites, el switch bloquea temporalmente el tráfico excesivo para evitar la degradación de la red. Esto protege los recursos del switch y mantiene el rendimiento y la estabilidad de la red en general.

<#root>

Switch#show interfaces counters

```
Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Gi1/0/1        125487955     550123004     250123555     105234788

Gi1/0/2           500123        100123          5123          1024
Gi1/0/3           250123         50123          1024           512
```

Switch#show platform hardware fed switch active qos queue stats internal cpu policer

```
                          CPU Queue Statistics
============================================================================================
                                                 (default) (set)     Queue         Queue
QId PlcIdx  Queue Name                Enabled    Rate      Rate      Drop(Bytes)   Drop(Frames)
--------------------------------------------------------------------------------------------
11   13     L2 LVX Data Pack            Yes      1000      1000      0             0

12   0      BROADCAST                   Yes      750       750       32529067      186363

13   10     Openflow                    Yes      250       250       0             0

14   13     Sw forwarding               Yes      1000      1000      48317658492   245507344

15   8      Topology Control            Yes      13000     16000     0             0
```

Tiempo de vencimiento de CAM vs ARP

El tiempo de desactualización de CAM (tabla de direcciones MAC) frente al tiempo de desactualización del protocolo de resolución de direcciones (ARP) también puede provocar latencia de red y caídas de paquetes. Esto sucede porque la tabla CAM, que almacena las asignaciones de direcciones MAC a puertos, generalmente desactualiza las entradas más rápido (por defecto alrededor de cinco minutos) que la tabla ARP, que almacena las asignaciones de direcciones IP a MAC (por defecto alrededor de cuatro horas). Cuando una dirección MAC se desactualiza de la tabla CAM pero aún existe en la tabla ARP, el switch ya no conoce el puerto específico para reenviar el tráfico de unidifusión para esa dirección MAC. Como resultado, el switch inunda el tráfico de unidifusión a todos los puertos de la VLAN, lo que provoca la congestión de la red y la posible pérdida de paquetes.

Cómo el tiempo de vencimiento de CAM vs ARP causa latencia y pérdidas de paquetes

- Cuando la entrada de la tabla CAM se desactualiza antes de la entrada ARP, el switch inunda los paquetes unicast porque carece de la asignación MAC a puerto.
- Esta inundación aumenta la carga de la CPU y consume ancho de banda innecesariamente, lo que conduce a la latencia de la red y a las caídas de paquetes.
- La discordancia también puede causar un reenvío ineficiente y un mayor procesamiento del plano de control.

<#root>

Switch#show mac address-table aging-time

Global Aging Time:

300 <===== MAC aging

Vlan Aging Time
---- ----------

Switch#show ip arp

Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.95.1

124

Incomplete ARPA

<===== Arp age

...

Switch#show interface vlan1

Vlan1 is up, line protocol is up , Autostate Enabled
Hardware is Ethernet SVI, address is 10b3.d6f0.1347 (bia 10b3.d6f0.1347)
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not supported
ARP type: ARPA,

ARP Timeout 04:00:00

Last input never, output never, output hang never

Configuring MAC Aging and ARP Timeout:

```
Switch#confure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Switch(config)#mac-address-table aging-time ?

```
  <0-0>         Enter 0 to disable aging
  <10-1000000>  Aging time in seconds
```

Switch(config)#mac-address-table aging-time 14400 ?

```
  routed-mac  Set RM Aging interval
  vlan        VLAN Keyword
```

Switch(config)#interface vlan 1

```
Switch(config-if)#arp timeout 300

Switch(config-if)#do show interface vlan 1

Vlan1 is up, line protocol is up , Autostate Enabled
  Hardware is Ethernet SVI, address is 10b3.d6f0.1347 (bia 10b3.d6f0.1347)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA,
```

ARP Timeout 00:05:00

```
  Last input never, output never, output hang never
```

sesión de monitoreo

Cuando se configuran sesiones de supervisión activas (SPAN) en un switch con varios puertos de origen y destino, pueden contribuir a la latencia de la red y a la eliminación de paquetes.

<#root>

Example:

```
Session 1

---------

Type                  : Local Session
Source Ports          :

    Both              : Po101,Po105,Po109,Po125,Po161,Po170      <===== Multiple source ports

Destination Ports     : Te9/8

Egress SPAN Replication State:
Operational mode      : Centralized
Configured mode       : Centralized (default)

Session 2

---------

Type                  : Local Session
Source Ports          :

    Both              : Po161,Po170

Destination Ports     : Te9/1

Egress SPAN Replication State:
Operational mode      : Centralized
Configured mode       : Centralized (default)
```

Cómo Funciona SPAN

SPAN (analizador de puerto conmutado) es una función asistida por hardware que duplica el tráfico de los puertos de origen a los puertos de destino sin que se realicen búsquedas de CPU. El ASIC de replicación en el módulo supervisor maneja la duplicación de paquetes, mientras que el motor de reenvío redirige los paquetes reflejados a los puertos de destino. Los paquetes duplicados se conmutan con la misma sincronización que el tráfico regular.

Impacto de varios puertos de origen y destino:

En el ejemplo anterior, el switch debe replicar el tráfico de todas las interfaces de origen a las interfaces de destino. Por ejemplo, el tráfico de la interfaz Po170 se duplica y se reenvía dos veces a dos destinos diferentes. Esta replicación aumenta la carga en el motor de reenvío y puede causar congestión en la placa de interconexiones del switch.

- Si un canal de puerto transporta tres GBPS de tráfico, la replicación de este tráfico a varios destinos puede dar lugar a más de 15 GBPS de tráfico reflejado.
- La carga en el ASIC de replicación aumenta proporcionalmente con la velocidad del tráfico en las interfaces de origen.
- A velocidades de tráfico más bajas, el impacto de la latencia puede ser mínimo, pero a medida que aumenta el tráfico, la latencia y la congestión pueden llegar a ser significativas.

Excepciones de nivel ASIC

Utilice estos comandos para verificar la interfaz a las asignaciones ASIC, que muestra la instancia ASIC donde reside la interfaz.

<#root>

Switch#show platform software fed switch active ifm mappings

```
Interface                IF_ID    Inst Asic Core Port SubPort Mac  Cntx LPN  GPN  Type Active

GigabitEthernet2/0/12    0x13
 1     0    1
     11     0      20    17   12   108  NIF   Y
<===== ASIC Instance 1 (Asic 0/Core 1)
```

Una vez identificada la instancia de ASIC, ejecute el siguiente comando para ver las excepciones de descarte de ASIC de reenvío para ese ASIC.

<#root>

Switch#show platform hardware fed switch active fwd-asic drops exceptions asic

Example output snippet for ASIC instance 1:

```
****EXCEPTION STATS ASIC INSTANCE 1 (asic/core 0/1)****
================================================================================
 Asic/core |                NAME                    |   prev       |  current  |  delta

================================================================================
0       1  NO_EXCEPTION                              2027072618    2028843223    1770605
0       1  ROUTED_AND_IP_OPTIONS_EXCEPTION          735           735           0
0       1  PKT_DROP_COUNT                           14556203     14556203        0
0       1  BLOCK_FORWARD                           14556171     14556171        0
0       1  IGR_EXCEPTION_L5_ERROR                   1             1             0
...
```

Bugs de software

Los errores de software a veces pueden causar directa o indirectamente comportamientos no deseados e inesperados. Estos errores pueden ocasionar problemas como la latencia de la red, la pérdida de paquetes u otras degradaciones del rendimiento. Para resolver estos problemas, un primer paso común es recargar el switch, que puede borrar los fallos transitorios y restaurar el funcionamiento normal. Además, es fundamental mantener actualizados los dispositivos mediante la aplicación periódica de las actualizaciones de firmware y software más recientes. Estas actualizaciones a menudo incluyen correcciones para errores conocidos y mejoras que mejoran la estabilidad y el rendimiento del dispositivo, lo que ayuda a evitar problemas relacionados con defectos de software.

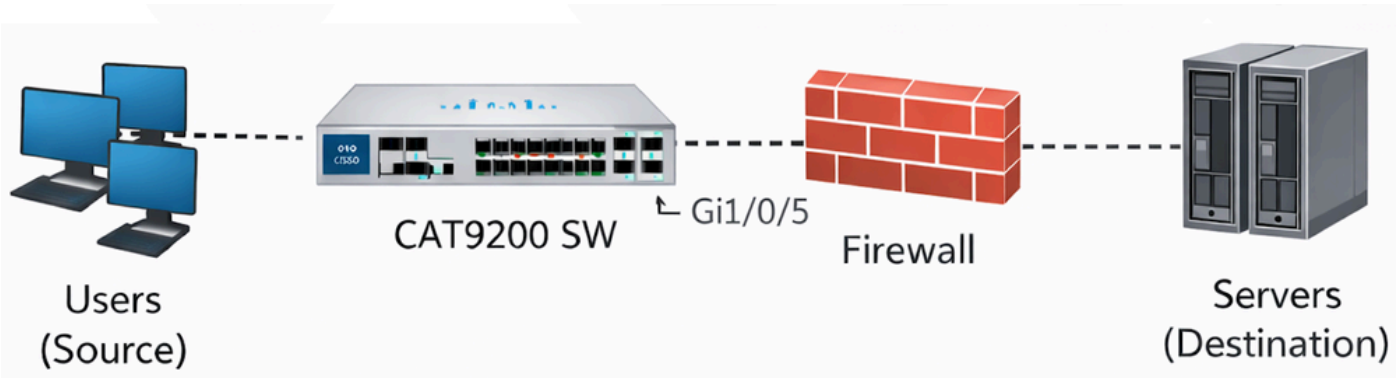
Herramienta Cisco Bug Search

Caso Práctico

Detalles del problema

Los usuarios experimentan una pérdida intermitente de conectividad de red durante los intentos de transferir grandes volúmenes de datos a través de vLAN, como durante las transferencias de archivos de alta capacidad. Estas interrupciones se manifiestan como fallos esporádicos en la transmisión de datos a pesar de varios intentos correctos, lo que afecta de forma significativa a la fiabilidad de la red y al rendimiento de las aplicaciones. El problema se resuelve temporalmente recargando el switch.

Topología



Síntomas observados

- Las transferencias de archivos entre el origen y el destino fallan intermitentemente después de varios intentos exitosos.
- El switch pierde la conectividad con el firewall durante los períodos de fallo.
- La autenticación 802.1X permanece operativa durante todos los incidentes.
- El switch sigue respondiendo a través de la consola durante los incidentes.
- El puerto conectado del firewall solo muestra el tráfico de difusión durante los períodos de error.
- Las pruebas de diagnóstico (DiagGoldPktTest) fallan constantemente en la interfaz Gi1/0/5, lo que indica un problema de ruta de datos.

Resolución de problemas realizada

- Se revisan los contadores de interfaz y las estadísticas del búfer de nivel de plataforma.
- La interfaz del switch Gi1/0/5 muestra un volumen muy alto de tramas de pausa 802.3x recibidas del firewall.
- Las estadísticas de caídas de salida y de trama de pausa se monitorean de cerca.
- Las estadísticas de cola del motor de reenvío de software de plataforma se examinan para identificar el comportamiento del búfer.
- Se verifica la configuración de control de flujo en la interfaz del switch.

Estadísticas de interfaz relevantes

<#root>

```
Switch#show interfaces GigabitEthernet 1/0/5

GigabitEthernet1/0/5 is up, line protocol is up (connected)
□
input flow-control is on,
 output flow-control is unsupported
<===== Input Flow-control is ON

Input queue: 0/2000/0/0 (size/max/drops/flushes);
Total output drops: 78444

5 minute input rate 8000 bits/sec, 8 packets/sec□
5 minute output rate 0 bits/sec, 0 packets/s                    <===== Output rate

0 watchdog, 5014620 multicast,
1989 pause input
```

0 unknown protocol drops□0 babbles, 0 late collision,
...

Switch#show controllers ethernet-controller GigabitEthernet 1/0/5

Transmit GigabitEthernet1/0/5. Receive
0 MacUnderrun frames 0 MacOverrun frames
0 Pause frames

1878 Pause frames

<===== Pause Frames In RX

...

Switch#diagnostic start switch 1 test DiagGoldPktTest port 5

Switch#show diagnostic result switch 1 test DiagGoldPktTest detail

□Test results: (. = Pass, F = Fail, U = Untested)
_____
1) DiagGoldPktTest:
Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24□
U U U U

F

U U U U U U U U U U U U U U U U U U U U.

<===== DiagGoldPktTest Failed For Port 5

Port 25 26 27 28□----------□U U U U

Switch#show flowcontrol interface GigabitEthernet 1/0/

Port Send FlowControl Receive FlowControl RxPause TxPause
admin oper admin Oper
---------- -------- -------- -------- -------- ------- -------
Gi1/0/5 Unsupp. Unsupp. on on.

13256

0

<===== Pause Frames In RX

Switch#show platform hardware fed switch active qos queue stats interface GigabitEthernet 1/0/5

```
Asic:0 Core:0 DATA Port:8 Hardware Drop Counters□
------------------------------------------------------------
Q   Drop-TH0     Drop-TH1      Drop-TH2      SBufDrop          QebDrop
□   (Bytes)       (Bytes)       (Bytes)       (Bytes)             (Bytes)□
------------------------------------------------------------
0     0               0
```

18106020

```
          0               0
```

Causa raíz identificada

La causa raíz se identificó como bloqueo del búfer debido a las tramas de pausa 802.3x excesivas enviadas por el firewall a la interfaz del switch. Las tramas de pausa Ethernet indican al switch que deje de transmitir para permitir que el dispositivo receptor se recupere de la congestión. Sin embargo, cuando las tramas de pausa se envían repetidamente o por duraciones extendidas:

- La cola de salida del buffer del switch para la interfaz se satura completamente.
- El switch continúa aceptando paquetes entrantes destinados a la interfaz pausada, que se acumulan en la cola de salida.
- La saturación de la cola conduce a caídas de salida y a la negritud del tráfico.
- En este caso, las memorias intermedias se bloquearon y el reenvío no se reanudó incluso después de que disminuyera la velocidad de las tramas de pausa.
- Se requirió una recarga del switch para borrar el estado del buffer bloqueado.

Este comportamiento se documenta en el error de funcionamiento de Cisco CSCwm14612, que describe cómo las tramas de pausa abrumadoras hacen que la interfaz contenga búferes incorrectamente, lo que resulta en caídas de salida.

Resolución

El control de flujo de entrada se inhabilitó en la interfaz de switch afectada mediante el comando:

<#root>

```
Switch#configure terminal
Switch(config)#interface GigabitEthernet 1/0/5
Switch(config-if)#
```

flowcontrol receive off

Conclusión

Los fallos de conectividad de red intermitentes y las caídas de paquetes entre el switch Cisco C9200L y el firewall se debieron a un bloqueo de cola de software provocado por un volumen excesivo de tramas de pausa 802.3x. Al deshabilitar el control de flujo de entrada en la interfaz

del switch se resolvió el problema al evitar que la cola se saturara y se bloqueara.

Información Relacionada

- Solución de problemas de caídas de salida en los switches Catalyst 9000
- Solucionar problemas del protocolo STP en los switches Catalyst
- Resolución de Problemas de MAC Flaps/Loop en Switches Cisco Catalyst
- 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).