Solución de problemas del router en la red empresarial

Contenido

Introducción

Este documento describe cómo identificar, resolver y resolver problemas de latencia en redes empresariales mediante routers Cisco.

Prerequisites

Requirements

No hay requisitos previos específicos para este documento.

Componentes Utilizados

Este documento no se limita a una versión de software y tipo de hardware específicos, pero los comandos se aplican a los routers Cisco IOS® XE como las familias ASR 1000, ISR 4000 y

Catalyst 8000.

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 describe una guía básica para entender, aislar y resolver problemas de latencia general, proporciona comandos y depuraciones útiles para detectar las causas principales y las prácticas recomendadas. Tenga en cuenta que no se pueden considerar todas las variables y escenarios posibles y que un análisis más profundo depende de situaciones específicas.

Definición de latencia

En términos generales, y citando la definición estricta para dispositivos de almacenamiento y reenvío (en RFC 1242), la latencia es el intervalo de tiempo que comienza cuando el último bit de la trama de entrada alcanza el puerto de entrada y termina cuando el primer bit de la trama de salida se ve en el puerto de salida.

La latencia de red puede referirse simplemente al retraso en la transferencia de datos a través de la red. Para cuestiones prácticas, esta definición es solo el punto de partida; necesita definir el problema de latencia del que habla en cada caso específico, aunque parezca obvio, el primer paso necesario para resolver un problema, y se vuelve realmente importante, es definirlo.

Uso de latencia

Muchas aplicaciones requieren baja latencia para la comunicación en tiempo real y las operaciones empresariales; con las mejoras de hardware y software cada día, hay más aplicaciones disponibles para la informática crítica, las aplicaciones de reuniones en línea y la transmisión por secuencias, entre otras; del mismo modo, el tráfico de red sigue creciendo y también aumenta la necesidad de diseños de red optimizados y de un mejor rendimiento de los dispositivos.

Además de ofrecer una mejor experiencia de usuario y ofrecer el mínimo necesario para aplicaciones sensibles a la latencia, identificar y reducir eficazmente los problemas de latencia en una red puede ahorrar una gran cantidad de tiempo y recursos de gran valor en una red.

Enfoque de problemas de latencia

La parte difícil de este tipo de problemas es el número de variables que debe tener en cuenta, además de que no puede haber un único punto de fallo. Por lo tanto, la definición de latencia se convierte en una clave importante para resolverla y algunos aspectos que debe tener en cuenta para tener una descripción útil del problema son los siguientes.

1. Expectativas y detección

Es importante diferenciar una latencia deseada, la latencia de trabajo esperada o de línea base y la actual. Dependiendo del diseño, los proveedores o los dispositivos de la red, a veces no se puede lograr la latencia deseada, es un buen procedimiento para medir la real en condiciones normales, pero es necesario ser coherente en los métodos de medición para evitar números engañosos; IP SLAs, y las herramientas de analizador de red pueden ayudar en este sentido.

Una de las herramientas más utilizadas y básicas para identificar la latencia por aplicaciones o incluso por IP SLA es a través de ICMP o ping:

<#root>

```
Router#
ping
 198.51.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.51.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5),
round-trip min/avg/max
 =
2/109/541 ms
```

Además de comprobar el alcance, el ping indica el tiempo de ida y vuelta (RTT) desde el origen al destino; el mínimo (2), el promedio (109) y el máximo (541) en milisegundos. Esto significa, la duración desde que el router envía la solicitud hasta que recibe la respuesta del dispositivo de destino. Sin embargo, no muestra cuántos saltos o información más profunda, pero es una manera fácil y rápida de detectar un problema.

2. Aislamiento

Al igual que ping, traceroute se puede utilizar como punto de partida para el aislamiento, detecta saltos y RTT por salto:

<#root>

```
Router#
traceroute
 198.51.100.1
Type escape sequence to abort.
Tracing the route to 198.51.100.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.0.3.1 5 msec 6 msec 1 msec
  2 10.0.1.1 1 msec 1 msec 1 msec
  3 10.60.60.1 1 msec 1 msec 1 msec
```

```
  4 10.90.0.2
362 msec 362 msec 362 msec


<<<< you can see the RTT of the three probes only on both hops
  5 10.90.1.2
363 msec 363 msec 183 msec

  6 10.90.7.7 3 msec 2 msec 2 msec
```

Traceroute funciona enviando un paquete con un TimeTo Live (TTL) de 1. El primer salto devuelve un mensaje de error ICMP que indica que el paquete no se pudo reenviar porque el TTL expiró y se mide el RTT, el segundo paquete se reenvía con un TTL de 2 y el segundo salto devuelve el TTL caducado. Este proceso continúa hasta que se alcanza el destino.

En el ejemplo, ahora puede reducir a dos hosts específicos y puede comenzar desde ahí con nuestro aislamiento.

A pesar de que estos son comandos útiles que pueden identificar fácilmente un problema, no toman en consideración otras variables como protocolos, marcas y tamaños de paquetes (aunque puede configurarlos como un segundo paso), diferentes fuentes IP, destinos entre múltiples factores.

Decir latencia puede ser un concepto muy amplio y a menudo solo se ve el síntoma en una aplicación, navegación, llamada o tareas específicas. Una de las primeras cosas a limitar es entender el impacto y definir el problema con más detalle, responder a las siguientes preguntas y elementos pueden ayudar para esta dimensionamiento:

- ¿Afecta la latencia solo a un tipo específico de tráfico o aplicación? Ejemplo: sólo UDP, TCP, ICMP...
- Si es así, ¿este tráfico tiene identificadores únicos? Ejemplo: marcación específica de QoS, solo tamaños de paquete determinados, opciones de IP...
- ¿Cuántos usuarios o sitios se ven afectados? Ejemplo: sólo una subred específica, uno o dos hosts finales, un sitio completo conectado a uno o varios dispositivos...
- ¿Se identifican marcas de tiempo específicas? Ejemplo: ¿esto ocurre solo durante las horas pico, cualquier patrón de tiempo o aleatorio completo...
- Aspectos de diseño. Ejemplo: el tráfico que pasa por un dispositivo específico, tal vez muchos dispositivos pero que se conecta a un solo proveedor, el tráfico que equilibra la carga pero afecta a una ruta...

Hay muchas otras consideraciones, pero el cruce de las diferentes respuestas (e incluso las pruebas que se pueden hacer para responderlas) puede aislar y limitar eficazmente el alcance para continuar con la solución de problemas. A modo de ejemplo, solo una aplicación (el mismo tipo de tráfico) se vio afectada en todas las sucursales que pasaban por diferentes proveedores y que terminaban en el mismo Data Center en las horas punta. En este caso, no comenzará a comprobar todos los switches de acceso de todas las sucursales, sino que se centrará en

recopilar más información sobre el Data Center e inspeccionará más en ese lado,

Las herramientas de supervisión y cierta automatización que puede tener en la red también ayudan mucho en este aislamiento, realmente depende de los recursos que tiene y situaciones únicas.

Solucionar problemas de causas comunes

Una vez que limite el alcance de la solución de problemas, puede comenzar a verificar causas específicas; por ejemplo, en el ejemplo de traceroute proporcionado, puede aislar a dos saltos diferentes y, a continuación, restringir a causas posibles.

Relacionado con la plataforma

Uso elevado de la CPU

Una de las causas más comunes puede ser un dispositivo con un retraso elevado en la realización de CPU en el proceso de todos los paquetes. Para los routers, los comandos más útiles y básicos para verificar los routers son

Rendimiento general del router:

<#root>

Router#

show platform resources

```
**State Acronym: H - Healthy, W - Warning, C - Critical
Resource                Usage                Max            Warning         Critical        State
-------------------------------------------------------------------------------------------------
RP0 (ok, active)                                                                              H

Control Processor       1.15%                100%           80%             90%             H



DRAM                    3631MB(23%)          15476MB        88%             93%             H

  bootflash             11729MB(46%)         25237MB        88%             93%             H
  harddisk              1121MB(0%)           225279MB       88%             93%             H
ESP0(ok, active)                                                                              H
 QFP                                                                                          H
  TCAM                  8cells(0%)           131072cells    65%             85%             H
  DRAM                  359563KB(1%)         20971520KB     85%             95%             H
  IRAM                  16597KB(12%)         131072KB       85%             95%             H

CPU Utilization         0.00%                100%           90%             95%             H
```

```
Crypto Utilization     0.00%                 100%            90%             95%             H

  Pkt Buf Mem (0)        1152KB(0%)            164864KB        85%             95%             H
  Pkt Buf CBlk (0)       14544KB(1%)           986112KB        85%             95%             H
```

Útil para ver la utilización de la memoria y la CPU a la vez, se divide en el plano de control y el plano de datos (QFP) igual que los umbrales para cada uno. La memoria en sí, no crea un problema de latencia, sin embargo, si no hay más memoria DRAM para el plano de control, Cisco Express Forwarding (CEF) se inhabilita e induce un uso alto de la CPU que puede producir latencia, es por eso que es importante mantener los números en estado saludable. La guía básica para la resolución de problemas de memoria está fuera del alcance, pero consulte el enlace útil en la sección Información relacionada.

Si se detecta un uso elevado de la CPU para el procesador de control, la CPU QFP o el cifrado, puede utilizar los siguientes comandos:

Para el plano de control:

show process cpu sorted

<#root>

```
Router#

show processes cpu sorted

CPU utilization for five seconds:

99%/0%

; one minute: 13%; five minutes: 3%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
  65        1621         638       2540 89.48%  1.82%  0.41%  0 crypto sw pk pro
   9         273          61       4475  1.56%  0.25%  0.05%   0 Check heaps
  51         212          64       3312  0.72%  0.21%  0.05%   0 Exec
 133         128          16       8000  0.60%  0.08%  0.01%   0 DBAL EVENTS
 473          25          12       2083  0.48%  0.04%  0.00%   0 WSMAN Process
  84        1173         353       3322  0.36%  0.07%  0.02%   0 IOSD ipc task
  87          23          12       1916  0.24%  0.02%  0.00%   0 PuntInject Keepa
  78         533         341       1563  0.12%  0.29%  0.07%   0 SAMsgThread
 225          25        1275         19  0.12%  0.00%  0.00%   0 SSS Feature Time
 386           4           4       1000  0.12%  0.00%  0.00%   0 Crypto WUI
 127         204       18810         10  0.12%  0.02%  0.00%   0 L2 LISP Punt Pro
```

Si la CPU del plano de control es alta (este ejemplo está en el 99% debido a los procesos), necesita aislar el proceso y, depende de él, proceder con el aislamiento (se pueden enviar paquetes para nosotros como ARP o paquetes de red de control, puede ser cualquier protocolo de ruteo, multidifusión, NAT, DNS, tráfico criptográfico o cualquier servicio).

Dependiendo de su flujo de tráfico, esto puede causar un problema en el procesamiento posterior; si el tráfico no está destinado al router, puede centrarse en el plano de datos:

Para el plano de datos:

show platform hardware qfp active datapath utilization [summary]

<#root>

```
Router#
show platform hardware qfp active datapath utilization

  CPP 0: Subdev 0

5 secs

        1 min        5 min       60 min
Input:  Priority (pps)            0            0            0            0
                 (bps)            0            0            0            0
    Non-Priority (pps)          231          192           68            6
                 (bps)       114616        95392        33920         3008
            Total (pps)          231          192           68            6
                 (bps)       114616        95392        33920         3008
Output: Priority (pps)            0            0            0            0
                 (bps)            0            0            0            0
    Non-Priority (pps)            3            2            2            0
                 (bps)        14896         9048         8968         2368


Total (pps)

         3323         2352          892            0


(bps)

        14896         9048         8968         2368

Processing: Load (pct)


3

            3            3            3

Crypto/IO


Crypto: Load (pct)            0

            0            0            0
        RX: Load (pct)            0            0            0            0
        TX: Load (pct)            1            1            0            0
            Idle (pct)           99           99           99           99
```

Si el plano de datos es alto (identificado por el número de carga de procesamiento que alcanza el 100%), debe ver la cantidad de tráfico que pasa a través del router (paquete total por segundos y bits por segundos) y el rendimiento de la plataforma (puede tener una idea en una hoja de datos específica).

Para determinar si este tráfico es esperado o no, la captura de paquetes (EPC) o cualquier función de monitoreo como Netflow se puede utilizar para análisis adicionales, algunas comprobaciones son:

- ¿El tráfico es válido y se espera que pase por este router?
- Identifique flujos de tráfico anormales o velocidades más altas.
- Si tiene números altos de paquetes por segundo, busque el tamaño de los paquetes. Determine si se espera que esto ocurra o si tiene un problema de fragmentación.

Si todo el tráfico es esperado, puede estar alcanzando una limitación de la plataforma, entonces, busque las funciones que se ejecutan en su router como segunda parte para el análisis a través de show running-config, principalmente en las interfaces, identifique las funciones innecesarias y desactívelas o equilibre el tráfico para liberar los ciclos de la CPU.

Sin embargo, si no hay indicación de un límite de plataforma, otra herramienta útil para corroborar si el router está agregando retardo en los paquetes es el seguimiento FIA, puede ver el tiempo de proceso exacto empleado para cada paquete y las funciones que toman la mayor parte del procesamiento. La resolución completa de problemas de uso elevado de la CPU está fuera del alcance de este documento, pero consulte los links en la sección Información Relacionada.

Tráfico relacionado

MTU y fragmentación

La unidad de transmisión máxima (MTU) es la longitud máxima de paquete que se transmitirá, que depende del número de octetos que puedan transmitir los links físicos.Cuando los protocolos de capa superior envían datos a la IP subyacente, y la longitud resultante del paquete IP es mayor que la MTU de trayectoria, el paquete se divide en fragmentos. Este tamaño más bajo de la red provoca más procesamiento y un tratamiento diferente en algunos casos y por eso debe evitarlo lo más posible.

Para algunas funciones como NAT o firewall basado en zona, se requiere un reensamblado virtual para "tener todo el paquete", aplicar lo que se necesita, reenviar sus fragmentos y descartar la copia reensamblada. Este proceso agrega ciclos de CPU y es propenso a errores.

Algunas aplicaciones no dependen de la fragmentación, una de las pruebas más básicas para verificar la MTU es un ping con una opción sin fragmento y probar diferentes tamaños de paquete: ping ip-address df-bit size number. Si el ping no es exitoso, corrija la MTU sobre la trayectoria cuando se produce la caída y causa más problemas.

Las funciones, como el ruteo basado en políticas y la ruta múltiple de igual costo en una red con paquetes fragmentados pueden crear problemas de demora y más errores principalmente en velocidades de datos altas, lo que provoca tiempos de ensamblaje altos, ID duplicadas y paquetes dañados. Si se identifican algunos de estos problemas, busque resolver esta fragmentación lo más posible. Un comando para verificar si tiene fragmentos y cualquier problema potencial es show ip traffic:

<#root>

```
Router#
```

show ip traffic

```
IP statistics:
  Rcvd:  9875429 total, 14340254 local destination
         0 format errors, 0 checksum errors, 0 bad hop count
         0 unknown protocol, 0 not a gateway
         0 security failures, 0 bad options, 0 with options
  Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 0 record route
         0 stream ID, 0 strict source route, 0 alert, 0 cipso, 0 ump
         0 other, 0 ignored
```

Frags:

150 reassembled

, 0

timeouts

,

0 could not reassemble

0

fragmented

, 600

fragments

, 0

could not fragment

```
         0 invalid hole
  Bcast: 31173 received, 6 sent
  Mcast: 0 received, 0 sent
  Sent:  15742903 generated, 0 forwarded
  Drop:  0 encapsulation failed, 0 unresolved, 0 no adjacency
         0 no route, 0 unicast RPF, 0 forced drop, 0 unsupported-addr
         0 options denied, 0 source IP address zero
<output omitted>
```

En el resultado anterior, las palabras en negrita de la sección Frags hacen referencia a:

- Reensamblado: Número de paquetes reensamblados.
- Tiempos de espera: cada vez que caduca el tiempo de reensamblado de un fragmento de paquete.
- No se pudo reensamblar: número de paquetes que no se pudieron reensamblar.
- Fragmentado: Número de paquetes que exceden la MTU y sujetos a fragmentación.
- Fragmentos: número de fragmentos en los que se fragmentaron los paquetes.
- No se pudo fragmentar: Número de paquetes que exceden la MTU pero no se pudieron

fragmentar.

Si se utiliza la fragmentación y tiene tiempos de espera o no pudo reensamblar los contadores para aumentar, una manera de corroborar los problemas causados por la plataforma es a través de caídas QFP, usando el mismo comando que se explicó más adelante en la sección de caídas: show platform hardware qfp active statistics drop. Busque errores como: TcpBadfrag, IpFragErr, FragTailDrop, ReassDrop, ReassFragTooBig, ReassTooManyFrags, ReassTimeout o relacionados. Cada caso puede tener diferentes causas como no obtener todos los fragmentos, duplicados, congestión de CPU entre otros. Una vez más, las herramientas útiles para un análisis adicional y una posible corrección pueden ser una comprobación de configuración y seguimiento de FIA.

TCP ofrece el mecanismo de tamaño máximo de segmento (MSS) para resolver este problema, pero puede inducir latencia si se descubre MTU de trayecto incorrecta, no negociada por MSS o incorrecta.

Como UDP no tiene este mecanismo de fragmentación, puede confiar en la implementación manual de PMTD o en cualquier solución de capa de aplicación, puede habilitarlos (cuando corresponda) para enviar paquetes de menos de 576 bytes, que es la MTU efectiva más pequeña para enviar números según RFC1122 en ayudas para evitar la fragmentación.

Relacionado con el diseño

Más que una sugerencia de solución de problemas, esta sección describe brevemente dos componentes clave más que pueden aumentar los problemas de latencia y requieren una discusión y un análisis exhaustivos fuera del alcance de este documento.

Routing subóptimo

El ruteo subóptimo en la red se refiere a una situación en la que los paquetes de datos no se dirigen a través del trayecto más eficiente o más corto disponible en una red. En su lugar, estos paquetes toman una ruta menos eficiente, lo que posiblemente resulta en una mayor latencia, congestión o afecta el rendimiento de la red. Los IGP eligen siempre las mejores trayectorias, lo que significa el costo más bajo, pero no necesariamente es la más barata o la trayectoria de demora más baja (la mejor puede ser la que tiene un ancho de banda más alto).

El ruteo subóptimo puede ocurrir por problemas con los protocolos de ruteo; ya sea configuración o cualquier situación como condiciones de carrera, cambios dinámicos (cambios de topología o fallas de link), ingeniería de tráfico intencional basada en políticas o costos de la compañía, redundancias o fallas (ir a la trayectoria de respaldo bajo ciertas condiciones) entre otras situaciones.

Herramientas como traceroutes o el dispositivo de supervisión pueden ayudar a identificar esta situación para flujos específicos, si este es el caso, y depende de muchos otros factores, satisfacer las demandas de las aplicaciones y una latencia más baja puede requerir un rediseño del routing o ingeniería del tráfico.

Quality of Service (QoS)

Al configurar la calidad del servicio (QoS), puede proporcionar un tratamiento preferente a tipos específicos de tráfico a expensas de otros tipos de tráfico. Sin QoS, el dispositivo ofrece el mejor servicio posible para cada paquete, independientemente del contenido o tamaño del paquete. dispositivo envía los paquetes sin ninguna garantía de fiabilidad, límites de retraso o rendimiento.

Si QoS está en su lugar, es muy importante identificar si el router marca, vuelve a marcar o simplemente clasifica los paquetes, verificar la configuración y mostrar policy-map [name_of_policy_map | sesión | interface interface_id] ayuda a comprender las clases afectadas por altas velocidades, caídas o paquetes erróneamente clasificados.

La implementación de QoS es una tarea de gran trabajo que requiere un análisis serio y que está fuera del alcance de este documento, pero se recomienda encarecidamente tener en cuenta esto para dar prioridad a las aplicaciones en las que el tiempo es un factor importante y resolver o evitar muchos problemas de latencia y aplicaciones.

Otros problemas de rendimiento

Otras condiciones pueden añadir lentitud, reconexión de la sesión o mal rendimiento general que necesita comprobar, algunas de ellas son:

Caídas

Un problema directamente relacionado con el procesamiento en un dispositivo son las caídas de paquetes, debe verificar el lado de entrada y salida desde la perspectiva de la interfaz:


```
Router#sh interfaces GigabitEthernet0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  Hardware is vNIC, address is 0ce0.995d.0000 (bia 0ce0.995d.0000)
  Internet address is 10.10.1.2/24
  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 set (10 sec)
  Full Duplex, 1000Mbps, link type is auto, media type is Virtual
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:19, output 00:08:33, output hang never
  Last clearing of "show interface" counters never


 Input queue: 0/375/6788/0 (size/max/drops/flushes); Total output drops: 18263

  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 114000 bits/sec, 230 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     193099 packets input, 11978115 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
```

```
     0 runts, 0 giants, 0 throttles

1572 input errors

,

12 CRC

, 0 frame,

1560 overrun

, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     142 packets output, 11822 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 0 interface resets
     23 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
Router#
```

En el lado de entrada tiene:

- Caídas de la cola de entrada: Cada interfaz posee una cola de entrada (es decir, un búfer de software que se puede modificar) en la que los paquetes entrantes se colocan en espera de procesamiento por parte del procesador de routing (RP). si la velocidad para los paquetes entrantes colocados en la cola de entrada excede la velocidad a la que el RP puede procesar los paquetes, puede tener un incremento de caídas. Sin embargo, tenga en cuenta que solo se colocan paquetes de control y tráfico "Para nosotros", por lo tanto, si se observa latencia al pasar a través del tráfico, incluso si tiene caídas esporádicas, esto no debe ser una causa.

- Sobrecargas: Esto ocurre cuando el hardware del receptor no puede entregar los paquetes recibidos a un buffer de hardware porque la velocidad de entrada excede la capacidad del receptor para manejar los datos. Este número puede indicar un problema con la velocidad y el rendimiento del router, capturar el tráfico solo para esta interfaz y buscar picos de tráfico. Una solución alternativa común es habilitar el control de flujo, pero esto puede aumentar la demora de los paquetes. Esto también puede ser una prueba de cuellos de botella y exceso de suscripción.
- CRCs: Se produce debido a problemas físicos, comprobar el cableado, los puertos y SFP conectados correctamente y el funcionamiento correcto.

En el lado de salida tiene:

- Caídas de la cola de salida: Cada interfaz posee una cola de salida donde se colocan los paquetes salientes que se enviarán a la interfaz. A veces, la velocidad de los paquetes salientes colocados en la cola de salida por el RP excede la velocidad a la que la interfaz puede enviar los paquetes. Esto puede causar problemas de rendimiento y problemas de latencia si no hay QoS en funcionamiento; de lo contrario, puede hacer que este número aumente debido a la aplicación de ciertas políticas y aconsejar que verifique o implemente la

configuración de QoS para proteger y asegurar el tráfico intencionado o crítico.

Finalmente, las caídas en QFP están directamente relacionadas con el alto procesamiento que puede causar latencia, verifíquelo a través de show platform hardware qfp active statistics drop:

```
<#root>

Router#

show platform hardware qfp active statistics drop

Last clearing of QFP drops statistics : never

-------------------------------------------------------------------------
Global Drop Stats                          Packets                 Octets
-------------------------------------------------------------------------
Disabled                                         2                    646
Ipv4NoAdj                                   108171                6706602
Ipv6NoRoute                                     10                    560
```

Las causas dependen del código, el seguimiento FIA ayuda a corroborar o descartar si el tráfico afectado por la latencia se descarta en este punto.

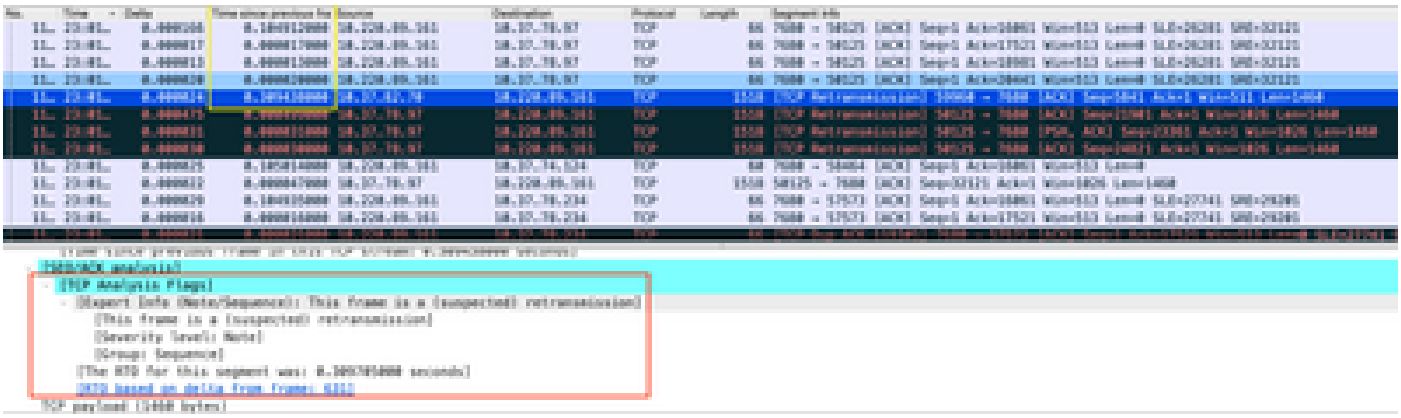
Retransmisión de TCP

La retransmisión TCP es un síntoma o puede ser una consecuencia debido a un problema subyacente como la pérdida de paquetes. Este problema puede inducir a la lentitud y mal rendimiento en la aplicación.

El protocolo de control de transmisión (TCP, Transmission Control Protocol) utiliza un temporizador de retransmisión para garantizar la entrega de datos sin que el receptor de datos remoto envíe información. La duración de este temporizador se denomina RTO (tiempo de espera de retransmisión). Cuando caduca el temporizador de retransmisión, el remitente retransmite el segmento más antiguo que no ha sido reconocido por el receptor TCP y se aumenta el RTO.

Algunas retransmisiones no se pueden eliminar por completo, si son mínimas, no puede reflejar un problema. Sin embargo, como puede inferir, más retransmisión vista, más latencia en la sesión TCP y necesita ser tratada.

La captura de paquetes analizada en Wireshark puede corroborar el problema como siguiente ejemplo:



Captura de conversación TCP

Si hay retransmisiones, utilice el mismo método de captura en la dirección de ingreso y egreso del router para verificar todos los paquetes enviados y recibidos. Por supuesto, hacer esto en cada salto puede representar un tremendo esfuerzo por lo que se necesita un análisis detallado sobre la captura para TCP, observando los TTL, tiempos de tramas anteriores en el mismo flujo TCP para entender desde qué dirección (servidor o cliente) tiene este retraso o falta de respuesta para dirigir su troubleshooting.

Sobresuscripción y cuellos de botella

La sobresuscripción se produce cuando los recursos necesarios (ancho de banda) son mayores que los realmente disponibles. Los comandos para identificar si tiene este problema en un router ya se han cubierto en la sección anterior.

Como consecuencia de esta situación, pueden producirse cuellos de botella cuando se ralentizan los flujos de tráfico debido a un ancho de banda o una capacidad de hardware insuficientes. Es importante identificar si esto sucede en un corto período de tiempo o si es una situación a largo plazo para aplicar soluciones.

No existe un consejo específico para resolverlo, pero algunas de las opciones son equilibrar el tráfico a diferentes plataformas, segmentar la red o actualizar a dispositivos más robustos en función de las necesidades actuales y el análisis de crecimiento futuro.

Información Relacionada

- Operaciones de eco ICMP de IP SLAs
- Resolución de problemas de memoria
- Resolución de Problemas con la Función Cisco IOS-XE Datapath Packet Trace
- Resolución de problemas de paquetes descartados en routers de servicios serie ASR 1000.
- Qos Información relacionada
- Configuración de QoS en routers
- 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).