Resolver problemas CPU elevada la utilización en el proceso de entrada IP

Contenido

Introducción

Este documento explica cómo resolver problemas CPU elevada el utilización debido a al proceso de entrada IP.

Note: Este documento no proporciona a las estrategias para prevenir diversos tipos de ataques.

Prerequisites

Requisitos

Cisco recomienda que usted lee resolver problemas CPU elevada la utilización en el Routers de Cisco antes de que usted proceda con este documento.

Componentes usados

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

La Información presentada en este documento fue creada de los dispositivos en un entorno específico del laboratorio. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Convenciones

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

Entrada de IP

El proceso del software del ® del Cisco IOS llamó la *entrada IP* toma el cuidado de los paquetes IP de la proceso-transferencia. Si el proceso de entrada IP utiliza inusualmente CPU elevada los recursos, el router es proceso-transferencia mucho tráfico IP. Controle estos problemas:

- **La transferencia de la interrupción se inhabilita en un interfaz (o los interfaces) que tenga (tenga) mucho tráfico**La transferencia de la interrupción refiere al uso de los algoritmos de la transferencia con excepción de la transferencia de proceso. Los ejemplos incluyen la transferencia rápida, Optimum Switching, transferencia de la expedición expresa de Cisco, y así sucesivamente (refiera a los fundamentos del ajuste del rendimiento para los detalles). Examine la salida del **comando show interfaces switching** de ver qué interfaz se carga con el tráfico. Usted puede controlar el **comando show ip interface** de ver qué método de Switching se utiliza en cada interfaz. Vuelva a permitir la transferencia de la interrupción en ese interfaz. Recuerde que la transferencia rápida regular está configurada en las interfaces de salida: si la transferencia rápida se configura en un interfaz, rápido-se cambian los paquetes que salen de ese interfaz. La transferencia de la expedición expresa de Cisco se configura en las interfaces de entrada. Para crear las entradas de tabla de la base de información de reenvío (BOLA) y de la adyacencia en una interfaz particular, configure la transferencia de la expedición expresa de Cisco en todos los interfaces que encaminen a ese interfaz.
- **La transferencia rápida en el mismo interfaz se inhabilita**Si un interfaz tiene muchas direcciones secundarias o los subinterfaces y allí son mucho tráfico originario del interfaz y destinado para un direccionamiento en ese mismo interfaz, después todos esos paquetes proceso-se cambian. En esta situación, usted debe activar el mismo-**interfaz del ruta-caché IP** en el interfaz. Cuando se utiliza la transferencia de la expedición expresa de Cisco, usted no necesita activar la transferencia de la expedición expresa de Cisco en el mismo interfaz por separado.
- **La transferencia rápida en un interfaz que proporciona a la encaminamiento de la directiva se inhabilita**Si una ruta-correspondencia se ha configurado en un interfaz, y mucho tráfico es manejado por la ruta-correspondencia, entonces el proceso-Switches del router este tráfico. En esta situación, usted debe activar la **directiva del ruta-caché IP** en el interfaz. Controle las restricciones mencionadas en “activando la sección de la encaminamiento Directiva-basada Rápido-cambiada” de configurar la encaminamiento Directiva-basada.
- **Trafique que no se puede interrupción-cambiar llega**Éste puede ser tipos de tráfico mencionados uces de los. Click on conectó los items para más información.Paquetes para los cuales no hay entrada con todo en el caché de la transferenciaIncluso si es rápido, óptimo, o se configura la transferencia de la expedición expresa de Cisco (CEF), un paquete para la cual allí es no se procesa ninguna coincidencia en el caché de la rápido-transferencia o las tablas de la BOLA y de la adyacencia. Una entrada entonces se crea en el caché o la tabla apropiado, y todos los paquetes subsiguientes que hacen juego los mismos criterios son rápidos, óptimos, o CEF-cambiado. En las Circunstancias normales, estos paquetes procesados no causan CPU elevada la utilización. Sin embargo, si hay un dispositivo en la red que 1) genera los paquetes a una velocidad extremadamente alta de los dispositivos accesible a través del router, y 2) utiliza los IP Addresses de las diferentes fuentes o del destino, no hay una coincidencia para estos paquetes en el caché o la tabla de la transferencia, así que son procesados por el proceso de entrada IP (si se configura el Switching de Netflow, la fuente y los puertos del destino TCP se controlan contra las entradas

en el caché de NetFlow también). Este dispositivo de origen puede ser un dispositivo no funcional o, más probable, un dispositivo intentando un ataque.(*) Solamente con las adyacencias de recolección. Refiera a la expedición expresa de Cisco para más información sobre las adyacencias de la expedición expresa de Cisco.Paquetes destinados para el routerÉstos son ejemplos de paquetes destinados para el router:Encaminando las actualizaciones que llegan a una tarifa de extremadamente alta. Si el router recibe una cantidad enorme de actualizaciones de la encaminamiento que tengan que ser procesadas, esta tarea pudo sobrecargar la CPU. Normalmente, esto no puede suceder en una red estable. La manera que usted puede recopilar más información depende del protocolo de la encaminamiento usted ha configurado. Sin embargo, usted puede comenzar a controlar la salida del **comando show ip route summary** periódicamente. Los valores que cambian rápidamente son una muestra de una red inestable. El medio frecuente de los cambios de la tabla de encaminamiento aumentó el protocolo de la encaminamiento que procesaba, que da lugar a la utilización de la CPU incrementada. Para más información sobre cómo resolver problemas este problema, refiera a la sección TCP/IP que resuelve problemas del guía de Troubleshooting de la red interna.Cualquier otra clase de tráfico destinada para el router. Control que se abre una sesión al router y a las acciones de usuario. Si abren una sesión y publica alguien los comandos que producen el resultado extenso, CPU elevada la utilización por el proceso entrado “IP” es seguida por una utilización mucho más alta CPU por el proceso de EXEC virtual.Ataque de simulación. Para identificar el problema, publique el **comando show ip traffic** de controlar la cantidad de tráfico IP. Si hay un problema, el número de paquetes recibidos con un destino local es significativo. Después, examine la salida del para controlar en qué interfaz están viniendo los paquetes. Una vez que usted ha identificado el interfaz de recepción, gire las **estadísticas IP** en la interfaz saliente y vea si hay un modelo. Si hay un ataque, la dirección de origen es casi siempre diferente, pero el direccionamiento de destino es lo mismo. Una lista de acceso se puede configurar para solucionar el problema temporalmente (preferiblemente en el dispositivo más cercano a la fuente de los paquetes), pero la solución real es rastrear el dispositivo de origen y parar el ataque.Tráfico de broadcastControle el número de paquetes de broadcast en la salida del **comando show interfaces**. Si usted compara la cantidad de difusiones a la cantidad total de paquetes que fueron recibidos en el interfaz, usted puede ganar una idea de si hay gastos indirectos de las difusiones. Si hay un LAN con vario Switches conectado con el router, después éste puede indicar un problema con atravesar - árbol.Paquetes IP con las opcionesPaquetes que requieren la Traducción de protocoloProtocolo multilink point-to-point (utilizado en la transferencia de la expedición expresa de Cisco)Tráfico comprimidoSi no hay adaptador de servicio de la compresión (CSA) en el router, los paquetes comprimidos deben proceso-ser cambiados.Tráfico encriptadoSi no hay adaptador del servicio de encripción (ESA) en el router, los paquetes encriptados deben proceso-ser cambiados.Paquetes que pasan a través de las interfaces en serie con la encapsulación X.25En la habitación de protocolo x.25, el control de flujo se ejecuta en la segunda capa del interconexión de sistema abierto (OSI).

- Muchos paquetes, eso llegan a una tarifa de extremadamente alta, para un destino en directamente una subred conectada, para la cual no hay entrada en la tabla del Address Resolution Protocol (ARP). Esto no debe suceder con tráfico TCP debido al mecanismo de ventanas, sino puede suceder con el tráfico del User Datagram Protocol (UDP). Para identificar el problema, relance las acciones sugeridas para rastrear un ataque de simulación.
- Mucho tráfico Multicast pasa a través del router. Desafortunadamente, no hay forma sencilla de examinar la cantidad de tráfico Multicast. **El comando show ip traffic** muestra solamente la información de resumen. Sin embargo, si usted ha configurado la encaminamiento del

Multicast en el router, usted puede activar la rápido-transferencia de los paquetes de multidifusión con el comando ip mroute-cache interface configuration (la rápido-transferencia de los paquetes de multidifusión está apagada por abandono).

- El router es oversubscribed. Si el router es usado en exceso y no puede manejar esta cantidad de tráfico, intente distribuir la carga entre el otro Routers o comprar a un router de mayor capacidad.
- El Network Address Translation (NAT) IP se configura en el router, y las porciones de paquetes del Domain Name System (DNS) pasan a través del router. Los paquetes UDP o TCP con el puerto de origen o de destino 53 (DNS) son llevados en batea siempre al nivel de proceso por el NAT.
- Hay otros tipos de paquete que se llevan en batea al proceso.
- Hay fragmentación del IP datagram. Hay un pequeño aumento en la CPU y memoria suplementaria debidas hacer fragmentos de un IP datagram. Refiera a la resolución fragmentación de IP, los problemas MTU, MSS, y PMTUD con GRE e IPSEC para más información sobre cómo resolver problemas este problema.

Sea cual sea la razón CPU elevada de la utilización en el proceso de entrada IP, la fuente del problema puede ser rastreada si usted pone a punto los paquetes IP. Puesto que la utilización CPU es ya alta, el proceso de la depuración tiene que ser realizado con la precaución extrema. El proceso de la depuración produce las porciones de mensajes, tan solamente registración protegidos debe ser configurado.

El registro a una consola aumenta las interrupciones innecesarias a la CPU y aumenta la utilización CPU. El registro a un host (o al registro de monitoreo) genera el tráfico adicional en los interfaces.

El proceso de la depuración se puede comenzar con el comando debug ip packet detail exec. Esta sesión no debe durar más de largo de tres a cinco segundos. Los mensajes de debugging se escriben en memoria intermedia de registro. Una captura de una sesión del debugging de IP de la muestra se proporciona en la sección de la sesión de ejemplo de debugging del paquete IP de este documento. Una vez que el dispositivo de origen de los paquetes indeseados IP se encuentra, este dispositivo puede ser disconnected de la red, o una lista de acceso se puede crear en el router para caer los paquetes de ese destino.

Sesión de depuración de paquete del IP de muestra

Los destinos de registro configurados se deben controlar primero con el **comando show logging**:

```
router#show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level debugging, 52 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 148 messages logged
    Trap logging: level informational, 64 message lines logged
        Logging to 192.168.100.100, 3 message lines logged
        Logging to 192.168.200.200, 3 message lines logged
 --More--
```

Inhabilite todos los destinos de registro excepto memoria intermedia de registro, y memoria intermedia de registro clara:

```
router#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#no logging console
router(config)#no logging monitor
router(config)#no logging 192.168.100.100
router(config)#no logging 192.168.200.200
router(config)#^Z
router#clear logging
Clear logging buffer [confirm]
router#
```

Para una mejor legibilidad de la salida del depuración, la fecha y hora y las indicaciones de fecha y hora en milisegundos deben ser activadas:

```
router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#service timestamps log datetime msec
router(config)#service timestamps debug datetime msec
router(config)#end
router#
```

Una sesión de debugging puede ahora ser comenzada:

```
router#debug ip packet detail
IP packet debugging is on (detailed)
```

El depuración no debe durar más de tres a cinco segundos. La sesión se puede parar con el comando undebug all exec:

```
router#undebug all
All possible debugging has been turned off
```

Los resultados se pueden controlar con el comando show logging exec:

```
router#show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 145 messages logged
    Trap logging: level informational, 61 message lines logged
Log Buffer (64000 bytes):

*Mar  3 03:43:27.320: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.204
   (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar  3 03:43:27.324: ICMP type=8, code=0
*Mar  3 03:43:27.324: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.205
   (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar  3 03:43:27.324: ICMP type=8, code=0
*Mar  3 03:43:27.328: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.206
   (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar  3 03:43:27.328: ICMP type=8, code=0
...
```

El registro muestra eso:

- Un paquete se ha recibido cada cuatro milisegundos
- La dirección IP de la fuente es 192.168.40.53
- Los paquetes han venido adentro en el interfaz Ethernet0/1
- Los paquetes tienen diversos IP Addresses del destino

- Los paquetes se han enviado en el interfaz Ethernet0/0
- La dirección IP del siguiente-salto es 10.200.40.1
- Los paquetes eran las peticiones ICMP (type=8)En este ejemplo, usted puede ver que CPU elevada la utilización en el proceso de entrada IP ha sido causada por una inundación de ping de la dirección IP 192.168.40.53.Las inundaciones del SYN se pueden fácilmente detectar esta manera porque la presencia de indicador SYN se indica en el depuración hecho salir:

```
router#show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 145 messages logged
    Trap logging: level informational, 61 message lines logged
Log Buffer (64000 bytes):

*Mar  3 03:43:27.320: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.204
   (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar  3 03:43:27.324: ICMP type=8, code=0
*Mar  3 03:43:27.324: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.205
   (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar  3 03:43:27.324: ICMP type=8, code=0
*Mar  3 03:43:27.328: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.206
   (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar  3 03:43:27.328: ICMP type=8, code=0
...
```

Información Relacionada

- Resolución de problemas por uso excesivo de las CPU de los routers de Cisco
- El comando show processes
- Alta utilización de la CPU en switches de Catalyst 2900XL/3500XL
- Fundamentos del ajuste de rendimiento
- Soporte técnico y documentación - Cisco Systems