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

Contenido

Introducción

Este documento explica cómo solucionar problemas de alta utilización de la CPU debido al proceso de entrada IP.

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

prerrequisitos

Requisitos

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

Componentes Utilizados

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

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. 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 del IP del Process-Switching. Si el proceso de entrada IP utiliza inusualmente CPU elevada los recursos, el router es Process-Switching mucho tráfico IP. Marque estos problemas:

- **El Interrupt Switching se inhabilita en una interfaz (o las interfaces) que tenga (tenga) mucho tráfico**El Interrupt Switching refiere al uso de los algoritmos de Switching con excepción del process switching. Los ejemplos incluyen la transferencia rápida, Optimum Switching, Cisco Express Forwarding Switching, y así sucesivamente (refiera a los fundamentos del ajuste de rendimiento para los detalles). Examine la salida del **comando show interfaces switching** de ver qué interfaz se carga con el tráfico. Usted puede marcar el **comando show ip interface** de ver qué método de Switching se utiliza en cada interfaz. Vuelva a habilitar la interrupción de conmutación en esa interfaz. Recuerde que el fast switching común se configura en las interfaces de salida: si la transferencia rápida se configura en una interfaz, los paquetes que salen de esa interfaz son Fast-Switched. El Cisco Express Forwarding Switching se configura en las interfaces de entrada. Para crear entradas de Base de información de reenvío (FIB) y tabla de adyacencia en una determinada interfaz, configure conmutación de Cisco Express Forwarding en todas las interfaces que enrutan a esa interfaz.
- **La transferencia rápida en la misma interfaz se inhabilita**Si una interfaz tiene muchas direcciones secundarias o las subinterfaces y allí son mucho tráfico originado de la interfaz y destinado para un direccionamiento en ese lo mismo la interfaz, después todos esos paquetes son process-switched. En esta situación, usted debe habilitar la mismo-**interfaz del route-cache del IP** en la interfaz. Cuando se usa la conmutación de Cisco Express Forwarding, no necesita habilitar esta conmutación en la misma interfaz por separado.
- **La transferencia rápida en una interfaz que proporciona al Policy Routing se inhabilita**Si un route-map se ha configurado en una interfaz, y mucho tráfico es manejado por el route-map, entonces el proceso-Switches del router este tráfico. En esta situación, usted debe habilitar el **ip route-cache policy** en la interfaz. Marque las restricciones mencionadas en “habilitando la sección del Policy-Based Routing Fast-Switched” de configurar el Policy-Based Routing.
- **Trafique que no puede ser interrupt-switched llega**Éste puede ser tipos de tráfico mencionados uces de los. Click on enlazó los elementos para más información.Paquetes que aún no tienen una entrada en la memoria caché de conmutación.Incluso si es rápido, óptimo, o se configura el (CEF) del Cisco Express Forwarding Switching, un paquete para las cuales allí es no se procesa ninguna coincidencia en memoria caché de Fast-Switching o la BOLA y las tablas de 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-Switched. 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 las diferentes fuentes o los IP Address de destino, no hay una coincidencia para estos paquetes en el Switching Cache o la tabla, así que son procesados por el proceso de entrada IP (si el Switching de Netflow los puertos se configura, de la fuente y del TCP de destino se marcan 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.(*) Sólo con adyacencias de recolección. Refiera al Cisco Express Forwarding para

más información sobre las adyacencias del Cisco Express Forwarding.Paquetes destinados para el routerÉstos son ejemplos de paquetes destinados para el router:Actualizaciones de ruteo que llegan a una tarifa de extremadamente alta. Si el router recibe una cantidad enorme de actualizaciones de ruteo que tengan que ser procesadas, esta tarea pudo sobrecargar el CPU. Normalmente, esto no puede suceder en una red estable. La forma en que puede reunir más información depende del protocolo de ruteo que haya configurado. Sin embargo, usted puede comenzar a marcar 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 ruteo aumentó el Routing Protocol 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 de la CPU mucho más alta por el proceso de EXEC virtual.Ataque de simulación. Para identificar el problema, publique el **comando show ip traffic** de marcar la cantidad de tráfico IP. Si hay un problema, el número de paquetes recibidos con un destino local es significativo. Después, examine la salida de los para marcar que interconectan los paquetes están viniendo adentro. Una vez que usted ha identificado la interfaz de recepción, gire el **IP que considera** en la interfaz saliente y vea si hay un modelo. Si hay un ataque, la dirección de origen es casi siempre diferente, pero la dirección 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 broadcastMarque el número de paquetes de broadcast en la salida del **comando show interfaces**. Si usted compara la cantidad de broadcasts a la cantidad total de paquetes que fueron recibidos en la interfaz, usted puede ganar una idea de si hay gastos indirectos de los broadcasts. Si hay un LAN con vario Switches conectado con el router, después éste puede indicar un problema con el Spanning-tree.Paquetes IP con opcionesPaquetes que requieren la traducción del protocoloProtocolo multilink point-to-point (soportado en el Cisco Express Forwarding Switching)Tráfico comprimidoSi hay el adaptador de servicio del No Compression (CSA) en el router, los paquetes comprimidos deben ser process-switched.Tráfico encriptadoSi hay el adaptador de servicio del no encryption (ESA) en el router, los paquetes encriptados deben ser process-switched.Paquetes que pasan a través de las interfaces seriales con la encapsulación X.25En la habitación de protocolo x.25, el control de flujo se implementa 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 de multidifusión. **El comando show ip traffic** muestra solamente la información de resumen. Sin embargo, si usted ha configurado el ruteo multicast en el router, usted puede habilitar el Fast-Switching de los paquetes de multidifusión con el **comando ip mroute-cache interface configuration** (el Fast-Switching de los paquetes de multidifusión está apagado 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.
- La traducción (NAT) del IP Network Address se configura en el router, y las porciones de paquetes del Domain Name System (DNS) pasan a través del router. El UDP o los paquetes TCP con el puerto de origen o de destino 53 (DNS) es llevado en batea siempre al nivel de proceso por el NAT.
- Existen otros tipos de paquetes que son impulsados al procesamiento.
- Hay fragmentación del IP datagram. Hay un pequeño aumento en el CPU y memoria suplementaria debidos hacer fragmentos de un IP datagram. Refiera a la resolución fragmentación de IP, los problemas MTU, MSS, y PMTUD con el GRE y 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 hace el debug de los paquetes del IP. Puesto que la utilización de la CPU es ya alta, el proceso del debug tiene que ser realizado con la precaución extrema. El proceso del debug produce las porciones de mensajes, tan solamente **registración mitigada** debe ser configurado.

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

El proceso del debug 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 del IP indeseados 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 marcar primero con el **comando show logging**:

```
router#show loggingSyslog 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 de debbuging, la fecha y hora y las indicaciones de fecha y hora en milisegundos deben ser habilitadas:

```
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 debugging 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 marcar 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 que:

- Un paquete se ha recibido cada cuatro milisegundos
- La dirección IP de origen es 192.168.40.53
- Los paquetes han ingresado en la interfaz Ethernet0/1
- Los paquetes tienen direcciones IP de destino diferentes.
- Los paquetes han sido enviados en la interfaz Ethernet0/0
- La dirección IP del salto siguiente 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 SYN se pueden detectar fácilmente de esta manera porque la presencia de la bandera SYN se indica en la salida de información de depuración:`*Mar 3 03:54:40.436: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.204 (Ethernet0/0), g=10.200.40.1, len 44, forward *Mar 3 03:54:40.440: TCP src=11004, dst=53, seq=280872555, ack=0, win=4128 SYN`

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