Resolución de Problemas de Uso Excesivo de CPU en Catalyst 9000 Causado por el Proceso SISF

Contenido

Introducción

Este documento describe el alto uso de la CPU en los switches Catalyst de Cisco serie 9000 causado por el proceso de las Funciones de seguridad integradas del switch.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de la tecnología de switching LAN
- Conocimientos sobre los switches Catalyst de Cisco serie 9000
- Familiaridad con la interfaz de línea de comandos (CLI) de Cisco IOS® XE
- Familiaridad con la función de seguimiento de dispositivos

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Switches Cisco Catalyst serie 9000
- Versión del software: Todas las versiones

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

Antecedentes

Las funciones de seguridad integradas en el switch (SISF) son un marco desarrollado para optimizar la seguridad en dominios de capa 2. Combina el seguimiento de dispositivos IP (IPDT) y *ciertas funciones de* seguridad de primer salto (FHS) IPv6, para simplificar la migración de una pila IPv4 a una IPv6 o de una pila doble.

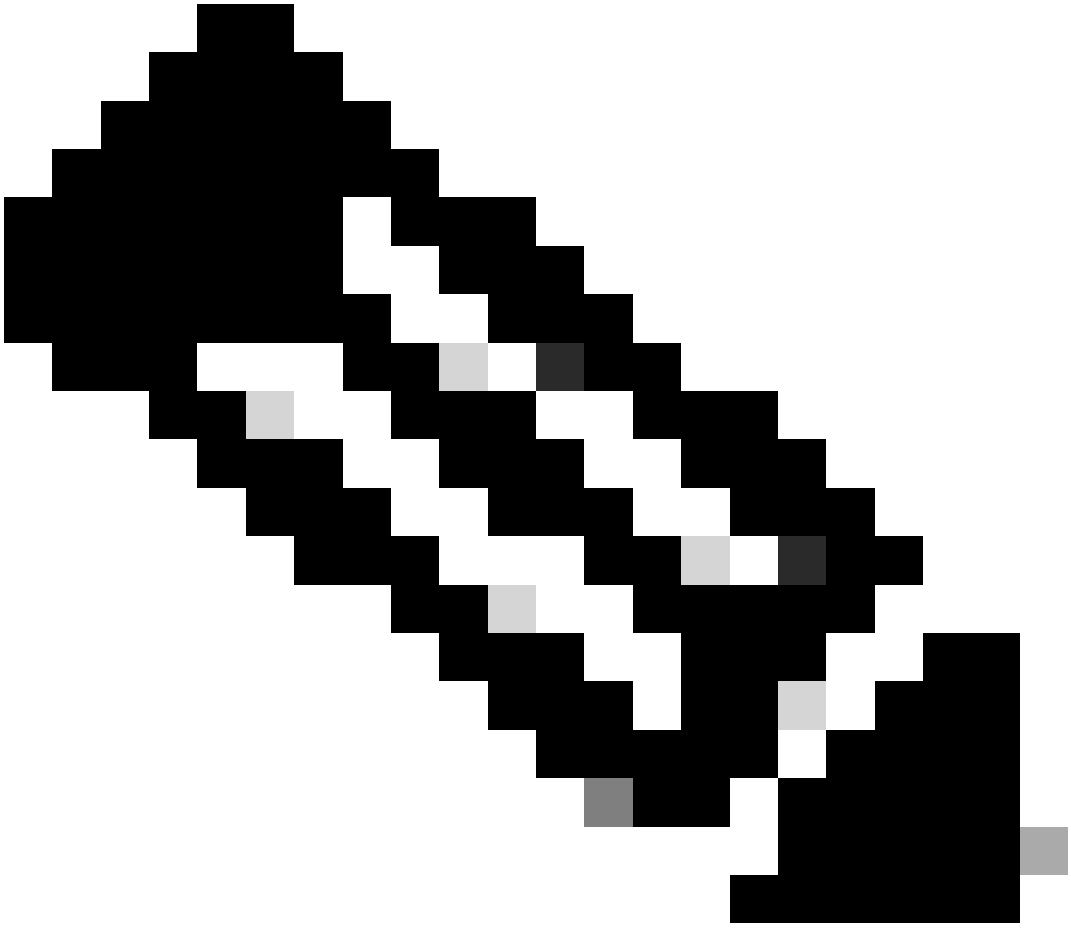
Esta sección proporciona una descripción general del problema de uso elevado de la CPU observado en los switches Catalyst de Cisco serie 9000 causado por el proceso SISF. El problema se identifica a través de comandos CLI específicos y está relacionado con el seguimiento de dispositivos en las interfaces troncales.

Problema

La sonda de señal de mantenimiento enviada por el switch se difunde fuera de todos los puertos cuando se habilita mediante programación SISF. Los switches conectados en el mismo dominio L2 envían estas difusiones a sus hosts, lo que hace que el switch de origen agregue hosts remotos a su base de datos de seguimiento de dispositivos. Las entradas de host adicionales aumentan el uso de memoria en el dispositivo y el proceso de agregar los hosts remotos aumenta el uso de CPU del dispositivo.

Se recomienda determinar el alcance de la política de programación configurando una política en el link ascendente a los switches conectados para definir el puerto como confiable y conectado a un switch.

El problema que se aborda en este documento es el alto uso de la CPU en los switches Catalyst de Cisco serie 9000 causado por el proceso SISF.



Nota: Tenga en cuenta que las funciones dependientes de SISF, como la indagación DHCP, habilitan a SISF, lo que puede activar este problema.

Paso 1: Comprobación del Uso de la CPU

Para identificar el uso elevado de la CPU, utilice el comando this:

<#root>

```
device#

show processes cpu sorted

CPU utilization for five seconds: 93%/6%; one minute: 91%; five minutes: 87%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process

 439     3560284      554004       6426 54.81% 52.37% 47.39%   0 SISF Main Thread


 438     2325444      675817       3440 22.67% 25.17% 26.15%   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
<SNIP>
```

Paso 2: Comprobar base de datos de rastreo de dispositivos

Utilice este comando para verificar la base de datos de rastreo de dispositivos:

<#root>

```
device#

show device-tracking database


Binding Table has 2188 entries, 2188 dynamic (limit 200000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DH
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


    Network Layer Address                  Link Layer Address     Interface  vlan       prlvl      ag

ARP 192.168.187.204                        c815.4ef1.d457         Po1        602        0005       546
ARP 192.168.186.161                        4c49.6c7b.6722         Po1        602        0005       171
ARP 192.168.186.117                        4c5f.702b.61eb         Po1        602        0005       459
ARP 192.168.185.254                        20c1.9bac.5765         Po1        602        0005       546
ARP 192.168.184.157                        c815.4eeb.3d04         Po1        602        0005       3mn


ARP 192.168.1.2                            0004.76e0.cff8         Gi1/0/19   901        0005       23

ARP 192.168.152.97                         001c.7f3c.fd08         Po1        620        0005       54s
ARP 169.254.242.184                        1893.4125.9c57         Po1        602        0005       209
ARP 169.254.239.56                         4c5f.702b.61ff         Po1        602        0005       142
ARP 169.254.239.4                          8c17.59c8.fff0         Po1        602        0005       223
ARP 169.254.230.139                        70d8.235f.2a08         Po1        600        0005       6mn
ARP 169.254.229.77                         4c5f.7028.4231         Po1        602        0005       107


<SNIP>
```

Es evidente que hay múltiples direcciones MAC rastreadas en la interfaz Po1. Esto no se espera si este dispositivo actúa como un switch de acceso y hay un dispositivo final conectado a la interfaz.

Puede verificar los miembros del canal de puerto mediante este comando:

Paso 3: Comprobar Etherchannels

<#root>

device#

show etherchannel summary

```
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)         LACP        Te1/1/1(P)      Te2/1/1(P)
```

Paso 3: Comprobar vecino CDP

Utilice este comando para verificar el vecino CDP:

<#root>

device#

show cdp neighbor

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

C9500            Ten 2/1/1         132              R S   C9500-48Y Twe 2/0/16
C9500            Ten 1/1/1         165              R S   C9500-48Y Twe 1/0/16
```

Un switch Catalyst 9500 está visiblemente conectado en el otro lado. Puede tratarse de otro dispositivo de acceso en configuración de cadena en margarita o de un switch de distribución/núcleo. En cualquier caso, estos dispositivos no pueden estar realizando un seguimiento de las direcciones MAC en interfaces troncales.

Solución

El problema de uso excesivo de la CPU se debe al seguimiento de dispositivos. Desactive el seguimiento de dispositivos en las interfaces troncales.

Para ello, cree una política de seguimiento de dispositivos y conéctela a las interfaces troncales:

Paso 1: Configurar directiva de seguimiento de dispositivos

Cree una política de seguimiento de dispositivos para tratar las interfaces troncales como puertos de confianza:

<#root>

```
device#
configure terminal

device(config)#
device-tracking policy DT_trunk_policy

device(config-device-tracking)#
trusted-port

device(config-device-tracking)#
device-role switch

device(config-device-tracking)#
end
```

Paso 2: Adjuntar la política a la interfaz troncal

<#root>

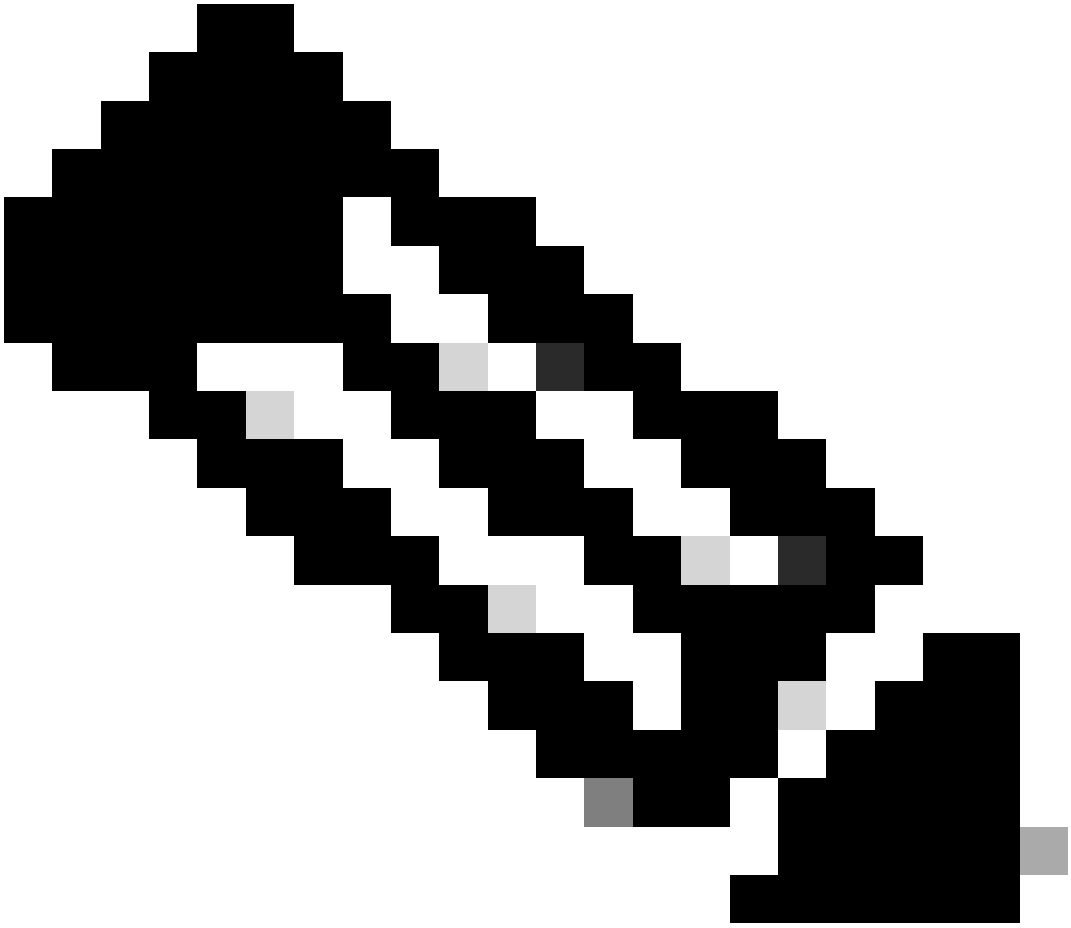
```
device#
cconfigure terminal

device(config)#
interface Po1
```

```
device(config-if)#
device-tracking attach-policy DT_trunk_policy
device(config-if)#
end
```

- **Las opciones de switch de función de dispositivo y de** puerto de confianza le ayudan a diseñar una zona segura eficaz y escalable. Cuando se utilizan juntos, estos dos parámetros ayudan a lograr una distribución eficaz de la creación de entradas en la tabla de enlace. Esto mantiene el tamaño de las tablas de enlace bajo control.
- **Laopción de** puerto **de confianza**: Inhabilita la función de protección en los destinos configurados. Los enlaces aprendidos a través de un puerto confiable tienen preferencia sobre los enlaces aprendidos a través de cualquier otro puerto. Un puerto confiable también recibe preferencia en caso de colisión mientras realiza una entrada en la tabla.
- **Laopción del** rol **de** dispositivo: Indica el tipo de dispositivo que está frente al puerto y que puede ser un nodo o un switch. Para permitir la creación de entradas de enlace para un puerto, configure el dispositivo como un nodo. Para detener la creación de entradas de enlace, configure el dispositivo como switch.

La configuración del dispositivo como un switch es adecuada para configuraciones de switches múltiples, donde la posibilidad de tablas de seguimiento de dispositivos grandes es muy alta. Aquí, un puerto orientado a un dispositivo (un puerto trunk de link ascendente) se puede configurar para detener la creación de entradas de enlace, y el tráfico que llega a dicho puerto puede ser confiable, porque el switch en el otro lado del puerto trunk tiene habilitado el rastreo de dispositivos y ha verificado la validez de la entrada de enlace.



Nota: Si bien hay escenarios donde la configuración de una sola de estas opciones puede ser adecuada, el caso práctico más común es que las opciones de switch de puerto confiable y función de dispositivo se configuren en el puerto.

Información Relacionada

- Soporte técnico y descargas de Cisco
- Solución de problemas de SISF en switches Catalyst serie 9000
- Guía de configuración de seguridad, Cisco IOS XE Dublin 17.12.x (switches Catalyst 9300)

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).