对SISF进程导致的Catalyst 9000上CPU使用率过高进行故障排除

目录

简介

本文档介绍Cisco Catalyst 9000系列交换机上由交换机集成安全功能进程导致的CPU使用率过高。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本了解LAN交换技术
- Cisco Catalyst 9000系列交换机知识
- 熟悉Cisco IOS® XE命令行界面(CLI)
- 熟悉设备跟踪功能

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Catalyst 9000 系列交换机
- 软件版本:全部版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

交换机集成安全功能(SISF)是为优化第2层域的安全性而开发的框架。它将IP设备跟踪(IPDT)和某些IPv6第一跳安全(FHS)功能融合，以简化从IPv4到IPv6堆栈或双堆栈的迁移。

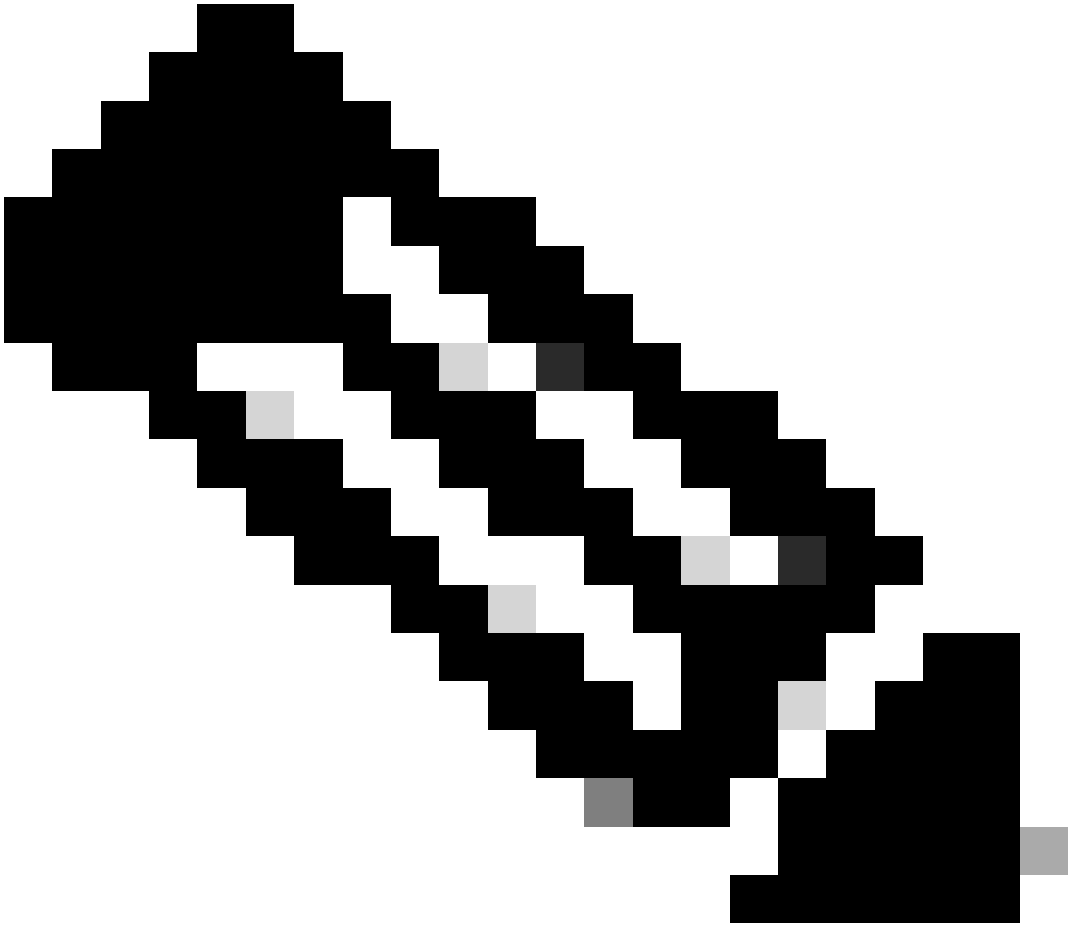
本节概述在Cisco Catalyst 9000系列交换机上观察到由SISF进程导致的CPU使用率较高的问题。此问题通过特定CLI命令确定，并与中继接口上的设备跟踪相关。

问题

当以编程方式启用SISF时，交换机发送的keepalive探针会从所有端口广播出去。同一L2域中的连接交换机将这些广播发送到其主机，导致源交换机将远程主机添加到其设备跟踪数据库中。增加的主机条目会增加设备上的内存使用率，而添加远程主机的过程会增加设备的CPU利用率。

建议通过在连接到交换机的上行链路上配置策略来限定编程策略的范围，以便将端口定义为受信任并连接到交换机。

本文档中涉及的问题是SISF进程导致的Cisco Catalyst 9000系列交换机上的CPU使用率过高。



注意：请注意，DHCP监听等SISF相关功能会启用SISF，从而触发此问题。

步骤 1：检查 CPU 使用率

要确定CPU使用率是否过高，请使用以下命令：

<#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>
```

步骤 2：检查设备跟踪数据库

使用以下命令检查设备跟踪数据库：

```
<#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>
```

很明显，在Po1接口中跟踪到了多个MAC地址。如果此设备用作接入交换机，并且有终端设备连接到接口，则此情况并非预期。

您可以使用以下命令检查端口通道的成员：

步骤 3：检查Etherchannel

<#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)

步骤 3：检查CDP邻居

使用以下命令检查CDP邻居：

<#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

Catalyst 9500交换机的另一端以可视方式连接。这可以是采用菊花链配置的另一接入设备或分布/核心交换机。无论如何，此设备无法跟踪TRUNK接口上的MAC地址。

解决方案

高CPU利用率问题由设备跟踪导致。禁用中继接口上的设备跟踪。

为此，请创建设备跟踪策略并将其连接到中继接口：

步骤 1：配置设备跟踪策略

创建设备跟踪策略，将中继接口视为可信端口：

```
<#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
```

步骤 2：将策略附加到中继接口

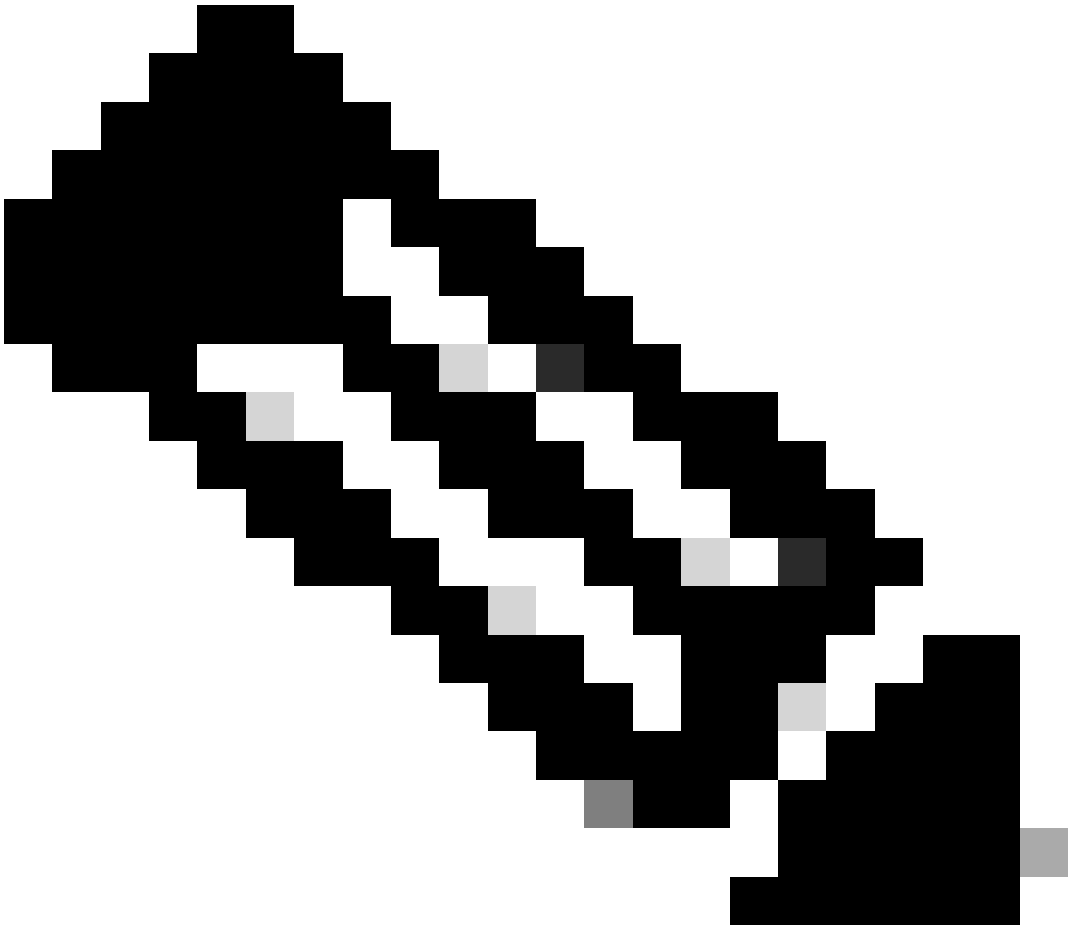
```
<#root>
device#
cconfigure terminal

device(config)#
interface Po1

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

- 设备角色**switchandtrusted-portoptions**可帮助您设计高效且可扩展的安全区域。当一起使用时，这两个参数有助于实现绑定表中条目的创建的高效分布。这样可以控制绑定表的大小。
- **可信端口**选项：在已配置目标上禁用防护功能。通过受信任端口获取的绑定优先于通过任何其他端口获取的绑定。在表中创建条目时，如果发生冲突，也会优先选择受信任端口。
- 设备角色选项：指示面向端口的设备类型，它可以是节点或交换机。要允许为端口创建绑定条目，请将设备配置为节点。要停止创建绑定条目，请将设备配置为交换机。

将设备配置为交换机适用于多台交换机设置，其中大型设备跟踪表的可能性非常高。在这里，面向设备的端口（上行链路中继端口）可配置为停止创建绑定条目，到达该端口的流量可受信任，因为中继端口另一端的交换机已启用设备跟踪并已检查绑定条目的有效性。



注意：虽然有些情况下只配置其中一个选项可能适用，但更常见的使用案例是在端口上配置受信任端口和设备角色交换机选项。

相关信息

- 思科技术支持和下载
- Catalyst 9000系列交换机上的SISF故障排除
- 安全配置指南，Cisco IOS XE Dublin 17.12.x（Catalyst 9300交换机）

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。