對Catalyst 9000上由SISF進程引起的高CPU問題進行故障排除

目錄

簡介

本檔案介紹交換器整合式安全功能程式導致的Cisco Catalyst 9000系列交換器上的CPU使用率高。

必要條件

需求

思科建議您瞭解以下主題：

- 對LAN交換技術有基礎認識
- Cisco Catalyst 9000系列交換機知識
- 熟悉Cisco IOS® XE命令列介面(CLI)
- 熟悉裝置跟蹤功能

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Catalyst 9000 系列交換器
- 軟體版本:所有版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

交換器整合式安全功能(SISF)是專為最佳化第2層網域的安全性而開發的框架。它將IP裝置跟蹤(IPDT)和某些IPv6第一躍點安全(FHS)功能融合，以簡化從IPv4到IPv6堆疊或雙堆疊的遷移。

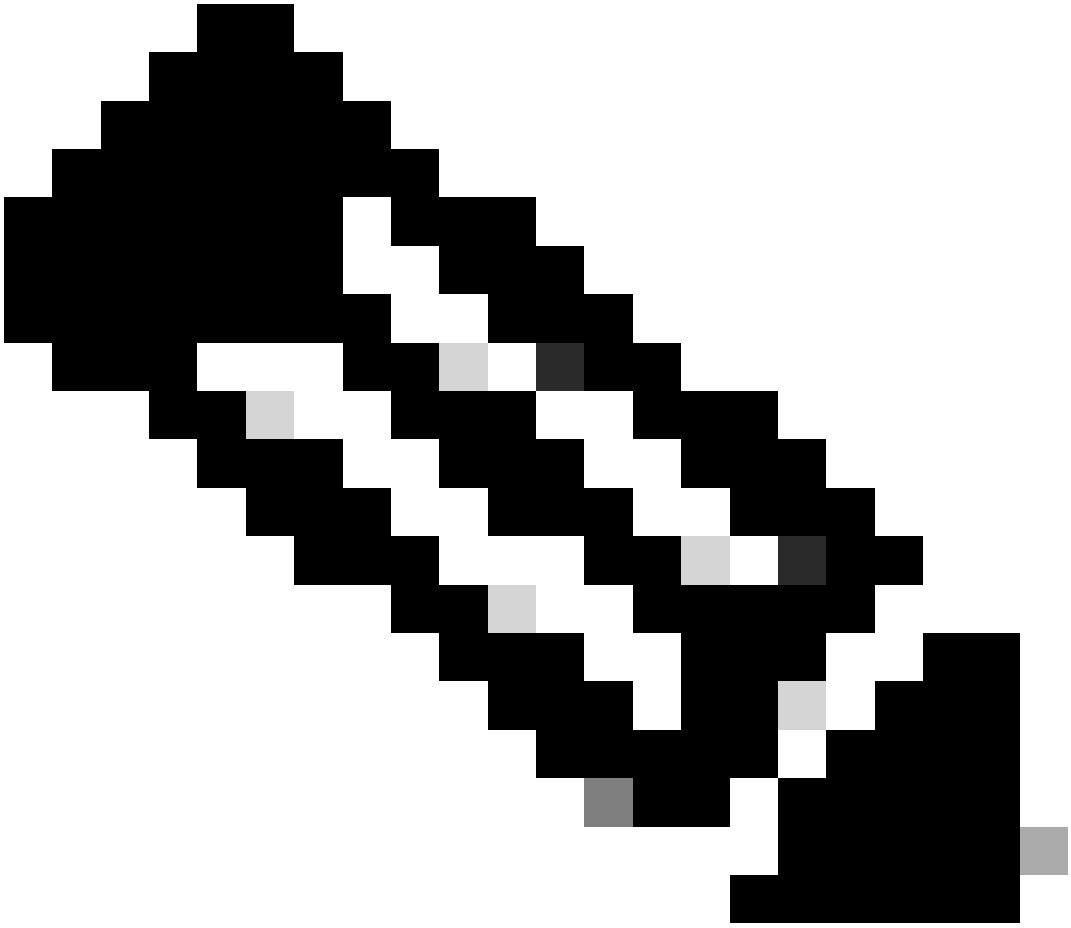
本節概述在Cisco Catalyst 9000系列交換機上觀察到的由SISF進程導致的CPU使用率較高的問題。問題通過特定的CLI命令確定，並與中繼介面上的裝置跟蹤相關。

問題

當以程式設計方式啟用SISF時，交換機傳送的keepalive探測器將從所有埠廣播。同一L2域中的連線交換機將這些廣播傳送到其主機，導致源交換機將遠端主機新增到其裝置跟蹤資料庫。附加主機條目增加了裝置上的記憶體使用率，新增遠端主機的過程增加了裝置的CPU使用率。

建議通過在連線到交換機的上行鏈路上配置策略來限定程式設計策略的範圍，將埠定義為受信任並連線到交換機。

本文所述的問題是SISF進程導致的Cisco Catalyst 9000系列交換機上的CPU使用率高。



附註：請注意，DHCP監聽等SISF相關功能會啟用SISF，從而觸發此問題。

步驟 1:檢查CPU利用率

要確定CPU使用率是否較高，請使用以下命令：

<#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>
```

步驟 2:檢查裝置跟蹤資料庫

使用以下命令檢查裝置跟蹤資料庫：

<#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>
```

很明顯，在Po1介面中有多個MAC地址被跟蹤。如果此裝置用作接入交換機，並且有終端裝置連線到介面，則不需要此功能。

您可以使用以下命令檢查連線埠通道的成員：

步驟 3:檢查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)

步驟 3:檢查CDP鄰居

使用以下命令檢查CDP鄰居：

<#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交換機的另一端可見連線。這可能是採用菊花鏈配置的另一接入裝置或分佈/核心交換機。在任何情況下，此裝置都無法跟蹤TRUNK介面上的MAC地址。

解決方案

CPU使用率較高的問題是由裝置跟蹤引起的。禁用中繼介面上的裝置跟蹤。

為此，請建立裝置跟蹤策略並將其連線到中繼介面：

步驟 1:配置裝置跟蹤策略

建立裝置跟蹤策略以將中繼介面視為可信埠：

```
<#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
```

步驟 2:將策略附加到中繼介面

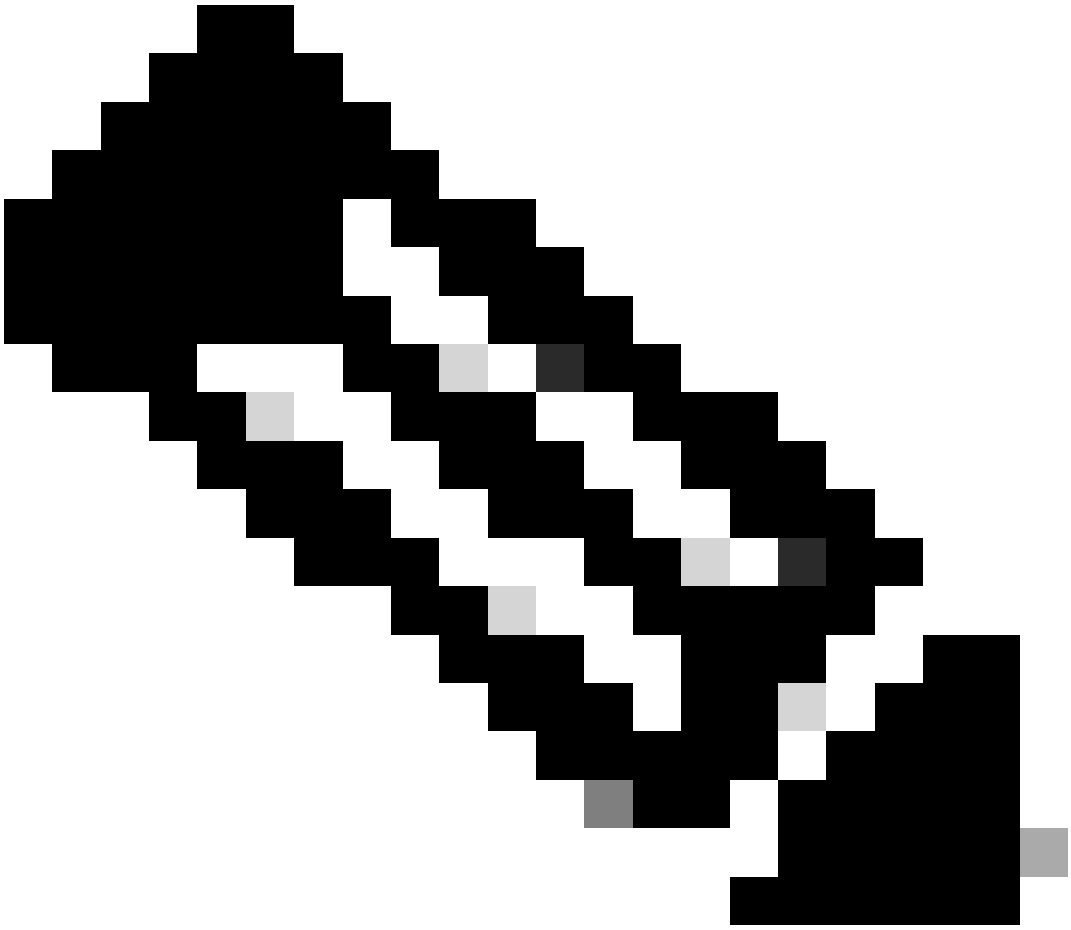
```
<#root>
device#
cconfigure terminal

device(config)#
interface Po1

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

- **裝置角色switchandtrusted-portoptions**可幫助您設計高效且可擴展的安全區域。當一起使用時，這兩個引數有助於實現繫結表中條目的建立的高效分佈。這樣可以控制繫結表的大小。
- **Trusted-**portoption:在已配置的目標上禁用防護功能。通過受信任埠獲知的繫結優先於通過任何其他埠獲知的繫結。在表中建立條目時，如果發生衝突，也會優先使用受信任埠。
- **Device-role**選項：指示面向埠的裝置的型別，可以是節點或交換機。要允許為埠建立繫結條目，請將裝置配置為節點。要停止建立繫結條目，請將裝置配置為交換機。

將裝置配置為交換機適用於多個交換機設定，在這些設定中，大型裝置跟蹤表的可能性非常高。在這裡，面向裝置的埠（上行鏈路中繼埠）可配置為停止建立繫結條目，到達該埠的流量可受信任，因為中繼埠另一端的交換機已啟用裝置跟蹤，並且已檢查繫結條目的有效性。



附註：雖然有些情況下只配置其中一個選項可能適合，但更常見的使用案例是在埠上配置受信任埠和裝置角色交換機選項。

相關資訊

- 思科技術支援與下載
- Catalyst 9000系列交換器上的SISF疑難排解
- 安全配置指南，Cisco IOS XE都柏林17.12.x（Catalyst 9300交換機）

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。