Dépannage d'une CPU élevée sur Catalyst 9000 causée par un processus SISF

Table des matières

Introduction

Ce document décrit l'utilisation élevée du CPU sur les commutateurs de la gamme Cisco Catalyst 9000 causée par le processus des fonctions de sécurité intégrées du commutateur.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base de la technologie de commutation LAN
- Connaissance des commutateurs Cisco Catalyst 9000
- Connaissance de l'interface de ligne de commande (CLI) de Cisco IOS® XE
- Familiarité avec la fonction de suivi des périphériques

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Commutateurs de la gamme Cisco Catalyst 9000
- Version du logiciel: Toutes les versions

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Les fonctions de sécurité intégrées des commutateurs (SISF) sont un cadre développé pour optimiser la sécurité dans les domaines de couche 2. Il fusionne la fonctionnalité IP Device Tracking (IPDT) et *certaines* fonctionnalités de sécurité au premier saut (FHS) IPv6, pour simplifier la migration d'une pile IPv4 vers une pile IPv6 ou une double pile.

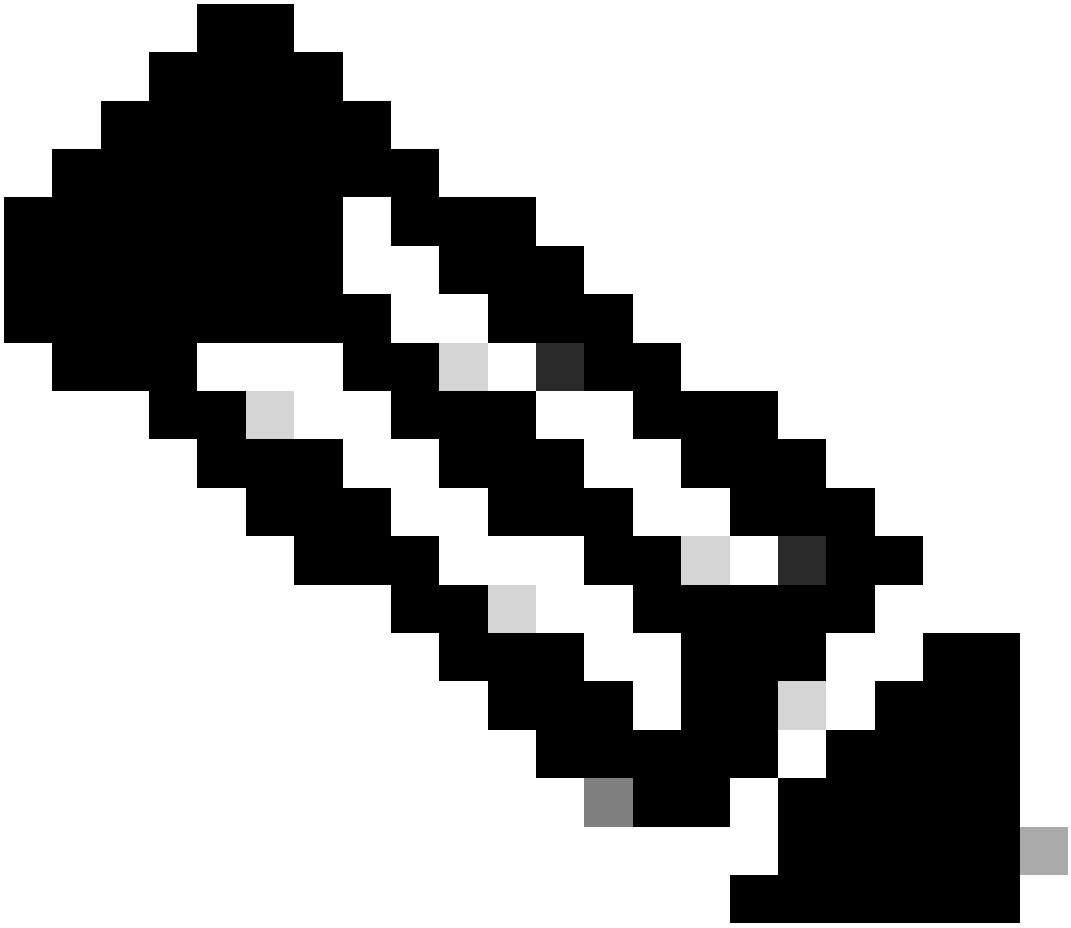
Cette section présente le problème d'utilisation élevée du CPU observé sur les commutateurs de la gamme Cisco Catalyst 9000 causé par le processus SISF. Le problème est identifié par des commandes CLI spécifiques et est lié au suivi des périphériques sur les interfaces trunk.

Problème

La sonde keepalive envoyée par le commutateur est diffusée à partir de tous les ports lorsque SISF est activé par programme. Les commutateurs connectés dans le même domaine de couche 2 envoient ces diffusions à leurs hôtes, ce qui a pour effet que le commutateur d’origine ajoute des hôtes distants à sa base de données de suivi des périphériques. Les entrées d'hôte supplémentaires augmentent l'utilisation de la mémoire sur le périphérique et le processus d'ajout des hôtes distants augmente l'utilisation du processeur du périphérique.

Il est recommandé de définir la stratégie de programmation en configurant une stratégie sur la liaison ascendante vers les commutateurs connectés afin de définir le port comme étant sécurisé et connecté à un commutateur.

Le problème abordé dans ce document est une utilisation CPU élevée sur les commutateurs de la gamme Cisco Catalyst 9000 causée par le processus SISF.



Remarque : N'oubliez pas que les fonctions SISF, telles que la surveillance DHCP, activent le protocole SISF, ce qui peut déclencher ce problème.

Étape 1 : Contrôle de l'utilisation de la CPU

Pour identifier l'utilisation élevée du CPU, utilisez la commande suivante :

<#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>
```

Étape 2 : Vérifier la base de données de suivi

Utilisez la commande suivante pour vérifier la base de données de suivi des périphériques :

<#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>
```

Il est évident que plusieurs adresses MAC sont suivies dans l'interface Po1. Cela n'est pas prévu si ce périphérique agit en tant que commutateur d'accès et qu'un périphérique final est connecté à l'interface.

Vous pouvez vérifier les membres du canal de port à l'aide de cette commande :

Étape 3 : Vérifier les 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)
```

Étape 3 : Vérifier le voisin CDP

Utilisez la commande suivante pour vérifier le voisin 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 commutateur Catalyst 9500 est visiblement connecté de l'autre côté. Il peut s'agir d'un autre périphérique d'accès en configuration en chaîne ou d'un commutateur de distribution/coeur de réseau. Dans tous les cas, ces périphériques ne peuvent pas effectuer le suivi des adresses MAC sur les interfaces d’agrégation.

Solution

Le problème d'utilisation élevée du CPU est causé par le suivi des périphériques. Désactivez le suivi des périphériques sur les interfaces d'agrégation.

Pour ce faire, créez une stratégie de suivi des périphériques et attachez-la aux interfaces d'agrégation :

Étape 1 : Configurer la stratégie de suivi des périphériques

Créez une stratégie de suivi des périphériques pour traiter les interfaces trunk comme des ports approuvés :

<#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
```

Étape 2 : Association de la stratégie à l'interface de liaison

<#root>

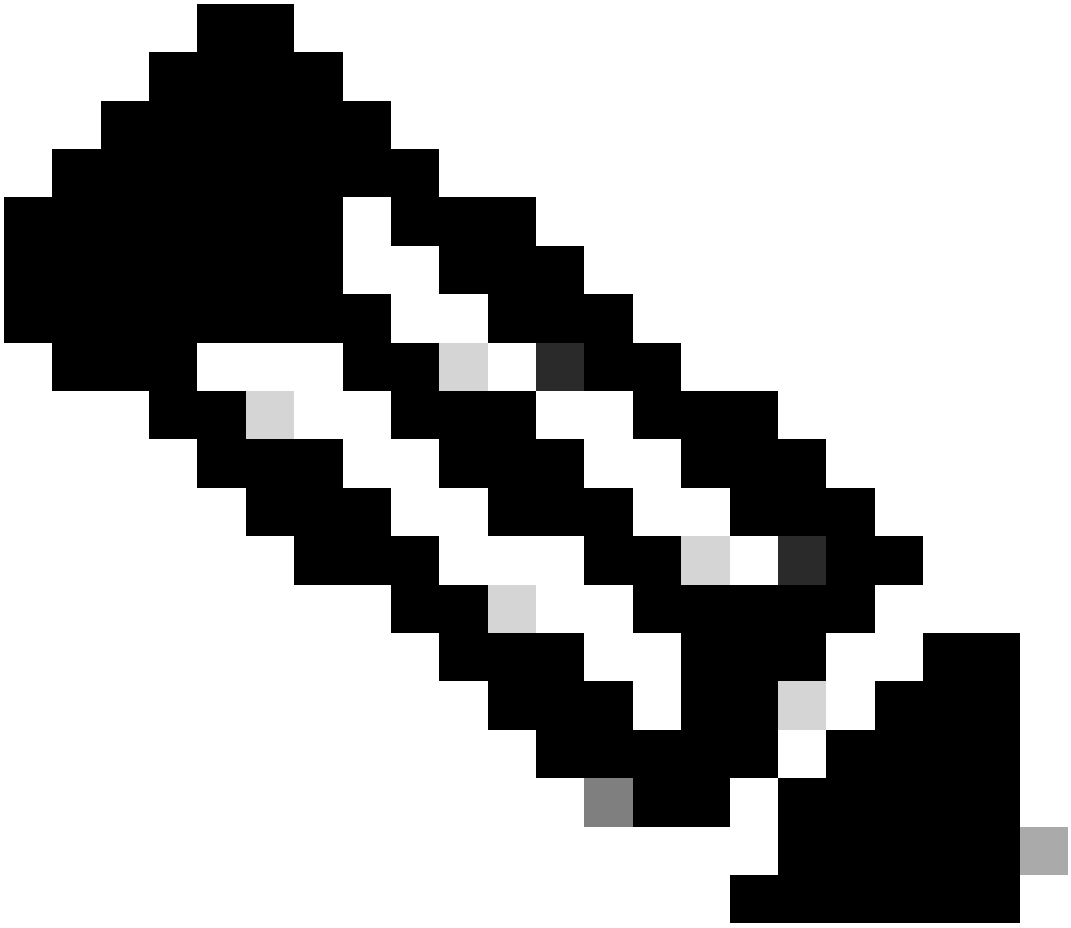
```
device#
cconfigure terminal

device(config)#
interface Po1
```

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

- **Le commutateur de rôle de périphérique et les options de** port **sécurisé** vous aident à concevoir une zone sécurisée efficace et évolutive. Utilisés conjointement, ces deux paramètres vous aident à répartir efficacement la création d'entrées dans la table de liaison. Cela permet de garder la taille des tables de liaison sous contrôle.
- **L'**option **de** port **approuvé** : Désactive la fonction de protection sur les cibles configurées. Les liaisons apprises via un port de confiance ont la préférence sur les liaisons apprises via tout autre port. Un port sécurisé est également privilégié en cas de collision lors de la création d'une entrée dans la table.
- **L'option device-**role : Indique le type de périphérique qui fait face au port et qui peut être un noeud ou un commutateur. Pour permettre la création d'entrées de liaison pour un port, vous devez configurer le périphérique en tant que noeud. Pour arrêter la création d'entrées de liaison, vous devez configurer le périphérique en tant que commutateur.

La configuration du périphérique en tant que commutateur est adaptée à plusieurs configurations de commutateurs, où la possibilité de grandes tables de suivi de périphériques est très élevée. Ici, un port faisant face à un périphérique (un port agrégé de liaison montante) peut être configuré pour arrêter la création d'entrées de liaison, et le trafic arrivant à un tel port peut être approuvé, parce que le commutateur de l'autre côté du port agrégé a le suivi de périphérique activé et il a vérifié la validité de l'entrée de liaison.



Remarque : Bien qu'il existe des scénarios dans lesquels la configuration de l'une ou l'autre de ces options peut convenir, le cas d'utilisation le plus courant est que les options de commutateur de port de confiance et de rôle de périphérique soient configurées sur le port.

Informations connexes

- Assistance technique de Cisco et téléchargements
- Dépannage du SISF sur les commutateurs de la gamme Catalyst 9000
- Guide de configuration de la sécurité, Cisco IOS XE Dublin 17.12.x (commutateurs Catalyst 9300)

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.