SISF 프로세스로 인한 Catalyst 9000의 높은 CPU 문제 해결

목차

소개

이 문서에서는 Cisco Catalyst 9000 Series 스위치에서 스위치 통합 보안 기능 프로세스로 인한 높은 CPU 사용률에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- LAN 스위칭 기술에 대한 기본 이해
- Cisco Catalyst 9000 Series 스위치에 대한 지식
- Cisco IOS® XE CLI(Command-Line Interface)에 익숙함
- 디바이스 추적 기능에 대한 숙지

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Catalyst 9000 Series Switches
- 소프트웨어 버전: 모든 버전

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

SISF(Switch Integrated Security Features)는 레이어 2 도메인의 보안을 최적화하기 위해 개발된 프레임워크입니다. IPDT(IP Device Tracking)와 특정 *IPv*6 FHS(First Hop Security) 기능을 병합하여 IPv4에서 IPv6 스택 또는 듀얼 스택으로의 마이그레이션을 간소화합니다.

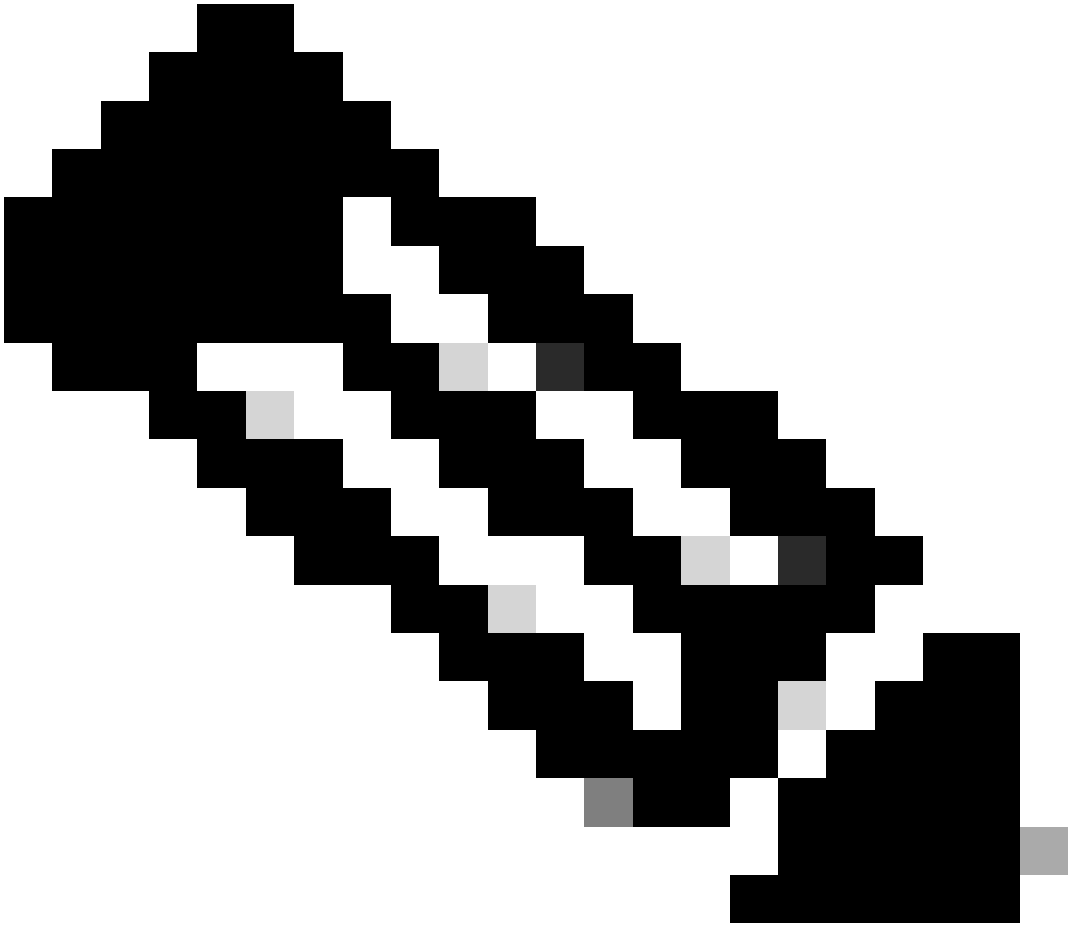
이 섹션에서는 SISF 프로세스로 인해 Cisco Catalyst 9000 Series 스위치에서 관찰되는 높은 CPU 사용률 문제에 대한 개요를 제공합니다. 이 문제는 특정 CLI 명령을 통해 식별되며 트렁크 인터페이스의 디바이스 추적과 관련이 있습니다.

문제

스위치에서 보낸 keepalive 프로브는 SISF가 프로그래밍 방식으로 활성화될 때 모든 포트에서 브로드캐스트됩니다. 동일한 L2 도메인에 연결된 스위치는 이러한 브로드캐스트를 호스트로 전송하여 원래 스위치가 디바이스 추적 데이터베이스에 원격 호스트를 추가하게 합니다. 추가 호스트 엔트리는 디바이스의 메모리 사용량을 증가시키고 원격 호스트를 추가하는 프로세스는 디바이스의 CPU 사용률을 증가시킵니다.

포트를 신뢰할 수 있고 스위치에 연결된 것으로 정의하려면 연결된 스위치에 대한 업링크에 정책을 구성하여 프로그래밍 정책의 범위를 지정하는 것이 좋습니다.

이 문서에서 다루는 문제는 SISF 프로세스로 인해 Cisco Catalyst 9000 Series 스위치의 CPU 사용률이 높다는 것입니다.



참고: DHCP 스누핑과 같은 SISF 종속 기능은 SISF를 활성화하며, 이는 이 문제를 유발할 수 있습니다.

1단계: CPU 사용률 확인

높은 CPU 사용률을 식별하려면 다음 명령을 사용합니다.

<#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>
```

2단계: 디바이스 추적 데이터베이스 확인

디바이스 추적 데이터베이스를 확인하려면 다음 명령을 사용합니다.

```
<#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       234

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>
```

Po1 인터페이스에서 추적되는 여러 MAC 주소가 있음이 분명합니다. 이 디바이스가 액세스 스위치로 작동하고 있으며 인터페이스에 연결된 엔드 디바이스가 있는 경우 이는 예상되지 않습니다.

다음 명령을 사용하여 포트 채널의 멤버를 확인할 수 있습니다.

3단계: Etherchannel 확인

<#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)

3단계: CDP 네이버 확인

CDP 인접 디바이스를 확인하려면 다음 명령을 사용합니다.

<#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 스위치가 다른 쪽에 시각적으로 연결되어 있습니다. 이는 데이지 체인 컨피그레이션의 또 다른 액세스 디바이스 또는 디스트리뷰션/코어 스위치일 수 있습니다. 어떤 경우에도 이 디바이스는 트렁크 인터페이스에서 MAC 주소를 추적할 수 없습니다.

솔루션

높은 CPU 사용률 문제는 장치 추적으로 인해 발생합니다. 트렁크 인터페이스에서 디바이스 추적을 비활성화합니다.

이렇게 하려면 디바이스 추적 정책을 생성하고 이를 트렁크 인터페이스에 연결합니다.

1단계: 디바이스 추적 정책 구성

트렁크 인터페이스를 신뢰할 수 있는 포트로 처리하기 위한 디바이스 추적 정책을 생성합니다.

```
<#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
```

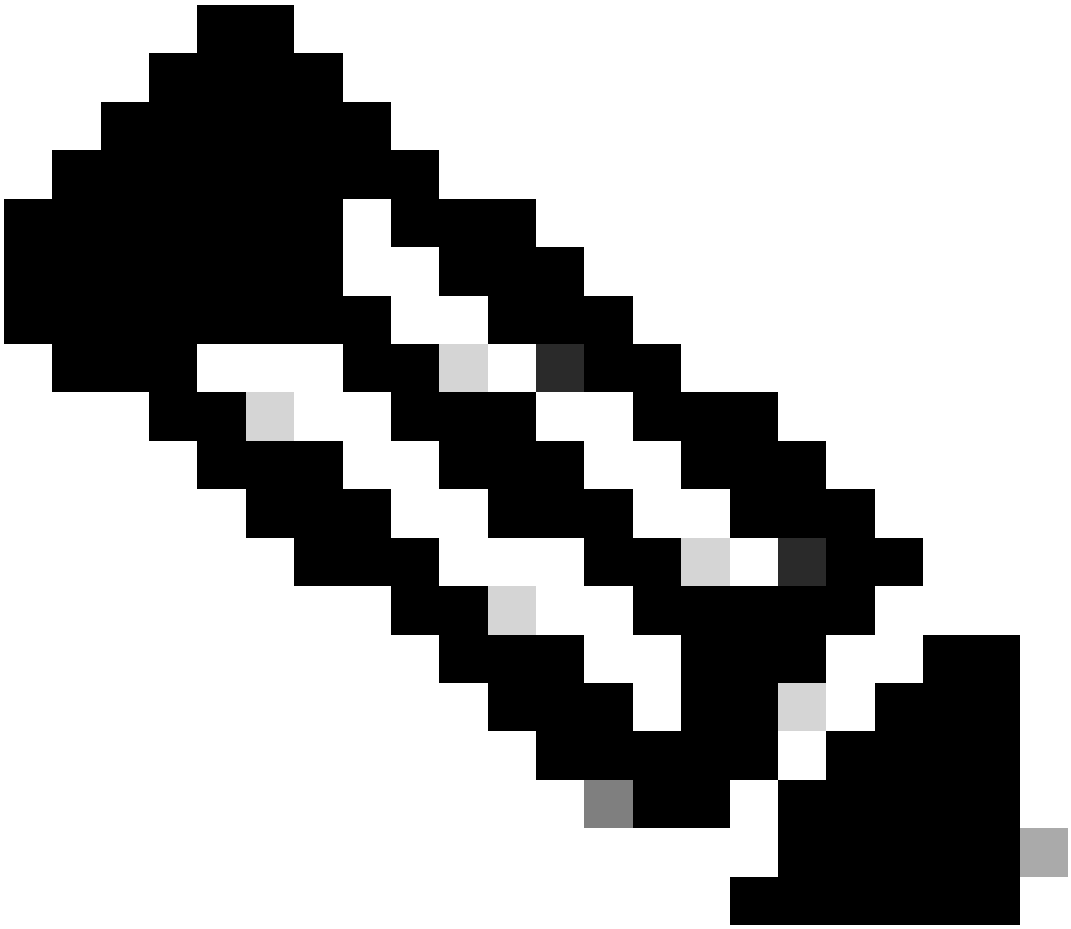
2단계: 트렁크 인터페이스에 정책 연결

```
<#root>
device#
cconfigure terminal

device(config)#
interface Po1

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

end

- **디바이스 역할 전환신뢰할 수 있는** 포트옵션을 통해 효율적이고 확장 가능한 보안 영역을 설계할 수 있습니다. 이 두 매개 변수를 함께 사용하면 바인딩 테이블의 항목 생성을 효율적으로 배포할 수 있습니다. 이렇게 하면 바인딩 테이블의 크기를 제어할 수 있습니다.
- **신뢰할 수 있는** 옵션: 구성된 대상에서 보호 기능을 비활성화합니다. 신뢰할 수 있는 포트를 통해 학습된 바인딩은 다른 포트를 통해 학습된 바인딩보다 우선합니다. 신뢰할 수 있는 포트에는 테이블의 항목을 입력하는 동안 충돌이 발생할 경우 기본 설정이 제공됩니다.
- **device-**roleoption: 포트를 향하는 디바이스 유형을 나타내며 노드 또는 스위치일 수 있습니다. 포트에 대한 바인딩 항목의 생성을 허용하려면 디바이스를 노드로 구성합니다. 바인딩 항목 생성을 중지하려면 디바이스를 스위치로 구성합니다.

디바이스를 스위치로 구성하는 것은 대규모 디바이스 추적 테이블의 가능성이 매우 높은 여러 스위치 설정에 적합합니다. 여기서, 트렁크 포트의 반대편에 있는 스위치는 장치 추적이 활성화되어 있고, 바인딩 엔트리의 유효성을 체크했기 때문에, 디바이스를 향하는 포트(업링크 트렁크 포트)는 바인딩 엔트리의 생성을 중단하도록 구성될 수 있으며, 이러한 포트에 도착하는 트래픽은 신뢰할 수 있다.



참고: 이러한 옵션 중 하나만 구성하는 것이 적합한 시나리오도 있지만, 가장 일반적인 활용 사례는 포트에 구성할 신뢰할 수 있는 포트 및 디바이스 역할 스위치 옵션 모두에 해당됩니다.

관련 정보

- Cisco 기술 지원 및 다운로드
- Catalyst 9000 Series 스위치의 SISF 문제 해결
- 보안 컨피그레이션 가이드, Cisco IOS XE Dublin 17.12.x(Catalyst 9300 스위치)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.