Catalyst 9000 Series 스위치의 SISF 문제 해결

목차

소개

이 문서에서는 Catalyst 9000 제품군 스위치에 사용되는 SISF(Switch Integrated Security Features)에 대해 설명합니다. 또한 SISF를 사용하는 방법과 다른 기능과 상호 작용하는 방법에 대해서도 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco IOS® XE 17.3.x를 실행하는 Cisco Catalyst 9300-48P를 기반으로 합니다

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

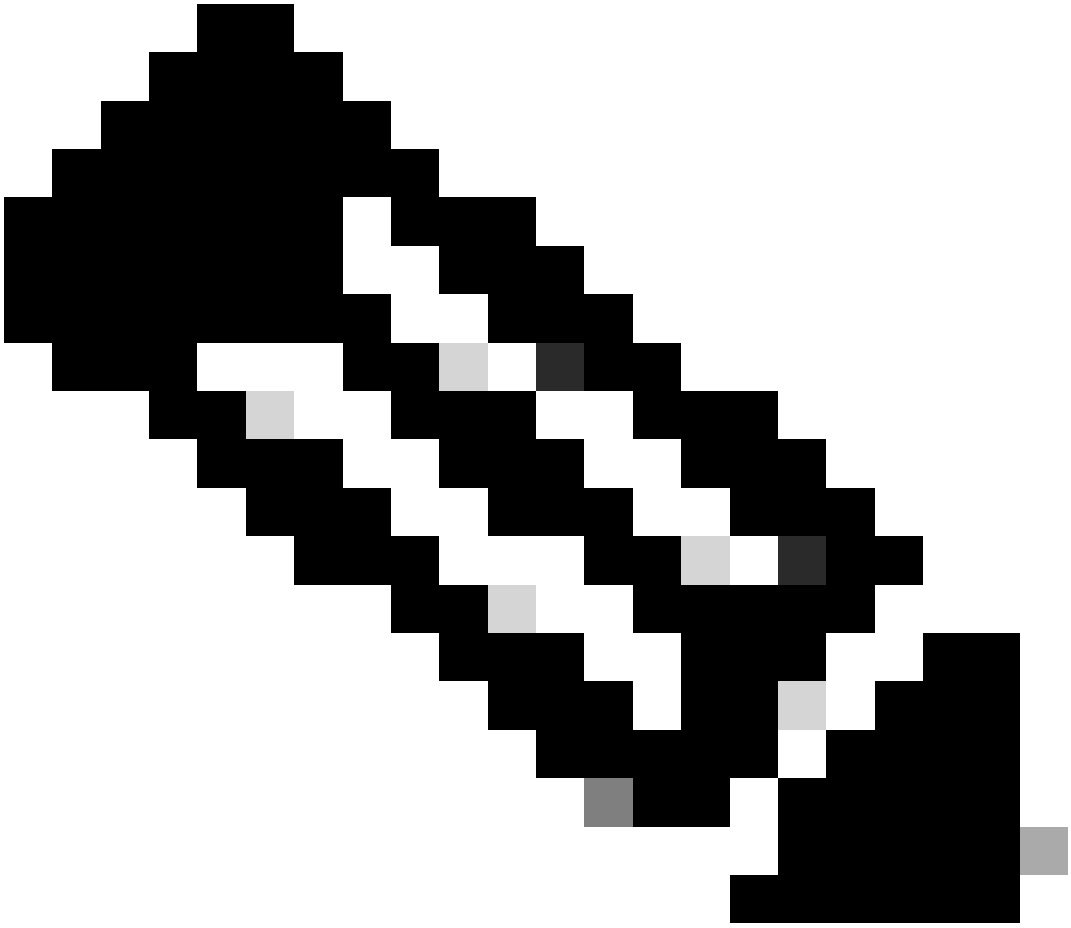
참고: 다른 Cisco 플랫폼에서 이러한 기능을 활성화하는 데 사용되는 명령은 해당 설정 가이드를 참조하십시오.

관련 제품

이 문서는 다음과 같은 하드웨어 및 소프트웨어 버전에서도 사용할 수 있습니다.

- Catalyst 9200
- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600

17.3.4 이상 Cisco IOS XE 소프트웨어 버전



참고: 이 문서는 SISF 대 디바이스 추적을 사용하는 대부분의 Cisco IOS XE 버전에도 적용됩니다.

배경 정보

개요

SISF는 호스트 바인딩 테이블을 제공하며, 이 테이블의 정보를 사용하는 기능 클라이언트가 있습니다. 호스트 활동을 추적하고 테이블을 동적으로 채우는 데 도움이 되는 DHCP, ARP, ND, RA와 같은 패킷을 조명하여 항목이 테이블에 채워집니다. L2 도메인에 무음 호스트가 있는 경우 정적 항목을 사용하여 SISF 테이블에 항목을 추가할 수 있습니다.

SISF는 정책 모델을 사용하여 스위치에서 디바이스 역할 및 추가 설정을 구성합니다. 단일 정책은 인터페이스 또는 VLAN 레벨에 적용할 수 있습니다. 정책이 VLAN에 적용되고 다른 정책이 인터페이스에 적용되는 경우 인터페이스 정책이 우선합니다.

SISF를 사용하여 테이블의 호스트 수를 제한할 수도 있지만 IPv4와 IPv6 동작 간에는 차이가 있습

니다. SISF 제한이 설정되어 있고 이에 도달한 경우:

- IPv4 호스트는 계속 작동하지만 제한을 초과하는 항목은 SISF 테이블에 추가되지 않습니다
- SISF 테이블에 추가되지 않은 IPv6 호스트는 네트워크에 진입할 수 없으며 SISF 테이블에 새 항목이 추가되지 않습니다.

16.9.x 이상부터 SISF 클라이언트 기능 우선 순위가 도입되었습니다. SISF에 대한 업데이트를 제어하는 옵션을 추가하며, 둘 이상의 클라이언트가 바인딩 테이블을 사용 중인 경우 우선 순위가 더 높은 기능의 업데이트가 적용됩니다. 여기서는 "mac당 IPv4/IPv6에 대한 주소 수 제한" 설정을 제외하고 우선순위가 가장 낮은 정책 설정이 적용됩니다.

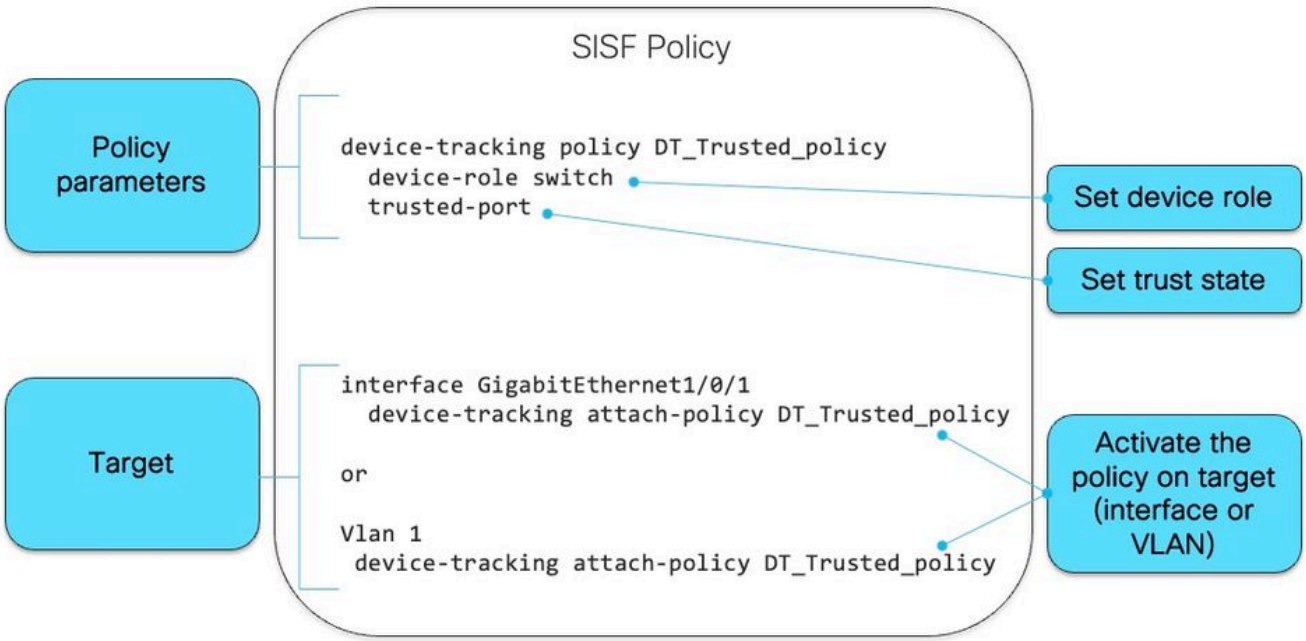
디바이스 추적을 활성화해야 하는 몇 가지 기능의 예는 다음과 같습니다.

- LISP/EVPN
- 점1x
- 웹 인증
- CTS
- DHCP 스누핑

참고: 우선순위는 정책 설정을 선택하는 데 사용됩니다.

CLI에서 만든 정책의 우선순위가 가장 높으므로(128) 사용자가 프로그래밍 방식의 정책과 다른 정책 설정을 적용할 수 있습니다. 사용자 지정 정책에서 구성 가능한 모든 설정을 수동으로 변경할 수 있습니다.

다음 이미지는 SISF 정책 및 읽기 방법의 예입니다.



정책 내부의 protocol 키워드에는 SISF 데이터베이스를 채우는 데 사용되는 패킷 유형을 확인할 수 있는 옵션이 있습니다.

<#root>

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

?

device-tracking policy configuration mode:
  data-glean            binding recovery by data traffic source address
                        gleaning
  default               Set a command to its defaults
  destination-glean     binding recovery by data traffic destination address
                        gleaning
  device-role           Sets the role of the device attached to the port
  distribution-switch   Distribution switch to sync with
  exit                  Exit from device-tracking policy configuration mode
  limit                 Specifies a limit
  medium-type-wireless  Force medium type to wireless
  no                    Negate a command or set its defaults
  prefix-glean          Glean prefixes in RA and DHCP-PD traffic


protocol              Sets the protocol to glean (default all) <--

  security-level        setup security level
  tracking              Override default tracking behavior
  trusted-port          setup trusted port
  vpc                   setup vpc port

switch(config-device-tracking)#

protocol ?

  arp    Glean addresses in ARP packets
  dhcp4  Glean addresses in DHCPv4 packets
  dhcp6  Glean addresses in DHCPv6 packets
  ndp    Glean addresses in NDP packets
  udp    Gleaning from UDP packets
```

SISF 프로그래밍 및 클라이언트 기능

다음 표의 기능은 활성화될 때 SISF를 프로그램적으로 활성화하거나 SISF에 대한 클라이언트 역할을 합니다.

SISF 프로그래밍 기능	SISF 클라이언트 기능
VLAN의 LISP	점1x
VLAN의 EVPN	웹 인증
DHCP 스누핑	CTS

SISF를 활성화하는 기능 없이 구성된 디바이스에서 SISF 클라이언트 기능이 활성화된 경우 호스트에 연결하는 인터페이스에 사용자 지정 정책을 구성해야 합니다.

SISF 정보를 사용하는 IPv4 기능

- CTS
- IEEE 802.1x
- 리스프
- EVPN
- DHCP 스누핑(SISF만 활성화하지만 이를 사용하지 않음)
- IP Source Guard

SISF 정보를 사용하는 IPv6 기능

- IPv6 RA(Router Advertisement) 가드
- IPv6 DHCP 가드, 레이어 2 DHCP 릴레이
- IPv6 DAD(Duplicate Address Detection) 프록시
- 플러딩 억제
- IPv6 소스 가드
- IPv6 대상 가드
- 라 스로틀러
- IPv6 프리픽스 가드

디바이스 추적

장치 추적의 주요 역할은 네트워크 내 엔드-노드의 존재, 위치, 이동을 추적하는 것이다. SISF는 스위치에서 수신한 트래픽을 스누핑하고 디바이스 ID(MAC 및 IP 주소)를 추출하여 바인딩 테이블에 저장합니다. IEEE 802.1X, 웹 인증, Cisco TrustSec 및 LISP 등 여러 기능은 이 정보의 정확성에 따라 올바르게 작동합니다. SISF 기반 디바이스 추적은 IPv4 및 IPv6를 모두 지원합니다. 클라이언트가 IP를 학습할 수 있는 5가지 방법이 지원됩니다.

- DHCPv4
- DHCPv6
- ARP
- NDP
- 데이터 청소

포트 채널의 SISF

포트 채널(또는 이더 채널)에서 디바이스 추적이 지원됩니다. 그러나 개별 포트 채널 멤버가 아닌 채널 그룹에 컨피그레이션을 적용해야 합니다. 바인딩 관점에서 볼 때 나타나는(알려진) 유일한 인터페이스는 port-channel입니다.

프로브 및 데이터베이스 튜닝

프로브:

- IPDT에는 초기 프로브를 10초 동안 지연시켜 중복된 주소 문제를 해결하는 명령이 있었습니다. 링크 작동 시 "ip 장치 추적 프로브 지연"입니다.
- SISF에는 첫 번째 프로브를 보내기 전에 대기하는 대기 타이머가 이미 내장되어 있습니다. 구성할 수 없으며 동일한 문제를 해결합니다. 이 명령은 SISF 코드에 있으므로 더 이상 이 명령이 필요하지 않습니다

데이터베이스:

SISF에서 몇 가지 옵션을 구성하여 데이터베이스에 항목이 유지되는 기간을 제어할 수 있습니다.

```
<#root>

tracking enable reachable-lifetime <second|infinite>

<-- how long an entry is kept reachable (or keep permanently reachable)


tracking disable stale-lifetime <seconds|infinite>

<-- how long and entry is kept inactive before deletion (or keep permanently inactive)
```

IP 디바이스 추적

호스트가 폴링되는 항목의 수명 주기:

- SISF는 mac당 IPv4/IPv6 바인딩을 유지 관리하며, IP 학습이 성공하면 바인딩이 REACHABLE 상태로 전환됩니다.
- SISF는 제어 패킷을 모니터링하여 라이브니스 클라이언트 추적
- 클라이언트에서 5분 동안 제어 패킷이 없는 경우 Binding은 VERIFY 상태로 전환되고 클라이언트로 프로브를 전송합니다
- 클라이언트가 프로브에 응답하지 않으면 바인딩은 STALE 상태 또는 REACHABLE 상태로 전환됩니다
- STALE 항목의 기본 시간 제한은 24시간이며 구성 가능합니다.
- STALE 항목은 24시간 후에 삭제됩니다(또는 구성된 시간 초과 값).

도난 감지

노드 절도 유형:

- IP 도난(동일한 ip, 다른 mac, 다른/동일한 포트)
- MAC 도난(동일한 MAC, 다른 IP, 다른 포트)
- MAC IP 도난(동일한 mac, 동일한 ip, 다른 포트)

IP 보안 기능

다음은 SISF 종속 기능의 일부입니다.

- NDP 검사: IPv6 NDP 메시지 검사

- NDP 주소 조정:NDP 트래픽을 스누핑하여 수집한 정보로 바인딩 테이블을 채웁니다.
- 디바이스 추적: 라이브니스 메커니즘을 통해 엔드 디바이스 활동 모니터링
- 스누핑: NDP, ARP 및 DHCP 메시지에서 주소를 수집합니다. 인증되지 않은 메시지 차단
- DHCPv4 Relay: 구성된 도우미 주소에 DHCP 브로드캐스트 패킷을 릴레이합니다.
- NDP & ARP 멀티캐스트 억제: 유니캐스트로 변환하거나 대상을 대신하여 응답함으로써 멀티캐스트 NDP 메시지를 억제합니다.
- DAD 프록시:중복 주소 감지 및 대상 클라이언트 대신 NA 전송
- DHCPv4 요구 사항: 클라이언트가 DHCP를 통해서만 IP를 가져오도록 강제합니다.

SISF 주의 사항

SISF와 관련하여 가장 자주 관찰되는 동작은 다음과 같습니다.

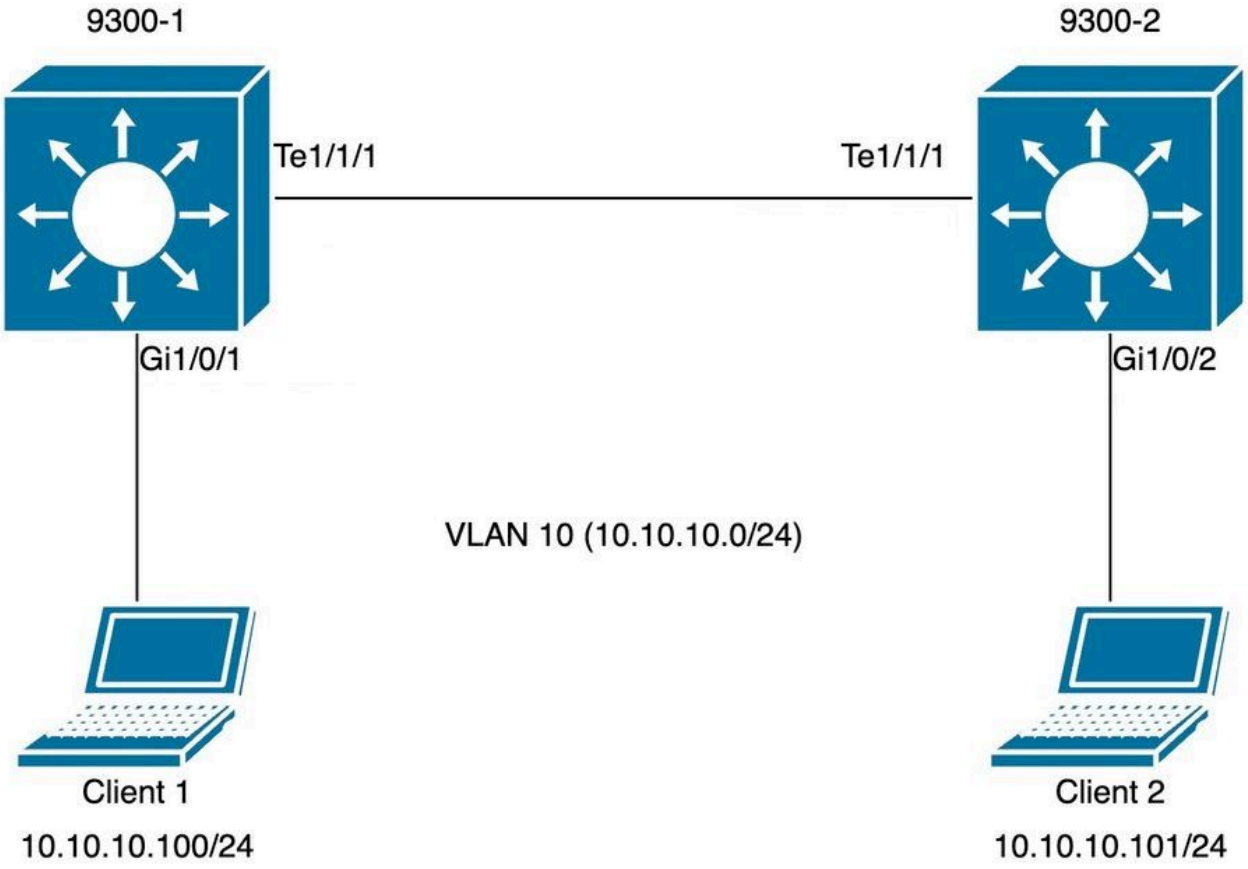
- SISF는 dhcp 스누핑과 같은 다른 기능을 활성화하여 활성화할 수 있습니다
- SISF의 기본 프로브 동작은 클라이언트 IP 주소 할당에 영향을 미칠 수 있습니다.
- SISF가 활성화되면 업링크 포트에서도 활성화되어 네트워크에 영향을 줄 수 있습니다.

문제 해결

토폴로지

토폴로지 다이어그램은 다음 SISF 시나리오에서 사용됩니다. 9300 스위치는 레이어 2만 해당하며 클라이언트 Vlan 10에 SVI가 구성되어 있지 않습니다.

참고: 이 실습에서는 SISF가 수동으로 활성화됩니다.



설정

기본 SISF 컨피그레이션은 액세스 포트를 향하는 9300 스위치 모두에서 설정되었지만, 예상되는 SISF 출력을 설명하기 위해 트렁크 포트에 사용자 지정 정책이 적용되었습니다.

스위치 9300-1:

```
<#root>

9300-1#

show running-config interface GigabitEthernet 1/0/1

Building configuration...

Current configuration : 111 bytes
!
interface GigabitEthernet1/0/1
 switchport access vlan 10
 switchport mode access

 device-tracking <-- enable default SISF policy

end
9300-1#

9300-1#

show running-config | section trunk-policy
```

device-tracking policy trunk-policy <-- custom policy

trusted-port   <-- custom policy parameters

device-role switch

<-- custom policy parameters

no protocol udp
9300-1#

9300-1#

show running-config interface tenGigabitEthernet 1/1/1

Building configuration...

Current configuration : 109 bytes
!
interface TenGigabitEthernet1/1/1
 switchport mode trunk

 device-tracking attach-policy trunk-policy <-- enable custom SISF policy

end

스위치 9300-2:

<#root>

9300-2#

show running-config interface GigabitEthernet 1/0/2

Building configuration...

Current configuration : 105 bytes
!
interface GigabitEthernet1/0/2
 switchport access vlan 10
 switchport mode access
 device-tracking

<-- enable default SISF policy

end

9300-2#

show running-config | section trunk-policy

```
device-tracking policy trunk-policy <-- custom policy


trusted-port                        <-- custom policy parameters


device-role switch


<-- custom policy parameters


no protocol udp

9300-2#

show running-config interface tenGigabitEthernet 1/1/1

Building configuration...

Current configuration : 109 bytes
!
interface TenGigabitEthernet1/1/1
 switchport mode trunk

 device-tracking attach-policy trunk-policy <-- custom policy applied to interface


end
```

확인

다음 명령을 사용하여 적용된 정책을 검증할 수 있습니다.

```
show device-tracking policy <policy name>
show device-tracking policies
show device-tracking database
```

스위치 9300-1:

<#root>

```
9300-1#

show device-tracking policy default

Device-tracking policy default configuration:
  security-level guard


device-role node  <--

  gleaning from Neighbor Discovery
```

```
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
Policy default is applied on the following targets:
```

Target

Type

Policy

Feature

Target range

Gi1/0/1

PORT

default

Device-tracking

vlan all

9300-1#

show device-tracking policy trunk-policy

```
Device-tracking policy trunk-policy configuration:
```

  trusted-port **<--**

  security-level guard

  device-role switch <--

```
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
Policy trunk-policy is applied on the following targets:
```

Target

Type

Policy

Feature

Target range

Te1/1/1

PORT

trunk-policy

Device-tracking

```
 vlan all
9300-1#

9300-1#
```

show device-tracking policies

```
Target               Type  Policy               Feature        Target range
Te1/1/1              PORT  trunk-policy         Device-tracking vlan all
Gi1/0/1              PORT  default              Device-tracking vlan all

9300-1#
```

show device-tracking database

```
Binding Table has 1 entries, 1 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 age    state     T
```

ARP 10.10.10.100   98a2.c07e.7902   Gi1/0/1   10   0005 8s   REACHABLE 3

```
9300-1#
```

스위치 9300-2:

<#root>

```
9300-2#
```

show device-tracking policy default

```
Device-tracking policy default configuration:
  security-level guard
```

** device-role node   <--**

```
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
Policy default is applied on the following targets:
```

Target

```
               Type
```

Policy

Feature

```
       Target range
Gi1/0/2
              PORT
default


Device-tracking
 vlan all
9300-2#
show device-tracking policy trunk-policy
Device-tracking policy trunk-policy configuration:
  trusted-port       <--
  security-level guard
  device-role switch <--
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
Policy trunk-policy is applied on the following targets:
Target
               Type
Policy


Feature
      Target range
Te1/1/1
              PORT
trunk-policy


Device-tracking
 vlan all
9300-2#

9300-2#
show device-tracking policies
Target               Type  Policy               Feature        Target range
Te1/1/1              PORT  trunk-policy         Device-tracking vlan all
Gi1/0/2              PORT  default              Device-tracking vlan all

9300-2#
show device-tracking database
```

```
Binding Table has 1 entries, 1 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 age    state     T

ARP 10.10.10.101                           98a2.c07e.9902     Gi1/0/2    10    0005  41s    REACHABLE 2


9300-2#
```

일반적인 시나리오

호스트 장치에 중복 IPv4 주소 오류가 있습니다.

문제

스위치가 보낸 "keepalive" 프로브는 L2 검사입니다. 스위치의 관점에서 볼 때 ARP에서 소스로 사용되는 IP 주소는 중요하지 않습니다. 이 기능은 IP 주소가 전혀 구성되지 않은 디바이스에서 사용할 수 있으므로 IP 소스 0.0.0.0은 관련이 없습니다. 호스트는 이 메시지를 받으면 다시 회신하고 수신 패킷에서 사용 가능한 유일한 IP 주소(자체 IP 주소)로 대상 IP 필드를 채웁니다. 이렇게 하면 응답하는 호스트에서 자체 IP 주소를 패킷의 소스와 대상 둘 다로 인식하기 때문에 잘못된 중복 IP 주소 알림이 발생할 수 있습니다.

keepalive 프로브에 자동 소스를 사용하도록 SISF 정책을 구성하는 것이 좋습니다.

참고: 자세한 내용은 중복 주소 문제에 대한 이 문서를 참조하십시오

기본 프로브

로컬 SVI가 없고 기본 프로브 설정이 없는 경우의 프로브 패킷입니다.

<#root>

```
Ethernet II,

Src: c0:64:e4:cc:66:02 (c0:64:e4:cc:66:02)

, Dst: Cisco_76:63:c6 (00:41:d2:76:63:c6)

<-- Probe source MAC is the BIA of physical interface connected to client

    Destination: Cisco_76:63:c6 (00:41:d2:76:63:c6)
        Address: Cisco_76:63:c6 (00:41:d2:76:63:c6)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)

    Source: c0:64:e4:cc:66:02 (c0:64:e4:cc:66:02)
```

```
        Address: c0:64:e4:cc:66:02 (c0:64:e4:cc:66:02)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)

    Type: ARP (0x0806)

    Padding: 000000000000000000000000000000000000
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: c0:64:e4:cc:66:02 (c0:64:e4:cc:66:02)

    Sender IP address: 0.0.0.0                                  <-- Sender IP is 0.0.0.0 (default)

    Target MAC address: Cisco_76:63:c6 (00:41:d2:76:63:c6)

    Target IP address: 10.10.10.101                             <-- Target IP is client IP
```

솔루션

프로브에 호스트 PC 이외의 주소를 사용하도록 프로브를 구성합니다. 이는 다음 방법으로 수행할 수 있습니다

"Keep-Alive" 프로브의 자동 소스

소스 IP로 0.0.0.0 사용을 줄이려면 "keep-alive" 프로브에 대한 자동 소스를 구성합니다.

```
device-tracking tracking auto-source fallback <IP> <MASK> [override]
```

auto-source 명령을 적용할 때의 논리는 다음과 같이 작동합니다.

<#root>

```
device-tracking tracking auto-source fallback 0.0.0.253 255.255.255.0 [override]

<-- Optional parameter
```

1. 소스가 있는 경우 VLAN SVI로 설정합니다.
2. 동일한 서브넷에 대한 IP 호스트 테이블에서 소스/MAC 쌍을 검색합니다. 프로브는 이미 데이터베이스에 있는 서브넷에 있는 다른 호스트의 IP + 스위치 물리적 인터페이스 MAC에서 제공된 것입니다.
3. 제공된 호스트 비트 및 마스크로 대상 IP에서 소스 IP를 계산합니다. 프로브는 클라이언트 IP를 듣고 마지막 비트가 구성된 서브넷에서 프로브를 생성하는 데 생성됩니다.

참고: 명령이 <override>와 함께 적용되면 항상 3단계로 이동합니다.

수정된 프로브

서브넷의 IP를 사용하도록 자동 소스 폴백 구성을 설정하면 프로브가 수정됩니다. 서브넷에 SVI와 다른 클라이언트가 없으므로 컨피그레이션에서 구성된 IP/마스크로 돌아갑니다.

<#root>

```
switch(config)#device-tracking tracking auto-source fallback 0.0.0.253 255.255.255.0 <-- it uses .253 fo
```

수정된 프로브 패킷입니다.

<#root>

```
Ethernet II, Src: c0:64:e4:cc:66:02 (c0:64:e4:cc:66:02), Dst: Cisco_76:63:c6 (00:41:d2:76:63:c6)

<-- Probe source MAC is the BIA of physical interface connected to client

    Destination: Cisco_76:63:c6 (00:41:d2:76:63:c6)

        Address: Cisco_76:63:c6 (00:41:d2:76:63:c6)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)

    Source: c0:64:e4:cc:66:02 (c0:64:e4:cc:66:02)

        Address: c0:64:e4:cc:66:02 (c0:64:e4:cc:66:02)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)

    Type: ARP (0x0806)

    Padding: 000000000000000000000000000000000000
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: c0:64:e4:cc:66:02 (c0:64:e4:cc:66:02)

    Sender IP address: 10.10.10.253                          <-- Note the new sender IP is now using t

    Target MAC address: Cisco_76:63:c6 (00:41:d2:76:63:c6)

    Target IP address: 10.10.10.101
```

프로브 동작에 대한 추가 세부 정보

명령을 사용합니다	작업	참고

	(디바이스 추적 ARP 프로브에 소스 IP 및 MAC 주소를 선택하려면)	
장치 추적 추적 자동 원본	• 소스가 있는 경우 VLAN SVI로 설정합니다. • 동일한 서브넷의 디바이스 추적 테이블에서 IP 및 MAC 바인딩을 찾습니다. • 0.0.0.0 사용	MAC 플래핑을 방지하려면 모든 트렁크 포트에서 디바이스 추적을 비활성화하는 것이 좋습니다.
장치 추적 추적 자동 원본 재정의	• 소스가 있는 경우 VLAN SVI로 설정 • 0.0.0.0 사용	SVI가 없는 경우에는 권장되지 않습니다.
디바이스 추적 자동 소스 폴백 <IP> <MASK>	• 소스가 있는 경우 VLAN SVI로 설정합니다. • 동일한 서브넷의 디바이스 추적 테이블에서 IP 및 MAC 바인딩을 찾습니다. • 제공된 호스트 비트 및 마스크를 사용하여 클라이언트 IP에서 소스 IP를 계산합니다. 소스 MAC는 클라이언트와 마주하는 switchport의 MAC 주소에서 가져옵니다.	MAC 플래핑을 방지하려면 모든 트렁크 포트에서 디바이스 추적을 비활성화하는 것이 좋습니다. 계산된 IPv4 주소는 어떤 클라이언트나 네트워크 장치에도 할당해서는 안 됩니다.
장치 추적 자동 소스 대체 <IP> <MASK> 재정의	• 소스가 있는 경우 VLAN SVI로 설정합니다. • 제공된 호스트 비트 및 마스크를 사용하여 클라이언트 IP에서 소스 IP를 계산합니다. 소스 MAC는 클라이언트와 마주하는 switchport의 MAC 주소에서 가져옵니다.	계산된 IPv4 주소는 어떤 클라이언트나 네트워크 장치에도 할당해서는 안 됩니다.

디바이스 추적 추적 자동 소스 폴백 <IP> <MASK> [override] 명령에 대한 설명:

호스트 ip에 따라 IPv4 주소를 예약해야 합니다.

```
<reserved IPv4 address> =  (<host-ip> & <MASK> ) | <IP>
```

참고: 부울 공식입니다.

예.

명령을 사용하는 경우:

```
device-tracking tracking auto-source fallback 0.0.0.1 255.255.255.0 override
```

호스트 IP = 10.152.140.25

IP = 0.0.0.1

마스크 = 24

부울 공식을 두 부분으로 나눕니다.

1. 10.152.140.25 및 255.255.255.0 작동:

```
10.152.140.25 = 00001010.10011000.10001100.00011001
                              AND
255.255.255.0 = 11111111.11111111.11111111.00000000
                            RESULT
10.152.140.0  = 00001010.10011000.10001100.00000000
```

2. 10.152.140.0 또는 0.0.0.1 작업:

```
10.152.140.0  = 00001010.10011000.10001100.00000000
                              OR
0.0.0.1       = 00000000.00000000.00000000.00000001
                            RESULT
10.152.140.1  = 00001010.10011000.10001100.00000001
```

예약된 IP = 10.152.140.1

예약된 IP = (10.152.140.25 및 255.255.255.0) | (0.0.0.1) = 10.152.140.1

참고: IP 소스로 사용되는 주소는 서브넷의 DHCP 바인딩에서 제외되어야 합니다.

중복 IPv6 주소 오류

문제

네트워크에서 IPv6가 활성화되고 VLAN에 SVI(Switched Virtual Interface)가 구성된 경우 IPv6 주소 중복 오류가 발생합니다.

일반 IPv6 DAD 패킷에서 IPv6 헤더의 Source Address 필드는 지정되지 않은 주소(0:0:0:0:0:0:0:0)로 설정됩니다. IPv4 사례와 유사합니다.

SISF 프로브에서 Source Address(소스 주소)를 선택하는 순서는 다음과 같습니다.

- 구성된 경우 SVI의 링크-로컬 주소
- 0:0:0:0:0:0:0:0 사용

솔루션

다음 명령을 SVI 컨피그레이션에 추가하는 것이 좋습니다. 이렇게 하면 SVI가 링크-로컬 주소를 자동으로 획득할 수 있습니다. 이 주소는 SISF 프로브의 소스 IP 주소로 사용되므로 중복 IP 주소 문제를 방지할 수 있습니다.

```
interface vlan <vlan>
 ipv6 enable
```

메모리 및 CPU 사용률 증가

문제

스위치에서 전송하는 "keepalive" 프로브는 프로그래밍으로 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.

참고: DHCP 스누핑과 같은 SISF 종속 기능은 SISF가 제대로 작동할 수 있게 하므로 이 문제가 발생할 수 있습니다.

솔루션

업링크(트렁크)에서 다른 스위치를 사랑하는 원격 호스트의 프로브 및 학습을 중지하도록 정책 구성(SISF는 로컬 호스트 테이블을 유지 관리하는 데만 필요)

```
<#root>

device-tracking policy DT_trunk_policy

 trusted-port
 device-role switch



interface <interface>
 device-tracking policy

DT_trunk_policy
```

디바이스 추적 도달 가능 시간이 너무 짧음

문제

IPDT에서 SISF 기반 디바이스 추적으로의 마이그레이션 문제로 인해 이전 릴리스에서 16.x 이상 릴리스로 마이그레이션할 때 기본이 아닌 연결 가능 시간이 도입되는 경우가 있습니다.

솔루션

다음을 구성하여 기본 연결 가능 시간으로 되돌리는 것이 좋습니다.

```
no device-tracking binding reachable-time <seconds>
```

Meraki 툴에 온보딩된 스위치(CPU 증가 및 포트 플러시)

문제

스위치가 Meraki Cloud Monitoring 툴에 온보딩되면 해당 툴은 맞춤형 디바이스 추적 정책을 푸시합니다.

```
device-tracking policy MERAKI_POLICY
 security-level glean
 no protocol udp
 tracking enable
```

이 정책은 구분이 없는 모든 인터페이스에 적용됩니다. 즉, 에지 포트와 다른 네트워크 디바이스(예: 스위치, 방화벽 라우터 등)와 마주하는 트렁크 포트를 구분하지 않습니다. 스위치는 MERAKI_POLICY가 구성된 트렁크 포트에 여러 SISF 항목을 생성할 수 있으므로 이러한 포트에 플러시가 발생하고 CPU 사용량이 증가합니다.

<#root>

```
switch#
show interfaces port-channel 5

Port-channel5 is up, line protocol is up (connected)
<omitted output>
  Input queue: 0/2000/0/
112327
 (size/max/drops/
flushes
); Total output drops: 0
<-- we have many flushes

<omitted output>

switch#
show process cpu sorted

CPU utilization for five seconds: 26%/2%; one minute: 22%; five minutes: 22%
PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
572     1508564      424873       3550 11.35%  8.73%  8.95%   0 SISF Main Thread
105      348502      284345       1225  2.39%  2.03%  2.09%   0 Crimson flush tr
```

솔루션

모든 비 에지 인터페이스에 다음 정책을 설정합니다.

```
configure terminal
device-tracking policy NOTRACK
 no protocol ndp
 no protocol dhcp6
 no protocol arp
 no protocol dhcp4
 no protocol udp
exit

interface <interface>
device-tracking policy NOTRACK
end
```

SISF 테이블에 없는 동일한 MAC의 IP 주소

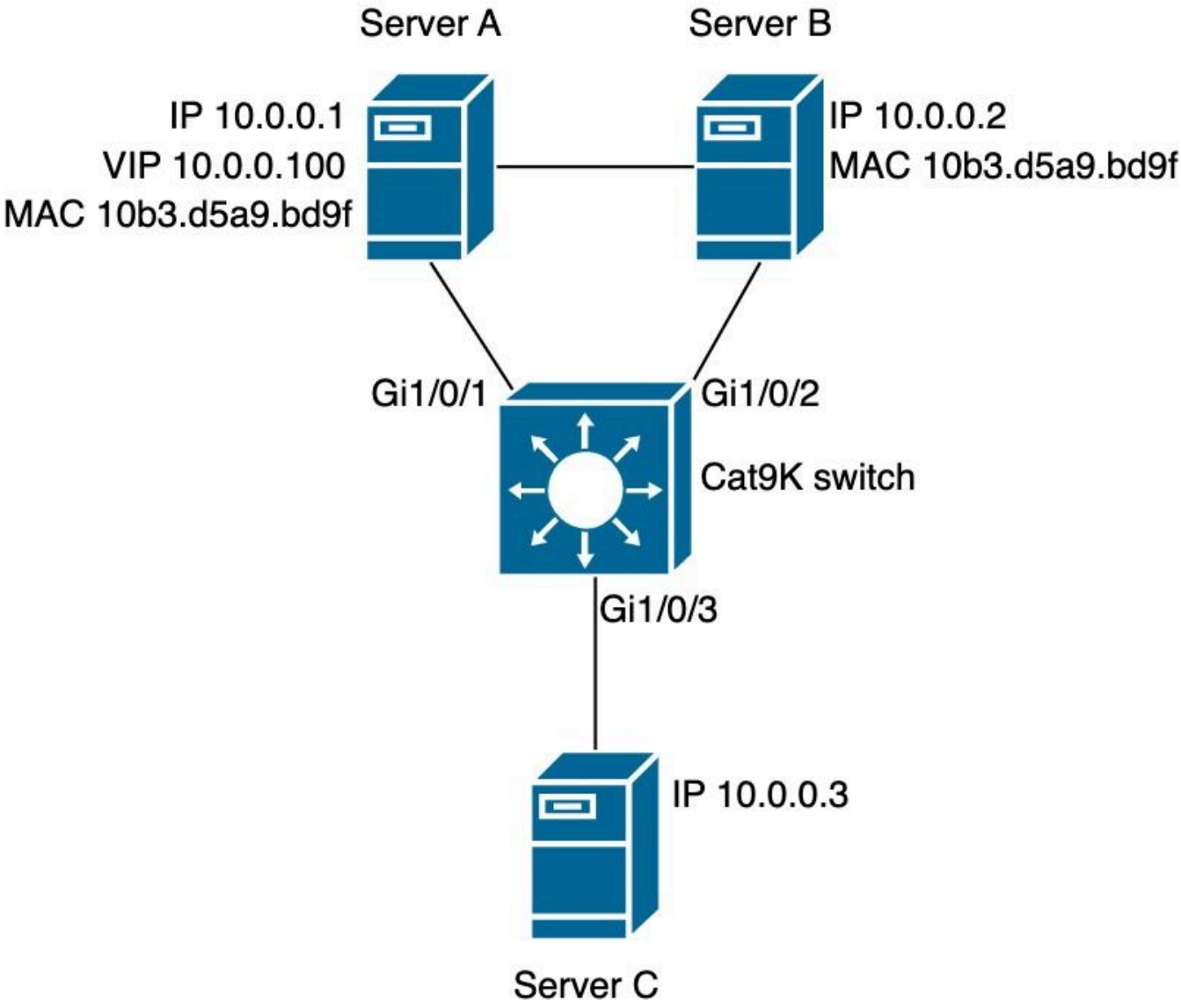
문제

이 시나리오는 HA(고가용성) 모드의 어플라이언스에서 일반적으로 IP 주소가 다르지만 동일한 MAC 주소를 공유합니다. 동일한 조건(둘 이상의 IP 주소에 대한 단일 MAC 주소)을 공유하는 VM 환경에서도 관찰됩니다. 이 조건은 보호 모드의 사용자 지정 SISF 정책이 있는 경우 SISF 테이블에 항목이 없는 모든 IP에 대한 네트워크 연결을 차단합니다.SISF 기능에 따라 MAC 주소당 하나의 IP만 학습됩니다.

 참고: 이 문제는 17.7.1 이후 릴리스에 있습니다.

예:

- MAC 주소가 10b3.d5a9.bd9f인 IP 10.0.0.1은 SISF 테이블에서 학습되며 네트워크 디바이스 10.0.0.3과 통신할 수 있습니다.
- 그러나 MAC 주소 10b3.d659.7858을 공유하는 두 번째 IP 10.0.0.2 및 가상 IP 10.0.0.100은 SISF 테이블에 프로그래밍되지 않으며 네트워크와의 통신이 허용되지 않습니다.



SISF 정책

<#root>

```
switch#

show run | sec IPDT_POLICY

device-tracking policy IPDT_POLICY
 no protocol udp
 tracking enable

switch#

show device-tracking policy IPDT_POLICY

Device-tracking policy IPDT_POLICY configuration:

  security-level guard <-- default mode

  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
```

```
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  tracking enable
Policy IPDT_POLICY is applied on the following targets:
Target               Type  Policy               Feature        Target range

Gi1/0/1              PORT  IPDT_POLICY          Device-tracking vlan all
Gi1/0/2              PORT  IPDT_POLICY          Device-tracking vlan all
```

SISF 데이터베이스

<#root>

```
switch#

show device-tracking database


Binding Table has 2 entries, 2 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 10.0.0.3                               10b3.d659.7858         Gi1/0/3    10         0005       90s
ARP 10.0.0.1                               10b3.d5a9.bd9f         Gi1/0/1    10         0005       84s
```

연결성 테스트 서버 A

<#root>

```
ServerA#

ping 10.0.0.3 source 10.0.0.1


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.3, timeout is 2 seconds:
Packet sent with a source address of 10.0.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ServerA#

ping 10.0.0.3 source 10.0.0.100 <-- entry for 10.0.0.100 is not on SISF table


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.3, timeout is 2 seconds:
Packet sent with a source address of 10.0.0.100
.....
```

연결 가능성 테스트 서버 B.

<#root>

ServerB#

ping 10.0.0.3 <-- entry for 10.0.0.2 is not on SISF table

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

스위치의 삭제를 확인하는 중입니다.

<#root>

switch(config)#

device-tracking logging

로그

<#root>

switch#

show logging

<omitted output>
%SISF-4-PAK_DROP: Message dropped

IP=10.0.0.100 VLAN=10 MAC=10b3.d5a9.bd9f

I/F=Gi1/0/1

P=ARP Reason=Packet accepted but not forwarded
%SISF-4-PAK_DROP: Message dropped

IP=10.0.0.100 VLAN=10 MAC=10b3.d5a9.bd9f

I/F=Gi1/0/1

P=ARP Reason=Packet accepted but not forwarded
%SISF-4-PAK_DROP: Message dropped

IP=10.0.0.100 VLAN=10 MAC=10b3.d5a9.bd9f

I/F=Gi1/0/1

 P=ARP Reason=Packet accepted but not forwarded
%SISF-4-PAK_DROP: Message dropped

IP=10.0.0.100 VLAN=10 MAC=10b3.d5a9.bd9f

I/F=Gi1/0/1

 P=ARP Reason=Packet accepted but not forwarded
%SISF-4-PAK_DROP: Message dropped

IP=10.0.0.100 VLAN=10 MAC=10b3.d5a9.bd9f

I/F=Gi1/0/1

 P=ARP Reason=Packet accepted but not forwarded
<omitted output>
%SISF-4-PAK_DROP: Message dropped

IP=10.0.0.2 VLAN=10 MAC=10b3.d5a9.bd9f

I/F=Gi1/0/2

 P=ARP Reason=Packet accepted but not forwarded
%SISF-4-MAC_THEFT:

 MAC Theft IP=10.0.0.2 VLAN=10 MAC=10b3.d5a9.bd9f IF=Gi1/0/1 New I/F=Gi1/0/2

%SISF-4-PAK_DROP: Message dropped

IP=10.0.0.2 VLAN=10 MAC=10b3.d5a9.bd9f

I/F=Gi1/0/2

 P=ARP Reason=Packet accepted but not forwarded
%SISF-4-MAC_THEFT:

MAC Theft IP=10.0.0.2 VLAN=10 MAC=10b3.d5a9.bd9f IF=Gi1/0/1 New I/F=Gi1/0/2

%SISF-4-PAK_DROP: Message dropped

IP=10.0.0.2 VLAN=10 MAC=10b3.d5a9.bd9f

I/F=Gi1/0/2

 P=ARP Reason=Packet accepted but not forwarded
%SISF-4-MAC_THEFT:

MAC Theft IP=10.0.0.2 VLAN=10 MAC=10b3.d5a9.bd9f IF=Gi1/0/1 New I/F=Gi1/0/2

%SISF-4-PAK_DROP: Message dropped

IP=10.0.0.2 VLAN=10 MAC=10b3.d5a9.bd9f

```
I/F=Gi1/0/2

 P=ARP Reason=Packet accepted but not forwarded
%SISF-4-MAC_THEFT:

MAC Theft IP=10.0.0.2 VLAN=10 MAC=10b3.d5a9.bd9f IF=Gi1/0/1 New I/F=Gi1/0/2


%SISF-4-PAK_DROP: Message dropped

IP=10.0.0.2 VLAN=10 MAC=10b3.d5a9.bd9f


I/F=Gi1/0/2

 P=ARP Reason=Packet accepted but not forwarded
%SISF-4-MAC_THEFT:

MAC Theft IP=10.0.0.2 VLAN=10 MAC=10b3.d5a9.bd9f IF=Gi1/0/1 New I/F=Gi1/0/2
```

솔루션

옵션 1: 포트에서 IPDT 정책을 제거하면 ARP 패킷 및 영향을 받는 디바이스에 연결할 수 있습니다

```
<#root>

switch(config)#interface gigabitEthernet 1/0/1
switch(config-if)#

no device-tracking attach-policy IPDT_POLICY


switch(config-if)#interface gigabitEthernet 1/0/2
switch(config-if)#

no device-tracking attach-policy IPDT_POLICY
```

옵션 2: 디바이스 추적 정책에서 프로토콜 arp 경사를 제거합니다.

```
<#root>

switch(config)#device-tracking policy IPDT_POLICY
switch(config-device-tracking)#

no protocol arp
```

옵션 3: IPDT_POLICY의 보안 수준을 glean으로 변경합니다.

```
<#root>

switch(config)#device-tracking policy IPDT_POLICY
```

```
switch(config-device-tracking)#
security-level glean
```

관련 정보

- Cisco IOS XE Bengaluru 17.6.x(Catalyst 9300 스위치) 보안 구성 설명서: 스위치 통합 보안 기능 구성
- 보안 구성 설명서, Cisco IOS XE Cupertino 17.9.x(Catalyst 9300 스위치): 스위치 통합 보안 기능 구성
- Cisco Catalyst 9000 Family Switch SISF(Integrated Security Features) 백서
- Cisco 버그 ID CSCvx75602 - AR 릴레이 및 ND 억제의 SISF 메모리 누수
- Cisco 버그 ID CSCwf33293 - [EVPN SISF] EVPN + DHCP를 사용하여 IPv4/V6에 대한 제한 주소 값을 수정하는 데 필요한 사용자 지정 방법입니다
- Cisco 버그 ID CSCvq22011 - IOS-XE는 IPDT가 ARP에서 기울면 ARP 응답을 삭제합니다.
- Cisco 버그 ID CSCwc20488 - vlan/evi당 255개의 의사 포트 제한
- Cisco 버그 ID CSCwh52315 - 9300 스위치는 포트에 IPDT 정책이 있을 때 ARP 응답을 삭제합니다
- Cisco 버그 ID CSCvd51480 - IP dhcp 스누핑 및 디바이스 추적 바인딩 해제

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.