Probleemoplossing SISF op Catalyst 9000 Series Switches

Inhoud

Inleiding

Dit document beschrijft de Switch Integrated Security Properties (SISF) die wordt gebruikt in Catalyst 9000 Series Switches. Het legt ook uit hoe SISF kan worden gebruikt en hoe er interactie is met andere functies.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Catalyst 9300-48P waarop Cisco IOS® XE 17.3.x wordt uitgevoerd

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

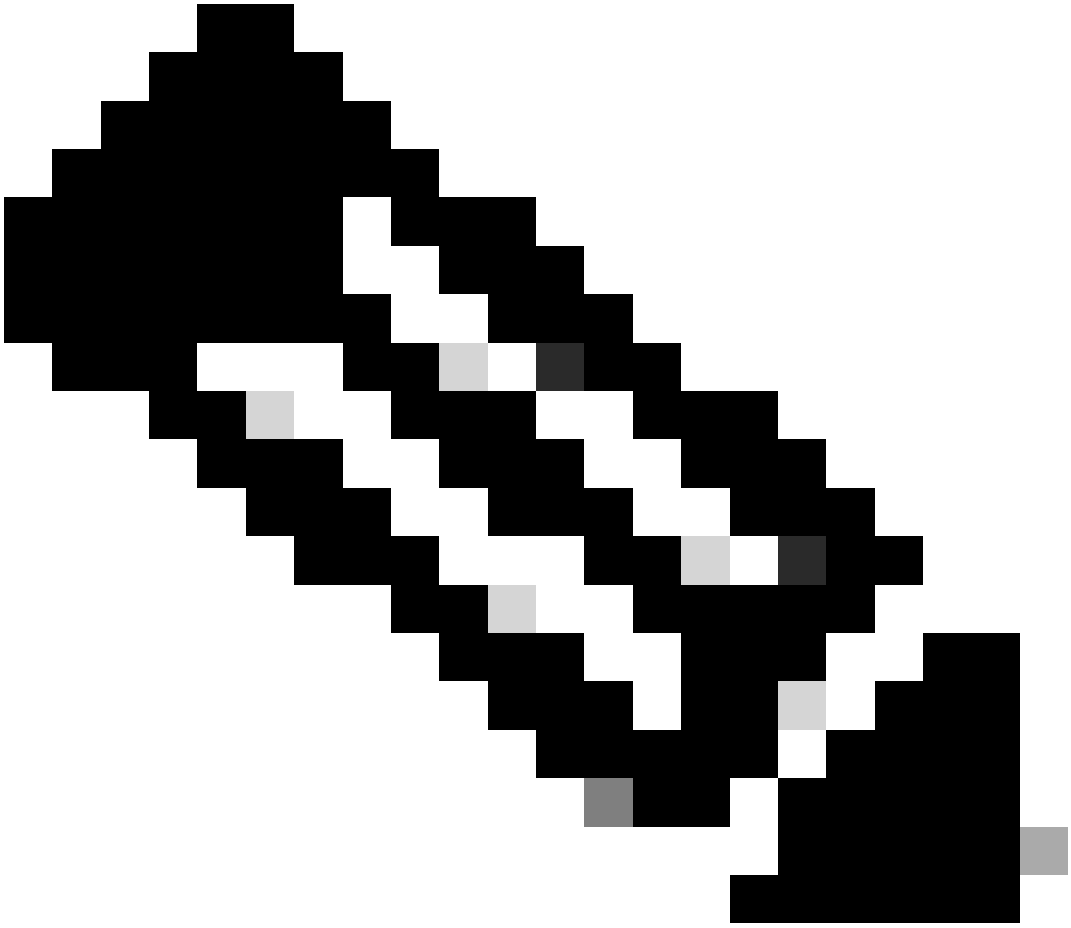
 Opmerking: raadpleeg de juiste configuratiehandleiding voor de opdrachten die worden gebruikt om deze functies op andere Cisco-platforms in te schakelen.

Verwante producten

Dit document kan ook worden gebruikt voor de volgende hardware- en softwareversies:

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

Met 17.3.4 en hoger Cisco IOS XE-softwareversies



Opmerking: dit document is ook van toepassing op de meeste Cisco IOS XE-versies die SISF tegen Apparaattracering gebruiken.

Achtergrondinformatie

Overzicht

SISF biedt een host bindende tabel, en er zijn functieclients die de informatie van het gebruiken. De ingangen worden bevolkt in de lijst door pakketten zoals DHCP, ARP, ND, RA te overzien die de gastheeractiviteit volgen en helpen om de lijst dynamisch te bevolken. Als er stille hosts zijn in het L2-domein, kunnen statische items worden gebruikt om items toe te voegen aan de SISF-tabel.

SISF gebruikt een beleidsmodel om apparaatrollen en extra instellingen op de switch te configureren. Eén enkel beleid kan worden toegepast op interface- of VLAN-niveau. Als een beleid op VLAN wordt toegepast en een ander beleid op interface wordt toegepast, krijgt het

interfacebeleid voorrang.

SISF kan ook worden gebruikt om het aantal hosts in de tabel te beperken, maar er zijn verschillen tussen IPv4- en IPv6-gedrag. Als SISF-limiet is ingesteld en deze wordt bereikt:

- IPv4-hosts blijven actief maar er worden geen vermeldingen over de limiet aan de SISF-tabel toegevoegd
- IPv6-hosts die niet in de SISF-tabel worden opgenomen, mogen niet in het netwerk worden ingevoerd en er moeten geen nieuwe vermeldingen worden toegevoegd aan de SISF-tabel.

Vanaf 16.9.x en de nieuwere release wordt een SISF-clientfunctieprioriteit geïntroduceerd. Het voegt opties toe om de updates in SISF te controleren en als twee of meer cliënten de bindende lijst gebruiken, worden de updates van hogere prioritaire eigenschap toegepast. De uitzonderingen zijn hier de "limietadrestelling voor IPv4/IPv6 per mac" instellingen, de instellingen van het beleid met de laagste prioriteit zijn effectief.

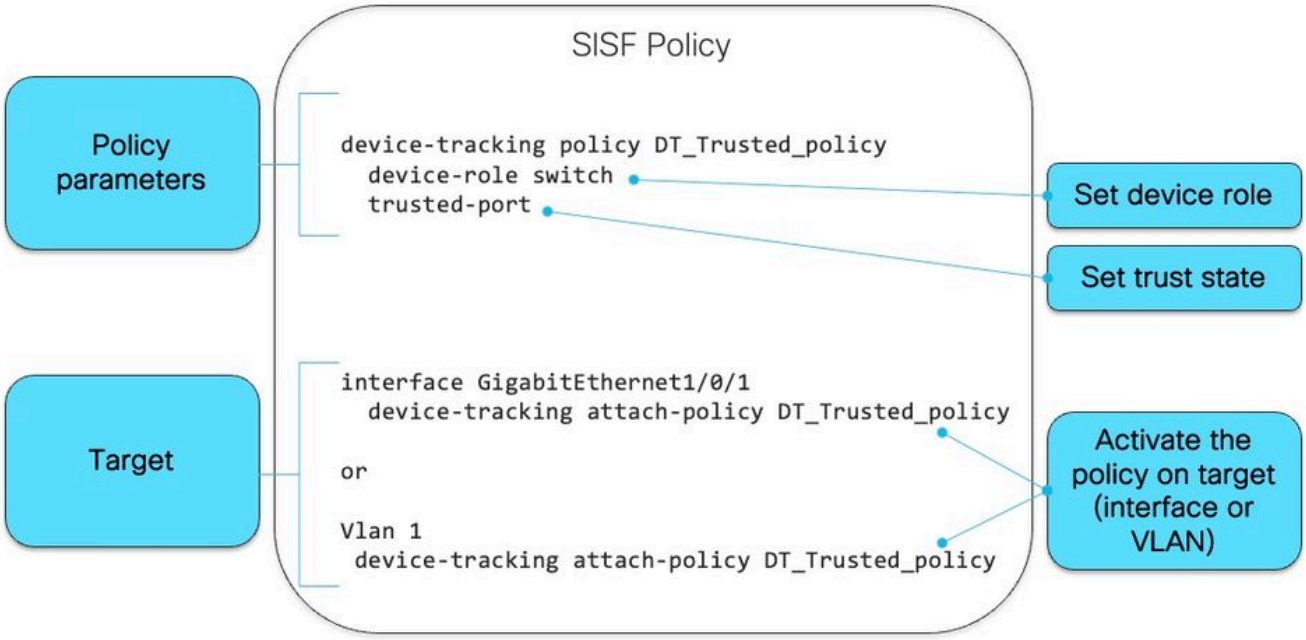
Enkele voorbeeldfuncties waarvoor apparaattracering is ingeschakeld, zijn:

- LISP/EVPN
- Dot1x
- Webautorisatie
- CTS
- DHCP-controle

Opmerking: prioritair wordt gebruikt om beleidsinstellingen te selecteren.

Beleid dat op basis van CLI is gemaakt, heeft de hoogste prioriteit (128) en stelt gebruikers daarom in staat om een andere beleidsbepaling toe te passen dan die in het programmatische beleid. Alle configureerbare instellingen onder het aangepaste beleid kunnen handmatig worden gewijzigd.

Volgende afbeelding is een voorbeeld van een SISF-beleid en hoe u het kunt lezen:



Binnen het beleid, onder protocol sleutelwoord, hebt u de optie om te zien welk type van pakketten worden gebruikt om het SISF- gegevensbestand te bevolken:

<#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-functies voor programmatie en client

De functies in de volgende tabel maken SISF programmeerbaar mogelijk als ze zijn ingeschakeld of fungeren als clients voor SISF:

SISF-programmatische functie	SISF-clientfuncties
LISP op VLAN	Dot1x
EVPN op VLAN	Webautorisatie
DHCP-controle	CTS

Als een SISF-clientfunctie is ingeschakeld op een apparaat dat is geconfigureerd zonder een functie die SISF inschakelt, moet een aangepast beleid worden geconfigureerd op interfaces die verbinding maken met hosts.

IPv4-functies die SISF-informatie gebruiken

- CTS
- IEEE 802.1x.
- LISP
- EVPN
- DHCP-controle (activeert alleen SISF, maar gebruikt deze niet)
- IP-bronbewaker

IPv6-functies die SISF-informatie gebruiken

- IPv6-routerbewaking (RA)
- IPv6 DHCP-bewaking, Layer 2 DHCP-relay
- IPv6-proxy (Duplicate Address Detection)
- Onderdrukking van overstromingen
- IPv6-bronbeveiliging
- IPv6-doelbewaker
- RA Throttler
- IPv6-prefixbeveiliging

Apparaattracering

De belangrijkste rol van apparaat het volgen is de aanwezigheid, de plaats, en de beweging van eindknooppunten in het netwerk te volgen. SISF snoops-verkeer dat door de switch is ontvangen, extraheert apparaatidentiteit (MAC- en IP-adres) en slaat deze op in een bindende tabel. Veel functies, zoals IEEE 802.1X, webverificatie, Cisco TrustSec en LISP enzovoort, zijn afhankelijk van de nauwkeurigheid van deze informatie om goed te werken. Op SISF gebaseerde apparaattracering ondersteunt zowel IPv4 als IPv6. Er zijn vijf ondersteunde methoden waarmee client IP kan leren:

- DHCPv4
- DHCPv6-software
- ARP
- NDP
- Gegevensverzameling

SISF op een poortkanaal

Apparaattracering op poortkanaal (of etherkanaal) wordt ondersteund. Maar de configuratie moet worden toegepast op de kanaalgroep, niet op de individuele poortkanaalleden. De enige interface die verschijnt (en bekend is) vanuit het bindende standpunt is het poortkanaal.

Sonde- en databasetuning

Sonde:

- In IPDT was er een opdracht om te helpen met dubbele adresproblemen door de eerste sonde 10 seconden te vertragen: "ip device tracking sonde vertraging" bij link up.
- In SISF is al een wachttijdtimer ingebouwd die wacht voordat de eerste sonde wordt verzonden. Het is niet configureerbaar, en lost hetzelfde probleem op. Aangezien dit in de SISF-code staat, is deze opdracht niet meer nodig.

Databank:

In SISF kunt u een paar opties configureren om te bepalen hoe lang een vermelding in de database wordt bewaard:

<#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-apparaattracering

Levenscyclus van een inzending waar de gastheer wordt ondervraagd:

- SISF handhaaft IPv4/IPv6-binding per computer, zodra IP leert succesvol is, bindt overgangen naar BEREIKBARE status
- SISF houdt client voor bewegende beelden bij door controlepakket te bewaken
- Als er 5 minuten lang geen besturingspakket van de client is, worden de overgangen bij het binden om de status te VERIFIËREN en wordt de sonde naar de client verzonden
- Als de cliënten niet aan sonde reageren, Bindende overgangen aan STABIELE staat anders BEREIKBARE staat
- Standaard timeout voor STALE entry is 24 uur en configureerbaar
- STALE-items worden na 24 uur verwijderd (of geconfigureerde tijdelijke waarde)

Diefstaldetectie

Soorten knoopdiefstallen:

- IP-diefstal (dezelfde ip, andere Mac, andere/dezelfde poort)
- MAC THEFT (zelfde MAC, verschillende IP, verschillende poort)
- MAC IP THEFT (dezelfde computer, dezelfde ip, andere poort)

IP-beveiligingsfuncties

Dit zijn enkele van de SISF-afhankelijke functies:

- NDP-inspectie: IPv6-NDP-berichten inspecteren
- NDP-adresomzetting:de bindende tabel met informatie vullen door NDP-verkeer te snuffelen
- Apparaattracering: monitoren van de activiteit van het eindapparaat, inclusief via een of ander hefboommechanisme
- Snooping: Glean adressen in NDP, ARP en DHCP berichten. Onbevoegde berichten blokkeren
- DHCPv4 Relay: Relay DHCP zond pakket uit naar geconfigureerd helperadres.
- NDP & ARP multicast onderdrukken: onderdruk multicast NDP-berichten door te converteren naar unicast, om te reageren in naam van doelen.
- DAD proxy:Dubbele adresdetectie en verzenden van NAC namens doelclient
- DHCPv4 Vereist: het dwingt de client om IP alleen door DHCP te krijgen

SISF-voorbehouden

Enkele van de meest geobserveerde gedragingen in verband met SISF zijn:

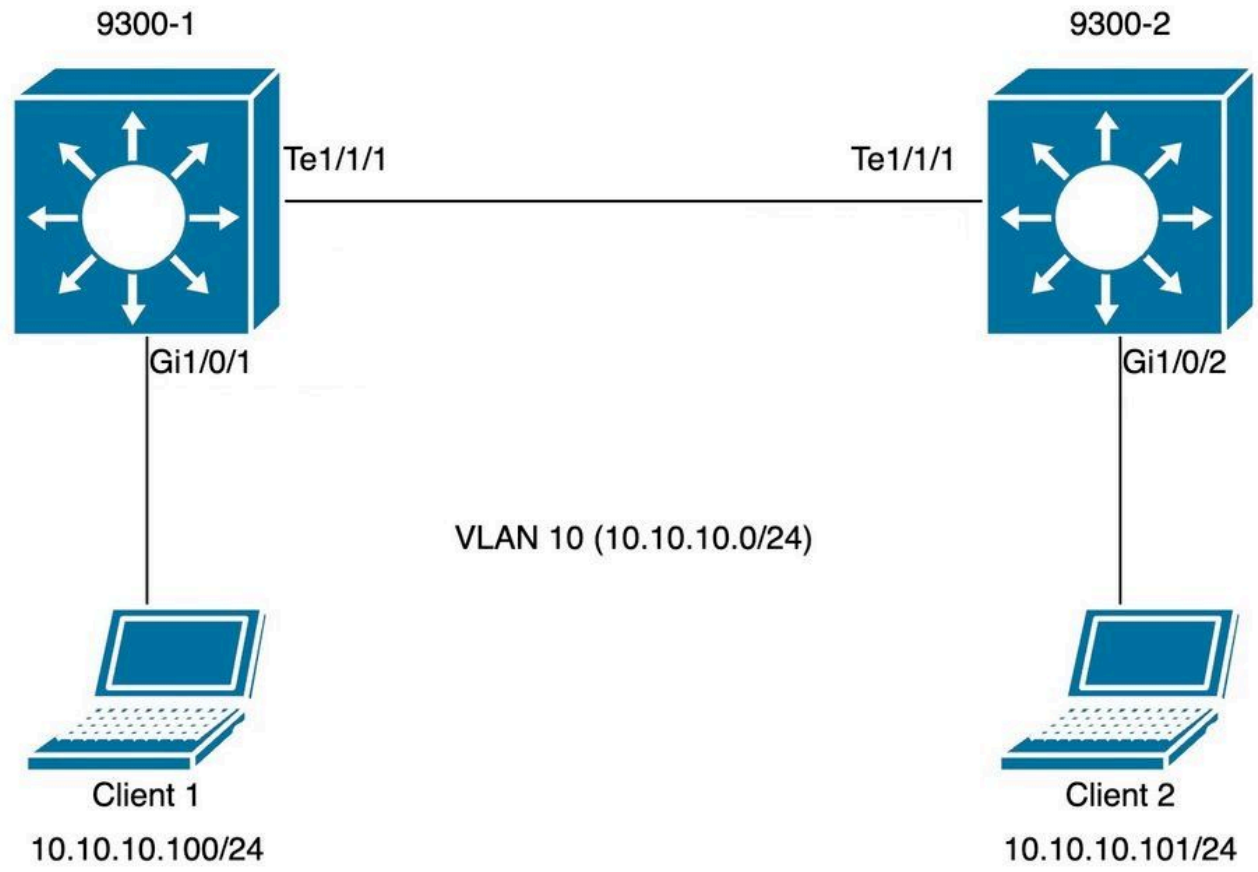
- SISF kan worden ingeschakeld door andere functies in te schakelen, zoals dhcp-snooping
- Het gedrag van de standaardsonde van SISF kan de toewijzing van het cliëntIP adres beïnvloeden.
- Wanneer SISF is ingeschakeld, is dit ook mogelijk op uplinkpoorten die een impact op het netwerk kunnen hebben.

Problemen oplossen

Topologie

Het topologiediagram wordt gebruikt op het volgende SISF-scenario. 9300 switches zijn alleen Layer 2 en hebben GEEN SVI geconfigureerd in client-VLAN 10.

Opmerking: SISF is in dit lab handmatig ingeschakeld.



Configuratie

De standaard SISF-configuratie is ingesteld op zowel 9300 switches met uitzicht op toegangspoorten, terwijl op trunkpoorten douanebeleid is toegepast om de verwachte SISF-uitgangen te illustreren.

Switch 930-1:

<#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
```

Switch 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
```

Verificatie

U kunt deze opdrachten gebruiken om het toegepaste beleid te valideren:

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

Switch 930-1:

<#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#

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


9300-2#
```

Gemeenschappelijke scenario's

Dubbele IPv4-adresfout op hostapparaat

Probleem

De "keepalive"-sonde die door de switch wordt verzonden is een L2-controle. Vanuit het oogpunt van de switch zijn de IP-adressen die als bron in de ARP's worden gebruikt, niet van belang: deze functie kan worden gebruikt op apparaten zonder IP-adres dat helemaal is ingesteld, zodat de IP-bron van 0.0.0.0 niet van belang is. Wanneer de host deze berichten ontvangt, antwoordt hij terug en vult het IP-doelveld met het enige IP-adres dat beschikbaar is in het ontvangen pakket, dat zijn eigen IP-adres is. Dit kan valse dubbele IP adreswaarschuwingen veroorzaken, omdat de gastheer die antwoordt zijn eigen IP adres als zowel bron als bestemming van het pakket ziet.

Aanbevolen wordt om het SISF-beleid te configureren voor het gebruik van een automatische bron voor de keepalive-sondes.

Opmerking: Zie dit artikel over dubbele adreskwesties voor meer informatie

---

Standaard sonde

Dit is het sondepakket wanneer er geen lokale SVI aanwezig is en standaardinstellingen heeft:

<#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
```

Oplossing

Configureer de sonde om een ander adres te gebruiken dan de host-pc voor de sonde. Dit kan met deze methoden worden bereikt

Auto-bron voor "Keep-Alive"-sonde

Configureer een autobron voor de "keep-alive"-sondes om het gebruik van 0.0.0.0 als bron-IP te beperken:

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

De logica als het toepassen van het autobronbevel werkt als volgt:

<#root>

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

1. Stel de bron in op VLAN SVI indien aanwezig.
2. Zoek naar een bron/MAC-paar in de IP-hosttabel voor dezelfde subnetverbinding. De sonde is afkomstig van de switch fysieke interface MAC + IP van een andere host in het subnetnet al in de database.
3. Bereken de bron-IP vanaf de bestemming-IP met het geleverde hostbit en -masker. Sonde wordt gegenereerd van gehoor client IP en het maken van een sonde in het subnetnet met de laatste bits geconfigureerd.

Opmerking: als commando wordt toegepast met <override> springen we altijd naar stap 3.

Aangepaste sonde

Door de automatische bronfallback-configuratie in te stellen op het gebruik van een IP in het netwerk, wordt de sonde aangepast. Aangezien er geen SVI en geen andere client op het subnetnetwerk is, vallen we terug naar het geconfigureerde IP/Mask in de configuratie.

<#root>

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

Dit is het aangepaste sonde-pakket:

<#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
```

Nadere gegevens over het gedrag van de sonde

Opdracht	Actie (Om bron IP en MAC adres voor apparaat het volgen ARP sonde te selecteren)	Opmerkingen
automatische bron voor het traceren van apparaten	• Stel de bron in op VLAN SVI indien aanwezig. • Zoek naar IP en MAC-binding in een apparaat-tracking tabel van dezelfde subnetverbinding. • Gebruik 0.0.0.0	Wij adviseren dat u apparaat-volgen op alle trunkpoorten uitschakelt om te voorkomen dat MAC flapping.
automatische bronoverschrijding bij het bijhouden van apparaten	• Bron instellen op VLAN SVI indien aanwezig • Gebruik 0.0.0.0	Niet aanbevolen bij afwezigheid van SVI.
automatische terugvalfunctie voor apparaattracering <IP> <MASK>	• Stel de bron in op VLAN SVI indien aanwezig. • Zoek naar IP en MAC-binding in een apparaat-tracking tabel van dezelfde subnetverbinding. • Bereken bron-IP vanaf client-IP met behulp van meegeleverd hostbit en -	Wij adviseren dat u apparaat-volgen op alle trunkpoorten uitschakelt om te voorkomen dat MAC flapping. Het berekende IPv4-adres mag niet aan een client of netwerkapparaat worden toegewezen.

	masker. Source MAC wordt genomen van het adres van MAC van de switchport die de cliënt onder ogen ziet.	
automatische terugvalfunctie voor apparaattracering <IP> <MASK> negeren	• Stel de bron in op VLAN SVI indien aanwezig. • Bereken bron-IP vanaf client-IP met behulp van meegeleverd hostbit en -masker. Source MAC wordt genomen van het adres van MAC van de switchport die de cliënt onder ogen ziet.	Het berekende IPv4-adres mag niet aan een client of netwerkapparaat worden toegewezen.

Uitleg over de automatische terugvalfunctie voor apparaattracering <IP> <MASK> [override]opdracht:

Afhankelijk van de host-ip moet er een IPv4-adres worden gereserveerd.

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

Opmerking: dit is een booleaanse formule

Voorbeeld.

Als we de opdracht gebruiken:

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

host IP = 10.152.140.25

IP = 0,0,0,1

masker = 24

Laat de Booleaanse formule in twee delen breken.

1. 10.152.140.25 EN 255.255.255.0. bedrijf:

```
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 OF 0.0.0.1. bedrijf:

```
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
```

Gereserveerd IP = 10.152.140.1

Gereserveerd IP = (10.152.140.25 en 255.255.255.0) | (0,0,0,1) = 10 152 140,1

Opmerking: het adres dat als IP-bron wordt gebruikt, moet uit de DHCP-bindingen voor het internet worden bestscand.

Dubbele IPv6-adresfout

Probleem

Dubbele IPv6-adresfout wanneer IPv6 in het netwerk is ingeschakeld en een switched Virtual Interface (SVI) op een VLAN is geconfigureerd.

In een normaal IPv6 DAD-pakket wordt het veld Bronadres in de IPv6-header ingesteld op het niet-opgegeven adres (0:0:0:0:0:0:0:0). Gelijkaardig aan IPv4 geval.

De volgorde voor het kiezen van bronadres in SISF-sonde is:

- Link-lokaal adres van SVI, indien geconfigureerd
- Gebruik 0:0:0:0:0:0:0:0

Oplossing

We raden u aan de volgende opdrachten aan de SVI-configuratie toe te voegen. Hierdoor kan de SVI automatisch een link-lokaal adres verkrijgen; dit adres wordt gebruikt als het IP-bronadres van de SISF-sonde, waardoor de dubbele IP-adreskwestie wordt voorkomen.

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

Verbeterd geheugen en CPU-gebruik

Probleem

De "keepalive"sonde die door de switch wordt verzonden wordt uitgezonden uit alle havens wanneer het programmatisch wordt toegelaten. Bijgevoegde switches in hetzelfde L2-domein sturen deze uitzendingen naar hun hosts wat resulteert in de switch van herkomst die externe hosts toevoegt aan de database voor apparaattracering. De extra hostvermeldingen verhogen het geheugengebruik op het apparaat en het proces van het toevoegen van de externe hosts verhoogt het CPU-gebruik van het apparaat.

Aanbevolen wordt om het programmatische beleid te bepalen door een beleid voor uplink naar aangesloten switches te configureren om de poort als vertrouwd en gekoppeld aan een switch te definiëren.

Opmerking: houd er rekening mee dat SISF-afhankelijke functies zoals DHCP-snuffelen SISF in staat stellen om goed te werken, wat dit probleem kan veroorzaken.

Oplossing

Configureer een beleid op de uplink (trunk) om sondes en het leren van externe hosts die houden van andere switches te stoppen (SISF is alleen nodig om lokale hosttabel te onderhouden)

<#root>

```
device-tracking policy DT_trunk_policy
```

```
 trusted-port
 device-role switch
```

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

```
DT_trunk_policy
```

Te korte tijd voor apparaattracering

Probleem

Vanwege een migratiekwestie van IPDT naar op SISF gebaseerde apparaattracering wordt er soms een niet-standaard bereikbare tijd geïntroduceerd bij het migreren van oudere release naar 16.x en nieuwere releases.

Oplossing

Het wordt aanbevolen om terug te keren naar de standaard bereikbare tijd door te configureren:

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

Switches aan boord van Meraki Tool (CPU uitbreiding en poortflushes)

Probleem

Wanneer switches worden ingesloten in de Meraki Cloud Monitoring tool, wordt er een aangepast beleid voor apparaattracering ontwikkeld.

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

Het beleid wordt toegepast op alle interfaces zonder onderscheid, dat betekent, het maakt geen onderscheid tussen randpoorten en trunkpoorten die naar andere netwerkapparaten kijken (bijvoorbeeld switches, firewalls routers enzovoort). Switch kan verschillende SISF-vermeldingen maken op trunkpoorten waar MERAKI_POLICY is geconfigureerd, waardoor flushes op deze poorten en toename van CPU-gebruik ontstaan.

<#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
```

Oplossing

Stel het volgende beleid in voor alle niet-edge interfaces:

```
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
```

IP-adressen met dezelfde MAC niet in SISF-tabel

Probleem

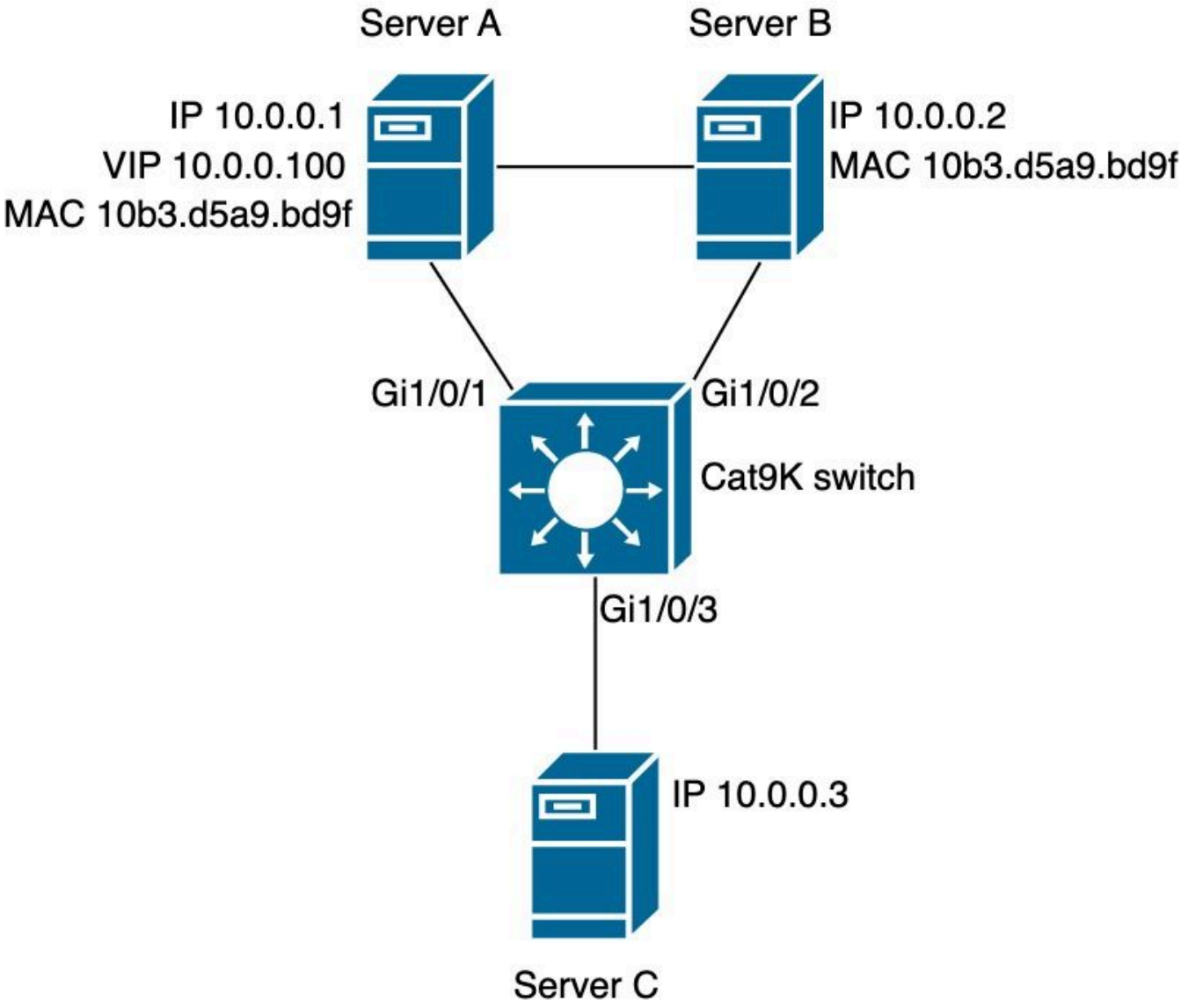
Dit scenario is gebruikelijk op apparaten in HA (hoge beschikbaarheid) modus die verschillende IP-adressen hebben, maar hetzelfde MAC-adres. Het wordt ook waargenomen op VM-omgevingen die dezelfde voorwaarde delen (één MAC-adres voor twee of meer IP-adressen). Deze voorwaarde verhindert netwerkconnectiviteit aan al die IPs die geen ingang in de SISF- lijst hebben wanneer het douanebeleid SISF in wachtwijze is op zijn plaats.Zoals per SISF eigenschap, wordt slechts één IP geleerd per adres van MAC.

Opmerking: dit probleem is aanwezig bij 17.7.1 en volgende releases

---

Voorbeeld:

- IP 10.0.0.1 met MAC-adres 10b3.d5a9.bd9f wordt geleerd op SISF-tabel en kan communiceren met het netwerkapparaat 10.0.0.3.
- Tweede IP 10.0.0.2 en Virtual IP 10.0.0.100 die een MAC-adres van 10b3.d659.7858 delen, is echter niet geprogrammeerd in SISF-tabel en communicatie met het netwerk is niet toegestaan.



SISF-beleid

<#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-database

<#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
```

Bereikbaarheidstest server 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
.....
```

Bereikbaarheidstest server 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)
```

Droppen op de switch valideren.

<#root>

```
switch(config)#

device-tracking logging
```

Logboeken

<#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
```

Oplossing

Optie 1: Verwijder het IPDT-beleid uit de poort waardoor ARP-pakketten en getroffen apparaten bereikbaar worden

<#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
```

Optie 2: Verwijder de protocolarp glealing uit het beleid voor het bijhouden van apparaten.

<#root>

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

no protocol arp
```

Optie 3: Verander het security-level van IPDT_POLICY naar glean.

<#root>

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

security-level glean

Gerelateerde informatie

- Security Configuration Guide, Cisco IOS XE Bengaluru 17.6.x (Catalyst 9300 Switches): Switch geïntegreerde security functies configureren
- Security Configuration Guide, Cisco IOS XE koppeling 17.9.x (Catalyst 9300 Switches): Switch geïntegreerde security functies configureren
- Cisco Catalyst 9000 Series Switch geïntegreerde security functies (SISF) - witboek
- Cisco bug-id CSCvx75602 - SISF-geheugenlek in AR-relay en NDH-onderdrukking
- Aangepaste methode voor Cisco bug-id CSCwf3293 - [EVPN SISF] vereist om de limietadreswaarden voor IPv4/V6 met EVPN + DHCP te wijzigen
- Cisco bug-id CSCvq2011 - IOS-XE laat ARP-antwoord vallen wanneer IPDT vanuit ARP wordt gegenereerd
- Cisco bug-id CSCwc2048 - 255 pseudo-poortbeperking per VLAN/evi
- Cisco bug-id CSCwh52315 - 9300 switch laat ARP-antwoord vallen wanneer u een IPDT-beleid in de poort hebt
- Cisco bug-id CSC51480 - IP DHCP-snooping en apparaattracering vrijmaken

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.