Fehlerbehebung bei SISF auf Catalyst Switches der Serie 9000

Inhalt

Einleitung

In diesem Dokument werden die in den Catalyst Switches der Serie 9000 verwendeten Switch Integrated Security Features (SISF) beschrieben. Außerdem wird erläutert, wie SISF verwendet werden kann und wie es mit anderen Funktionen interagiert.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Catalyst 9300-48P mit Cisco IOS® XE 17.3.x

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

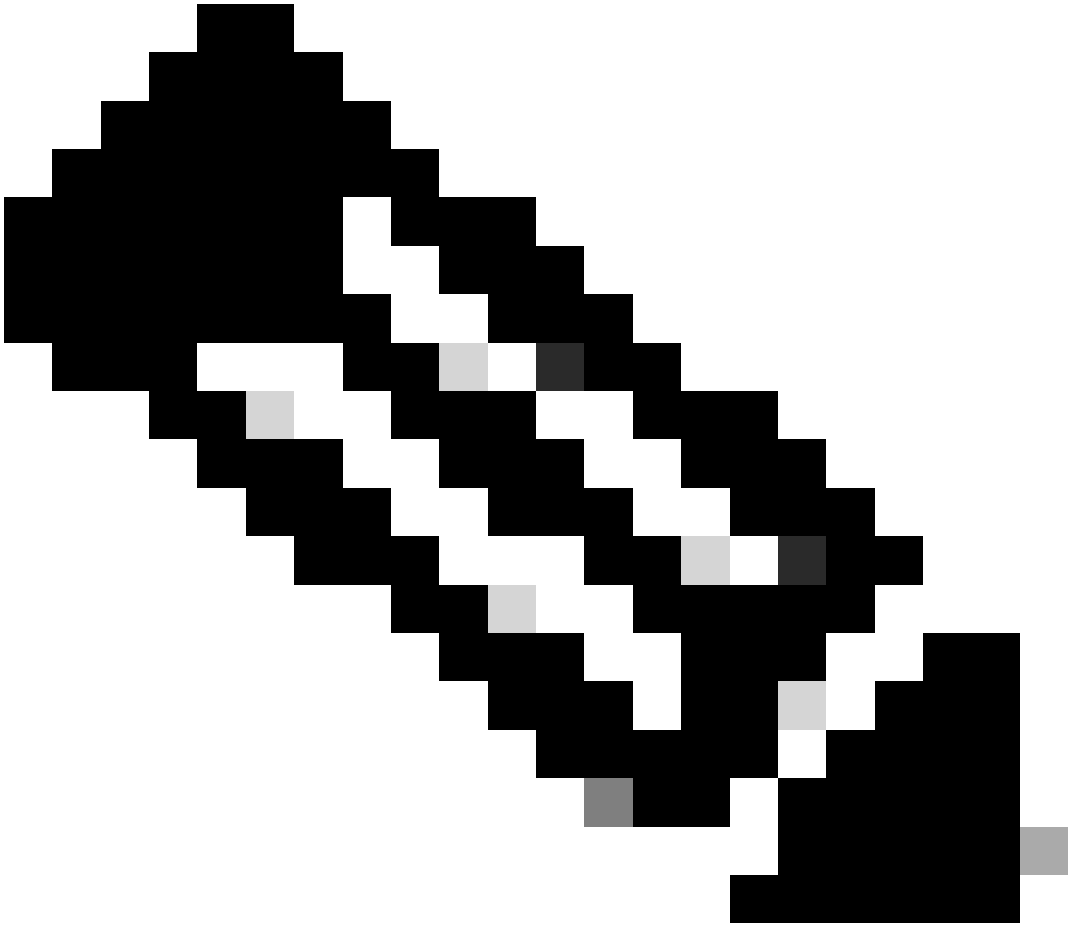
 Hinweis: Informationen zu den Befehlen, die zur Aktivierung dieser Funktionen auf anderen Cisco Plattformen verwendet werden, finden Sie im entsprechenden Konfigurationsleitfaden.

Verwandte Produkte

Dieses Dokument kann auch mit folgenden Hardware- und Softwareversionen verwendet werden:

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

Ab Version 17.3.4 der Cisco IOS XE Software



Hinweis: Dieses Dokument gilt auch für die meisten Cisco IOS XE-Versionen, bei denen SISF und Geräteverfolgung zum Einsatz kommen.

Hintergrundinformationen

Überblick

SISF stellt eine Host-Binding-Tabelle bereit, und es gibt Feature-Clients, die die Informationen aus dieser Tabelle verwenden. Die Einträge werden in die Tabelle durch gelesene Pakete wie DHCP, ARP, ND oder RA aufgenommen, die die Host-Aktivität verfolgen und dabei helfen, die Tabelle dynamisch zu füllen. Wenn die L2-Domäne über unbeaufsichtigte Hosts verfügt, können statische Einträge verwendet werden, um der SISF-Tabelle Einträge hinzuzufügen.

SISF verwendet ein Richtlinienmodell, um Geräterollen und zusätzliche Einstellungen auf dem Switch zu konfigurieren. Eine einzelne Richtlinie kann auf Schnittstellen- oder VLAN-Ebene angewendet werden. Wenn eine Richtlinie für das VLAN und eine andere Richtlinie für die

Schnittstelle angewendet wird, hat die Schnittstellenrichtlinie Vorrang.

SISF kann auch verwendet werden, um die Anzahl der Hosts in der Tabelle zu begrenzen, es bestehen jedoch Unterschiede zwischen dem IPv4- und dem IPv6-Verhalten. Wenn der SISF-Grenzwert festgelegt und erreicht wird:

- IPv4-Hosts funktionieren weiterhin, es müssen jedoch keine weiteren Einträge über dem Grenzwert zur SISF-Tabelle hinzugefügt werden.
- IPv6-Hosts, die es nicht in die SISF-Tabelle schaffen, dürfen keine Einträge in das Netzwerk eingeben, und der SISF-Tabelle dürfen keine neuen Einträge hinzugefügt werden.

Ab Version 16.9.x und neuerer Version wird eine SISF-Client-Funktionspriorität eingeführt. Es fügt Optionen hinzu, um die Updates in SISF zu steuern. Wenn zwei oder mehr Clients die Bindungstabelle verwenden, werden Updates von der Funktion mit höherer Priorität angewendet. Die Ausnahmen sind die "limit address-count for IPv4//IPv6 per mac"-Einstellungen. Die Einstellungen der Richtlinie mit der niedrigsten Priorität sind wirksam.

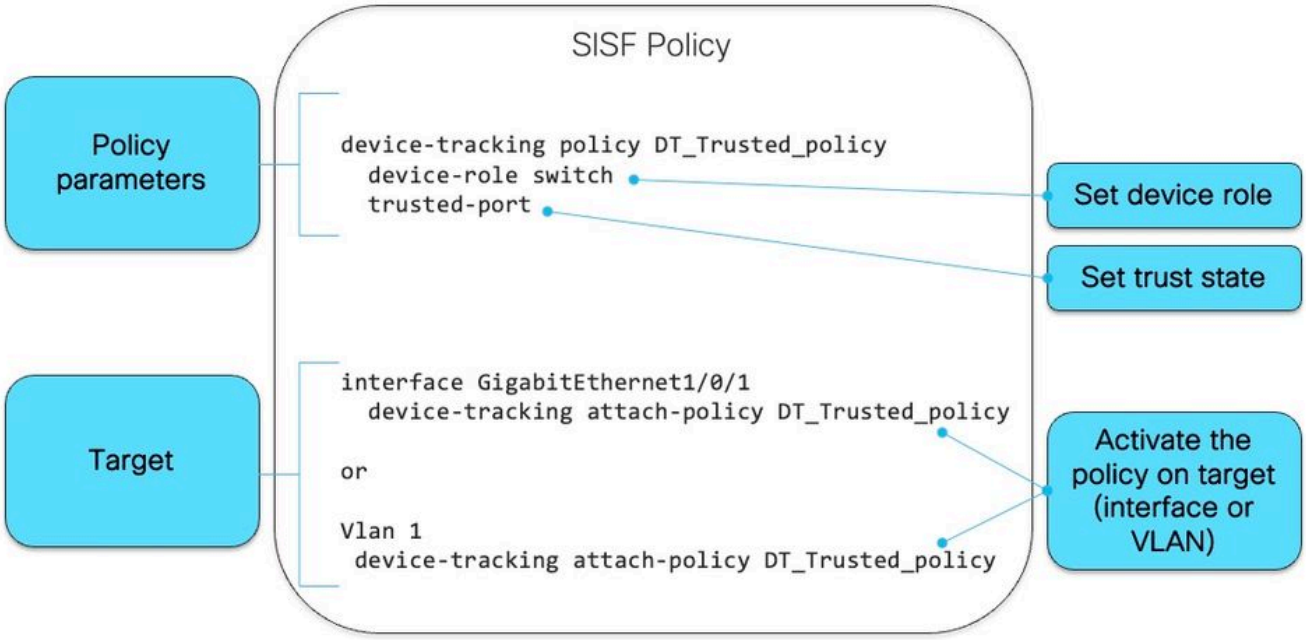
Hier einige Beispiele, bei denen die Geräteverfolgung aktiviert sein muss:

- LISP/EVPN
- Punkt 1x
- Webauthentifizierung
- CTS
- DHCP-Snooping

Hinweis: Zur Auswahl der Richtlinieneinstellungen wird die Priorität verwendet.

Die über die CLI erstellte Richtlinie hat die höchste Priorität (128). Dadurch können Benutzer eine andere Richtlinieneinstellung anwenden als in den programmgesteuerten Richtlinien. Alle konfigurierbaren Einstellungen unter der benutzerdefinierten Richtlinie können manuell geändert werden.

Das nächste Bild zeigt eine SISF-Richtlinie und wie sie gelesen wird:



Innerhalb der Richtlinie können Sie unter "protocol Keyword" (Protokollschlüsselwort) feststellen, welche Pakettypen zum Füllen der SISF-Datenbank verwendet werden:

<#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 - Programmgesteuerte und Client-Funktionen

Die Funktionen in der nächsten Tabelle aktivieren SISF entweder programmgesteuert, wenn sie aktiviert sind, oder fungieren als SISF-Client:

SISF-Programmfunktion	Funktionen des SISF-Clients
LISP im VLAN	Punkt 1x
EVPN im VLAN	Webauthentifizierung
DHCP-Snooping	CTS

Wenn eine SISF-Clientfunktion auf einem Gerät aktiviert ist, das ohne eine Funktion konfiguriert ist, die SISF aktiviert, muss eine benutzerdefinierte Richtlinie auf Schnittstellen konfiguriert werden, die mit Hosts verbunden sind.

IPv4-Funktionen, die SISF-Informationen nutzen

- CTS
- IEEE 802.1x
- LISTE
- EVPN
- DHCP-Snooping (aktiviert nur SISF, verwendet es jedoch nicht)
- IP-Quellschutz

IPv6-Funktionen, die SISF-Informationen nutzen

- IPv6 Router Advertisement (RA) Guard
- IPv6 DHCP Guard, Layer 2 DHCP Relay
- IPv6-DAD-Proxy (Duplicate Address Detection)
- Unterdrückung von Hochwasser
- IPv6 Source Guard
- IPv6-Zielschutz
- RA Throttler
- IPv6-Präfix-Guard

Geräteverfolgung

Die Hauptrolle der Geräteverfolgung besteht darin, die Präsenz, den Standort und die Bewegung von Endknoten im Netzwerk zu verfolgen. SISF tastet den vom Switch empfangenen Datenverkehr ab, extrahiert die Geräteidentität (MAC- und IP-Adresse) und speichert sie in einer Bindungstabelle. Viele Funktionen, wie IEEE 802.1X, Web-Authentifizierung, Cisco TrustSec und LISP usw., hängen von der Genauigkeit dieser Informationen ab, um ordnungsgemäß zu funktionieren. Die SISF-basierte Geräteverfolgung unterstützt IPv4 und IPv6. Es gibt fünf Methoden, mit denen der Client IP lernen kann:

- DHCPv4
- DHCPv6
- ARP
- NDP
- Datenerhebung

SISF auf einem Port-Channel

Die Geräteverfolgung auf Port-Channels (oder Etherchannels) wird unterstützt. Die Konfiguration muss jedoch auf die Channel-Gruppe und nicht auf die einzelnen Port-Channel-Mitglieder angewendet werden. Die einzige Schnittstelle, die vom Bindungsstandpunkt aus angezeigt wird (und bekannt ist), ist der Port-Channel.

Optimierung von Tests und Datenbanken

Sonde:

- In IPDT gab es einen Befehl, um bei doppelten Adressproblemen zu helfen, indem die erste Überprüfung für 10 Sekunden verzögert wurde: "ip device tracking probe delay" upon link up.
- In SISF ist bereits ein Wait-Timer integriert, der wartet, bevor der erste Test gesendet wird. Es ist nicht konfigurierbar und löst das gleiche Problem. Da dies im SISF-Code enthalten ist, ist dieser Befehl nicht mehr erforderlich.

Datenbank:

In SISF können Sie einige Optionen konfigurieren, um zu steuern, wie lange ein Eintrag in der Datenbank gespeichert wird:

<#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-Geräteverfolgung

Lebenszyklus eines Eintrags, zu dem der Host abgefragt wird:

- SISF erhält die IPv4-/IPv6-Bindung pro Mac aufrecht, sobald das IP-Learning erfolgreich abgeschlossen wurde und die Bindung in den REACHABLE-Status wechselt
- SISF verfolgt Lebensdauerclient durch Überwachung des Steuerungspakets
- Wenn 5 Minuten lang kein Steuerungspaket vom Client vorhanden ist, wechselt Binding in den Status VERIFY und sendet Probe an Client
- Wenn Clients nicht auf die Anfrage reagieren, wechselt Bindung in den STALE-Zustand, andernfalls REACHABLE-Zustand
- Das Standard-Timeout für den STALE-Eintrag beträgt 24 Stunden und ist konfigurierbar.
- STALE-Einträge werden nach 24 Stunden gelöscht (oder konfigurierter Timeout-Wert)

Diebstahlerkennung

Arten von Knotendiebstählen:

- IP-Diebstahl (gleiche IP-Adresse, verschiedene MAC-Adressen, verschiedene Ports)
- MAC-DIEBSTAHL (gleiche MAC-Adresse, unterschiedliche IP-Adresse, anderer Port)
- MAC IP THEFT (gleiche MAC-Adresse, gleiche IP-Adresse, anderer Port)

IP-Sicherheitsfunktionen

Dies sind einige der SISF-abhängigen Funktionen:

- NDP-Inspektion: IPv6-NDP-Nachrichten inspizieren
- NDP-Adressenanalyse:Füllen Sie die Bindungstabelle mit der Informationssuche durch Snooping von NDP-Datenverkehr auf.
- Geräteverfolgung: Überwachung der Endgeräteaktivität, auch über einen Livefunktionsmechanismus
- Snooping: Glean-Adressen in NDP-, ARP- und DHCP-Nachrichten Blockieren nicht autorisierter Nachrichten
- DHCPv4-Relay: Relay DHCP-Broadcast-Paket an konfigurierte Helper-Adresse.
- NDP- und ARP-Multicast-Unterdrückung: Unterdrückung von Multicast-NDP-Nachrichten durch Umwandlung in Unicast, um im Namen von Zielen zu antworten.
- DAD-Proxy: Erkennung doppelter Adressen und Senden von NA im Auftrag des Ziel-Clients
- DHCPv4 erforderlich: Erzwingt, dass der Client IP nur über DHCP durchlässt

SISF-Hinweise

Zu den häufigsten Verhaltensweisen im Zusammenhang mit SISF gehören:

- SISF kann durch Aktivieren anderer Funktionen wie DHCP-Snooping aktiviert werden.
- Das standardmäßige Testverhalten von SISF kann sich auf die Client-IP-Adresszuweisung auswirken.
- Wenn SISF aktiviert ist, wird es auch auf Uplink-Ports aktiviert, was zu

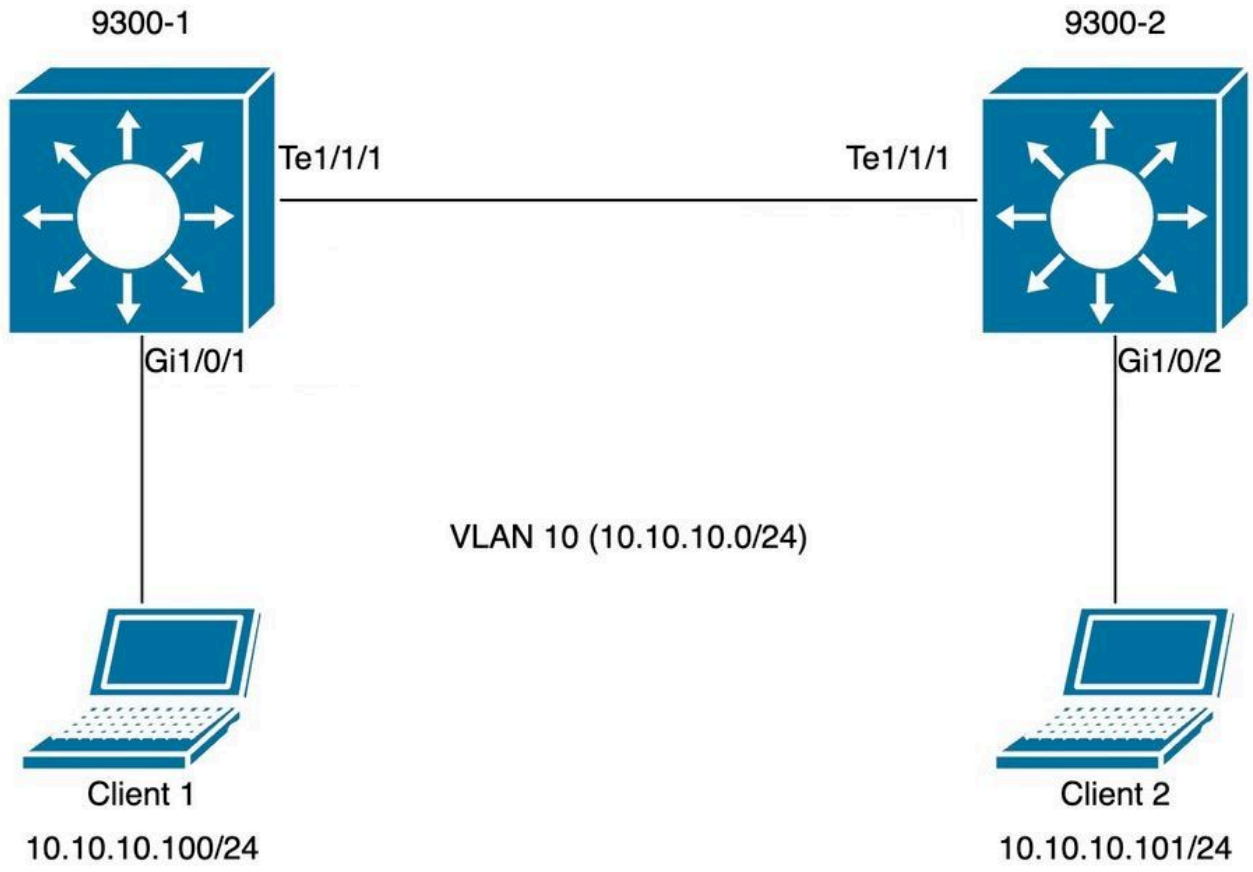
Netzwerkbeeinträchtigungen führen kann.

Fehlerbehebung

Topologie

Das Topologiediagramm wird für das nächste SISF-Szenario verwendet. Bei 9300-Switches handelt es sich nur um Layer-2-Switches, für die im Client-VLAN 10 KEINE SVI konfiguriert ist.

Hinweis: SISF wird in dieser Übung manuell aktiviert.



Konfiguration

Die Standard-SISF-Konfiguration wurde auf beiden 9300 Switches mit Access-Ports eingerichtet, während auf die Trunk-Ports eine benutzerdefinierte Richtlinie angewendet wurde, um die erwarteten SISF-Ausgaben zu veranschaulichen.

Switch 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
```

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
```

Verifizierung

Mit den folgenden Befehlen können Sie die angewendeten Richtlinien validieren:

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

Switch 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#
```

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     T

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


9300-2#
```

Gängige Szenarien

Fehler bei doppelter IPv4-Adresse auf Hostgerät

Problem

Die vom Switch gesendete Keepalive-Anfrage ist eine L2-Prüfung. Aus Sicht des Switches sind daher die in den ARPs als Quelle verwendeten IP-Adressen unwichtig: Diese Funktion kann auf Geräten verwendet werden, auf denen überhaupt keine IP-Adresse konfiguriert ist, sodass die IP-Quelle 0.0.0.0 nicht relevant ist. Wenn der Host diese Nachrichten empfängt, antwortet er zurück und füllt das Ziel-IP-Feld mit der einzigen im empfangenen Paket verfügbaren IP-Adresse, nämlich der eigenen IP-Adresse, auf. Dies kann zu Warnungen über falsche doppelte IP-Adressen führen, da der Host, der antwortet, seine eigene IP-Adresse sowohl als Quelle als auch als Ziel des Pakets sieht.

Es wird empfohlen, die SISF-Richtlinie so zu konfigurieren, dass für ihre Keepalive-Tests eine automatische Quelle verwendet wird.

Hinweis: Weitere Informationen finden Sie in diesem Artikel über doppelte Adressprobleme.

Standardprobe

Dies ist das Testpaket, wenn keine lokale SVI vorhanden ist, und die Standardeinstellungen für Tests:

<#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
```

Lösung

Konfigurieren Sie den Prüfpunkt so, dass er eine andere Adresse als den Host-PC für den Prüfpunkt verwendet. Dies kann mit diesen Methoden erreicht werden

Automatische Quelle für "Verbindung aufrecht halten"

Konfigurieren Sie eine automatische Quelle für die Keepalive-Tests, um die Nutzung von 0.0.0.0 als Quell-IP zu reduzieren:

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

Die Logik bei Anwendung des Auto-Source-Befehls funktioniert wie folgt:

<#root>

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

<-- Optional parameter

1. Legen Sie die Quelle auf VLAN SVI fest, falls vorhanden.
2. Suchen Sie in der IP-Hosttabelle nach einem Quell-/MAC-Paar für dasselbe Subnetz. Die Anfrage stammt von der physischen Switch-Schnittstelle MAC + der IP-Adresse eines anderen Hosts im Subnetz, der sich bereits in der Datenbank befindet.
3. Berechnen Sie die Quell-IP aus der Ziel-IP mit dem bereitgestellten Host-Bit und der bereitgestellten Maske. Der Prüfpunkt wird vom Hören der Client-IP generiert und erstellt einen Prüfpunkt im Subnetz, für den die letzten Bits konfiguriert sind.

Hinweis: Wenn der Befehl mit **<override>** angewendet wird, springen wir immer zu Schritt 3.

Modifizierte Sonde

Durch das Festlegen der Konfiguration für den automatischen Quell-Fallback zur Verwendung einer IP im Subnetz wird der Prüfpunkt geändert. Da keine SVI und kein anderer Client im Subnetz vorhanden ist, greifen wir auf die konfigurierte IP/Maske in der Konfiguration zurück.

<#root>

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

Dies ist das modifizierte Probe-Paket:

<#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
```

Weitere Informationen zum Verhalten von Sonden

Command	Aktion (Zur Auswahl der Quell-IP- und MAC-Adresse für die ARP-Anfrage zur Geräteverfolgung)	Hinweise
automatische Geräteverfolgung	• Legen Sie die Quelle ggf. auf VLAN SVI fest. • Suchen Sie in der Geräteverfolgungstabelle nach IP- und MAC-Bindungen aus demselben Subnetz. • 0.0.0.0 verwenden	Wir empfehlen, die Geräteverfolgung auf allen Trunk-Ports zu deaktivieren, um MAC-Flapping zu vermeiden.
Überschreiben der automatischen Geräteverfolgung	• Quelle auf VLAN-SVI einstellen, falls vorhanden • 0.0.0.0 verwenden	Wird nicht empfohlen, wenn keine SVI vorhanden ist.
Device-Tracking Auto-Source Fallback <IP> <MASK>	• Legen Sie die Quelle ggf. auf VLAN SVI fest. • Suchen Sie in der Geräteverfolgungstabelle nach IP- und MAC-Bindungen aus	Wir empfehlen, die Geräteverfolgung auf allen Trunk-Ports zu deaktivieren, um MAC-Flapping zu vermeiden. Die berechnete IPv4-Adresse darf keinem Client oder

	demselben Subnetz. • Quell-IP aus Client-IP unter Verwendung des bereitgestellten Host-Bit und der bereitgestellten Maske berechnen. Die Quell-MAC-Adresse wird von der MAC-Adresse des zum Client gerichteten Switch-Ports übernommen.	Netzwerkgerät zugewiesen werden.
Device-Tracking Autosource-Fallback <IP> <MASK> überschreiben	• Legen Sie die Quelle ggf. auf VLAN SVI fest. • Quell-IP aus Client-IP unter Verwendung des bereitgestellten Host-Bit und der bereitgestellten Maske berechnen. Die Quell-MAC-Adresse wird von der MAC-Adresse des zum Client gerichteten Switch-Ports übernommen.	Die berechnete IPv4-Adresse darf keinem Client oder Netzwerkgerät zugewiesen werden.

Erläuterung des Befehls device-tracking auto-source fallback <IP> <MASK> [override]:

Je nach Host-IP muss eine IPv4-Adresse reserviert werden.

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

Hinweis: Dies ist eine boolesche Formel.

Beispiel.

Wenn wir den Befehl verwenden:

```
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

Maske = 24

Lässt die boolesche Formel in zwei Teile unterbrechen.

1. Betrieb: 10.152.140.25 UND 255.255.255.0

```
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. Betrieb: 10.152.140.0 ODER 0.0.0.1:

```
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
```

Reservierte IP = 10,152.140,1

Reservierte IP = (10.152.140.25 und 255.255.255.0) | (0,0.0,1) = 10,152.140,1

Hinweis: Die als IP-Quelle verwendete Adresse muss einen Bereich außerhalb der DHCP-Bindungen für das Subnetz aufweisen.

Fehler bei doppelter IPv6-Adresse

Problem

Fehler bei doppelter IPv6-Adresse, wenn IPv6 im Netzwerk aktiviert und eine Switched Virtual Interface (SVI) in einem VLAN konfiguriert ist.

In einem normalen IPv6-DAD-Paket wird das Feld "Source Address" (Quelladresse) im IPv6-Header auf die nicht angegebene Adresse (0:0:0:0:0:0:0:0) festgelegt. Ähnlich wie bei IPv4.

Wählen Sie im SISF-Test die Quelladresse aus:

- Link-Local-Adresse der SVI, falls konfiguriert
- 0:0:0:0:0:0:0:0

Lösung

Es wird empfohlen, der SVI-Konfiguration die nächsten Befehle hinzuzufügen. Auf diese Weise kann die SVI automatisch eine Link-Local-Adresse abrufen. Diese Adresse wird als Quell-IP-Adresse des SISF-Tests verwendet, um ein Duplikat der IP-Adresse zu vermeiden.

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

Erhöhte Arbeitsspeicher- und CPU-Auslastung

Problem

Die vom Switch gesendete Keepalive-Anfrage wird über alle Ports gesendet, wenn sie programmgesteuert aktiviert ist. Verbundene Switches in derselben L2-Domäne senden diese Broadcasts an ihre Hosts, sodass der ursprüngliche Switch Remote-Hosts seiner Geräteverfolgungsdatenbank hinzufügt. Die zusätzlichen Hosteinträge erhöhen die Speichernutzung auf dem Gerät, und der Vorgang des Hinzufügens der Remote-Hosts erhöht die CPU-Nutzung des Geräts.

Es wird empfohlen, die programmatische Richtlinie durch Konfigurieren einer Richtlinie für den Uplink zu angeschlossenen Switches zu erweitern, um den Port als vertrauenswürdig und an einen Switch angeschlossen zu definieren.

Hinweis: Beachten Sie, dass SISF-abhängige Funktionen wie DHCP-Snooping das ordnungsgemäße Funktionieren von SISF ermöglichen, was dieses Problem auslösen kann.

Lösung

Konfigurieren Sie eine Richtlinie für den Uplink (Trunk), um Tests und das Lernen von Remote-Hosts zu stoppen, die von anderen Switches bevorzugt werden (SISF wird nur zum Verwalten der lokalen Hosttabelle benötigt).

<#root>

```
device-tracking policy DT_trunk_policy
 trusted-port
 device-role switch

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

Erreichbarkeit der Geräteverfolgung zu kurz

Problem

Aufgrund eines Migrationsproblems von IPDT zu SISF-basierter Geräteverfolgung kommt es bei der Migration von älteren Versionen auf 16.x und neuere Versionen manchmal zu einer nicht standardmäßigen erreichbaren Zeit.

Lösung

Es wird empfohlen, die erreichbare Standardzeit wiederherzustellen. Hierzu konfigurieren Sie:

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

In Meraki-Tool integrierte Switches (Erhöhung der CPU und Leerung von Ports)

Problem

Wenn Switches in das Meraki Cloud-Überwachungstool integriert werden, wendet dieses Tool benutzerdefinierte Richtlinien für die Geräteverfolgung an.

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

Die Richtlinie wird unterschiedslos auf alle Schnittstellen angewendet, d. h. sie unterscheidet nicht zwischen Edge-Ports und Trunk-Ports, die anderen Netzwerkgeräten (z. B. Switches, Firewalls, Router usw.) gegenüberliegen. Der Switch kann mehrere SISF-Einträge auf Trunk-Ports erstellen, auf denen MERAKI_POLICY konfiguriert ist, was zu Leerungen an diesen Ports sowie zu einem Anstieg der CPU-Auslastung führt.

<#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
```

Lösung

Richten Sie die nächste Richtlinie für alle Nicht-Edge-Schnittstellen ein:

```
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 mit derselben MAC nicht in SISF-Tabelle

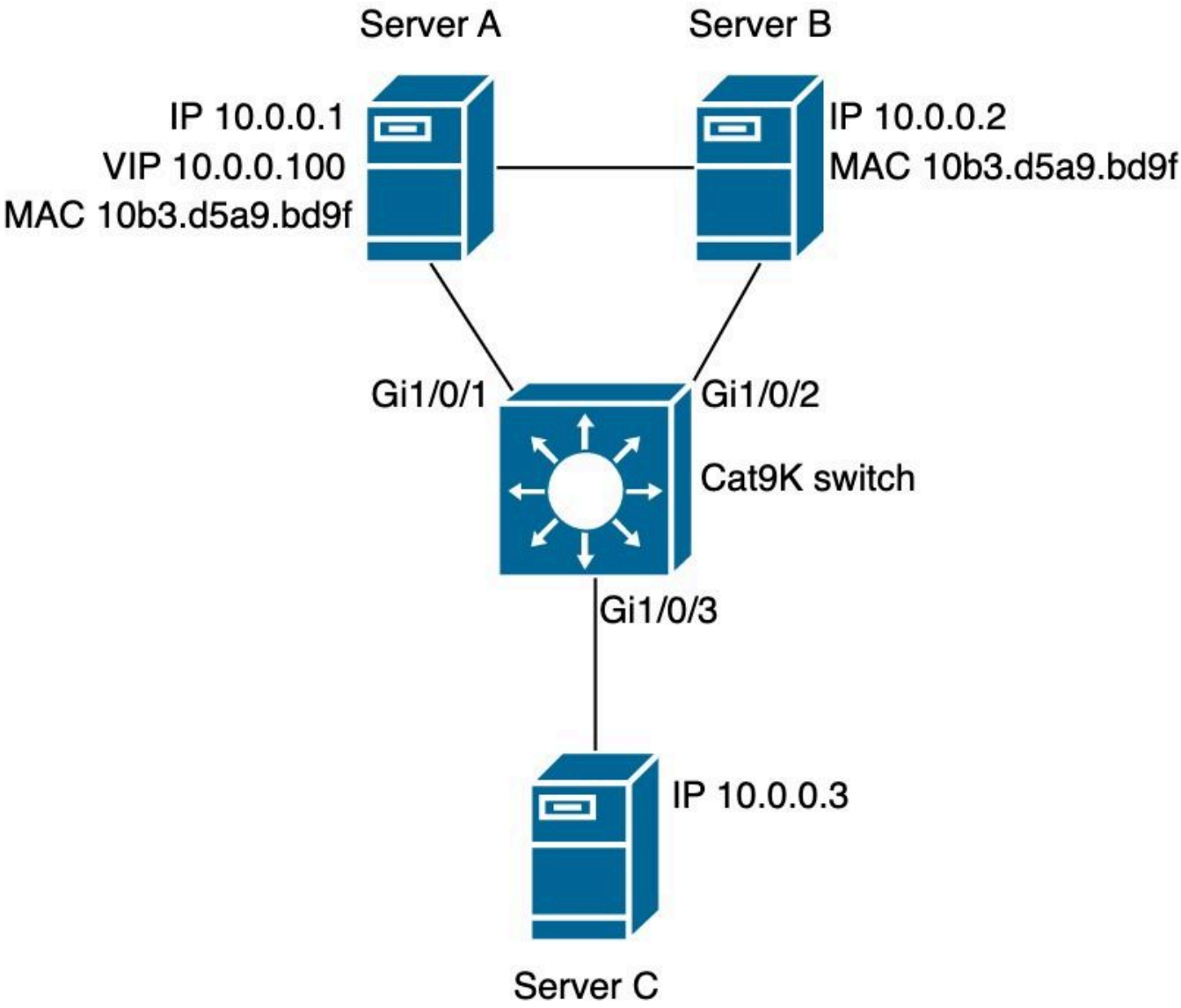
Problem

Dieses Szenario tritt häufig bei Appliances im HA-Modus (hohe Verfügbarkeit) auf, die unterschiedliche IP-Adressen, aber dieselbe MAC-Adresse verwenden. Sie wird auch in VM-Umgebungen beobachtet, die denselben Zustand aufweisen (eine MAC-Adresse für zwei oder mehr IP-Adressen). Diese Bedingung verhindert Netzwerkverbindungen zu allen IPs, die keinen Eintrag in der SISF-Tabelle haben, wenn eine benutzerdefinierte SISF-Richtlinie im Schutzmodus aktiviert ist.Gemäß der SISF-Funktion wird nur eine IP pro MAC-Adresse gelernt.

Hinweis: Dieses Problem tritt bei Versionen 17.7.1 und höher auf.

Beispiel:

- Die IP-Adresse 10.0.0.1 mit der MAC-Adresse 10b3.d5a9.bd9f wird in der SISF-Tabelle erfasst und kann mit dem Netzwerkgerät 10.0.0.3 kommunizieren.
- Die zweiten IP-Adressen 10.0.0.2 und Virtual IP 10.0.0.100, die die MAC-Adresse 10b3.d659.7858 gemeinsam nutzen, sind jedoch nicht in der SISF-Tabelle programmiert, und eine Kommunikation mit dem Netzwerk ist nicht zulässig.



SISF-Richtlinie

<#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-Datenbank

<#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
```

Erreichbarkeitstest 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
.....
```

Erreichbarkeitstest 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)
```

Validierung verwirft auf Switch.

<#root>

```
switch(config)#
```

device-tracking logging

Protokolle

<#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

Lösung

Option 1: Wenn Sie die IPDT-Richtlinie vom Port entfernen, können ARP-Pakete und betroffene Geräte erreicht werden

<#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

Option 2: Entfernen Sie Protokoll-ARP-Läuterung aus der Richtlinie zur Geräteverfolgung.

<#root>

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

no protocol arp

Option 3: Ändern Sie die Sicherheitsstufe von "IPDT_POLICY" in "Glean".

<#root>

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

security-level glean

Zugehörige Informationen

- Leitfaden zur Sicherheitskonfiguration, Cisco IOS XE Bengaluru 17.6.x (Catalyst 9300-Switches): Konfigurieren der integrierten Sicherheitsfunktionen des Switches
- Leitfaden zur Sicherheitskonfiguration, Cisco IOS XE Cupertino 17.9.x (Catalyst 9300-Switches): Konfigurieren der integrierten Sicherheitsfunktionen des Switches
- Cisco Catalyst Switches der Serie 9000 - SISF (Integrated Security Features) (Whitepaper)
- Cisco Bug-ID CSCvx75602 - SISF-Speicherleck in AR-Relay und ND-Unterdrückung
- Cisco Bug-ID CSCwf3293 - [EVPN SISF] Benutzerdefinierte Methode erforderlich, um die Adressgrenzwerte für IPv4/V6 mit EVPN + DHCP zu ändern
- Cisco Bug-ID CSCvq2011 - IOS-XE verwirft ARP-Antwort, wenn IPDT von ARP erkannt wird
- Cisco Bug-ID: CSCwc2048 - 255 Pseudo-Ports mit Beschränkung pro VLAN/EVI
- Cisco Bug-ID CSCwh52315 - 9300-Switch beendet ARP-Antwort, wenn eine IPDT-Richtlinie im Port vorhanden ist
- Cisco Bug-ID CSCvd51480 - Unbinding ip dhcp snooping and device-tracking

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.