排除Catalyst 9000系列交換機上的SISF故障

目錄

簡介

本檔案將說明Catalyst 9000系列交換器中所使用的交換器整合式安全功能(SISF)。 它還解釋了如何使用SISF以及如何與其他功能互動。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據執行Cisco IOS® XE 17.3.x的Cisco Catalyst 9300-48P

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

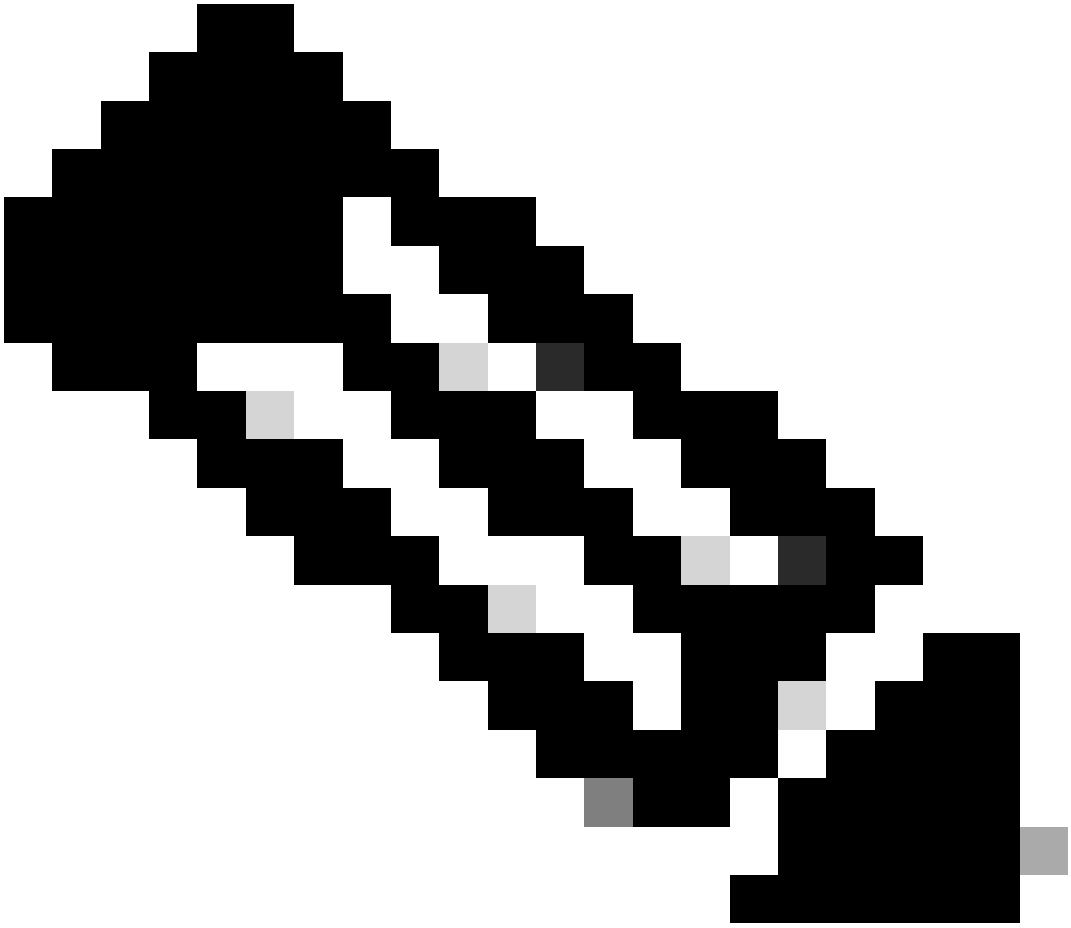
注意：有關用於在其他Cisco平台上啟用這些功能的命令，請參閱相應的配置指南。

相關產品

本文件也適用於以下硬體和軟體版本：

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

包含17.3.4及更高版本的Cisco IOS XE軟體



注意：本文檔還適用於大多數使用SISF與裝置跟蹤的Cisco IOS XE版本。

背景資訊

概觀

SISF提供了一個主機繫結表，並且有一些功能客戶端使用該表中的資訊。透過收集DHCP、ARP、ND和RA等跟蹤主機活動並幫助動態填充表的資料包，可將條目填充到表中。如果L2域中有無訊息主機，則可使用靜態條目將條目增加到SISF表中。

SISF使用策略模型來配置交換機上的裝置角色和其他設定。可在介面或VLAN級別上應用單個策略。如果在VLAN上應用了策略，而在介面上應用了不同的策略，則優先使用介面策略。

SISF也可用於限製表中的主機數量，但IPv4和IPv6行為之間存在差異。如果已設定SISF限制且已達到：

- IPv4主機繼續運行，但不會向SISF表中增加超出限制的條目

- 未進入SISF表的IPv6主機不允許進入網路，並且不會向SISF表增加新條目。

從16.9.x和更新版本開始引入SISF客戶端功能優先順序。它會增加選項來控制對SISF的更新，如果兩個或更多客戶端正在使用繫結表，則會應用來自更高優先順序功能的更新。 此處例外的是「限制每個mac的IPv4//IPv6地址計數」設定，具有最低優先順序的策略設定是有效的。

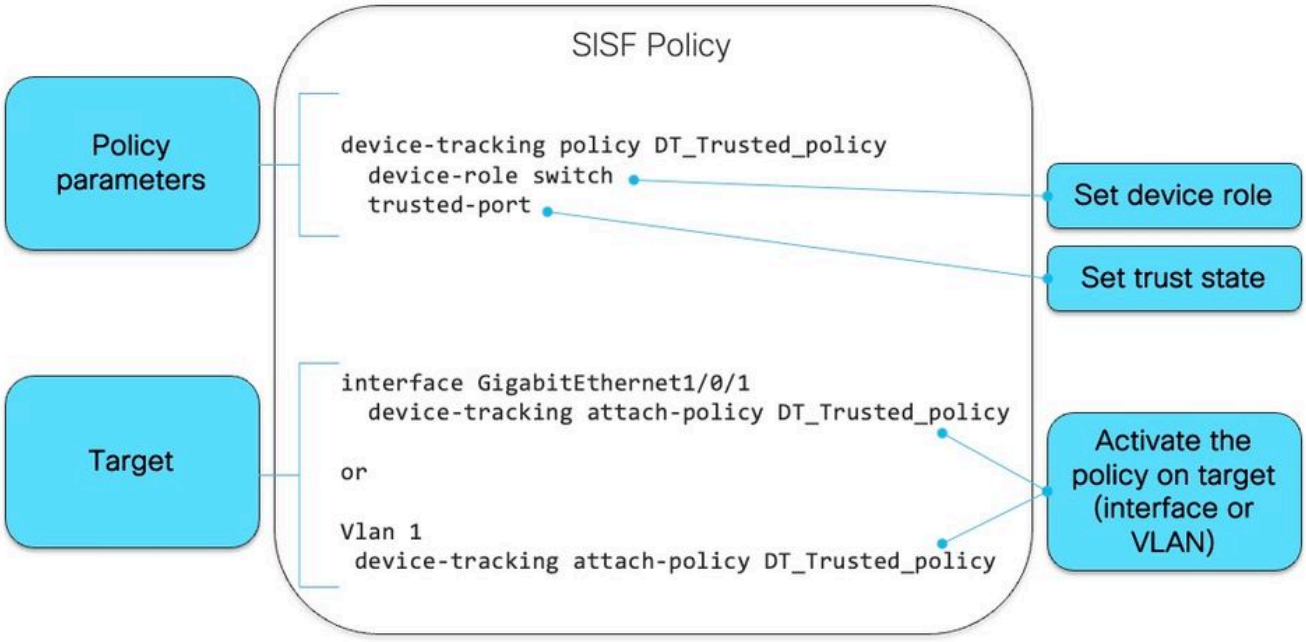
需要啟用裝置跟蹤的一些示例功能包括：

- LISP/EVPN
- Dot1x
- Web身份驗證
- CTS
- DHCP窺探

注意：優先順序用於選擇策略設定。

從CLI建立的策略具有最高優先順序(128)，因此允許使用者應用與程式設計策略中的策略設定不同的策略設定。可以手動更改自定義策略下的所有可配置設定。

下一張圖是SISF策略的示例以及如何讀取該策略：



在策略內部，在protocol關鍵字下，您可以選擇檢視用於填充SISF資料庫的資料包型別：

```
<#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程式與使用者端功能

下表中的功能可在啟用SISF時以程式設計方式啟用SISF，或作為SISF的客戶端：

SISF程式設計功能	SISF客戶端功能
VLAN上的LISP	Dot1x
VLAN上的EVPN	Web身份驗證
DHCP窺探	CTS

如果在未配置啟用SISF功能的裝置上啟用了SISF客戶端功能，則必須在連線到主機的介面上配置自定義策略。

使用SISF資訊的IPv4功能

- CTS
- IEEE 802.1x
- LISP

- EVPN
- DHCP監聽（僅啟用SISF，但不使用）
- IP來源防護

使用SISF資訊的IPv6功能

- IPv6路由器通告(RA)防護
- IPv6 DHCP防護，第2層DHCP中繼
- IPv6重複位址偵測(DAD)代理
- 泛洪抑制
- IPv6來源防護
- IPv6目的地防護
- RA節流器
- IPv6首碼防護

裝置追蹤

裝置跟蹤的主要作用是跟蹤網路中終端節點的存在、位置和移動。SISF監聽交換機接收的流量，提取裝置標識（MAC和IP地址），並將它們儲存在繫結表中。 許多功能（如IEEE 802.1X、Web身份驗證、Cisco TrustSec和LISP等）依賴於此資訊的準確性才能正常運行。 基於SISF的裝置跟蹤支援IPv4和IPv6。 客戶端可透過以下五種受支援的方法學習IP：

- DHCPv4
- DHCPv6
- ARP
- NDP
- 資料收集

埠通道上的SISF

支援埠通道（或ether-channel）上的裝置跟蹤。但配置必須應用於通道組，而不是單個埠通道成員。從繫結角度顯示（且已知）的唯一介面是埠通道。

探測和資料庫調整

探測：

- 在IPDT中，有一個命令透過將初始探測延遲了10秒來幫助解決重複地址問題：「ip device tracking probe delay」。
- 在SISF中，已經內建了等待計時器，在傳送第一個探測器之前等待該計時器。它不可配置，可解決相同的問題。由於此命令位於SISF代碼中，因此不再需要此命令

資料庫：

在SISF中，您可以配置一些選項來控制條目在資料庫中的保留時間：

```
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裝置追蹤

輪詢主機的條目的生命週期：

- SISF維護每個Mac的IPv4/IPv6繫結，一旦IP學習成功，繫結將轉換為可訪問狀態
- SISF透過監控控制資料包跟蹤活動客戶端
- 如果5分鐘內沒有來自客戶端的控制資料包，繫結將轉換為VERIFY狀態並傳送探測到客戶端
- 如果客戶端不響應探測，則繫結將轉換為STALE狀態，否則為REACHABLE狀態
- STALE條目的預設超時為24小時，並且可以配置
- 過時的條目將在24小時後（或配置的超時值）刪除

竊盜偵測

節點盜竊型別：

- IP竊盜（相同IP、不同MAC、不同/相同埠）
- MAC失竊（相同MAC、不同IP、不同埠）
- MAC IP竊盜（相同mac、相同ip、不同埠）

IP安全功能

以下是SISF相關的一些功能：

- NDP檢查：檢查IPv6 NDP消息
- NDP地址收集：使用透過監聽NDP流量收集的資訊填充繫結表
- 裝置跟蹤：監控終端裝置活動，包括透過某種活動機制
- 監聽：收集NDP、ARP和DHCP消息中的地址。阻止未授權的郵件
- DHCPv4中繼：將DHCP廣播的資料包中繼到已配置的幫助程式地址。
- NDP和ARP組播抑制：透過轉換為單播或代表目標做出響應來抑制組播NDP消息。
- DAD代理：重複地址檢測和代表目標客戶端傳送NA
- DHCPv4要求：它強制客戶端僅透過DHCP獲取IP

SISF警告

觀察到的一些與SISF相關的最常見行為包括：

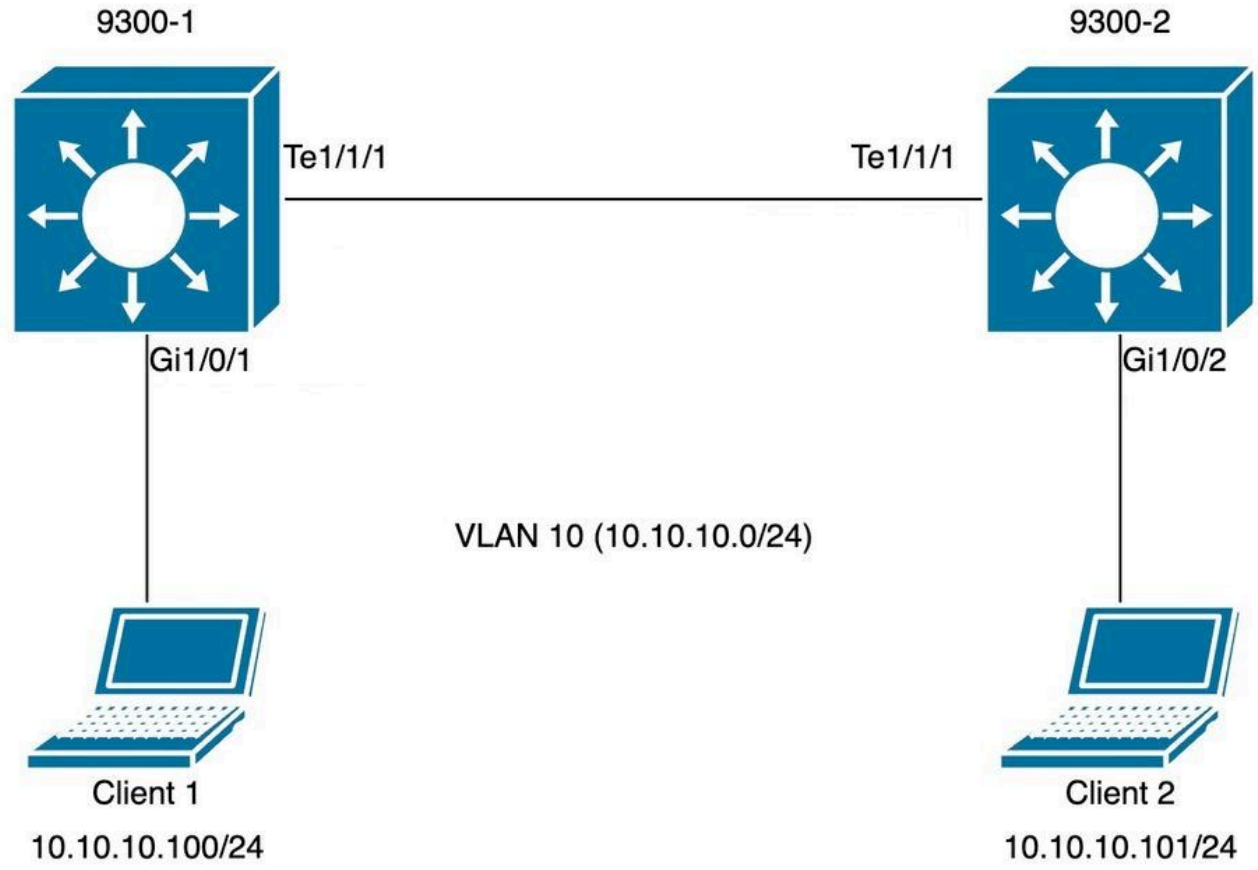
- 可透過啟用其他功能（如dhcp監聽）啟用SISF
- SISF的預設探測行為可能影響客戶端IP地址分配。
- 啟用SISF後，上行鏈路埠上也會啟用它，這會對網路造成影響。

疑難排解

拓撲

拓撲圖用於下一個SISF方案。9300交換機僅為第2層，在客戶端Vlan 10中未配置SVI。

注意：本實驗手動啟用了SISF。



組態

預設SISF配置是在面向接入埠的兩台9300交換機上設定的，而自定義策略則應用於中繼埠，以說明預期的SISF輸出。

交換機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
```

交換機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
```

驗證

可以使用以下命令驗證應用的策略：

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

交換機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#
```

交換機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#
```

常見案例

主機裝置上的IPv4地址重複錯誤

問題

交換機傳送的「keepalive」探測是L2檢查。因此，從交換機的角度來看，在ARP中用作源的IP地址並不重要：此功能可用於未配置IP地址的裝置，因此0.0.0.0的IP源並不相關。 當主機收到此消息時，它會回覆並以接收的資料包中唯一可用的IP地址（即它自己的IP地址）填充目標IP欄位。這可能會導致錯誤重複的IP地址警報，因為回覆的主機將自己的IP地址同時視為資料包的源和目標。

建議將SISF策略配置為對其keepalive探測使用自動源。

備註：如需進一步資訊，請參閱有關重複位址問題的本文

預設探查

這是不存在本地SVI和預設探測設定時的探測資料包：

<#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
```

解決方案

將探測配置為使用主機PC以外的地址進行探測。這可以透過以下方法實現

「Keep-Alive」探測的自動源

為「keep-alive」探測功能配置一個自動源，以減少將0.0.0.0用作源IP：

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

應用auto-source命令時的邏輯工作如下：

```
<#root>

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

<-- Optional parameter
```

1. 將源設定為VLAN SVI（如果有）。
2. 在IP主機表中搜尋同一子網的源/MAC對。 探測源自交換機物理介面MAC和資料庫中某個子網

中其他主機的IP。
3. 使用提供的主機位和掩碼計算目標IP的源IP。探測功能是透過偵聽客戶端IP並在配置最後位的情況下在子網中建立探測功能生成的。

附註：如果命令與<override>一起套用，我們一律會跳到步驟3。

已修改的探測

將auto-source fallback config設定為使用子網中的IP將修改探測。由於子網中沒有SVI和其他客戶端，因此我們返回到配置中配置的IP/掩碼。

<#root>

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

以下是已修改的探測封包：

<#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
```

有關探測行為的更多詳細資訊

指令	動作 （為了選擇裝置跟蹤ARP探測的源IP和MAC地址）	備註
裝置跟蹤跟蹤跟蹤自動源	• 如果存在，將源設定為VLAN SVI。 • 在裝置跟蹤表中查詢來自同一子網的IP和MAC繫結。 • 使用0.0.0.0	我們建議停用所有中繼埠上的裝置跟蹤以避免MAC抖動。
裝置跟蹤跟蹤跟蹤自動源覆蓋	• 如果存在，將源設定為VLAN SVI • 使用0.0.0.0	不建議沒有SVI時使用。
裝置跟蹤跟蹤自動源回退<IP> <MASK>	• 如果存在，將源設定為VLAN SVI。 • 在裝置跟蹤表中查詢來自同一子網的IP和MAC繫結。 • 使用提供的主機位和掩碼計算來自客戶端IP的源IP。源MAC地址取自面向客戶端的交換機埠的MAC地址。	我們建議停用所有中繼埠上的裝置跟蹤以避免MAC抖動。 不得將計算的IPv4地址分配給任何客戶端或網路裝置。
裝置跟蹤跟蹤自動源回退<IP> <MASK>覆蓋	• 如果存在，將源設定為VLAN SVI。 • 使用提供的主機位和掩碼計算來自客戶端IP的源IP。源MAC地址取自面向客戶端的交換機埠的MAC地址。	不得將計算的IPv4地址分配給任何客戶端或網路裝置。

device-tracking tracking auto-source fallback <IP> <MASK> [override]命令的說明：

根據主機ip，需要保留IPv4地址。

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

注意：這是布林公式

範例.

如果我們使用命令：

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

主機IP = 10.152.140.25

IP = 0.0.0.1

遮罩= 24

將布林公式分為兩部分。

1. 10.152.140.25和255.255.255.0操作：

```
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或0.0.0.1操作：

```
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
```

保留的IP = 10.152.140.1

保留的IP = （10.152.140.25和255.255.255.0）| (0.0.0.1) = 10.152.140.1

註：用作子網的DHCP繫結中必須包含作為IP源的地址。

重複IPv6地址錯誤

問題

在網路中啟用IPv6並在VLAN上配置交換虛擬介面(SVI)時出現重複IPv6地址錯誤。

在普通IPv6 DAD資料包中，IPv6報頭中的Source Address欄位設定為未指定的地址(0:0：0:0：0:0：0:0)。類似於IPv4情況。

在SISF探測中選擇源地址的順序為：

- SVI的本地鏈路地址（如果已配置）
- 使用0:0：0:0：0:0：0:0

解決方案

我們建議您向SVI配置增加以下命令。這使SVI能夠自動獲取本地鏈路地址；該地址用作SISF探測的源IP地址，從而防止重複的IP地址問題。

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

記憶體和CPU利用率提高

問題

當以程式設計方式啟用時，交換機傳送的「keepalive」探測會從所有埠廣播。 同一L2域中的連線交換機將這些廣播傳送到其主機，導致源交換機將遠端主機增加到其裝置跟蹤資料庫。 額外的主機條目會增加裝置上的記憶體使用，而增加遠端主機的過程會增加裝置的CPU利用率。

建議透過在連線到交換機的上行鏈路上配置策略來限定程式設計策略的範圍，以便將埠定義為受信任且連線到交換機。

注意：請注意，SISF相關功能（如DHCP監聽）使SISF能夠正常運行，這可能會引發此問題。

解決方案

在上行鏈路（中繼）上配置策略以停止探測和學習喜歡在其他交換機上的遠端主機(僅需要使用SISF來維護本地主機表)

```
<#root>
device-tracking policy DT_trunk_policy
 trusted-port
```

```
 device-role switch


interface <interface>
 device-tracking policy
```

DT_trunk_policy

裝置跟蹤可達時間太短

問題

由於從IPDT遷移到基於SISF的裝置跟蹤的問題，從較舊版本遷移到16.x和更新版本時，有時會引入非預設的可達時間。

解決方案

建議透過配置以下內容恢復到預設的可訪問時間：

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

交換機已連線到Meraki工具（CPU增加和埠刷新）

問題

當交換機連線到Meraki雲監控工具時，此類工具會推送自定義裝置跟蹤策略。

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

該策略應用於所有介面時沒有任何區別，也就是說，它不會區分面向其他網路裝置（例如交換機、防火牆路由器等）的邊緣埠和中繼埠。交換機可以在配置了MERAKI_POLICY的中繼埠上建立多個SISF條目，因此將引起這些埠上的刷新以及CPU使用率增加。

<#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
```

解決方案

在所有非邊緣介面上設定下一個策略：

```
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
```

具有相同MAC的IP地址不在SISF表中

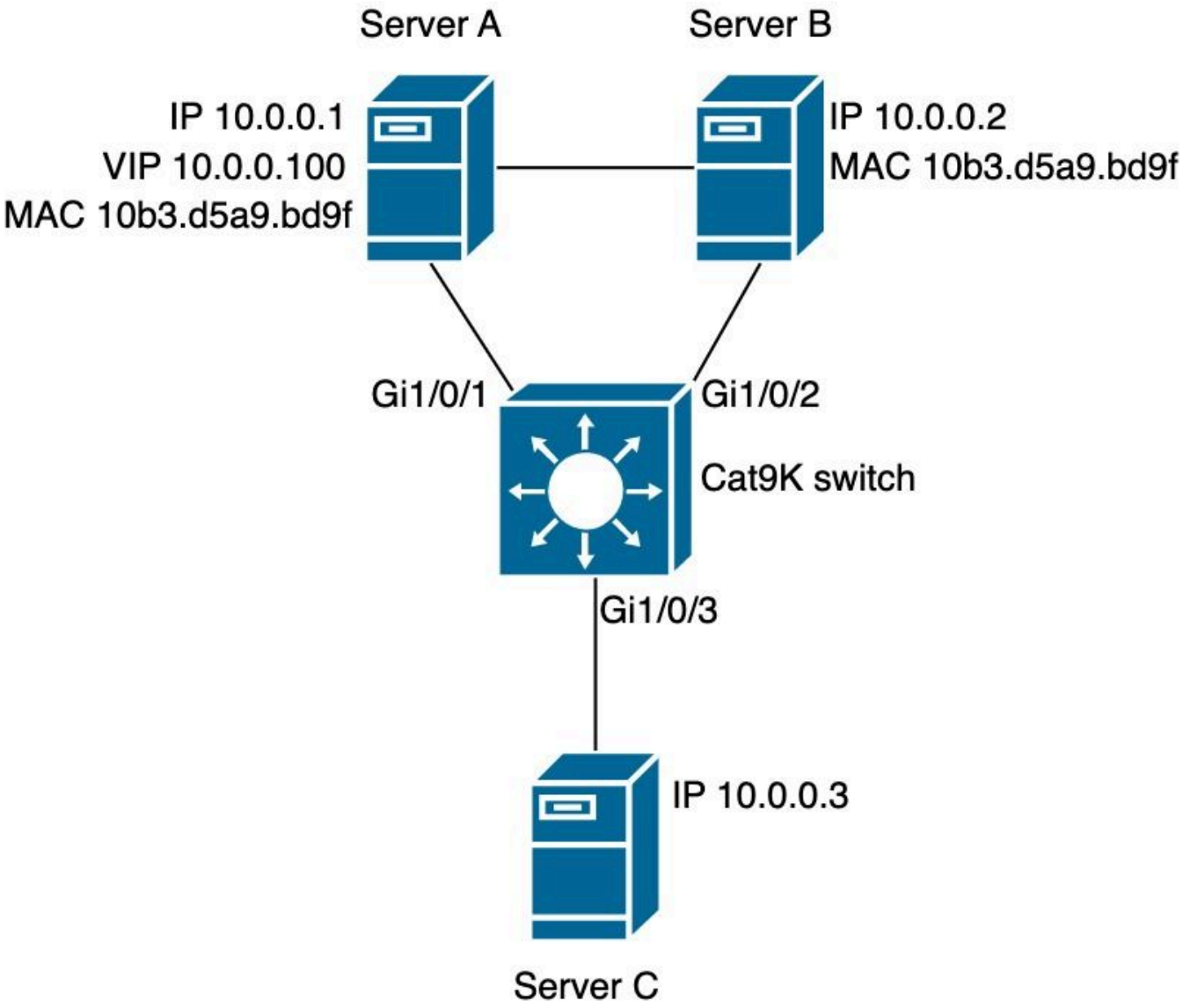
問題

此情況常見於HA（高可用性）模式中具有不同IP地址但共用相同MAC地址的裝置。在共用相同條件（兩個或多個IP地址使用單個MAC地址）的VM環境中也可觀察到此情況。當處於保護模式的自定義SISF策略到位時，此情況將阻止連線到在SISF表中沒有條目的所有IP。根據SISF功能，每個MAC地址只獲知一個IP。

注意：此問題存在於17.7.1及後續版本中

範例：

- MAC地址為10b3.d5a9.bd9f的IP 10.0.0.1在SISF表上獲知並允許與網路裝置10.0.0.3通訊。
- 但是，共用MAC地址10b3.d659.7858的第二個IP 10.0.0.2和虛擬IP 10.0.0.100未在SISF表中程式設計，並且不允許與網路通訊。



SISF策略

<#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資料庫

<#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
```

可接通性測試伺服器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
.....
```

可接通性測試伺服器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)
```

正在驗證交換機上的丟棄。

<#root>

```
switch(config)#
```

device-tracking logging

記錄檔

<#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

解決方案

選項1：從埠刪除IPDT策略，允許ARP資料包和受影響的裝置到達埠

<#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

選項2：從裝置跟蹤策略中刪除協定ARP收集。

<#root>

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

no protocol arp

選項3：將IPDT_POLICY的安全級別更改為收集。

<#root>

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

security-level glean

相關資訊

- 安全配置指南，Cisco IOS XE Bengaluru 17.6.x（Catalyst 9300交換機）：配置交換機整合安全功能
- 安全配置指南，Cisco IOS XE Cupertino 17.9.x（Catalyst 9300交換機）：配置交換機整合安全功能
- Cisco Catalyst 9000系列交換機整合安全功能(SISF)白皮書
- 思科漏洞ID CSCvx75602 - AR中繼和ND抑制中的SISF記憶體洩漏
- 思科漏洞ID CSCwf33293 - [EVPN SISF]使用EVPN + DHCP修改IPv4/V6的限制地址值所需的自定義方法
- 思科漏洞ID CSCvq22011 - IPDT從ARP進行聚合時，IOS-XE丟棄ARP應答
- 思科漏洞ID CSCwc20488 - 每個vlan/evi的255個偽埠限制
- 思科漏洞ID CSCwh52315 - 9300交換機在埠中具有IPDT策略時丟棄ARP應答
- 思科漏洞ID CSCvd51480 - 解除繫結ip dhcp監聽和裝置跟蹤

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。