排除Catalyst 9000系列交换机上的SISF故障

目录

简介

本文档介绍Catalyst 9000系列交换机中使用的交换机集成安全功能(SISF)。 它还说明了如何使用SISF以及如何与其他功能交互。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于运行Cisco IOS® XE 17.3.x的Cisco Catalyst 9300-48P

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

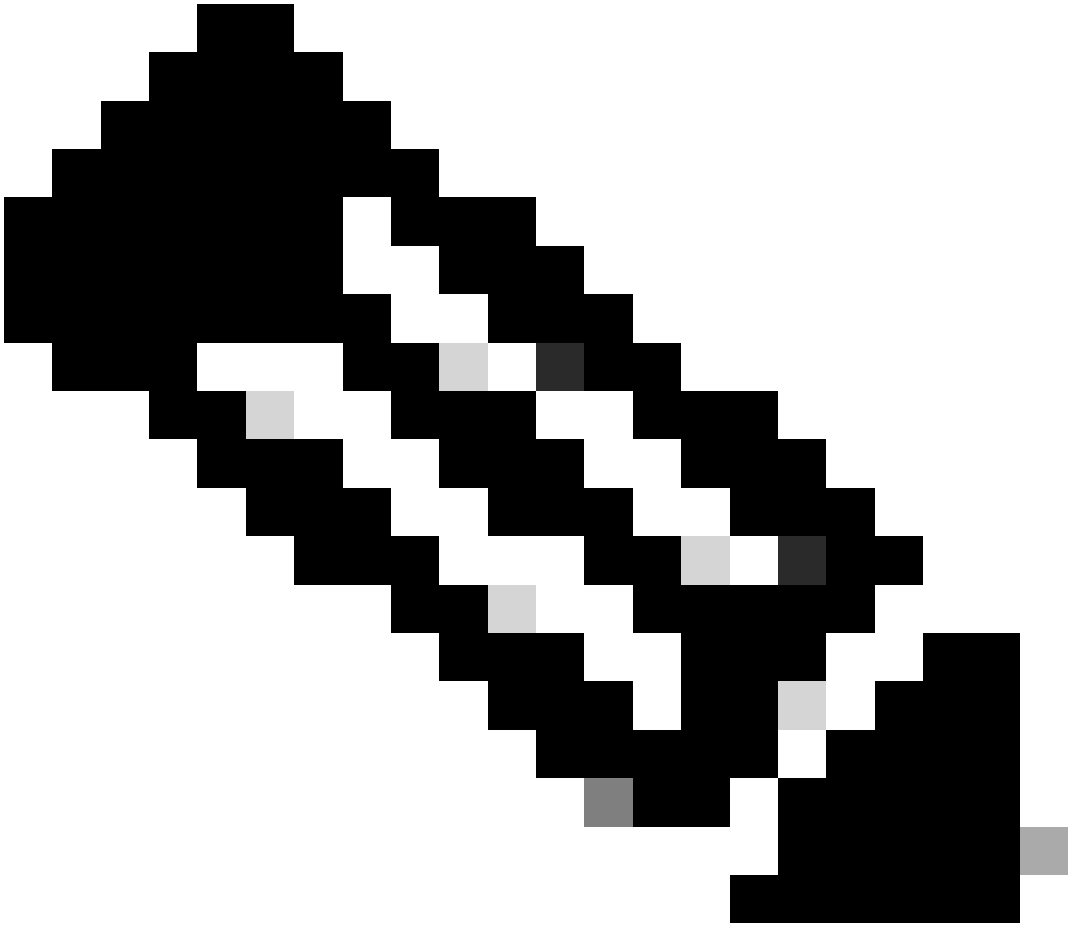
注意：有关在其他思科平台上启用这些功能的命令，请参阅相应的配置指南。

相关产品

本文档也可用于以下硬件和软件版本：

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

具有17.3.4及更高版本的Cisco IOS XE软件



注意：本文档也适用于大多数使用SISF与设备跟踪的Cisco IOS XE版本。

背景信息

概述

SISF提供了一个主机绑定表，并且有一些功能客户端使用其信息。通过收集跟踪主机活动并帮助动态填充表的数据包（如DHCP、ARP、ND和RA），这些条目会填充到表中。如果L2域中存在静默主机，则可以使用静态条目将条目添加到SISF表中。

SISF使用策略模型来配置交换机上的设备角色和其他设置。单个策略可应用于接口或VLAN级别。如果策略应用在VLAN上，而另一个策略应用在接口上，则优先使用接口策略。

SISF还可用于限制表中的主机数量，但IPv4和IPv6行为之间存在差异。如果设置了SISF限制且达到该限制：

- IPv4主机继续运行，但不会再向SISF表中添加超过限制的条目

- 未将其添加到SISF表中的IPv6主机不允许进入网络，并且不会向SISF表添加新条目。

从16.9.x及更高版本中引入了SISF客户端功能优先级。它添加了选项来控制对SISF的更新，如果两个或更多客户端正在使用绑定表，则会应用优先级较高的功能的更新。 此处的例外是“每个mac的IPv4//IPv6限制地址计数”设置，具有最低优先级的策略设置是有效的。

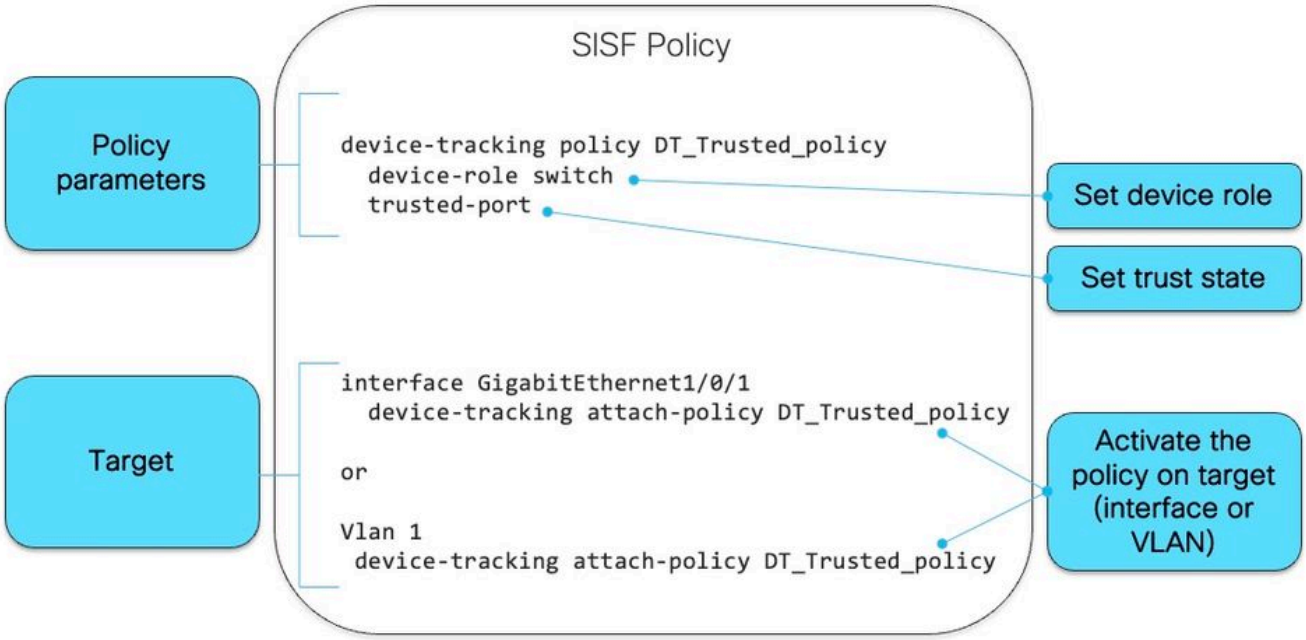
需要启用设备跟踪的一些示例功能包括：

- LISP/EVPN
- Dot1x
- Web身份验证
- CTS
- DHCP 监听

注意：优先级用于选择策略设置。

从CLI创建的策略具有最高优先级(128)，因此允许用户应用不同于编程策略中的策略设置。可以手动更改自定义策略下的所有可配置设置。

下一张图是SISF策略以及如何读取的示例：



在策略内部，在protocol关键字下，您可以选择查看用于填充SISF数据库的数据包类型：

<#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编程和客户端功能

下表中的功能在启用SISF时以编程方式启用，或作为SISF的客户端：

SISF编程功能	SISF客户端功能
VLAN上的LISP	Dot1x
VLAN上的EVPN	Web身份验证
DHCP 监听	CTS

如果在未配置启用SISF功能的设备上启用了SISF客户端功能，则必须在连接到主机的接口上配置自定义策略。

使用SISF信息的IPv4功能

- CTS
- IEEE 802.1x
- LISP

- EVPN
- DHCP监听（仅激活SISF，但不使用它）
- IP 源防护

使用SISF信息的IPv6功能

- IPv6路由器通告(RA)防护
- IPv6 DHCP保护，第2层DHCP中继
- IPv6重复地址检测(DAD)代理
- 泛洪抑制
- IPv6源防护
- IPv6目标防护
- RA扼杀器
- IPv6前缀防护

设备跟踪

设备跟踪的主要作用是跟踪网络中终端节点的存在、位置和移动。SISF监听交换机接收的流量，提取设备身份（MAC和IP地址），并将它们存储在绑定表中。 许多功能（如IEEE 802.1X、Web身份验证、Cisco TrustSec和LISP等）依赖于此信息的准确性才能正常运行。 基于SISF的设备跟踪支持IPv4和IPv6。 客户端可以通过五种受支持的方法学习IP：

- DHCPv4
- DHCPv6
- ARP
- NDP
- 数据收集

端口通道上的SISF

支持端口通道（或ether-channel）上的设备跟踪。但是，配置必须应用于信道组，而不是单个端口信道成员。从绑定角度来看，唯一显示（且已知）的接口是port-channel。

探测和数据库调整

探测：

- 在IPDT中，有一个命令通过将初始探测延迟为10秒来帮助解决重复地址问题：链路开启时“ip device tracking probe delay”。
- 在SISF中，已经内置了等待计时器，等待发送第一个探测。它不可配置，并且解决了相同的问题。由于此代码在SISF代码中，因此不再需要此命令

数据库：

在SISF中，您可以配置几个选项来控制条目在数据库中保留的时间：

```
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设备跟踪

轮询主机的条目的生命周期：

- SISF维护每个mac的IPv4/IPv6绑定，一旦IP学习成功，绑定将转换为可访问状态
- SISF通过监控控制包跟踪活动客户端
- 如果5分钟内没有来自客户端的控制数据包，绑定将转换为VERIFY状态并向客户端发送探测
- 如果客户端不响应探测，绑定将转换为STALE状态，否则为REACHABLE状态
- STALE条目的默认超时为24小时，并且可以配置
- 过时的条目将在24小时后（或配置的超时值）删除

盗窃检测

节点盗窃类型：

- IP盗窃（相同IP、不同MAC、不同/同一端口）
- MAC盗窃（相同MAC、不同IP、不同端口）
- MAC IP THEFT（相同MAC、相同IP、不同端口）

IP安全功能

以下是SISF相关的一些功能：

- NDP检查：检查IPv6 NDP消息
- NDP地址收集：使用通过监听NDP流量收集的信息填充绑定表
- 设备跟踪：监控终端设备活动，包括通过某些活动机制
- 监听：收集NDP、ARP和DHCP消息中的地址。阻止未授权的邮件
- DHCPv4中继：将DHCP广播的数据包中继到已配置的帮助地址。
- NDP和ARP组播抑制：通过转换为单播或代表目标响应来抑制组播NDP消息。
- DAD代理：重复地址检测和代表目标客户端发送NA
- DHCPv4要求：它强制客户端仅通过DHCP获取IP

SISF警告

观察到的一些与SISF相关的最常见行为包括：

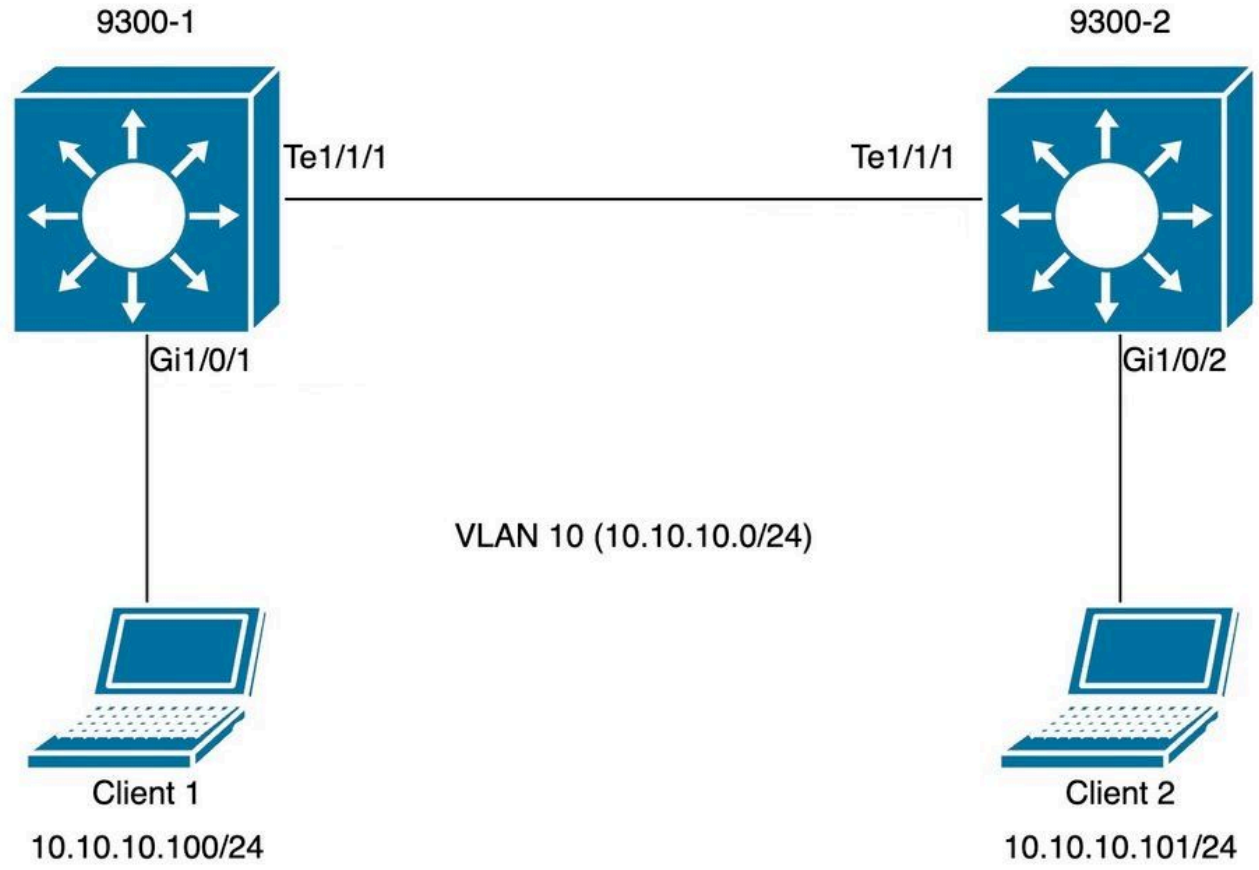
- 可通过启用其他功能（如dhcp监听）启用SISF
- SISF的默认探测行为可能影响客户端IP地址分配。
- 启用SISF后，上行链路端口上也会启用该功能，这可能会影响网络。

故障排除

拓扑

拓扑图用于下一个SISF场景。9300交换机仅属于第2层，在客户端Vlan 10中没有配置SVI。

注意：在本实验中手动启用SISF。



配置

在面向接入端口的两台9300交换机上设置默认SISF配置，而在中继端口上应用自定义策略来说明预期的SISF输出。

交换机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
```

交换机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
```

确认

您可以使用以下命令验证应用的策略：

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

交换机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#
```

交换机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#
```

常见情况

主机设备上的IPv4地址重复错误

问题

交换机发送的“keepalive”探测是L2检查。因此，从交换机的角度来看，ARP中用作源的IP地址并不重要：此功能可用于根本没有配置IP地址的设备，因此IP源0.0.0.0不相关。 当主机收到此消息时，它会回复并使用收到的数据包中唯一可用的IP地址（即自己的IP地址）填充目标IP字段。这可能会导致错误重复IP地址警报，因为作出回复的主机将自己的IP地址同时视为数据包的源和目标。

建议将SISF策略配置为对其keepalive探测使用自动源。

注意：有关详细信息，请参阅有关重复地址问题的本文

默认探测

这是不存在本地SVI和默认探测设置时的探测数据包：

<#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
```

解决方案

将探测配置为使用除主机PC以外的地址进行探测。这可以通过以下方法实现

“保持连接”探测的自动来源

为“keep-alive”探测功能配置一个自动源，以减少将0.0.0.0用作源IP的使用：

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

如果应用auto-source命令，逻辑工作如下：

```
<#root>

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

<-- Optional parameter
```

1. 将源设置为VLAN SVI（如果有）。
2. 在IP主机表中搜索同一子网的源/MAC对。 探测源自交换机物理接口MAC +数据库中已存在子

网中其他主机的IP。
3. 根据提供的主机位和掩码，从目标IP计算源IP。探测功能是通过侦听客户端IP并在配置有最后一位的子网中创建探测功能而生成的。

注意：如果命令与<override>一起应用，我们将始终跳到第3步。

已修改的探测

将auto-source fallback config设置为在子网中使用IP会修改探测。由于子网中没有SVI和其他客户端，因此我们返回到配置中配置的IP/掩码。

<#root>

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

这是修改的探测数据包：

<#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
```

有关探测行为的更多详细信息

命令	操作 （为了选择设备跟踪ARP探测的源IP和MAC地址）	备注
设备跟踪跟踪自动源	• 将源设置为VLAN SVI（如果存在）。 • 在来自同一子网的设备跟踪表中查找IP和MAC绑定。 • 使用0.0.0.0	我们建议禁用所有中继端口上的设备跟踪，以避免MAC抖动。
设备跟踪跟踪自动源覆盖	• 将源设置为VLAN SVI（如果存在） • 使用0.0.0.0	不建议在没有SVI时使用。
device-tracking tracking auto-source fallback <IP> <MASK>	• 将源设置为VLAN SVI（如果存在）。 • 在来自同一子网的设备跟踪表中查找IP和MAC绑定。 • 使用提供的主机位和掩码计算来自客户端IP的源IP。源MAC地址取自面向客户端的交换机端口的MAC地址。	我们建议禁用所有中继端口上的设备跟踪，以避免MAC抖动。 计算得出的IPv4地址不能分配给任何客户端或网络设备。
设备跟踪跟踪自动源回退<IP> <MASK>覆盖	• 将源设置为VLAN SVI（如果存在）。 • 使用提供的主机位和掩码计算来自客户端IP的源IP。源MAC地址取自面向客户端的交换机端口的MAC地址。	计算得出的IPv4地址不能分配给任何客户端或网络设备。

介绍device-tracking auto-source fallback <IP> <MASK> [override]命令：

根据主机ip，需要保留IPv4地址。

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

注意：这是一个布尔公式

示例。

如果我们使用命令：

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

主机IP = 10.152.140.25

IP = 0.0.0.1

掩码= 24

让我们将布尔公式分为两部分。

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

注意：用作IP源的地址必须从子网的DHCP绑定中划出。

重复IPv6地址错误

问题

在网络中启用IPv6并在VLAN上配置交换虚拟接口(SVI)时出现重复IPv6地址错误。

在普通IPv6 DAD数据包中，IPv6报头中的Source Address字段设置为未指定的地址(0:0：0:0：0:0：0:0)。类似于IPv4的情况。

在SISF探测功能中选择源地址的顺序为：

- SVI的本地链路地址（如果已配置）
- 使用0:0：0:0：0:0：0:0

解决方案

我们建议您向SVI配置添加以下命令。这使SVI能够自动获取本地链路地址；此地址用作SISF探测的源IP地址，从而防止重复IP地址问题。

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

内存和CPU利用率增加

问题

交换机发送的“keepalive”探测功能在以编程方式启用时从所有端口广播。 同一L2域中连接的交换机将这些广播发送给它们的主机，导致源交换机将远程主机添加到其设备跟踪数据库中。 额外的主机条目会增加设备的内存使用率，而添加远程主机的过程会增加设备的CPU利用率。

建议在连接到交换机的上行链路上配置策略，将端口定义为受信任端口并连接到交换机，从而确定编程策略的范围。

注意：请注意，SISF相关功能（如DHCP监听）使SISF能够正常工作，从而可能触发此问题。

解决方案

在上行链路（中继）上配置策略以停止探测和学习其他交换机上的远程主机(只需使用SISF来维护本地主机表)

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

```
 device-role switch
```

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

DT_trunk_policy

设备跟踪可达时间太短

问题

由于存在从IPDT到基于SISF的设备跟踪的迁移问题，从旧版本迁移到16.x及更高版本时，有时会引入非默认的可达时间。

解决方案

建议通过配置以下各项恢复到默认的可访问时间：

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

已注册到Meraki工具的交换机（CPU增加和端口刷新）

问题

当交换机连接到Meraki云监控工具时，此工具会推送自定义设备跟踪策略。

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

此策略将应用于所有接口，而不会有任何区别，也就是说，它不会区分面向其他网络设备（例如交换机、防火墙路由器等）的边缘端口和中继端口。交换机可以在配置了MERAKI_POLICY的中继端口上创建多个SISF条目，从而造成这些端口上的刷新以及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
```

解决方案

在所有非边缘接口上设置下一个策略：

```
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

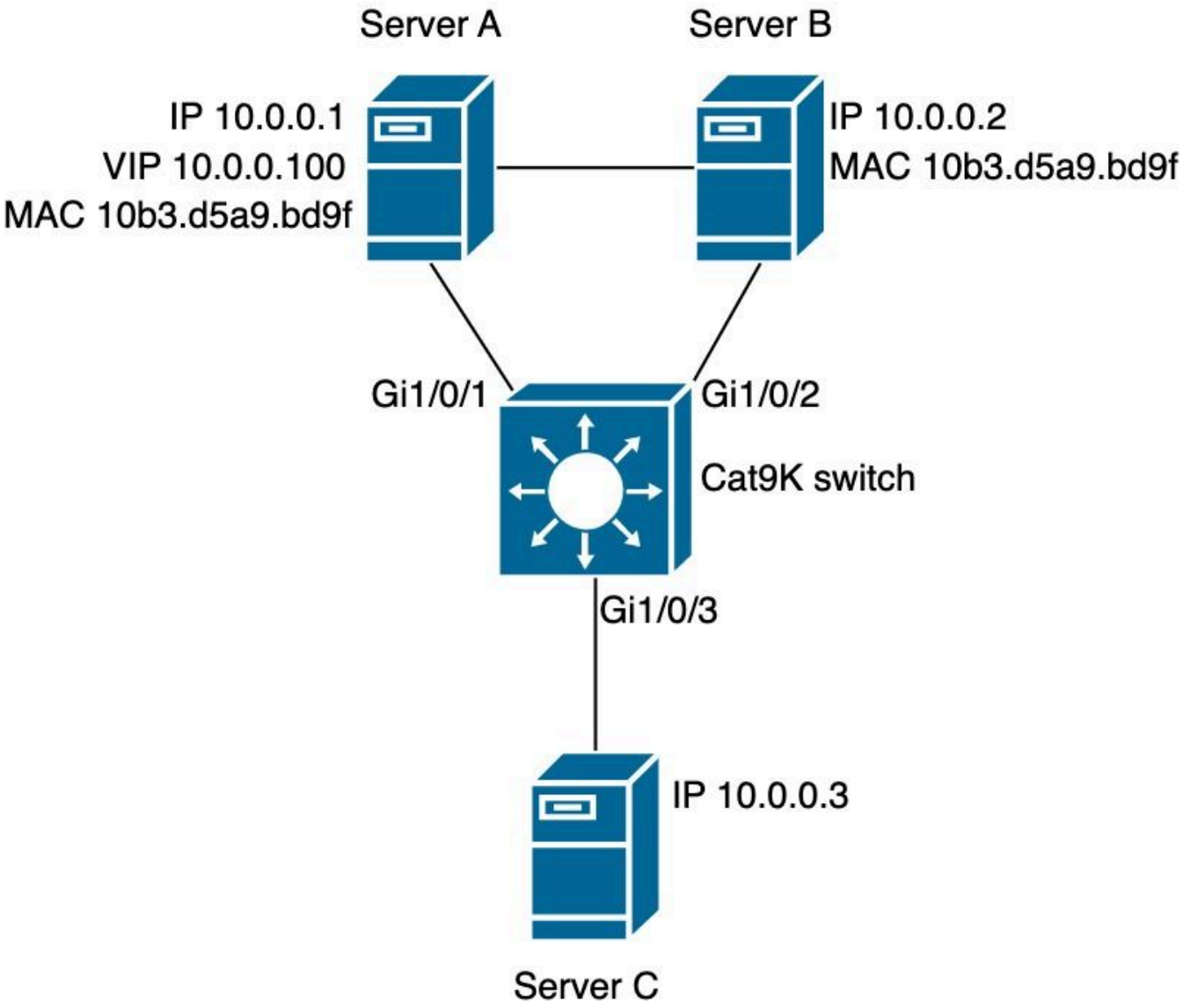
问题

此情况常见于HA（高可用性）模式中具有不同IP地址但共享相同MAC地址的设备。在共享相同条件（两个或多个IP地址的单个MAC地址）的VM环境中也可以观察到。当处于保护模式的自定义SISF策略时，此情况会阻止连接至所有在SISF表中没有条目的IP。根据SISF功能，每个MAC地址只能获知一个IP。

注意：此问题存在于17.7.1及后续版本中

示例：

- MAC地址为10b3.d5a9.bd9f的IP 10.0.0.1在SISF表上获知并允许与网络设备10.0.0.3通信。
- 但是，共享MAC地址10b3.d659.7858的第二个IP 10.0.0.2和虚拟IP 10.0.0.100未在SISF表中编程，并且不允许与网络通信。



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数据库

<#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
```

可达性测试服务器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
.....
```

可达性测试服务器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)
```

正在验证交换机上的丢包。

<#root>

```
switch(config)#
```

device-tracking logging

日志

<#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

解决方案

选项1：从端口删除IPDT策略允许ARP数据包和受影响的设备变为可访问

<#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

选项2：从设备跟踪策略中删除协议arp收集。

<#root>

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

no protocol arp

选项3：将IPDT_POLICY的安全级别更改为收集。

<#root>

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

security-level glean

相关信息

- 安全配置指南，Cisco IOS XE Bengaluru 17.6.x（Catalyst 9300交换机）：配置交换机集成安全功能
- 安全配置指南，Cisco IOS XE Cupertino 17.9.x（Catalyst 9300交换机）：配置交换机集成安全功能
- Cisco Catalyst 9000系列交换机集成安全功能(SISF)白皮书
- 思科漏洞ID CSCvx75602 - AR中继和ND抑制中的SISF内存泄漏
- 思科漏洞ID CSCwf33293 - [EVPN SISF]通过EVPN + DHCP修改IPv4/V6的限制地址值所需的自定义方法
- 思科漏洞ID CSCvq22011 - IOS-XE在IPDT从ARP收集数据时丢弃ARP应答
- 思科漏洞ID CSCwc20488 - 每个vlan/evi 255个伪端口限制
- 思科漏洞ID CSCwh52315 - 9300交换机在端口中具有IPDT策略时丢弃ARP应答
- 思科漏洞ID CSCvd51480 - Unbinding ip dhcp snooping and device-tracking

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。