Identificar e Solucionar Problemas do SISF nos Catalyst 9000 Series Switches

Contents

Introdução

Este documento descreve os Recursos de Segurança Integrada do Switch (SISF - Switch Integrated Security Features) usados nos Switches da Família Catalyst 9000. Ele também explica como o SISF pode ser usado e como interage com outros recursos.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Catalyst 9300-48P que executa o Cisco IOS® XE 17.3.x

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

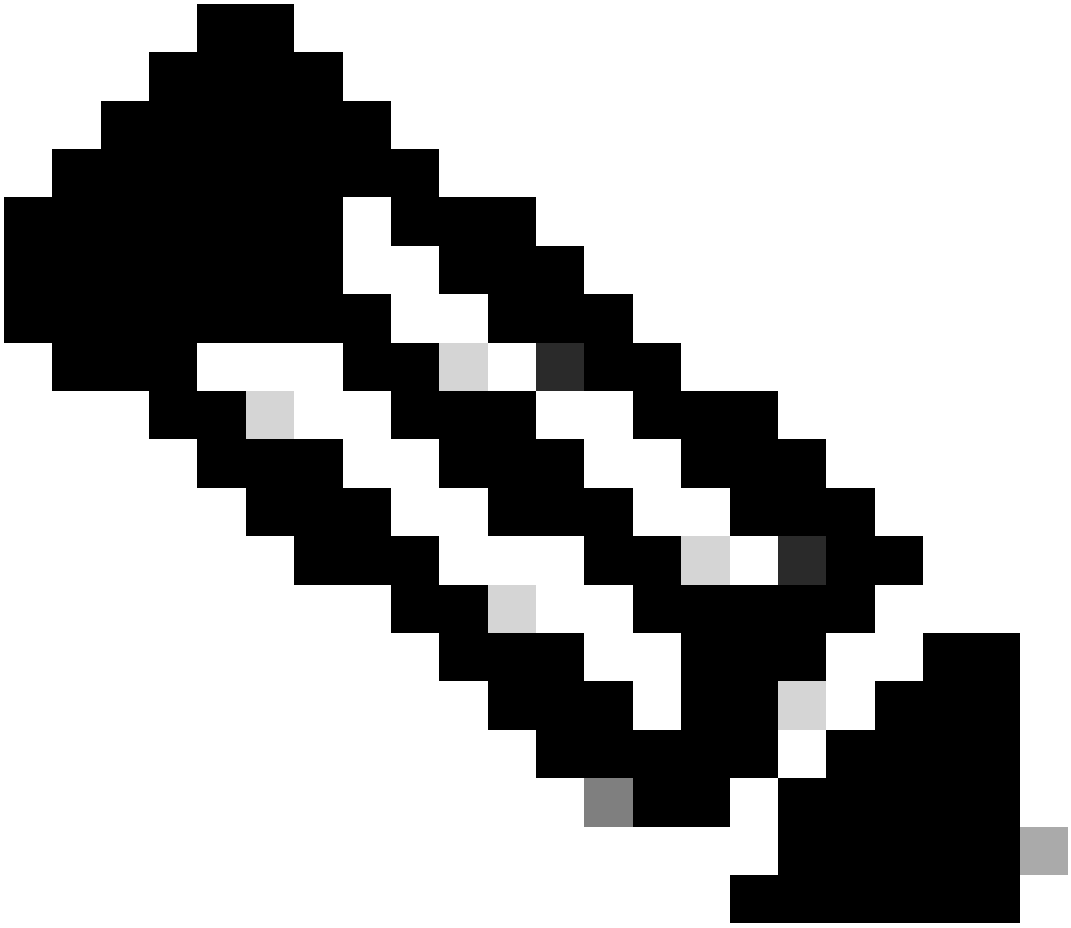
 Observação: consulte o guia de configuração apropriado para obter os comandos que são usados para habilitar esses recursos em outras plataformas Cisco.

Produtos Relacionados

Este documento também pode ser usado com as seguintes versões de hardware e software:

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

Com 17.3.4 e versões posteriores do software Cisco IOS XE



Observação: este documento também se aplica à maioria das versões do Cisco IOS XE que usam SISF versus Rastreamento de dispositivo.

Informações de Apoio

Overview

O SISF fornece uma tabela de vinculação de host e existem clientes de recursos que usam as informações dela. As entradas são preenchidas na tabela ao coletar pacotes como DHCP, ARP, ND, RA que rastreiam a atividade do host e ajudam a preencher dinamicamente a tabela. Se houver hosts silenciosos no domínio L2, as entradas estáticas podem ser usadas para adicionar entradas à tabela SISF.

O SISF usa um modelo de política para configurar funções de dispositivo e configurações adicionais no switch. Uma única política pode ser aplicada no nível da interface ou da VLAN. Se uma política for aplicada à VLAN e uma política diferente for aplicada à interface, a política da

interface terá precedência.

O SISF também pode ser usado para limitar o número de hosts na tabela, mas há diferenças entre o comportamento de IPv4 e IPv6. Se o limite SISF for definido e for atingido:

- Os hosts IPv4 continuam a operar, mas nenhuma outra entrada acima do limite deve ser adicionada à tabela SISF
- Os hosts IPv6 que não chegarem à tabela SISF não poderão entrar na rede e nenhuma entrada nova será adicionada à tabela SISF.

A partir da versão 16.9.x e mais recente é introduzida uma prioridade de recurso de cliente SISF. Ele adiciona opções para controlar as atualizações no SISF e, se dois ou mais clientes estiverem usando a tabela de vinculação, as atualizações do recurso de prioridade mais alta serão aplicadas. As exceções aqui são as configurações de "contagem de endereços limite para IPv4/IPv6 por mac", as configurações da política com a prioridade mais baixa são efetivas.

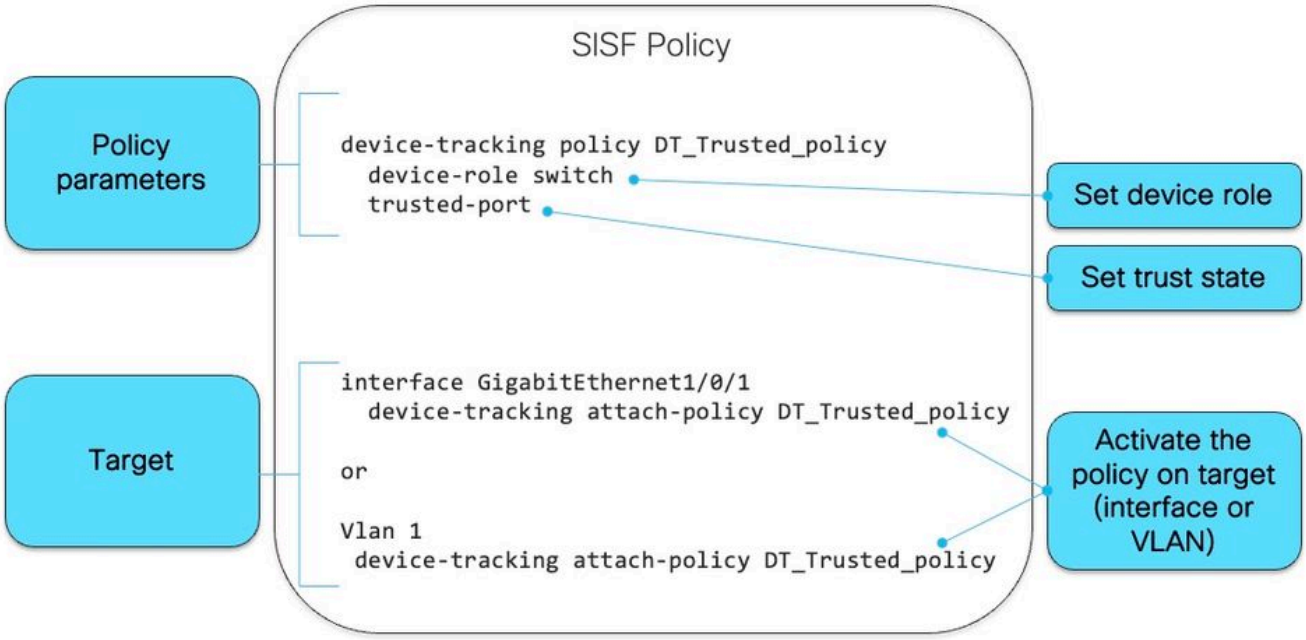
Alguns recursos de exemplo que exigem que o controle de dispositivos esteja habilitado são:

- LISP/EVPN
- Ponto1x
- Autenticação da Web
- CTS
- Rastreamento de DHCP

Observação: a prioridade é usada para selecionar configurações de política.

A política criada a partir do CLI tem a prioridade mais alta (128), permitindo, portanto, que os usuários apliquem uma configuração de política diferente daquela nas políticas programáticas. Todas as configurações configuráveis na política personalizada podem ser alteradas manualmente.

A próxima imagem é um exemplo de uma política SISF e como lê-la:



Dentro da política, sob a palavra-chave protocol, você tem a opção de ver que tipos de pacotes são usados para preencher o banco de dados SISF:

<#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 Programática e Recursos do Cliente

Os recursos na próxima tabela ativam o SISF programaticamente quando estão ativados ou atuam como clientes para o SISF:

Recurso programático SISF	Recursos do cliente SISF
LISP na VLAN	Ponto1x
EVPN em VLAN	Autenticação da Web
Rastreamento de DHCP	CTS

Se um recurso de cliente SISF estiver habilitado em um dispositivo configurado sem um recurso que habilite o SISF, uma política personalizada deverá ser configurada nas interfaces que se conectam aos hosts.

Recursos IPv4 que consomem informações SISF

- CTS
- IEEE 802,1x
- LISP
- EVPN
- Rastreamento de DHCP (só ativa o SISF, mas não o usa)
- Proteção de origem de IP

Recursos IPv6 que consomem informações SISF

- Proteção de anúncio de roteador (RA) IPv6
- IPv6 DHCP Guard, retransmissão de DHCP da camada 2
- Proxy de detecção de endereço duplicado (DAD) IPv6
- Supressão de Inundação
- Proteção de origem IPv6
- Proteção de destino IPv6
- Acelerador de RA
- Proteção de prefixo IPv6

Rastreamento de dispositivo

A principal função do rastreamento de dispositivos é rastrear a presença, o local e o movimento dos nós finais na rede. O SISF rastreia o tráfego recebido pelo switch, extrai a identidade do dispositivo (endereço MAC e IP) e os armazena em uma tabela de vinculação. Muitos recursos, como IEEE 802.1X, autenticação da Web, Cisco TrustSec e LISP, entre outros, dependem da precisão dessas informações para funcionar corretamente. O rastreamento de dispositivo baseado em SISF suporta IPv4 e IPv6. Há cinco métodos suportados pelos quais o cliente pode aprender o IP:

- DHCPv4
- DHCPv6
- ARP
- NDP
- Coleta de dados

SISF em um canal de porta

O rastreamento de dispositivo no canal de porta (ou canal de ether) é suportado. Mas a configuração deve ser aplicada no grupo de canais, não nos membros individuais do port channel. A única interface que aparece (e é conhecida) do ponto de vista da ligação é o canal de porta.

Teste e ajuste de banco de dados

Sonda:

- No IPDT, havia um comando para ajudar com problemas de endereço duplicado, atrasando o teste inicial por 10 segundos: "ip device tracking probe delay" no link ativo.
- No SISF já existe um temporizador de espera incorporado que aguarda antes de enviar a primeira prova. Ele não é configurável e resolve o mesmo problema. Como isso está no código SISF, não há mais necessidade desse comando

Banco de dados:

No SISF, você pode configurar algumas opções para controlar por quanto tempo uma entrada é mantida no banco de dados:

<#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)

Rastreamento de dispositivo IP

Ciclo de vida de uma entrada em que o host é interrogado:

- O SISF mantém a ligação IPv4/IPv6 por mac, assim que o IP aprende é bem-sucedido, as transições de ligação para o estado ACESSÍVEL
- O SISF rastreia o cliente de vida monitorando o pacote de controle
- Se não houver um pacote de controle do cliente por 5 minutos, a vinculação passará para o estado VERIFY e enviará a sonda ao cliente
- Se os clientes não responderem à sonda, a vinculação passará para o estado STALE ou para o estado REACHABLE
- O tempo limite padrão para entrada STALE é de 24 horas e configurável
- Entradas STALE são excluídas após 24 horas (ou valor de tempo limite configurado)

Detecção de roubo

Tipos de roubo de nós:

- Roubo de IP (mesmo IP, MAC diferente, porta diferente/mesma)
- ROUBO DE MAC (mesmo MAC, IP diferente, porta diferente)
- ROUBO DE IP MAC (mesmo mac, mesmo ip, porta diferente)

Recursos de segurança IP

Estes são alguns dos recursos dependentes do SISF:

- Inspeção de NDP: inspecionar mensagens de NDP IPv6
- limpeza de endereço NDP:preencha a tabela de ligação com informações coletadas ao rastrear o tráfego NDP
- Rastreamento de dispositivos: monitora a atividade do dispositivo final, inclusive por meio de algum mecanismo de vida
- Rastreamento: obtém endereços em mensagens NDP, ARP e DHCP. Bloquear mensagens não autorizadas
- Retransmissão DHCPv4: retransmite o pacote de transmissão DHCP para o endereço auxiliar configurado.
- Supressão de multicast NDP e ARP: Suprima mensagens NDP de multicast convertendo em unicast para responder em nome de destinos.
- Proxy DAD:Detecção de endereço duplicado e envio de NA em nome do cliente de destino
- Exigência de DHCPv4: ele impõe que o cliente obtenha o IP somente por DHCP

Avisos SISF

Alguns dos comportamentos mais frequentes observados em relação ao SISF são:

- O SISF pode ser habilitado habilitando outros recursos, como rastreamento de dhcp
- O comportamento de investigação padrão do SISF pode afetar a atribuição de endereço IP do cliente.

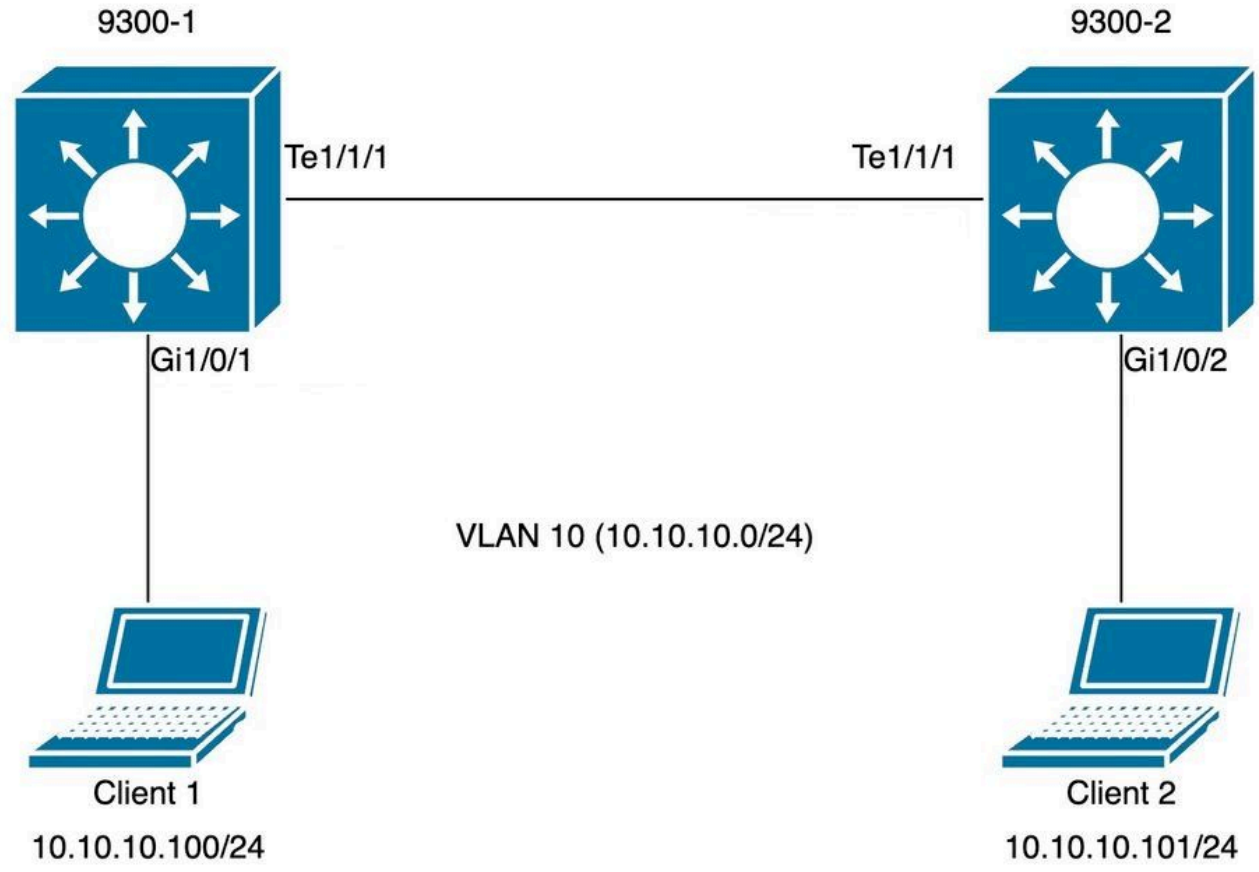
- Quando o SISF está habilitado, ele também é habilitado em portas de uplink que podem causar impacto na rede.

Troubleshooting

Topologia

O diagrama de topologia é usado no próximo cenário SISF. Os switches 9300 são apenas da camada 2 e NÃO têm o SVI configurado na VLAN 10 do cliente.

Observação: o SISF é ativado manualmente neste laboratório.



Configuração

A configuração SISF padrão foi definida em ambos os switches 9300 voltados para as portas de acesso, enquanto a política personalizada foi aplicada às portas de tronco para ilustrar as saídas SISF esperadas.

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
```

Verificação

Você pode usar estes comandos para validar as políticas aplicadas:

```
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#
```

Cenários comuns

Erro de Endereço IPv4 Duplicado no Dispositivo Host

Problema

O teste "keepalive" enviado pelo switch é uma verificação L2. Dessa forma, do ponto de vista do switch, os endereços IP usados como origem nos ARPs não são importantes: esse recurso pode ser usado em dispositivos sem nenhum endereço IP configurado, portanto a origem IP de 0.0.0.0 não é relevante. Quando o host recebe essas mensagens, ele responde e preenche o campo IP de destino com o único endereço IP disponível no pacote recebido, que é seu próprio endereço IP. Isso pode causar alertas falsos de endereço IP duplicado, pois o host que responde vê seu próprio endereço IP como a origem e o destino do pacote.

É recomendável configurar a política SISF para usar uma fonte automática para seus testes de keepalive.

Observação: consulte este artigo sobre problemas de endereço duplicado para obter mais informações

---

Sonda padrão

Este é o pacote de teste quando não há SVI local presente e configurações de teste padrão:

<#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
```

Solução

Configure a sonda para usar um endereço diferente do PC host para a sonda. Isso pode ser feito por esses métodos

Origem automática para sonda "Keep-Alive"

Configure uma fonte automática para os testes "keep-alive" para reduzir o uso de 0.0.0.0 como o IP de origem:

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

A lógica se aplicar o comando autosource funciona da seguinte maneira:

<#root>

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

<-- Optional parameter

1. Defina a origem como VLAN SVI, se houver.
2. Procure um par origem/MAC na tabela de hosts IP para a mesma sub-rede. A sonda foi originada do MAC da interface física do switch + o IP de algum outro host na sub-rede que já está no banco de dados.
3. Calcule o IP de origem a partir do IP de destino com o bit e a máscara de host fornecidos. A sonda é gerada a partir da escuta do IP do cliente e da criação de uma sonda na sub-rede com os últimos bits configurados.

Observação: se o comando for aplicado com <override>, sempre vamos para a etapa 3.

Sonda modificada

A definição de configuração de fallback de origem automática para usar um IP na sub-rede modifica a sonda. Como não há SVI e nenhum outro cliente na sub-rede, retornamos ao IP/Máscara configurado na configuração.

<#root>

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

Este é o pacote de teste modificado:

<#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
```

Mais detalhes sobre o comportamento da sonda

Comando	Ação (Para selecionar o endereço IP e MAC de origem para o dispositivo que monitora a sonda ARP)	Notas
origem automática de rastreamento de dispositivo	• Defina a origem como VLAN SVI, se houver. • Procure a associação IP e MAC na tabela de rastreamento de dispositivo da mesma sub-rede. • Usar 0.0.0.0	Recomendamos que você desabilite o rastreamento de dispositivo em todas as portas de tronco para evitar a oscilação de MAC.
substituição de origem automática de rastreamento de dispositivo	• Defina a origem como VLAN SVI, se houver • Usar 0.0.0.0	Não recomendado quando não há SVI.
rastreamento de dispositivo fallback de origem automática <IP> <MASK>	• Defina a origem como VLAN SVI, se houver. • Procure a associação IP e MAC na tabela de rastreamento de	Recomendamos que você desabilite o rastreamento de dispositivo em todas as portas de tronco para evitar a oscilação de MAC.

	dispositivo da mesma sub-rede. • Calcular o IP de origem do IP do cliente usando o bit de host e a máscara fornecidos. O MAC de origem é obtido do endereço MAC da porta do switch voltada para o cliente.	O endereço IPv4 calculado não deve ser atribuído a nenhum cliente ou dispositivo de rede.
device-tracking autossource fallback <IP> <MASK> override	• Defina a origem como VLAN SVI, se houver. • Calcular o IP de origem do IP do cliente usando o bit de host e a máscara fornecidos. O MAC de origem é obtido do endereço MAC da porta do switch voltada para o cliente.	O endereço IPv4 calculado não deve ser atribuído a nenhum cliente ou dispositivo de rede.

Explicação do comando device-tracking autossource fallback <IP> <MASK> [override]:

Dependendo do IP do host, um endereço IPv4 precisa ser reservado.

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

Observação: esta é uma fórmula booleana

Exemplo.

Se usarmos o comando:

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

IP do host = 10.152.140.25

IP = 0.0.0.1

máscara = 24

Vamos quebrar a fórmula booleana em duas partes.

1. Operação 10.152.140.25 E 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. Operação 10.152.140.0 OU 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
```

IP reservado = 10.152.140.1

IP Reservado = (10.152.140.25 & 255.255.255.0) | (0.0.0.1) = 10.152.140.1

Observação: o endereço usado como origem de IP deve ter o escopo das associações DHCP para a sub-rede.

Erro de Endereço IPv6 Duplicado

Problema

Erro de endereço IPv6 duplicado quando o IPv6 está habilitado na rede e uma interface virtual comutada (SVI) está configurada em uma VLAN.

Em um pacote DAD IPv6 normal, o campo Endereço de origem no cabeçalho IPv6 é definido como o endereço não especificado (0:0:0:0:0:0:0:0). Semelhante ao caso IPv4.

A ordem para escolher o endereço de origem na sonda SISF é:

- Endereço de link local do SVI, se configurado
- Usar 0:0:0:0:0:0:0:0

Solução

Recomendamos que você adicione os próximos comandos à configuração do SVI. Isso permite

que o SVI adquira um endereço de link local automaticamente; esse endereço é usado como o endereço IP origem da prova SISF, evitando, assim, o problema de endereço IP duplicado.

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

Maior utilização de memória e CPU

Problema

O teste "keepalive" enviado pelo switch é transmitido para todas as portas quando é ativado programaticamente. Os switches conectados no mesmo domínio L2 enviam esses broadcasts para seus hosts, resultando no switch de origem adicionando hosts remotos ao seu banco de dados de rastreamento de dispositivo. As entradas adicionais do host aumentam o uso de memória no dispositivo e o processo de adição dos hosts remotos aumenta a utilização da CPU do dispositivo.

Recomenda-se definir o escopo da política programática configurando uma política no uplink para switches conectados para definir a porta como confiável e conectada a um switch.

Observação: lembre-se de que os recursos dependentes de SISF, como rastreamento de DHCP, permitem que o SISF funcione corretamente, o que pode disparar esse problema.

Solução

Configurar uma política no uplink (tronco) para interromper as sondas e o aprendizado de hosts remotos que amam em outros switches (o SISF é necessário apenas para manter a tabela de hosts local)

<#root>

```
device-tracking policy DT_trunk_policy
```

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

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

DT_trunk_policy

Tempo Acessível de Rastreamento de Dispositivo Muito Curto

Problema

Devido a um problema de migração do IPDT para o rastreamento de dispositivo baseado em SISF, um tempo não padrão acessível às vezes é introduzido ao migrar de versões mais antigas para 16.x e versões mais recentes.

Solução

É recomendável reverter para o horário acessível padrão configurando:

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

Switches integrados à ferramenta Meraki (aumento da CPU e liberações de porta)

Problema

Quando os switches são integrados à ferramenta de monitoramento de nuvem da Meraki, essa ferramenta aplica políticas personalizadas de rastreamento de dispositivos.

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

A política é aplicada a todas as interfaces sem distinção, ou seja, ela não distingue entre portas de borda e portas de tronco que enfrentam outros dispositivos de rede (por exemplo, switches, firewalls, roteadores e assim por diante). O switch pode criar várias entradas SISF em portas de tronco onde MERAKI_POLICY está configurado, causando, portanto, liberações nessas portas, bem como o aumento do uso da CPU.

<#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
```

Solução

Configure a próxima política em todas as interfaces sem borda:

```
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
```

Endereços IP com o Mesmo MAC Fora da Tabela SISF

Problema

Esse cenário é comum em dispositivos no modo HA (alta disponibilidade) que têm endereços IP diferentes, mas compartilham o mesmo endereço MAC. Também é observado em ambientes VM que compartilham a mesma condição (endereço MAC único para dois ou mais endereços IP). Essa condição impede a conectividade de rede para todos os IPs que não têm uma entrada na tabela SISF quando a política SISF personalizada no modo de proteção está em vigor.De acordo com o recurso SISF, apenas um IP é aprendido por endereço MAC.

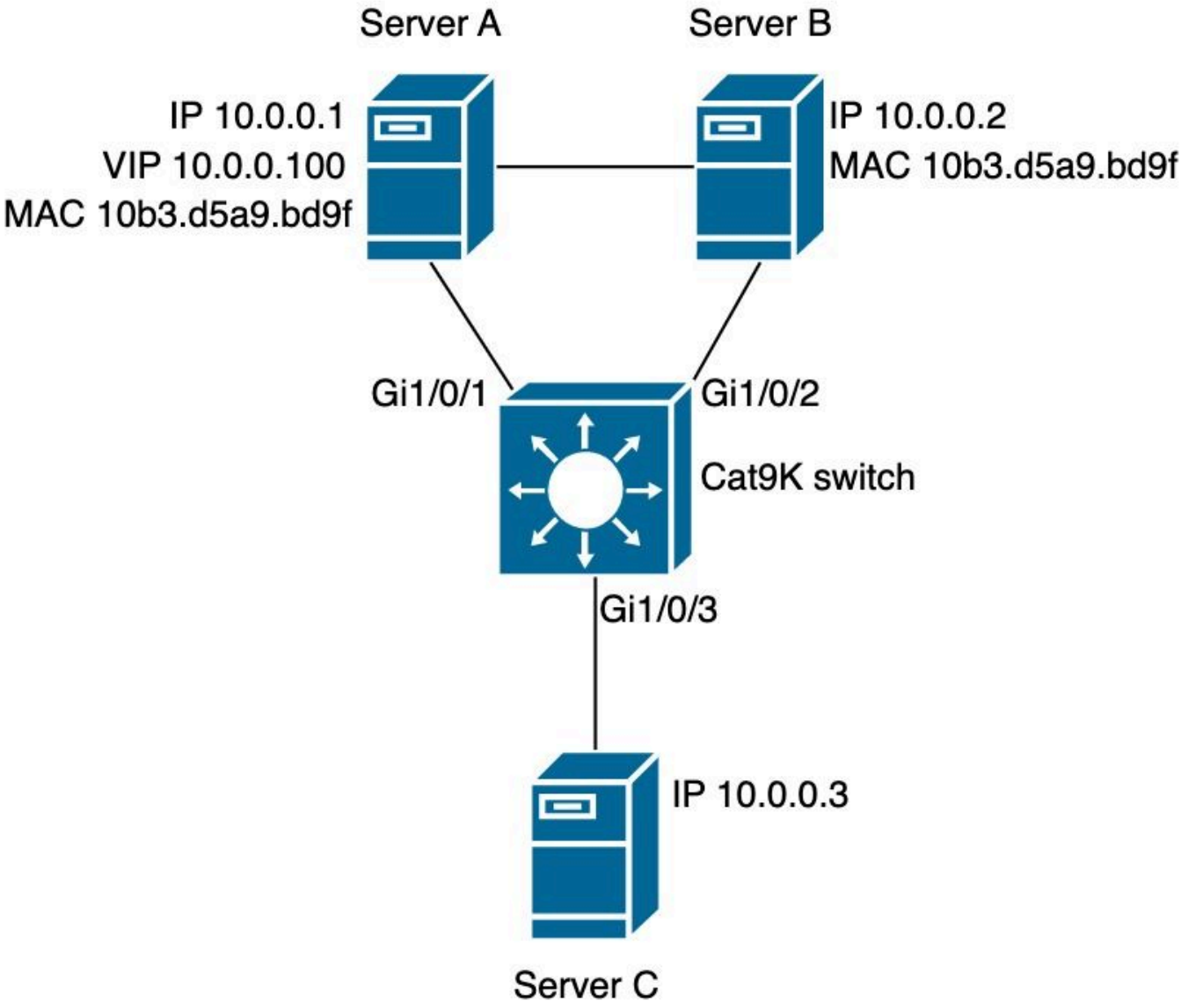
Observação: esse problema está presente nas versões 17.7.1 e posteriores

---

Exemplo:

- O IP 10.0.0.1 com endereço MAC 10b3.d5a9.bd9f é aprendido na tabela SISF e tem permissão para se comunicar com o dispositivo de rede 10.0.0.3.

- No entanto, o segundo IP 10.0.0.2 e o IP virtual 10.0.0.100 que compartilham o endereço MAC 10b3.d659.7858 não são programados na tabela SISF e a comunicação com a rede não é permitida.



política SISF

<#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
```

Banco de dados SISF

<#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
```

Teste de acessibilidade Servidor 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
.....
```

Teste de acessibilidade Servidor 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)
```

Validando quedas no switch.

<#root>

```
switch(config)#
```

device-tracking logging

Logs

<#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

Solução

Opção 1: Remover a política IPDT da porta permite que os pacotes ARP e os dispositivos afetados se tornem alcançáveis

<#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

Opção 2: Remova o protocolo arp da política de controle de dispositivos.

<#root>

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

no protocol arp

Opção 3: Altere o nível de segurança de IPDT_POLICY para glean.

<#root>

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

security-level glean

Informações Relacionadas

- Guia de configuração de segurança, Cisco IOS XE Bengaluru 17.6.x (Catalyst 9300 Switches): Configurando recursos de segurança integrados do switch
- Guia de configuração de segurança, Cisco IOS XE Cupertino 17.9.x (Catalyst 9300 Switches): Configurando recursos de segurança integrados do switch
- White paper sobre os recursos de segurança integrada (SISF) do switch da família Cisco Catalyst 9000
- ID de bug Cisco CSCvx75602 - Vazamento de memória SISF em retransmissão AR e supressão ND
- ID de bug Cisco CSCwf3293 - [EVPN SISF] Método personalizado necessário para modificar os valores de endereço limite para IPv4/V6 com EVPN + DHCP
- ID de bug da Cisco CSCvq22011 - IOS-XE descarta resposta ARP quando IPDT obtém do ARP
- ID de bug da Cisco CSCwc20488 - limitação de 255 pseudo-portas por vlan/evi
- ID de bug Cisco CSCwh52315 - Switch 9300 descarta resposta ARP quando tem uma política IPDT na porta
- ID de bug Cisco CSCvd51480 - Desligando rastreamento de dhcp de ip e rastreamento de dispositivo

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.