

Solución de problemas de SISF en switches Catalyst serie 9000

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Productos Relacionados](#)

[Antecedentes](#)

[Overview](#)

[Funciones programáticas y de cliente de SISF](#)

[Funciones de IPv4 que consumen información de SISF](#)

[Funciones de IPv6 que consumen información de SISF](#)

[Seguimiento de dispositivos](#)

[SISF en un canal de puerto](#)

[Sondeo y ajuste de base de datos](#)

[Seguimiento de dispositivos IP](#)

[Detección de robos](#)

[Funciones de seguridad IP](#)

[Advertencias de SISF](#)

[Troubleshoot](#)

[Topología](#)

[Configuración](#)

[Verificación](#)

[Escenarios de ejemplo](#)

[Error de dirección IPv4 duplicada en el dispositivo host](#)

[Error de dirección IPv6 duplicada](#)

[Mayor uso de memoria y CPU](#)

[Tiempo de seguimiento de dispositivos alcanzable demasiado corto](#)

[Switches incorporados a la herramienta Meraki \(aumento de CPU y vaciado de puertos\)](#)

[Direcciones IP con el mismo MAC No están en la Tabla SISF](#)

[Información Relacionada](#)

Introducción

Este documento describe las Funciones de seguridad integrada del switch (SISF) utilizadas en los switches de la familia Catalyst 9000. También explica cómo se puede utilizar SISF y cómo interactúa con otras funciones.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Catalyst 9300-48P que ejecuta Cisco IOS® XE 17.3.x

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.



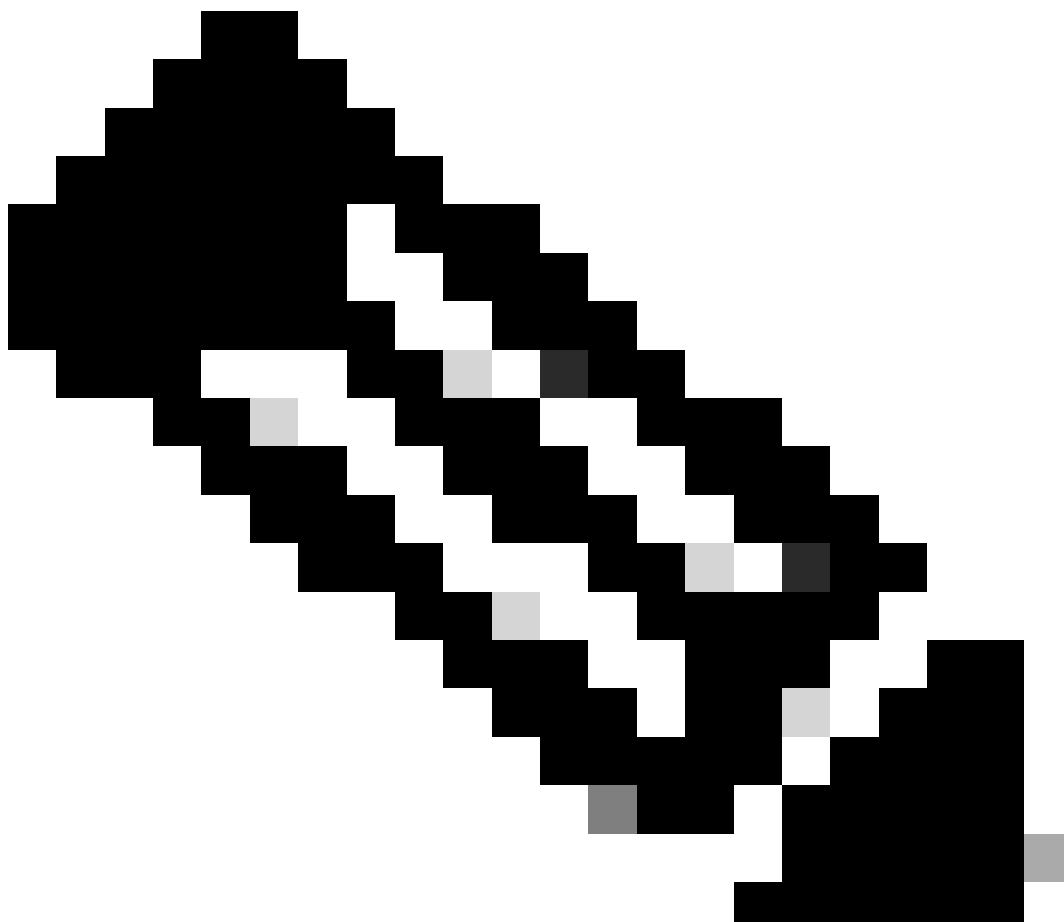
Nota: Consulte la guía de configuración adecuada para conocer los comandos que se utilizan para habilitar estas funciones en otras plataformas de Cisco.

Productos Relacionados

Este documento también puede utilizarse con estas versiones de software y hardware:

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

Con las versiones 17.3.4 y posteriores del software Cisco IOS XE



Nota: Este documento también se aplica a la mayoría de las versiones de Cisco IOS XE que utilizan SISF frente a Device Tracking.

Antecedentes

Overview

SISF proporciona una tabla de enlace de host, y hay clientes de función que utilizan la información de la misma. Las entradas se rellenan en la tabla mediante la recopilación de paquetes como DHCP, ARP, ND, RA que realizan un seguimiento de la actividad del host y ayudan a rellenar dinámicamente la tabla. Si hay hosts silenciosos en el dominio L2, las entradas estáticas se pueden utilizar para agregar entradas en la tabla SISF.

SISF utiliza un modelo de políticas para configurar los roles de los dispositivos y los ajustes adicionales en el switch. Se puede aplicar una sola política en el nivel de interfaz o de VLAN. Si se aplica una política en la VLAN y se aplica una política diferente en la interfaz, la política de la

interfaz tiene prioridad.

SISF también se puede utilizar para limitar el número de hosts en la tabla, pero hay diferencias entre el comportamiento de IPv4 e IPv6. Si se establece el límite SISF y se alcanza:

- Los hosts IPv4 continúan funcionando pero no se deben agregar más entradas sobre el límite a la tabla SISF
- Los hosts IPv6 que no entran en la tabla SISF no pueden entrar en la red y no se deben agregar nuevas entradas a la tabla SISF.

A partir de la versión 16.9.x y posterior se introduce una prioridad de función de cliente SISF. Agrega opciones para controlar las actualizaciones en SISF y si dos o más clientes están utilizando la tabla de enlace, se aplican las actualizaciones de la función de mayor prioridad. Las excepciones aquí son la configuración "limit address-count for IPv4/IPv6 per mac", la configuración de la política con la prioridad más baja es efectiva.

Algunas funciones de ejemplo que requieren que se habilite el seguimiento de dispositivos son:

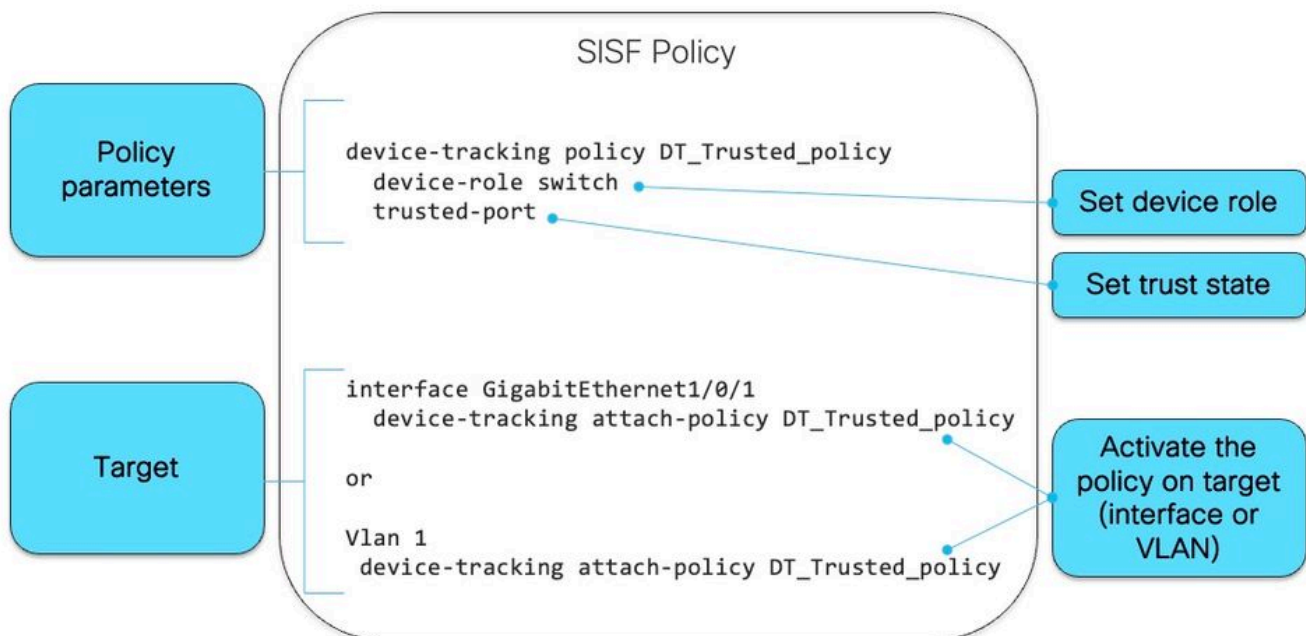
- LISP/EVPN
- Punto1x
- Autenticación web
- CTS
- Snooping DHCP



Nota: La prioridad se utiliza para seleccionar la configuración de directivas.

La directiva creada a partir de CLI tiene la prioridad más alta (128), lo que permite a los usuarios aplicar una configuración de directiva diferente de la de las directivas de programación. Todos los parámetros configurables de la directiva personalizada se pueden cambiar manualmente.

La siguiente imagen es un ejemplo de una política SISF y cómo leerla:



Dentro de la política, bajo palabra clave protocol, tiene la opción de ver qué tipo de paquetes se utilizan para llenar la base de datos 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

Funciones programáticas y de cliente de SISF

Las funciones de la siguiente tabla habilitan SISF mediante programación cuando están habilitadas o actúan como clientes de SISF:

Función programática de SISF	Características del cliente SISF
LISP en VLAN	Punto1x
EVPN en VLAN	Autenticación web
Snooping DHCP	CTS

Si se habilita una función de cliente SISF en un dispositivo configurado sin una función que habilita SISF, se debe configurar una política personalizada en las interfaces que se conectan a los hosts.

Funciones de IPv4 que consumen información de SISF

- CTS
- IEEE 802.1x
- LISP
- EVPN
- Snooping DHCP (sólo activa el SISF pero no lo utiliza)
- IP Source Guard

Funciones de IPv6 que consumen información de SISF

- Protección de anuncio de router IPv6 (RA)
- Protección DHCP IPv6, retransmisión DHCP de capa 2
- Proxy de detección de direcciones duplicadas (DAD) IPv6
- Supresión de inundaciones
- Protector de origen IPv6
- Protección de destino IPv6
- Regulador RA
- Protección de prefijo IPv6

Seguimiento de dispositivos

La función principal del seguimiento de dispositivos es realizar un seguimiento de la presencia, la ubicación y el movimiento de los nodos extremos en la red. SISF detecta el tráfico recibido por el switch, extrae la identidad del dispositivo (dirección MAC e IP) y los almacena en una tabla de enlace. Muchas funciones, como IEEE 802.1X, autenticación web, Cisco TrustSec y LISP, entre otras, dependen de la precisión de esta información para funcionar correctamente. El seguimiento de dispositivos basado en SISF admite tanto IPv4 como IPv6. Hay cinco métodos admitidos por los cuales el cliente puede aprender IP:

- DHCPv4
- DHCPv6
- ARP
- NDP
- Recopilación de datos

SISF en un canal de puerto

Se admite el seguimiento de dispositivos en el canal de puerto (o en el canal Ether). Pero la configuración debe aplicarse en el grupo de canal, no en los miembros individuales del canal de puerto. La única interfaz que aparece (y que se conoce) desde el punto de vista de enlace es el canal de puerto.

Sondeo y ajuste de base de datos

Sondeo:

- En IPDT había un comando para ayudar con los problemas de dirección duplicada retrasando la sonda inicial por 10 segundos: "ip device tracking probe delay" upon link up.
- En SISF ya hay un temporizador de espera incorporado que espera antes de enviar la primera sonda. No se puede configurar y resuelve el mismo problema. Dado que esto está en el código SISF, ya no hay necesidad de este comando

Base de datos:

En SISF puede configurar algunas opciones para controlar cuánto tiempo se mantiene una entrada en la base de datos:

```
<#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)
```

Seguimiento de dispositivos IP

Ciclo de vida de una entrada en la que se sondea el host:

- SISF mantiene el enlace IPv4/IPv6 por mac, una vez que el aprendizaje de IP es exitoso, vinculando las transiciones al estado REACHABLE
- SISF realiza un seguimiento del cliente de actividad supervisando el paquete de control
- Si no hay ningún paquete de control del cliente durante 5 minutos, el enlace pasa al estado VERIFY y envía la sonda al cliente
- Si los clientes no responden a la sonda, el enlace pasa al estado STALE o al estado REACHABLE
- El tiempo de espera predeterminado para la entrada STALE es de 24 horas y configurable
- Las entradas OBSOLETAS se eliminan después de 24 horas (o se configura el valor del tiempo de espera)

Detección de robos

Tipos de robos de nodos:

- Robo de IP (misma IP, MAC diferente, diferente/mismo puerto)
- ROBO DE MAC (mismo MAC, IP diferente, puerto diferente)
- MAC IP THEFT (mismo MAC, misma IP, puerto diferente)

Funciones de seguridad IP

Estas son algunas de las funciones dependientes de SISF:

- Inspección NDP: Inspeccionar mensajes NDP IPv6
- Detección de direcciones NDP: llene la tabla de enlace con información obtenida mediante el sondeo del tráfico NDP
- Seguimiento de dispositivos: supervise la actividad del dispositivo final, incluso a través de algún mecanismo activo.
- Snooping: recopila direcciones en los mensajes NDP, ARP y DHCP. Bloquear mensajes no autorizados
- Retransmisión DHCPv4: retransmite el paquete transmitido por DHCP a la dirección del ayudante configurada.
- Supresión de multidifusión NDP y ARP: suprime los mensajes NDP de multidifusión mediante la conversión a unidifusión para responder en nombre de los destinos.
- proxy DAD: detección de direcciones duplicadas y envío de un nombre NA del cliente de destino
- Requisito DHCPv4: Exige al cliente que obtenga la dirección IP únicamente mediante DHCP

Advertencias de SISF

Algunos de los comportamientos más frecuentes observados en relación con la FSI son:


- SISF se puede habilitar habilitando otras características como la indagación DHCP

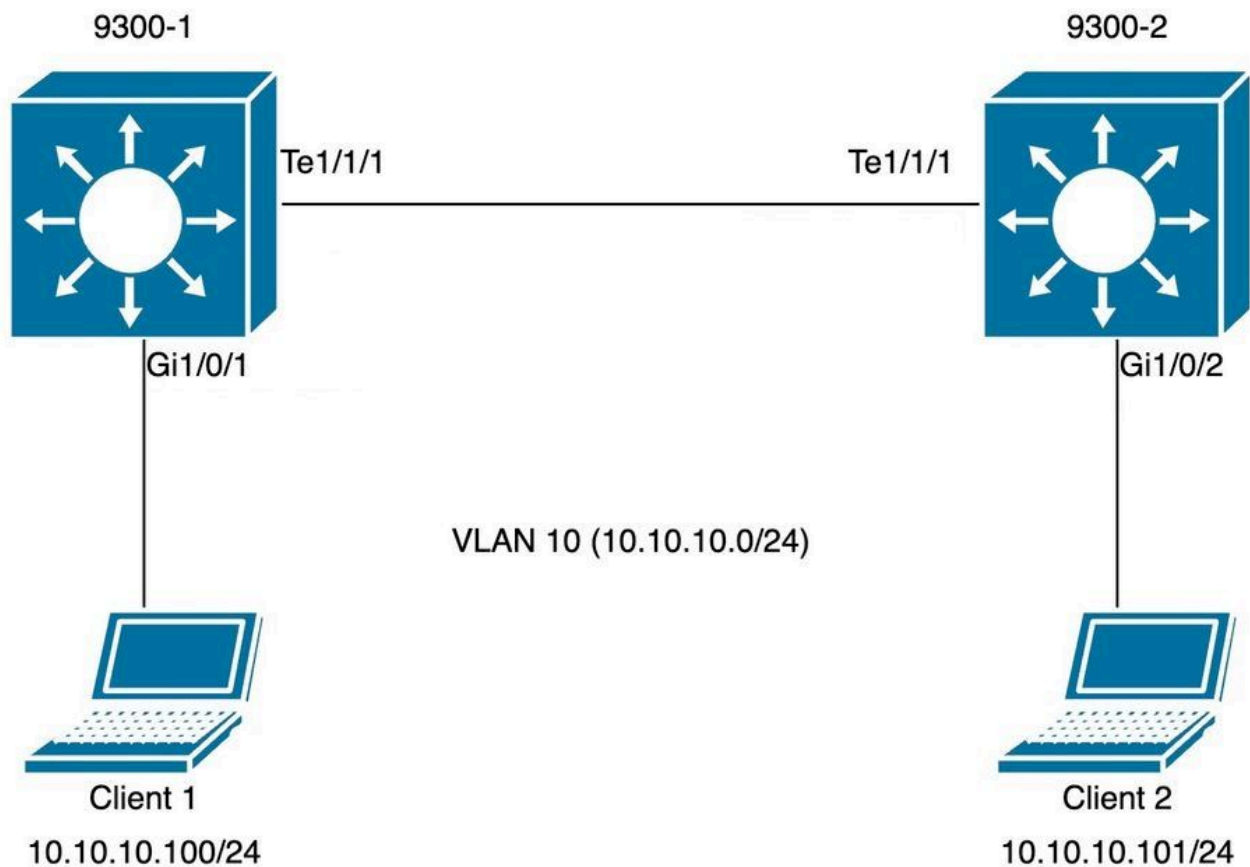
- El comportamiento de sondeo predeterminado de SISF puede afectar a la asignación de la dirección IP del cliente.
- Cuando se habilita SISF, también se habilita en los puertos de link ascendente que pueden causar impacto en la red.

Troubleshoot

Topología

El diagrama de topología se utiliza en el siguiente escenario SISF. Los switches 9300 son solo de capa 2 y NO tienen SVI configurado en la Vlan 10 del cliente.

 Nota: SISF se habilita en este laboratorio manualmente.



Configuración

La configuración predeterminada de SISF se configuró en ambos switches 9300 que se enfrentan a los puertos de acceso, mientras que la política personalizada se aplicó en los puertos troncales para ilustrar las salidas de 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
```

Verificación

Puede utilizar estos comandos para validar las 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, DHCP - IPv4 DHCP

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 10.10.10.100	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, DHCP - IPv4 DHCP
```

```
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#
```

Escenarios de ejemplo

Error de dirección IPv4 duplicada en el dispositivo host

Problema

La sonda "keepalive" enviada por el switch es una verificación L2. Como tal desde el punto de vista del switch, las direcciones IP utilizadas como fuente en los ARP no son importantes: esta función se puede utilizar en dispositivos sin ninguna dirección IP configurada, por lo que la fuente IP de 0.0.0.0 no es relevante. Cuando el host recibe estos mensajes, responde y rellena el campo IP de destino con la única dirección IP disponible en el paquete recibido, que es su propia dirección IP. Esto puede causar falsas alertas de direcciones IP duplicadas, porque el host que responde ve su propia dirección IP como el origen y el destino del paquete.

Se recomienda configurar la política SISF para utilizar un origen automático para sus sondeos keepalive.

 Nota: Consulte este [artículo sobre problemas de direcciones duplicadas](#) para obtener más información

Sondeo predeterminado

Este es el paquete de sondeo cuando no hay un SVI local presente y la configuración de sondeos predeterminada:

<#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: 00000000000000000000000000000000

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

Solución

Configure el sondeo para que utilice una dirección distinta del equipo host para el sondeo. Esto se puede lograr mediante estos métodos

Fuente automática para la sonda "Keep-Alive"

Configure un origen automático para los sondeos "keepalive" para reducir el uso de 0.0.0.0 como IP de origen:

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


La lógica si se aplica el comando auto-source funciona de la siguiente manera:

```
<#root>
```

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

```
<-- Optional parameter
```

1. Establezca el origen en VLAN SVI si está presente.
2. Busque un par de origen/MAC en la tabla de host IP para la misma subred. La sonda se originó en la interfaz física del switch MAC + la IP de algún otro host en la subred que ya se encuentra en la base de datos.
3. Calcule la IP de origen desde la IP de destino con el bit de host y la máscara proporcionados. La sonda se genera al escuchar la IP del cliente y crear una sonda en la subred con los últimos bits configurados.



Nota: Si el comando se aplica con <override>, siempre saltamos al paso 3.

Sondeo modificado

La configuración de la configuración de reserva de origen automático para utilizar una dirección IP en la subred modifica la sonda. Dado que no hay SVI ni ningún otro cliente en la subred, recurrimos a la IP/máscara configurada en la configuración.

```
<#root>
```

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

Este es el paquete de sonda 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: 00000000000000000000000000000000

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

Más detalles sobre el comportamiento de la sonda

Comando	Acción (Para seleccionar la IP de origen y la dirección MAC para la sonda ARP de seguimiento de dispositivos)	Notas
device-tracking tracking auto-source	<ul style="list-style-type: none">• Establezca el origen en VLAN SVI si está presente.• Busque el enlace IP y MAC en la tabla de seguimiento de dispositivos de la misma subred.• Usar 0.0.0.0	Recomendamos que desactive el seguimiento de dispositivos en todos los puertos troncales para evitar el inestabilidad de MAC.
device-tracking tracking auto-source override	<ul style="list-style-type: none">• Establezca el origen en VLAN SVI si está presente• Usar 0.0.0.0	No se recomienda cuando no hay SVI.
device-tracking tracking auto-source fallback <IP> <MASK>	<ul style="list-style-type: none">• Establezca el origen en VLAN SVI si está presente.	Recomendamos que desactive el seguimiento de dispositivos en todos los puertos troncales para evitar el inestabilidad de

	<ul style="list-style-type: none"> • Busque el enlace IP y MAC en la tabla de seguimiento de dispositivos de la misma subred. • Calcule la IP de origen a partir de la IP del cliente mediante el bit de host y la máscara proporcionados. La MAC de origen se toma de la dirección MAC del puerto de switch que se encuentra frente al cliente. 	<p>MAC.</p> <p>La dirección IPv4 calculada no se debe asignar a ningún cliente o dispositivo de red.</p>
<pre>device-tracking tracking auto- source fallback <IP> <MASK> override</pre>	<ul style="list-style-type: none"> • Establezca el origen en VLAN SVI si está presente. • Calcule la IP de origen a partir de la IP del cliente mediante el bit de host y la máscara proporcionados. La MAC de origen se toma de la dirección MAC del puerto de switch que se encuentra frente al cliente. 	<p>La dirección IPv4 calculada no se debe asignar a ningún cliente o dispositivo de red.</p>

Explicación del comando device-tracking auto-source fallback <IP> <MASK> [override]:

En función de la IP del host, se debe reservar una dirección IPv4.

$\langle \text{reserved IPv4 address} \rangle = (\langle \text{host-ip} \rangle \& \langle \text{MASK} \rangle) | \langle \text{IP} \rangle$

 Nota: Esta es una fórmula booleana

Ejemplo.

Si utilizamos el comando:

```
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

máscara = 24

Dividamos la fórmula booleana en dos partes.

1. 10.152.140.25 Y 255.255.255.0 operación:

```
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. Operación 10.152.140.0 O 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 reservada = 10.152.140.1

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

 Nota: La dirección utilizada como origen IP debe estar fuera de los enlaces DHCP para la subred.

Error de dirección IPv6 duplicada

Problema

Error de dirección IPv6 duplicado cuando IPv6 está habilitado en la red y se ha configurado una interfaz virtual conmutada (SVI) en una VLAN.

En un paquete DAD IPv6 normal, el campo Dirección de origen del encabezado IPv6 se establece en la dirección no especificada (0:0:0:0:0:0:0:0). Similar a un caso de IPv4.

El orden para elegir la dirección de origen en la sonda SISF es:

- Dirección local del enlace de SVI, si está configurada
- Utilizar 0:0:0:0:0:0:0:0

Solución

Recomendamos que agregue los siguientes comandos a la configuración de SVI. Esto permite que la SVI adquiera una dirección local de link automáticamente; esta dirección se utiliza como la dirección IP de origen de la sonda SISF, evitando así el problema de la dirección IP duplicada.


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

Mayor uso de memoria y CPU

Problema

La sonda "keepalive" enviada por el switch se difunde fuera de todos los puertos cuando se habilita mediante programación. Los switches conectados en el mismo dominio L2 envían estas difusiones a sus hosts, lo que hace que el switch de origen agregue hosts remotos a su base de datos de seguimiento de dispositivos. Las entradas de host adicionales aumentan el uso de memoria en el dispositivo y el proceso de agregar los hosts remotos aumenta el uso de CPU del dispositivo.

Se recomienda determinar el alcance de la política de programación configurando una política en el link ascendente a los switches conectados para definir el puerto como confiable y conectado a un switch.

 Nota: Tenga en cuenta que las funciones dependientes de SISF, como la indagación DHCP, permiten que SISF funcione correctamente, lo que puede desencadenar este problema.

Solución

Configure una política en el enlace ascendente (troncal) para detener los sondeos y el aprendizaje de los hosts remotos que gustan en otros switches (SISF solo es necesario para mantener una tabla de host local)

```
<#root>
```

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

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

DT_trunk_policy

Tiempo de seguimiento de dispositivos alcanzable demasiado corto

Problema

Debido a un problema de migración desde IPDT al seguimiento de dispositivos basado en SISF, a veces se introduce un tiempo no predeterminado alcanzable cuando se migra desde una versión anterior a la 16.x y versiones más recientes.

Solución

Se recomienda volver a la hora de acceso predeterminada mediante la configuración de:

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

Switches incorporados a la herramienta Meraki (aumento de CPU y vaciado de puertos)

Problema

Cuando los switches se incorporan a la herramienta de supervisión en la nube de Meraki, dicha herramienta aplica políticas de seguimiento de dispositivos personalizadas.

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

La política se aplica a todas las interfaces sin distinción, es decir, no distingue entre puertos de borde y puertos troncales que se enfrentan a otros dispositivos de red (por ejemplo, switches, routers de firewalls, etc.). El switch puede crear varias entradas SISF en los puertos troncales donde se configura MERAKI_POLICY, lo que provoca vaciados en estos puertos, así como aumentos en el uso de la 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

Solución

Configure la siguiente política en todas las interfaces que no sean de borde:

```
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
```

Direcciones IP con el mismo MAC No están en la Tabla SISF

Problema

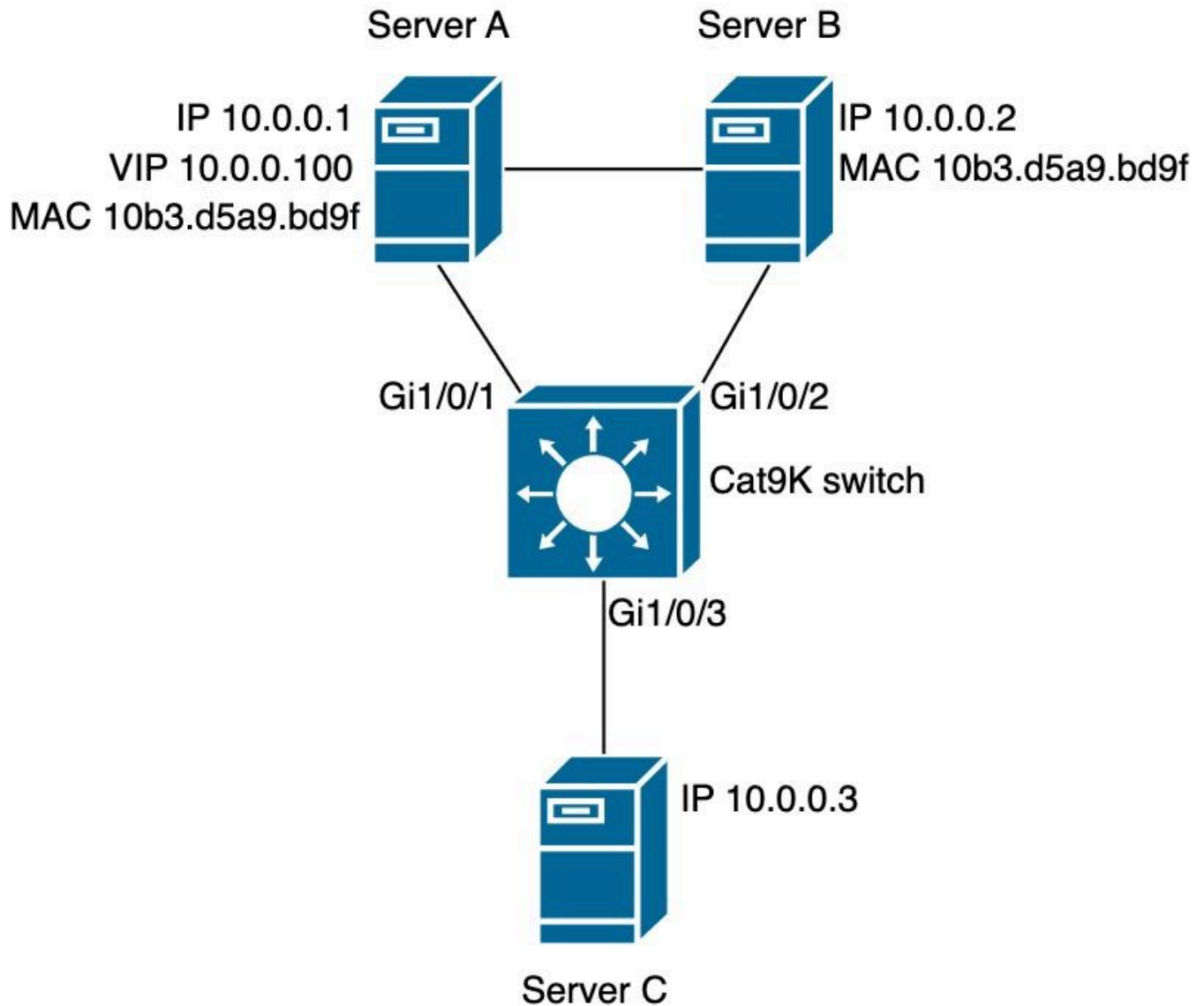
Este escenario es común en dispositivos en modo HA (alta disponibilidad) que tienen diferentes direcciones IP, pero comparten la misma dirección MAC. También se observa en entornos de VM que comparten la misma condición (una sola dirección MAC para dos o más direcciones IP). Esta condición evita la conectividad de red a todas aquellas IPs que no tienen una entrada en la tabla SISF cuando la política personalizada SISF en el modo de guardia está en su lugar. Según la función SISF, solamente se aprende una IP por dirección MAC.



Nota: Este problema está presente en la versión 17.7.1 y versiones posteriores

Ejemplo:

- La IP 10.0.0.1 con la dirección MAC 10b3.d5a9.bd9f se aprende en la tabla SISF y se le permite comunicarse con el dispositivo de red 10.0.0.3.
- Sin embargo, la segunda IP 10.0.0.2 y la IP virtual 10.0.0.100 que comparten la dirección MAC 10b3.d5a9.bd9f no están programadas en la tabla SISF, y la comunicación con la red no está 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

Base de datos 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 DHCP

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

Servidor A de prueba de disponibilidad

<#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

.....

Servidor B de prueba de disponibilidad.

<#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 caídas en el switch.

<#root>

```
switch(config)#
```

```
device-tracking logging
```

Registros

<#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=Gil/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=Gil/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=Gil/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=Gil/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=Gil/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=Gil/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=Gil/0/1 New I/F=Gil/0/2

%SISF-4-PAK_DROP: Message dropped

IP=10.0.0.2 VLAN=10 MAC=10b3.d5a9.bd9f

I/F=Gil/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=Gil/0/1 New I/F=Gil/0/2

%SISF-4-PAK_DROP: Message dropped

IP=10.0.0.2 VLAN=10 MAC=10b3.d5a9.bd9f

I/F=Gil/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=Gil/0/1 New I/F=Gil/0/2
```

```
%SISF-4-PAK_DROP: Message dropped
IP=10.0.0.2 VLAN=10 MAC=10b3.d5a9.bd9f
```

```
I/F=Gil/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=Gil/0/1 New I/F=Gil/0/2
```

```
%SISF-4-PAK_DROP: Message dropped
IP=10.0.0.2 VLAN=10 MAC=10b3.d5a9.bd9f
```

```
I/F=Gil/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=Gil/0/1 New I/F=Gil/0/2
```

Solución

Opción 1: elimine la política IPDT del puerto para permitir que los paquetes ARP y los dispositivos afectados sean alcanzables

```
<#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
```

Opción 2: Eliminar la limpieza arp de protocolo de la política de rastreo de dispositivos.

```
<#root>
```

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

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

```
no protocol arp
```

Opción 3: Cambie el nivel de seguridad de IPDT_POLICY a glean.

```
<#root>
```

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

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

```
security-level glean
```

Información Relacionada

- [Guía de Configuración de Seguridad, Cisco IOS XE Bengaluru 17.6.x \(Switches Catalyst 9300\): Configuración de las Funciones de Seguridad Integradas del Switch](#)
- [Guía de Configuración de Seguridad, Cisco IOS XE Cupertino 17.9.x \(Switches Catalyst 9300\): Configuración de las Funciones de Seguridad Integradas del Switch](#)
- [Informe técnico sobre las funciones de seguridad integrada \(SISF\) del switch de la familia Cisco Catalyst 9000](#)
- ID de bug Cisco [CSCvx75602](#) - Pérdida de memoria SISF en AR-relay y ND-suppression
- Id. de error de Cisco [CSCwf3293](#) - [EVPN SISF] Método personalizado necesario para modificar los valores de dirección límite para IPv4/V6 con EVPN + DHCP
- ID de bug de Cisco [CSCvq22011](#) - IOS-XE descarta la respuesta ARP cuando IPDT obtiene de ARP
- Cisco bug ID [CSCwc20488](#) - limitación de 255 pseudo-puertos por vlan/evi
- Cisco bug ID [CSCwh52315](#) - El switch 9300 descarta la respuesta ARP cuando tiene una política IPDT en el puerto
- Cisco bug ID [CSCvd51480](#) - Desvinculación de IP DHCP Snooping y Device-Tracking

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).