Dépannage du SISF sur les commutateurs de la gamme Catalyst 9000

Table des matières

Introduction

Ce document décrit les fonctions de sécurité intégrées (SISF) des commutateurs de la gamme Catalyst 9000. Il explique également comment le SISF peut être utilisé et comment interagit avec d'autres fonctionnalités.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Catalyst 9300-48P qui exécute Cisco IOS® XE 17.3.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

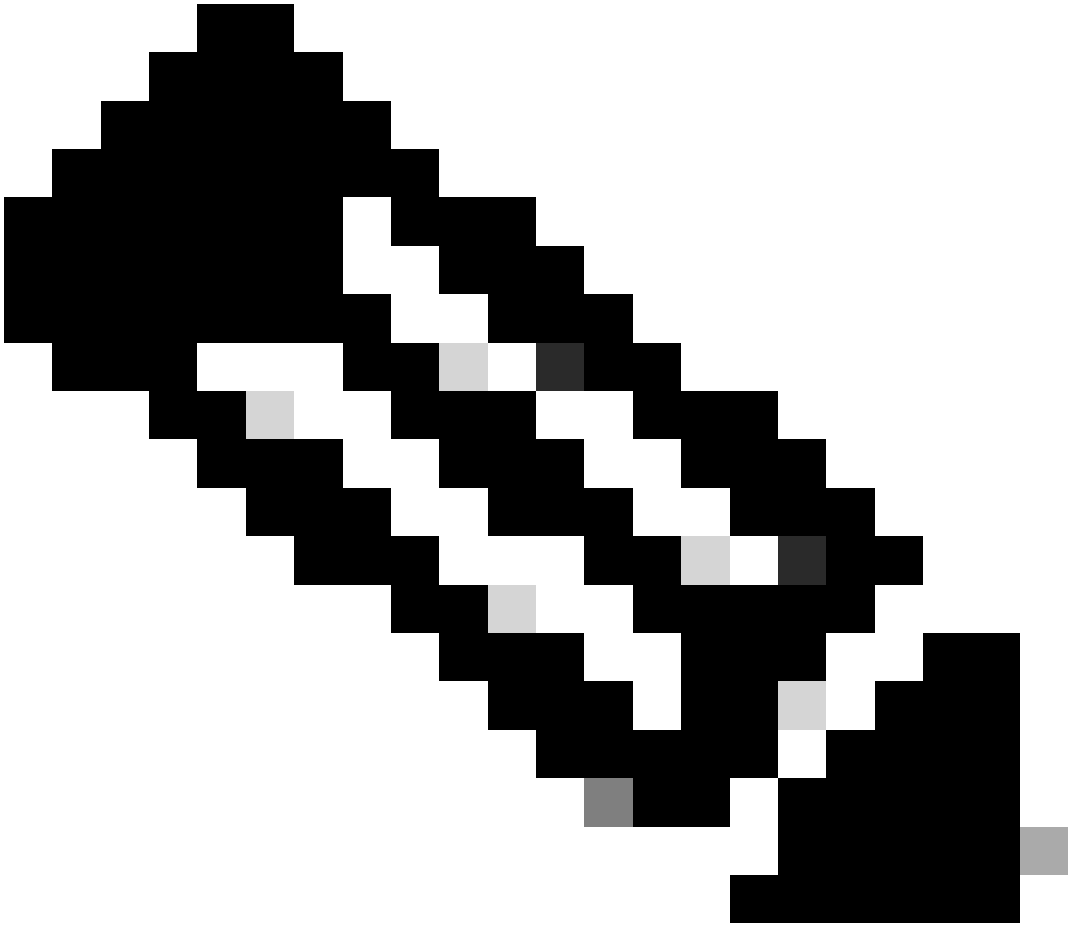
 Remarque : consultez le guide de configuration approprié pour connaître les commandes utilisées afin d'activer ces fonctionnalités sur d'autres plates-formes Cisco.

Produits connexes

Ce document peut également être utilisé avec les versions de matériel et de logiciel suivantes :

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

Avec 17.3.4 et versions ultérieures du logiciel Cisco IOS XE



Remarque : ce document s'applique également à la plupart des versions de Cisco IOS XE qui utilisent le SISF par rapport au suivi des périphériques.

Informations générales

Aperçu

Le protocole SISF fournit une table de liaison d'hôte et certains clients de fonctionnalités utilisent les informations qu'elle contient. Les entrées sont renseignées dans la table en glanant des paquets tels que DHCP, ARP, ND, RA qui suivent l'activité de l'hôte et aident à remplir dynamiquement la table. Si des hôtes silencieux sont présents dans le domaine L2, des entrées statiques peuvent être utilisées pour ajouter des entrées dans la table SISF.

Le SISF utilise un modèle de stratégie pour configurer les rôles des périphériques et des paramètres supplémentaires sur le commutateur. Une seule stratégie peut être appliquée au niveau de l'interface ou du VLAN. Si une stratégie est appliquée sur le VLAN et qu'une autre

stratégie est appliquée sur l'interface, la stratégie d'interface est prioritaire.

SISF peut également être utilisé pour limiter le nombre d'hôtes dans la table, mais il existe des différences entre les comportements IPv4 et IPv6. Si la limite SISF est définie et qu'elle est atteinte :

- Les hôtes IPv4 continuent à fonctionner, mais aucune entrée supérieure à la limite ne doit être ajoutée à la table SISF
- Les hôtes IPv6 qui n'entrent pas dans la table SISF ne sont pas autorisés à entrer dans le réseau et aucune nouvelle entrée ne doit être ajoutée à la table SISF.

À partir de la version 16.9.x et des versions plus récentes, une priorité de fonctionnalité client SISF est introduite. Il ajoute des options pour contrôler les mises à jour dans SISF et si deux clients ou plus utilisent la table de liaison, les mises à jour de la fonctionnalité de priorité plus élevée sont appliquées. Les exceptions ici sont les paramètres « limit address-count for IPv4/IPv6 per mac », les paramètres de la stratégie avec la priorité la plus basse sont effectifs.

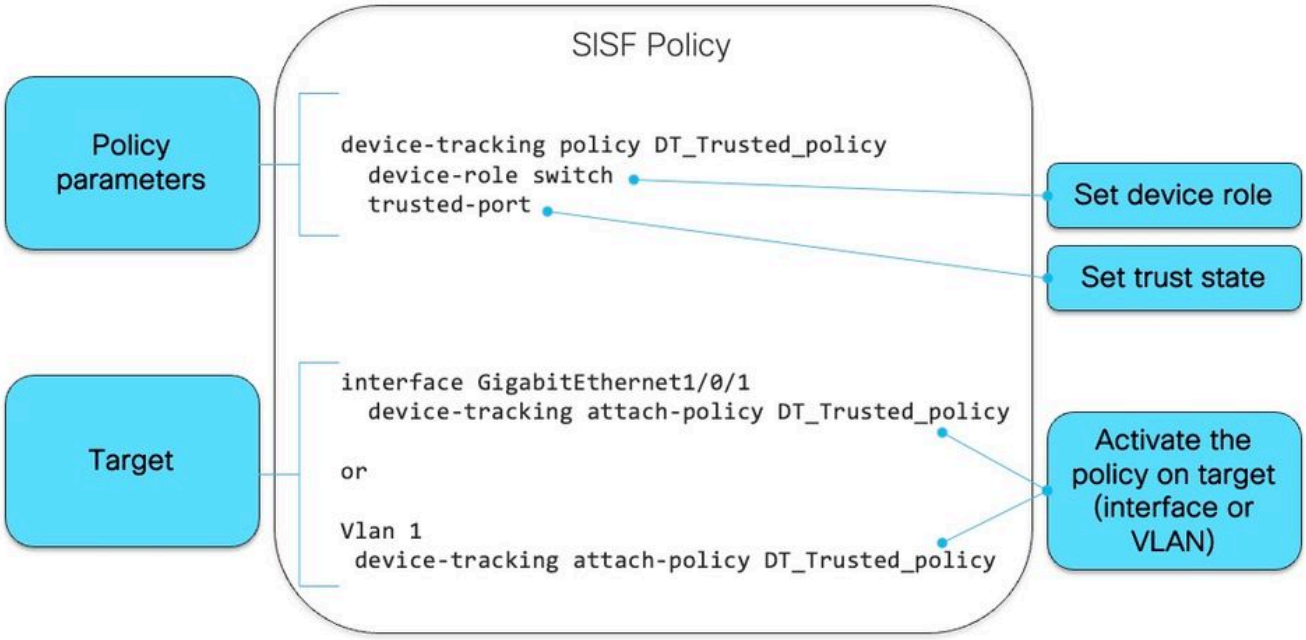
Voici quelques exemples de fonctionnalités qui nécessitent l'activation du suivi des périphériques :

- LISP/EVPN
- Point1x
- Authentification Web
- CTS
- Surveillance DHCP

Remarque : la priorité est utilisée pour sélectionner les paramètres de stratégie.

La politique créée à partir de l'interface de ligne de commande a la priorité la plus élevée (128), ce qui permet aux utilisateurs d'appliquer un paramètre de politique différent de celui des politiques de programmation. Tous les paramètres configurables de la stratégie personnalisée peuvent être modifiés manuellement.

L'image suivante est un exemple de politique SISF et explique comment la lire :



À l'intérieur de la stratégie, sous mot-clé de protocole, vous avez la possibilité de voir quel type de paquets sont utilisés pour remplir la base de données 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
```

Fonctionnalités de programmation et de client SISF

Les fonctions du tableau suivant activent le SISF par programme lorsqu'elles sont activées ou agissent comme des clients du SISF :

Fonction programmatique SISF	Fonctionnalités du client SISF
LISP sur VLAN	Point1x
EVPN sur VLAN	Authentification Web
Surveillance DHCP	CTS

Si une fonctionnalité client SISF est activée sur un périphérique configuré sans fonctionnalité qui active SISF, une stratégie personnalisée doit être configurée sur les interfaces se connectant aux hôtes.

Fonctionnalités IPv4 utilisant les informations SISF

- CTS
- IEEE 802.1x
- ZÉZAIEMENT
- EVPN
- Surveillance DHCP (active uniquement SISF mais ne l'utilise pas)
- Protection de la source IP

Fonctionnalités IPv6 qui consomment des informations SISF

- Protection de l'annonce de routeur IPv6
- Protection DHCP IPv6, relais DHCP de couche 2
- Proxy de détection d'adresse en double (DAD) IPv6
- Suppression Des Inondations
- Protection de la source IPv6
- Protection de la destination IPv6
- Limiteur RA
- Protection de préfixe IPv6

Suivi des périphériques

Le rôle principal du suivi des périphériques est de suivre la présence, l'emplacement et le déplacement des noeuds d'extrémité dans le réseau. Le protocole SISF surveille le trafic reçu par le commutateur, extrait l'identité du périphérique (adresse MAC et adresse IP) et les stocke dans une table de liaison. De nombreuses fonctionnalités, telles que IEEE 802.1X, l'authentification Web, Cisco TrustSec et LISP, dépendent de la précision de ces informations pour fonctionner correctement. Le suivi des périphériques basé sur SISF prend en charge les protocoles IPv4 et IPv6. Il existe cinq méthodes prises en charge par le client pour apprendre l'IP :

- DHCPv4
- DHCPv6
- ARP
- NDP
- Nettoyage des données

SISF sur un Port-Channel

Le suivi des périphériques sur port-channel (ou éther-channel) est pris en charge. Mais la configuration doit être appliquée au groupe de canaux, et non aux membres individuels du canal de port. La seule interface qui apparaît (et qui est connue) du point de vue de la liaison est le port-channel.

Réglage des sondes et des bases de données

Sonde :

- Dans IPDT, il y avait une commande pour aider à résoudre les problèmes d'adresse en double en retardant la sonde initiale de 10 secondes : « ip device tracking probe delay » upon link up.
- Dans SISF, il existe déjà un compteur d'attente intégré qui attend avant d'envoyer la première sonde. Il n'est pas configurable et résout le même problème. Comme il s'agit du code SISF, cette commande n'est plus nécessaire

Base de données :

Dans SISF, vous pouvez configurer quelques options pour contrôler la durée de conservation d'une entrée dans la base de données :

<#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)

Suivi des périphériques IP

Cycle de vie d'une entrée dans laquelle l'hôte est interrogé :

- SISF conserve la liaison IPv4/IPv6 par mac, une fois que l'apprentissage IP a réussi, la liaison passe à l'état REACHABLE
- SISF assure le suivi du client actif en surveillant le paquet de contrôle
- S'il n'y a aucun paquet de contrôle du client pendant 5 minutes, Binding passe à l'état VERIFY et envoie une sonde au client
- Si les clients ne répondent pas à la sonde, la liaison passe à l'état STALE sinon à l'état REACHABLE
- Le délai d'attente par défaut pour les entrées OBSOLÈTES est de 24 heures et peut être configuré
- Les entrées STALE sont supprimées après 24 heures (ou valeur de délai d'attente configurée)

Détection du vol

Types de vols de noeuds :

- Vol d'IP (même IP, mac différent, port différent/identique)
- VOL MAC (même MAC, IP différente, port différent)
- MAC IP THEFT (même mac, même ip, port différent)

Fonctionnalités de sécurité IP

Voici quelques-unes des fonctions dépendantes du SISF :

- Inspection NDP : messages Inspect IPv6 NDP
- Nettoyage d'adresses NPD : renseignez la table de liaison avec les informations collectées en surveillant le trafic NPD
- Suivi des périphériques : surveillance de l'activité des périphériques finaux, notamment par le biais d'un mécanisme d'activité
- Snooping : Glean les adresses dans les messages NDP, ARP et DHCP. Bloquer les messages non autorisés
- Relais DHCPv4 : relais du paquet DHCP diffusé vers l'adresse d'assistance configurée.
- Suppression de multidiffusion NDP et ARP : supprimez les messages NDP de multidiffusion en les convertissant en monodiffusion ou en répondant au nom des cibles.
- Proxy DAD : détection d'adresse dupliquée et envoi de l'adresse réseau pour le compte du client cible
- DHCPv4 Require : il impose au client d'obtenir l'adresse IP uniquement par DHCP

Avertissements SISF

Voici quelques-uns des comportements les plus fréquents associés au FSIS :

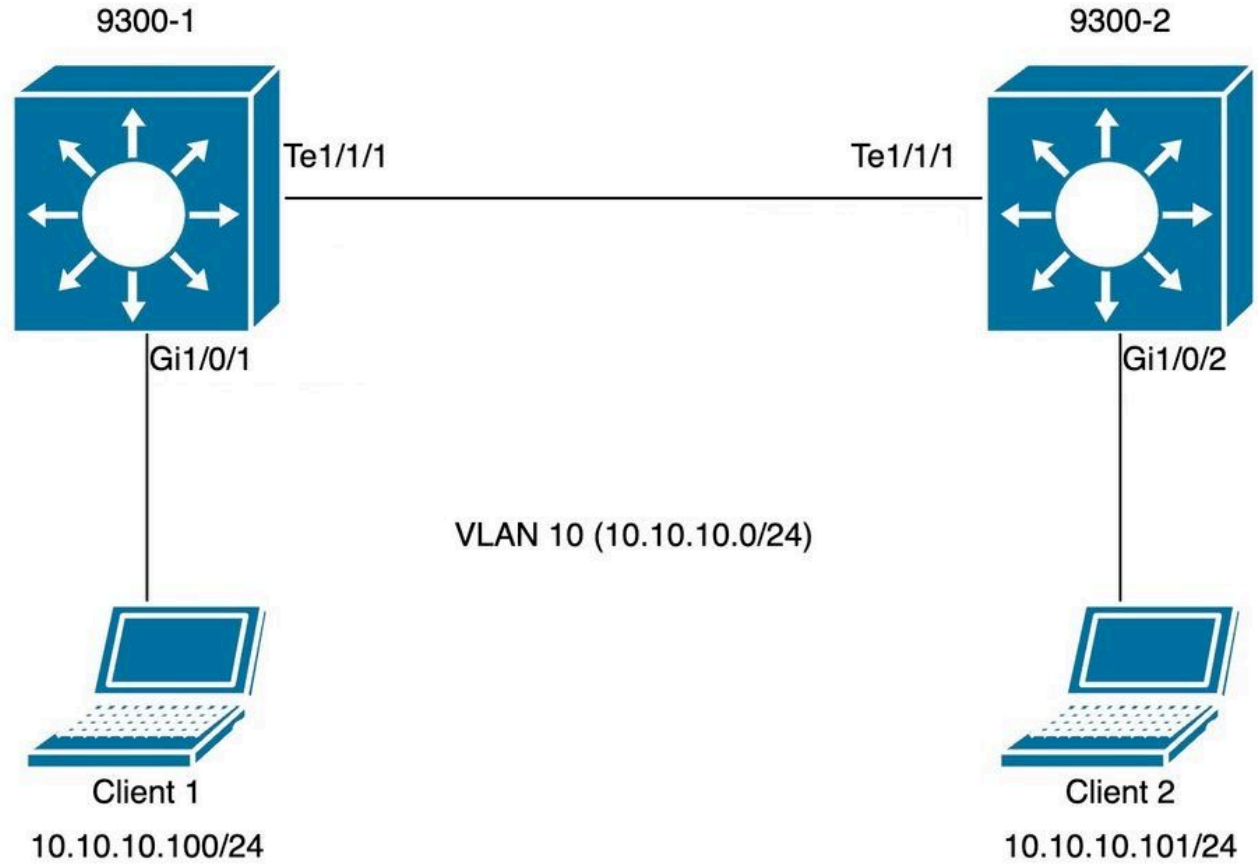
- SISF peut être activé en activant d'autres fonctionnalités telles que la surveillance DHCP
- Le comportement d'exploration par défaut de SISF peut avoir un impact sur l'attribution des adresses IP client.
- Lorsque le SISF est activé, il est également activé sur les ports de liaison ascendante, ce qui peut avoir un impact sur le réseau.

Dépannage

Topologie

Le schéma de topologie est utilisé dans le scénario SISF suivant. Les commutateurs 9300 sont uniquement de couche 2 et ne disposent PAS d'interface SVI configurée dans le VLAN client 10.

Remarque : SISF est activé manuellement dans ces travaux pratiques.



Configuration

La configuration SISF par défaut a été configurée sur les deux commutateurs 9300 faisant face aux ports d'accès, tandis que la stratégie personnalisée a été appliquée aux ports d'agrégation pour illustrer les sorties SISF attendues.

Commutateur 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
```

Commutateur 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
```

Vérification

Vous pouvez utiliser ces commandes pour valider les stratégies appliquées :

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

Commutateur 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#
```

Commutateur 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#
```

Scénarios courants

Erreur d'adresse IPv4 dupliquée sur le périphérique hôte

Problème

La sonde « keepalive » envoyée par le commutateur est un contrôle de couche 2. En tant que telle, du point de vue du commutateur, les adresses IP utilisées comme source dans les ARP ne sont pas importantes : cette fonctionnalité peut être utilisée sur des périphériques sans aucune adresse IP configurée, de sorte que la source IP 0.0.0.0 n'est pas pertinente. Lorsque l'hôte reçoit ces messages, il répond et renseigne le champ IP de destination avec la seule adresse IP disponible dans le paquet reçu, qui est sa propre adresse IP. Cela peut entraîner de fausses alertes d'adresse IP dupliquée, car l'hôte qui répond voit sa propre adresse IP à la fois comme source et comme destination du paquet.

Il est recommandé de configurer la stratégie SISF pour qu'elle utilise une source automatique pour ses sondes de test d'activité.

Remarque : consultez cet article sur les problèmes d'adresses en double pour plus

d'informations

Sonde par défaut

Il s'agit du paquet d'analyse lorsqu'aucune interface SVI locale n'est présente et que les paramètres d'analyse par défaut sont définis :

<#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
```

Solution

Configurez la sonde de sorte qu'elle utilise une adresse autre que celle du PC hôte. Ces méthodes permettent d'y parvenir

Source automatique pour la sonde « Keep-Alive »

Configurez une source automatique pour les sondes « keep-alive » afin de réduire l'utilisation de 0.0.0.0 en tant qu'IP source :

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

La logique d'application de la commande auto-source fonctionne comme suit :

```
<#root>

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

<-- Optional parameter
```

1. Définissez la source sur VLAN SVI, le cas échéant.
2. Recherchez une paire source/MAC dans la table d'hôtes IP pour le même sous-réseau. La sonde provient de l'interface physique MAC du commutateur + l'adresse IP d'un autre hôte du sous-réseau déjà présent dans la base de données.
3. Calculez l'adresse IP source à partir de l'adresse IP de destination avec le bit et le masque d'hôte fournis. La sonde est générée à partir de l'écoute de l'IP client et de la création d'une sonde dans le sous-réseau avec les derniers bits configurés.

Remarque : si la commande est appliquée avec <override>, nous passons toujours à l'étape 3.

Sonde modifiée

Le paramétrage de la configuration de secours auto-source pour utiliser une adresse IP dans le sous-réseau modifie la sonde. Puisqu'il n'y a pas d'interface SVI et aucun autre client sur le sous-réseau, nous revenons à l'IP/masque configuré dans la configuration.

```
<#root>

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

Il s'agit du paquet de sonde modifié :

```
<#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
```

Détails supplémentaires sur le comportement de la sonde

Commande	Action (Afin de sélectionner l'adresse IP et MAC source pour le suivi de périphérique sonde ARP)	Remarques
autosource de poursuite de poursuite de dispositif	• Définissez la source sur VLAN SVI, le cas échéant. • Recherchez la liaison IP et MAC dans la table de suivi des périphériques du même sous-réseau. • Utiliser 0.0.0.0	Nous vous recommandons de désactiver le suivi des périphériques sur tous les ports agrégés afin d'éviter le battement MAC.
correction automatique de la source de poursuite du suivi des dispositifs	• Définissez la source sur VLAN SVI, le cas échéant • Utiliser 0.0.0.0	Déconseillé en l'absence d'interface SVI.
suivi du suivi de périphérique auto-source fallback <IP> <MASK>	• Définissez la source sur VLAN SVI, le cas échéant. • Recherchez la liaison IP	Nous vous recommandons de désactiver le suivi des périphériques sur tous les ports agrégés afin d'éviter le

	et MAC dans la table de suivi des périphériques du même sous-réseau. • Calculez l'adresse IP source à partir de l'adresse IP du client en utilisant le bit hôte et le masque fournis. L'adresse MAC source est extraite de l'adresse MAC du port de commutation en face du client.	battement MAC. L'adresse IPv4 calculée ne doit être attribuée à aucun client ou périphérique réseau.
suivi de suivi de périphérique auto-source fallback <IP> <MASK> override	• Définissez la source sur VLAN SVI, le cas échéant. • Calculez l'adresse IP source à partir de l'adresse IP du client en utilisant le bit hôte et le masque fournis. L'adresse MAC source est extraite de l'adresse MAC du port de commutation en face du client.	L'adresse IPv4 calculée ne doit être attribuée à aucun client ou périphérique réseau.

Explication de la commande device-tracking auto-source fallback <IP> <MASK> [override] :

Selon l'adresse IP de l'hôte, une adresse IPv4 doit être réservée.

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

Remarque : il s'agit d'une formule booléenne

Exemple .

Si nous utilisons la commande :

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

IP hôte = 10.152.140.25

IP = 0.0.0.1

masque = 24

Scindons la formule booléenne en deux parties.

1. 10.152.140.25 ET 255.255.255.0 fonctionnement :

```
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 OU 0.0.0.1 opération :

```
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
```

Adresse IP réservée = 10.152.140.1

Adresse IP réservée = (10.152.140.25 & 255.255.255.0) | (0.0.0.1) = 10.152.140.1

Remarque : l'adresse utilisée comme source IP doit être étendue à partir des liaisons DHCP du sous-réseau.

Erreur d'adresse IPv6 en double

Problème

Erreur d'adresse IPv6 dupliquée lorsque IPv6 est activé sur le réseau et qu'une interface virtuelle commutée (SVI) est configurée sur un VLAN.

Dans un paquet DAD IPv6 normal, le champ Adresse source de l'en-tête IPv6 est défini sur l'adresse non spécifiée (0:0:0:0:0:0:0:0). Similaire au cas IPv4.

L'ordre de sélection de l'adresse source dans la sonde SISF est le suivant :

- Adresse link-local de l'interface SVI, si elle est configurée
- Utiliser 0:0:0:0:0:0:0:0

Solution

Nous vous recommandons d'ajouter les commandes suivantes à la configuration SVI. Cela permet à l'interface SVI d'acquérir automatiquement une adresse link-local ; cette adresse est utilisée comme adresse IP source de la sonde SISF, évitant ainsi le problème de doublon d'adresse IP.

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

Mémoire et utilisation CPU accrues

Problème

La sonde « keepalive » envoyée par le commutateur est diffusée à partir de tous les ports lorsqu'elle est activée par programme. Les commutateurs connectés dans le même domaine de couche 2 envoient ces diffusions à leurs hôtes, ce qui a pour effet que le commutateur d'origine ajoute des hôtes distants à sa base de données de suivi des périphériques. Les entrées d'hôte supplémentaires augmentent l'utilisation de la mémoire sur le périphérique et le processus d'ajout des hôtes distants augmente l'utilisation du processeur du périphérique.

Il est recommandé de définir la stratégie de programmation en configurant une stratégie sur la liaison ascendante vers les commutateurs connectés afin de définir le port comme étant sécurisé et connecté à un commutateur.

Remarque : sachez que les fonctionnalités dépendant du SISF, telles que la surveillance DHCP, permettent au SISF de fonctionner correctement, ce qui peut déclencher ce problème.

Solution

Configurez une stratégie sur la liaison ascendante (trunk) pour arrêter les analyses et l'apprentissage des hôtes distants qui aiment sur d'autres commutateurs (SISF est uniquement nécessaire pour gérer une table d'hôtes locale)

<#root>

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

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

Temps d'accès au suivi des périphériques trop court

Problème

En raison d'un problème de migration d'IPDT vers le suivi de périphérique basé sur SISF, un délai d'accessibilité non par défaut est parfois introduit lors de la migration d'une ancienne version vers 16.x et les versions plus récentes.

Solution

Il est recommandé de rétablir l'heure d'accessibilité par défaut en configurant :

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

Commutateurs intégrés à l'outil Meraki (augmentation du CPU et purges de ports)

Problème

Lorsque des commutateurs sont intégrés à l'outil de surveillance cloud Meraki, celui-ci applique des politiques de suivi des périphériques personnalisées.

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

La politique est appliquée à toutes les interfaces sans distinction, ce qui signifie qu'elle ne fait pas de distinction entre les ports de périphérie et les ports agrégés qui font face à d'autres périphériques réseau (par exemple, commutateurs, pare-feu, routeurs, etc.). Le commutateur peut créer plusieurs entrées SISF sur les ports d'agrégation où MERAKI_POLICY est configuré, provoquant ainsi des vidages sur ces ports ainsi qu'une augmentation de l'utilisation du 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
```

Solution

Configurez la stratégie suivante sur toutes les interfaces non périphériques :

```
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
```

Adresses IP avec le même MAC ne figurant pas dans la table SISF

Problème

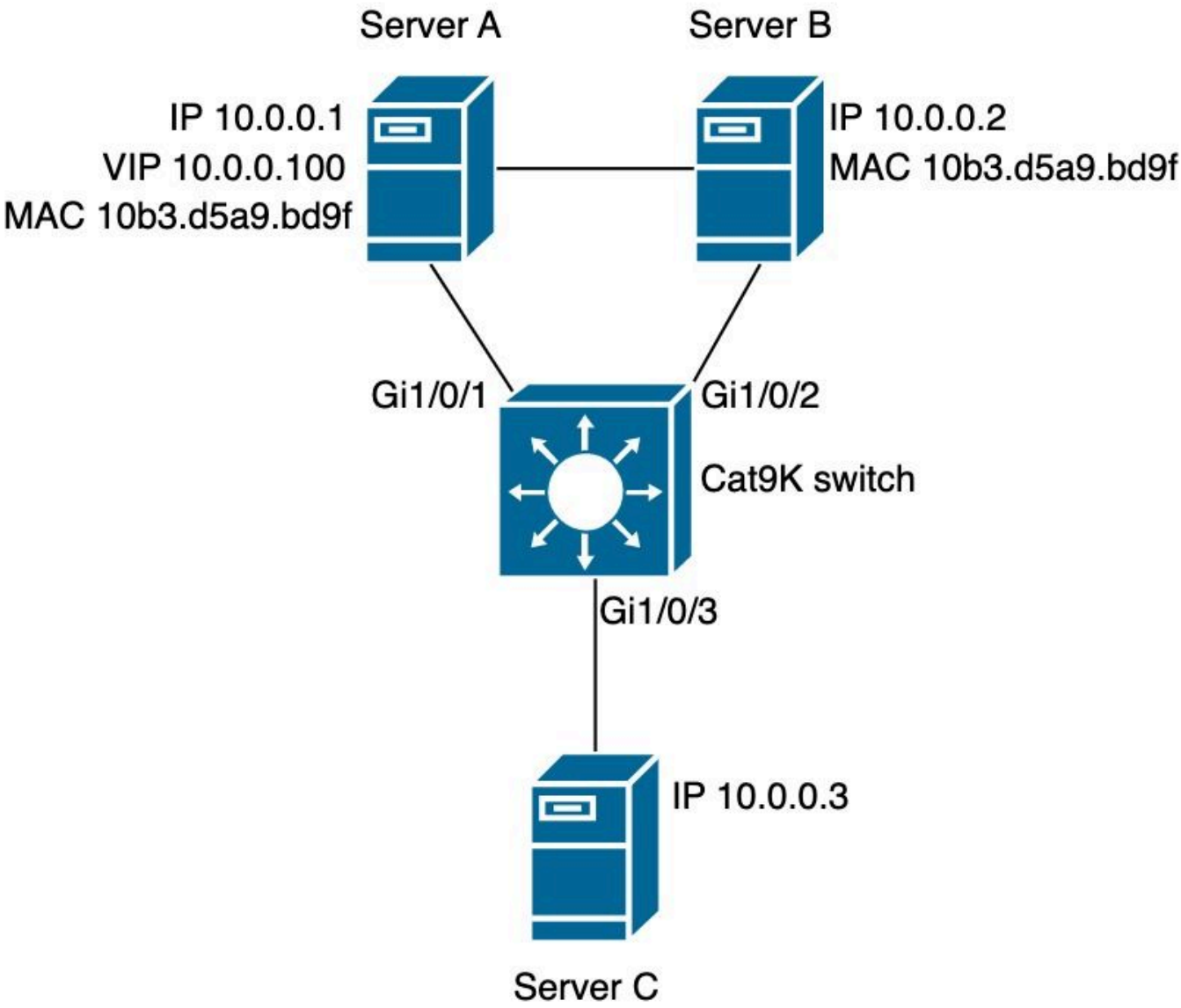
Ce scénario est courant sur les appareils en mode haute disponibilité (HA) qui ont des adresses IP différentes, mais qui partagent la même adresse MAC. Elle est également observée dans les environnements de machines virtuelles qui partagent la même condition (adresse MAC unique pour deux adresses IP ou plus). Cette condition empêche la connectivité réseau à toutes les adresses IP qui n'ont pas d'entrée dans la table SISF lorsque la stratégie SISF personnalisée en mode de garde est en place.Selon la fonctionnalité SISF, une seule adresse IP est apprise par adresse MAC.

Remarque : ce problème est présent dans les versions 17.7.1 et ultérieures

---

Exemple :

- L’adresse IP 10.0.0.1 avec l’adresse MAC 10b3.d5a9.bd9f est apprise sur la table SISF et autorisée à communiquer avec le périphérique réseau 10.0.0.3.
- Cependant, la deuxième adresse IP 10.0.0.2 et l'adresse IP virtuelle 10.0.0.100 qui partagent l'adresse MAC 10b3.d659.7858 ne sont pas programmées dans la table SISF et la communication avec le réseau n'est pas autorisée.



politique de fonds d'investissement stratégiques

<#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 données 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
```

Serveur de test d'accessibilité 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
.....
```

Test d'accessibilité Serveur 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)
```

Validation des abandons sur le commutateur.

<#root>

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

Journaux

<#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

Solution

Option 1 : supprimer la stratégie IPDT du port permet aux paquets ARP et aux périphériques affectés d'être accessibles

<#root>

```
switch(config)#interface gigabitEthernet 1/0/1
switch(config-if)#
```

no device-tracking attach-policy IPDT_POLICY

```
switch(config-if)#interface gigabitEthernet 1/0/2
switch(config-if)#
```

no device-tracking attach-policy IPDT_POLICY

Option 2 : supprimez le glanage arp de protocole de la stratégie de suivi des périphériques.

<#root>

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

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

no protocol arp

Option 3 : Modifiez le niveau de sécurité de IPDT_POLICY sur glean.

<#root>

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

security-level glean

Informations connexes

- Guide de configuration de la sécurité, Cisco IOS XE Bengaluru 17.6.x (commutateurs Catalyst 9300) : Configuration des fonctions de sécurité intégrées du commutateur
- Guide de configuration de la sécurité, Cisco IOS XE Cupertino 17.9.x (commutateurs Catalyst 9300) : Configuration des fonctions de sécurité intégrées du commutateur
- Livre blanc sur les fonctionnalités de sécurité intégrées (SISF) des commutateurs de la gamme Cisco Catalyst 9000
- ID de bogue Cisco CSCvx75602 - Fuite de mémoire SISF dans le relais AR et suppression ND
- ID de bogue Cisco CSCwf3293 - [EVPN SISF] Méthode personnalisée requise pour modifier les valeurs d'adresse limite pour IPv4/V6 avec EVPN + DHCP
- ID de bogue Cisco CSCvq22011 - IOS-XE abandonne la réponse ARP lorsque IPDT est glané à partir d'ARP
- ID de bogue Cisco CSCwc20488 - Limitation de 255 pseudo-ports par VLAN/Version
- ID de bogue Cisco CSCwh52315 - Le commutateur 9300 abandonne la réponse ARP lorsqu'une stratégie IPDT est présente sur le port
- ID de bogue Cisco CSCvd51480 - Désassociation de la surveillance ip dhcp et du suivi des périphériques

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.