Risoluzione dei problemi relativi a SISF sugli switch Catalyst serie 9000

Sommario

Introduzione

In questo documento viene descritto il SISF (Switch Integrated Security Features) usato negli switch Catalyst della famiglia 9000. Vengono inoltre illustrate le modalità di utilizzo di SISF e l'interazione con altre funzionalità.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per questo documento, è stato usato Cisco Catalyst 9300-48P con Cisco IOS® XE 17.3.x

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

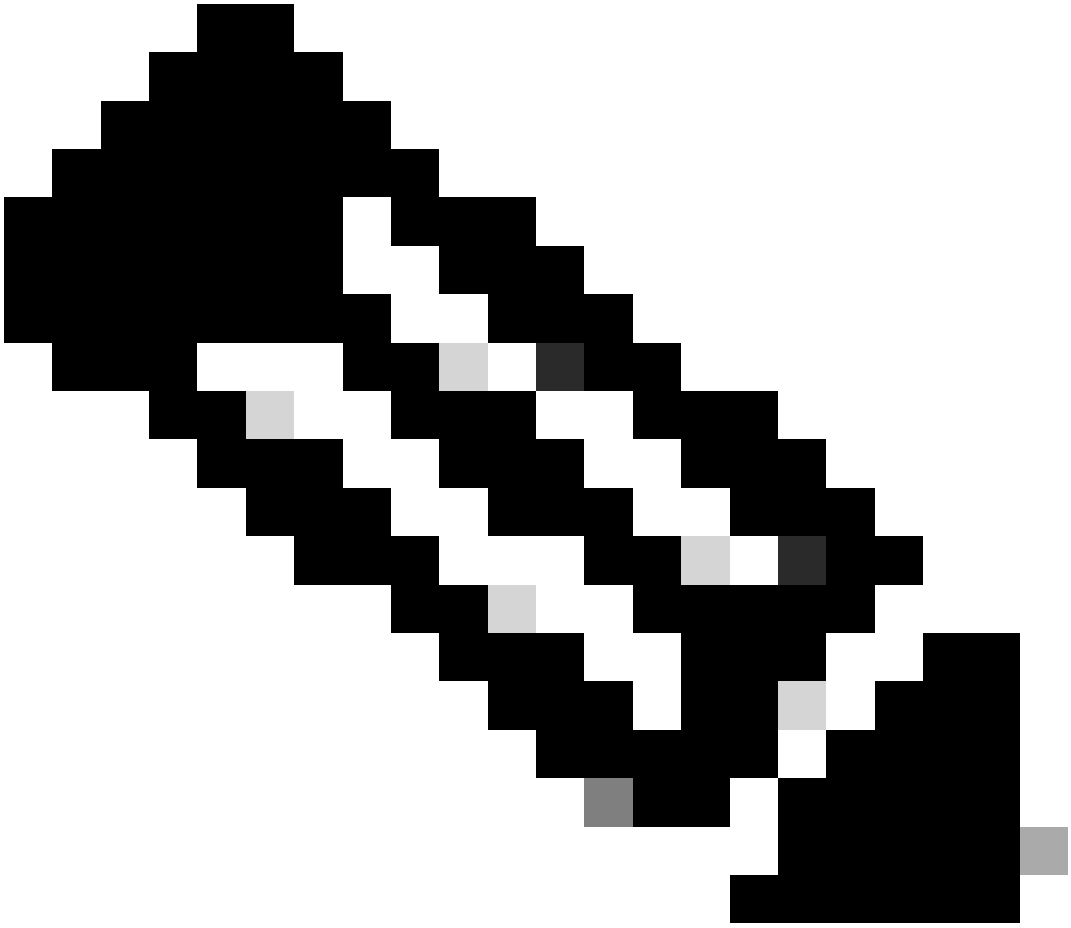
 Nota: per i comandi che vengono usati per abilitare queste funzionalità su altre piattaforme Cisco, consultare la guida alla configurazione appropriata.

Prodotti correlati

Il presente documento può essere utilizzato anche per le seguenti versioni hardware e software:

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

Con la versione 17.3.4 e successive del software Cisco IOS XE



Nota: questo documento è applicabile anche alla maggior parte delle versioni di Cisco IOS XE che utilizzano SISF rispetto a Device Tracking.

Premesse

Panoramica

SISF fornisce una tabella di binding host e vi sono client di funzionalità che utilizzano le informazioni da essa fornite. Le voci vengono popolate nella tabella mediante la raccolta di pacchetti come DHCP, ARP, ND, RA che tengono traccia dell'attività dell'host e consentono di popolare dinamicamente la tabella. Se nel dominio L2 sono presenti host invisibili all'utente, è possibile utilizzare le voci statiche per aggiungere voci alla tabella SISF.

SISF utilizza un modello di criteri per configurare i ruoli dei dispositivi e le impostazioni aggiuntive sullo switch. È possibile applicare una singola policy a livello di interfaccia o di VLAN. Se una policy viene applicata alla VLAN e una policy diversa viene applicata all'interfaccia, la policy di

interfaccia ha la precedenza.

È inoltre possibile utilizzare SISF per limitare il numero di host nella tabella, ma esistono differenze tra il comportamento di IPv4 e IPv6. Se il limite SISF è impostato e viene raggiunto:

- Gli host IPv4 continuano a funzionare, ma non è possibile aggiungere altre voci oltre il limite alla tabella SISF
- Gli host IPv6 che non consentono l'accesso alla tabella SISF non possono accedere alla rete e non è necessario aggiungere nuove voci alla tabella SISF.

Dalla versione 16.9.x e successive è stata introdotta una priorità per le funzionalità client SISF. Aggiunge opzioni per controllare gli aggiornamenti in SISF e, se due o più client utilizzano la tabella di binding, vengono applicati gli aggiornamenti dalla funzionalità con priorità più alta. Fanno eccezione le impostazioni "Limita il conteggio degli indirizzi per IPv4/IPv6 per mac", mentre le impostazioni dei criteri con la priorità più bassa sono effettive.

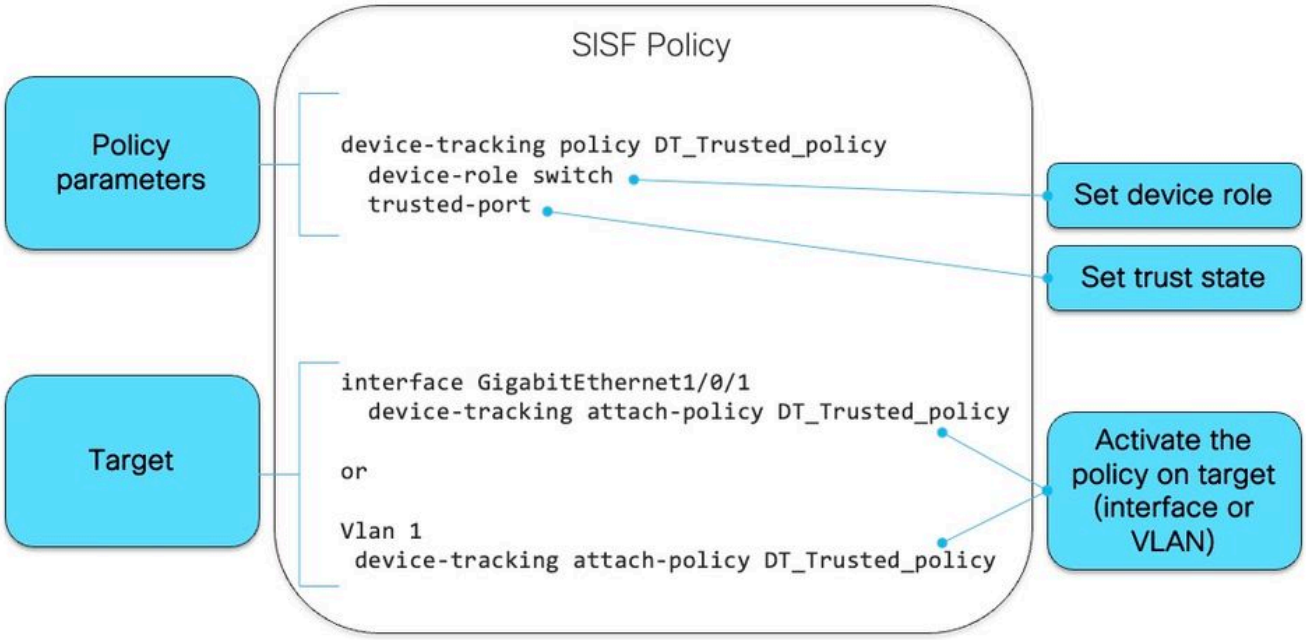
Di seguito sono riportati alcuni esempi di funzionalità che richiedono l'attivazione del rilevamento dei dispositivi:

- LISP/EVPN
- Punto1x
- Autenticazione Web
- CTS
- Snooping DHCP

Nota: per selezionare le impostazioni dei criteri viene utilizzata la priorità.

Il criterio creato dalla CLI ha la priorità più alta (128), pertanto consente agli utenti di applicare un'impostazione del criterio diversa da quella dei criteri programmatici. Tutte le impostazioni configurabili nel criterio personalizzato possono essere modificate manualmente.

Nell'immagine seguente viene illustrato un esempio di criteri SISF e viene illustrato come leggerli:



All'interno del criterio, in parola chiave protocol, è possibile visualizzare il tipo di pacchetti utilizzati per popolare il database 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
```

Funzioni client e programmatiche SISF

Le funzioni riportate nella tabella seguente consentono di attivare SISF a livello di codice quando sono attivate oppure di agire come client per SISF:

Funzione programmatica SISF	Funzioni del client SISF
LISP su VLAN	Punto1x
EVPN on VLAN	Autenticazione Web
Snooping DHCP	CTS

Se una funzionalità del client SISF è abilitata su un dispositivo configurato senza una funzionalità che abilita SISF, è necessario configurare un criterio personalizzato sulle interfacce che si connettono agli host.

Funzioni IPv4 che utilizzano le informazioni SISF

- CTS
- IEEE 802.1x
- LISP
- EVPN
- Snooping DHCP (attiva solo SISF ma non lo utilizza)
- Protezione origine IP

Funzioni IPv6 che utilizzano le informazioni SISF

- Protezione annuncio router IPv6 (RA)
- Protezione DHCP IPv6, inoltro DHCP di livello 2
- Proxy DAD (Duplicate Address Detection) IPv6
- Soppressione flooding
- Protezione origine IPv6
- Protezione destinazione IPv6
- RA Throttler
- Protezione prefissi IPv6

Tracciamento dispositivi

Il ruolo principale del rilevamento dei dispositivi è tenere traccia della presenza, della posizione e dello spostamento dei nodi finali nella rete. SISF analizza il traffico ricevuto dallo switch, estrae l'identità del dispositivo (indirizzo MAC e IP) e li memorizza in una tabella di binding. Molte caratteristiche, quali IEEE 802.1X, l'autenticazione Web, Cisco TrustSec, LISP e così via, dipendono dall'accuratezza di queste informazioni per funzionare correttamente. Il rilevamento dei dispositivi basato su SISF supporta sia IPv4 che IPv6. Esistono cinque metodi supportati per l'apprendimento dell'IP da parte del client:

- DHCPv4
- DHCPv6
- ARP
- NDP
- Data gleaning

SISF su port-channel

È supportato il rilevamento dei dispositivi sul canale della porta (o sul canale etere). Tuttavia, la configurazione deve essere applicata al gruppo di canali, non ai singoli membri del canale di porta. L'unica interfaccia che viene visualizzata (ed è nota) dal punto di vista del binding è port-channel.

Tuning del database e del probe

Sonda:

- In IPDT c'era un comando per aiutare a risolvere i problemi di indirizzo duplicato ritardando la sonda iniziale per 10 secondi: "ip device tracking probe delay" al momento del collegamento.
- Nel SISF è già presente un timer di attesa incorporato che attende prima di inviare la prima sonda. Non è configurabile e risolve lo stesso problema. Poiché è incluso nel codice SISF, questo comando non è più necessario

Database:

In SISF è possibile configurare alcune opzioni per controllare per quanto tempo una voce viene mantenuta nel database:

<#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)

Tracciamento dispositivi IP

Ciclo di vita di una voce in cui viene eseguito il polling dell'host:

- SISF mantiene il binding IPv4/IPv6 per mac, una volta che l'apprendimento IP è riuscito, le transizioni del binding allo stato REACHABLE
- SISF tiene traccia del client di liveness monitorando il pacchetto di controllo
- Se il client non invia alcun pacchetto di controllo per 5 minuti, il binding passa allo stato VERIFY e invia la sonda al client
- Se i client non rispondono al probe, l'associazione passa allo stato NON AGGIORNATO o allo stato RAGGIUNGIBILE
- Il timeout predefinito per la voce STALE è di 24 ore ed è configurabile
- Le voci STALE vengono eliminate dopo 24 ore (o dopo il valore di timeout configurato)

Rilevamento furti

Tipi di furti di nodi:

- Furto IP (stesso IP, mac diverso, porta diversa)
- FURTO TRAMITE MAC (stesso MAC, IP diverso, porta diversa)
- MAC IP THEFT (stesso MAC, stesso IP, porta diversa)

Funzioni di sicurezza IP

Di seguito sono riportate alcune delle funzioni dipendenti da SISF:

- Ispezione NDP: ispeziona messaggi NDP IPv6
- nDP address-gleaning:popolare la tabella di binding con informazioni glean mediante snooping del traffico NDP
- Tracciamento dei dispositivi: monitoraggio dell'attività dei dispositivi finali, anche tramite un meccanismo di vivacità
- Snooping: cancella gli indirizzi nei messaggi NDP, ARP e DHCP. Blocca messaggi non autorizzati
- Inoltro DHCPv4: inoltra il pacchetto trasmesso DHCP all'indirizzo dell'helper configurato.
- Soppressione multicast NDP e ARP: i messaggi NDP multicast vengono soppressi convertendo in unicast in risposta per conto delle destinazioni.
- Proxy DAD:rilevamento indirizzi duplicati e invio di ND per conto del client di destinazione
- DHCPv4 Require: impone al client di ottenere l'indirizzo IP solo tramite DHCP

Avvertenze SISF

Alcuni dei comportamenti più frequenti osservati relativi a SISF sono:

- Il SISF può essere abilitato abilitando altre funzioni, ad esempio lo snooping dhcp
- Il comportamento predefinito del probe SISF può influire sull'assegnazione degli indirizzi IP dei client.
- Quando il protocollo SISF è abilitato, è abilitato anche sulle porte uplink che possono

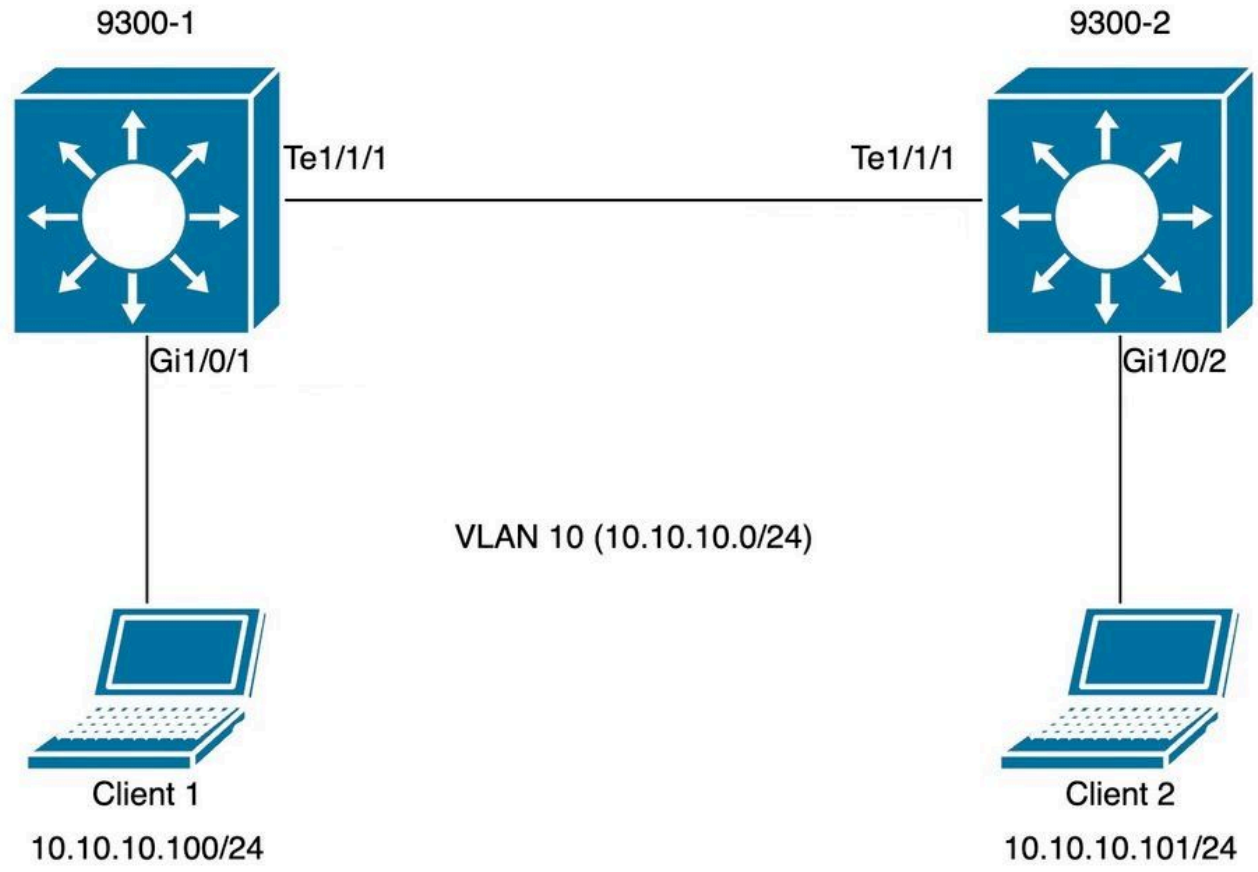
causare un impatto sulla rete.

Risoluzione dei problemi

Topologia

Il diagramma della topologia viene utilizzato nello scenario SISF successivo. Gli switch 9300 sono solo al layer 2 e NON dispongono di una SVI configurata nella Vlan client 10.

Nota: SISF è abilitato manualmente in questa esercitazione.



Configurazione

La configurazione SISF predefinita è stata configurata su entrambi gli switch 9300 con porte di accesso, mentre alle porte trunk è stato applicato un criterio personalizzato per illustrare gli output SISF previsti.

Switch 930-1:

```
<#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
```

Verifica

È possibile utilizzare questi comandi per convalidare i criteri applicati:

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

Switch 930-1:

<#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#
```

Scenari comuni

Errore di indirizzo IPv4 duplicato sul dispositivo host

Problema

La sonda keepalive inviata dallo switch è un controllo L2. Dal punto di vista dello switch, gli indirizzi IP utilizzati come origine negli ARP non sono importanti: questa funzione può essere utilizzata su dispositivi senza alcun indirizzo IP configurato, quindi l'origine IP di 0.0.0.0 non è rilevante. Quando l'host riceve questi messaggi, risponde e popola il campo relativo all'IP di destinazione con l'unico indirizzo IP disponibile nel pacchetto ricevuto, ossia il proprio indirizzo IP. Questo può causare falsi avvisi di indirizzi IP duplicati, perché l'host che risponde vede il proprio indirizzo IP sia come origine che come destinazione del pacchetto.

Si consiglia di configurare il criterio SISF in modo che utilizzi un'origine automatica per le relative sonde keepalive.

Nota: per ulteriori informazioni, vedere questo articolo sui problemi relativi agli indirizzi duplicati

---

Sonda predefinita

Questo è il pacchetto di sonda quando non è presente alcuna SVI locale e le impostazioni predefinite delle sonde:

<#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
```

Soluzione

Configurare il probe in modo che utilizzi un indirizzo diverso dal PC host per il probe. A tale scopo, è possibile utilizzare i seguenti metodi

Origine automatica per sonda "Keep-Alive"

Configurare una sorgente automatica per le sonde "keep-alive" per ridurre l'uso di 0.0.0.0 come IP di origine:

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

La logica di applicazione del comando auto-source è la seguente:

<#root>

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

<-- Optional parameter

1. Impostare l'origine su VLAN SVI, se presente.
2. Cercare una coppia di origine/MAC nella tabella di host IP per la stessa subnet. La sonda ha avuto origine dall'indirizzo MAC dell'interfaccia fisica dello switch + l'indirizzo IP di un altro host nella subnet già presente nel database.
3. Calcolare l'IP di origine dall'IP di destinazione con la mask e il bit dell'host forniti. La sonda viene generata dall'ascolto dell'IP del client e dalla creazione di una sonda nella subnet con gli ultimi bit configurati.

Nota: se il comando viene applicato con **<override>**, si passa sempre al passaggio 3.

Sonda modificata

L'impostazione della configurazione di fallback automatica dell'origine per l'utilizzo di un indirizzo IP nella subnet modifica la sonda. Poiché non è presente una SVI e non sono presenti altri client nella subnet, viene eseguito il fallback all'IP/Mask configurato nella configurazione.

<#root>

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

Questo è il pacchetto di richiesta modificato:

<#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
```

Ulteriori dettagli sul comportamento della sonda

Comando	Azione (Per selezionare l'indirizzo IP e MAC di origine per la sonda ARP di tracciamento del dispositivo)	Note
origine automatica rilevamento dispositivi	• Impostare source (Origine) su VLAN SVI, se presente. • Cercare l'associazione IP e MAC nella tabella di rilevamento dispositivi dalla stessa subnet. • Usa 0.0.0.0	È consigliabile disattivare la traccia dei dispositivi su tutte le porte trunk per evitare il flapping degli indirizzi MAC.
sostituzione origine automatica rilevamento dispositivi	• Impostare l'origine sulla VLAN SVI, se presente • Usa 0.0.0.0	Non consigliato in assenza di SVI.
device-tracking auto-source fallback <IP> <MASK>	• Impostare source (Origine) su VLAN SVI, se presente. • Cercare l'associazione IP e MAC nella tabella di	È consigliabile disattivare la traccia dei dispositivi su tutte le porte trunk per evitare il flapping degli indirizzi MAC. L'indirizzo IPv4 calcolato non

	rilevamento dispositivi dalla stessa subnet. • Calcolare l'indirizzo IP di origine dall'indirizzo IP del client utilizzando il bit host e la maschera forniti. L'indirizzo MAC di origine viene ricavato dall'indirizzo MAC della porta dello switch rivolta verso il client.	deve essere assegnato ad alcun client o dispositivo di rete.
override <IP> <MASK> di fallback <IP> di rilevamento dell'origine automatica	• Impostare source (Origine) su VLAN SVI, se presente. • Calcolare l'indirizzo IP di origine dall'indirizzo IP del client utilizzando il bit host e la maschera forniti. L'indirizzo MAC di origine viene ricavato dall'indirizzo MAC della porta dello switch rivolta verso il client.	L'indirizzo IPv4 calcolato non deve essere assegnato ad alcun client o dispositivo di rete.

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

A seconda dell'indirizzo IP dell'host, è necessario riservare un indirizzo IPv4.

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

Nota: si tratta di una formula booleana

Esempio.

Se si utilizza il comando:

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

IP host = 10.152.140.25

IP = 0.0.0.1

maschera = 24

Consente di suddividere la formula booleana in due parti.

1. Funzionamento: 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. Funzionamento 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 riservato = 10.152.140.1

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

Nota: l'indirizzo utilizzato come origine IP deve essere escluso dai binding DHCP per la subnet.

Errore indirizzo IPv6 duplicato

Problema

Errore di indirizzo IPv6 duplicato quando IPv6 è abilitato nella rete e un'interfaccia virtuale commutata (SVI) è configurata su una VLAN.

In un pacchetto DAD IPv6 normale, il campo Source Address nell'intestazione IPv6 è impostato sull'indirizzo non specificato (0:0:0:0:0:0:0:0). Simile al caso IPv4.

L'ordine per la scelta dell'indirizzo di origine nel probe SISF è il seguente:

- Indirizzo locale del collegamento della SVI, se configurato
- Usa 0:0:0:0:0:0:0:0

Soluzione

Si consiglia di aggiungere i comandi successivi alla configurazione SVI. Questo consente alla SVI di acquisire automaticamente un indirizzo locale del collegamento; questo indirizzo viene utilizzato come indirizzo IP di origine della sonda SISF, evitando così il problema dell'indirizzo IP duplicato.

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

Maggiore utilizzo della memoria e della CPU

Problema

La sonda "keepalive" inviata dallo switch viene trasmessa a tutte le porte quando è attivata a livello di programmazione. Gli switch collegati nello stesso dominio L2 inviano queste trasmissioni ai loro host. Di conseguenza, lo switch di origine aggiunge host remoti al proprio database di rilevamento dispositivi. Le voci host aggiuntive aumentano l'utilizzo della memoria sul dispositivo e il processo di aggiunta degli host remoti aumenta l'utilizzo della CPU del dispositivo.

È consigliabile definire l'ambito della policy a livello di programmazione configurando una policy sull'uplink sugli switch collegati in modo da definire la porta come attendibile e collegata a uno switch.

Nota: le funzionalità dipendenti da SISF, come lo snooping DHCP, consentono al SISF di funzionare correttamente e possono causare il problema.

Soluzione

Configurare una policy sull'uplink (trunk) per interrompere le richieste e l'apprendimento degli host remoti che amano altri switch (il protocollo SISF è necessario solo per mantenere una tabella host locale)

<#root>

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

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

Tempo di raggiungibilità di Tracciamento dispositivi troppo breve

Problema

A causa di un problema di migrazione dal rilevamento dei dispositivi basato su IPDT a SISF, talvolta viene introdotto un tempo di raggiungibilità non predefinito durante la migrazione da versioni precedenti a 16.x e successive.

Soluzione

Si consiglia di ripristinare il tempo raggiungibile predefinito configurando:

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

Switch integrati nello strumento Meraki (aumento della CPU e scaricamenti delle porte)

Problema

Quando si collegano gli switch allo strumento Meraki Cloud Monitoring, questo strumento spinge le policy personalizzate di monitoraggio dei dispositivi.

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

Il criterio viene applicato a tutte le interfacce senza distinzione, ovvero non distingue tra porte perimetrali e porte trunk collegate ad altri dispositivi di rete (ad esempio switch, firewall, router e così via). Lo switch può creare diverse voci SISF sulle porte trunk in cui è configurato MERAKI_POLICY, causando svuotamenti su queste porte e un aumento dell'utilizzo della 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
```

Soluzione

Imposta il criterio successivo su tutte le interfacce non edge:

```
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
```

Indirizzi IP con lo stesso MAC non presenti nella tabella SISF

Problema

Questo scenario è comune negli accessori in modalità HA (alta disponibilità) con indirizzi IP diversi, ma con lo stesso indirizzo MAC. Si osserva anche in ambienti VM che condividono la stessa condizione (indirizzo MAC singolo per due o più indirizzi IP). Questa condizione impedisce la connettività di rete a tutti gli IP per cui non è presente una voce nella tabella SISF quando è attivo il criterio SISF personalizzato in modalità guardia.Per la funzionalità SISF, viene appreso un solo IP per indirizzo MAC.

Nota: questo problema è presente nella release 17.7.1 e successive

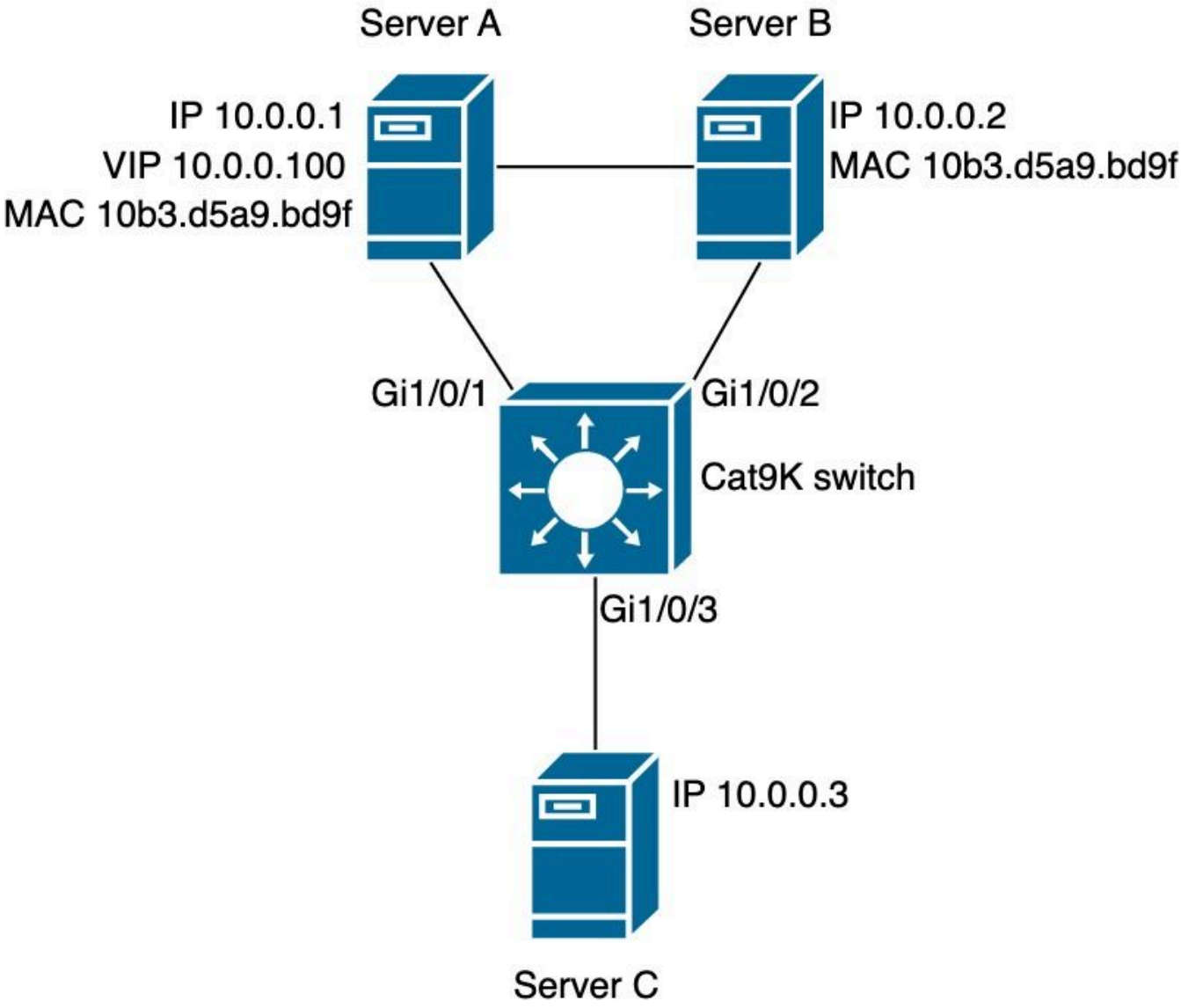
---

Esempio:

- IP 10.0.0.1 con indirizzo MAC 10b3.d5a9.bd9f viene appreso sulla tabella SISF e gli viene

consentito di comunicare con il dispositivo di rete 10.0.0.3.

- Tuttavia, il secondo IP 10.0.0.2 e l'IP virtuale 10.0.0.100 che condividono l'indirizzo MAC 10b3.d659.7858 non sono programmati nella tabella SISF e la comunicazione con la rete non è consentita.



politica 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
```

Database 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
```

Server di prova della raggiungibilità 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 di raggiungibilità del server 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)
```

Convalida dei rilasci sullo switch in corso.

<#root>

```
switch(config)#
```

device-tracking logging

Log

<#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

Soluzione

Opzione 1: la rimozione del criterio IPDT dalla porta consente di raggiungere i pacchetti ARP e i dispositivi interessati

<#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

Opzione 2: rimuovere la spaziatura arp del protocollo dal criterio di rilevamento dispositivi.

<#root>

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

no protocol arp

Opzione 3: modificare il livello di protezione di IPDT_POLICY in modo che sia deformato.

<#root>

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

security-level glean

Informazioni correlate

- Guida alla configurazione della sicurezza, Cisco IOS XE Bengaluru 17.6.x (switch Catalyst 9300): configurazione delle funzionalità di sicurezza integrate nello switch
- Guida alla configurazione della sicurezza, Cisco IOS XE Cupertino 17.9.x (switch Catalyst 9300): configurazione delle funzionalità di sicurezza integrate nello switch
- White paper sulle funzioni di sicurezza integrate (SISF) degli switch della famiglia Cisco Catalyst 9000
- ID bug Cisco CSCvx75602 - Perdita di memoria SISF in AR-relay e soppressione di ND
- ID bug Cisco CSCwf33293 - [EVPN SISF] Metodo personalizzato richiesto per modificare i valori degli indirizzi limite per IPv4/V6 con EVPN + DHCP
- Cisco bug ID CSCvq22011 - IOS-XE rifiuta la risposta ARP quando IPDT si illumina da ARP
- ID bug Cisco CSCwc20488 - Limitazione di 255 pseudo porte per vlan/evi
- Cisco bug ID CSCwh52315 - lo switch 9300 rifiuta la risposta ARP quando nella porta è presente un criterio IPDT
- Cisco bug ID CSCvd51480 - Rimozione del binding dallo snooping ip dhcp e rilevamento dispositivi

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).