Catalyst 9000シリーズスイッチのSISFのトラブルシューティング

内容

はじめに

このドキュメントでは、Catalyst 9000ファミリスイッチで使用されるスイッチ統合型セキュリティ機能(SISF)について説明します。 また、SISFの使用方法や、他の機能との相互対話についても説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco IOS® XE 17.3.xが稼働するCisco Catalyst 9300-48Pに基づくものです

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

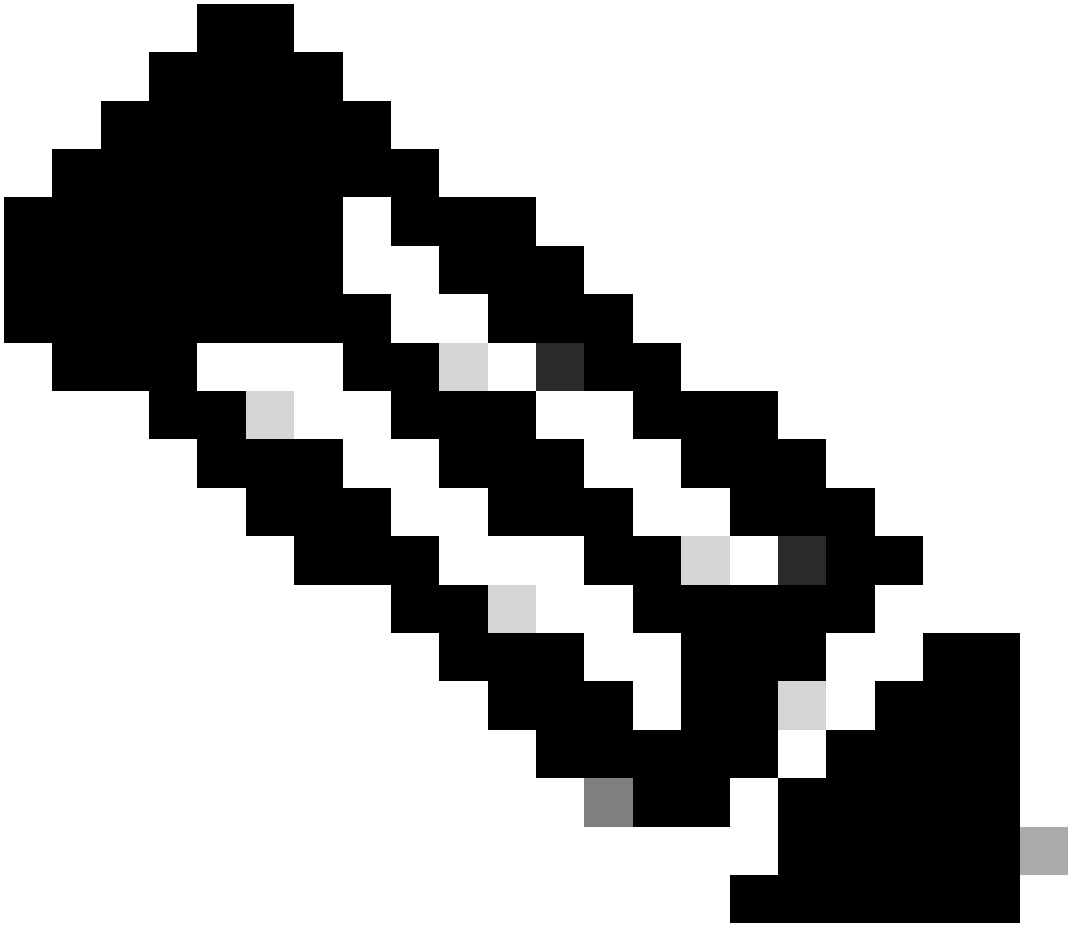
注：シスコの他のプラットフォームでこれらの機能を有効にするために使用されるコマンドについては、該当するコンフィギュレーション ガイドを参照してください。

関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

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

Cisco IOS XEソフトウェアバージョン17.3.4以降



注：このドキュメントは、SISFとデバイストラッキングを使用するほとんどのCisco IOS XEバージョンにも適用されます。

背景説明

概要

SISFはホストバインディングテーブルを提供し、その情報を使用する機能クライアントがあります。エントリは、DHCP、ARP、ND、RAなどのパケットを収集してテーブルに入力されます。収集されたパケットは、ホストのアクティビティを追跡し、テーブルの動的な入力に役立ちます。L2ドメインにサイレントホストがある場合は、スタティックエントリを使用してSISFテーブルにエントリを追加できます。

SISFは、ポリシーモデルを使用して、スイッチのデバイスのロールと追加設定を設定します。単一のポリシーをインターフェイスまたはVLANレベルで適用できます。ポリシーがVLANに適用されていて、別のポリシーがインターフェイスに適用されている場合、インターフェイスポリシー

が優先されます。

SISFを使用してテーブルに含まれるホスト数を制限することもできますが、IPv4とIPv6の動作には違いがあります。SISF制限が設定され、制限に達した場合：

- IPv4ホストは引き続き動作しますが、この制限を超えるエントリはSISFテーブルに追加されません
- SISFテーブルに登録されていないIPv6ホストはネットワークへの参加を許可されず、新しいエントリはSISFテーブルに追加されません。

16.9.x以降のリリースでは、SISFクライアント機能の優先度が導入されています。SISFへのアップデートを制御するオプションが追加され、2つ以上のクライアントがバインディングテーブルを使用している場合は、より優先度の高い機能からのアップデートが適用されます。 ここでの例外は、「macごとのIPv4//IPv6のアドレス数を制限する」設定であり、優先順位が最も低いポリシーの設定が有効です。

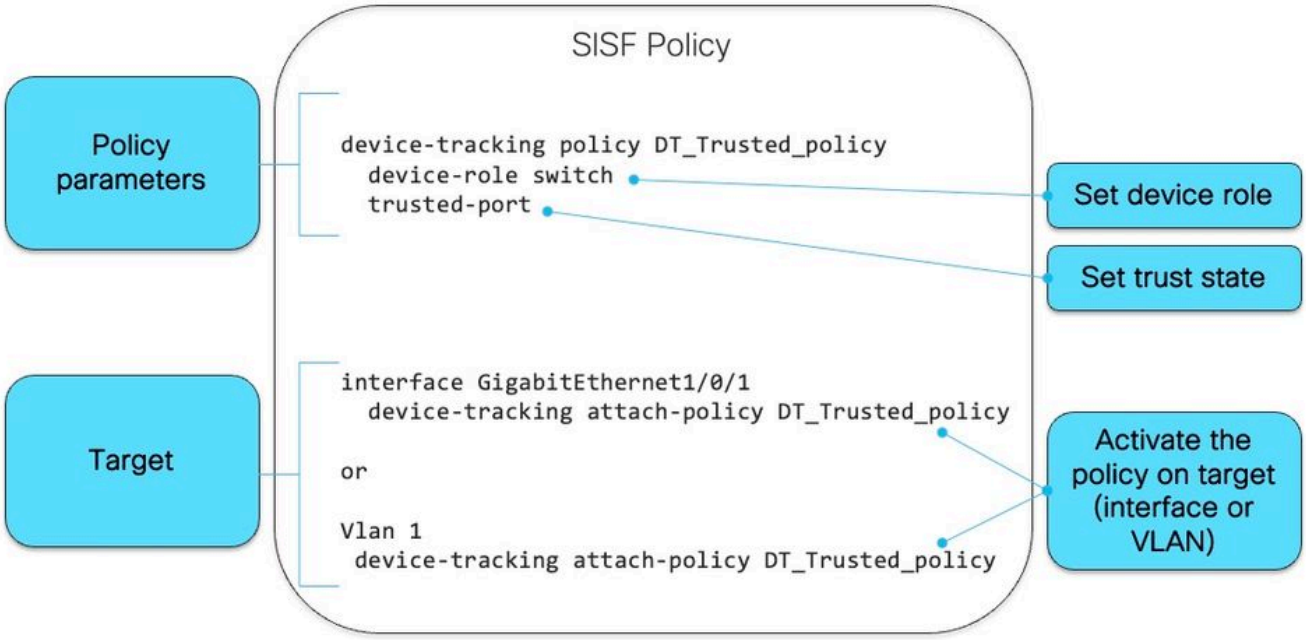
デバイストラッキングを有効にする必要がある機能の例を次に示します。

- LISP/EVPN
- Dot1x
- Web認証
- CTS
- DHCP スヌーピング

注：ポリシー設定の選択にはプライオリティが使用されます。

CLIから作成されたポリシーは最も高い優先順位(128)を持つため、ユーザはプログラマティックポリシーとは異なるポリシー設定を適用できます。カスタマイズされたポリシーの下で設定可能なすべての設定は、手動で変更できます。

次の図は、SISFポリシーの例とその読み方です。



ポリシー内のprotocolキーワードの下には、SISFデータベースの入力に使用されるパケットのタイプを確認するオプションがあります。

<#root>

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

?

device-tracking policy configuration mode:
  data-glean            binding recovery by data traffic source address
                        gleaning
  default               Set a command to its defaults
  destination-glean     binding recovery by data traffic destination address
                        gleaning
  device-role           Sets the role of the device attached to the port
  distribution-switch   Distribution switch to sync with
  exit                  Exit from device-tracking policy configuration mode
  limit                 Specifies a limit
  medium-type-wireless  Force medium type to wireless
  no                    Negate a command or set its defaults
  prefix-glean          Glean prefixes in RA and DHCP-PD traffic


protocol              Sets the protocol to glean (default all) <--

  security-level        setup security level
  tracking              Override default tracking behavior
  trusted-port          setup trusted port
  vpc                   setup vpc port

switch(config-device-tracking)#

protocol ?

  arp    Glean addresses in ARP packets
  dhcp4  Glean addresses in DHCPv4 packets
  dhcp6  Glean addresses in DHCPv6 packets
```

```
  ndp    Glean addresses in NDP packets
  udp    Gleaning from UDP packets
```

SISFのプログラム機能とクライアント機能

次の表に示す機能は、有効になったときにSISFをプログラムで有効にするか、SISFのクライアントとして機能します。

SISFプログラム機能	SISFクライアントの機能
VLAN上のLISP	Dot1x
VLAN上のEVPN	Web認証
DHCP スヌーピング	CTS

SISFを有効にする機能が設定されていないデバイスでSISFクライアント機能を有効にする場合は、ホストに接続するインターフェイスでカスタムポリシーを設定する必要があります。

SISF情報を使用するIPv4機能

- CTS
- IEEE 802.1x
- LISP
- EVPN
- DHCPスヌーピング（SISFのみをアクティブ化し、使用しない）
- IP ソース ガード

SISF情報を使用するIPv6機能

- IPv6ルータアドバタイズメント(RA)ガード
- IPv6 DHCPガード、レイヤ2 DHCPリレー
- IPv6重複アドレス検出(DAD)プロキシ
- フラッディング抑制
- IPv6 ソース ガード
- IPv6宛先ガード
- RAスロットル
- IPv6プレフィックスガード

デバイストラッキング

デバイストラッキングの主な役割は、ネットワーク内のエンドノードの存在、位置、および移動を追跡することです。SISFは、スイッチが受信したトラフィックをスヌーピングし、デバイスID（MACおよびIPアドレス）を抽出して、バインディングテーブルに保存します。 IEEE 802.1X、Web認証、Cisco TrustSec、LISPなどの多くの機能は、適切に動作するためにこの情報の精度に依存しています。 SISFベースのデバイストラッキングは、IPv4とIPv6の両方をサポートしています。 クライアントがIPを学習する方法として、次の5つの方法がサポートされています。

- DHCPv4
- DHCPv6
- ARP
- NDP
- データ収集

ポートチャネル上のSISF

ポートチャネル（またはイーサチャネル）でのデバイストラッキングがサポートされています。ただし、設定は個々のポートチャネルメンバーではなく、チャネルグループに適用する必要があります。バインディングの観点から表示される（既知の）唯一のインターフェイスはポートチャネルです。

プローブとデータベースのチューニング

Probe:

- IPDTでは、最初のプローブを10秒間遅らせてアドレスの重複の問題に対処するコマンドがありました。リンクアップ時の「ip device tracking probe delay」。
- SISFには、最初のプローブを送信する前に待機する待機タイマーがすでに組み込まれています。これは設定できず、同じ問題を解決します。これはSISFコード内にあるため、このコマンドは不要です

データベース:

SISFでは、エントリがデータベースに保持される期間を制御するために、いくつかのオプションを設定できます。

<#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)

IPデバイストラッキング

ホストがポーリングされるエントリのライフサイクル：

- SISFはMACごとにIPv4/IPv6バインディングを維持し、IPラーニングが成功するとバインディングがREACHABLE状態に移行します
- SISFは、制御パケットを監視してクライアントの活性を追跡
- クライアントから制御パケットがない状態が5分間続くと、バインディングがVERIFY状態に移行し、プローブがクライアントに送信されます
- クライアントがプローブに応答しない場合、バインディングはSTALE状態に移行し、それ以外はREACHABLE状態になります
- STALEエントリのデフォルトのタイムアウトは24時間で、設定可能
- 古いエントリは24時間後に削除されます（またはタイムアウト値が設定されています）。

盗難検知

ノード変換のタイプ：

- IP窃盗（同じIP、異なるMAC、異なる/同じポート）
- MAC窃盗（同じMAC、異なるIP、異なるポート）
- MAC IP窃盗（同じMAC、同じIP、異なるポート）

IPセキュリティ機能

SISFに依存する機能の一部を次に示します。

- NDPインスペクション：IPv6 NDPメッセージを検査します。
- NDPアドレス収集：NDPトラフィックをスヌーピングして、バインディングテーブルに情報を収集します。
- デバイストラッキング：一部の活性メカニズムを介したエンドデバイスのアクティビティの監視
- スヌーピング：NDP、ARP、およびDHCPメッセージ内のアドレスを収集します。許可されていないメッセージをブロックする
- DHCPv4リレー：DHCPブロードキャストされたパケットを、設定されたヘルパーアドレスにリレーします。
- NDPおよびARPマルチキャストの抑制：マルチキャストNDPメッセージを抑制するには、ユニキャストに変換するか、ターゲットの代わりに応答します。
- DADプロキシ：重複アドレス検出とターゲットクライアントのNA送信
- DHCPv4 Require:クライアントがDHCPによってのみIPを取得するように強制します。

SISFの警告

SISFに関連して最もよく見られる動作は次のとおりです。

- SISFは、dhcpスヌーピングなどの他の機能を有効にすることで有効にできます
- SISFのデフォルトのプローブ動作は、クライアントのIPアドレス割り当てに影響を与える可能性があります。

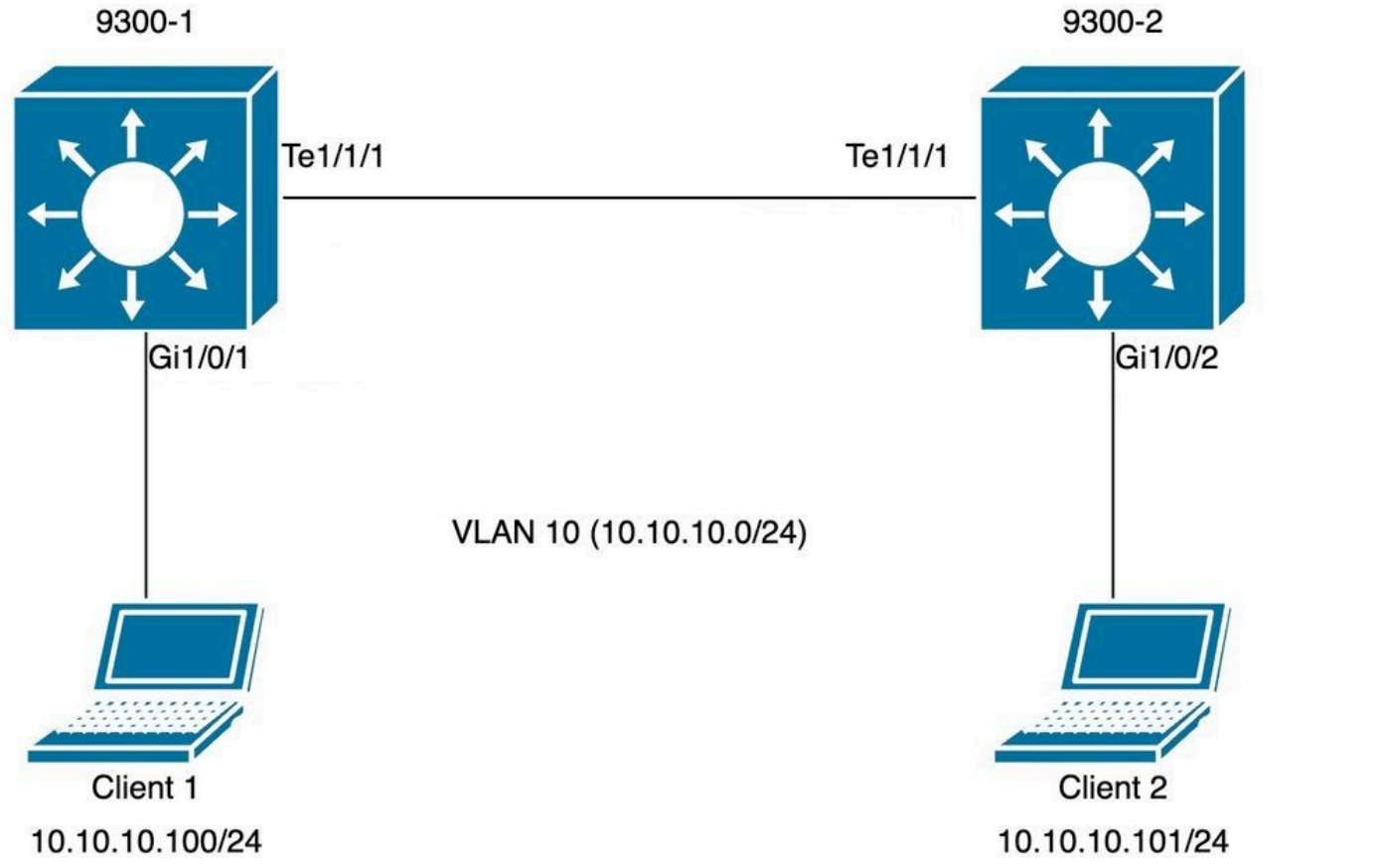
- SISFを有効にすると、アップリンクポートでも有効になり、ネットワークに影響を与えることがあります。

トラブルシュート

トポロジ

トポロジダイアグラムは、次のSISFシナリオで使用されます。9300スイッチはレイヤ2専用であり、クライアントVlan 10ではSVIが設定されていません。

注：この実習では、SISFは手動で有効にします。



コンフィギュレーション

デフォルトのSISF設定は、アクセスポートに面した両方の9300スイッチで設定されていましたが、予想されるSISF出力を示すために、カスタムポリシーがトランクポートに適用されました。

スイッチ 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
```

スイッチ 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
```

検証

次のコマンドを使用して、適用されたポリシーを検証できます。

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

スイッチ 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#
```

スイッチ 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#
```

一般的なシナリオ

ホストデバイスでのIPv4アドレスの重複エラー

問題

スイッチから送信される「キープアライブ」プローブはL2チェックです。スイッチから見ると、ARPの送信元として使用されるIPアドレスは重要ではありません。この機能は、IPアドレスがまったく設定されていないデバイスで使用できるため、0.0.0.0のIP送信元は該当しません。 ホストはこのメッセージを受信すると、応答して受信パケットに使用できる IP アドレス (自身の IP アドレス) のみを宛先 IP フィールドに入力します。これにより、重複IPアドレスの誤ったアラートが発生する可能性があります。これは、応答するホストが自身のIPアドレスをパケットの送信元と宛先の両方として認識するためです。

キープアライブプローブに自動ソースを使用するようにSISFポリシーを設定することを推奨します。

注：詳細については、重複アドレスの問題に関するこの記事を参照してください

デフォルトプローブ

これは、ローカルSVIが存在しない場合のプローブパケットと、デフォルトのプローブ設定です。

<#root>

```
Ethernet II,

Src: c0:64:e4:cc:66:02 (c0:64:e4:cc:66:02)

, Dst: Cisco_76:63:c6 (00:41:d2:76:63:c6)

<-- Probe source MAC is the BIA of physical interface connected to client

    Destination: Cisco_76:63:c6 (00:41:d2:76:63:c6)
        Address: Cisco_76:63:c6 (00:41:d2:76:63:c6)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)

    Source: c0:64:e4:cc:66:02 (c0:64:e4:cc:66:02)

        Address: c0:64:e4:cc:66:02 (c0:64:e4:cc:66:02)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)

    Type: ARP (0x0806)

    Padding: 000000000000000000000000000000000000
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: c0:64:e4:cc:66:02 (c0:64:e4:cc:66:02)

    Sender IP address: 0.0.0.0                                  <-- Sender IP is 0.0.0.0 (default)

    Target MAC address: Cisco_76:63:c6 (00:41:d2:76:63:c6)

    Target IP address: 10.10.10.101                             <-- Target IP is client IP
```

解決方法

プローブにホストPC以外のアドレスを使用するようにプローブを設定します。これは、次の方法で実行できます

「キープアライブ」プローブの自動ソース

「キープアライブ」プローブの自動ソースを設定し、送信元IPとしての0.0.0.0の使用を減らします。

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

auto-sourceコマンドを適用する場合のロジックは、次のようになります。

<#root>

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

1. VLAN SVI に送信元を設定します（存在する場合）。
2. 同じサブネットの IP ホスト テーブルで送信元と MAC のペアを検索します。 プローブの送信元は、スイッチの物理インターフェイスMACと、データベースにすでに存在するサブネット内の他のホストのIPです。
3. ホスト ビットとマスクが指定された宛先 IP から送信元 IP を計算します。プローブは、クライアントIPをヒアリングし、最後のビットが設定されたサブネット内にプローブを作成することによって生成されます。

注：コマンドが<override>を指定して適用されている場合は、必ず手順3に進みます。

修正プローブ

サブネットでIPを使用するようにauto-source fallback configを設定すると、プローブが変更されます。サブネット上にSVIと他のクライアントがないため、設定で設定したIP/マスクにフォールバックします。

<#root>

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

変更されたプローブパケットを次に示します。

<#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
```

プローブ動作の詳細

コマンド	アクション （デバイストラッキングARPプローブの送信元IPおよびMACアドレスを選択するため）	注意事項
デバイストラッキングの自動ソース	• 送信元をVLAN SVIに設定します（存在する場合）。 • 同じサブネットのデバイストラッキングテーブルでIPとMACのバインディングを探します。 • 0.0.0.0を使用	MACフラッピングを回避するために、すべてのトランクポートでデバイストラッキングを無効にすることを推奨します。
デバイストラッキングの自動ソースオーバーライド	• VLAN SVIがある場合は送信元を設定 • 0.0.0.0を使用	SVIがない場合は推奨されません。
device-tracking auto-source fallback <IP> <MASK>	• 送信元をVLAN SVIに設定します（存在する場合）。 • 同じサブネットのデバイストラッキングテーブルでIPとMACのバインディ	MACフラッピングを回避するために、すべてのトランクポートでデバイストラッキングを無効にすることを推奨します。 計算されたIPv4アドレスをクライアントまたはネットワークデ

	ングを探します。 • 指定されたホストビットとマスクを使用して、クライアントIPから送信元IPを計算します。送信元MACは、クライアントに面しているスイッチポートのMACアドレスから取得されます。	バイスに割り当てることはできません。
device-tracking auto-source fallback <IP> <MASK>の上書き	• 送信元をVLAN SVIに設定します (存在する場合) 。 • 指定されたホストビットとマスクを使用して、クライアントIPから送信元IPを計算します。送信元MACは、クライアントに面しているスイッチポートのMACアドレスから取得されます。	計算されたIPv4アドレスをクライアントまたはネットワークデバイスに割り当てることはできません。

device-tracking auto-source fallback <IP> <MASK> [override]コマンドの説明：

ホストIPに応じて、IPv4アドレスを予約する必要があります。

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

注：これはブール式です

例：

次のコマンドを使用します。

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

ホストIP = 10.152.140.25

IP = 0.0.0.1

マスク= 24

ブール式を2つの部分に分割します。

1. 10.152.140.25および255.255.255.0の動作：

```
10.152.140.25 = 00001010.10011000.10001100.00011001
                              AND
255.255.255.0 = 11111111.11111111.11111111.00000000
                            RESULT
10.152.140.0  = 00001010.10011000.10001100.00000000
```

2. 10.152.140.0または0.0.0.1の動作：

```
10.152.140.0  = 00001010.10011000.10001100.00000000
                              OR
0.0.0.1       = 00000000.00000000.00000000.00000001
                            RESULT
10.152.140.1  = 00001010.10011000.10001100.00000001
```

予約済みIP = 10.152.140.1

予約済みIP = （10.152.140.25および255.255.255.0）| (0.0.0.1) = 10.152.140.1

注:IP送信元として使用されるアドレスは、サブネットのDHCPバインディングからスコープを絞る必要があります。

IPv6アドレスの重複エラー

問題

Duplicate IPv6 address」エラーが発生する場合があります。

通常のIPv6 DADパケットでは、IPv6ヘッダーのSource Addressフィールドは未指定アドレス(0:0:0:0:0:0:0:0)に設定されます。IPv4の場合と同様です。

SISFプローブで送信元アドレスを選択する順序は次のとおりです。

- SVIのリンクローカルアドレス（設定されている場合）
- 0:0:0:0:0:0:0:0を使用

解決方法

次のコマンドをSVI設定に追加することを推奨します。これにより、SVIはリンクローカルアドレスを自動的に取得できます。このアドレスはSISFプローブの送信元IPアドレスとして使用され、

重複IPアドレスの問題を回避できます。

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

メモリおよびCPU使用率の向上

問題

スイッチから送信される「キープアライブ」プローブは、プログラム的に有効にされると、すべてのポートからブロードキャストされます。 同じL2ドメイン内の接続されたスイッチは、これらのブロードキャストをホストに送信します。その結果、発信元スイッチはデバイス追跡データベースにリモートホストを追加します。 ホストエントリを追加すると、デバイスのメモリ使用量が増加し、リモートホストを追加するプロセスによってデバイスのCPU使用率が増加します。

接続されたスイッチへのアップリンクにポリシーを設定して、信頼できるポートとして定義し、スイッチに接続されたポートとして定義することで、プログラムポリシーの範囲を設定することを推奨します。

注:DHCPスヌーピングなどのSISF従属機能によってSISFが適切に動作し、この問題を引き起こす可能性があることに注意してください。

解決方法

アップリンク（トランク）にポリシーを設定し、他のスイッチを必要とするリモートホストのプローブと学習を停止します(SISFはローカルホストテーブルの維持にのみ必要です)

<#root>

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

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

DT_trunk_policy

デバイストラッキングの到達可能時間が短すぎる

問題

IPDTからSISFベースのデバイストラッキングへの移行の問題により、古いリリースから16.x以降

のリリースに移行する際に、デフォルト以外の到達可能時間が導入されることがあります。

解決方法

次のように設定して、デフォルトの到達可能時間に戻すことをお勧めします。

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

Merakiツールにオンボーディングされたスイッチ (CPUの増加とポートフラッシュ)

問題

スイッチがMerakiクラウド監視ツールにオンボーディングされると、このツールがカスタムデバイストラッキングポリシーをプッシュします。

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

ポリシーはすべてのインターフェイスに区別なく適用されます。つまり、エッジポートと、他のネットワークデバイス (スイッチ、ファイアウォールルータなど) に面しているトランクポートとを区別しません。スイッチは、MERAKI_POLICYが設定されているトランクポートに複数のSISFエントリを作成できるため、これらのポートでのフラッシュやCPU使用率の増加を引き起こします。

<#root>

```
switch#
```

show interfaces port-channel 5

```
Port-channel5 is up, line protocol is up (connected)
<omitted output>
  Input queue: 0/2000/0/
```

112327

```
 (size/max/drops/
```

flushes

```
); Total output drops: 0
```

<-- we have many flushes

```
<omitted output>
```

```
switch#

show process cpu sorted

CPU utilization for five seconds: 26%/2%; one minute: 22%; five minutes: 22%
PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process

572     1508564      424873       3550 11.35%  8.73%  8.95%   0 SISF Main Thread

105      348502      284345       1225  2.39%  2.03%  2.09%   0 Crimson flush tr
```

解決方法

すべての非エッジインターフェイスで次のポリシーを設定します。

```
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
```

SISFテーブルにない同じMACを持つIPアドレス

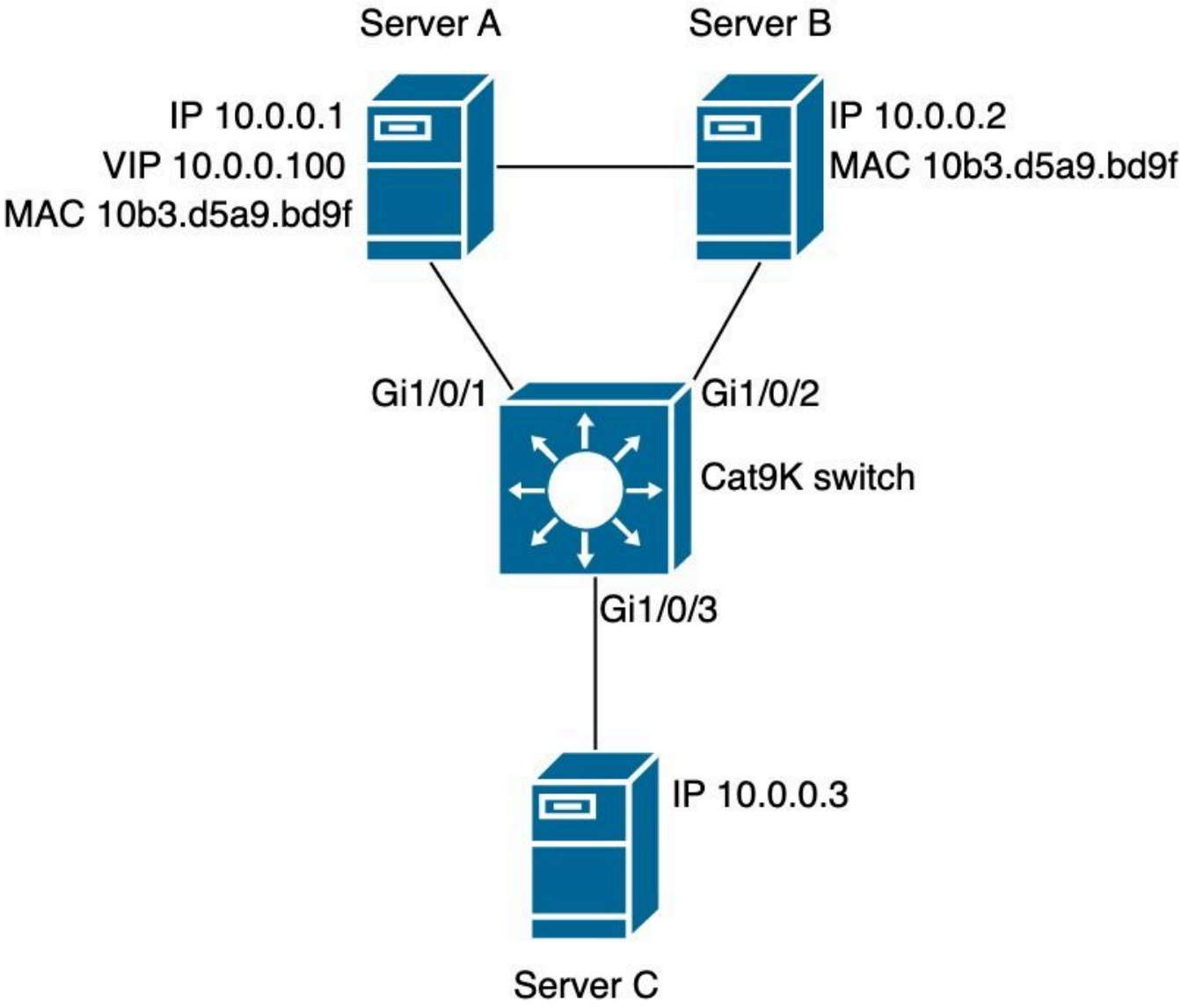
問題

このシナリオは、異なるIPアドレスを持つが同じMACアドレスを共有するHA（ハイアベイラビリティ）モードのアプライアンスで共通です。また、同じ条件を共有するVM環境（2つ以上のIPアドレスに対して1つのMACアドレス）でも発生します。この状況が発生すると、ガードモードのカスタムSISFポリシーが設定されている場合に、SISFテーブルにエントリがないすべてのIPへのネットワーク接続が妨げられます。SISF機能により、MACアドレスごとに1つのIPだけが学習されます。

注：この問題は、17.7.1以降のリリースに存在します

以下に例を挙げます。

- MACアドレス10b3.d5a9.bd9fのIP 10.0.0.1はSISFテーブルで学習され、ネットワークデバイス10.0.0.3との通信が許可されます。
- ただし、MACアドレス10b3.d659.7858を共有する2番目のIP 10.0.0.2と仮想IP 10.0.0.100はSISFテーブルにプログラムされていないため、ネットワークとの通信は許可されません。



SISFポリシー

<#root>

```
switch#

show run | sec IPDT_POLICY

device-tracking policy IPDT_POLICY
 no protocol udp
 tracking enable

switch#

show device-tracking policy IPDT_POLICY

Device-tracking policy IPDT_POLICY configuration:

  security-level guard <-- default mode

  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
```

```
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  tracking enable
Policy IPDT_POLICY is applied on the following targets:
Target               Type  Policy               Feature        Target range

Gi1/0/1              PORT  IPDT_POLICY          Device-tracking vlan all
Gi1/0/2              PORT  IPDT_POLICY          Device-tracking vlan all
```

SISFデータベース

<#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
```

到達可能性テストサーバ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
.....
```

到達可能性テストサーバ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)

スイッチのドロップを検証しています。

<#root>

switch(config)#

device-tracking logging

ログ

<#root>

switch#

show logging

<omitted output>
%SISF-4-PAK_DROP: Message dropped

IP=10.0.0.100 VLAN=10 MAC=10b3.d5a9.bd9f

I/F=Gi1/0/1

P=ARP Reason=Packet accepted but not forwarded
%SISF-4-PAK_DROP: Message dropped

IP=10.0.0.100 VLAN=10 MAC=10b3.d5a9.bd9f

I/F=Gi1/0/1

P=ARP Reason=Packet accepted but not forwarded
%SISF-4-PAK_DROP: Message dropped

IP=10.0.0.100 VLAN=10 MAC=10b3.d5a9.bd9f

I/F=Gi1/0/1

P=ARP Reason=Packet accepted but not forwarded
%SISF-4-PAK_DROP: Message dropped

IP=10.0.0.100 VLAN=10 MAC=10b3.d5a9.bd9f

I/F=Gi1/0/1

P=ARP Reason=Packet accepted but not forwarded
%SISF-4-PAK_DROP: Message dropped

IP=10.0.0.100 VLAN=10 MAC=10b3.d5a9.bd9f

I/F=Gi1/0/1

P=ARP Reason=Packet accepted but not forwarded
<omitted output>
%SISF-4-PAK_DROP: Message dropped

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

I/F=Gi1/0/2

P=ARP Reason=Packet accepted but not forwarded
%SISF-4-MAC_THEFT:

MAC Theft IP=10.0.0.2 VLAN=10 MAC=10b3.d5a9.bd9f IF=Gi1/0/1 New I/F=Gi1/0/2

%SISF-4-PAK_DROP: Message dropped

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

I/F=Gi1/0/2

P=ARP Reason=Packet accepted but not forwarded
%SISF-4-MAC_THEFT:

MAC Theft IP=10.0.0.2 VLAN=10 MAC=10b3.d5a9.bd9f IF=Gi1/0/1 New I/F=Gi1/0/2

%SISF-4-PAK_DROP: Message dropped

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

I/F=Gi1/0/2

P=ARP Reason=Packet accepted but not forwarded
%SISF-4-MAC_THEFT:

MAC Theft IP=10.0.0.2 VLAN=10 MAC=10b3.d5a9.bd9f IF=Gi1/0/1 New I/F=Gi1/0/2

%SISF-4-PAK_DROP: Message dropped

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

```
I/F=Gi1/0/2

 P=ARP Reason=Packet accepted but not forwarded
%SISF-4-MAC_THEFT:

MAC Theft IP=10.0.0.2 VLAN=10 MAC=10b3.d5a9.bd9f IF=Gi1/0/1 New I/F=Gi1/0/2


%SISF-4-PAK_DROP: Message dropped

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


I/F=Gi1/0/2

 P=ARP Reason=Packet accepted but not forwarded
%SISF-4-MAC_THEFT:

MAC Theft IP=10.0.0.2 VLAN=10 MAC=10b3.d5a9.bd9f IF=Gi1/0/1 New I/F=Gi1/0/2
```

解決方法

オプション1：ポートからIPDTポリシーを削除すると、ARPパケットと影響を受けるデバイスが到達可能になります

```
<#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
```

オプション2：デバイス追跡ポリシーからプロトコルARP収集を削除します。

```
<#root>

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

no protocol arp
```

オプション3: IPDT_POLICYのセキュリティレベルをgleanに変更します。

```
<#root>
```

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

security-level glean

関連情報

- セキュリティコンフィギュレーションガイド、Cisco IOS XE Bengaluru 17.6.x（Catalyst 9300スイッチ）：スイッチ統合セキュリティ機能の設定
- セキュリティコンフィギュレーションガイド、Cisco IOS XE Cuppertino 17.9.x（Catalyst 9300スイッチ）：スイッチ統合セキュリティ機能の設定
- Cisco Catalyst 9000ファミリスイッチ統合型セキュリティ機能(SISF)ホワイトペーパー
- Cisco Bug ID CSCvx75602:ARリレーとND抑制でのSISFメモリリーク
- Cisco Bug ID CSCwf33293:[EVPN SISF] EVPN + DHCPを使用するIPv4/V6の制限アドレス値を変更するために必要なカスタム方式
- Cisco Bug ID CSCvq22011 - IPDTがARPから情報を取得する際にIOS-XEがARP応答をドロップする
- Cisco Bug ID CSCwc20488:vlan/eviごとの255擬似ポートの制限
- Cisco Bug ID CSCwh52315:ポートにIPDTポリシーが設定されていると、9300スイッチがARP応答をドロップする
- Cisco Bug ID CSCvd51480 - ip dhcp snoopingとデバイストラッキングのバインド解除

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。