スイッチ統合セキュリティ機能の設定

SISF に関する情報

概要

スイッチ統合セキュリティ機能（SISF）は、レイヤ2ドメインのセキュリティを最適化するために開発されたフレームワークです。これは、IPデバイストラッキング（IPDT）と特定のIPv6ファーストホップ セキュリティ（FHS）機能の[1]を統合して、IPv4 から IPv6 スタックまたはデュアルスタックへの移行を簡素化します。

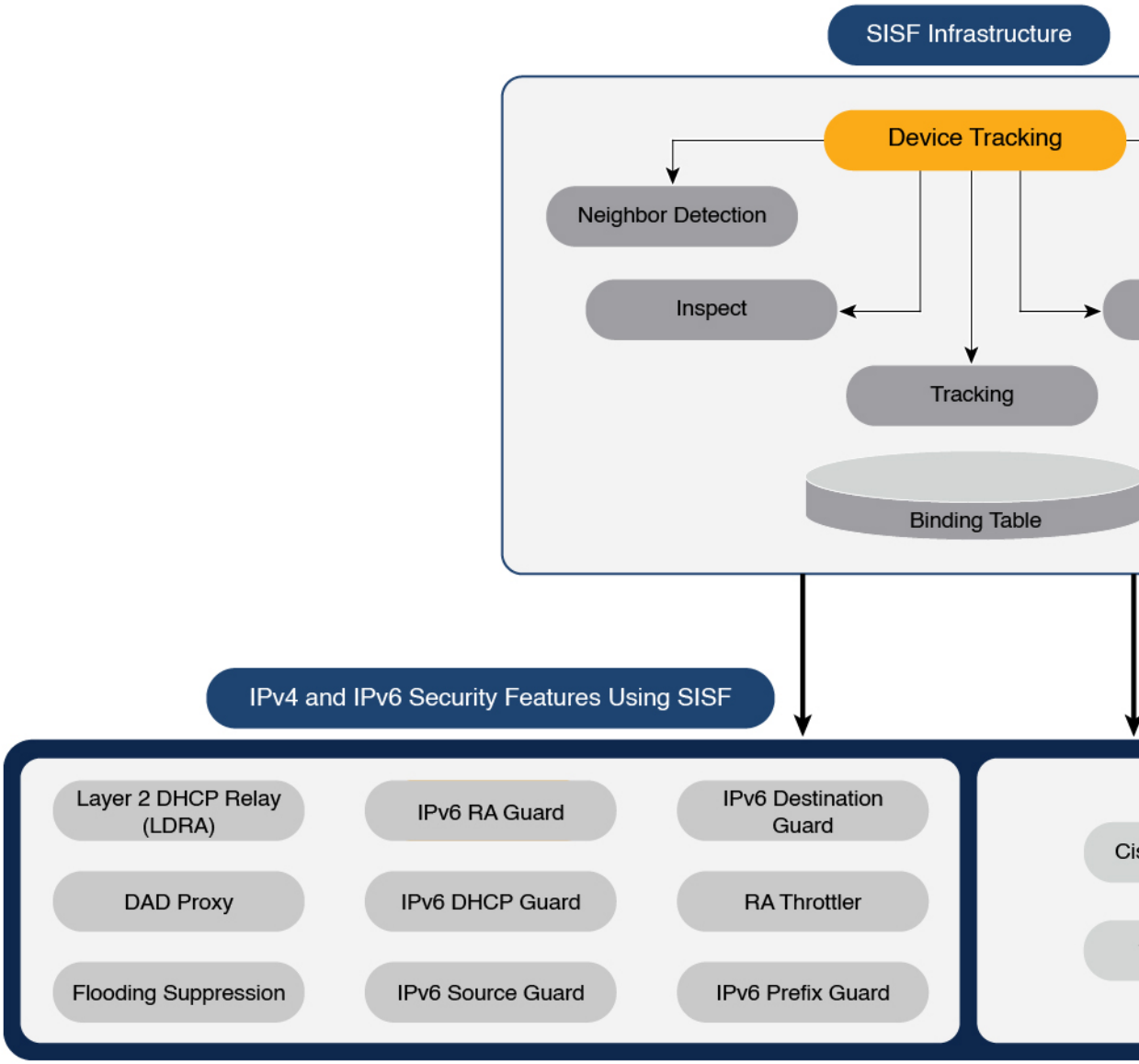
SISF インフラストラクチャは、以下によって使用される統合データベースを提供します。

- IPv6 FHS 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 スロットラ、および IPv6 プレフィックスガード。
- Cisco TrustSec、IEEE 802.1X、Locator ID Separation Protocol（LISP）、イーサネット VPN（EVPN）、および SISF のクライアントとして機能する Web 認証などの機能。

以下の図は、これを示しています。

[1] IPv6 スヌーピングポリシー、IPv6 FHS バインディング テーブル コンテンツ、および IPv6 ネイバー探索検査

図 *1* : *SISF* フレームワーク



（注） 「SISF」、「デバイス トラッキング」および「SISF ベースのデバイストラッキング」という用語は、本書では同じ意味で使用され、同じ機能を指します。どの用語も、従来の IPDT または IPv6 スヌーピング機能を意味するものではなく、混同すべきではありません。

SISF インフラストラクチャについて

このセクションでは、図 1 : SISF フレームワーク （2 ページ）に示す SISF インフラストラクチャのさまざまな要素について説明します。

バインディングテーブル

SISFインフラストラクチャは、バインディングテーブルを中心に構築されています。このバインディングテーブルには、スイッチのポートに接続されているホストに関する情報と、これらのホストの IP アドレスと MAC アドレスが含まれています。これは、スイッチに接続されているすべてのホストの物理マップを作成するうえで役立ちます。

バインディングテーブルの各エントリは、接続されたホストに関する次の情報を提供します。

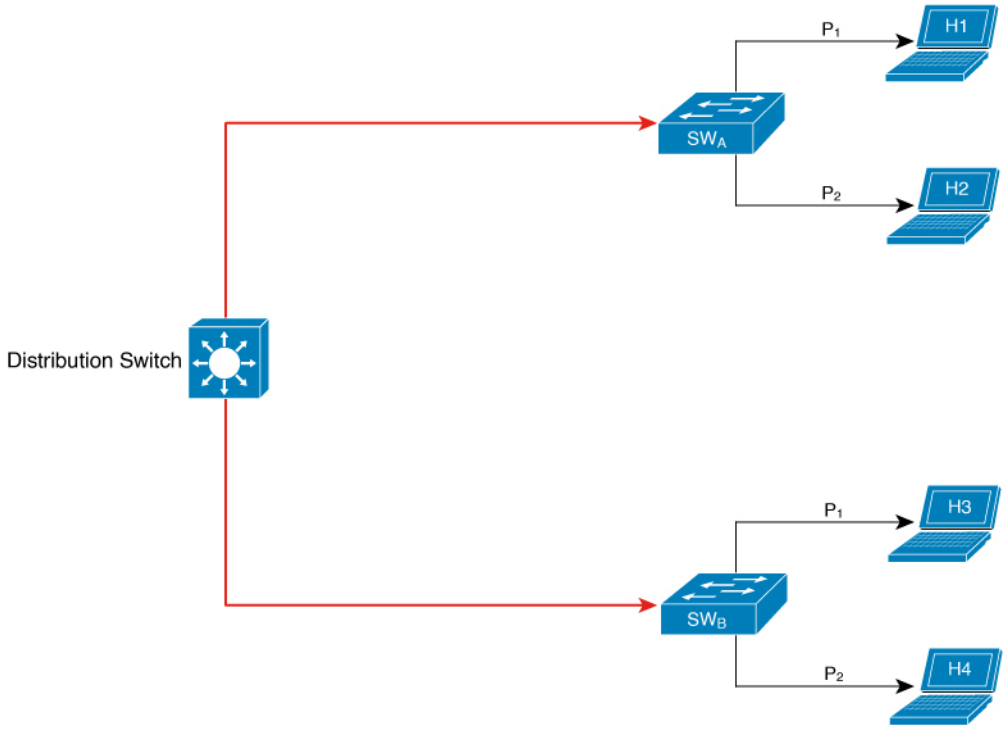
- ホストの IPv4 アドレスまたは IPv6 アドレス。
- ホストの MAC アドレス。同じ MAC アドレスが IPv4 アドレスおよび IPv6 アドレスにリンクされる場合があります。
- ホストが接続されているスイッチのインターフェイスまたはポート、および関連付けられた VLAN。
- エントリの到達可能性を示すエントリの状態。

次の図は、シンプルなネットワークトポロジと、ネットワーク内の各アクセススイッチの代表的なバインディングテーブルを示しています。SW_A と SW_B は、ネットワーク内の 2 つのアクセススイッチです。この2つのアクセススイッチは、同じ分散スイッチに接続されています。H1、H2、H3、H4 はホストです。

これは分散バインディングテーブルの例で、ネットワーク内の各アクセススイッチには独自のテーブルがあります。別のセットアップとして、SW_A と SW_B のエントリを持つ分散スイッチ上に、1 つの集中管理型バインディングテーブルを置くことも可能です。

分散型または集中管理型のバインディングテーブルを置くことは、ネットワークに SISF を導入するプロセスにおける重要な設計上の選択肢であり、この章のポリシーパラメータについて（9 ページ）セクションで詳しく説明します。

図 *2:* バインディングテーブル



VLAN	IPv4/ I
200	192.0.
200	192.0.

VLAN	IPv4/ I
100	198.51
100	198.51

バインディング テーブル エントリの状態とライフタイム

エントリの状態は、ホストが到達可能かどうかを示します。バインディング テーブル エントリの安定した状態は、REACHABLE、DOWN、および STALE です。ある状態から別の状態に変化するとき、エントリは、VERIFY、INCOMPLETE、TENTATIVE など、他の一時的な状態または過渡的な状態になる場合があります。

エントリが特定の状態を維持する期間は、その有効期間と、エントリが正常に検証されたかどうかによって決まります。エントリの有効期間は、ポリシー主導、またはグローバルに設定できます。

REACHABLE、DOWN、および STALE の有効期間を設定するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

device-tracking binding { **reachable-lifetime** { *seconds* | **infinite** } | **stale-lifetime** { *seconds* | **infinite** } | **down-lifetime** { *seconds* | **infinite** } }

状態：**REACHABLE**

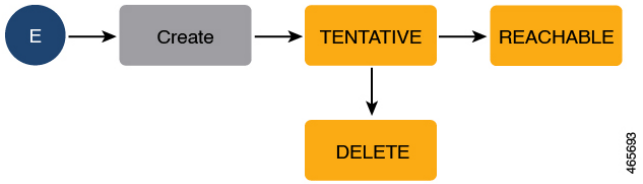
エントリにこの状態がある場合、それは、制御パケットを受信したホスト（IP アドレスおよび MAC アドレス）が検証済みの有効なホストであることを意味します。到達可能なエントリのデフォルトの有効期間は 5 分です。期間を設定することもできます。到達可能な有効期間を設定することにより、ホストからの最後の着信制御パケットの後、ホストが REACHABLE 状態を維持できる期間を指定します。

エントリの到達可能な有効期間が切れる前にイベントが検出された場合、到達可能な有効期間はリセットされます。

新しいエントリが REACHABLE 状態になるには、次の図に示すプロセスを通ります。スイッチは接続されたホストからの着信制御パケットなどのイベント（E）を検出し、エントリを作成します。さまざまなイベントによってエントリが作成されます。これらについては、「バインディングテーブルのソース」セクションで説明します。エントリの作成に続いて、TENTATIVE や INCOMPLETE などの過渡的な状態になります。過渡的な状態の間に、スイッチはバインディングエントリの完全性を検証し、確認します。エントリが有効であることが判明した場合、状態は REACHABLE に変わります。

ただし、アドレスの盗難や類似のイベントが検出された場合、エントリは無効とみなされて削除されます。たとえば、攻撃者がターゲット IP と同じ IP およびその（攻撃者の）独自の MAC アドレスを使用して、勝手にネイバーアドバタイズメントメッセージを送信して、トラフィックをリダイレクトする場合です。

図 *3:* 到達可能なエントリの作成

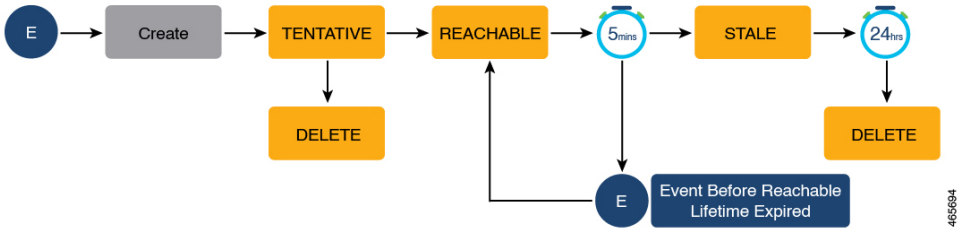


状態：Stale

エントリがこの状態にある場合、エントリの到達可能な有効期間が切れ、対応するホストがまだサイレントである（ホストからの着信パケットがない）ことを意味します。古いエントリのデフォルトの有効期間は 24 時間です。期間を設定することもできます。古い有効期間を過ぎても STALE 状態のままであるエントリは削除されます。

以下の図は、エントリの有効期間を示しています。

図 *4:* エントリの有効期間



状態：Down

エントリがこの状態の場合、ホストの接続インターフェイスがダウンしていることを意味します。Downエントリのデフォルトの有効期間は24時間です。期間を設定することもできます。有効期間を過ぎても DOWN 状態のままであるエントリは削除されます。

ホストのポーリングとバインディング テーブル エントリの更新

ポーリングは、ホストの状態、まだ接続されているかどうか、および通信しているかどうかを確認するための、ホストの定期的な条件付きチェックです。エントリの状態を判断するだけでなく、ポーリングを使用してエントリの状態を再確認できます。

グローバル コンフィギュレーション モードで **device-tracking tracking** コマンドを使用して、ポーリングを有効にできます。有効にした後も、特定のインターフェイスまたはVLANのポーリングを柔軟にオンまたはオフにできます。このためには、ポリシーで**tracking enable**または**tracking disable** キーワードを設定します（デバイス トラッキング コンフィギュレーション モード）。ポーリングが有効な場合、スイッチは指定された間隔でホストをポーリングし、到達可能な有効期間中の到達可能性を再確認します。

ポーリングが有効な場合、スイッチは到達可能な有効期間が切れた後、システムが決定した間隔で、最大3つのポーリング要求を送信します。または、グローバル コンフィギュレーション モードで **device-tracking tracking retry-interval** *seconds* コマンドでこの間隔を設定することもできます。

以下の図は、ホストがポーリングされるエントリの有効期間を示しています。図には、デフォルトの到達可能で古い有効期間、および再試行間隔が使用されています。

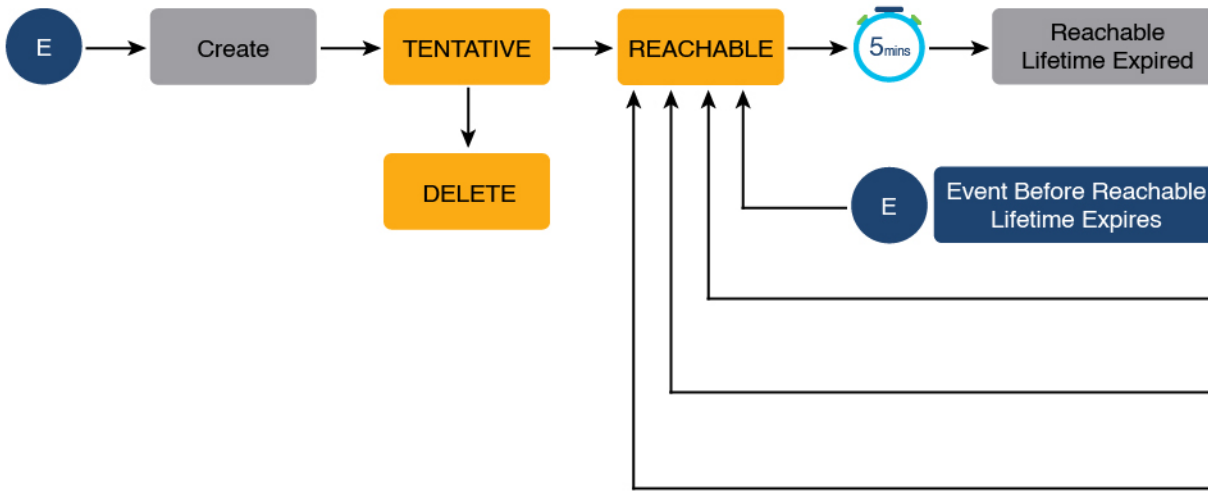
イベント（E）が検出され、REACHABLE エントリが作成されます。

到達可能な有効期間の間にイベントが検出されると、到達可能な有効期間タイマーがリセットされます。

到達可能な有効期間が切れると、スイッチはポーリング要求を送信します。スイッチは、システムが決定した固定の間隔で、最大3回ホストをポーリングします。ポーリング要求には、ユニキャスト Address Resolution Protocol（ARP）プローブ、またはネイバー要請メッセージの形式があります。この間、エントリの状態はVERIFYに変わります。ポーリング応答が受信されると（ホストの到達可能性が確認されると）、エントリの状態は REACHABLE に戻ります。

スイッチが 3 回試行してもポーリング応答を受信しない場合、エントリは STALE 状態に変わります。この状態が 24 時間維持されます。古い有効期間中にイベントが検出された場合、エントリの状態は REACHABLE に戻ります。古い有効期間が切れたときに、デバイスは到達可能性を確認するために最後のポーリングを1回送信します。この最後のポーリング試行で応答を受信した場合、エントリの状態は REACHABLE に戻ります。最後のポーリングの試行で応答が受信されない場合、エントリは削除されます。

図 *5*: ホストがポーリングされるエントリの有効期間



バインディングテーブルのソース

このセクションでは、バインディング テーブル エントリの作成と更新の原因となる情報とイベントのソースについて説明します。

- バインディングテーブルに動的にデータを取り込む学習イベント：
  - Dynamic Host Configuration Protocol（DHCP）のネゴシエーション（DHCP REQUEST、および DHCP REPLY）。これには、DHCPv4 と DHCPv6 が含まれます。
  - Address Resolution Protocol（ARP）パケット。
  - Neighbor Discovery Protocol（NDP）パケット。
  - 複数の Identity Association-Nontemporary Address（IA_NA）および Identity Association-Prefix Delegation（IA_PD）。

    場合によっては、ネットワークデバイスが DHCP サーバーから複数の IPv6 アドレスを要求して受信することがあります。これは、レジデンシャルゲートウェイがアドレスをその LAN クライアントに配布することを要求する場合など、デバイスの複数のクライアントにアドレスを提供するために実行できます。デバイスが DHCPv6 パケットを送信すると、パケットにはデバイスに割り当てられているすべてのアドレスが含まれます。

SISF は DHCPv6 パケットを分析する際に、パケットの IA_NA（Identity Association-Nontemporary Address）および IA_PD（Identity Association-Prefix Delegation）コンポーネントを検査し、パケットに含まれる各 IPv6 アドレスを抽出します。SISF は、抽出された各アドレスをバインディングテーブルに追加します。

- 静的バインディングエントリの設定。

  レイヤ 2 ドメインにサイレントでも到達可能なホストがある場合、静的バインディングエントリを作成して、ホストがサイレントになった場合でもバインディング情報を保持できます。

  このためには、グローバルコンフィギュレーションモードで次のコマンドを設定します：**device-tracking binding vlan** *vlan-id* {*ipv4_address ipv6_address ipv6_prefix*} {**interface** *interface-type_no* }。

（注） 上記のプライマリイベントまたはキーイベントに加えて、ping によってデバイス トラッキング エントリが発生する特定のシナリオがあります。送信者の ARP キャッシュまたは IPv6 ネイバーテーブルにターゲットの IP アドレスがまだない場合、ping は IPv4 の ARP パケットまたは IPv6 の ND パケットをトリガーします。これにより、デバイス トラッキング エントリが発生する可能性があります。

ただし、ターゲット IP がすでに ARP キャッシュまたは IPv6 ネイバーテーブルにある場合、ping を実行しても ARP または ND パケットは生成されません。その場合、SISF は IP アドレスを学習できません。

デバイストラッキング

デフォルトでは、SISF ベースのデバイストラッキングは無効になっています。インターフェイスまたは VLAN でこの機能を有効にできます。

この機能を有効にすると、バインディングテーブルが作成され、続いてバインディングテーブルがメンテナンスされます。

バインディングテーブルのソース （7 ページ） セクションに示されるイベントは、SISF ベースのデバイストラッキングのトリガーとして機能し、ネットワーク内のホストの存在、場所、および移動を追跡し、バインディングテーブルに入力して保持します。たとえば、ホストに関する情報が ARP または ND パケットによって学習される場合、同じホストからの後続のすべての ARP または ND パケットは、SISF ベースのデバイストラッキングのアラートとして機能し、バインディングテーブルのエントリを更新し、ホストがまだ同じ場所に存在するか、移動したかを示します。

スイッチが受信するパケットのスヌーピング、デバイスアイデンティティ（MAC および IP アドレス）の抽出、およびスイッチのバインディングテーブルへの情報保存の継続的なプロセスにより、バインディングの整合性が保証され、バインディングテーブル内のホストの到達可能性ステータスが保持されます 。

SISF ベースのデバイストラッキングを有効にする方法については、SISF の設定方法 （25 ページ） を参照してください。

デバイス トラッキング ポリシー

デバイス トラッキング ポリシーは、SISF ベースのデバイストラッキングが従う一連のルールです。ポリシーは、どのイベントがリッスンされるか、ホストがプローブされるかどうか、ホストがプローブされるまでの待機時間などを指示します。これらのルールは、ポリシーパラメータと呼ばれます。

（注） このポリシーは、インターフェイスまたは VLAN に適用する必要があります。その場合にのみ、ポリシーパラメータに従って、インターフェイスまたは VLAN のバインディングテーブルが読み込まれます。

ポリシーを作成するさまざまな方法については、SISF の設定方法 （25 ページ） を参照してください。

ポリシー設定を表示するには、特権 EXEC モードで **show device-tracking policy** *policy_name* コマンドを使用します。

ポリシーパラメータについて

ポリシーパラメータは、デバイストラッキング コンフィギュレーション モードでの設定に使用できるキーワードです。各ポリシーパラメータは、ネットワークセキュリティの 1 つ以上の側面に対応します。

このセクションでは、ポリシーを要件に合わせて設定できるように、いくつかの重要なポリシーパラメータの目的について説明します。

```
Device(config)# device-tracking policy example_policy
Device(config-device-tracking)# ?
device-tracking policy configuration mode:

  device-role           Sets the role of the device attached to the port
  limit                 Specifies a limit
  security-level        setup security level
  tracking              Override default tracking behavior
  trusted-port          setup trusted port
```

デバイストラッキング コンフィギュレーション モードで表示されるすべてのパラメータの詳細については、対応するリリースのコマンドリファレンスドキュメントを参照してください。

Glean 対 Guard 対 Inspect

パケットがネットワークに入ると、SISF が IP アドレスと MAC アドレス（パケットの送信元）を抽出し、後続のアクションは、ポリシーで設定されているセキュリティレベルによって決まります。

Glean、guard、inspectは、セキュリティレベルパラメータで使用できるオプションです。Glean は最も安全性の低いオプションで、 inspect は中程度の安全性で、guard は最も安全です。

ポリシーでこのパラメータを設定するには、デバイス トラッキング コンフィギュレーション モードで **security-level** キーワードを入力します。

Glean

セキュリティレベルが **glean** に設定されている場合、SISF が IP アドレスと MAC アドレスを抽出し、検証なしでバインディングテーブルに入力します。したがって、このオプションはバインディングの整合性を保証しません。たとえば、IEEE 802.1X や SANET などのクライアントアプリケーションがホストについてのみ学習し、認証のために SISF に依存しない設定に適しています。

このセキュリティレベルのバインディングエントリの追加に影響する唯一の要因は、アドレス数の制限です。ポートあたりの IP の最大数、MAC あたりの IPv4、MAC あたりの IPv6 には、個別の制限があります。制限に達すると、エントリは拒否されます。このパラメータの詳細については、アドレス数の制限を参照してください。

Guard

これは、セキュリティレベル パラメータのデフォルト値です。

セキュリティレベルが **guard** に設定されている場合、SISF はネットワークに入るパケットの IP アドレスと MAC アドレスを抽出して検証します。検証の結果により、バインディングエントリが追加または更新されるか、またはパケットがドロップされてクライアントが拒否されるかが決まります。

検証のプロセスは、データベースで一致するエントリを検索することから始まります。データベースは、一元化または分散化できます。一致するエントリが見つからない場合は、新しいエントリが追加されます。

一致するエントリが見つかり、接続ポイント（MAC、VLAN、またはインターフェイス）が同じであることがわかった場合、タイムスタンプのみが更新されます。そうでない場合、検証の範囲は、アドレス所有者の検証を含むように拡張されます。これには、接続ポイントの変更（別の MAC または VLAN）が有効かどうかを判断するためのホストポーリングが含まれる場合があります。変更が有効な場合、エントリは更新されます。盗難の場合、エントリはバインディングテーブルに追加されません。

バインディングエントリが追加または更新されると、対応するクライアントにネットワークへのアクセスが許可されます。エントリが検証に合格しない場合、対応するクライアントは拒否されます。

（注） 検証プロセスは、バインディングエントリだけでなく、対応する着信パケットにも影響します。

SISF は、IPv4 の場合、パケットのコピーのみを使用します。IPv6 パケットの場合、SISF は検証の間、元のパケットを停止します。拒否されたエントリは、対応するパケットについて次のことを意味します。

- 着信パケットが IPv4 の場合、エントリが拒否されてもパケットは通過できます。
- 着信パケットが IPv6 の場合、エントリが拒否されたということは、パケットもドロップされることを意味します。

Inspect

CLI でセキュリティレベルの **inspect** を使用できますが、これを使用しないことを推奨します。上記の **glean** および **guard** オプションは、ほぼすべての使用例とネットワーク要件に対応します。

Trusted-Port および Device-Role Switch

device-role switch と **trusted-port** オプションは、効率的で拡張可能な「セキュアゾーン」を設計するのに役立ちます。これら 2 つのパラメータを合わせて使用することで、バインディングテーブルのエントリの作成を効率的に分散できます。これにより、バインディングテーブルのサイズを制御できます。

trusted-port オプション：設定されたターゲットでガード機能を無効にします。trusted-port を経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。また、テーブル内にエントリを作成しているときに衝突が発生した場合も、信頼できるポートが優先されます。

device-role オプション：ポートに面するデバイスのタイプを示し、ノードまたはスイッチです。ポートのバインディングエントリを作成できるようにするには、デバイスをノードとして設定します。バインディングエントリの作成を停止するには、デバイスをスイッチとして設定します。

デバイスをスイッチとして設定することは、大規模なデバイス トラッキング テーブルの可能性が非常に高いマルチスイッチセットアップに適しています。ここで、デバイスに面するポート（アップリンクトランクポート）は、バインディングエントリの作成を停止するように設定できます。トランクポートの反対側のスイッチではデバイストラッキングが有効化され、バインディングエントリの有効性がチェックされるため、このようなポートに到着するトラフィックは信頼できます。

（注） これらのオプションのいずれか 1 つだけを設定することが適切な場合もありますが、より一般的な導入例は、ポートで **trusted-port** と **device-role switch** オプションの両方を設定することです。以下の例は、これについて詳しく説明しています。これらのオプションのいずれか 1 つだけが適している場合、またはこれが必要な場合についても、このセクションの最後で説明しています。

ポリシーでこれらのパラメータを設定するには、デバイストラッキング コンフィギュレーション モードで、**trusted-port** および **device-role** キーワードを入力します。

例：マルチスイッチセットアップで Trusted-Port および Device-Role Switch オプションを使用する

次の例では、**device-role switch** および **trusted-port** オプションが、効率的で拡張可能な「セキュアゾーン」の設計にどのように役立つかを説明します。

以下の図 図 6 : Trusted-Port および Device-Role Switch オプションのないマルチスイッチセットアップ （13 ページ） では、SW_A、SW_B、および SW_C が 3 つのアクセススイッチです。これらはすべて共通の分散スイッチに接続されています。この場合、分散スイッチで唯一必要な設定は、あらゆる種類のトラフィックがブロックされないようにすることです。

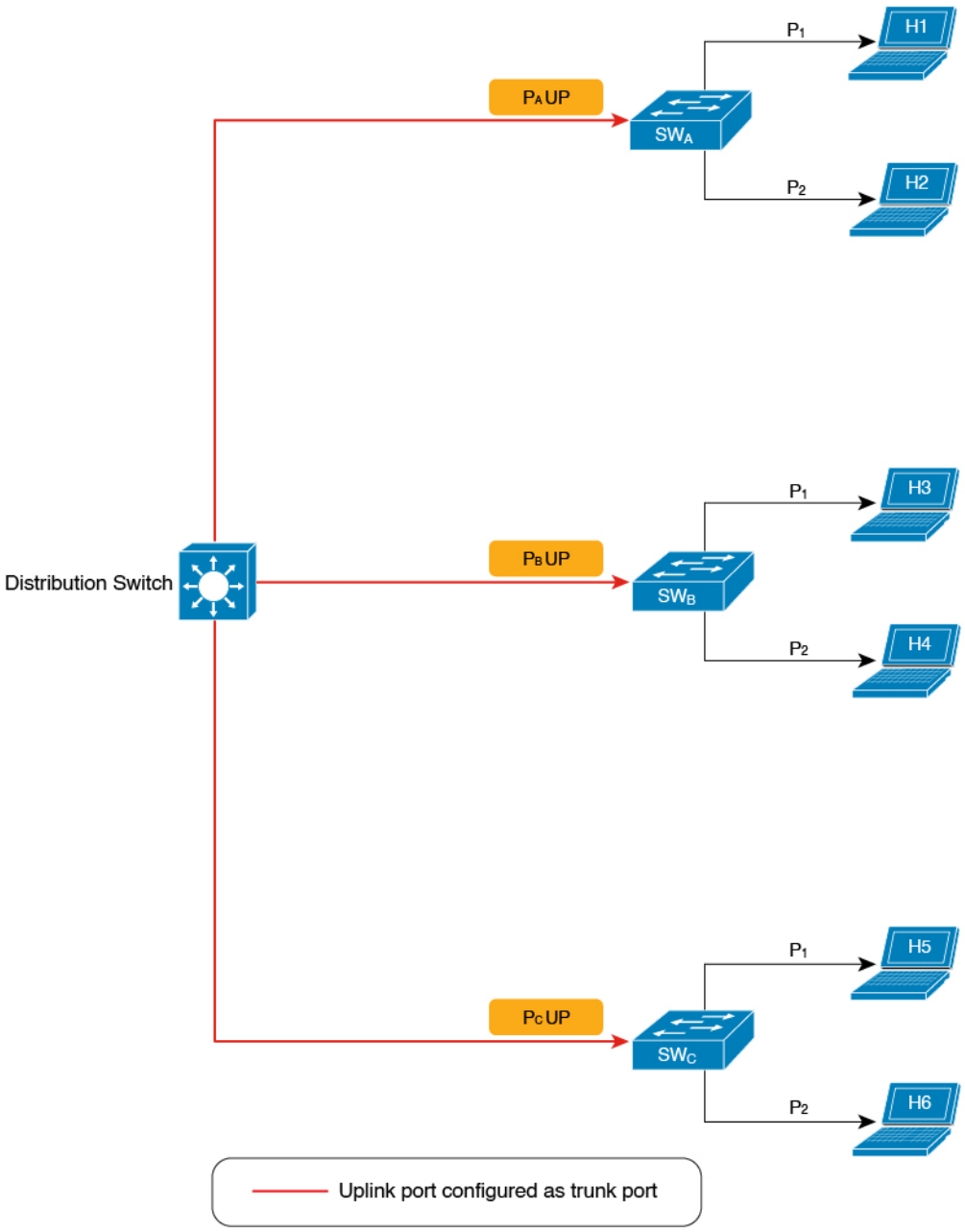
H1、H2、…H6 はホストです。各スイッチには、直接接続されたホストが 2 つあります。すべてのホストが相互に通信していて、制御パケットが転送されています。すべてのホストはまた、同じ VLAN 境界内にあります。各スイッチは、直接接続されているホストから、および他のスイッチに接続されているホストから、制御パケットを受信しています。これは、SW_A が、SW_B および SW_C と同様、H1、H2、…H6 から制御パケットを受信していることを意味します。

スイッチごとに、直接接続されたホストのエントリには、バインディングテーブル内のインターフェイス、またはポート P_1 および P_2があります。他のスイッチに接続されているホストから発信されたエントリには、アップリンクポートを介して学習されたことを示すために、インターフェイスまたはポート名 P_xUP が付けられます（x は、各スイッチに対応するアップリンクポートを表します）。たとえば、SW_A がアップリンク ポートを介して学習したエントリのインターフェイスまたはポート名は P_AUP で、SW_B の場合は P_BUP などです。

最終的な結果は、各スイッチが学習し、セットアップ内のすべてのホストのバインディングエントリを作成することです。

このシナリオでは、バインディングテーブルの非効率的な使用を示します。これは各ホストが複数回検証されるためであり、1 つのスイッチだけがホストを検証する場合よりも安全性は低くなります。次に、複数のバインディングテーブル内の同じホストのエントリは、より早くアドレス数の制限に達する可能性があります。制限に達すると、それ以上のエントリは拒否され、それにより必要なエントリが不足する可能性があります。

図 *6 : Trusted-Port* および *Device-Role Switch* オプションのないマルチスイッチセットアップ



VLAN	IPv
100	192
100	192
200	192
200	192
300	192
300	192

VLAN	IPv
200	192
200	192
100	192
100	192
300	192
300	192

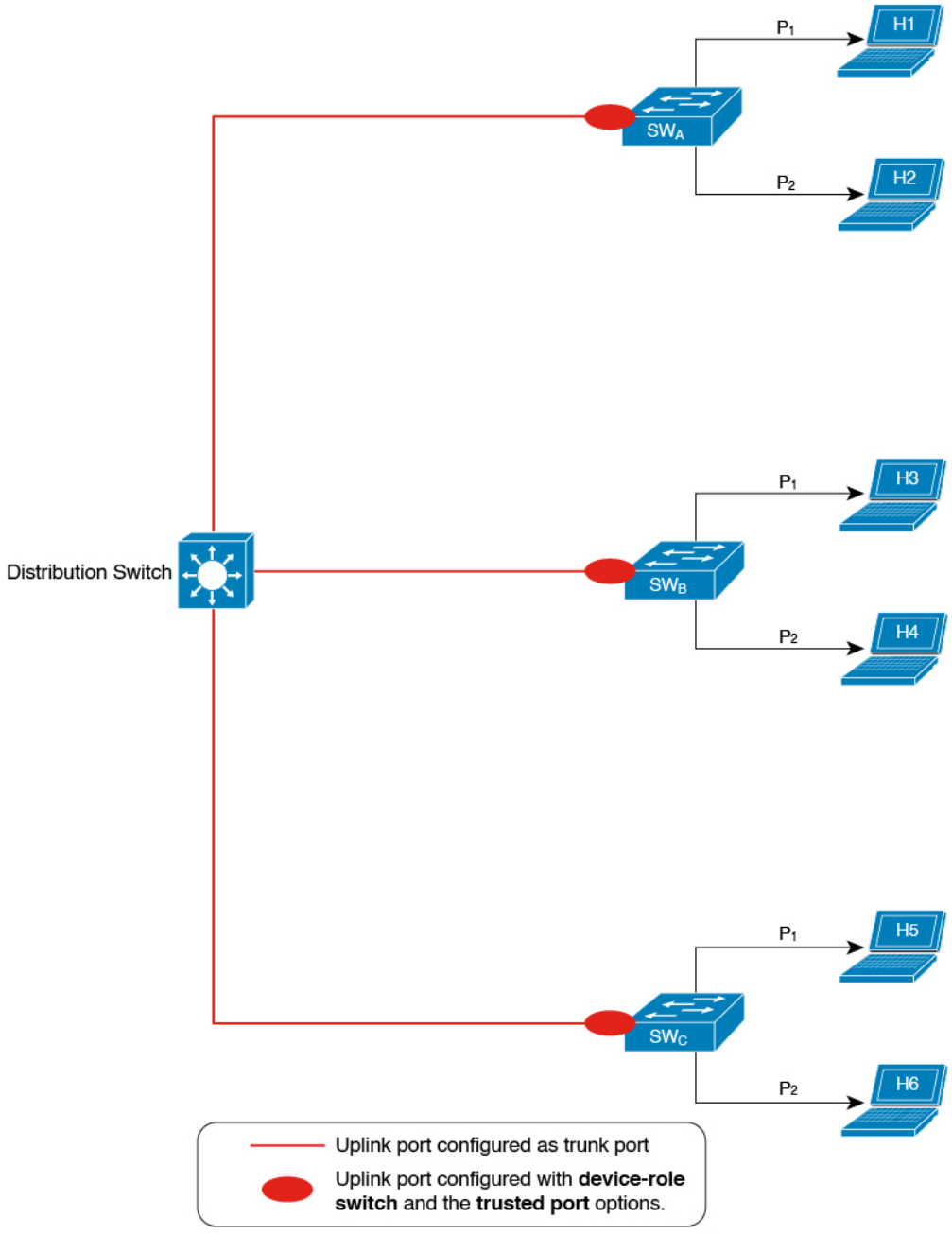
VLAN	IPv
300	192
300	192
100	192
100	192
200	192
200	192

比較のため、以下の図 図 7 : Trusted-Port および Device-Role Switch オプションを使用したマルチスイッチセットアップ（15 ページ） を参照してください。ここで、SW_A が接続されていないホストのパケット（SW_B に直接接続されている H3 など）を傍受すると、H3 がスイッチとして設定されているデバイス（**device-role switch** オプション）に接続されていることが検出され、スイッチのアップリンクポート（パケットの送信元）が信頼できるポート（**trusted-port** オプション）であるため、エントリは作成されません。

ホストがアクセスポート（各スイッチのポート P_1 および P_2）に表示されるスイッチにのみバインディングエントリを作成し、アップリンクポートまたは信頼できるポート（P_x UP）に表示されるホストのエントリを作成しないことにより、各セットアップのスイッチは、必要なエントリのみを検証して作成するため、バインディング テーブル エントリの作成を効率的に分散できます。

マルチスイッチシナリオで **device-role switch** および **trusted-port** オプションを設定する 2 番目の利点は、ホスト、たとえば H1 があるスイッチから別のスイッチに移動するときに、エントリの重複を防ぐことです。以前の場所（たとえば SW_A）にある H1 の IP および MAC バインディングは、STALE 状態に達するまでそこに留まり続けます。しかし、H1 が移動して 2 番目のスイッチ（SW_C など）に接続すると、SW_A はアップリンクポートを介して重複するバインディングエントリを受信します。このような状況で、2 番目のスイッチ（SW_C）のアップリンクポートが信頼できるポートとして設定されている場合、SW_A は古いエントリを削除します。さらに、SW_C にはすでに最新のエントリがあり、このエントリは信頼できるため、別の新しいバインディングエントリは作成されません。

図 *7 : Trusted-Port* および *Device-Role Switch* オプションを使用したマルチスイッチセットアップ



VLAN	IPv
100	192
100	192

VLAN	IPv
200	192
200	192

VLAN	IPv
300	192
300	192

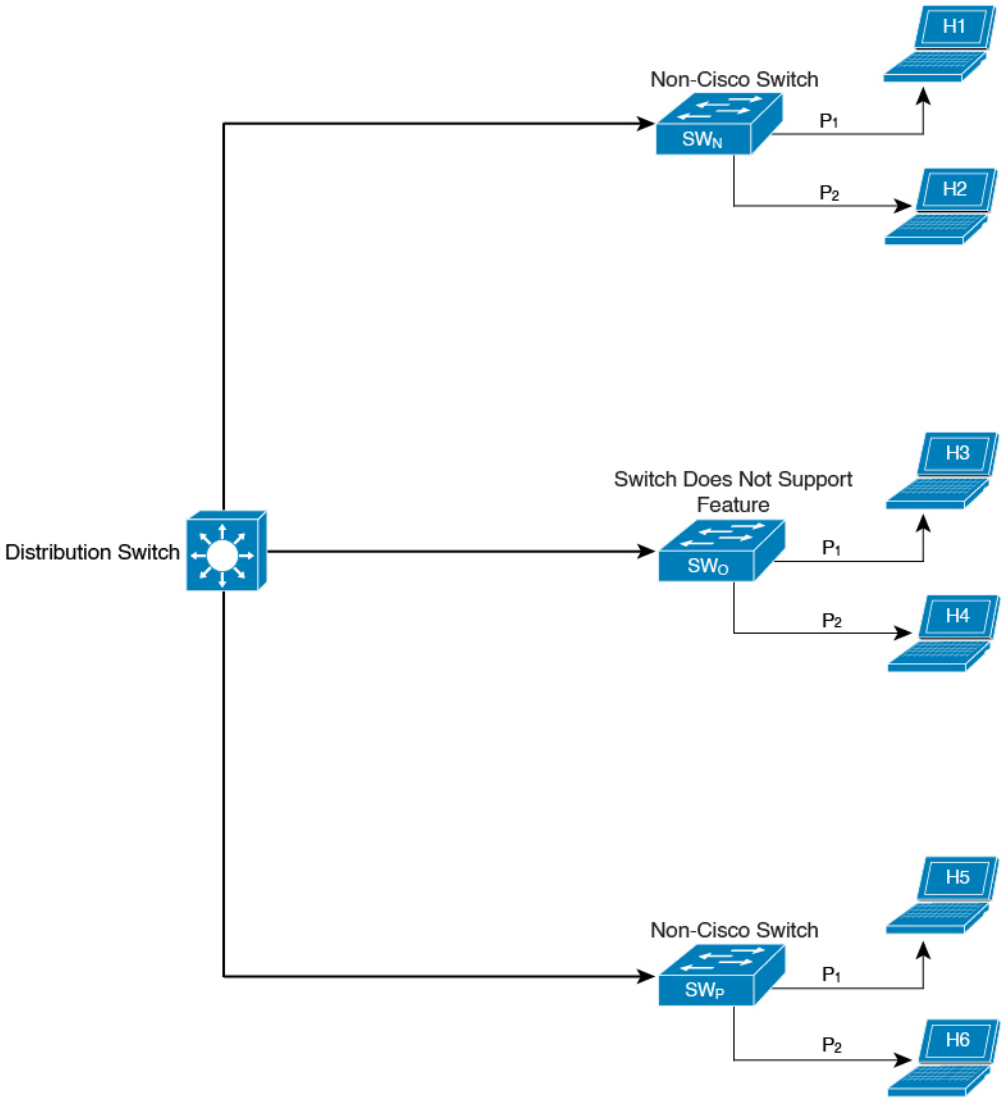
例：Trusted-Port および Device-Role Switch オプションを使用しない場合

前の例では、分散型バインディングテーブルを使用するマルチスイッチセットアップが **device-role switch** および **trusted-port** オプションからどのようなメリットを受けるかを明確に示していますが、次の種類のネットワークには適していない可能性があります。

- シスコ以外のスイッチが使用されているネットワーク
- スイッチが SISF ベースのデバイストラッキング機能をサポートしていないネットワーク。

どちらの場合も、**device-role switch** および **trusted-port** オプションを設定しないことを推奨しました。さらに、分散スイッチ上で集中管理型のバインディングテーブルを維持することを推奨しました。これにより、シスコ以外のスイッチやこの機能をサポートしていないスイッチに接続されているすべてのホストについて、すべてのバインディングエントリが分散スイッチによって検証され、引き続きネットワークが保護されます。以下の図に、この例を示します。

図 *8* : 集中管理型のバインディングテーブル



VLAN	IPv
100	192
100	192
200	192
200	192
300	192
300	192

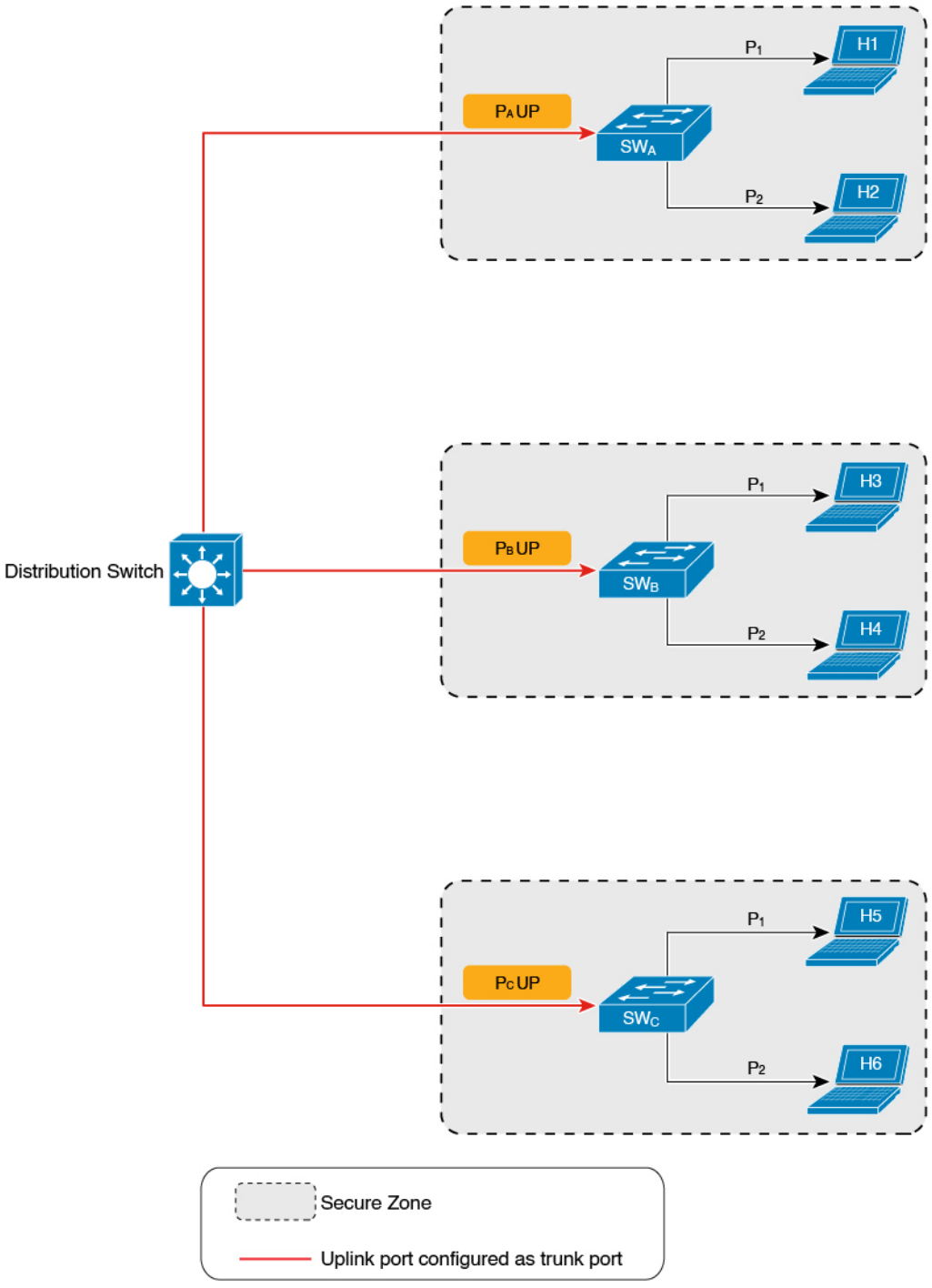
効率的で拡張可能なセキュアゾーンの作成

適切なネットワークで **trusted-port** オプションと **device-role switch** オプションを使用し、他のネットワークではそれらを除外することにより、効率的で拡張可能なセキュアゾーンを実現できます。

セキュアゾーン 1、2、3 には、3 つの異なるセットアップと、それぞれの場合に確立されるセキュアゾーンが表示されます。

セキュアゾーン：	図 9：セキュアゾーン 1 - 非効率的で拡張不可能なセキュアゾーン （19 ページ）	図 10：セキュアゾーン 2 - バインディングテーブルが分散化されている場合の効率的で拡張可能なセキュアゾーン （20 ページ）	図 11：セキュアゾーン 3 - バインディングテーブルが一元管理されている場合の効率的なセキュアゾーン （21 ページ）
拡張性：	拡張不可、各スイッチにネットワーク内のすべてのホストのエントリがある	拡張可能、直接接続されたホストのみのエントリとしての各スイッチ	拡張不可、分散スイッチにネットワーク内のすべてのホストのエントリがある
ポーリングとネットワークへの影響： n＝ホストの数 m＝スイッチの数 ポーリング要求の総数：＝n X m	18 のポーリング要求が送信されている（ホスト 6 つ X スイッチ 3 つ）。 各ホストは、ネットワーク内のすべてのスイッチによってポーリングされる（**trusted-port** および **device-role switch** オプションがない場合）。 ネットワーク負荷が非常に高い。	6 つのポーリング要求が送信されている（スイッチごとに、ホスト 2 つ X スイッチ 1 つ）。 最小限のネットワーク負荷（ポーリング要求は、ローカルアクセススイッチによって直接接続されたホストに送信される。各ポーリング要求は、ネットワーク内の少数のポイントを通過する）。	6 つのポーリング要求が送信されている（ホスト 6 つ X スイッチ 1 つ）。 ネットワーク負荷はセキュアゾーン 2 よりも高いが、セキュアゾーン 1 ほど高くはない（ポーリング要求は分散スイッチから送信され、ホストに到達する前にアクセススイッチを通過する）。
効率：	バインディングテーブルが各スイッチで複製されるため、非効率的なバインディングテーブル。	効率的なバインディングテーブル。各ホストのバインディング情報は 1 回だけ、1 つのバインディングテーブルとこれが直接接続されたスイッチのバインディングテーブルに入力されるため。	効率的なバインディングテーブル。各ホストのバインディング情報は 1 回だけ入力され、これは分散スイッチ上の一元管理されたバインディングテーブルにあるため。
推奨するアクション：	適切なポリシーを再適用して、セキュアゾーンをセキュアゾーン 2 のようにする。	なし。これは効率的で拡張可能なセキュアゾーン。	なし。セットアップのタイプを考えると、これが可能な限り最高のセキュアゾーン（ネットワーク内の他のスイッチがシスコ以外のものであるか、この機能をサポートしていない場合）。

図 *9 :* セキュアゾーン *1* - 非効率的で拡張不可能なセキュアゾーン

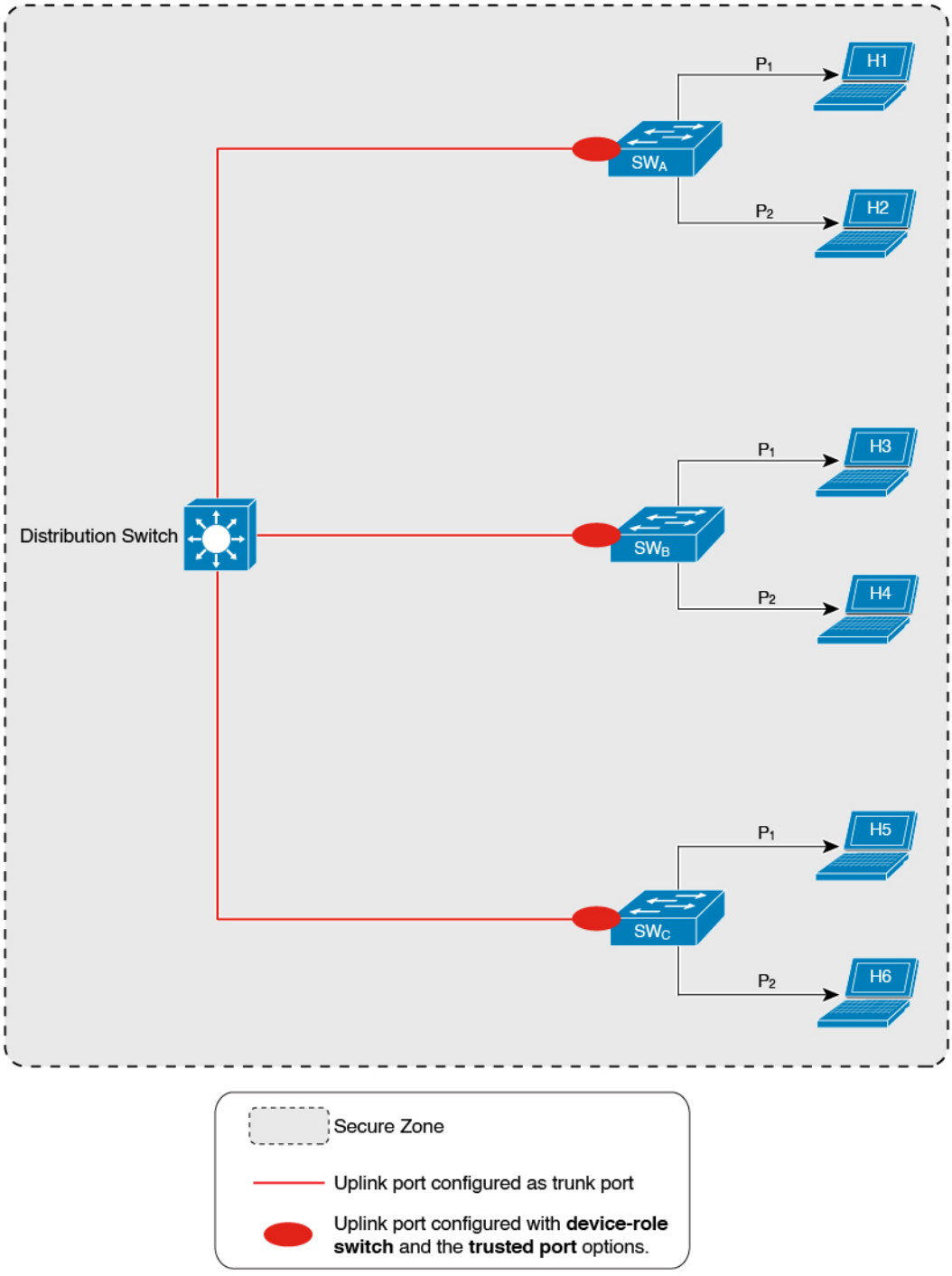


VLAN	IPv
100	192
100	192
200	192
200	192
300	192
300	192

VLAN	IPv
200	192
200	192
100	192
100	192
300	192
300	192

VLAN	IPv
300	192
300	192
100	192
100	192
200	192
200	192

図 *10* : セキュアゾーン *2* - バインディングテーブルが分散化されている場合の効率的で拡張可能なセキュアゾーン

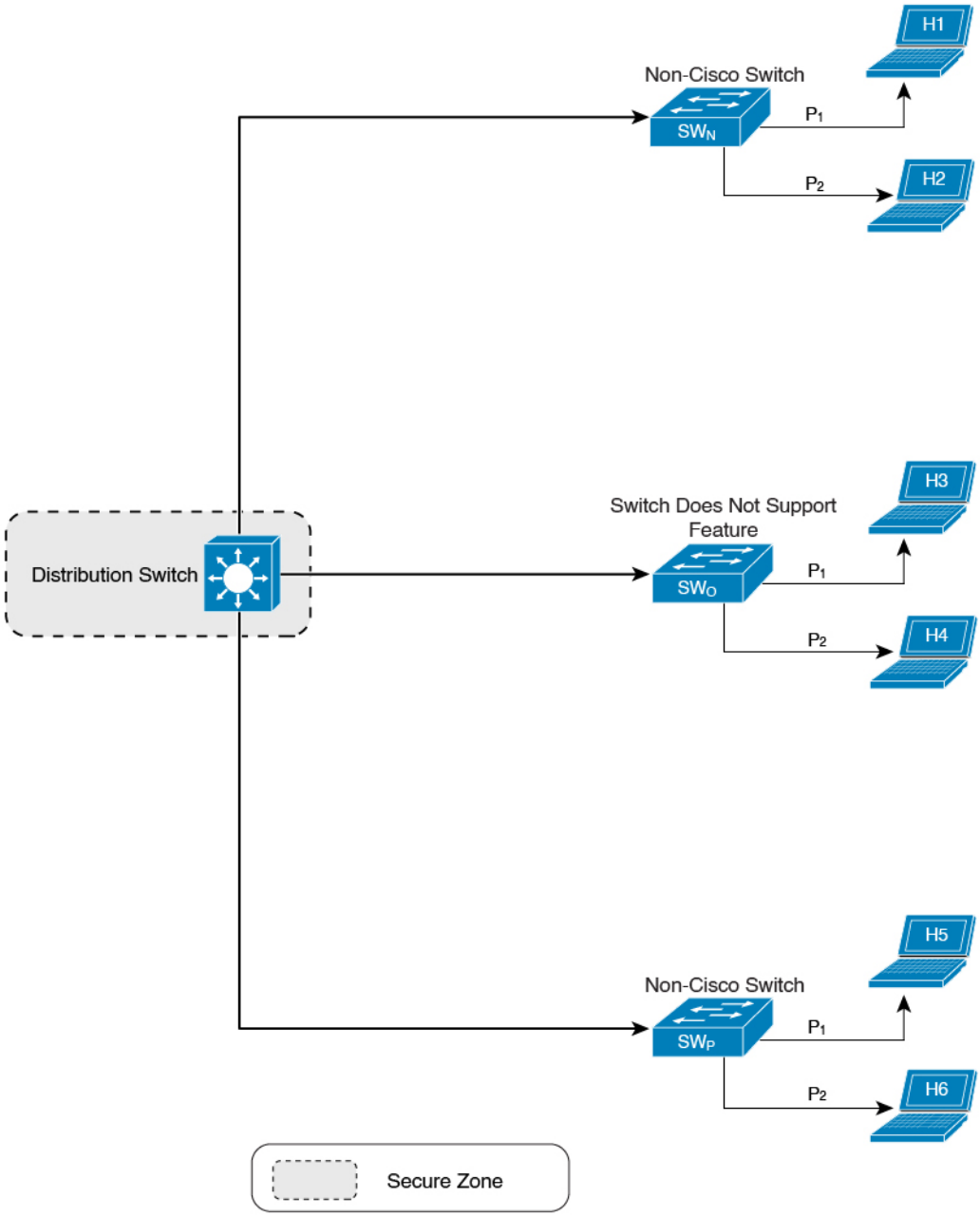


VLAN	IPv4/
100	192.0
100	192.0

VLAN	IPv4/
200	192.0
200	192.0

VLAN	IPv4/
300	192.0
300	192.0

図 *11* : セキュアゾーン *3* - バインディングテーブルが一元管理されている場合の効率的なセキュアゾーン



VLAN	
100	
100	
200	
200	
300	
300	

Trusted-Port または Device-Role Switch のみを使用する場合

device-role switch のみを設定することは、エントリをリッスンする必要はあるが、学習する必要はない場合に適しています。たとえば、重複アドレス検出（DAD）の場合、またはスイッチに面したポートで IPv6 またはネイバー要請（NS）メッセージを送信する場合です。

スイッチポート（またはインターフェイス）でこのオプションを設定すると、SISF ベースのデバイストラッキングはポートをトランクポートとして扱い、ポートが他のスイッチに接続されていることを意味します。ポートが実際にトランクポートであるかどうかは関係ありません。したがって、NS パケットまたはクエリが新しいエントリの検証のためにネットワーク内のスイッチに送信されると、セキュアポート（**device-role switch**が設定されているポート）だけがパケットまたはクエリを受信します。これにより、ネットワークが保護されます。コマンドがどのポートにも設定されていない場合、クエリの一般的なブロードキャストが送信されます。

trusted-port のみを設定するのは、アクセスポートを信頼できるポートとして設定する必要がある場合に適しています。アクセスポートが、スイッチが使用している DHCP サーバーまたは同様のサービスに接続されている場合、アクセスポートを信頼できるポートとして設定すると、そのようなポートからのトラフィックが信頼されるため、サービスは中断されません。これにより、アクセスポートを含むセキュアゾーンも拡張されます。

アドレス数の制限

アドレス数制限パラメータは、バインディングテーブルに入力できる IP アドレスと MAC アドレスの数の制限を指定します。これらの制限の目的は、既知および予期されるホストの数に基づくバインディングテーブルのサイズを含めることです。これにより、ネットワーク内の不正なホストまたは IP に対してプリエンプティブなアクションを実行できるようになります。

ポリシーレベルでは、ポートあたりの IP アドレス数、MAC あたりの IPv4 アドレス数、MAC あたりの IPv6 アドレス数に個別の制限があります。ポートあたりの IP アドレスの数のみを設定または変更できます。

ポートあたりの IP

ポートあたりの IP オプションは、ポートに許可される IP アドレスの総数です。アドレスは IPv4 または IPv6 を使用できます。制限に達すると、それ以上の IP アドレス（すなわちエントリ）はバインディングテーブルに追加されません。

ポリシーでこのパラメータを設定するには、デバイス トラッキング コンフィギュレーション モードで **limit address-count** *ip-per-port* キーワードを入力します。現在設定されている制限よりも低い制限を設定すると、新しい（より低い）制限は新しいエントリにのみ適用されます。既存のエントリはバインディングテーブルに残り、バインディングエントリのライフサイクルを通過します。

MAC あたりの IPv4 および MAC あたりの IPv6

1 つの MAC アドレスにマッピングできる IPv4 アドレスの数と、1 つの MAC アドレスにマッピングできる IPv6 アドレスの数。制限に達すると、バインディングテーブルにエントリを追加できなくなり、新しいホストからのトラフィックはドロップされます。

（注） インターフェイスまたは VLAN で有効な MAC あたりの IPv4 制限および MAC あたりの IPv6 制限は、適用されるポリシーで定義されているとおりです。ポリシーで制限が指定されていない場合、制限が存在しないことを意味します。いかなる種類のポリシー（プログラム可能、カスタムポリシー、またはデフォルトポリシー）についても、MAC あたりの IPv4 または MAC あたりの IPv6 の制限を変更または設定することはできません。

制限があるかどうかを確認するには、**show device-tracking policy** *policy name* を入力します。次に、MAC あたりの IPv4 制限と MAC あたりの IPv6 制限が存在するポリシーの出力例を示します。

```
Device# show device-tracking policy LISP-DT-GUARD-VLAN
Policy LISP-DT-GUARD-VLAN configuration:
  security-level guard (*)
  <output truncated>

  limit address-count for IPv4 per mac 4 (*)
  limit address-count for IPv6 per mac 12 (*)
  tracking enable

<output truncated>
```

全体的なアドレス数の制限に関する考慮事項

- 制限に階層はありませんが、各制限に設定されたしきい値は他の制限に影響します。

  たとえば、ポートあたりの IP 制限が 100 で、MAC あたりの IPv4 制限が 1 の場合、1 つのホストの IPv4-MAC バインディングエントリで制限に達します。ポートにさらに 99 個の IP アドレスがプロビジョニングされていても、それ以上のエントリは許可されません。

- アドレス数の制限とセキュリティレベルのパラメータ。

  アドレス数制限がセキュリティレベルのパラメータ **glean** とどのように相互作用するかについては、Glean （10 ページ） を参照してください。

  セキュリティレベルのパラメータが **guard** の場合、アドレス数の制限に達すると、エントリが拒否されます。これにより、着信パケットに次の影響があります。

  - 着信パケットが IPv4 の場合、エントリは拒否されますが、パケットの通過は許可されます。
  - 着信パケットが IPv6 の場合、エントリが拒否されたということは、パケットもドロップされたことを意味します。

- グローバルおよびポリシーレベルの制限

  device-tracking binding max-entries コマンドで設定される制限はグローバルレベルで、デバイス トラッキング コンフィギュレーション モードの **limit address-count** コマンドで設定される制限は、インターフェイスまたは VLAN レベルのポリシー用です。

ポリシーレベルの値およびグローバルで設定された値が存在する場合、*1* つの制限に達するとバインディングエントリの作成が停止します。これは、グローバル値またはポリシーレベルの値のいずれかです。

グローバルに設定された値のみが存在する場合、*1* つの制限に達すると、バインディングエントリの作成が停止します。

ポリシーレベルの値のみが存在する場合、ポリシーレベルの制限に達すると、バインディングエントリの作成が停止します。

トラッキング

追跡パラメータには、ネットワーク内のホストの追跡が含まれます。上のセクションホストのポーリングとバインディング テーブル エントリの更新 （6 ページ） では、これを「ポーリング」と呼びます。また、ポーリングの動作についても詳しく説明します。

グローバルレベルでポーリングパラメータを設定するには、グローバルコンフィギュレーションモードで**device-tracking tracking** コマンド入力します。このコマンドを設定した後も、個々のインターフェイスおよび VLAN で、ポーリングを柔軟にオンまたはオフにできます。このためには、ポリシーでポーリングを有効または無効にする必要があります。

ポリシーでポーリングを有効にするには、デバイストラッキング コンフィギュレーション モードで**tracking enable** キーワードを入力します。デフォルトでは、ポリシーでポーリングは無効になっています。

ポリシーの作成に関するガイドライン

- 特定のターゲットで複数のポリシーを使用できる場合、システム内部のポリシーの優先度によって、どのポリシーが優先されるかが決まります。

  手動で作成されたポリシーが最も優先されます。プログラムで作成されたポリシーの設定を上書きする場合は、カスタムポリシーを作成して、その優先度を高くすることができます。

- プログラムで作成されたポリシーのパラメータは変更できません。カスタムポリシーの特定の属性を設定できます。

ポリシー適用のガイドライン

- 複数のポリシーを同じ VLAN に適用できます。
- プログラムポリシーが VLAN に適用されていて、ポリシー設定を変更する場合は、カスタム デバイストラッキング ポリシーを作成して VLAN に適用します。
- 優先順位が異なる複数のポリシーが同じ VLAN に適用されている場合、優先順位が最も高いポリシーの設定が有効になります。ここでの例外は、mac あたりの IPv4 制限アドレス数、および mac あたりの IPv6 制限アドレス数の設定です。優先順位が最も低いポリシーの設定が有効になります。

- デバイストラッキング ポリシーが VLAN のインターフェイスに適用されると、インターフェイスのポリシー設定が VLAN のポリシー設定よりも優先されます。ここでの例外は、mac あたりの IPv4 制限アドレス数、および mac あたりの IPv6 制限アドレス数の値で、インターフェイスと VLAN の両方のポリシーから集約されます。
- デバイス トラッキング クライアント機能の設定が削除されない限り、ポリシーは削除できません。

SISF の設定方法

デフォルトでは、SISF または SISF ベースのデバイストラッキングは無効になっています。これを有効にするには、デバイストラッキング ポリシーを定義し、そのポリシーを特定のターゲットに適用します。ターゲットは、インターフェイスまたは VLAN です。ポリシーを定義する方法は複数あり、優先または推奨されるメソッドは 1 つではありません。要件に合ったオプションを使用してください。

SISF を有効にするメソッド	適用可能な設定タスク	結果
Option 1： 手動で、インターフェイス コンフィギュレーション コマンドを使用して**デフォルト**ポリシーを作成し、ターゲットに適用します。	ターゲットへのデフォルト デバイス トラッキング ポリシーの適用 （27 ページ）	指定されたターゲットに**デフォルト**のデバイス トラッキング ポリシーを自動的に適用します。 **デフォルト**ポリシーは、デフォルト設定の組み込みポリシーで、 デフォルトポリシーの属性は変更できません。デバイストラッキングポリシー属性を設定する場合は、**Option 2** を参照してください。

SISF を有効にするメソッド	適用可能な設定タスク	結果
Option 2：手動で、グローバル コンフィギュレーション コマンドを使用してカスタムポリシーを作成し、そのカスタムポリシーをターゲットに適用します。	1. カスタム設定を使用したカスタム デバイス トラッキング ポリシーの作成（28 ページ） 2. カスタムポリシーをインターフェイスまたはVLANに適用します。 デバイス トラッキング ポリシーのインターフェイスへの適用 （33 ページ） または デバイス トラッキング ポリシーの VLAN への適用（34 ページ）	設定した名前とポリシーパラメータを使用してカスタムポリシーを作成し、そのポリシーを指定したターゲットに適用します。
Option 3：スヌーピングコマンドを設定することにより、プログラムで実行する。	グローバル コンフィギュレーション モードで、**ip dhcp snooping vlan***vlan* コマンドを入力します。 例：DHCP スヌーピングを設定してプログラムで SISF を有効にする （38 ページ）	コマンドを設定すると、ポリシー `DT-PROGRAMMATIC` が自動的に作成されます。 IEEE 802.1X、Web 認証、Cisco TrustSec、IP ソースガード、およびSANET クライアントに対して SISF ベースのデバイストラッキングを有効にする場合、このメソッドを使用します。
Option 4： Locator ID Separation Protocol（LISP）を設定することにより、プログラムで実行します。	例：LISP（LISP-DT-GUARD-VLAN）を設定し、プログラムで SISF を有効にする （40 ページ） 例：LISP（LISP-DT-GLEAN-VLAN）を設定してプログラムで SISF を有効にする （39 ページ）	LISP を設定すると、ポリシー `LISP-DT-GUARD-VLAN` または `LISP-DT-GLEAN-VLAN` が自動的に作成されます。
Option 5：EVPN VLAN を設定することにより、プログラムで実行します。	例：VLAN で EVPN を設定してプログラムで SISF を有効にする （39 ページ）	VLAN で EVPN を設定すると、ポリシー `evpn-sisf-policy` が自動的に作成されます。

SISF を有効にするメソッド	適用可能な設定タスク	結果
Option 6：インターフェイステンプレートを使用する	インターフェイス テンプレートを使用して SISF を有効にする （35 ページ）	ポリシーをインターフェイステンプレートに追加することにより、ターゲットごとに個別にポリシーを作成せずに、同じポリシーを複数のターゲットに適用できます。
Option 7：従来の IPDT および IPv6 スヌーピングからの移行。	レガシー IPDT と IPv6 スヌーピングから SISF ベースのデバイストラッキングへの移行 （37 ページ）	IPDT および IPv6 スヌーピング設定を、SISF ベースの device-tracking コマンドに移行します。

ターゲットへのデフォルト デバイス トラッキング ポリシーの適用

デフォルトのデバイス トラッキング ポリシーをインターフェイスまたは VLAN に適用するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** **例**： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** **例**： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	インターフェイスまたは VLAN を指定します。
	• **interface** *interface*
	• **vlan configuration** *vlan_list*
	例：
	`Device(config)# interface gigabitethernet 1/1/4`
	OR
	`Device(config)# vlan configuration 333`
		interface *type number*：インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。デバイス トラッキング ポリシーは、指定されたインターフェイスに適用されます。
		vlan configuration *vlan_list*：VLAN を指定し、VLAN機能コンフィギュレーション モードを開始します。デバイス トラッキング ポリシーは、指定された VLAN に適用されます。

	コマンドまたはアクション	目的

ステップ 4	**device-tracking**
	例：
	`Device(config-if)# device-tracking`
	OR
	`Device(config-vlan-config)# device-tracking`
		SISF ベースのデバイストラッキングを有効にし、デフォルトポリシーをインターフェイスまたは VLAN に適用します。
		デフォルトポリシーは、デフォルト設定の組み込みポリシーです。デフォルトポリシーの属性は変更できません。

ステップ 5	**end**
	例：
	`Device(config-if)# end`
	OR
	`Device(config-vlan-config)# end`
		インターフェイスコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
		VLAN機能コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

ステップ 6	**show device-tracking policy** *policy-name* 例： `Device# show device-tracking policy default`	デバイストラッキング ポリシーの設定と、それが適用されるすべてのターゲットを表示します。

カスタム設定を使用したカスタム デバイス トラッキング ポリシーの作成

デバイス トラッキング ポリシーを作成して設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	[**no**] **device-tracking policy** *policy-name* 例： `Device(config)# device-tracking policy example_policy`	ポリシーを作成し、デバイストラッキング コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	[**data-glean** | **default** | **destination-glean** | **device-role** | **distribution-switch** | **exit** | **limit** | **no** | **prefix-glean** | **protocol** | **security-level** | **tracking** | **trusted-port** | **vpc**] 例： `Device(config-device-tracking)# destination-glean log-only`	システムプロンプトに疑問符（?）を入力すると、このモードで使用できるオプションのリストが表示されます。IPv4 と IPv6 の両方に対して以下を設定できます。 • （任意）**data-glean**：ネットワーク内の送信元からスヌーピングされたデータパケットからのアドレスの学習を有効にし、データトラフィックの送信元アドレスとともにバインディングテーブルを読み込みます。次のいずれかのオプションを入力します。 • log-only：データパケット通知時に syslog メッセージを生成します。 • recovery：プロトコルを使用してバインディングテーブルの回復を有効にします。**NDP**または**DHCP**の入力。 • （任意）**default**：ポリシー属性をデフォルト値に設定します。次のポリシー属性をデフォルト値に設定できます。**data-glean**、**destination-glean**、**device-role**、**limit**、**prefix-glean**、**protocol**、**security-level**、**tracking**、**trusted-port**。 • （任意）**destination-glean**：データトラフィックの宛先アドレスを収集して、バインディングテーブルを読み込みます。次のいずれかのオプションを入力します。 • **log-only**：データパケット通知時に syslog メッセージを生成します。 • **recovery**：プロトコルを使用してバインディングテーブルの回

	コマンドまたはアクション	目的
		復を有効にします。**DHCP** を入力します。 • （任意）**device-role**：ポートに接続されているデバイスのロールを設定します。ノードまたはスイッチを指定できます。次のいずれかのオプションを入力します。 • node：接続されているデバイスをノードとして設定します。これがデフォルトのオプションです。 • switch：接続されているデバイスをスイッチとして設定します。 • （任意）**distribution-switch**：このオプションは CLI には表示されますが、サポートされていません。行った設定は有効になりません。 • **exit**：デバイストラッキング ポリシー コンフィギュレーション モードを終了します。 • **limit** address-count：ポートごとのアドレスカウント制限を指定します。有効な範囲は 1 ～ 32000 です。 • **no**：コマンドを無効にするか、デフォルト値を設定します。 • （任意）**prefix-glean**：IPv6 ルータ アドバタイズメントまたは DHCP-PD のどちらかからのプレフィックスの学習を有効にします。次のオプションがあります。 • （任意）**only**：プレフィックスのみを収集し、ホストアドレスは収集しません。 • （任意）**protocol**：収集するプロトコルを設定します。デフォルトで

	コマンドまたはアクション	目的
		は、すべて収集されます。次のいずれかのオプションを入力します。 • **arp** ［**prefix-list** *name*］：ARP パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。 • **dhcp4** ［**prefix-list** *name*］：DHCPv4 パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。 • **dhcp6** ［**prefix-list** *name*］：DHCPv6 パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。 • **ndp** ［**prefix-list** *name*］：NDP パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。 • **udp** ［**prefix-list** *name*］：このオプションは CLI には表示されますが、サポートされていません。行った設定は有効になりません。 • （任意）**security-level**：この機能によって適用されるセキュリティのレベルを指定します。次のいずれかのオプションを入力します。 • **glean** ：アドレスをパッシブに収集します。 • **guard**：不正なメッセージを検査してドロップします。これはデフォルトです。 • **inspect**：メッセージを収集して検証します。

	コマンドまたはアクション	目的
		• （任意）**tracking**：トラッキングオプションを指定します。次のいずれかのオプションを入力します。 • **disable** ［**stale-lifetime** ［*1-86400-seconds* | **infinite**］ ］：デバイストラッキングをオフにします。 必要に応じて、エントリを削除するまで非アクティブにする期間を入力することも、永続的に非アクティブにすることもできます。 • **enable** ［**reachable-lifetime** ［*1-86400-seconds* | **infinite**］ ］：デバイストラッキングをオンにします。 必要に応じて、エントリを到達可能にする期間を入力することも、永続的に到達可能にすることもできます。 • （任意）**trusted-port**：信頼できるポートを設定します。該当するターゲットに対するガードがディセーブルになります。信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。テーブル内にエントリを作成しているときに衝突が発生した場合、信頼できるポートが優先されます。 • （任意）**vpc**：このオプションはCLIには表示されますが、サポートされていません。行った設定は有効になりません。
ステップ5	**end** 例： `Device(config-device-tracking)# end`	デバイストラッキングコンフィギュレーションモードを終了し、特権EXECモードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show device-tracking policy** *policy-name* 例： `Device# show device-tracking policy example_policy`	デバイス トラッキング ポリシー設定を表示します。

次のタスク

ポリシーをインターフェイスまたは VLAN に適用します。

デバイス トラッキング ポリシーのインターフェイスへの適用

デバイス トラッキング ポリシーをインターフェイスにアタッチするには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface* 例： `Device(config-if)# interface gigabitethernet 1/1/4`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**device-tracking attach-policy** *policy name* 例： `Device(config-if)# device-tracking attach-policy example_policy`	インターフェイスにデバイス トラッキング ポリシーを適用します。デバイス トラッキングは、EtherChannel でもサポートされます。

	コマンドまたはアクション	目的
		（注） SISF ベースのデバイス トラッキング ポリシーは、カスタムポリシーである場合にのみ無効にできます。プログラムによって作成されたポリシーは、対応するデバイストラッキング クライアント機能の設定が削除された場合にのみ削除できます。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show device-tracking policies** [**interface** *interface*] 例： `Device# show device-tracking policies interface gigabitethernet 1/1/4`	指定されたインターフェイスの種類と番号に一致するポリシーを表示します。

デバイス トラッキング ポリシーの VLAN への適用

複数のインターフェイスでデバイス トラッキング ポリシーを VLAN にアタッチするには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan configuration** *vlan_list* 例： `Device(config)# vlan configuration 333`	デバイス トラッキング ポリシーを適用する VLAN を指定し、その VLAN インターフェイスのコンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**device-tracking attach-policy** *policy_name* 例： `Device(config-vlan-config)# device-tracking attach-policy example_policy`	すべてのスイッチインターフェイスで、デバイス トラッキング ポリシーを指定された VLAN にアタッチします。 （注） SISF ベースのデバイス トラッキング ポリシーは、カスタムポリシーである場合にのみ無効にできます。プログラムによって作成されたポリシーは、対応するデバイストラッキング クライアント機能の設定が削除された場合にのみ削除できます。
ステップ 5	**do show device-tracking policies vlan** *vlan-ID* 例： `Device(config-vlan-config)# do show device-tracking policies vlan 333`	VLAN インターフェイス コンフィギュレーション モードを終了しないで、ポリシーが指定された VLAN に割り当てられていることを確認します。
ステップ 6	**end** 例： `Device(config-vlan-config)# end`	VLAN機能コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

インターフェイス テンプレートを使用して SISF を有効にする

インターフェイステンプレートは、設定またはポリシーのコンテナです。これは、複数のコマンドを同時に設定してターゲット（インターフェイスなど）に関連付けるメカニズムを提供します。Cisco IOS XE Amsterdam 17.3.1 以降では、**device-tracking policy***policy_name* グローバル コンフィギュレーション コマンドをテンプレートに追加して、複数のターゲットに適用できます。

802.1x 認証を通じてテンプレートを適用することもできます。802.1x 認証プロセス中、さまざまなテンプレート（さまざまなポリシー）をさまざまなインターフェイスにダイナミックに割り当てることができます。

（注） 1 つのポートに適用できるインターフェイス テンプレートは 1 つだけです。

始める前に

カスタムポリシーは既に作成されています。カスタム設定を使用したカスタムデバイストラッキング ポリシーの作成 （28 ページ）を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**template interface***template_name* 例： `Device(config)# template interface template_w_sisf`	指定した名前でテンプレートを作成し、テンプレート コンフィギュレーション モードを開始します。添付の例では、「template_w_sisf」というテンプレートが作成されています。
ステップ 4	**device-tracking attach-policy***policy_name* 例： `Device (config-template)# device-tracking attach-policy sisf_policy_for_template`	ポリシーをテンプレートにアタッチします。SISF ベースのデバイストラッキングが有効になっており、テンプレートが適用される場所であればどこでもポリシーが適用されます。
ステップ 5	**exit** 例： `Device (config-template)# exit`	テンプレート コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/1/4`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**source template***template_name* 例： `Device(config-if)# source template template_w_sisf`	インターフェイス テンプレートの静的バインドの設定この添付の例では、「template_w_sisf」がインターフェイスに静的に適用されています。
ステップ 8	**end** 例： `Device(config-if)# end`	インターフェイスコンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

	コマンドまたはアクション	目的

ステップ 9	**show running-config interface** *type number*
	例：
	`Device# show running-config interface gigabitethernet 1/1/4`
	`Building configuration...`
	`<output truncated>`
	`Current configuration : 71 bytes`
	`!`
	`interface GigabitEthernet1/1/14`
	`source template template_w_sisf`
	`end`
	`<output truncated>`
		実行コンフィギュレーションの内容を表示します。

レガシー IPDT と IPv6 スヌーピングから SISF ベースのデバイストラッキングへの移行

デバイスにあるレガシー設定に基づいて、**device-tracking upgrade-cli** コマンドは CLI を異なる方法でアップグレードします。既存の設定を移行する前に、次の設定シナリオ、および対応する移行結果を検討します。

（注） 古い IPDT と IPv6 スヌーピング CLI を SISF ベースのデバイストラッキング CLI と併用することはできません。

IPDT 設定のみが存在する

デバイスに IPDT 設定のみがある場合は、**device-tracking upgrade-cli** コマンドを実行すると、設定が変換され、新しく作成されてインターフェイスで適用される SISF ポリシーが使用されます。これにより、この SISF ポリシーを更新できます。

引き続きレガシーコマンドを使用する場合、レガシーモードでの操作に制限されます。このモードでは、レガシー IPDT と IPv6 スヌーピングコマンドのみがデバイスで使用可能になります。

IPv6 スヌーピング設定のみが存在する

既存の IPv6 スヌーピング設定があるデバイスで、古い IPv6 スヌーピングコマンドを以降の設定に使用できます。次のオプションを使用できます。

- （推奨）**device-tracking upgrade-cli** コマンドを使用して、レガシー設定をすべて、新しい SISF ベースのデバイス トラッキング コマンドに変換します。変換後は、新しいデバイス トラッキング コマンドのみがデバイスで動作します。

- レガシー IPv6 スヌーピングコマンドを今後の設定に使用し、**device-tracking upgrade-cli** コマンドは実行しません。このオプションでは、デバイスで使用可能なのはレガシー IPv6 スヌーピングコマンドのみであり、新しい SISF ベースのデバイストラッキング CLI コマンドは使用できません。

IPDT と IPv6 スヌーピングの両方の設定が存在する

レガシー IPDT 設定と IPv6 スヌーピング設定の両方が存在するデバイスでは、レガシーコマンドを SISF ベースのデバイストラッキング CLI コマンドに変換できます。ただし、インターフェイスに適用することができるスヌーピングポリシーは 1 つだけであり、IPv6 スヌーピング ポリシー パラメータは IPDT 設定よりも優先される、ということに注意してください。

（注） 新しい SISF ベースのコマンドに移行しておらず、レガシー IPv6 スヌーピングや IPDT コマンドを使用し続けている場合、IPv4 デバイストラッキング設定情報が IPv6 スヌーピングコマンドに表示される可能性があります。SISF ベースのデバイストラッキング機能では、IPv4 と IPv6 の両方の設定を扱うためです。これを回避するには、レガシー設定を SISF ベースのデバイストラッキング コマンドに変換することを推奨します。

IPDT または IPv6 スヌーピング設定が存在しない

デバイスにレガシー IP デバイストラッキング設定も IPv6 スヌーピング設定もない場合は、今後の設定に使用できるのは新しい SISF ベースのデバイス トラッキング コマンドのみです。レガシー IPDT コマンドと IPv6 スヌーピングコマンドは使用できません。

SISF の設定例

例：DHCP スヌーピングを設定してプログラムで SISF を有効にする

次の例は、グローバル コンフィギュレーション モードで **ip dhcp snooping vlan** *vlan* コマンドを設定して、SISF ベースのデバイストラッキングを有効にする方法を示しています。この方法で SISF を有効にすると、`DT-PROGRMMATIC` ポリシーが作成されます。

特権 EXEC モードで **show device-tracking policy** *policy_name* コマンドを入力して、`DT-PROGRMMATIC` ポリシーの設定を表示します。

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp snooping vlan 10
Device(config)# end

Device# show device-tracking policy DT-PROGRAMMATIC

Policy DT-PROGRAMMATIC configuration:
  security-level glean (*)
  device-role node
  gleaning from Neighbor Discovery
```

```
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 1 (*)
  tracking enable
Policy DT-PROGRAMMATIC is applied on the following targets:
Target      Type    Policy              Feature           Target range
vlan 10     VLAN    DT-PROGRAMMATIC     Device-tracking   vlan all


  note:
  Binding entry Down timer: 24 hours (*)
  Binding entry Stale timer:   24 hours (*)
```

例：VLAN で EVPN を設定してプログラムで SISF を有効にする

EVPN を設定すると、プログラムのポリシー `evpn-sisf-policy` が自動的に作成されます。ポリシー設定を表示するには、特権 EXEC モードで **show device-tracking policy** *policy_name* コマンドを入力します。

```
Device# show device-tracking policy evpn-sisf-policy

Policy evpn-sisf-policy configuration:
  security-level glean (*)
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  tracking enable
Policy evpn-sisf-policy is applied on the following targets:
Target      Type    Policy                  Feature           Target range
vlan 10     VLAN    evpn-sisf-policy        Device-tracking   vlan all
  note:
  Binding entry Down timer: 24 hours (*)
  Binding entry Stale timer:   24 hours (*)
```

例：LISP（LISP-DT-GLEAN-VLAN）を設定してプログラムで SISF を有効にする

LISP を設定すると、プログラムのポリシー `LISP-DT-GUARD-VLAN` が自動的に作成されます。ポリシー設定を表示するには、特権 EXEC モードで **show device-tracking policy** *policy_name* コマンドを入力します。

（注） システムは、LISP の設定方法に応じて `LISP-DT-GUARD-VLAN` または `LISP-DT-GLEAN-VLAN` を作成します。これを変更することはできませんが、必要に応じて、カスタム設定でカスタムポリシーを作成し、それを必要なターゲットにアタッチできます。

```
Device# show device-tracking policy LISP-DT-GLEAN-VLAN

Policy LISP-DT-GLEAN-VLAN configuration:
```

```
  security-level glean (*)
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 4 (*)
  limit address-count for IPv6 per mac 12 (*)
  tracking enable
Policy LISP-DT-GUARD-VLAN is applied on the following targets:
Target     Type   Policy                 Feature            Target range
vlan 10    VLAN   LISP-DT-GLEAN-VLAN     Device-tracking    vlan all

  note:
  Binding entry Down timer: 10 minutes (*)
  Binding entry Stale timer:   30 minutes (*)
```

例：LISP（LISP-DT-GUARD-VLAN）を設定し、プログラムでSISFを有効にする

LISP を設定すると、プログラムのポリシー `LISP-DT-GUARD-VLAN` が自動的に作成されます。ポリシー設定を表示するには、特権 EXEC モードで **show device-tracking policy** *policy_name* コマンドを入力します。

（注） システムは、LISP の設定方法に応じて `LISP-DT-GUARD-VLAN` または `LISP-DT-GLEAN-VLAN` を作成します。これを変更することはできませんが、必要に応じて、カスタム設定でカスタムポリシーを作成し、それを必要なターゲットにアタッチできます。

```
Device# show device-tracking policy LISP-DT-GUARD-VLAN

Policy LISP-DT-GUARD-VLAN 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
  limit address-count for IPv4 per mac 4 (*)
  limit address-count for IPv6 per mac 12 (*)
  tracking enable
Policy LISP-DT-GUARD-VLAN is applied on the following targets:
Target      Type    Policy                   Feature            Target range
vlan 10     VLAN    LISP-DT-GUARD-VLAN       Device-tracking    vlan all
  note:
  Binding entry Down timer: 10 minutes (*)
  Binding entry Stale timer:   30 minutes (*)
```

例：IPv4 重複アドレスの問題の緩和

次に、Microsoft Windows を実行しているクライアントによって発生した`重複 IP アドレス 0.0.0.0` エラーメッセージの問題に対応する例を示します。

device-tracking tracking auto-source コマンドをグローバル コンフィギュレーション モードで設定します。このコマンドは、デバイストラッキング テーブル内のエントリを維持するために、スイッチがクライアントをプローブするよう送信するアドレス解決パケット（ARP）要求で使用される送信元 IP および MAC アドレスを決定します。その目的は、送信元 IP アドレスとして 0.0.0.0 を使用しないようにすることです。

（注） スイッチ仮想インターフェイス（SVI）が設定されていない場合に、**device-tracking tracking auto-source** コマンドを設定します。SVI が VLAN で IPv4 アドレスを使用して設定されている場合は、設定する必要はありません。

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）	注記
device-tracking tracking auto-source	• 存在する場合、VLAN SVI に送信元を設定します。 • 同じサブネットからデバイストラッキング テーブルで IP および MAC バインディングを検索します。 • 0.0.0.0 を使用します	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。
device-tracking tracking auto-source override	• 存在する場合、VLAN SVI に送信元を設定します。 • 0.0.0.0 を使用します。	SVI がない場合は推奨しません。

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）	注記
ip device tracking probe auto-source fallback 0.0.0.X 255.255.255.0	• 存在する場合、VLAN SVI に送信元を設定します。 • 同じサブネットからデバイストラッキング テーブルで IP および MAC バインディングを検索します。 • 提供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、クライアント側のスイッチポートの MAC アドレスから取得されます*。	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 アドレスは、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 tracking auto-source fallback 0.0.0.X 255.255.255.0 override	• 存在する場合、VLAN SVI に送信元を設定します。 提供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、クライアント側のスイッチポートの MAC アドレスから取得されます*。	

* クライアント IP アドレスによっては、IPv4 アドレスを送信元 IP 用に予約する必要があります。

予約済み送信元 IPv4 アドレス = (host-ip and mask) | client-ip

- クライアント IP = 192.0.2.25
- 送信元 IP = (192.0.2.25 and 255.255.255.0) | (0.0.0.1) = 192.0.2.1

IP アドレス 192.0.2.1 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ないでください。

例：ターゲットでの IPv6 デバイストラッキングの無効化

デフォルトで、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ます。次の設定例は、サポートされている場合に IPv6 デバイストラッキングを無効にする方法を示しています。

カスタムポリシーがターゲットに適用されている場合に、IPv6 のデバイストラッキングを無効にする（すべてのリリース）：

```
Device(config)# device-tracking policy example-policy
 Device(config-device-tracking)# no protocol ndp
 Device(config-device-tracking)# no protocol dhcp6
 Device(config-device-tracking)# end
```

プログラムポリシーがターゲットに適用されている場合に、IPv6 のデバイストラッキングを無効にする（Cisco IOS XE Everest 16.6.x および Cisco IOS XE Fuji 16.8.x のみ）：

```
Device(config)# device-tracking policy DT-PROGRAMMATIC
Device(config-device-tracking)# no protocol ndp
Device(config-device-tracking)# no protocol dhcp6
Device(config-device-tracking)# end
```

（注）
- Cisco IOS XE Everest 16.5.x リリースでは、プログラムポリシーが適用されている場合、IPv6 のデバイストラッキングを無効にすることはできません。
- Cisco IOS XE Everest 16.6.x および Cisco IOS XE Fuji 16.8.x では、プログラムポリシーが適用されている場合、上の例に示すように、IPv6 のデバイストラッキングを無効にすることができます。
- Cisco IOS XE Fuji 16.9.x 以降では、プログラムポリシーの設定を変更できません。

例：VLAN 上の SVI に対する IPv6 の有効化（重複アドレスの問題を軽減するため）

ネットワークで IPv6 が有効になっており、VLAN 上でスイッチ仮想インターフェイス（SVI）が設定されている場合は、SVI 設定に次の内容を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るため、重複 IP アドレスの問題を防止できます。

```
Device> enable
Device# configure terminal
Device(config)# interface vlan 10
Device(config-if)# ipv6 enable
Device(config-if)# end
```

例：トランクポートからのバインディングエントリの作成を停止するためのマルチスイッチネットワークの設定

マルチスイッチネットワークでは、SISFベースのデバイストラッキングにより、機能を実行しているスイッチ間でバインディング テーブル エントリを分散できます。バインディングエントリは、ホストがアクセスポートに表示されるスイッチでのみ作成されます。トランクポート経由で表示されるホストのエントリは作成されません。これは、**trusted-port**および**device-role switch**オプションを使用してポリシーを設定し、トランクポートに適用することで実現されます。

（注） ポリシーで、**trusted-port** および **device-role switch** オプションの両方を設定する必要があります。

さらに、SISFベースのデバイストラッキングが有効になっているデバイス側のポートに、このようなポリシーを適用することを推奨します。

```
Device> enable
Device# configure terminal
Device(config)# device-tracking policy example_trusted_policy
Device(config-device-tracking)# device-role switch
Device(config-device-tracking)# trusted-port
Device(config-device-tracking)# exit
Device(config)# interface gigabitethernet 1/0/25
Device(config-if)# device-tracking attach-policy  example_trusted_policy
Device(config-if)# end
```

例：短いデバイストラッキング バインディング到達可能時間の回避

以前のリリースから移行する場合、次の設定が存在している可能性があります。

```
device-tracking binding reachable-time 10
```

コマンドの **no** バージョンを入力して、これを削除します。

```
Device> enable
Device# configure terminal
Device(config)# no device-tracking binding reachable-time 10
Device(config)# end
```

SISF の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	SISF ベースのデバイス トラッキング	この機能が導入されました。 SISF ベースのデバイストラッキングは、ネットワーク内のエンドノードの存在、ロケーション、移動を追跡します。この機能は、スイッチが受信したトラフィックをスヌーピングし、デバイスアイデンティティ（MAC と 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。（デバイス トラッキング クライアントと呼ばれる）その他の機能の適切な動作は、この情報の正確性に依存します。 IPv4 および IPv6 のどちらもサポートされています。 デフォルトでは、SISF ベースのデバイストラッキングは無効になっています。
Cisco IOS XE Everest 16.6.1	DT_PROGRAMMATIC のパラメータを変更するオプション	このリリース以降、プログラムで作成されたデバイス トラッキング ポリシー（DT_PROGRAMMATIC）の特定の設定をデバイス トラッキング コンフィギュレーション モード（config-device-tracking）で変更できます。
Cisco IOS XE Fuji 16.9.1	ポリシーの優先順位 追加のデバイス追跡クライアント プログラムで作成されたポリシーの変更	ポリシーの優先順位のサポートが導入されました。優先順位は、ポリシーの作成方法によって決まります。手動で作成されたポリシーが最も優先されます。これにより、プログラムで生成されたポリシーとは異なるポリシー設定を適用できます。 デバイストラッキング クライアント機能が追加されました。プログラムで作成されるポリシーは、デバイストラッキング クライアントごとに異なります。 任意のプログラムで作成されるポリシーのパラメータを変更するオプションは廃止されました。

リリース	機能	機能情報
Cisco IOS XE Amsterdam 17.3.1	Interface template	インターフェイス テンプレートを使用して SISF ベースのデバイストラッキングを有効にするオプションが導入されました。 **device-tracking policy** *policy_name* グローバル コンフィギュレーション コマンドをテンプレートに追加して、複数のターゲットに適用できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com に進みます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。