# Configuring SISF-Based Device Tracking

# Information About SISF-Based Device Tracking

## Overview of SISF-Based Device Tracking

The Switch Integrated Security Features based (SISF-based) device tracking feature is part of the suite of first-hop security features.

The main role of the feature is to track the presence, location, and movement of end-nodes in the network. SISF snoops traffic received by the switch, extracts device identity (MAC and IP address), and stores them in a binding table. Many features, such as, IEEE 802.1X, web authentication, Cisco TrustSec and LISP etc., depend on the accuracy of this information to operate properly.

SISF-based device tracking supports both IPv4 and IPv6.

Even with the introduction of SISF-based device tracking, the legacy device tracking CLI (IP Device Tracking (IPDT) and IPv6 Snooping CLI) continues to be available. When you bootup the switch, the set of commands that are available depend on existing configuration, and only one of the following is available:

- SISF-based device tracking CLI
- IPDT and IPv6 Snooping CLI

**Note** The IPDT and IPv6 Snooping commands are deprecated, but continue to be available. We recommend that you upgrade to SISF-based device tracking.

If you are using the IPDT and IPv6 Snooping CLI and want to migrate to SISF-based device tracking, see *Migrating from legacy IPDT and IPv6 Snooping to SISF-Based Device Tracking*, for more information.

SISF-based device tracking can be enabled manually (by using **device-tracking** commands), or programmatically (which is the case when providing device tracking services to other features).

# Options to Enable SISF-Based Device Tracking

SISF-Based device tracking is disabled by default.

You can enable it by defining a device tracking policy and attaching the policy to a specific target.

**Note** The target could be an interface or a VLAN.

### Manually Enabling the Feature SISF-Based Device Tracking Commands

- Option 1: Apply the **default** device tracking policy to a target.

  Enter the **device-tracking** command in the interface configuration mode or in the VLAN configuration mode. The system then attaches the **default** policy it to the interface or VLAN.

  **Note** The **default** policy is a built-in policy with default settings; you cannot change any of the attributes of the **default** policy. In order to be able to configure device tracking policy attributes you must create a custom policy. See *Option 2: Create a custom policy with custom settings*.

- Option 2: Create a custom policy with custom settings.

  Enter the device-tracking policy command in global configuration mode and enter a custom policy name. The system creates a policy with the name you specify. You can then configure the available settings, in the device tracking configuration mode (config-device-tracking), and attach the policy to a specified target.

### Programmatically Enabling the Feature

Some features rely on device tracking and utilize the trusted database of binding entries that SISF-based device tracking builds and maintains. These features, also called device tracking clients, enable device tracking programmatically (create and attach the device tracking policy).

**Note** The exceptions here are IEEE 802.1X, web authentication, Cisco TrustSec, and IP Source Guard (IPSG) - they also rely on device tracking, but they do not enable it. For these device tracking clients, you must enter the **ip dhcp snooping vlan** *vlan* command, to programmatically enable device tracking on a particular target.

Note the following about programmatically enabling SISF-based device tracking:

- A device tracking client *requires* device tracking to be enabled.

  There are several device tracking clients, therefore, multiple programmatic policies could be created. The settings of each policy differ depending on the device tracking client that creates the policy.

- The policy that is created, and its settings, are system-defined.

Configurable policy attributes are available in the device tracking configuration mode (config-device-tracking) and vary from one release to another. If you try to modify an attribute that is not configurable, the configuration change is rejected and an error message is displayed.

For release-specific information about programmatically created policies, see *Programmatically Enabling SISF-Based Device Tracking in Cisco IOS XE <release name> <release number>* in the required version of the document.

# Migrating from Legacy IPDT and IPv6 Snooping to SISF-Based Device Tracking

Based on the legacy configuration that exists on your device, the **device-tracking upgrade-cli** command upgrades your CLI differently. Consider the following configuration scenarios and the corresponding migration results before you migrate your existing configuration.

**Note** You cannot configure a mix of the old IPDT and IPv6 snooping CLI with the SISF-based device tracking CLI.

### Only IPDT Configuration Exists

If your device has only IPDT configuration, running the **device-tracking upgrade-cli** command converts the configuration to use the new SISF policy that is created and attached to the interface. You can then update this SISF policy.

If you continue to use the legacy commands, this restricts you to operate in a legacy mode where only the legacy IPDT and IPv6 snooping commands are available on the device.

### Only IPv6 Snooping Configuration Exists

On a device with existing IPv6 snooping configuration, the old IPv6 Snooping commands are available for further configuration. The following options are available:

- (Recommended) Use the **device-tracking upgrade-cli** command to convert all your legacy configuration to the new SISF-based device tracking commands. After conversion, only the new device tracking commands will work on your device.
- Use the legacy IPv6 Snooping commands for your future configuration and do not run the **device-tracking upgrade-cli** command. With this option, only the legacy IPv6 Snooping commands are available on your device, and you cannot use the new SISF-based device tracking CLI commands.

### Both IPDT and IPv6 Snooping Configuration Exist

On a device that has both legacy IPDT configuration and IPv6 snooping configuration, you can convert legacy commands to the SISF-based device tracking CLI commands. However, note that only one snooping policy can be attached to an interface, and the IPv6 snooping policy parameters override the IPDT settings.

**Note** If you do not migrate to the new SISF-based commands and continue to use the legacy IPv6 snooping or IPDT commands, your IPv4 device tracking configuration information may be displayed in the IPv6 snooping commands, as the SISF-based device tracking feature handles both IPv4 and IPv6 configuration. To avoid this, we recommend that you convert your legacy configuration to SISF-based device tracking commands.

#### No IPDT or IPv6 Snooping Configuration Exists

If your device has no legacy IP Device Tracking or IPv6 Snooping configurations, you can use only the new SISF-based device tracking commands for all your future configuration. The legacy IPDT commands and IPv6 snooping commands are not available.

# How to Configure SISF-Based Device Tracking

## Manually Enabling SISF-Based Device Tracking

### Applying the Default Device Tracking Policy to a Target

Beginning in privileged EXEC mode, follow these steps to apply the default device tracking policy to an interface or VLAN:

#### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters the global configuration mode. |
| **Step 2** | Specify an interface or a VLAN<br>- **interface** *interface*<br>- **vlan configuration** *vlan_list*<br>**Example:**<br>`Device(config)# interface gigabitethernet 1/1/4`<br>`OR`<br>`Device(config)# vlan configuration 333` | **interface** *type number*—Specifies the interface and enters the interface configuration mode. The device tracking policy will be attached to the specified interface.<br>**vlan configuration** *vlan_list*—Specifies the VLANs and enters the VLAN feature configuration mode. The device tracking policy will be attached to the specified VLAN. |
| **Step 3** | **device-tracking**<br>**Example:**<br>`Device(config-if)# device-tracking`<br>`OR`<br>`Device(config-vlan-config)# device-tracking` | Enables SISF-based device tracking and attaches the default policy it to the interface or VLAN.<br>The default policy is a built-in policy with default settings; none of the attributes of the default policy can be changed. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **exit**<br>**Example:**<br>`Device(config-if)# exit`<br>`OR`<br>`Device(config-vlan-config)# exit` | Exits configuration mode. |
| **Step 5** | **show device-tracking policy** *policy-name*<br>**Example:**<br>`Device# show device-tracking policy default` | Displays device-tracking policy configuration, and all the targets it is applied to. |

## Creating a Custom Device Tracking Policy with Custom Settings

Beginning in privileged EXEC mode, follow these steps to create and configure a device tracking policy:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters the global configuration mode. |
| **Step 2** | [**no**] **device-tracking policy** *policy-name*<br>**Example:**<br>`Device(config)# device-tracking policy example_policy` | Creates the policy and enters the device-tracking configuration mode. |
| **Step 3** | [**data-glean** \| **default** \| **destination-glean** \| **device-role** \| **distribution-switch** \| **exit** \| **limit** \| **no** \| **prefix-glean** \| **protocol** \| **security-level** \| **tracking** \| **trusted-port** \| **vpc**]<br>**Example:**<br>`Device (config-device-tracking)# destination-glean log-only` | Enter the question mark (?) at the system prompt to obtain a list of available options in this mode. You can configure the following for both IPv4 and IPv6:<br>• (Optional) **data-glean**—Enables learning of addresses from a data packet snooped from a source inside the network and populates the binding table with the data traffic source address. Enter one of these options:<br>  • log-only—Generates a syslog message upon data packet notification<br>  • recovery—Uses a protocol to enable binding table recovery. Enter **NDP** or **DHCP**.<br>• (Optional) **default**—Sets the policy attribute to its default value. You can set |

| | Command or Action | Purpose |
|---|---|---|
| | | these policy attributes to their default values: **data-glean**, **destination-glean**, **device-role**, **limit**, **prefix-glean**, **protocol**, **security-level**, **tracking**, **trusted-port**.<br>• (Optional) **destination-glean**—Populates the binding table by gleaning data traffic destination address. Enter one of these options:<br>  • log-only—Generates a syslog message upon data packet notification<br>  • recovery—Uses a protocol to enable binding table recovery. Enter **DHCP**.<br>• (Optional) **device-role**—Sets the role of the device attached to the port. It can be a node or a switch. Enter one of these options:<br>  • node—Configures the attached device as a node. This is the default option.<br>  • switch—Configures the attached device as a switch.<br>• (Optional) **distribution-switch**—Although visible on the CLI, this option is not supported. Any configuration settings you make will not take effect.<br>• **exit**—Exits the device-tracking policy configuration mode.<br>• **limit** address-count—Specifies an address count limit per port. The range is 1 to 32000.<br>• **no**—Negates the command or sets it to defaults.<br>• (Optional) **prefix-glean**—Enables learning of prefixes from either IPv6 Router Advertisements or from DHCP-PD. You have the following option:<br>  • (Optional) **only**—Gleans only prefixes and not host addresses.<br>• (Optional) **protocol**—Sets the protocol to glean; by default, all are gleaned. Enter one of these options: |

| | Command or Action | Purpose |
|---|---|---|
| | | • **arp** [**prefix-list** *name*]—Gleans addresses in ARP packets. Optionally, enter the name of prefix-list that is to be matched.<br>• **dhcp4** [**prefix-list** *name*]—Glean addresses in DHCPv4 packets. Optionally, enter the name of prefix-list that is to be matched.<br>• **dhcp6** [**prefix-list** *name*]—Glean addresses in DHCPv6 packets. Optionally, enter the name of prefix-list that is to be matched.<br>• **ndp** [**prefix-list** *name*]—Glean addresses in NDP packets. Optionally, enter the name of prefix-list that is to be matched.<br>• **udp** [**prefix-list** *name*]—Although visible on the CLI, this option is not supported. Any configuration settings you make will not take effect.<br>• (Optional) **security-level**—Specifies the level of security enforced by the feature. Enter one of these options:<br>• **glean**—Gleans addresses passively.<br>• **guard**—Inspects and drops un-authorized messages. This is the default.<br>• **inspect**—Gleans and validates messages.<br>• (Optional) **tracking**—Specfies a tracking option. Enter one of these options:<br>• **disable** [**stale-lifetime** [*1-86400-seconds* \| **infinite**] ]—Turns of device-tracking.<br>Optionally, you can enter the duration for which the entry is kept inactive before deletion, or keep it permanently inactive.<br>• **enable** [**reachable-lifetime** [*1-86400-seconds* \| **infinite**] ]—Turns on device-tracking. |

| | Command or Action | Purpose |
|---|---|---|
| | | Optionally, you can enter the duration for which the entry is kept reachable, or keep it permanently reachable.<br>• (Optional) **trusted-port**—Sets up a trusted port. Disables the guard on applicable targets. Bindings learned through a trusted port have preference over bindings learned through any other port. A trusted port is given preference in case of a collision while making an entry in the table.<br>• (Optional) **vpc**—Although visible on the CLI, this option is not supported. Any configuration settings you make will not take effect. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config-device-tracking)# exit` | Exits configuration mode. |
| **Step 5** | **show device-tracking policy** *policy-name*<br>**Example:**<br>`Device# show device-tracking policy example_policy` | Displays the device-tracking policy configuration. |

### What to do next

Attach the policy to an interface or VLAN.

## Attaching a Device Tracking Policy to an Interface

Beginning in privileged EXEC mode, follow these steps to attach a device tracking policy to an interface:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters the global configuration mode. |
| **Step 2** | **interface** *interface*<br>**Example:**<br>`Device(config)# interface gigabitethernet 1/1/4` | Specifies an interface and enters the interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | [**no**]**device-tracking attach-policy** *policy name*<br>**Example:**<br>`Device(config-if)# device-tracking attach-policy example_policy` | Attaches the device tracking policy to the interface. Device tracking is also supported on EtherChannels.<br>**Note** SISF based device-tracking policies can be disabled only if they are custom policies. Programmatically created policies can be removed only if the corresponding device-tracking client feature configuration is removed. |
| **Step 4** | **end**<br>**Example:**<br>`Device# end` | Returns to the privileged EXEC mode. |
| **Step 5** | **show device-tracking policies** [**interface** *interface*]<br>**Example:**<br>`Device# show device-tracking policies interface gigabitethernet 1/1/4` | Displays policies that match the specified interface type and number. |

## Attaching a Device Tracking Policy to a VLAN

Beginning in privileged EXEC mode, follow these steps to attach a device-tracking policy to VLANs across multiple interfaces:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters the global configuration mode. |
| **Step 2** | **vlan configuration** *vlan_list*<br>**Example:**<br>`Device(config)# vlan configuration 333` | Specifies the VLANs to which the device tracking policy will be attached; enters the VLAN interface configuration mode. |
| **Step 3** | [**no**]**device-tracking attach-policy** *policy_name*<br>**Example:** | Attaches the device tracking policy to the specified VLANs across all switch interfaces. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-vlan-config)# device-tracking attach-policy example_policy` | **Note** SISF based device-tracking policies can be disabled only if they are custom policies. Programmatically created policies can be removed only if the corresponding device-tracking client feature configuration is removed. |
| **Step 4** | **do show device-tracking policies vlan** *vlan-ID*<br>**Example:**<br>`Device(config-vlan-config)# do show device-tracking policies vlan 333` | Verifies that the policy is attached to the specified VLAN, without exiting the VLAN interface configuration mode. |

# Programmatically Enabling SISF-Based Device Tracking in Cisco IOS XE Everest 16.5.x

*Table 1: Programmatically Enabling SISF-Based Device Tracking in Cisco IOS XE Everest 16.5.x*

| | |
|---|---|
| Device tracking client features that can enable SISF-based device tracking | In this release, you can programmatically enable SISF-based device tracking for these features:<br>• IEEE 802.1X, web authentication, Cisco TrustSec, and IPSG features: enter the **ip dhcp snooping vlan** *vlan* command.<br>• Cisco Locator/ID Separation Protocol.<br>**Note** LISP settings are effective, if there is more than one programmatically created policy. This does not adversely affect the way, any of the other device tracking client features work. For example, if you have configured the **ip dhcp snooping vlan** *vlan* command for IEEE 802.1X, and also enabled SISF-based device tracking by configuring LISP, the IEEE 802.1X feature continues to work as expected. |
| Policy Name | DT-PROGRAMMATIC<br>Although there is more than one device tracking client feature, the system-generated policy is one and the same; the list of settings may differ with each programmatically created policy. See the examples for more information. |

| | |
|---|---|
| User Options | • Only one policy can be attached to the same interface or VLAN.<br>• The policy cannot be replaced by another policy.<br>• The policy cannot be removed unless the device tracking client feature configuration is removed.<br>• The policy attributes cannot be changed.<br>• The address count limit per MAC setting cannot be changed (This refers to the **limit address-count for IPv4 per mac** and **limit address-count for IPv6 per mac** commands), but the address count limit per port or interface can be changed.<br>• When a device-tracking policy is attached to an interface under a VLAN, the policy settings on the interface take precedence over those on its VLAN; exceptions here are the values for **limit address-count for IPv4 per mac** and **limit address-count for IPv6 per mac**, which are aggregated from the policy on both the interface and VLAN. |

# Configuring a Multi-Switch Network to Stop Creating Binding Entries from a Trunk Port

In a multi-switch network, SISF-based device tracking provides the capability to distribute binding table entries between switches running the feature. Binding entries are only created on the switches where the host appears on an access port. No entry is created for a host that appears over a trunk port. This is achieved by configuring a policy with the **trusted-port** and **device-role switch** options, and attaching it to the trunk port.

**Important** Both, the **trusted-port**, and **device-role switch** options, must be configured in the policy.

Further, we recommended that you apply such a policy on a port facing a device, which also has SISF-based device tracking enabled.

Complete the following steps:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters the global configuration mode. |
| **Step 2** | **device-tracking policy** *policy-name*<br>**Example:**<br>`Device(config)# device-tracking policy example_trusted_policy` | Enters the device-tracking policy configuration mode, for the specified policy. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **device-role switch**<br>**Example:**<br>`Device(config-device-tracking)# device-role switch` | Specifies the role of the device attached to the port. Default is node. Enter the **device-role switch** option to stop the creation of binding entries for the port. |
| **Step 4** | **trusted-port**<br>**Example:**<br>`Device(config-device-tracking)# trusted-port` | Sets up a trusted port. Disables the guard on applicable targets. Bindings learned through a trusted port have preference over bindings learned through any other port. A trusted port is given preference in case of a collision while making an entry in the table. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-device-tracking)# end` | Exits the device-tracking policy configuration mode and enters the global configuration mode |
| **Step 6** | **interface** *interface*<br>**Example:**<br>`Device(config)# interface gigabitethernet 1/0/25` | Specifies an interface and enters the interface configuration mode. |
| **Step 7** | **device-tracking attach-policy** *policy-name*<br>**Example:**<br>`Device(config-if)# device-tracking attach-policy  example_trusted_policy` | Attaches a device tracking policy to the interface or the specified VLANs on the interface. |

# Configuration Examples for SISF-Based Device Tracking

These examples show sample device-tracking configuration and other recommended or related configuration for certain situations.

## Example: Programmatically Enabling SISF-Based Device Tracking in Cisco IOS XE Everest 16.5.x

The sample output in the examples show the different settings of programmatically created policies.

### Device tracking client: LISP

The LISP configuration here is only meant to serve as an example.

After you configure LISP, enter the **show device-tracking policy** command in privileged EXEC mode, to display the `DT-PROGRAMMATIC` policy that is created and the corresponding settings:

```
Device(config)# router lisp
<output truncated>
Device(config-router-lisp)# instance-id 3
Device(config-router-lisp-instance)# service ethernet
Device(config-router-lisp-instance-service)# eid-table vlan 10
Device(config-router-lisp-instance-dynamic-eid)# database-mapping 10.1.1.0/24 locator-set
set1
Device(config-router-lisp-instance-service)# exit-service-ethernet
Device(config-router-lisp-instance)# exit-instance-id
Device(config-router-lisp)# exit-router-lisp

Device# show device-tracking policy DT-PROGRAMMATIC
Policy DT-PROGRAMMATIC 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
  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: 10 minutes (*)
 Binding entry Stale timer: 60 minutes (*)
```

### Device tracking clients: IEEE 802.1X, Web Authentication, Cisco TrustSec, IPSG

Configure the **ip dhcp snooping vlan** *vlan* command in global configuration mode to enable device-tracking for the IEEE 802.1X, web authentication, Cisco TrustSec, and IPSG features. Enter the **show device-tracking policy** command in privileged EXEC mode, to display the `DT-PROGRMMATIC` policy that is created and the corresponding settings that are made:

```
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
  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 (*)
```

# Example: Disabling IPv6 Device Tracking on a Target

By default, SISF-based device tracking supports both IPv4 and IPv6. The following configuration examples show how you can disable IPv6 device tracking if you have to:

**Disabling IPv6 device tracking when the target is attached to a custom policy:**

```
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
```

**Note** In the Cisco IOS XE Everest 16.5.x release, you cannot disable IPv6 device tracking for a programmatically created policy.

# Example: Enabling IPv6 for SVI on VLAN (To Mitigate the Duplicate Address Problem)

When IPv6 is enabled in the network and a switched virtual interface (SVI) is configured on a VLAN, we recommend that you add the following to the SVI configuration. This enables the SVI to acquire a link-local address automatically; this address is used as the source IP address of the SISF probe, thus preventing the duplicate IP address issue.

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

# Example: Mitigating the IPv4 Duplicate Address Problem

This example shows how you can tackle the `Duplicate IP Address 0.0.0.0 error message` problem encountered by clients that run Microsoft Windows:

Configure the **device-tracking tracking auto-source** command in global configuration mode. This command determines the source IP and MAC address used in the Address Resolution Packet (ARP) request sent by the switch to probe a client, in order to maintain its entry in the device-tracking table. The purpose, is to avoid using 0.0.0.0 as source IP address.

**Note** Configure the **device-tracking tracking auto-source** command when a switch virtual interface (SVI) is not configured. You do not have to configure it when a SVI is configured with an IPv4 address on the VLAN.

| Command | Action<br>**(In order to select source IP and MAC address for device tracking ARP probe)** | Notes |
|---|---|---|
| **device-tracking tracking auto-source** | • Set source to VLAN SVI if present.<br>• Look for IP and MAC binding in device-tracking table from same subnet.<br>• Use 0.0.0.0 | We recommend that you disable device-tracking on all trunk ports to avoid MAC flapping. |
| **device-tracking tracking auto-source override** | • Set source to VLAN SVI if present<br>• Use 0.0.0.0 | Not recommended when there is no SVI. |
| **ip device tracking probe auto-source fallback 0.0.0.X 255.255.255.0** | • Set source to VLAN SVI if present.<br>• Look for IP and MAC binding in device-tracking table from same subnet.<br>• Compute source IP from client IP using host bit and mask provided. Source MAC is taken from the MAC address of the switchport facing the client*. | We recommend that you disable device-tracking on all trunk ports to avoid MAC flapping.<br>The computed IPv4 address must not be assigned to any client or network device. |
| **device-tracking tracking auto-source fallback 0.0.0.X 255.255.255.0 override** | • Set source to VLAN SVI if present.<br>Compute source IP from client IP using host bit and mask provided*. Source MAC is taken from the MAC address of the switchport facing the client*. | |

* Depending on the client IP address, an IPv4 address has to be reserved for the source IP.

A reserved source IPv4 address = (host-ip and mask) | client-ip

- Client IP = 192.0.2.25
- Source IP = (192.0.2.25 and 255.255.255.0) | (0.0.0.1) = 192.0.2.1

IP address 192.0.2.1 should not be assigned to any client or network device.

## Example: Avoiding a Short Device-Tracking Binding Reachable Time

When migrating from an older release, the following configuration may be present:

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

Remove this by entering the **no** version of the command.

# Feature History and Information for SISF-Based Device Tracking

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

| Release | Modification |
|---|---|
| Cisco IOS XE Everest 16.5.1a | This feature was introduced. |