Verify IPDT Device Operations

Contents

Introduction

Prerequisites

- Requirements
- Components Used

IPDT Overview

- Definition and Usage
- Excerpt
- Problem
- Default State and Operation
- Functionality Areas
- Feature Matrix
- Features

Disable IPDT

- Enter the IP Device Tracking Probe Delay 10 Command
- Enter the IP Device Tracking Probe Use SVI Command
- Enter the IP Device Tracking Probe Auto-Source [fallback] [override] Command
- Enter the IP Device Tracking Probe Auto-Source Command
- Enter the IP Device Tracking Probe Auto-Source Fallback 0.0.0.1 255.255.255.0 Command
- Enter the IP Device Tracking Probe Auto-Source Fallback 0.0.0.1 255.255.255.0 Override Command
- Enter the IP Device Tracking Maximum 0Command
- Turn Off Active Features that Trigger IPDT
  - Example:

Verify IPDT Operation

Introduction

This document describes how to verify IP Device Tracking (IPDT) operations and some troubleshooting actions.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The outputs in this document were based on these software and hardware versions:

- Cisco WS-C2960X
- Cisco IOS® 15.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

IPDT Overview

Definition and Usage

The main IPDT task is to keep track of connected hosts (association of MAC and IP address). To do this, it sends unicast Address Resolution Protocol (ARP) probes with a default interval of 30 seconds. These probes are sent to the MAC address of the host connected on the other side of the link, and uses Layer 2 (L2) as the default source. This allows the MAC address of the physical interface out of which the ARP goes and a sender IP address of 0.0.0.0, based on the ARP Probe definition listed in RFC 5227.

Note: IPDT has been deprecated in favor of SISF-Based (Switch Integrated Security Features) Device Tracking. SISF provides enhanced IP tracking and supports both IPv4 and IPv6.

Starting with Cisco IOS® XE Denali 16.1.1, the existing IPv6 snooping and IP Device Tracking (IPDT) commands have corresponding SISF-based device-tracking commands that allow you to apply your configuration to both IPv4 and IPv6 address families.

This document is preserved for reference as it pertains to legacy IP Device Tracking (IPDT) functionality. Current deployments can use SISF-based device-tracking, which supersedes IPDT in modern Cisco IOS-XE platforms. For additional guidance on troubleshooting SISF, see Troubleshoot SISF on Catalyst 9000 Series Switches.

Excerpt

In this document, the term ARP Probe is used to refer to an ARP Request packet, broadcast on the local link, with an all-zero sender IP address. The sender hardware address MUST contain the hardware address of the interface that sends the packet. The sender IP address field MUST be set to all zeroes to avoid corruption that ARP caches in other hosts, on the same link, in the case where the address turns out to be already in use by another host. The target IP address field MUST be set to the address that is probed. An ARP Probe conveys both a question (Does anyone use this address?) and an implied statement (This is the address you hope to use.)

The purpose of IPDT is for the switch to obtain and maintain a list of devices that are connected to the switch via an IP address. The probe does not populate the tracking entry; it is simply used to maintain the entry in the table after it is learned through an ARP request/reply from the host.

IP ARP Inspection is enabled automatically when IPDT is enabled. It detects the presence of new hosts when it monitors ARP packets. If dynamic ARP inspection is enabled, only the ARP packets it validates are used to detect new hosts for the Device Tracking table.

IP DHCP snooping, if enabled, detects the presence or removal of new hosts when DHCP assigns or revokes their IP addresses. When DHCP traffic is seen for a given host, the IPDT ARP probe interval timer is reset.

IPDT is a feature that has always been available, however, on more recent Cisco IOS® releases, its interdependencies are enabled by default (see Cisco bug ID CSCuj04986). It can be extremely useful when its database of IP/MAC hosts associations are used to populate the source IP of dynamic Access Control Lists (ACLs), or to maintain a binding of an IP address to a security group tag.

The ARP probe is sent under two circumstances:

- The link associated with a current entry in the IPDT database moves from a DOWN to an UP state, and the ARP entry has been populated.
- A link already in the UP state that is associated with an entry in the IPDT database has an expired probe interval.

Problem

The keepalive probe sent by the switch is a L2 check. As such, from the switch's point of view, the IP addresses used as source in the ARPs are not important: this feature can be used on devices without an IP address configured, so the IP source of 0.0.0.0 is not relevant.

When the host receives this messages, it replies back and populates the destination IP field with the only IP address available in the received packet, which is its own IP address. This can cause false duplicate IP address alerts because the host that replies, sees its own IP address as both the source and the destination of

the packet; refer to the Troubleshoot "Duplicate IP Address 0.0.0.0" Error Messages article for more information on duplicate IP address scenarios.

Default State and Operation

The global on/off config for IPDT is a legacy behavior which caused issues in the field as customers were not always aware they must turn on IPDT for certain features to work. In current releases, IPDT is solely controlled at the interface level when it enables a feature that requires IPDT.

IPDT is on globally by default within these releases; that is, no global config command:

- Catalyst 2K/3K: 15.2(1)E
- Catalyst 3850: 3.2.0SE
- Catalyst 4K: 15.2(1)E / 3.5.0E

It is important to note that, even if IPDT is enabled globally, that does not necessarily imply that IPDT actively monitors a given port.

On releases where IPDT is always on, and where IPDT can be globally toggled off/on when IPDT is enabled globally, other features determine whether it is active on a specific interface (see the Functionality Areas section).

Functionality Areas

IPDT and its ARP probes sent out of a given interface are used for these features:

- Network Mobility Services Protocol (NMSP), Versions 3.2.0E, 15.2(1)E, 3.5.0E and later
- Device sensor, Versions 15.2(1)E, 3.5.0E and later
- 1X, MAC Authentication Bypass (MAB), session manager
- Web-based authentication
- Auth-proxy
- IP Source Guard (IPSG) for static hosts
- Flexible netflow
- Cisco TrustSec (CTS)
- Media trace
- HTTP redirects

Feature Matrix

Platform	Feature	Default on (Start In)	Disable Method	Disable CLI
Cat 2960/3750 (Cisco IOS)	IPDT	15.2(1)E *	Global CLI (older releases) * per-interface	No ip device tracking * IP device tracking maximum 0 ***
Cat 2960/3750 (Cisco IOS)	NMSP	No	Global CLI or per-interface CLI	No NMSP enable NMSP attachment suppress ****
Cat 2960/3750 (Cisco IOS)	Device Sensor	15.0(1)SE	Global CLI	No macro auto-monitor
Cat 2960/3750 (Cisco IOS)	ARP Snooping	15.2(1)E **	N/A	N/A
Cat 3850	IPDT	All releases *	Per-interface *	IP device-tracking maximum 0 ***
Cat 3850	NMSP	All releases	Per-interface	NMSP attachment suppress
Cat 3850	Device Sensor	No	N/A	N/A
Cat 3850	ARP Snooping	All releases **	N/A	N/A
Cat 4500	IPDT	15.2(1)E / 3.5.0E *	Global CLI (older releases) * per-interface	No IP device-tracking * IP device-tracking maximum 0 ***
Cat 4500	NMSP	No	Global CLI or per-interface CLI	No NMSP enable NMSP attachment suppress ****

Cat 4500	Device Sensor	15.1(1)SG / 3.3.0SG	Global CLI	No macro auto monitor
Cat 4500	ARP Snooping	15.2(1)E / 3.5.0E **	N/A	N/A

Features

- IPDT cannot be disabled globally in newer releases, however, IPDT is only active on ports, if features that require it are active.
- ARP snooping is only active if specific feature combinations enable it.
- If you disable IPDT on a per-interface basis, it does not stop ARP snooping, it does prevent IPDT tracking. This is available from 3.3.0SE, 15.2(1)E, 3.5.0E and later.
- Per-interface, NMSP suppression is only available if NMSP is enabled globally.

Disable IPDT

On releases where IPDT is not enabled by default, IPDT can be turned off globally by running this command:

<#root>

```
Switch(config)#
```

no ip device tracking

On releases where IPDT is always on, running the previous command is not available, or it does not allow you to disable IPDT (Cisco bug ID CSCuj04986). In this case, there are several ways to ensure IPDT does not monitor a specific port or it does not generate duplicate IP alerts.

Enter the IP Device Tracking Probe Delay 10 Command

This command does not allow a switch to send a probe for 10 seconds when it detects a link UP/flap, which minimizes the possibility to have the probe sent while the host on the other side of the link checks for duplicate IP addresses. The RFC specifies a 10-second window for duplicate address detection. If you delay the device-tracking probe, the issue can be solved in most cases.

If the switch sends out an ARP Probe for the client while the host (for example, a Microsoft Windows PC) is

in its Duplicate-Address Detection phase, the host detects the probe as a duplicate IP address and presents the user with a message that a duplicate IP address was found on the network. If the PC does not obtain an address, and the user must manually release/renew the address; disconnect and reconnect to the network, or reboot the PC to gain network access.

In addition to probe-delay, the delay also resets itself when the switch detects a probe from the PC/host. For example, if the probe timer has counted down to five seconds and detects an ARP Probe from the PC/host, the timer resets back to 10-seconds.

This configuration has been made available through Cisco bug ID CSCtn27420.

Enter the IP Device Tracking Probe Use SVI Command

With this command, you can configure the switch to send a non-RFC compliant ARP Probe; the IP source is not 0.0.0.0, but it is the Switch Virtual Interface (SVI) in the VLAN where the host resides. Microsoft Windows machines no longer see the probe as a probe as defined by RFC 5227 and it does not flag it as potential duplicate IP.

Enter the IP Device Tracking Probe Auto-Source [fallback <host-ip> <mask>] [override] Command

For customers who do not have predictable/controllable end devices, or for those who have many switches in an L2-only role, the configuration of an SVI, which introduces a Layer 3 variable in the design, is not a suitable solution. An enhancement introduced in Version 15.2(2)E and later, the possibility to allow arbitrary assignment of an IP address does not need to belong to the switch for use as the source address in ARP probes generated by IPDT. This enhancement introduces the chance to modify the automatic behavior of the system in these ways (this list shows how the system automatically behaves after each command is used):

Enter the IP Device Tracking Probe Auto-Source Command

1. Set the source to VLAN SVI, if present.
2. Search for a source/MAC pair in the IP host table for the same subnet.
3. Send the zero IP source as in the default case.

Enter the IP Device Tracking Probe Auto-Source Fallback 0.0.0.1 255.255.255.0 Command

1. Set the source to VLAN SVI, if present.
2. Search for a source/MAC pair in the IP host table for the same subnet.
3. Compute the source IP from the destination IP with the host bit and mask provided.

Enter the IP Device Tracking Probe Auto-Source Fallback 0.0.0.1 255.255.255.0 Override Command

1. Set the source to VLAN SVI, if present.
2. Compute the source IP from the destination IP with the host bit and mask provided.

> **Note**: An override makes you skip the search for an entry in the table.

As an example of the previous computations, assume you probe host 192.168.1.200, with the mask and host bits provided, you generate a source address of 192.168.1.1. If you probe entry 10.5.5.20, you can generate an ARP probe with source address 10.5.5.1, and so on.

Enter the IP Device Tracking Maximum 0 Command

This command does not truly disable IPDT, however, it does limit the number of tracked hosts to zero. This is not a recommended solution, and it must be used with caution because it affects all other features that rely on IPDT, which includes the port-channels configurations described in Cisco bug ID CSCun81556.

Turn Off Active Features that Trigger IPDT

Some features that can trigger IPDT include NMSP, device sensor, dot1x/MAB, WebAuth, and IPSG. These features are not recommended to be enabled on trunk ports. This solution is reserved for the most difficult or complex situations, where either all the solutions previously available did not work as expected, or they created additional problems. This is, however, the only solution that allows extreme granularity when you disable IPDT, because you can turn off only the IPDT-related features that cause problems and leave everything else unaffected.

In the most recent Cisco IOS, Versions15.2(2)E and later, you see an output similar to this:

<#root>

```
Switch#
```

```
show ip device tracking interface GigabitEthernet 1/0/9
```

```
------------------------------------------
Interface GigabitEthernet1/0/9 is: STAND ALONE
IP Device Tracking = Disabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 180000
IPv6 Device Tracking Client Registered Handle: 75
IP Device Tracking Enabled Features:
       HOST_TRACK_CLIENT_ATTACHMENT
       HOST_TRACK_CLIENT_SM
```

The two lines in all caps at the bottom of the output are those that use IPDT in order to work. Most of the problems created when you disable the device tracking can be avoided, if you disable the single services that run in the interface.

In earlier versions of Cisco IOS, the easy way to know which modules are enabled under an interface is not available yet, so you must go through a more involved process to obtain the same results. You must turn on debug ip device track interface, which is a low-frequency log that must be safe in most setups. Be careful not to turn on debug ip device tracking all because this, on the contrary, floods the console in scaled situations.

Once the debug is on, bring an interface back to default, and then add and remove an IPDT service from the interface configuration. The results from the debugs tell you which service has been enabled/disabled with the command you used.

Example:

<#root>

```
Switch(config)#
```

```
interface GigabitEthernet 1/0/9
```

```
Switch(config-if)#
```

```
ip device tracking maximum 10
```

```
Switch(config-if)#
*Mar 27 09:58:49.470: sw_host_track-interface:Feature 00000008 enabled on port Gi1/0/9, mask now 000000
*Mar 27 09:58:49.471: sw_host_track-interface:Gi1/0/9[L2 DOWN, IPHOST DIS]IP host tracking max set to 1
Switch(config-if)#
```

What the output reveals is that you enabled feature 00000008, and that the new feature mask is 0000004C.

Now, remove the configuration you just added:

<#root>

```
Switch(config-if)#
```

no ip device tracking maximum 10

```
Switch(config-if)#
*Mar 27 10:02:31.154: sw_host_track-interface:Feature 00000008 disabled on port
Gi1/0/9, mask now 00000044, 65 ports enabled
*Mar 27 10:02:31.154: sw_host_track-interface:Gi1/0/9[L2 DOWN, IPHOST DIS]IP
host tracking max cleared
*Mar 27 10:02:31.154: sw_host_track-interface:Max limit has been removed from
the interface GigabitEthernet1/0/9.
Switch(config-if)#
```

Once you remove feature 00000008, you see the 00000044 mask, which must have been the original default mask. The value of 00000044 is expected since AIM is 0x00000004 and SM is 0x00000040, which together results in 0x00000044.

There are several IPDT services that can run under an interface:

IPT Service	**Interface**
HOST_TRACK_CLIENT_IP_ADMISSIONS	= 0x00000001
HOST_TRACK_CLIENT_DOT1X	= 0x00000002
HOST_TRACK_CLIENT_ATTACHMENT	= 0x00000004
HOST_TRACK_CLIENT_TRACK_HOST_UPTO_MAX	= 0x00000008
HOST_TRACK_CLIENT_RSVP	= 0x00000010
HOST_TRACK_CLIENT_CTS	= 0x00000020
HOST_TRACK_CLIENT_SM	= 0x00000040

HOST_TRACK_CLIENT_WIRELESS	= 0x00000080

In the example, HOST_TRACK_CLIENT_SM (SESSION-MANAGER) and HOST_TRACK_CLIENT_ATTACHMENT (also known as AIM/NMSP), modules are configured for IPDT. To turn off IPDT on this interface, you must disable both because IPDT is disabled ONLY when all functions that use it are disabled as well.

After you disable those features, you have an output similar to this:

<#root>

```
Switch(config-if)#

do show ip device tracking interface GigabitEthernet 1/0/9


------------------------------------------
Interface GigabitEthernet1/0/9 is: STAND ALONE
IP Device Tracking = Disabled     ß IPDT is disabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 180000
IP Device Tracking Enabled Features:
ß No active features
------------------------------------------
```

In this way, IPDT is disabled with more granularity.

Here are some examples of commands used to disable some of the functions discussed previously:

- **nmsp attach suppress**
- **no macro auto monitor**

Note: The latest feature must be available only on platforms that support Smart Ports, which are used to enable features based on the location of a switch in the network (and for mass configuration deployments across the network.)

Verify IPDT Operation

Run these commands to verify the IPDT status on your device:

- **show ip device tracking**
  - This command displays interfaces where IPDT is enabled, and where MAC/IP/interface

associations are currently tracked.

- **clear ip device tracking**
  - This command clears IPDT-related entries.

Note: The switch sends ARP probes to the hosts that were removed. If a host is present, it responds to the ARP probe and the switch adds an IPDT entry for the host. You must disable ARP probes before the clear IPDT command; that way, all ARP entries are gone. If ARP probes are enabled after the **clear ip device tracking** command, all entriescome back again.

- **debug ip device tracking**
  - This command allows you to collect debugs in order to display IPDT activity in real time.