IP Device Tracking (IPDT) Overview

Document ID: 118630

Contributed by Jennifer Denise Mazzarelli, Cisco TAC Engineer.
Nov 25, 2014

Contents

Introduction

The document describes IP Device Tracking (IPDT) and how to disable it and verify its operation.

IPDT Overview

Definition and Usage

The main IPDT task is to keep track of connected hosts (association of MAC and IP address). In order 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 use Layer 2 (L2) as the default source 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 excerpted here:

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 sending the packet. The 'sender IP address' field MUST be set to all zeroes, to avoid polluting 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 being probed. An ARP Probe conveys both a question ("Is anyone using this address?") and an implied statement ("This is the address I 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 in order 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 that it validates are used in order 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.

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 is used in order 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.

Known Issue

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 with no IP address configured at all, 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 Duplicate IP Address 0.0.0.0. Error Message Troubleshoot article for more information about the duplicate IP address scenario.

Default State and Operation

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 actually 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 Services Gateway (IPSG) for static hosts
- Flexible netflow
- Cisco TrustSec (CTS)
- Media trace
- HTTP redirects

Disable IPDT

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

```
# no ip device tracking
```

On releases where IPDT is always on, 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 that 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, so 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. The PC might not obtain an address, and the user must manually release/renew the address, disconnect and reconnect to the network, or reboot the PC in order 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 in order to send a non−RFC compliant ARP Probe; the IP source will not be 0.0.0.0, but it will be 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 do not flag a 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 that 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 would 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, but it does limit the number of tracked hosts to zero. This is not a recommended solution and it should be used with caution, because it affects all of the other features that rely on IPDT, which includes the port−channels configuration as described in Cisco bug ID CSCun81556.

Turn Off Active Features that Trigger IPDT

Some features that might trigger IPDT include NMSP, device sensor, dot1x/MAB, WebAuth, and IPSG. This solution is reserved for the most difficult or complex situations, where either all of 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:

```
Switch#show ip device tracking interface gig 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, this 'easy' way to know which modules are enabled under an interface is not

available yet, so you must go through a more involved process in order to get the same results. You must turn on ***debug ip device track interface***, which is a low−frequency log that should 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 scale 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.

Here is an example:

```
Switch(config)#int gig 1/0/9
Switch(config−if)#ip device track max 10
Switch(config−if)#
*Mar 27 09:58:49.470: sw_host_track−interface:Feature 00000008 enabled on port
Gi1/0/9, mask now 0000004C, 65 ports enabled
*Mar 27 09:58:49.471: sw_host_track−interface:Gi1/0/9[L2 DOWN, IPHOST DIS]IP
host tracking max set to 10
Switch(config−if)#
```

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

Now, remove the configuration you just added:

```
Switch(config−if)#no ip device track max 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 can see the ***00000044*** mask, which must have been the original, default mask. This value of ***00000044*** is expected since AIM is ***0x00000004*** and SM is ***0x00000040***, which together result in ***0x00000044***.

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

IPDT 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. In order to turn off IPDT on this interface, you must disable both, because IPDT is disabled ONLY when all of the functions that use it are disabled as well.

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

```
Switch(config−if)#do show ip dev trac int gig 1/0/9
−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−
Interface GigabitEthernet1/0/9 is: STAND ALONE
IP Device Tracking = Disabled      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 example of commands used in order to disable some of the functions discussed previously:

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

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

Verify IPDT Operation

Use these commands in order to verify 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; in that way, all of the ARP entries should be gone. If ARP probes are enabled after the ***clear ip device tracking*** command, all of the entries come back again.

- ***debug ip device tracking ...***

  This command allows you to collect debugs in order to display IPDT activity in realtime.

Updated: Nov 25, 2014 Document ID: 118630