检验IPDT设备操作

目录

简介

本文档介绍如何验证IP设备跟踪(IPDT)操作以及如何禁用这些操作。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的输出基于以下软件和硬件版本：

- 思科WS-C2960X
- Cisco IOS® 15.2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

IPDT概述

定义和使用情况

IPDT的主要任务是跟踪连接的主机（MAC和IP地址的关联）。为此，它以默认间隔30秒发送单播地址解析协议(ARP)探测。根据RFC 5227中列出的ARP探测功能定义，这些探测功能将发送到链路另一端所连接主机的MAC地址，并使用第2层(L2)作为ARP所通过的物理接口的MAC地址和发送方IP地址0.0.0.0的默认源

摘录

在本文档中，术语“ARP探测”用于指在本地链路上以全零发送方IP地址广播的ARP请求数据包。发送方硬件地址必须包含发送数据包的接口的硬件地址。必须将发送方IP地址字段设置为全零，以避免同一链路上其他主机的ARP缓存被损坏，以防地址已被其他主机使用。必须将目标IP地址字段设置为已探测的地址。ARP探测功能可传递一个问题（有人使用这个地址吗？）和一个隐含的语句（我希望使用这个地址。）。

IPDT的目的是让交换机获取并维护通过IP地址连接到交换机的设备列表。探测功能不会填充跟踪条目；它只是用于在通过主机的ARP请求/应答获知条目后维护表中的条目。

启用IPDT时，IP ARP检测会自动启用。它在监控ARP数据包时检测新主机的存在。如果启用动态ARP检测，则仅使用其验证的ARP数据包来检测设备跟踪表中的新主机。

IP DHCP监听（如果已启用）在DHCP分配或撤销新主机的IP地址时检测新主机的存在或删除。 当发现给定主机的DHCP流量时，IPDT ARP探测间隔计时器重置。

IPDT是一项始终可用的功能。但是，在较新的Cisco IOS®版本上，默认情况下会启用其相互依赖关系(请参阅Cisco Bug ID CSCuj04986)。当使用其IP/MAC主机关联数据库填充动态访问控制列表(ACL)的源IP或维护IP地址到安全组标记的绑定时，它可能非常有用。

在以下两种情况下发送ARP探测：

- 与IPDT数据库中当前条目关联的链路从DOWN状态变为UP状态，并且ARP条目已填充。
- 与IPDT数据库中的条目关联的链路已处于UP状态，且其探测间隔已过期。

问题

交换机发送的keepalive探针是L2检查。因此，从交换机的角度来看，在ARP中用作源的IP地址并不重要：此功能可以在根本没有配置IP地址的设备上使用，因此0.0.0.0的IP源并不相关。

当主机收到此消息时，它会回复并填写目标IP字段，该字段将使用收到的数据包中唯一可用的IP地址，即主机自己的IP地址。这会导致错误重复IP地址警报，因为作出回复的主机将自己的IP地址同

时视为数据包的源和目标；请参阅重复IP地址0.0.0.0。有关重复IP地址方案的详细信息，请参阅“错误消息故障排除”文章。

默认状态和操作

IPDT的全局开/关配置是一种传统行为，会导致现场出现问题，因为客户并不总是知道他们需要打开IPDT才能使用某些功能。在当前版本中，IPDT仅在启用需要IPDT的功能时受接口级别的控制。

默认情况下，IPDT在这些版本中处于全局启用状态；即no global config命令：

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

需要注意的是，即使全局启用IPDT，这并不一定意味着IPDT主动监控给定端口。

在IPDT始终打开以及全局启用IPDT时可以全局开启/关闭的版本中，其他功能实际上确定它是否在特定接口上处于活动状态（请参阅“功能区域”部分）。

功能领域

从给定接口发出的IPDT及其ARP探测用于以下功能：

- 网络移动服务协议(NMSP)，版本3.2.0E、15.2(1)E、3.5.0E及更高版本
- 设备传感器，版本15.2(1)E、3.5.0E及更高版本
- 1X，MAC身份验证绕行(MAB)，会话管理器
- 基于Web的身份验证
- 身份验证代理
- 静态主机的IP源保护(IPSG)
- Flexible Netflow
- 思科TrustSec(CTS)
- 媒体跟踪
- HTTP重定向

功能表

Platform	功能	默认打开（开始于）	禁用方法	禁用CLI
Cat 2960/3750(Cisco IOS)	IPDT	15.2(1)E *	全局CLI（旧版本）* 每个接口	no ip device tracking * ip device tracking maximum 0 ***
Cat 2960/3750(Cisco	NMSP	否	全局CLI或 每个接口的CLI	no nmsp enable NMSP附件禁止传****

IOS)				
Cat 2960/3750(Cisco IOS)	设备传感器	15.0(1)SE	全局CLI	no macro auto monitor
Cat 2960/3750(Cisco IOS)	ARP监听	15.2(1)E**	不适用	不适用
Cat 3850	IPDT	所有版本*	每个接口*	ip device tracking maximum 0 ***
Cat 3850	NMSP	所有版本	每个接口	NMSP附件抑制
Cat 3850	设备传感器	否	不适用	不适用
Cat 3850	ARP监听	所有版本**	不适用	不适用
Cat 4500	IPDT	15.2(1)E / 3.5.0E *	全局CLI（旧版本）* 每个接口	no ip device tracking * ip device tracking maximum 0 ***
Cat 4500	NMSP	否	全局CLI或 每个接口的CLI	no nmsp enable NMSP附件禁止传****
Cat 4500	设备传感器	15.1(1)SG/3.3.0SG	全局CLI	no macro auto monitor
Cat 4500	ARP监听	15.2(1)E/3.5.0E电**	不适用	不适用

功能

- IPDT不能在较新版本中全局禁用，但是，如果需要它的功能处于活动状态，IPDT仅在端口上处于活动状态。

- 只有在特定功能组合启用时，ARP监听才处于活动状态。
- 如果在每个接口上禁用IPDT，则它不会停止ARP监听，而是会阻止IPDT跟踪。这可以从i3.3.0SE、15.2(1)E、3.5.0E及更高版本获得。
- 只有全局启用NMSP时，每个接口的NMSP抑制才可用。

禁用IPDT

在默认情况下未启用IPDT的版本中，可以使用以下命令全局关闭IPDT:

<#root>

Switch(config)#

no ip device tracking

在IPDT始终开启的版本中，上一个命令不可用，或者不允许禁用IPDT(Cisco bug ID CSCuj04986)。在这种情况下，有几种方法可以确保IPDT不监控特定端口或不生成重复的IP警报。

输入IP Device Tracking Probe Delay 10命令

此命令不允许交换机在检测到链路UP/flap时发送10秒的探测，这样可最大程度地降低在链路另一端的主机检查重复IP地址时发送探测的可能性。RFC为重复地址检测指定了10秒的窗口，因此，如果您延迟设备跟踪探测，则可以在大多数情况下解决此问题。

如果交换机在主机（例如，Microsoft Windows PC）处于重复地址检测阶段时发出客户端的ARP探测，则主机将探测检测为重复的IP地址，并向用户显示一条消息，提示在网络上发现重复的IP地址。如果PC无法获取地址，且用户必须手动释放/更新地址，断开连接并重新连接到网络，或者重新启动PC以获取网络访问权限。

除了探测延迟，当交换机检测到来自PC/主机的探测时，延迟还会自行重置。例如，如果探测计时器倒计到五秒钟，并且检测到来自PC/主机的ARP探测，则该计时器会重置回10秒。

此配置已通过Cisco Bug ID CSCtn27420提供。

输入IP Device Tracking Probe Use SVI命令

使用此命令，您可以配置交换机以发送不符合RFC的ARP探测；IP源不是0.0.0.0，但它是主机所在的VLAN中的交换机虚拟接口(SVI)。Microsoft Windows计算机不再将探测视为RFC 5227定义的探测，并且不会标记潜在的重复IP。

输入IP设备跟踪探测功能自动源[fallback <host-ip> <mask>] [override]命令

对于没有可预测/可控制的终端设备的客户，或者对于拥有许多交换机且仅具有L2角色的客户，SVI的配置（在设计中引入第3层变量）不是合适的解决方案。版本15.2(2)E及更高版本中引入的一项增强功能，允许任意分配不需要属于交换机的IP地址，用作IPDT生成的ARP探测中的源地址。此增强功能引入了通过以下方式修改系统自动行为的机会（此列表显示使用每个命令后系统如何自

动行为）：

输入IP设备跟踪探测功能自动源命令

1. 将源设置为VLAN SVI（如果有）。
2. 在IP主机表中搜索同一子网的源/MAC对。
3. 发送零IP源，与默认情况相同。

输入IP设备跟踪探测功能自动源回退0.0.0.1 255.255.255.0命令

1. 将源设置为VLAN SVI（如果有）。
2. 在IP主机表中搜索同一子网的源/MAC对。
3. 根据提供的主机位和掩码，从目标IP计算源IP。

输入IP设备跟踪探测功能自动源回退0.0.0.1 255.255.255.0覆盖命令

1. 将源设置为VLAN SVI（如果有）。
2. 根据提供的主机位和掩码，从目标IP计算源IP。

> 注：覆盖会使您跳过对表中条目的搜索。

作为上述计算的一个示例，假设您探测主机192.168.1.200。使用提供的掩码和主机位，可以生成源地址192.168.1.1。 如果探测条目10.5.5.20，则可以生成源地址为10.5.5.1的ARP探测，以此类推。

输入IP Device Tracking Maximum 0命令

此命令不会真正禁用IPDT，但确实将跟踪的主机数量限制为零。这不是推荐的解决方案，必须谨慎使用，因为它会影响依赖于IPDT的所有其他功能，包括端口通道配置(如Cisco Bug ID CSCun81556中所述)。

关闭触发IPDT的活动功能

可以触发IPDT的某些功能包括NMSP、设备传感器、dot1x/MAB、WebAuth和IPSG。建议不要在中继端口上启用这些功能。此解决方案专用于最困难或最复杂的情况。在这些情况下，所有以前提供的解决方案要么未按预期运行，要么产生了其他问题。但是，这是在禁用IPDT时允许极精细度的唯一解决方案，因为您只能关闭导致问题的与IPDT相关的功能，而所有其他功能不会受到影响。

在最新的Cisco IOS版本15.2(2)E及更高版本中，您会看到类似下面的输出：

<#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
```

输出底部所有帽中的两行是使用IPDT工作的两行。如果禁用接口中运行的单个服务，则可以避免禁用设备跟踪时产生的大多数问题。

在Cisco IOS的早期版本中，尚没有这种知道接口下启用了哪些模块的简单方法，因此您必须经过更复杂的过程才能获得相同的结果。您必须打开debug ip device track interface，它是在大多数设置中必须安全的低频日志。请注意不要打开debug ip device tracking all，因为反之，这会使控制台在扩展情况下泛洪。

一旦启动调试，将接口恢复为默认值，然后从接口配置中添加和删除IPDT服务。调试的结果会告诉您哪些服务已用您使用的命令启用/禁用。

示例

```
<#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 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)#
```

输出显示您已启用功00000008掩码，新功能掩码为0000004C。

现在，删除您刚才添加的配置：

```
<#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)#
```

删除特征掩00000008后，您可以看到00000044始掩码，该掩码必须是原始的默认掩码。预期值为00000044，因为AIM为0x00000004，而SM为0x00000040，两者共同导致0x00000044。

接口下可以运行多个IPDT服务：

IPT服务	接口
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

在本示例中，为IPDT配置了HOST_TRACK_CLIENT_SM(SESSION-MANAGER)和HOST_TRACK_CLIENT_ATTACHMENT（也称为AIM/NMSP）模块。要关闭此接口上的IPDT，您必须同时禁用这两个接口，因为只有在同时禁用了使用该接口的所有功能时，才会禁用IPDT。

禁用这些功能后，您会看到如下所示的输出：

<#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
-----------------------------------------
```

通过这种方式，IPDT会以更精细的方式禁用。

以下是用来禁用前面讨论的一些功能的命令示例：

- nmsp attach suppress
- no macro auto monitor

注：最新功能必须仅在支持智能端口的平台上可用，智能端口用于根据交换机在网络中的位置启用功能，以及在整个网络中进行大规模配置部署。

检验IPDT操作

使用以下命令验证设备上的IPDT状态：

- show ip device tracking
  此命令显示启用IPDT的接口以及当前跟踪MAC/IP/接口关联的接口。
- clear ip device tracking
- 此命令清除与IPDT相关的条目。

注意：交换机将ARP探测发送到已删除的主机。如果存在主机，它会响应ARP探测功能，并且交换机会为该主机添加一个IPDT条目。您必须先禁用ARP探测功能，然后发出clear IPDT命令；这样，所有ARP条目都将丢失。如果在clear ip device tracking命令后启用ARP探测，则所有条目都会再次返回。

- debug ip device tracking
  此命令允许您收集调试以实时显示IPDT活动。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。