# 跟踪(IPDT)概述的IP设备

## 目录



## 简介

本文描述跟踪的IP设备(IPDT)和如何禁用它和验证其操作。

## IPDT概述

### 定义和使用情况

主IPDT任务是记录连接的主机(MAC和IP地址的关联)。为了执行此，它发送单播有默认间隔的地址解析服务(ARP)探测器30秒;这些探测器被发送对在链路的另一侧连接的主机的MAC地址和使用第2层(L2)，当默认来源外面ARP去和0.0.0.0的发送方IP地址物理接口的MAC地址在，根据在RFC 5227列出的ARP探测器定义摘抄了得此处：

在本文中，用语‘ARP探测器’用于参考ARP请求数据包，在本地链路的广播，与全部清零‘发送方IP地址’。‘发送器硬件地址的必须包含发送数据包的接口的硬件地址。必须设置‘发送方IP地址’字段为所有零，避免污染其他主机的ARP缓存在地址结果是已经在使用中的由另一台主机的案件的同一条链路。必须设置‘目标IP地址’字段为被探查的地址。ARP探测器表达问题(“谁使用此地址？")和一个暗示的语句(“这是我希望到use.")的地址。

IPDT目的是为了维护的交换机能得到和连接到交换机通过IP地址设备的列表。探测器不填充跟踪条

目;在通过一ARP请求/回复了解从主机后，它在表里用于为了维护条目。

当IPDT启用时， IP ARP检查自动地启用;当监控ARP数据包时，它检测新的主机出现。如果动态ARP检查启用，只有验证的ARP数据包用于为了检测跟踪表的设备的新建的主机。

Ip dhcp snooping，如果启用，检测新的主机出现或删除，当DHCP分配或取消他们的IP地址时。

IPDT是总是可用的功能。然而，在更加最近的Cisco IOS版本，其相互依赖性启用默认情况下(请参阅Cisco Bug ID CSCuj04986)。它能是非常有用的，当IP/MAC主机关联其数据库用于为了填充来源IP动态访问控制控制目录(ACL)时，或者维护约束IP地址到安全组标记。

ARP探测器被发送在两个情况以下：

- 链路关联与在IPDT数据库的一个当前条目从DOWN移动向UP状态，并且ARP条目填充。
- 关联与在IPDT数据库的一个条目的一条链路已经在UP状态有一个已到期探测器间隔。

### 已知问题

交换机发送的'Keepalive'探测器是L2检查。象这样从交换机的观点，作为来源使用的IP地址在ARPs不是重要：此功能在设备可以使用没有配置的IP地址，因此0.0.0.0 IP源不是相关的。

当主机收到此消息时，回复返回并且填充有唯一的IP地址联机的目的地IP字段在收到的信息包，是其自己的IP地址。这能导致错误重复IP地址警报，因为回复看到其自己的IP地址作为来源和数据包的目的地的主机;参考重复IP地址0.0.0.0。错误消息排除故障条款关于重复IP地址方案的更多信息。

### 默认状态和操作

请注意，即使IPDT启用全局，那不一定暗示IPDT积极地监控一个给的端口。在IPDT总是的版本上，并且IPDT可以是全局再按乒乓键的off/on的地方，当IPDT启用全局时，其它特性实际上确定是否是活跃的在一个特定接口(请参阅功能地区部分)。

### 功能地区

IPDT和其ARP探测器被发送在指定接口外面使用这些功能：

- 网络移动服务协议(NMSP)，版本3.2.0E、15.2(1)E， 3.5.0E和以后
- 设备传感器、版本15.2(1)E， 3.5.0E和以后
- 1X， MAC验证旁路(MAB)，会话管理器
- 基于Web的验证
- 验证代理
- IP服务网关(IPSG)静态主机的
- 灵活NetFlow
- 思科TrustSec (CTS)
- 梅迪亚trace
- HTTP重定向

## 禁用IPDT

默认情况下在IPDT没有启用的版本上， IPDT可以用此命令关闭全局：

```
# no ip device tracking
```

在IPDT总是的版本上，前面的命令不是可用的或不允许您禁用IPDT (Cisco Bug ID CSCuj04986)。在这种情况下，有几个方式保证IPDT不监控一个特定端口或不生成相同的IP警报。

## 输入跟踪探测器延迟10命令的IP设备

此命令不允许交换机发送一台探测器10秒，当检测链路UP/flap时，最小化可能性有被发送的探测器，当在链路检查另一侧的主机复制IP地址的时。RFC指定重复地址检测的10秒钟的窗口，因此，如果延迟设备跟踪探测器，问题可以是解决的在大多数情况下。

如果交换机派出客户端的一台ARP探测器，当主机(例如， Microsoft Windows PC)时是在其重复地址检测相位，主机检测探测器作为重复IP地址并且提交有消息的用户重复IP地址在网络被找到。PC也许不得到地址，并且用户必须手工发布/更新地址，断开并且重新连接对网络或者重新启动PC为了获得网络访问。

除探测器迪莱之外，当交换机检测从PC/host时的一台探测器延迟也重置。例如，如果探测器计时器计数下来对五秒并且检测从PC/host的一台ARP探测器，计时器重新设置到10秒。

此配置被做了可用的通过Cisco Bug ID CSCtn27420。

## 输入跟踪探测器使用SVI的IP设备。命令

用此命令，您能配置交换机为了发送非RFC兼容ARP探测器;IP源不会是0.0.0.0，但是它将是在主机驻留的VLAN的Switch Virtual Interface (SVI)。Microsoft Windows机器不再看到探测器作为探测器如定义由RFC 5227，并且不标记潜在的相同的IP。

## 输入跟踪探测器自动来源[fallback <host-ip> <mask>] [override]命令的IP设备

对于没有可预测/可控制的终端设备或那些人的有许多交换机在L2-only角色的客户， SVI的配置，在设计引入第3层变量，不是一适当的解决方案。在版本15.2(2)E和以上介绍的，增强，可能性允许不需要属于交换机为使用作为在ARP探测器的源地址IP地址的任意分配由IPDT生成。此增强引入机会修改系统的自动行为用这些方式(此列表显示系统如何自动地正常运行，在使用每命令)后：

### 输入跟踪探测器自动来源命令的IP设备

1. 若有设置来源为VLAN SVI。
2. 搜索一个source/MAC对在相同子网的IP主机表里。
3. 发送零的IP源正如在默认事例。

### 输入跟踪探测器自动来源fallback 0.0.0.1 255.255.255.0命令的IP设备

1. 若有设置来源为VLAN SVI。

2. 搜索一个source/MAC对在相同子网的IP主机表里。

3. 从目的地IP计算来源IP用主机位并且屏蔽提供。

**输入跟踪探测器自动来源fallback 0.0.0.1 255.255.255.0覆盖命令的IP设备**

1. 若有设置来源为VLAN SVI。

2. 从目的地IP计算来源IP用主机位并且屏蔽提供。

**注意**：覆盖使您未参加一个条目的搜索在表里。
例如上一个计算，假设您探测器主机192.168.1.200。使用提供的掩码和主机位，您生成192.168.1.1源地址。

如果探查条目10.5.5.20，您会生成有源地址的10.5.5.1一台ARP探测器，等等。

## 输入跟踪最大数量0的IP设备命令

此命令真不禁用IPDT，但是限制被跟踪的主机数量到零。这不是推荐的解决方案，并且应该小心地使用，因为影响依靠IPDT，包括信道配置正如Cisco Bug ID CSCun81556所描述的所有其它特性。

## 关闭触发IPDT的活动功能

可能的一些功能触发IPDT包括NMSP、设备传感器、dot1x/MAB、Webauth和IPSG。此解决方案为最困难保留或复杂情况的解决方案之一以前提供全部没有运作正如所料，或者他们创建另外的问题。这是，然而，允许极其粒度的唯一的解决方案，当您禁用IPDT时，因为您能关闭引起问题并且留给一切别的东西未受影响仅的IPDT相关功能。

在最最近的Cisco IOS， Versions15.2(2)E和以后，您看到输出类似于此：

```
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
```

在所有盖帽的两条线路在输出的底部是使用IPDT为了工作的那些。创建的大多问题，当您禁用设备跟踪时可以避免，如果禁用在接口运作的单个服务。

在Cisco IOS中更早版本，‘容易’这样知道哪些模块启用在接口下不是可用的，因此您必须通过一更加包含的进程为了取得同样结果。您必须打开**debug ip设备跟踪接口**，是一本低频率日志应该是安全在多数设置。因为这，相反，充斥缩放情况的，控制台小心不启动**跟踪所有的debug ip设备**。

一旦调试打开，请建立接口回到默认，然后从接口配置添加并且取消IPDT服务。从调试的结果告诉您哪服务用您使用的命令启用/禁用。

示例如下：

```
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)#
```

什么输出显示是您启用功能00000008，并且新特性的掩码是0000004C。

现在，请删除您添加的配置：

```
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)#
```

一旦删除功能00000008，您能看到00000044掩码，一定是原始，默认掩码。此值为00000044预计，因为AIM是0x00000004和SM是0x00000040，一起导致0x00000044。

有能运作在接口下的几IPDT服务：

| IPDT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 |

在示例中， HOST_TRACK_CLIENT_SM (会话管理器)和HOST_TRACK_CLIENT_ATTACHMENT (亦称AIM/NMSP)模块为IPDT配置。为了关闭在此接口的IPDT，您必须禁用两个，因为IPDT禁用，只有当使用它时的所有功能禁用。

在您禁用那些功能后，您有一输出类似于此：

```
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:
? No active features
------------------------------------------
```

这样， IPDT禁用与更多粒度。

这是用于的命令某示例为了禁用以前讨论的某些功能：

- **nmsp附上抑制**
- **没有宏观自动监视器**

  **注意**：最新的功能应该仅取得到在支持巧妙的端口的平台(Smartport闪存演示)，用于为了启用根据一交换机位置和设置的功能在网络和在间网络的质量配置部署的。

# 验证IPDT操作

请使用这些命令为了验证在您的设备的IPDT状态：

- **show ip device tracking…**

  此命令显示IPDT启用的接口，并且MAC/IP/interface关联当前被跟踪的地方。

- **清楚IP设备跟踪…**

  此命令清除IPDT相关条目。

  **注意**：交换机发送ARP探测器到删除的主机。如果主机存在，响应到ARP探测器，并且交换机添加主机的一个IPDT条目。您必须禁用ARP探测器，在结算IPDT命令前;用那个方式，应该去所有ARP条目。如果ARP探测器启用，在**清楚IP设备trace命令**，所有条目再后回来。

- **debug ip设备跟踪…**

  此命令在实时允许您收集调试为了显示IPDT活动。