驗證IPDT裝置操作

目錄

簡介

本文說明如何驗證IP裝置追蹤(IPDT)作業以及如何停用這些動作。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的輸出是根據以下軟體和硬體版本：

- Cisco WS-C2960X
- Cisco IOS® 15.2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

IPDT概述

定義與使用

IPDT的主要任務是跟蹤連線的主機（MAC和IP地址的關聯）。為此，它以預設間隔30秒傳送單播地址解析協定(ARP)探測。根據RFC 5227中列出的ARP探測定義，這些探測將被傳送到鏈路另一端所連線主機的MAC地址，並使用第2層(L2)作為ARP所通過的物理介面的MAC地址和0.0.0.0的傳送方IP地址的預設源

摘錄

在本文檔中，術語ARP探測用於指在本地鏈路上以全零傳送方IP地址廣播的ARP請求資料包。傳送方硬體地址必須包含傳送資料包的介面的硬體地址。必須將傳送方IP地址欄位設定為全零，以避免在同一鏈路上的其他主機中（如果該地址已被另一台主機使用）發生損壞ARP快取。目標IP地址欄位必須設定為要探測的地址。ARP探測功能可傳遞一個問題（有人使用這個地址嗎？）和一個隱含的語句（這個地址我希望使用。）。

IPDT的用途是讓交換器取得和維護透過IP位址連線到交換器的裝置清單。探測器不會填充跟蹤條目；它只是用於在通過主機的ARP請求/應答獲知條目後維護表中的條目。

啟用IPDT時，IP ARP檢測會自動啟用。它在監視ARP資料包時檢測新主機的存在。如果啟用動態ARP檢測，則僅使用它所驗證的ARP資料包來檢測裝置跟蹤表中的新主機。

IP DHCP監聽（如果已啟用）在DHCP分配或撤銷新主機的IP地址時檢測新主機的存在或刪除。 當看到給定主機的DHCP流量時，IPDT ARP探測間隔計時器被重置。

IPDT是一項始終可用的功能。但是在新近的Cisco IOS®版本中，預設會啟用其互依關係(請參閱思科錯誤ID CSCuj04986)。當使用其IP/MAC主機關聯資料庫來填充動態訪問控制清單(ACL)的源IP或維護IP地址與安全組標籤的繫結時，它非常有用。

ARP探測是在兩種情況下傳送的：

- 與IPDT資料庫中當前條目關聯的鏈路從DOWN狀態移動到UP狀態，並且ARP條目已填充。
- 已處於UP狀態的連結與IPDT資料庫中的條目相關聯，該連結的探測間隔已過期。

問題

交換機傳送的keepalive探測是L2檢查。因此，從交換機的角度來看，在ARP中用作源的IP地址並不重要：此功能可以在根本沒有配置IP地址的裝置上使用，因此0.0.0.0的IP源不相關。

當主機收到此消息時，它會回覆並填寫目標IP欄位，其中包含所接收資料包中唯一可用的IP地址，即其自己的IP地址。這可能會導致錯誤重複IP地址警報，因為作出回覆的主機將自己的IP地址同

時視為資料包的源和目標；請參閱重複IP地址0.0.0.0。有關重複IP地址方案的詳細資訊，請參閱「Error Message Troubleshoot」文章。

預設狀態和操作

IPDT的全域性開啟/關閉設定是舊有行為，會導致現場出現問題，因為客戶並不總是知道他們需要開啟IPDT才能使用某些功能。在當前版本中，IPDT僅在啟用需要IPDT的功能時受介面級別的控制。

在這些版本中，IPDT預設為全域性開啟；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

必須注意的是，即使IPDT是全域性啟用的，這也不一定意味著IPDT主動監控給定埠。

在IPDT始終開啟以及當IPDT全域性啟用時可以全域性關閉/開啟IPDT的發行版中，其他功能實際上決定了它是否在特定介面上處於活動狀態（請參閱「功能區域」部分）。

功能領域

從給定介面發出的IPDT及其ARP探測器用於以下功能：

- 網路行動化服務通訊協定(NMSP)，版本3.2.0E、15.2(1)E、3.5.0E及更新版本
- 裝置感測器，版本15.2(1)E、3.5.0E及更高版本
- 1X，MAC Authentication Bypass(MAB)，會話管理器
- 基於Web的身份驗證
- Auth-proxy
- 適用於靜態主機的IP來源防護
- Flexible netflow
- Cisco TrustSec(CTS)
- 媒體跟蹤
- HTTP重定向

功能表

平台	功能	預設開啟（啟動）	禁用方法	禁用CLI
Cat 2960/3750(Cisco IOS)	IPDT	15.2(1)E *	全域CLI（舊版本）* 每個介面	no ip device tracking * ip裝置跟蹤最大0 ***
Cat 2960/3750(Cisco	NMSP	否	全域性CLI或 每個介面的CLI	no nmsp enable nmsp附件禁止使****

IOS)				
Cat 2960/3750(Cisco IOS)	裝置感測器	15.0(1)SE	全域性CLI	無宏自動監控
Cat 2960/3750(Cisco IOS)	ARP窺探	15.2(1)E**	不適用	不適用
Cat 3850	IPDT	所有版本*	每個介面*	ip裝置跟蹤最大0 ***
Cat 3850	NMSP	所有版本	每個介面	nmsp附件抑制
Cat 3850	裝置感測器	否	不適用	不適用
Cat 3850	ARP窺探	所有版本**	不適用	不適用
Cat 4500	IPDT	15.2(1)E / 3.5.0E *	全域CLI（舊版本）* 每個介面	no ip device tracking * ip裝置跟蹤最大0 ***
Cat 4500	NMSP	否	全域性CLI或 每個介面的CLI	no nmsp enable nmsp附件禁止使****
Cat 4500	裝置感測器	15.1(1)SG/3.3.0SG	全域性CLI	無宏自動監控
Cat 4500	ARP窺探	15.2(1)E/3.5.0E節**	不適用	不適用

功能

- 在較新版本中，無法全域性禁用IPDT，但是IPDT僅在埠上處於活動狀態（如果需要它的功能處於活動狀態）。
- 只有在特定功能組合啟用時，ARP監聽才會處於活動狀態。

- 如果在每個介面上禁用IPDT，它不會停止ARP監聽，但會阻止IPDT跟蹤。可從i3.3.0SE、15.2(1)E、3.5.0E及更高版本獲得此功能。
- 只有全域性啟用NMSP時，每個介面的NMSP抑制才可用。

禁用IPDT

在預設未啟用IPDT的版本中，可以使用以下命令全域性關閉IPDT:

```
<#root>

Switch(config)#

no ip device tracking
```

在IPDT一律開啟的版本中，上一個命令無法使用，或不允許停用IPDT(思科錯誤ID CSCuj04986)。在這種情況下，有幾種方法可以確保IPDT不監控特定連線埠或不會產生重複的IP警報。

輸入IP Device Tracking Probe Delay 10命令

此命令不允許交換器在偵測到連結啟動/翻動時傳送10秒的探測，這可以最大程度地降低在連結另一側的主機檢查重複IP位址時傳送探測的可能性。RFC為重複地址檢測指定了10秒的視窗，因此，如果您延遲裝置跟蹤探測，則可以在大多數情況下解決該問題。

如果在主機（例如Microsoft Windows PC）處於重複地址檢測階段時，交換機為客戶端傳送ARP探測，則主機將探測檢測為重複的IP地址，並向使用者顯示一條消息，說明在網路上找到了重複的IP地址。如果PC沒有獲得地址，並且使用者必須手動釋放/續訂地址，斷開連線並重新連線到網路，或者重新啟動PC以獲得網路訪問許可權。

除了探測延遲，當交換機檢測到來自PC/主機的探測時，延遲也會自行重置。例如，如果探測計時器已計為五秒鐘，並且檢測到來自PC/主機的ARP探測，則該計時器將重置回10秒。

此組態已透過思科錯誤ID CSCtn27420提供。

輸入IP裝置跟蹤探測使用SVI命令

使用此命令，可以配置交換機以傳送不符合RFC的ARP探測；IP源不是0.0.0.0，而是主機所在的VLAN中的交換機虛擬介面(SVI)。Microsoft Windows電腦不再將探測視為由RFC 5227定義的探測，並且不會標籤潛在的重複IP。

輸入IP Device Tracking Probe Auto-Source [fallback <host-ip> <mask>] [override]命令

對於沒有可預測/可控制的終端裝置的客戶，或者對於擁有許多隻使用L2角色的交換機的客戶來說，SVI的配置（它在設計中引入了第3層變數）不是一個合適的解決方案。15.2(2)E版及更新版本中引入的一項增強功能，允許任意分配不需要屬於交換機的IP地址，以在IPDT生成的ARP探測中用作源地址。此增強功能提供機會，以便按以下方式修改系統的自動行為（此清單顯示使用每個指令後

系統如何自動行為）：

輸入IP Device Tracking Probe Auto-Source命令

1. 將源設定為VLAN SVI（如果存在）。
2. 在IP主機表中搜尋同一子網的源/MAC對。
3. 傳送零IP來源（與預設情況相同）。

輸入IP Device Tracking Probe Auto-Source Fallback 0.0.0.1 255.255.255.0命令

1. 將源設定為VLAN SVI（如果存在）。
2. 在IP主機表中搜尋同一子網的源/MAC對。
3. 使用提供的主機位和遮罩從目的地IP計算來源IP。

輸入IP裝置跟蹤探測功能自動源回退0.0.0.1 255.255.255.0覆蓋命令

1. 將源設定為VLAN SVI（如果存在）。
2. 使用提供的主機位和遮罩從目的地IP計算來源IP。

> 註：覆蓋可使您跳過對表中條目的搜尋。

作為上述計算的示例，假設您探測主機192.168.1.200。使用提供的掩碼和主機位，可以生成源地址192.168.1.1。 如果探測條目10.5.5.20，可以生成源地址為10.5.5.1的ARP探測，以此類推。

輸入IP Device Tracking Maximum 0命令

此命令不會真正禁用IPDT，但會將跟蹤的主機數量限製為零。這不是推薦的解決方案，必須謹慎使用，因為它會影響依賴IPDT的所有其他功能，包括思科錯誤ID CSCun81556所述的埠通道配置。

關閉觸發IPDT的活動功能

可能觸發IPDT的某些功能包括NMSP、裝置感測器、dot1x/MAB、WebAuth和IPSG。建議不要在主幹埠上啟用這些功能。此解決方案專用於最困難或最複雜的情況，在這些情況下，以前提供的所有解決方案要麼都不如預期工作，要麼產生了其他問題。但是，這是在禁用IPDT時允許極端粒度的唯一解決方案，因為您只能關閉導致問題的與IPDT相關的功能，而所有其他功能均不受影響。

在最新的Cisco IOS版本15.2(2)E及更高版本中，您會看到類似以下的輸出：

```
<#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
```

輸出底部所有帽中的兩行是使用IPDT工作的兩行。如果禁用介面中運行的單個服務，則可以避免禁用裝置跟蹤時產生的大多數問題。

在早期版本的Cisco IOS中，目前還無法獲得這種知道介面下啟用哪些模組的簡易方法，因此您必須執行更多相關的程式才能取得相同的結果。您必須開啟debug ip device track interface，該介面是低頻率日誌，在大多數設定中必須安全。請注意不要啟用debug ip device tracking all，因為反之，這會使控制檯在擴展情況下泛洪。

啟用調試後，將介面恢復為預設值，然後從介面配置中新增和刪除IPDT服務。調試的結果會告訴您哪個服務已使用您使用的命令啟用/禁用。

範例

```
<#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)#
```

輸出顯示您已啟用功00000008掩碼，且新功能掩碼為0000004C。

現在，移除剛新增的組態：

```
<#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)#
```

刪除特徵掩00000008後，您會看到原始00000044認遮罩，該遮罩必須是原始的預設遮罩。此值為00000044，因為AIM為0x00000004，而SM為0x00000040，二者共同導致0x00000044。

有幾種IPDT服務可以在介面下運行：

IPT服務	介面
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，為IPDT配置了HOST_TRACK_CLIENT_SM(SESSION-MANAGER)和HOST_TRACK_CLIENT_ATTACHMENT（也稱為AIM/NMSP）模組。若要關閉此介面上的IPDT，您必須同時停用這二者，因為只有同時停用所有使用它的功能時，IPDT才會停用。

停用這些功能後，您會得到類似以下的輸出：

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

透過這種方式，IPDT會以更精細的方式停用。

以下是用來停用之前討論的一些功能的命令範例：

- nmsp attach suppress
- 無宏自動監控

註：最新功能必須僅在支援智慧埠的平台上可用，智慧埠用於根據交換機在網路中的位置啟用功能，以及針對整個網路的大規模配置部署。

驗證IPDT操作

使用以下命令驗證裝置上的IPDT狀態：

- show ip device tracking
  此命令顯示啟用IPDT的介面以及當前跟蹤MAC/IP/介面關聯的介面。
- clear ip device tracking
- 此命令清除與IPDT相關的條目。

注意：交換機將ARP探測傳送到已刪除的主機。如果存在主機，它會響應ARP探測功能，然後交換機將為該主機新增一個IPDT條目。在clear IPDT命令之前必須禁用ARP探測；這樣，所有ARP條目都將丟失。如果在clear ip device tracking命令後啟用ARP探測，則所有條目都會再次返回。

- debug ip device tracking
  此命令允許您收集調試以即時顯示IPDT活動。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。