IPDTデバイスの動作の確認

内容

はじめに

このドキュメントでは、IPデバイストラッキング(IPDT)の動作を確認する方法と、これらのアクションを無効にする方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの出力は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco WS-C2960X
- Cisco IOS® 15.2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

IPDT の概要

定義と用途

IPDT の主要なタスクは、接続されたホストを追跡することです（MAC および IP アドレスの関連付け）。これを行うために、ユニキャストAddress Resolution Protocol(ARP)プローブを30秒のデフォルト間隔で送信します。これらのプローブは、リンクの反対側に接続されているホストのMACアドレスに送信され、RFC 5227に記載されているARPプローブ定義に基づいて、ARPの送信元である物理インターフェイスのMACアドレスと送信元IPアドレス0.0.0.0を宛先とするデフォルトソースとしてレイヤ2(L2)を使用します

抜粋

このドキュメントでは、ARPプローブという用語は、すべてゼロの送信元IPアドレスを持つARP要求パケット（ローカルリンク上のブロードキャスト）を指すために使用されます。送信側のハードウェアアドレスには、パケットを送信するインターフェイスのハードウェアアドレスが含まれている必要があります。送信元IPアドレスフィールドは、アドレスが別のホストによってすでに使用されていることが判明した場合に、同じリンク上の他のホストでARPキャッシュが破損しないように、すべて0に設定する必要があります。ターゲットIPアドレスフィールドは、プローブされるアドレスに設定する必要があります。ARPプローブは、質問（このアドレスを使用する人はいますか？）と暗黙の文（このアドレスを使用したいと考えています）の両方を伝えます。

IPDT の目的は、スイッチが IP アドレスによりそのスイッチに接続されているデバイスのリストを取得して維持することです。プローブはトラッキングエントリを入力しません。これは、ホストからのARP要求/応答を通じて学習されたエントリをテーブル内に保持するためだけに使用されます。

IP ARPインスペクションは、IPDTが有効になると自動的に有効になります。これにより ARP パケットの監視時に新しいホストの出現が検出されます。ダイナミック ARP インスペクションが有効になっている場合、検証対象の ARP パケットのみを使用して、デバイス トラッキング テーブルの新しいホストを検出します。

IP DHCP スヌーピングが有効になっている場合、DHCP が IP アドレスを割り当てたり取り消したりすると、新しいホストの出現や削除が検出されます。 特定のホストのDHCPトラフィックが確認されると、IPDT ARPプローブ間隔タイマーがリセットされます。

IPDT は常時使用できる機能でした。ただし、最新の Cisco IOS® リリースでは、相互依存性がデフォルトで有効になっています（Cisco Bug ID CSCuj04986 を参照）。ダイナミック アクセス コントロール

リスト（ACL）の送信元 IP を入力したり、セキュリティ グループ タグへの IP アドレスのバインディングを維持したりするために、IP/MAC ホストの関連付けのデータベースを使用する場合、これは非常に有用です。

ARP プローブは、次の 2 つの状況下で送信されます。

- IPDT データベースの現在のエントリに関連付けられたリンクが DOWN 状態から UP 状態に移り、ARP エントリが入力されました。
- IPDT データベースのエントリに関連付けられたすでに UP 状態のリンクには期限切れのプローブ間隔があります。

問題

スイッチから送信されるキープアライブプローブはL2チェックです。したがって、スイッチから見ると、ARPの送信元として使用されるIPアドレスは重要ではありません。この機能は、IPアドレスがまったく設定されていないデバイスで使用できるため、IP送信元0.0.0.0は関係ありません。

ホストはこのメッセージを受信すると、応答して受信パケットに使用できる IP アドレス（自身の IP アドレス）のみを宛先 IP フィールドに入力します。これにより、誤った重複IPアドレスのアラートが発生する可能性があります。これは、応答するホストが自身のIPアドレスをパケットの送信元と宛先の両方として認識するためです。「重複IPアドレス0.0.0.0」を参照してください。エラー メッセージのトラブルシューティング』を参照してください。

デフォルトの状態と動作

IPDTのグローバルオン/オフ設定は従来の動作であり、特定の機能を動作させるためにIPDTをオンにする必要があることをお客様が必ずしも認識していなかったため、フィールドで問題が発生しました。現在のリリースでは、IPDTを必要とする機能を有効にした場合、IPDTはインターフェイスレベルでのみ制御されます。

これらのリリースでは、IPDTはデフォルトでグローバルに有効になっています。つまり、グローバル設定コマンドはありません。

- Catalyst 2000/3000:15.2(1)E
- Catalyst 3850:3.2.0SE
- Catalyst 4k:15.2(1)E/3.5.0E

IPDT がグローバルに有効になっていても、必ずしも IPDT が特定のポートをアクティブに監視することを意味するわけではないため、注意が必要です。

IPDTが常に有効なリリース、およびIPDTがグローバルに有効な場合にIPDTをグローバルにオフ/オンに切り替えることができるリリースでは、他の機能によって、実際には特定のインターフェイスでアクティブかどうかが決まります（「機能領域」のセクションを参照）。

機能エリア

特定のインターフェイスから送信される IPDT とその ARP プローブは次の機能で使用されます。

- ネットワーク モビリティ サービス プロトコル（NMSP）、バージョン 3.2.0E、15.2(1) E、3.5.0E 以降
- デバイス センサー、バージョン 15.2(1) E、3.5.0E 以降
- 1X、MAC 認証バイパス（MAB）、セッション マネージャ
- Web ベースの認証
- 認証プロキシ
- スタティックホスト用のIPソースガード(IPSG)
- Flexible NetFlow
- Cisco TrustSec（CTS）
- メディア トレース
- HTTP リダイレクト

機能マトリクス

Platform	機能	既定のオン（開始する場所）	Disableメソッド	CLIの無効化
Cat 2960/3750(Cisco IOS)	IPDT	15.2(1)E *	グローバルCLI（旧リリース）* インターフェイスごと	no ip device tracking * ipデバイストラッキング最大0 ***
Cat 2960/3750(Cisco IOS)	NMSP	いいえ	グローバルCLIまたは インターフェイスごとのCLI	no nmsp enable nmsp添付ファイル抑制****
Cat 2960/3750(Cisco IOS)	デバイスセンサー	15.0(1)SE	グローバルCLI	no macro auto monitor
Cat 2960/3750(Cisco IOS)	ARPスヌーピング	15.2(1)E **	該当なし	該当なし
Cat 3850	IPDT	すべてのリリース *	インターフェイスごと*	ipデバイストラッキング最大0 ***

Cat 3850	NMSP	すべてのリリース	インターフェイスごと	nmsp添付の抑制
Cat 3850	デバイスセンサー	いいえ	該当なし	該当なし
Cat 3850	ARPスヌーピング	すべてのリリース **	該当なし	該当なし
Cat 4500	IPDT	15.2(1)E / 3.5.0E *	グローバルCLI（旧リリース）* インターフェイスごと	no ip device tracking * ipデバイストラッキング最大0 ***
Cat 4500	NMSP	いいえ	グローバルCLIまたは インターフェイスごとのCLI	no nmsp enable nmsp添付ファイル抑制****
Cat 4500	デバイスセンサー	15.1(1)SG / 3.3.0SG	グローバルCLI	no macro auto monitor
Cat 4500	ARPスヌーピング	15.2(1)E / 3.5.0E **	該当なし	該当なし

機能

- 新しいリリースではIPDTをグローバルに無効にすることはできませんが、IPDTを必要とする機能がアクティブな場合、IPDTはポートでのみアクティブになります。
- ARPスヌーピングは、特定の機能の組み合わせによって有効になっている場合にのみアクティブになります。
- インターフェイスごとにIPDTを無効にしても、ARPスヌーピングは停止せず、IPDTの追跡も妨げられます。これは、i3.3.0SE、15.2(1)E、3.5.0E以降で使用できます。
- インターフェイスごとのNMSP抑制は、NMSPがグローバルに有効になっている場合にのみ使用できます。

IPDT の無効化

IPDT がデフォルトで有効になっていないリリースでは、次のコマンドを使用して IPDT をグローバルに無効にすることができます。

<#root>

```
Switch(config)#
no ip device tracking
```

IPDTが常にオンになっているリリースでは、以前のコマンドが使用できないか、IPDTを無効にできません(Cisco Bug ID CSCuj04986)。この場合、IPDT が特定のポートを監視しないようにしたり、重複 IP のアラートを生成しないようにしたりするための方法がいくつかあります。

ip device tracking probe delay 10 コマンドの入力

このコマンドを使用すると、スイッチはリンク アップまたはリンク フラップを検出したときに 10 秒間プローブを送信できなくなります。これにより、リンクの反対側のホストが重複 IP アドレスを確認している間にプローブが送信される可能性が最小限に抑えられます。RFCでは、重複アドレス検出に10秒のウィンドウを指定しています。そのため、デバイストラッキングプローブを遅らせた場合、ほとんどの場合この問題は解決します。

ホスト（たとえば Microsoft Windows PC）が重複アドレス検出のフェーズにある間に、スイッチでクライアントへの ARP プローブが送信された場合、ホストはこのプローブを重複 IP アドレスとして検知し、ネットワークで重複 IP アドレスが見つかったというメッセージをユーザに表示します。PCがアドレスを取得できず、ユーザがネットワークアクセスを取得するために、アドレスを手動で解放/更新するか、ネットワークを切断して再接続するか、PCをリブートする必要がある場合。

プローブ遅延に加えて、スイッチが PC/ホストからのプローブを検出したときも遅延がリセットされます。たとえば、プローブのタイマーが 5 秒までカウントしてから PC/ホストからの ARP プローブを検出した場合、タイマーはリセットされて 10 秒に戻ります。

この設定は Cisco Bug ID CSCtn27420 によって使用可能になりました。

IP Device Tracking Probe Use SVIコマンドの入力

このコマンドを使用すると、RFC非準拠のARPプローブを送信するようにスイッチを設定できます。IPソースは0.0.0.0ではなく、ホストが存在するVLAN内のスイッチ仮想インターフェイス(SVI)です。Microsoft Windows マシンでは、プローブが RFC 5227 で定義されているプローブとして見なされなくなり、潜在的な重複 IP がフラグされません。

ip device tracking probe auto-source [fallback <host-ip> <mask>] [override] コマンドの入力

予測可能または制御可能なエンドデバイスを持たないお客様、またはL2のみの役割で多数のスイッチを持つお客様には、設計にレイヤ3変数を導入するSVIの設定は適切なソリューションではあ

りません。バージョン15.2(2)E以降で導入された機能拡張では、IPDTによって生成されたARPプローブの送信元アドレスとして使用するために、スイッチに属している必要のないIPアドレスを任意に割り当てることができます。この拡張機能では、次の方法でシステムの自動動作を変更できます（次のリストで、各コマンドの使用後に行われるシステムの自動動作を示します）。

ip device tracking probe auto-source コマンドの入力

1. 送信元をVLAN SVIに設定します（存在する場合）。
2. 同じサブネットの IP ホスト テーブルで送信元と MAC のペアを検索します。
3. デフォルトの場合と同様に 0 の IP ソースを送信します。

ip device tracking probe auto-source fallback 0.0.0.1 255.255.255.0 コマンドの入力

1. 送信元をVLAN SVIに設定します（存在する場合）。
2. 同じサブネットの IP ホスト テーブルで送信元と MAC のペアを検索します。
3. ホスト ビットとマスクが指定された宛先 IP から送信元 IP を計算します。

ip device tracking probe auto-source fallback 0.0.0.1 255.255.255.0 override コマンドの入力

1. 送信元をVLAN SVIに設定します（存在する場合）。
2. ホスト ビットとマスクが指定された宛先 IP から送信元 IP を計算します。

> 注記：オーバーライドを指定すると、テーブル内のエントリの検索がスキップされます。

前述の計算の例として、ホスト 192.168.1.200 をプローブすると仮定します。指定のマスクとホスト ビットを使用して、送信元アドレス 192.168.1.1 を生成します。 エントリ10.5.5.20をプローブする場合は、送信元アドレス10.5.5.1などのARPプローブを生成できます。

ip device tracking maximum 0 コマンドの入力

このコマンドは実際に IPDT を無効にするのではなく、追跡されるホストの数を 0 に制限します。これは推奨されるソリューションではなく、IPDTに依存する他のすべての機能(Cisco Bug ID CSCun81556で説明されているポートチャネルの設定など)に影響するため、注意して使用する必要があります。

IPDT をトリガーするアクティブな機能の無効化

IPDTをトリガーできる機能には、NMSP、デバイスセンサー、dot1x/MAB、WebAuth、および

IPSGなどがあります。これらの機能は、トランクポートで有効にすることは推奨されません。このソリューションは、従来の使用可能なソリューションでは期待どおりの動作が得られなかったり、さらに問題が発生したりといった、最も困難な状況や複雑な状況に備えて用意されています。ただし、これは他の機能に影響を与えずに、問題の原因となる IPDT 関連機能のみを無効にすることができるので、IPDT の無効化時に詳細な設定を可能にする唯一のソリューションです。

最新の Cisco IOS、バージョン 15.2(2) E 以降では、次のような出力が表示されます。

<#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
```

出力の最下部にあるすべて大文字の 2 行は、IPDT を使用して動作する機能です。デバイス トラッキングを無効にしたときに発生する問題のほとんどは、インターフェイスで動作する 1 つのサービスを無効化すれば回避できます。

以前のバージョンのCisco IOSでは、インターフェイスで有効になっているモジュールを簡単に確認する方法がまだ利用できないため、同じ結果を得るためにより複雑なプロセスを実行する必要があります。debug ip device track interfaceをオンにする必要があります。これは、ほとんどのセットアップで安全でなければならない低頻度のログです。反対に、debug ip device tracking all はスケール状況のコンソールをフラッディングするため、有効にしないよう注意してください。

デバッグを有効にすると、インターフェイスがデフォルトに戻り、インターフェイス設定の IPDT サービスが追加および削除されます。デバッグの結果から、使用したコマンドによって有効または無効になったサービスがわかります。

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)#
```

出力から分かるのは、機能00000008を有効にしていて、新しい機能マスクが0000004Cであるということです。

ここでは、追加した設定を削除します。

<#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)#
```

機能 00000008 を削除すると、元のデフォルト マスクである 00000044 マスクが表示されます。AIM の 0x00000004 と SM の 0x00000040 を合わせた結果が 0x00000044 であることから、この 00000044 という値が予想されます。

インターフェイスで動作できる複数の IPDT サービスを次に示します。

IPTサービス	インターフェイス
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

例では、HOST_TRACK_CLIENT_SM (SESSION-MANAGER) および HOST_TRACK_CLIENT_ATTACHMENT (別名 AIM/NMSP) モジュールが IPDT に設定されます。IPDT を使用するすべての機能も無効になっている場合にのみ IPDT が無効化されるため、このインターフェイスで IPDT を無効にするには、両方を無効にする必要があります。

これらの機能を無効にすると、次のような出力が表示されます。

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

このように、IPDT はより詳細に無効化されます。

前述した機能の一部を無効にするために使用するコマンドの例は次のとおりです。

- nmsp attach suppress
- no macro auto monitor

注：最新の機能は、スマートポートをサポートするプラットフォームでのみ使用可能である必要があります。スマートポートは、ネットワーク内のスイッチの場所に基づいて、およびネットワーク全体の大規模構成の展開で機能を有効にするために使用されます。

IPDT の動作確認

デバイスの IPDT の状態を確認するには、次のコマンドを使用します。

- show ip device tracking
  このコマンドは、IPDTが有効で、MAC/IP/インターフェイスの関連付けが現在追跡されているインターフェイスを表示します。
- clear ip device tracking
- このコマンドは IPDT 関連のエントリをクリアします。

注：スイッチは、削除されたホストにARPプローブを送信します。ホストが存在する場合はARP プローブに応答し、スイッチがホストの IPDT エントリを追加します。clear IPDTコマンドを実行する前にARPプローブを無効にする必要があります。このようにすると、すべてのARPエントリが削除されます。clear ip device tracking コマンド後に ARP プローブを有効にすると、すべてのエントリが戻されます。

- debug ip device tracking
  このコマンドを使用すると、IPDTアクティビティをリアルタイムで表示するためにデバッグを収集できます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。