IP デバイス追跡 (IPDT) の概要

目次

概要

このドキュメントでは、IP デバイス トラッキング (IPDT) について、無効化する方法と動作の確認方法を説明します。

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)。 追跡のために、ユニキャスト アドレス解決プロトコル (ARP) プローブが 30 秒のデフォルト間隔で送信されます。 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、次に抜粋する RFC 5227 に記載されている ARP プローブの定義に基づいて、デフォルトの送信元 (ARP の送信元である物理インターフェイスの MAC アドレスおよび送信者 IP アドレス (0.0.0.0) としてレイヤ 2 (L2) を使用します。

このドキュメントでは、「ARP プローブ」という用語は、「送信者 IP アドレス」がすべて 0 の ARP 要求パケット (ローカル リンク上のブロードキャスト) を指して使われます。 「送信者ハードウェア 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 アドレスを含める必要があります。 アドレスが別のホストによってすでに使用中であった場合、同じリンク上

にある他のホストの ARP キャッシュへの影響を避けるため、「送信者 IP アドレス」フィールドはすべて 0 に設定する必要があります。 「ターゲット IP アドレス」フィールドではプローブ対象のアドレスを設定する必要があります。 ARP プローブは、質問 (「このアドレスは使用されているか」) と黙示的宣言 (「このアドレスの使用を希望する」) の両方を伝送します。」) を再生します。

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。 プローブでは、トラッキング エントリは入力されません。 ホストからの ARP 要求または応答によってエントリが特定された後、テーブルでエントリを保持するためだけに使用されます。

IPDT が有効になっている場合は、IP ARP インスペクションが自動的に有効化されます。 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。

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。

既知の問題

スイッチによって送信される「キープアライブ」プローブは L2 チェックです。 スイッチの観点からすると、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されるので、0.0.0.0 の IP 送信元は関連しないということです。

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。 その結果、重複 IP アドレスの誤ったアラートが発生する可能性があります。これは、応答するホストがパケットの送信元と宛先の両方で自身の IP アドレスを参照することが原因です。 重複 IP アドレスのシナリオの詳細については、『重複 IP アドレス 0.0.0.0. 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 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 が常に有効で、オン/オフをグロー

バルに切り換えられるリリースでは、IPDT がグローバルに有効になっている場合、実際は、特定のインターフェイスでアクティブであるかどうかを判断するのは他の機能です（「機能エリア」の項を参照）。

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 ホストの IP サービス ゲートウェイ（IPSG）
- Flexible NetFlow
- Cisco TrustSec（CTS）
- メディア トレース
- HTTP リダイレクト

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。

```
# no ip device tracking
```

IPDT が常に有効になっているリリースでは、前述のコマンドを使用することも、IPDT を無効にすることもできません（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 は重複アドレス検出の間隔を 10 秒間に指定しており、デバイストラッキング プローブを遅らせた場合、ほとんどのケースで問題は解決します。

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 でアドレスが取得できない場合、ネットワーク アクセスを確保するために、ユーザは手動でアドレスを解放/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ります。

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

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 のスイッチ仮想インターフェイス（SVI）になります。 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 デバイスがない場合や、L2 専用ロールに多数のスイッチがある場合は、設計でレイヤ 3 の変数が導入されている 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、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、スイッチが使用する必要がない IP アドレスを任意に割り当てられるようにする拡張機能が導入されました。 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. VLAN SVI に送信元を設定します（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. VLAN SVI に送信元を設定します（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. VLAN SVI に送信元を設定します（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: オーバーライドするとテーブルのエントリの検索はスキップされます。
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 の ARP プローブを生成できます。他も同様です。

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。 Cisco Bug ID CSCun81556 に記載されているように、このソリューションは IPDT に依存する他のすべての機能（ポート チャネル設定など）に影響を与えるため、推奨されていません。使用する場合は注意が必要です。

IPDT をトリガーするアクティブな機能の無効化

IPDT をトリガーする機能には、NMSP、デバイス センサー、dot1x/MAB、Web 認証、および IPSG が含まれます。 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。

```
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
```

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。

Cisco IOS の以前のバージョンでは、この「簡単な」方法を使用してインターフェイスで有効になっているモジュールを特定することができないので、同じ結果を得るために、より複雑なプロセスを経る必要があります。 **debug ip device track interface** を有効にしてください。これは、ほとんどのセットアップで安全に使用できる低頻度の口グです。 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。

次に例を示します。

```
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)#
```

出力によって判明することは、機能 00000008 を有効にしたこと、および新機能のマスクが 0000004C であることです。

ここでは、追加した設定を削除します。

```
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)#
```

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。

IPDT サービス	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

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。

```
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
-----------------------------------------
```

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: 最新機能は、スマート ポート (SmartPort Flash プレゼンテーション) をサポートするプラットフォームでのみ使用できます。スマート ポートは、ネットワークのスイッチの位置に基づいて機能および設定を有効にしたり、ネットワーク全体の導入された大量の設定を有効にしたりできます。

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 ...**

  このコマンドによって、IPDT が有効で、MAC/IP/インターフェイスの関連付けが監視対象になっているインターフェイスが表示されます。

- **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。 IPDT コマンドをクリアする前に ARP プローブを無効にする必要があります。 この方法ですべての ARP エントリを削除してください。 **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、デバッグを収集してリアルタイムの IPDT アクティビティを表示することができます。