

重複した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

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[問題](#)

[重複 IP アドレスの原因](#)

[解決方法](#)

[関連情報](#)

はじめに

このドキュメントでは、Microsoft Windows Vista以降のバージョンのユーザが受信する「Duplicate IP Address 0.0.0.0」エラーメッセージとその解決策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内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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。

問題

Microsoft Windows Vista以降では、Dynamic Host Configuration Protocol(DHCP)プロセスの発生時にネットワーク上の重複アドレスを検出するために使用される新しいメカニズムが導入されました。この新しい検出のフローは、[RFC 5227](#)^[2] に記述されます。

この検出フローのトリガーの1つは、セクション[2.1.1](#)^[2]で定義されています。次に定義を示しま

す。

また、この期間中にホストがAddress Resolution Protocol (ARP ; アドレス解決プロトコル) プロローブを受信したときに、パケットの「ターゲットIPアドレス」がプロローブ対象のアドレスであり、パケットの「送信元ハードウェアアドレス」がホストのインターフェイスのハードウェアアドレスでない場合、ホストは同様にこれをアドレス競合として扱い、上記のように設定エージェントにエラーを通知する必要があります。これは、複数のホストで同じアドレスが何らかの理由で誤って設定されている場合に、そのアドレスが安全に使用できるかどうかについての調査が同時に行われる場合に発生する可能性があります。

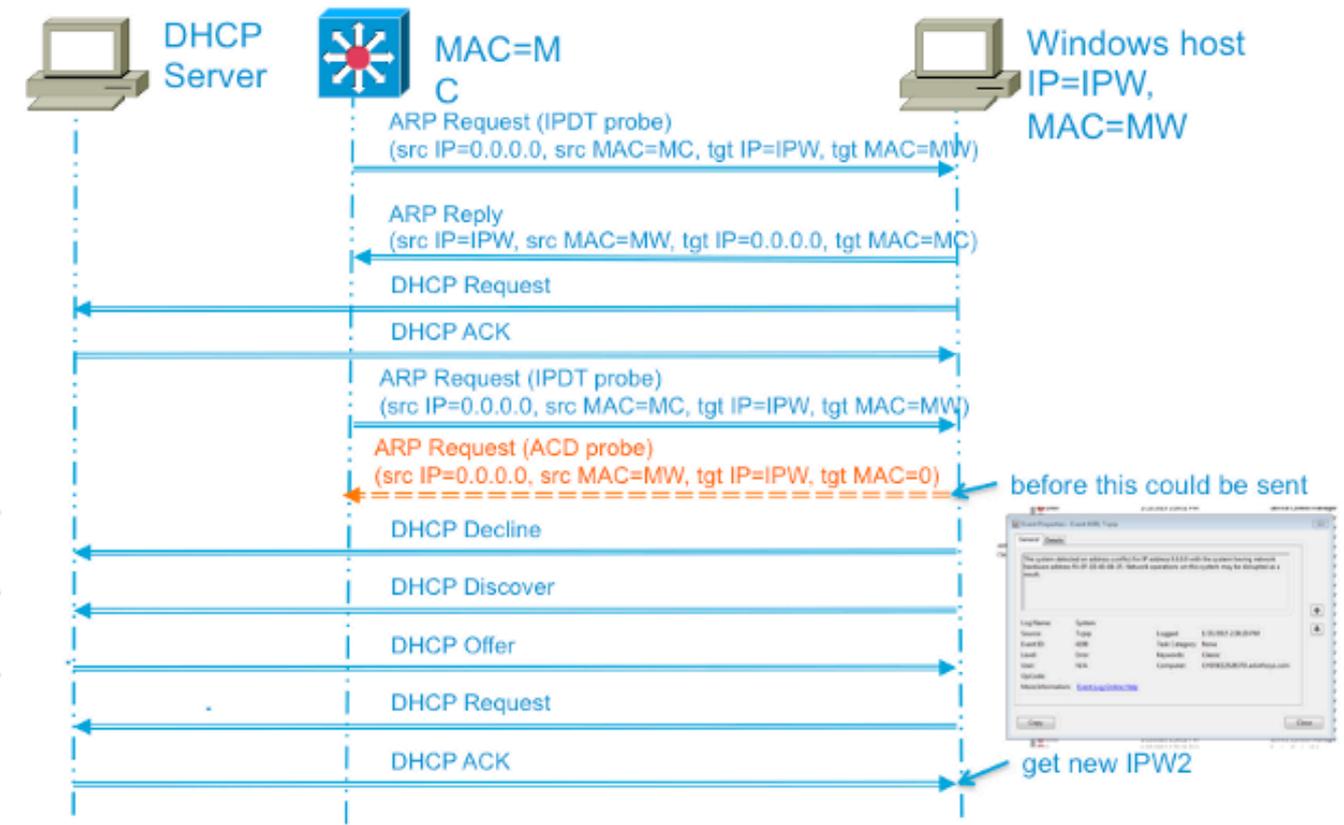
Cisco IOS®では、IPデバイストラックが発生し、それを使用する機能 (802.1xなど) がCisco IOSスイッチでイネーブルにされると、アドレス0.0.0.0を送信元とするAddress Resolution Protocol (ARP ; アドレス解決プロトコル) プロローブを使用してIPデバイストラッキングのキャッシュが維持されます。IPデバイストラックの目的は、スイッチがIPアドレスによってスイッチに接続されているデバイスのリストを取得して維持することです。プロローブはトラックエントリに入力されません。学習後にテーブル内のエントリをアクティブにして維持するために使用されます。このIPアドレスは、アクセスコントロールリスト(ACL)がインターフェイスに適用されるときに使用され、ACL内の送信元アドレスがクライアントIPアドレスで置き換えられます。この機能は、アクセスリストが802.1xまたはシスコのスイッチ上の他のFlex-Auth機能で使用される場合に重要です。

重複 IP アドレスの原因

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プロローブが送信された場合、Microsoft Windows ではこのプロローブを重複したIPアドレスとして検知し、0.0.0.0のネットワークで重複したIPアドレスが見つかったというメッセージを表示します。PCはIPアドレスを取得しないため、ユーザは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を再起動してネットワークアクセスを取得する必要があります。

失敗したパケットシーケンスの例を次に示します。

Failing Sequence Packet Flow



© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential



解決方法

この問題を回避するために使用できる複数の方法があります。次に、考えられる回避策のリストを示します。

- この問題を回避するために使用される最も効果的な方法は、PCが存在するVLANのスイッチ仮想インターフェイス(SVI)からプローブを送信するように、RFC非準拠のARPプローブをスイッチに設定することです。SVIが仮想ローカルエリアネットワーク(VLAN)用に設定され、次の2つのコマンドのいずれかを使用する場合、IPデバイストラッキング(IPDT)プローブの送信元IPアドレスは0.0.0.0にはなりません。したがって、重複IPアドレスのエラーが発生しないことは確実です。

次のコマンド形式は、古いコードバージョン用です。

```
<#root>
```

```
ip device tracking probe use-svi
```

この設定は、現在 Microsoft Windows の重複アドレス検出のエラーメッセージをトリガー

しません。このメソッドでの注意点は、DHCP を実行する Microsoft Windows のクライアントが存在するすべての VLAN のすべてのスイッチに SVI が存在する必要があります。この方式は拡張が困難なため、シスコではIPデバイストラッキングプロブの遅延を主要な方式として使用することを推奨しています。SVI は 6500 シリーズ スイッチのプラットフォームで現在使用できません。このコマンドは、2900、3500、および 3700 シリーズ スイッチ プラットフォーム上の Cisco IOS バージョン 12.2(55)SE、および 4500 シリーズ スイッチ プラットフォーム上の Cisco IOS バージョン 15.1(1)SG に実装されました。

新しいコードバージョン用のコマンド形式は次のとおりです。

```
<#root>
```

```
ip device tracking probe auto-source fallback
```

```
[override]
```

この最新のCommand Line Interface (CLI ; コマンドラインインターフェイス) コマンドは、Cisco IOSバージョン15.2EでCisco Bug ID [CSCtn27420](#)によって導入されました。これは、デフォルトの送信元IPアドレス0.0.0.0を使用する代わりに、ユーザ定義のARP要求の送信元IPアドレスを許可するために追加されました。新しいグローバルコマンド `ip device tracking probe auto-source fallback 0.0.0.x 255.255.255.0 override` ユーザはサブネットで0.0.0.xのホストアドレスを使用して、IPアドレスの重複の問題を回避できます。特定のVLANのSVIがない場合、代わりにプロブの送信元としてフォールバックホストIPが使用されます。

- この問題を回避するために使用される非SVIの主な代替手段は、Microsoft Windowsが重複IPアドレスの検出を完了する時間を確保できるように、スイッチからのプロブを遅らせることです。これは、アクセスポートおよびリンクアップシナリオでのみ有効です。プロブを遅延させるには、次のコマンドを入力します。

```
<#root>
```

```
ip device tracking probe delay 10
```

RFCでは、重複アドレスを検出するための10秒間のウィンドウを指定しています。デバイストラッキングプローブを遅らせると、ほとんどすべてのケースで問題が解決します。プローブ遅延に加えて、スイッチが PC 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せん。たとえば、プローブタイマーが5秒までカウントされ、PCからのARPプローブを検出した場合、タイマーは10秒にリセットされます。同様にタイマーをリセットするため、DHCPスヌープも有効にすると、このウィンドウをさらに短縮できます。まれに、スイッチからプローブが送信される数ミリ秒前に PC から ARP プローブが送信される場合があり、この場合もエンド ユーザへの重複アドレスのメッセージがトリガーされます。このコマンドは、2900、3500、および 3700 シリーズ スイッチ プラットフォーム上の Cisco IOS バージョン 15.0(1)SE、4500 シリーズ スイッチ プラットフォーム上の Cisco IOS バージョン 15.0(2)SG、および 6500 シリーズ スイッチ プラットフォーム上の Cisco IOS バージョン 12.2(33)SX17 で導入されました。

- この問題を解決するために使用されるもう1つの方法は、リンクがオンラインになった後に重複アドレス検出がこれほど遅く発生する理由を判断するために、クライアントのトラブルシューティングを行うことです。スイッチにはこのプロセスが発生する時間を判断する方法がないため、競合を防ぐためにプローブ遅延に設定されている時間を見積もります。重複アドレス検出がこれほど遅く発生する原因を効果的にトラブルシューティングするには、IPデバイストラッキングプローブの動作に関する詳細な情報が役立ちます。

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は DOWN 状態から UP 状態に移行します。
- IPDTデータベース内のエントリに関連付けられたリンクがすでにUP状態にあり、プローブ間隔が期限切れになっている。

IPデバイストラッキングプローブの間隔を設定するには、次のコマンドを入力します。

```
<#root>
```

```
ip device tracking probe interval
```

デフォルトの間隔は 30 秒です。この情報を表示するには、次のコマンドを入力します。

```
<#root>
```

```
show ip device tracking all
```

```
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
```

```
-----
IP Address  MAC Address  Vlan  Interface          STATE
-----
10.0.0.1    a820.661b.b384  301  GigabitEthernet0/1  INACTIVE
```

```
Total number interfaces enabled: 1
Enabled interfaces:
  Gi0/1
```

最初のエントリがDOWN状態からUP状態に移行した後は、プローブの遅延期間中にスイッチがそのデバイスからのトラフィックを認識しない限り、それ以上のプローブは送信されません。また、前述のとおり、スイッチで ARP プローブを（同時に）送信する数ミリ秒前に PC で ARP プローブが送信された場合にのみ競合が発生します。

関連情報

- [シスコテクニカルサポートおよびダウンロード](#)

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。