

Fehlerbehebung bei doppelten IP-Adressen 0.0.0.0-Fehlermeldungen

Inhalt

[Einleitung](#)

[Problem](#)

[Ursache für doppelte IP-Adresse](#)

[Lösung](#)

Einleitung

Dieses Dokument beschreibt die Fehlermeldung "Duplicate IP Address 0.0.0.0" (IP-Adresse duplizieren), die von Benutzern von Microsoft Windows Vista und späteren Versionen empfangen wurde, sowie die entsprechende Auflösung.

Problem

Mit Microsoft Windows Vista und höheren Versionen hat Microsoft einen neuen Mechanismus eingeführt, mit dem doppelte Adressen im Netzwerk erkannt werden, wenn der DHCP-Prozess (Dynamic Host Configuration Protocol) auftritt. Dieser neue Erkennungsablauf wird in [RFC 5227](#) beschrieben.

Einer der Auslöser für diesen Erkennungsablauf ist in Abschnitt [2.1.1](#) definiert:

Wenn der Host in diesem Zeitraum einen ARP-Prüfpunkt (Address Resolution Protocol) empfängt, bei dem die Ziel-IP-Adresse des Pakets die Adresse ist, nach der gesucht wird, und die Absender-Hardware-Adresse des Pakets nicht die Hardware-Adresse einer der Schnittstellen des Hosts ist, SOLLTE der Host dies ebenfalls als Adresskonflikt behandeln und dem Konfigurierungs-Agenten wie oben einen Fehler signalisieren. Dies kann passieren, wenn zwei (oder mehrere) Hosts aus irgendeinem Grund versehentlich mit derselben Adresse konfiguriert wurden und beide diese Adresse gleichzeitig testen, um festzustellen, ob sie sicher verwendet werden kann.

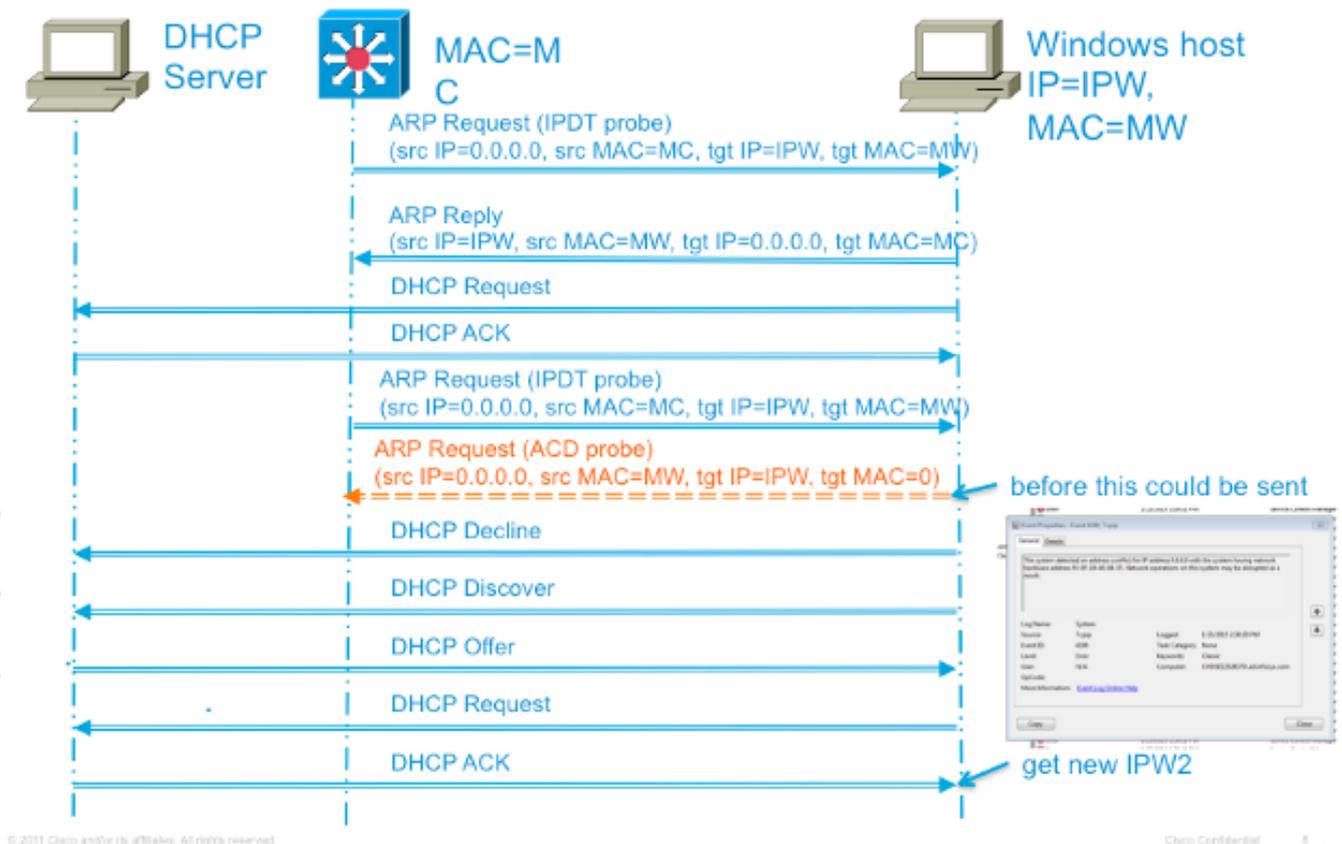
Cisco IOS[®] verwendet den Address Resolution Protocol (ARP)-Probe, der von einer Adresse von 0.0.0.0 stammt, um den IP-Geräte-Tracking-Cache aufrechtzuerhalten, wenn der IP-Geräte-Track auftritt. Eine Funktion, die diesen Cache verwendet, ist auf einem Cisco IOS-Switch aktiviert (z. B. 802.1x). Der Zweck der IP-Geräte-Spur besteht darin, dass der Switch eine Liste der Geräte abrufen und verwaltet, die über eine IP-Adresse mit dem Switch verbunden sind. Die Sonde füllt den Track-Eintrag nicht aus. Er wird verwendet, um den Eintrag in der Tabelle zu aktivieren und zu verwalten, nachdem er gelernt wurde. Diese IP-Adresse wird dann verwendet, wenn eine Zugriffskontrollliste (ACL) auf die Schnittstelle angewendet wird, um die Quelladresse in der ACL durch die Client-IP-Adresse zu ersetzen. Diese Funktion ist besonders wichtig, wenn Zugriffslisten mit 802.1x oder einer anderen FlexAuth-Funktion auf Cisco Switches verwendet werden.

Ursache für doppelte IP-Adresse

Wenn der Switch einen ARP-Prüfpunkt für den Client sendet, während sich der Microsoft Windows-PC in der Phase der Erkennung doppelter Adressen befindet, erkennt Microsoft Windows den Prüfpunkt als doppelte IP-Adresse und zeigt eine Meldung an, dass eine doppelte IP-Adresse im Netzwerk für 0.0.0.0 gefunden wurde. Der PC erhält keine IP-Adresse, und der Benutzer muss die Adresse manuell freigeben/erneuern, die Verbindung zum Netzwerk trennen und erneut herstellen oder den PC neu starten, um Netzwerkzugriff zu erhalten ...

Dies ist ein Beispiel für die fehlgeschlagene Paketsequenz:

Failing Sequence Packet Flow



Lösung

Es gibt mehrere Methoden, mit denen dieses Problem umgangen werden kann. Dies ist eine Liste möglicher Problemumgehungen:

- Die effektivste Methode zur Vermeidung dieses Problems besteht darin, den Switch so zu konfigurieren, dass er einen nicht RFC-konformen ARP-Prüfpunkt sendet, um den Prüfpunkt von der Switch Virtual Interface (SVI) im VLAN zu beziehen, in dem sich der PC befindet. Wenn eine SVI für das Virtual Local Area Network (VLAN) konfiguriert ist und einer der beiden folgenden Befehle verwendet wird, ist die Absender-IP-Adresse in den IPDT-Tests niemals 0.0.0.0. Daher ist sicher, dass der Fehler "Duplicate IP address" nicht auftritt.

Dieses Befehlsformat gilt für ältere Codeversionen:

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

Diese Konfiguration löst derzeit nicht die Fehlermeldung zur Erkennung doppelter Adressen in Microsoft Windows aus. Der Nachteil dieser Methode ist, dass eine SVI auf jedem Switch in jedem VLAN vorhanden sein muss, in dem sich Microsoft Windows-Clients befinden, die DHCP ausführen. Diese Methode ist schwer skalierbar. Cisco empfiehlt daher, die IP-Geräte-Nachverfolgung als primäre Methode zu verwenden. SVI ist derzeit auf der Switch-Plattform der 6500 Serie nicht verfügbar. Dieser Befehl wurde in Cisco IOS Version 12.2(55)SE auf Switch-Plattformen Serien 2900, 3500 und 3700 und in Version 15.1(1)SG auf der Switch-Plattform der 4500 Serie implementiert.

Dieses Befehlsformat ist für neuere Codeversionen geeignet:

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

Dieser neueste CLI-Befehl (Command Line Interface) wurde über die Cisco Bug-ID [CSCtn27420](#) in Cisco IOS Version 15.2(2)E eingeführt. Sie wurde hinzugefügt, um eine benutzerdefinierte IP-Adresse für die ARP-Anforderungsquelle zuzulassen, anstatt die Standard-IP-Quelladresse 0.0.0.0 verwenden zu müssen. Der neue globale Befehl `ip device tracking probe auto-source fallback 0.0.0.x 255.255.255.0 override` ermöglicht es dem Benutzer, die Host-Adresse 0.0.0.x im Subnetz zu verwenden, um doppelte IP-Adressprobleme zu vermeiden. Wenn es für ein bestimmtes VLAN keine SVI gibt, wird stattdessen die Fallback-Host-IP verwendet, um die Probe zu beziehen.

- Die primäre Nicht-SVI-Alternative zur Umgehung des Problems besteht darin, die Überprüfung vom Switch aus zu verzögern, sodass Microsoft Windows Zeit hat, die Erkennung doppelter IP-Adressen abzuschließen. Dies gilt nur für Access Ports und das Herstellen von Verbindungen. Geben Sie den folgenden Befehl ein, um den Test zu verzögern:

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

Der RFC gibt ein Fenster von zehn Sekunden für die Erkennung doppelter Adressen an. Wenn Sie die Geräteverfolgung verzögern, wird das Problem in fast allen Fällen behoben. Zusätzlich zur Verzögerung der Probe wird der Timer auch zurückgesetzt, wenn der Switch eine Probe vom PC erkennt. Wenn beispielsweise der Prüfpunkt-Timer auf fünf Sekunden heruntergezählt wurde und einen ARP-Prüfpunkt vom PC erkennt, wird der Timer auf zehn Sekunden zurückgesetzt. Dieses Fenster kann weiter reduziert werden, wenn Sie auch DHCP-Snoop aktivieren, da der Timer auf ähnliche Weise zurückgesetzt wird. In seltenen Fällen sendet der PC einen ARP-Prüfpunkt in Millisekunden, bevor der Switch seinen Prüfpunkt sendet, was immer noch eine doppelte Adressnachricht an den Endbenutzer auslöst. Dieser Befehl wurde in Cisco IOS Version 15.0(1)SE auf Switch-Plattformen der Serien 2900, 3500 und 3700, in Version 15.0(2)SG auf der Switch-Plattform der Serie 4500 und in Version 12.2(33)SX17 auf der Switch-Plattform der Serie 6500 eingeführt.

- Eine weitere Methode zur Behebung dieses Problems besteht in der Fehlerbehebung durch den Client, um den Grund für die Duplikaterkennung zu ermitteln, die so spät erfolgt, nachdem der Link online ist. Der Switch hat keine Möglichkeit, die Zeit zu bestimmen, zu der dieser Prozess stattfindet. Schätzen Sie daher die Zeit, die für die Testverzögerung festgelegt wurde, um den Konflikt zu verhindern. Um den Grund für die späte Erkennung doppelter Adressen wirksam zu beheben, sind weitere Informationen über das Verhalten der IP-Geräteüberwachungssonde nützlich.

Die ARP-Probe wird unter zwei Umständen gesendet:

Ein Link, der einem aktuellen Eintrag in der IPDT-Datenbank zugeordnet ist, wechselt vom Status DOWN in den Status UP. Ein Link, der sich bereits im UP-Status befindet und einem Eintrag in der IPDT-Datenbank zugeordnet ist, hat ein abgelaufenes Testintervall.

Geben Sie den folgenden Befehl ein, um das Testintervall für die IP-Geräteverfolgung festzulegen:

```
ip device tracking probe interval
```

Das Standardintervall beträgt dreißig Sekunden. Geben Sie den folgenden Befehl ein, um diese Informationen anzuzeigen:

```
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
```

Nachdem der erste Eintrag den Status "DOWN" in "UP" geändert hat, werden keine weiteren Tests gesendet, es sei denn, der Switch erkennt den Datenverkehr von diesem Gerät nicht für das Verzögerungsintervall. Außerdem tritt der Konflikt, wie bereits erwähnt, nur auf, wenn der PC die ARP-Probe wenige Millisekunden vor dem Senden der ARP-Probe durch den Switch sendet (also praktisch gleichzeitig).

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.