

# Solucionar problemas de mensagens de erro de endereço IP duplicado 0.0.0.0

## Contents

[Introduction](#)

[Problema](#)

[Causa de Endereço IP Duplicado](#)

[Solução](#)

## Introduction

Este documento descreve a mensagem de erro Duplicate IP Address 0.0.0.0 recebida pelos usuários do Microsoft Windows Vista e versões posteriores e sua resolução.

## Problema

Com o Microsoft Windows Vista e versões posteriores, a Microsoft introduziu um novo mecanismo usado para detectar endereços duplicados na rede quando o processo DHCP (Dynamic Host Configuration Protocol) ocorre. Esse novo fluxo de detecção é descrito no [RFC 5227](#).

Um dos acionadores desse fluxo de detecção é definido na seção [2.1.1](#):

Além disso, se durante esse período o host receber qualquer Probe ARP (Address Resolution Protocol Protocolo de Resolução de Endereços) em que o "endereço IP de destino" do pacote seja o endereço que está sendo sondado, e o "endereço de hardware do remetente" do pacote não seja o endereço de hardware de nenhuma das interfaces do host, o host DEVERÁ tratar isso da mesma forma como um conflito de endereço e sinalizar um erro para o agente de configuração conforme acima. Isso pode ocorrer se dois (ou mais) hosts tiverem, por algum motivo, sido configurados inadvertidamente com o mesmo endereço e ambos estiverem simultaneamente no processo de sondar esse endereço para ver se ele pode ser usado com segurança.

O Cisco IOS<sup>®</sup> usa a sonda ARP (Address Resolution Protocol) originada de um endereço de 0.0.0.0 para manter o cache de rastreamento de dispositivo IP quando ocorre o rastreamento de dispositivo IP e um recurso que o utiliza é ativado (como 802.1x) em um switch Cisco IOS. A finalidade do rastreamento de dispositivo IP é que o switch obtenha e mantenha uma lista de dispositivos conectados ao switch por um endereço IP. A sonda não preenche a entrada da faixa. É usado para ativar e manter a entrada na tabela depois que ela é aprendida. Esse endereço IP é usado quando uma ACL (Access Control List, Lista de controle de acesso) é aplicada à interface para substituir o endereço origem na ACL pelo endereço IP do cliente. Essa função é crítica quando as listas de acesso são usadas com 802.1x ou qualquer outra função Flex-Auth em switches Cisco.

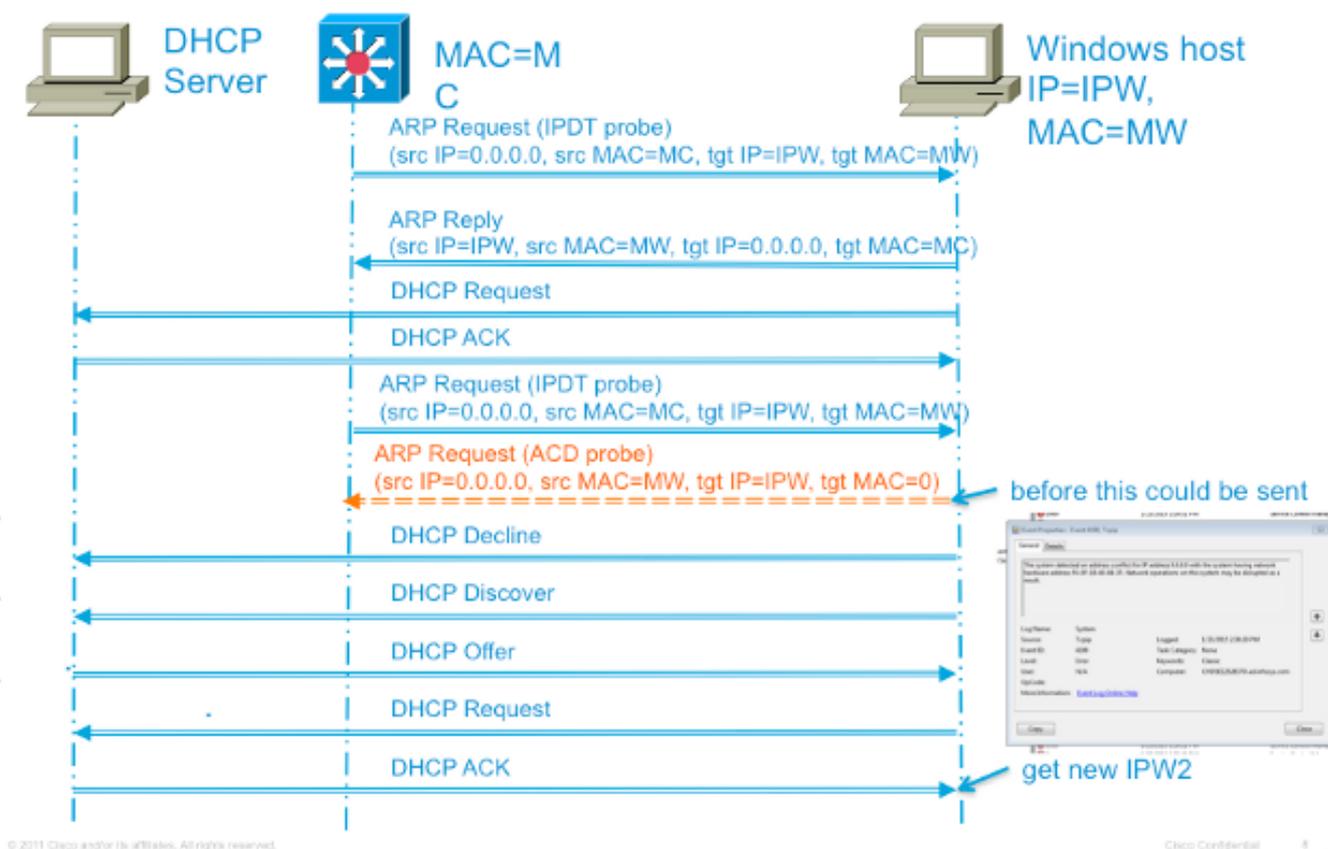
## Causa de Endereço IP Duplicado

Se o switch enviar uma Prova ARP para o cliente enquanto o PC com Microsoft Windows estiver

em sua fase de detecção de endereço duplicado, o Microsoft Windows detectará a prova como um endereço IP duplicado e apresentará uma mensagem de que um endereço IP duplicado foi encontrado na rede para 0.0.0.0. O PC não obtém um endereço IP e o usuário deve liberar/renovar manualmente o endereço, desconectar e reconectar à rede ou reinicializar o PC para obter acesso à rede.

Este é um exemplo da sequência de pacotes com falha:

## Failing Sequence Packet Flow



## Solução

Há vários métodos que podem ser usados para contornar esse problema. Esta é uma lista de possíveis soluções:

- O método mais eficaz usado para evitar esse problema é configurar o switch para que ele envie uma Sonda ARP não compatível com RFC para originar a sonda da Interface Virtual do Switch (SVI) na VLAN onde o PC reside. Se uma SVI for configurada para a Rede local virtual (VLAN) e qualquer um dos dois comandos a seguir for usado, o endereço IP do remetente nos testes IP Device Tracking (IPDT) nunca será 0.0.0.0. Portanto, é certo que o erro de endereço IP duplicado não ocorre.

Este formato de comando é para versões de código mais antigas:

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

No momento, essa configuração não dispara a mensagem de erro de detecção de endereço duplicado no Microsoft Windows. A advertência para esse método é que uma SVI deve existir em cada switch em cada VLAN onde residam clientes Microsoft Windows que executam DHCP. Esse método é difícil de escalar, por isso a Cisco recomenda usar o atraso de sonda de rastreamento de dispositivo IP como o método principal. O SVI não está disponível atualmente na plataforma do switch 6500 Series. Esse comando foi implementado na versão 12.2(55)SE do Cisco IOS nas plataformas de Switch 2900, 3500 e 3700 Series e na versão 15.1(1)SG na plataforma de Switch 4500 Series.

Este formato de comando é para versões de código mais recentes:

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

Este comando mais recente da Interface de Linha de Comando (CLI) foi introduzido através do bug da Cisco ID [CSCtn27420](#) no Cisco IOS versão 15.2(2)E. Ele foi adicionado para permitir um endereço IP de origem de solicitação ARP definido pelo usuário em vez do requisito de usar o endereço IP de origem padrão 0.0.0.0. O novo comando global `ip device tracking probe auto-source fallback 0.0.0.x 255.255.255.0 override` permite que o usuário use o endereço de host 0.0.0.x na sub-rede para evitar problemas de endereço IP duplicado. Se não houver SVI para uma VLAN específica, o host-ip de fallback será usado para originar a sonda.

- A principal alternativa não-SVI usada para contornar o problema é atrasar a sonda do switch para que o Microsoft Windows tenha tempo para concluir a detecção de endereço IP duplicado. Isso só é eficaz em portas de acesso e cenários de link-up. Digite este comando para atrasar a sonda:

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

O RFC especifica uma janela de dez segundos para detecção de endereço duplicado. Se você atrasar a sonda de rastreamento de dispositivo, o problema será resolvido em quase todos os casos. Além do retardo de sonda, o retardo também é redefinido quando o switch detecta uma sonda do PC. Por exemplo, se o temporizador de sondagem for contado para cinco segundos e detectar uma Sondagem ARP do PC, o temporizador será redefinido para dez segundos. Essa janela também poderá ser reduzida ainda mais se você ativar o rastreamento de DHCP, pois isso também redefinirá o temporizador. Em raras circunstâncias, o PC envia uma Sondagem ARP milissegundos antes que o switch envie sua sondagem, o que ainda dispara uma mensagem de endereço duplicada para o usuário final. Esse comando foi introduzido na versão 15.0(1)SE do Cisco IOS nas plataformas de Switch 2900, 3500 e 3700 Series, na versão 15.0(2)SG na plataforma de Switch 4500 Series e na versão 12.2(33)SX17 na plataforma de Switch 6500 Series.

- Outro método usado para resolver esse problema envolve a identificação e solução de problemas do cliente para determinar a razão pela qual a detecção de endereços duplicados ocorre tão tarde depois que o link fica on-line. O switch não tem como determinar o tempo em

que esse processo ocorre, portanto, estime o tempo definido para o atraso do teste para evitar o conflito. Para solucionar com eficiência a razão pela qual a detecção de endereço duplicado ocorre tão tarde, é útil obter mais informações sobre o comportamento da sonda de rastreamento de dispositivo IP.

A prova ARP é enviada sob duas circunstâncias:

Um link associado a uma entrada atual no banco de dados IPDT move-se de um estado INATIVO para um estado ATIVO. Um link que já está no estado UP associado a uma entrada no banco de dados IPDT tem um intervalo de sondagem expirado.

Digite este comando para definir o intervalo de sondagem de rastreamento de dispositivo IP:

```
ip device tracking probe interval
```

O intervalo padrão é de trinta segundos. Para exibir essas informações, digite este comando:

```
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
```

Depois que a entrada inicial passa de um estado DOWN para um estado UP, nenhum outro teste é enviado, a menos que o switch não veja o tráfego desse dispositivo para o intervalo de atraso do teste. Além disso, como dito anteriormente, o conflito só ocorre se o PC enviar a Prova ARP milissegundos antes que o switch envie a Prova ARP (simultaneamente).

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.