

# Contenido

[Introducción](#)

[Problema](#)

[Causa de la dirección IP duplicada](#)

[Solución](#)

## Introducción

Este documento describe un problema que se encuentra cuando un mensaje de error de **0.0.0.0 de la dirección IP duplicada** es recibido por los clientes que funcionan con las versiones de Microsoft Windows Vista y posterior. Los métodos que se utilizan para resolver y resolver problemas el problema también se describen.

## Problema

Con las versiones de Microsoft Windows Vista y posterior, Microsoft introdujo un nuevo mecanismo que se utiliza para detectar a las direcciones duplicadas en la red cuando ocurre el proceso DHCP. Este nuevo flujo de la detección se describe en el [RFC 5227](#).

Uno de los activadores para este flujo de la detección se define en la sección [2.1.1](#):

Además, si durante este período el host recibe cualquier sonda ARP para donde IP Address de destino del paquete están el direccionamiento los “que es sondado, y las direcciones de hardware del remitente del paquete “no son la dirección de hardware de las interfaces del host un de los, después el host DEBE tratar semejantemente esto como conflicto de dirección y señalar un error al agente que configura como arriba. Esto puede ocurrir si dos (o más) host, por la razón que sea, se han configurado inadvertidamente con el mismo direccionamiento, y ambos están simultáneamente en curso de sondear ese direccionamiento para ver si puede ser utilizado con seguridad.

El Cisco IOS<sup>®</sup> utiliza la sonda del Address Resolution Protocol (ARP) que es originada de un direccionamiento de 0.0.0.0 para mantener el caché de dispositivo-seguimiento IP durante el dispositivo IP que sigue, y una característica que utilice se habilita (por ejemplo el 802.1x) en un Switch del Cisco IOS. El propósito del seguimiento del dispositivo IP está para que el Switch obtenga y mantenga una lista de dispositivos que estén conectados con el Switch vía una dirección IP. La sonda no puebla la entrada de seguimiento. Se utiliza para activar y mantener la entrada en la tabla después de que sea docta. Esta dirección IP entonces se utiliza cuando una lista de control de acceso (ACL) se aplica a la interfaz para substituir a la dirección de origen en el ACL con el dirección IP del cliente. Esta función es crítica siempre que las Listas de acceso se utilicen con el 802.1x o cualquier otra función del Flexión-auth en los switches Cisco.

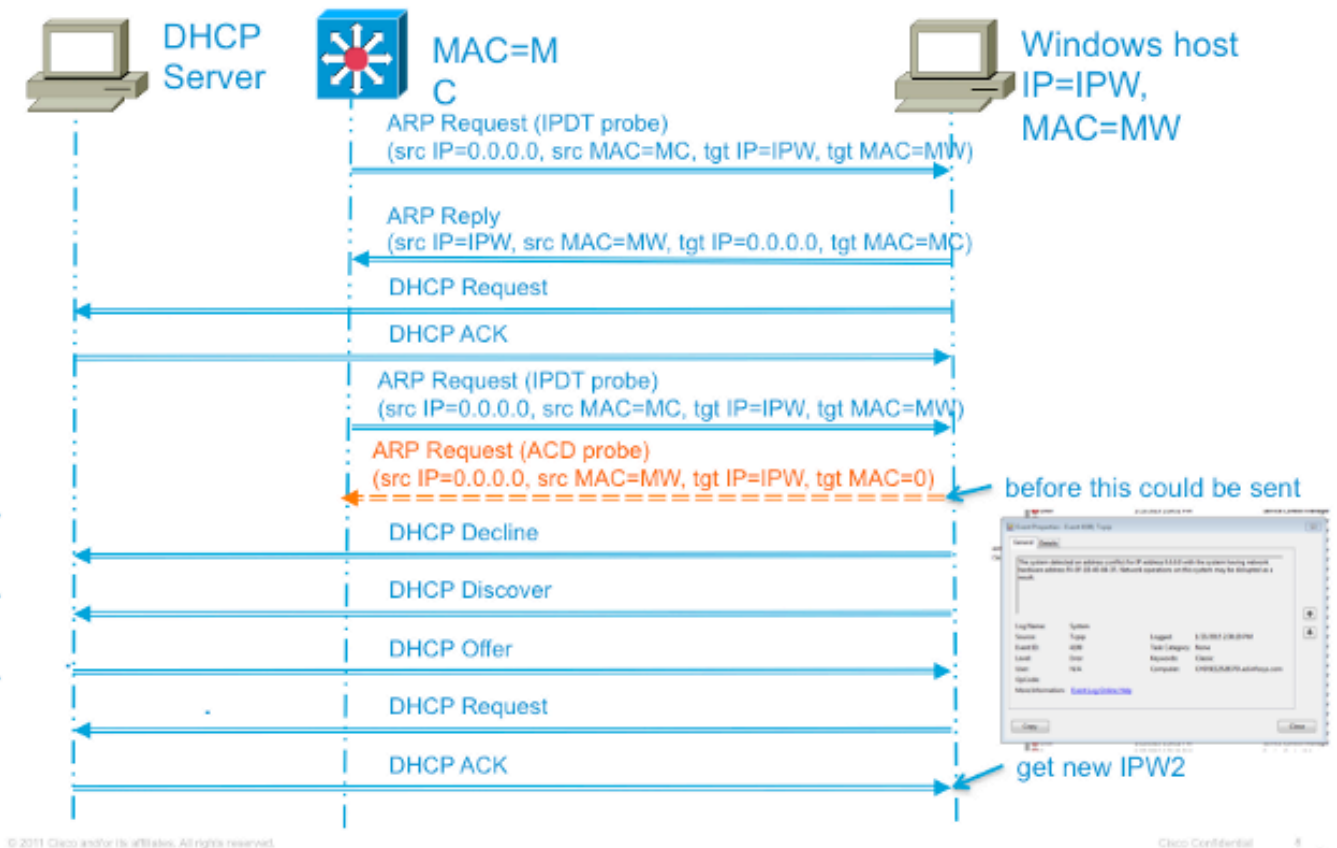
## Causa de la dirección IP duplicada

Si el Switch envía una sonda ARP para el cliente mientras que Microsoft Windows PC es en su fase de la detección de la dirección duplicada, después Microsoft Windows detecta la sonda como dirección IP duplicada y presenta un mensaje que una dirección IP duplicada fue encontrada en la red para 0.0.0.0. El PC no obtiene un direccionamiento, y el usuario debe liberar

manualmente/renueva el direccionamiento, lo desconecta y vuelve a conectar a la red, o reinicia el PC para tener el acceso a la red.

Aquí está un ejemplo de la secuencia fallada del paquete:

## Failing Sequence Packet Flow



## Solución

Hay los métodos múltiples que se utilizan para trabajar alrededor de este problema. Aquí está una lista de soluciones alternativas posibles:

- La mayoría del método eficaz que se utiliza para prevenir este problema es configurar el Switch de modo que envíe un NON-RFC la sonda obediente ARP a la fuente la sonda de la interfaz virtual del Switch (SVI) en el VLA N donde reside el PC. Si un SVI se configura para el VLA N y cualquiera de los dos comandos que siguen se utilizan, después la dirección IP del remitente en las sondas IPDT nunca será 0.0.0.0. Así, es cierto que no ocurrirá el error de dirección IP duplicada.

Aquí está el comando format para más viejas versiones del código:

Esta configuración no acciona actualmente el mensaje de error de la detección de la dirección duplicada en el Microsoft Windows. La advertencia a este método es que un SVI debe existir en cada Switch en cada VLA N donde residen los clientes de Microsoft Windows que ejecutan

el DHCP. Este método es difícil de escalar, así que Cisco recomienda que usted utiliza el retardo de dispositivo-seguimiento de la sonda IP como el método principal. El SVI no está actualmente disponible en la plataforma del 6500 Series Switch. Este comando fue implementado en la versión deL Cisco IOS 12.2(55)SE en 2900, 3500, y las Plataformas del 3700 Series Switch, y en la versión 15.1(1)SG en la plataforma del 4500 Series Switch.

Aquí está el comando format para más nuevas versiones del código:

Presentaron a este último comando CLI con el Id. de bug Cisco [CSCtn27420](#) en la versión deL Cisco IOS 15.2(2)E. Fue agregado para permitir una dirección IP de origen definida por el usuario del pedido ARP en vez del requisito de utilizar la dirección IP de origen predeterminada de 0.0.0.0. El nuevo **dispositivo del IP del comando global que sigue la invalidación del retraso 0.0.0.x 255.255.255.0 de la auto-fuente de la sonda** permite que el usuario utilice a la dirección de host de 0.0.0.x en la subred para evitar cualquier problema de IP Address duplicado. Si no hay SVI para un VLAN determinado el retraso IP del host será utilizado a la fuente la sonda en lugar de otro.

- La alternativa primaria NON-SVI que se utiliza para trabajar alrededor del problema es retrasar la sonda del Switch de modo que Microsoft Windows tenga tiempo para acabar la detección de la dirección IP duplicada. Esto es eficaz solamente en los puertos de acceso y los escenarios de la conexión. Ingrese este comando para retrasar la sonda:

El RFC especifica una diez-segunda ventana para la detección de la dirección duplicada, así que si usted retrasa la sonda de dispositivo-seguimiento, resuelve el problema en casi todos los casos. Además del sonda-retardo, del retardo las restauraciones también cuando el Switch detecta una sonda del PC. Por ejemplo, si el temporizador de la sonda ha contado abajo a cinco segundos y detecta una sonda ARP del PC, las restauraciones del temporizador de nuevo a diez segundos. Esta ventana se puede reducir más a fondo si usted habilita el snooping del DHCP también, como esto reajusta semejantemente el temporizador. En las circunstancias poco probables, el PC envía los milisegundos de una sonda ARP antes de que el Switch envíe su sonda, que todavía acciona un mensaje de la dirección duplicada al usuario final. Este comando fue introducido en la versión deL Cisco IOS 15.0(1)SE en 2900, 3500, y las Plataformas del 3700 Series Switch, versión 15.0(2)SG en la plataforma del 4500 Series Switch, y versión 12.2(33)SX17 en la plataforma del 6500 Series Switch.

- Otro método que se utiliza para resolver este problema implica un Troubleshooting del cliente para determinar la razón que ocurre la detección de la dirección duplicada tan tarde después de que venga el link en línea. El Switch no tiene ninguna manera de determinar el tiempo que ocurre este proceso, así que usted debe estimar la hora que se fija para el retardo de la sonda para prevenir el conflicto. Para resolver problemas con eficacia la razón que ocurre la detección de la dirección duplicada tan tarde, la Más información en el comportamiento de la sonda de dispositivo-seguimiento IP es útil.

La sonda ARP se envía bajo dos circunstancias:

Un link que se asocia a una entrada actual en la base de datos IPDT se mueve desde un PLUMÓN a un estado ASCENDENTE. Un link ya en el estado ASCENDENTE que se asocia a

una entrada en la base de datos IPDT tiene un intervalo expirado de la sonda.

Ingrese este comando para fijar el intervalo de dispositivo-seguimiento de la sonda IP:

El intervalo predeterminado es treinta segundos. Para ver esta información, ingrese este comando:

Después de que la entrada inicial se mueva desde un PLUMÓN a un estado ASCENDENTE, no se envía ningunas otras sondas a menos que el Switch no considere el tráfico de ese dispositivo para el intervalo del sonda-retardo. También, según lo expuesto anterior, el conflicto ocurre solamente si el PC envía los milisegundos de la sonda ARP antes de que el Switch envíe la sonda ARP (simultáneamente).

- El método final que es para solución alternativa usada el problema que se describe en este documento es inhabilitar la detección de la dirección duplicada en el client cara. Este procedimiento se describe en [cómo inhabilitar el](#) artículo de la base de apoyo de Microsoft de la [función del ARP gratuito](#). Centralmente despliegue este cambio para hacer esta opción más scalable.