Troubleshooting de Mensajes de Error de Dirección IP Duplicada 0.0.0.0

Contenido

Introducción

Este documento describe el mensaje de error Duplicate IP Address 0.0.0.0 recibido por los usuarios de Microsoft Windows Vista y versiones posteriores y su resolución.

Problema

Con Microsoft Windows Vista y versiones posteriores, Microsoft introdujo un nuevo mecanismo que se utiliza para detectar direcciones duplicadas en la red cuando se produce el proceso de protocolo de configuración dinámica de host (DHCP). Este nuevo flujo de detección se describe en RFC 5227.

Uno de los desencadenadores de este flujo de detección se define en la sección 2.1.1:

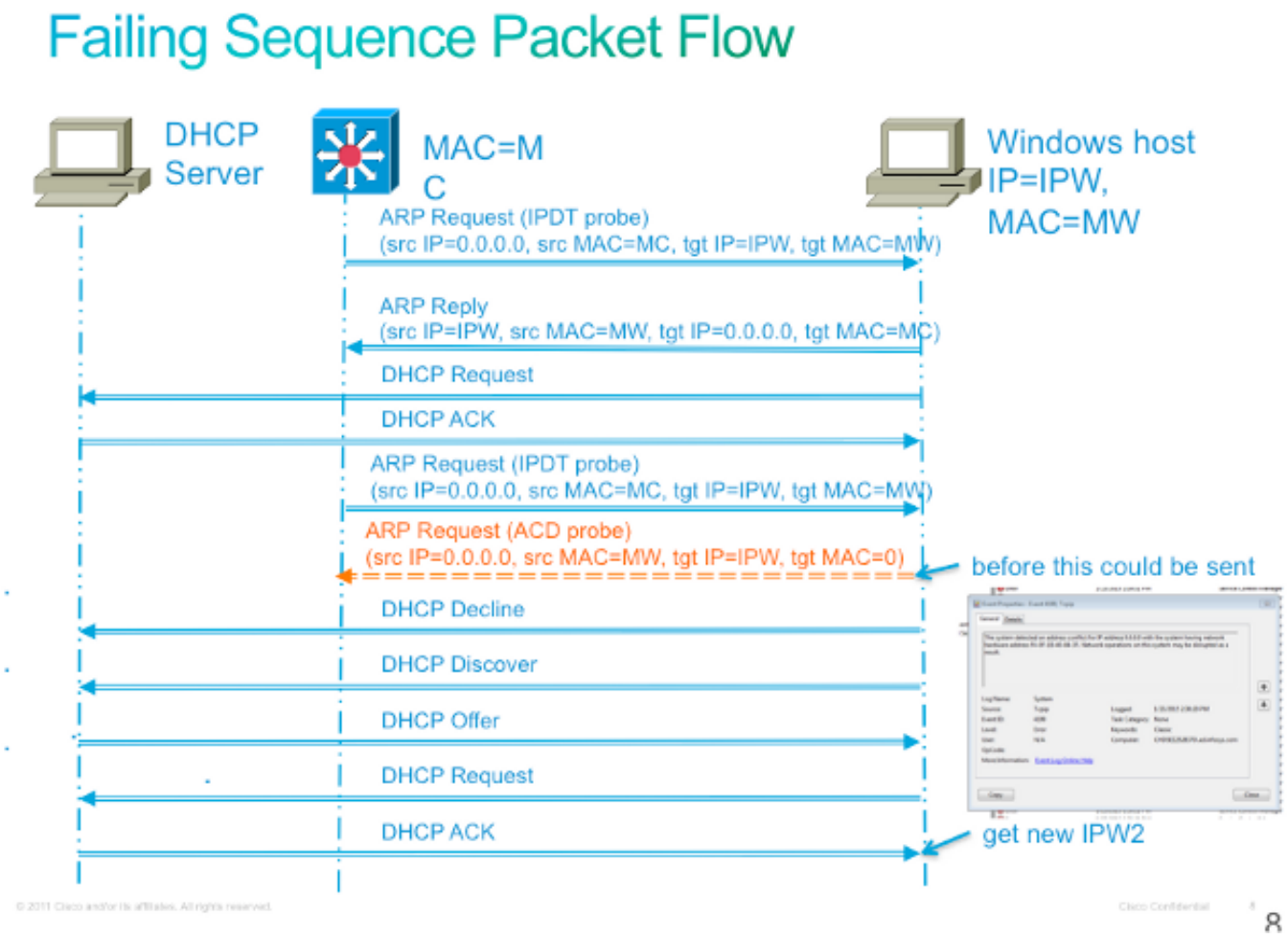
Además, si durante este período el host recibe cualquier sonda de protocolo de resolución de direcciones (ARP) donde la 'dirección IP de destino' del paquete es la dirección que se está sondeando, y la 'dirección de hardware del remitente' del paquete no es la dirección de hardware de ninguna de las interfaces del host, el host DEBE tratar de manera similar esto como un conflicto de direcciones y señalar un error al agente de configuración como se indicó anteriormente. Esto puede ocurrir si dos (o más) hosts han sido configurados inadvertidamente con la misma dirección, por cualquier razón, y ambos están simultáneamente en el proceso de sondear esa dirección para ver si se puede utilizar de manera segura.

Cisco IOS® utiliza la sonda de protocolo de resolución de direcciones (ARP, Address Resolution Protocol) originada en una dirección 0.0.0.0 para mantener la caché de seguimiento de dispositivos IP cuando se realiza el seguimiento de dispositivos IP, y una función que la utiliza está habilitada (como 802.1x) en un switch Cisco IOS. El propósito de la pista de dispositivos IP es que el switch obtenga y mantenga una lista de dispositivos conectados al switch por una dirección IP. El sondeo no rellena la entrada de pista. Se utiliza para activar y mantener la entrada en la tabla después de aprenderla. Esta dirección IP se utiliza cuando se aplica una lista de control de acceso (ACL) a la interfaz para sustituir la dirección de origen en la ACL por la dirección IP del cliente. Esta función es fundamental cuando se utilizan listas de acceso con 802.1x o cualquier otra función Flex-Auth en switches Cisco.

Causa de dirección IP duplicada

Si el switch envía una sonda ARP para el cliente mientras el equipo con Microsoft Windows está en su fase de detección de direcciones duplicadas, Microsoft Windows detecta la sonda como una dirección IP duplicada y presenta un mensaje que indica que se encontró una dirección IP duplicada en la red para 0.0.0.0. El equipo no obtiene una dirección IP y el usuario debe liberar/renovar manualmente la dirección, desconectarse y volver a conectarse a la red, o reiniciar el equipo para obtener acceso a la red.

Este es un ejemplo de la secuencia de paquetes fallida:



Solución

Existen varios métodos que se pueden utilizar para solucionar este problema. Esta es una lista de posibles soluciones alternativas:

- El método más efectivo utilizado para evitar este problema es configurar el switch para que envíe una sonda ARP no compatible con RFC para obtener la sonda de la interfaz virtual del switch (SVI) en la VLAN donde reside la PC. Si se configura una SVI para la red de área local virtual (VLAN) y se utiliza cualquiera de los dos comandos siguientes, la dirección IP del remitente en los sondeos de seguimiento de dispositivos IP (IPDT) nunca es 0.0.0.0. Por lo tanto, es seguro que no se produzca el error de dirección IP duplicada.

  Este formato de comando es para versiones de código anteriores:

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

Esta configuración actualmente no activa el mensaje de error de detección de dirección duplicada en Microsoft Windows. La advertencia a este método es que debe existir una SVI en cada switch en cada VLAN donde residen los clientes de Microsoft Windows que ejecutan DHCP. Este método es difícil de escalar, por lo que Cisco recomienda utilizar la demora de la sonda de seguimiento de dispositivos IP como método principal. SVI no está disponible actualmente en la plataforma de switches de la serie 6500. Este comando se implementó en Cisco IOS Version 12.2(55)SE en las plataformas de switches de las series 2900, 3500 y 3700, y en la versión 15.1(1)SG en la plataforma de switches de la serie 4500.

Este formato de comando es para versiones de código más recientes:

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

Este último comando de la interfaz de línea de comandos (CLI) se introdujo a través del ID de error de Cisco CSCtn27420 en la versión 15.2(2)E del IOS de Cisco. Se agregó para permitir una dirección IP de origen de solicitud ARP definida por el usuario en lugar del requisito de utilizar la dirección IP de origen predeterminada 0.0.0.0. El nuevo comando global ip device tracking probe auto-source fallback 0.0.0.x 255.255.255.0 override permite al usuario utilizar la dirección de host 0.0.0.x en la subred para evitar cualquier problema de dirección IP duplicada. Si no hay SVI para una VLAN determinada, se utiliza el host-ip de reserva para originar la sonda en su lugar.

- La principal alternativa no SVI utilizada para solucionar el problema es retrasar la sonda del switch para que Microsoft Windows tenga tiempo de finalizar la detección de direcciones IP duplicadas. Esto es efectivo sólo en los puertos de acceso y escenarios de link-up. Ingrese este comando para retrasar la sonda:

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

El RFC especifica una ventana de diez segundos para la detección de direcciones duplicadas. Si retrasa la sonda de seguimiento de dispositivos, se resuelve el problema en casi todos los casos. Además de la demora de sondeo, la demora también se restablece cuando el switch detecta una sonda del PC. Por ejemplo, si el temporizador de la sonda ha contado hasta cinco segundos y detecta una sonda ARP desde el PC, el temporizador se restablece a diez segundos. Esta ventana se puede reducir aún más si habilita la sonda DHCP también, ya que esto igualmente restablece el temporizador. En circunstancias excepcionales, el PC envía una sonda ARP milisegundos antes de que el switch envíe su sonda, lo que todavía dispara un mensaje de dirección duplicado al usuario final. Este comando se introdujo en Cisco IOS Version 15.0(1)SE en las plataformas de switches de las series 2900, 3500 y 3700, Version 15.0(2)SG en la plataforma de switches de la serie 4500 y Version 12.2(33)SXI7 en la plataforma de switches de la serie 6500.

- Otro método utilizado para resolver este problema implica un troubleshooting del cliente para

determinar la razón por la que la detección de direcciones duplicadas ocurre tan tarde después de que el link se conecta. El switch no tiene forma de determinar la hora a la que ocurre este proceso, por lo que debe estimar el tiempo establecido para el retraso de la sonda para evitar el conflicto. Para resolver eficazmente el motivo por el cual la detección de direcciones duplicadas ocurre tan tarde, es útil obtener más información sobre el comportamiento de la sonda de seguimiento de dispositivos IP.

La sonda ARP se envía en dos circunstancias:

Un vínculo asociado a una entrada actual de la base de datos IPDT pasa de un estado DOWN a un estado UP.Un enlace que ya se encuentra en el estado ACTIVO asociado a una entrada de la base de datos IPDT tiene un intervalo de sondeo caducado.

Ingrese este comando para establecer el intervalo de sondeo de seguimiento de dispositivos IP:

```
ip device tracking probe interval
```

El intervalo predeterminado es de treinta segundos. Para ver esta información, ingrese 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
```

Después de que la entrada inicial pasa de un estado DOWN a un estado UP, no se envían más sondeos, a menos que el switch no vea el tráfico de ese dispositivo para el intervalo de demora de sondeo. Además, como se indicó anteriormente, el conflicto solo ocurre si la PC envía la sonda ARP milisegundos antes de que el switch envíe la sonda ARP (simultáneamente).

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).