Verificar operaciones del dispositivo IPDT

Contenido

Introducción

Este documento describe cómo verificar las operaciones de IP Device Tracking (IPDT) y cómo inhabilitar estas acciones.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Los resultados de este documento se basaron en estas versiones de software y hardware:

- Cisco WS-C2960X
- Cisco IOS® 15.2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Descripción general de IPDT

Definición y uso

La tarea principal de IPDT es realizar un seguimiento de los hosts conectados (asociación de direcciones MAC e IP). Para ello, envía sondeos de protocolo de resolución de direcciones (ARP) de unidifusión con un intervalo predeterminado de 30 segundos. Estos sondeos se envían a la dirección MAC del host conectado en el otro lado del link, y utilizan la Capa 2 (L2) como el origen predeterminado a la cual se dirige la dirección MAC de la interfaz física de la cual sale el ARP y una dirección IP del remitente de 0.0.0.0, basada en la definición de sonda ARP enumerada en RFC 5227

Extracto

En este documento, el término ARP Probe se utiliza para referirse a un paquete de Solicitud ARP, difundido en el link local, con una dirección IP de remitente completamente nula. La dirección de hardware del remitente DEBE contener la dirección de hardware de la interfaz que envía el paquete. El campo de dirección IP del remitente DEBE configurarse en todos los ceros para evitar la corrupción de las memorias caché ARP en otros hosts, en el mismo link, en el caso en que la dirección resulte estar ya en uso por otro host. El campo de dirección IP de destino DEBE establecerse en la dirección que se sondea. Una sonda ARP transmite una pregunta (¿alguien utiliza esta dirección?) y una instrucción implícita (ésta es la dirección que espero utilizar).

El propósito de IPDT es que el switch obtenga y mantenga una lista de dispositivos que están conectados al switch a través de una dirección IP. El sondeo no rellena la entrada de seguimiento; simplemente se utiliza para mantener la entrada en la tabla después de que se aprende a través de una solicitud/respuesta ARP del host.

La inspección ARP IP se activa automáticamente cuando se activa IPDT. Detecta la presencia de nuevos hosts cuando monitorea paquetes ARP. Si se habilita la inspección ARP dinámica, sólo se utilizan los paquetes ARP que valida para detectar nuevos hosts para la tabla de rastreo de dispositivos.

El snooping DHCP IP, si está activado, detecta la presencia o eliminación de nuevos hosts cuando DHCP asigna o revoca sus direcciones IP. Cuando se observa tráfico DHCP para un host determinado, se reinicia el temporizador del intervalo de sondeo ARP IPDT.

IPDT es una función que siempre ha estado disponible. Sin embargo, en las versiones más recientes de Cisco IOS®, sus interdependencias están habilitadas de forma predeterminada

(consulte el Id. de error de Cisco CSCuj04986). Puede ser extremadamente útil cuando se utiliza su base de datos de asociaciones de hosts IP/MAC para rellenar la IP de origen de las listas de control de acceso (ACL) dinámicas, o para mantener un enlace de una dirección IP a una etiqueta de grupo de seguridad.

La sonda ARP se envía en dos circunstancias:

- El link asociado con una entrada actual en la base de datos IPDT pasa de un estado DOWN a un estado UP, y la entrada ARP se ha llenado.
- Un link que ya se encuentra en el estado ACTIVO y que está asociado a una entrada de la base de datos IPDT tiene un intervalo de sondeo caducado.

Problema

La sonda de señal de mantenimiento enviada por el switch es una verificación L2. Como tal, desde el punto de vista del switch, las direcciones IP utilizadas como fuente en los ARP no son importantes: esta función se puede utilizar en dispositivos sin ninguna dirección IP configurada, por lo que la fuente IP de 0.0.0.0 no es relevante.

Cuando el host recibe estos mensajes, responde y rellena el campo IP de destino con la única dirección IP disponible en el paquete recibido, que es su propia dirección IP. Esto puede causar falsas alertas de direcciones IP duplicadas, porque el host que responde ve su propia dirección IP como el origen y el destino del paquete; consulte la Dirección IP Duplicada 0.0.0.0. Artículo de Troubleshooting de Mensaje de Error para obtener más información sobre el escenario de dirección IP duplicada.

Estado y funcionamiento predeterminados

La configuración global on/off para IPDT es un comportamiento heredado que causó problemas en el campo ya que los clientes no siempre eran conscientes de que necesitaban activar IPDT para que ciertas funciones funcionaran. En las versiones actuales, IPDT se controla únicamente a nivel de interfaz cuando habilita una función que requiere IPDT.

IPDT está activado globalmente de forma predeterminada en estas versiones; es decir, no hay un comando de configuración global:

- Catalyst 2000/3000: 15.2(1)E
- Catalyst 3850: 3.2.0SE
- Catalyst 4k: 15.2(1)E / 3.5.0E

Es importante tener en cuenta que, incluso si IPDT está habilitado globalmente, eso no implica necesariamente que IPDT monitoree activamente un puerto dado.

En las versiones en las que IPDT está siempre activado y en las que IPDT se puede activar/desactivar globalmente cuando IPDT está activado globalmente, otras funciones determinan en realidad si está activo en una interfaz específica (consulte la sección Áreas de Funcionalidad).

Áreas de funcionalidad

IPDT y sus sondas ARP enviadas desde una interfaz dada se utilizan para estas funciones:

- Protocolo de servicios de movilidad de red (NMSP), versiones 3.2.0E, 15.2(1)E, 3.5.0E y posteriores
- Sensor de dispositivos, versiones 15.2(1)E, 3.5.0E y posteriores
- 1X, MAC Authentication Bypass (MAB), administrador de sesiones
- Autenticación basada en Web
- Auth-proxy
- IP Source Guard (IPSG) para hosts estáticos
- Flexible NetFlow
- Cisco TrustSec (CTS)
- Seguimiento de medios
- Redireccionamiento HTTP

Matriz de características

Platform	Función	Valor predeterminado activado (Iniciar en)	Método Disable	Desactivar CLI
Cat 2960/3750 (Cisco IOS)	IPDT	15.2(1)E *	CLI global (versiones anteriores) * por interfaz	no ip device tracking * ip device tracking maximum 0 ***
Cat 2960/3750 (Cisco IOS)	NMSP	no	CLI global o CLI por interfaz	no nmsp enable nmsp attachment suppress ****
Cat 2960/3750 (Cisco IOS)	Sensor de dispositivos	15.0(1)SE	CLI global	no macro auto monitor
Cat 2960/3750 (Cisco IOS)	Detección ARP	15.2(1)E **	n/a	n/a
CAT 3850	IPDT	todas las versiones *	por interfaz *	ip device tracking maximum 0 ***

CAT 3850	NMSP	todas las versiones	por interfaz	nmsp attachment suppress
CAT 3850	Sensor de dispositivos	no	n/a	n/a
CAT 3850	Detección ARP	todas las versiones **	n/a	n/a
CAT 4500	IPDT	15.2(1)E / 3.5.0E *	CLI global (versiones anteriores) * por interfaz	no ip device tracking * ip device tracking maximum 0 ***
CAT 4500	NMSP	no	CLI global o CLI por interfaz	no nmsp enable nmsp attachment suppress ****
CAT 4500	Sensor de dispositivos	15.1(1)SG / 3.3.0SG	CLI global	no macro auto monitor
CAT 4500	Detección ARP	15.2(1)E / 3.5.0E **	n/a	n/a

Funciones

- IPDT no se puede inhabilitar globalmente en las versiones más recientes, pero IPDT sólo está activo en los puertos, si las funciones que lo requieren están activas.
- La indagación ARP solo está activa si las combinaciones de funciones específicas la habilitan.
- Si inhabilita IPDT por interfaz, no detiene la indagación ARP, evita el seguimiento IPDT. Está disponible en i3.3.0SE, 15.2(1)E, 3.5.0E y versiones posteriores.
- La supresión de NMSP por interfaz sólo está disponible si NMSP está habilitado globalmente.

Desactivar IPDT

En las versiones en las que IPDT no está habilitado de forma predeterminada, IPDT se puede

desactivar globalmente con este comando:

<#root>

```
Switch(config)#
```

no ip device tracking

En las versiones en las que IPDT está siempre activado, el comando anterior no está disponible o no le permite inhabilitar IPDT (Id. de error de Cisco CSCuj04986). En este caso, hay varias maneras de asegurarse de que IPDT no monitoree un puerto específico o no genere alertas IP duplicadas.

Introduzca el comando IP Device Tracking Probe Delay 10

Este comando no permite que un switch envíe una sonda durante 10 segundos cuando detecta un link UP/flap, lo que minimiza la posibilidad de que se envíe la sonda mientras el host del otro lado del link verifica si hay direcciones IP duplicadas. El RFC especifica una ventana de 10 segundos para la detección de direcciones duplicadas, por lo que si retrasa la sonda de seguimiento de dispositivos, el problema se puede resolver en la mayoría de los casos.

Si el switch envía una sonda ARP para el cliente mientras el host (por ejemplo, una PC con Microsoft Windows) está en su fase de detección de dirección duplicada, el host detecta la sonda como una dirección IP duplicada y presenta al usuario un mensaje indicando que se ha encontrado una dirección IP duplicada en la red. Si el PC no obtiene una dirección, y el usuario debe liberar/renovar manualmente la dirección, desconectar y volver a conectar a la red, o reiniciar el PC para obtener acceso a la red.

Además de la demora de sondeo, la demora también se restablece cuando el switch detecta una sonda del PC/host. Por ejemplo, si el temporizador de la sonda ha contado hasta cinco segundos y detecta una sonda ARP del PC/host, el temporizador se restablece nuevamente a 10 segundos.

Esta configuración se ha hecho disponible a través del ID de bug Cisco CSCtn27420.

Introduzca el comando IP Device Tracking Probe Use SVI

Con este comando, puede configurar el switch para enviar una sonda ARP no compatible con RFC; el origen IP no es 0.0.0.0, sino que es la interfaz virtual del switch (SVI) en la VLAN donde reside el host. Las máquinas con Microsoft Windows ya no ven la sonda como una sonda tal como se define en RFC 5227 y no marcan una IP duplicada potencial.

Introduzca el comando IP Device Tracking Probe Auto-Source [fallback <host-ip> <mask>] [override]

Para los clientes que no tienen dispositivos finales predecibles/controlables, o para aquellos que tienen muchos switches con una función solo de L2, la configuración de una SVI, que introduce

una variable de capa 3 en el diseño, no es una solución adecuada. Una mejora introducida en la versión 15.2(2)E y posteriores, la posibilidad de permitir la asignación arbitraria de una dirección IP que no necesita pertenecer al switch para su uso como dirección de origen en sondas ARP generadas por IPDT. Esta mejora introduce la posibilidad de modificar el comportamiento automático del sistema de las siguientes maneras (esta lista muestra cómo se comporta automáticamente el sistema después de utilizar cada comando):

Ingrese el comando IP Device Tracking Probe Auto-Source

1. Establezca el origen en VLAN SVI, si está presente.
2. Busque un par de origen/MAC en la tabla de host IP para la misma subred.
3. Envíe el origen de IP cero como en el caso predeterminado.

Introduzca el comando IP Device Tracking Probe Auto-Source Fallback 0.0.0.1 255.255.255.0

1. Establezca el origen en VLAN SVI, si está presente.
2. Busque un par de origen/MAC en la tabla de host IP para la misma subred.
3. Calcule la IP de origen desde la IP de destino con el bit de host y la máscara proporcionados.

Ingrese el comando IP Device Tracking Probe Auto-Source Fallback 0.0.0.1 255.255.255.0 Override

1. Establezca el origen en VLAN SVI, si está presente.
2. Calcule la IP de origen desde la IP de destino con el bit de host y la máscara proporcionados.

Nota: Una sustitución hace que se omita la búsqueda de una entrada en la tabla.

Como ejemplo de los cálculos anteriores, suponga que sondea el host 192.168.1.200. Con la máscara y los bits de host proporcionados, se genera una dirección de origen de 192.168.1.1. Si usted sondea la entrada 10.5.5.20, puede generar una sonda ARP con la dirección de origen 10.5.5.1, y así sucesivamente.

Introduzca el comando IP Device Tracking Maximum 0

Este comando realmente no inhabilita IPDT, pero limita el número de hosts rastreados a cero. Esta no es una solución recomendada, y debe usarse con precaución porque afecta a todas las otras funciones que dependen de IPDT, que incluye la configuración de canales de puerto como

se describe en el Id. de bug Cisco CSCun81556.

Desactivar las funciones activas que activan IPDT

Algunas características que pueden activar IPDT incluyen NMSP, sensor de dispositivos, dot1x/MAB, WebAuth e IPSG. No se recomienda habilitar estas características en los puertos troncales. Esta solución se reserva para las situaciones más difíciles o complejas, en las que todas las soluciones disponibles anteriormente no funcionaban como se esperaba o creaban problemas adicionales. Sin embargo, esta es la única solución que permite una granularidad extrema al deshabilitar IPDT, ya que sólo puede desactivar las características relacionadas con IPDT que causan problemas y dejar todo lo demás intacto.

En la versión más reciente de Cisco IOS, Versions 15.2(2)E y posteriores, verá un resultado similar al siguiente:

<#root>

```
Switch#

show ip device tracking interface GigabitEthernet 1/0/9


-------------------------------------------
Interface GigabitEthernet1/0/9 is: STAND ALONE
IP Device Tracking = Disabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 180000
IPv6 Device Tracking Client Registered Handle: 75
IP Device Tracking Enabled Features:
       HOST_TRACK_CLIENT_ATTACHMENT
       HOST_TRACK_CLIENT_SM
```

Las dos líneas en mayúsculas en la parte inferior de la salida son las que utilizan IPDT para funcionar. La mayoría de los problemas creados al deshabilitar el seguimiento de dispositivos se pueden evitar si deshabilita los servicios individuales que se ejecutan en la interfaz.

En versiones anteriores de Cisco IOS, esta forma fácil de saber qué módulos están habilitados bajo una interfaz aún no está disponible, por lo que debe pasar por un proceso más involucrado para obtener los mismos resultados. Debe activar debug ip device track interface, que es un registro de baja frecuencia que debe ser seguro en la mayoría de las configuraciones. Tenga cuidado de no activar debug ip device tracking all porque esto, por el contrario, inunda la consola en situaciones de escala.

Una vez activada la depuración, vuelva a establecer una interfaz predeterminada y, a continuación, agregue y quite un servicio IPDT de la configuración de la interfaz. Los resultados de las depuraciones indican qué servicio se ha habilitado o deshabilitado con el comando que ha utilizado.

Ejemplo:

<#root>

```
Switch(config)#
```

interface GigabitEthernet 1/0/9

```
Switch(config-if)#
```

ip device tracking maximum 10

```
Switch(config-if)#
*Mar 27 09:58:49.470: sw_host_track-interface:Feature 00000008 enabled on port
Gi1/0/9, mask now 0000004C, 65 ports enabled
*Mar 27 09:58:49.471: sw_host_track-interface:Gi1/0/9[L2 DOWN, IPHOST DIS]IP
host tracking max set to 10
Switch(config-if)#
```

Lo que la salida revela es que usted habilitó la función 00000008, y que la nueva máscara de función es 0000004C.

Ahora, elimine la configuración que acaba de agregar:

<#root>

```
Switch(config-if)#
```

no ip device tracking maximum 10

```
Switch(config-if)#
*Mar 27 10:02:31.154: sw_host_track-interface:Feature 00000008 disabled on port
Gi1/0/9, mask now 00000044, 65 ports enabled
*Mar 27 10:02:31.154: sw_host_track-interface:Gi1/0/9[L2 DOWN, IPHOST DIS]IP
host tracking max cleared
*Mar 27 10:02:31.154: sw_host_track-interface:Max limit has been removed from
the interface GigabitEthernet1/0/9.
Switch(config-if)#
```

Una vez quitada la función 00000008, puede ver la máscara 00000044, que debe haber sido la máscara original predeterminada. Se espera este valor de 00000044 ya que AIM es 0x00000004 y SM es 0x00000040, lo que en conjunto resulta en 0x00000044.

Hay varios servicios IPDT que se pueden ejecutar bajo una interfaz:

Servicio IPT	Interfaz
HOST_TRACK_CLIENT_IP_ADMISSIONS	= 0x00000001

HOST_TRACK_CLIENT_DOT1X	= 0x00000002
HOST_TRACK_CLIENT_ATTACHMENT	= 0x00000004
HOST_TRACK_CLIENT_TRACK_HOST_UPTO_MAX	= 0x00000008
HOST_TRACK_CLIENT_RSVP	= 0x00000010
HOST_TRACK_CLIENT_CTS	= 0x00000020
HOST_TRACK_CLIENT_SM	= 0x00000040
HOST_TRACK_CLIENT_WIRELESS	= 0x00000080

En el ejemplo, los módulos HOST_TRACK_CLIENT_SM (SESSION-MANAGER) y HOST_TRACK_CLIENT_ATTACHMENT (también conocido como AIM/NMSP) se configuran para IPDT. Para desactivar IPDT en esta interfaz, debe desactivar ambos, ya que IPDT está desactivado SOLO cuando todas las funciones que lo utilizan también están desactivadas.

Después de desactivar estas funciones, tendrá una salida similar a la siguiente:

<#root>

```
Switch(config-if)#
```

do show ip device tracking interface GigabitEthernet 1/0/9

```
-----------------------------------------
Interface GigabitEthernet1/0/9 is: STAND ALONE
IP Device Tracking = Disabled     ß IPDT is disabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 180000
IP Device Tracking Enabled Features:
ß No active features
-----------------------------------------
```

De esta manera, IPDT se inhabilita con más granularidad.

A continuación se muestra un ejemplo de comandos utilizados para inhabilitar algunas de las funciones mencionadas anteriormente:

- nmsp attach suppress
- no macro auto monitor

Nota: la función más reciente debe estar disponible sólo en plataformas compatibles con puertos inteligentes, que se utilizan para habilitar funciones basadas en la ubicación de un switch en la red y para implementaciones de configuración masiva en toda la red.

Verifique el funcionamiento de IPDT

Utilice estos comandos para verificar el estado de IPDT en su dispositivo:

- show ip device tracking
  Este comando muestra las interfaces en las que IPDT está habilitado y en las que se realiza un seguimiento de las asociaciones de interfaz/IP/MAC actualmente.
- clear ip device tracking
- Este comando borra las entradas relacionadas con IPDT.

Nota: El switch envía sondas ARP a los hosts que se eliminaron. Si un host está presente, responde a la sonda ARP y el switch agrega una entrada IPDT para el host. Debe inhabilitar los sondeos ARP antes del comando clear IPDT; de esa manera, todas las entradas ARP han desaparecido. Si se habilitan los sondeos ARP después del comando clear ip device tracking, todas las entradas regresan nuevamente.

- debug ip device tracking
  Este comando le permite recopilar depuraciones para mostrar la actividad IPDT en tiempo real.

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).