Descripción de seguimiento del dispositivo IP (IPDT)

Contenido

Introducción

El documento describe el dispositivo IP que sigue (IPDT) y cómo inhabilitarlo y verificar su operación.

Descripción IPDT

Definición y uso

La tarea principal IPDT es no perder de vista los host conectados (asociación del MAC y de la dirección IP). Para hacer esto, envía las sondas del Address Resolution Protocol (ARP) del unicast con un intervalo predeterminado de 30 segundos; estas sondas se envían a la dirección MAC del host conectado en el otro lado del link, y de la capa 2 (L2) del uso como la fuente predeterminada la dirección MAC de la interfaz física de la cual el ARP va y una dirección IP del remitente de 0.0.0.0, sobre la base de la definición de la sonda ARP enumerada en el RFC 5227

extractado aquí:

En este documento, la “sonda ARP” del término se utiliza para referir a un paquete de pedido de ARP, broadcast en el link local, con las todas-cero “direcciones IP del remitente. La NECESIDAD “de las direcciones de hardware del remitente contiene a la dirección de hardware de la interfaz que envía el paquete. El campo “de las direcciones IP del remitente SE DEBE fijar a todos los ceros, para evitar contaminar memorias caché ARP en otros host en el mismo link en el caso donde el direccionamiento resulta ser ya funcionando por otro host. El “campo de IP Address de destino SE DEBE fijar al direccionamiento que es sondado. ¿Una sonda ARP transporta una pregunta (“cualquier persona está utilizando este direccionamiento? ") y una declaración implicada (“ésta es la esperanza del direccionamiento I a use.").

El propósito de IPDT 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 simplemente para mantener la entrada en la tabla después de que sea docta con un pedido ARP/una contestación del host.

La inspección ARP IP se habilita automáticamente cuando se habilita IPDT; detecta la presencia de nuevos host cuando monitorea los paquetes ARP. Si se habilita la inspección ARP dinámica, sólo los paquetes ARP que valida se utilizan para detectar los nuevos host para el dispositivo que sigue la tabla.

El snooping IP DHCP, si está habilitado, detecta la presencia o el retiro de los nuevos host cuando el DHCP asigna o revoca sus IP Addresses.

IPDT es una característica que ha estado siempre disponible. Sin embargo, en versiones más recientes del ® del Cisco IOS, sus interdependencias se habilitan por abandono (véase el Id. de bug Cisco CSCuj04986). Puede ser extremadamente útil cuando su base de datos de las asociaciones de los host IP/MAC se utiliza para poblar el IP de la fuente de las listas de control de acceso dinámico (ACL), o mantener un atascamiento de una dirección IP a una etiqueta del grupo de seguridad.

La sonda ARP se envía bajo dos circunstancias:

- El link asociado a una entrada actual en la base de datos IPDT se mueve desde un PLUMÓN a un estado ASCENDENTE, y se ha poblado la entrada ARP.

- 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.

Problema conocido

La sonda del “keepalive” enviada por el Switch es un control L2. Como tal desde el punto de vista del Switch, los IP Addresses usados como fuente en los ARP no son importantes: esta característica se puede utilizar en los dispositivos sin la dirección IP configurada en absoluto, así que el IP de origen de 0.0.0.0 no es relevante.

Cuando el host recibe este los mensajes, contesta detrás y puebla el campo del IP de destino con la única dirección IP disponible en el paquete recibido, que es su propia dirección IP. Esto puede causar las alertas falsas de la dirección IP duplicada, porque el host que contesta considera su propia dirección IP como la fuente y el destino del paquete; refiera a la dirección IP duplicada 0.0.0.0. Artículo del Troubleshooting del mensaje de error para más información sobre el

escenario de la dirección IP duplicada.

Estado predeterminado y operación

Es importante observar que, incluso si IPDT se habilita global, ése no implica necesariamente que IPDT monitorea activamente un puerto dado. En las versiones donde está IPDT siempre encendido y donde IPDT puede ser off/on global conectado, cuando IPDT se habilita global, las otras funciones determinan realmente si es activo en una interfaz específica (véase la sección de las áreas de las funciones).

Áreas de las funciones

IPDT y sus sondas ARP enviados de una interfaz dada se utilizan para estas características:

- Protocolo de los Servicios de movilidad de la red (NMSP), versiones 3.2.0E, 15.2(1)E, 3.5.0E y posterior
- Sensor del dispositivo, versiones 15.2(1)E, 3.5.0E y posterior
- 1X, puente de la autenticación de MAC (MAB), administrador de sesión
- Autenticación basada en web
- Auténtico-proxy
- Gateway de los Servicios IP (IPSG) para los host estáticos
- NetFlow Flexible
- Cisco TrustSec (CTS)
- Traza de los media
- El HTTP reorienta

Neutralización IPDT

En las versiones donde IPDT no se habilita por abandono, IPDT se puede apagar global con este comando:

```
# no ip device tracking
```

En las versiones donde está IPDT siempre encendido, el comando anterior no está disponible o no permite que usted inhabilite IPDT (Id. de bug Cisco CSCuj04986). En este caso, hay varias maneras de asegurarse de que no lo hace IPDT monitorea un puerto específico o no genera las alertas del IP duplicado.

Ingrese el dispositivo del IP que sigue el comando 10 del retardo de la sonda

Este comando no permite que un Switch envíe una sonda por 10 segundos en que detecta un link UP/flap, que minimiza la posibilidad para tener la sonda enviada mientras que el host en el otro lado de las Verificaciones del link para las dirección IP duplicadas. El RFC especifica una ventana de 10 segundos para la detección de la dirección duplicada, así que si usted retrasa la sonda de dispositivo-seguimiento, el problema se puede solucionar en la mayoría de los casos.

Si el Switch envía una sonda ARP para el cliente mientras que el host (por ejemplo, Microsoft Windows PC) es en su fase de la detección de la dirección duplicada, el host detecta la sonda

como dirección IP duplicada y presenta al usuario con un mensaje que una dirección IP duplicada fue encontrada en la red. El PC no pudo obtener 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.

Además del sonda-retardo, el retardo también se reajusta cuando el Switch detecta una sonda del PC/host. Por ejemplo, si el temporizador de la sonda ha contado abajo a cinco segundos y detecta una sonda ARP del PC/host, las restauraciones del temporizador de nuevo a 10 segundos.

Esta configuración se ha hecho el Id. de bug Cisco directo disponible CSCtn27420.

Ingrese el dispositivo del IP que sigue la sonda uso-SVI. Comando

Con este comando, usted puede configurar el Switch para enviar un NON-RFC la sonda obediente ARP; el IP de origen no será 0.0.0.0, sino que será la interfaz virtual del Switch (SVI) en el VLA N donde reside el host. Las máquinas de Microsoft Windows ven no más la sonda como sonda según lo definido por el RFC 5227 y no señalan un IP duplicado por medio de una bandera potencial.

Ingrese el comando de seguimiento del [fallback <host-ip> <mask>] de la auto-fuente de la sonda del dispositivo del IP [override]

Para los clientes que no tienen dispositivos extremos fiables/controlables o para los que tengan mucho Switches en un papel L2-only, la configuración de un SVI, que introduce una variable de la capa 3 en el diseño, no es una solución conveniente. Una mejora introdujo, en la versión 15.2(2)E y posterior, la posibilidad para permitir la asignación arbitraria de una dirección IP que no necesita pertenecer al Switch para el uso pues la dirección de origen en las sondas ARP generadas por IPDT. Esta mejora introduce la ocasión de modificar el comportamiento automático del sistema de estas maneras (esta lista muestra cómo el sistema se comporta automáticamente después de que se utilice cada comando):

Ingrese el comando de seguimiento de la auto-fuente de la sonda del dispositivo del IP

1. Fije la fuente al VLA N SVI si presente.
2. Busque para un par source/MAC en la tabla del host IP para la misma subred.
3. Envíe el IP de origen cero como en el caso predeterminado.

Ingrese el comando de seguimiento de 0.0.0.1 255.255.255.0 del retraso de la auto-fuente de la sonda del dispositivo del IP

1. Fije la fuente al VLA N SVI si presente.
2. Busque para un par source/MAC en la tabla del host IP para la misma subred.

3. Compute el IP de la fuente del IP de destino con el bit y la máscara del host proporcionados.

Ingrese el comando de seguimiento de la invalidación de 0.0.0.1 255.255.255.0 del retraso de la auto-fuente de la sonda del dispositivo del IP

1. Fije la fuente al VLA N SVI si presente.

2. Compute el IP de la fuente del IP de destino con el bit y la máscara del host proporcionados.

Nota: Una invalidación hace que usted salta la búsqueda para una entrada en la tabla.

Como ejemplo de los cómputos anteriores, asúmale host 192.168.1.200 de la sonda. Con los bits de la máscara y del host proporcionados, usted genera a una dirección de origen de 192.168.1.1.

Si usted sonda la entrada 10.5.5.20, usted generaría una sonda ARP con la dirección de origen 10.5.5.1, y así sucesivamente.

Ingrese el dispositivo del IP que sigue el comando 0 máximo

Este comando no inhabilita verdad IPDT, sino que limita el número de host seguidos a cero. Esto no es una solución recomendada y debe ser utilizada con cautela, porque afecta a todas las otras funciones que confíen en IPDT, que incluye la configuración de los canales del puerto según lo descrito en el Id. de bug Cisco CSCun81556.

Apague las características activas que accionan IPDT

Algunas características que pudieron accionar IPDT incluyen NMSP, el sensor del dispositivo, dot1x/MAB, WebAuth, y el IPSG. Esta solución es reservada para el más difícil o las situaciones complejas, en donde cualquier todas las soluciones previamente disponibles no trabajaron como se esperaba, o ellas crearon los problemas adicionales. Ésta es, sin embargo, la única solución que permite el granularity extremo cuando usted inhabilita IPDT, porque usted puede apagar solamente las características IPDT-relacionadas que causan los problemas y salen todo lo demás inafectado.

En el Cisco IOS más reciente, Versions15.2(2)E y posterior, usted ve una salida similar a esto:

```
Switch#show ip device tracking interface gig 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 todos los casquillos en la parte inferior de la salida son las que utilizan IPDT para trabajar. La mayor parte de los problemas creados cuando usted inhabilita el seguimiento del dispositivo pueden ser evitados si usted inhabilita los solos servicios que se ejecutan en la interfaz.

En las versiones anteriores del Cisco IOS, esta manera “fácil” de saber qué módulos se habilitan bajo interfaz no está disponible todavía, así que usted debe pasar con un proceso más implicado para conseguir los mismos resultados. Usted debe girar la **interfaz de la pista del dispositivo del IP del debug**, que es un registro de baja fricción que debe ser seguro en la mayoría de las configuraciones. Tenga cuidado de no girar el **dispositivo del IP del debug que sigue todos** porque esto, por el contrario, inunda la consola en las situaciones de la escala.

El debug está una vez prendido, trae una interfaz de nuevo al valor por defecto, y entonces agrega y quita un servicio IPDT de la configuración de la interfaz. Los resultados de los debugs le dicen qué servicio se ha habilitado/se ha inhabilitado con el comando que usted utilizó.

Aquí tiene un ejemplo:

```
Switch(config)#int gig 1/0/9
Switch(config-if)#ip device track max 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)#
```

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

Ahora, quite la configuración que usted acaba de agregar:

```
Switch(config-if)#no ip device track max 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 que usted quita la característica **00000008**, usted puede ver la máscara **00000044**, que debe haber sido la original, máscara predeterminada. Este valor de **00000044** se espera puesto que AIM es **0x00000004** y SM es **0x00000040**, que juntos dan lugar a **0x00000044**.

Hay varios servicios IPDT que pueden ejecutarse bajo interfaz:

Servicio IPDT	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 (ADMINISTRADOR DE SESIÓN) y HOST_TRACK_CLIENT_ATTACHMENT (también conocido como AIM/NMSP) se configuran para IPDT. Para apagar IPDT en esta interfaz, usted debe inhabilitar ambos, porque se inhabilita IPDT SOLAMENTE cuando todas las funciones que lo utilizan se inhabilitan también.

Después de que usted inhabilite esas características, usted tiene una salida similar a esto:

```
Switch(config-if)#do show ip dev trac int gig 1/0/9
-----------------------------------------
Interface GigabitEthernet1/0/9 is: STAND ALONE
IP Device Tracking = Disabled IPDT is disabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 180000
IP Device Tracking Enabled Features:
? No active features
-----------------------------------------
```

De esta manera, IPDT se inhabilita con más granularity.

Aquí está un cierto ejemplo de los comandos usados para inhabilitar algunas de las funciones discutidas previamente:

- **la fijación del nmsp suprime**
- **ningún monitor auto macro**

  Nota: La última característica debe estar disponible solamente en las Plataformas que soportan los puertos elegantes (presentación de destello de SmartPort), que se utilizan para habilitar las características y las configuraciones basadas en la ubicación de un Switch en la red y para las instalaciones de la configuración totales a través de la red.

Verifique la operación IPDT

Utilice estos comandos para verificar el estatus IPDT en su dispositivo:

- **muestre el seguimiento del dispositivo del IP…**

  Este comando visualiza las interfaces donde se habilita IPDT y donde las asociaciones MAC/IP/interface se siguen actualmente.

- **borre el seguimiento del dispositivo del IP…**

  Este comando borra las entradas IPDT-relacionadas.

  Nota: El Switch envía las sondas ARP a los host que fueron quitados. Si un host está presente, responde a la sonda ARP y el Switch agrega una entrada IPDT para el host. Usted debe inhabilitar las sondas ARP antes del comando claro IPDT; de esa manera, todas las entradas ARP deben ser idas. Si las sondas ARP se habilitan después del comando de **seguimiento del dispositivo claro del IP**, todas las entradas se vuelven otra vez.

- **seguimiento del dispositivo del IP del debug…**

  Este comando permite que usted recoja los debugs para visualizar la actividad IPDT en el tiempo real.