Dispositivo IP que segue a vista geral (IPDT)

Índice

Introdução

O documento descreve o dispositivo IP que segue (IPDT) e como desabilitá-lo e verificar sua operação.

Vista geral IPDT

Definição e uso

A tarefa principal IPDT é manter-se a par dos host conectados (associação do MAC e do endereço IP de Um ou Mais Servidores Cisco ICM NT). A fim fazer isto, envia pontas de prova do Address Resolution Protocol (ARP) do unicast com um intervalo padrão de 30 segundos; estas pontas de prova são enviadas ao MAC address do host conectado no outro lado do link, e da camada 2 do uso (L2) como a fonte do padrão o MAC address da interface física fora de que o ARP vai e um endereço IP de Um ou Mais Servidores Cisco ICM NT do remetente de 0.0.0.0, com base na definição da ponta de prova ARP alistada no RFC 5227 excerpted aqui:

Neste documento, “a ponta de prova ARP” do termo é usada para referir um pacote de solicitação ARP, transmitiu no link local, com todos-zero do “endereços IP de Um ou Mais Servidores Cisco ICM NT remetente. A OBRIGAÇÃO do “dos endereços do hardware remetente contém o endereço do hardware da relação que envia o pacote. O campo do “dos endereços IP de Um ou Mais Servidores Cisco ICM NT remetente DEVE ser ajustado a todos os zero, para evitar poluir caches ARP em outros anfitriões no mesmo link no caso onde o endereço despeja ser já dentro uso por um outro host. De “o campo endereços IP de destino DEVE ser ajustado ao endereço que está sendo sondado. Uma ponta de prova ARP transporta uma pergunta (“qualquer um está usando este endereço? ") e uma indicação implicada (“este é o endereço que eu espero a use.").

A finalidade de IPDT é para que o interruptor obtenha e mantenha uma lista de dispositivos que são conectados ao interruptor através de um endereço IP de Um ou Mais Servidores Cisco ICM NT. A ponta de prova não povoa a entrada de seguimento; está usada simplesmente a fim manter a entrada na tabela depois que é instruída com uma requisição ARP/resposta do host.

A inspeção ARP IP está permitida automaticamente quando IPDT é permitido; detecta a presença de anfitriões novos quando monitora pacotes ARP. Se a inspeção ARP dinâmica é permitida, simplesmente os pacotes ARP que valida estão usados a fim detectar anfitriões novos para o dispositivo que segue a tabela.

A espião IP DHCP, se permitida, detecta a presença ou a remoção de anfitriões novos quando o DHCP atribui ou revoga seus endereços IP de Um ou Mais Servidores Cisco ICM NT.

IPDT é uma característica que esteja sempre disponível. Contudo, em um Cisco IOS que mais recente o ® se libera, suas interdependências são permitidos à revelia (veja a identificação de bug Cisco CSCuj04986). Pode ser extremamente útil quando seu base de dados de associações dos anfitriões IP/MAC está usado a fim povoar o IP da fonte das lista de controle de acesso dinâmico (ACL), ou manter um emperramento de um endereço IP de Um ou Mais Servidores Cisco ICM NT a uma etiqueta do grupo de segurança.

A ponta de prova ARP é enviada sob duas circunstâncias:

- O link associado com uma entrada atual no base de dados IPDT move-se de uma PENA para um estado ASCENDENTE, e a entrada de ARP foi povoada.

- Um link já no estado ASCENDENTE que é associado com uma entrada no base de dados IPDT tem um intervalo expirado da ponta de prova.

Problema conhecido

A ponta de prova do “keepalive” enviada pelo interruptor é uma verificação L2. Como esta' do ponto de vista do interruptor, os endereços IP de Um ou Mais Servidores Cisco ICM NT usados como a fonte nos ARP não são importantes: esta característica pode ser usada em dispositivos sem o endereço IP de Um ou Mais Servidores Cisco ICM NT configurado de todo, assim que o origem de IP de 0.0.0.0 não é relevante.

Quando o host recebe este mensagens, responde para trás e povoa o campo do IP de destino com o único endereço IP de Um ou Mais Servidores Cisco ICM NT disponível no pacote recebido, que é seu próprio endereço IP de Um ou Mais Servidores Cisco ICM NT. Isto pode causar alertas falsos do endereço de IP duplicado, porque o host que responde considera seu próprio endereço IP de Um ou Mais Servidores Cisco ICM NT como a fonte e o destino do pacote; refira o endereço de IP duplicado 0.0.0.0. O Mensagem de Erro pesquisa defeitos o artigo para obter mais

informações sobre da encenação do endereço de IP duplicado.

Estado padrão e operação

Éimportante notar que, mesmo se IPDT é permitido globalmente, aquele não implica necessariamente que IPDT monitora ativamente uma porta dada. Nas liberações onde IPDT está sempre sobre e onde IPDT pode ser ligar/desligar globalmente firmado, quando IPDT é permitido globalmente, os outros recursos determinam realmente se é ativo em uma relação específica (veja a seção das áreas da funcionalidade).

Áreas da funcionalidade

IPDT e suas pontas de prova ARP enviados fora de uma dada interface são usados para estas características:

- Protocolo dos Serviços de mobilidade da rede (NMSP), versões 3.2.0E, 15.2(1)E, 3.5.0E e mais tarde
- Sensor do dispositivo, versões 15.2(1)E, 3.5.0E e mais tarde
- 1X, desvio da autenticação de MAC (MAB), gerente de sessão
- Autenticação com base na Web
- Autêntico-proxy
- Gateway dos Serviços IP (IPSG) para host estáticos
- Flexible NetFlow
- Cisco TrustSec (CTS)
- Traço dos media
- O HTTP reorienta

Desabilitação IPDT

Nas liberações onde IPDT não é permitido à revelia, IPDT pode ser desligado globalmente com este comando:

```
# no ip device tracking
```

Nas liberações onde IPDT está sempre sobre, o comando precedente não está disponível ou não permite que você desabilite IPDT (identificação de bug Cisco CSCuj04986). Neste caso, há diversas maneiras de assegurar-se de que IPDT não faça monitore uma porta específica ou não gerencia alertas do IP duplicado.

Entre no dispositivo IP que segue o comando 10 do atraso da ponta de prova

Este comando não permite que um interruptor envie uma ponta de prova pelos segundos 10 em que detecta um link UP/flap, que minimizar a possibilidade para ter a ponta de prova enviada quando o host no outro lado das verificações de link para endereços de IP duplicados. O RFC especifica um 10-segundo indicador para a detecção do endereço duplicado, assim que se você atrasa a ponta de prova deseguimento, a edição pode ser resolvida na maioria dos casos.

Se o interruptor manda uma ponta de prova ARP para o cliente quando o host (por exemplo,

Microsoft Windows PC) se realizar em sua fase da detecção do endereço duplicado, o host detecta a ponta de prova como um endereço de IP duplicado e apresenta o usuário com uma mensagem que um endereço de IP duplicado esteve encontrado na rede. O PC não pôde obter um endereço, e o usuário deve manualmente liberar-se/renova o endereço, desliga-o e reconecta-o à rede, ou recarrega-o o PC a fim ganhar o acesso de rede.

Além do que o ponta de prova-atraso, o atraso igualmente restaura-se quando o interruptor detecta uma ponta de prova do PC/host. Por exemplo, se o temporizador da ponta de prova contou para baixo a cinco segundos e detecta uma ponta de prova ARP do PC/host, as restaurações do temporizador de volta aos segundos 10.

Esta configuração foi feita à identificação de bug Cisco direta disponível CSCtn27420.

Entre no dispositivo IP que segue a ponta de prova uso-SVI. Comando

Com este comando, você pode configurar o interruptor a fim enviar a um NON-RFC a ponta de prova complacente ARP; o origem de IP não será 0.0.0.0, mas será a interface virtual do interruptor (SVI) no VLAN onde o host reside. As máquinas de Microsoft Windows já não veem a ponta de prova como uma ponta de prova como definida pelo RFC 5227 e não embandeiram um IP duplicado potencial.

Incorpore o comando de seguimento do [override] do [fallback <host-ip> <mask>] da auto-fonte da ponta de prova do dispositivo IP

Para os clientes que não têm dispositivos finais predizíveis/verificáveis ou para aqueles que têm muito Switches em um papel L2-only, a configuração de um SVI, que introduza uma variável da camada 3 no projeto, não é uma solução apropriada. Um realce introduzido, na versão 15.2(2)E e mais recente, a possibilidade para permitir a atribuição arbitrária de um endereço IP de Um ou Mais Servidores Cisco ICM NT que não precise de pertencer ao interruptor para o uso porque o endereço de origem nas pontas de prova ARP geradas por IPDT. Este realce introduz a possibilidade alterar o comportamento automático do sistema nestas maneiras (esta lista mostra como o sistema se comporta automaticamente depois que cada comando é usado):

Incorpore o comando de seguimento da auto-fonte da ponta de prova do dispositivo IP

1. Ajuste a fonte a VLAN SVI se presente.
2. Procure por um par source/MAC na tabela do Host IP para a mesma sub-rede.
3. Envie o origem de IP zero como no exemplo do padrão.

Incorpore o comando de seguimento de 0.0.0.1 255.255.255.0 da reserva da auto-fonte da ponta de prova do dispositivo IP

1. Ajuste a fonte a VLAN SVI se presente.
2. Procure por um par source/MAC na tabela do Host IP para a mesma sub-rede.

3. Compute o IP da fonte do IP de destino com o bit e a máscara do host fornecidos.

Incorpore o comando de seguimento da ultrapassagem de 0.0.0.1 255.255.255.0 da reserva da auto-fonte da ponta de prova do dispositivo IP

1. Ajuste a fonte a VLAN SVI se presente.

2. Compute o IP da fonte do IP de destino com o bit e a máscara do host fornecidos.

Nota: Uma ultrapassagem fá-lo saltar a busca para uma entrada na tabela.

Como exemplo das computações precedentes, supõe-no host 192.168.1.200 da ponta de prova. Com os bit da máscara e do host fornecidos, você gerencie um endereço de origem de 192.168.1.1.

Se você sonda a entrada 10.5.5.20, você geraria uma ponta de prova ARP com endereço de origem 10.5.5.1, e assim por diante.

Entre no dispositivo IP que segue o comando 0 máximo

Este comando não desabilita verdadeiramente IPDT, mas limita o número de anfitriões seguidos a zero. Esta não é uma solução recomendada e deve ser usado com cuidado, porque afeta todos os outros recursos que confiam em IPDT, que inclui a configuração dos canais de porta como descrito na identificação de bug Cisco CSCun81556.

Desligue as características ativas que provocam IPDT

Algumas características que puderam provocar IPDT incluem NMSP, sensor do dispositivo, dot1x/MAB, WebAuth, e IPSG. Esta solução é reservada para o mais difícil ou as situações complexas, onde uma ou outra todas as soluções previamente disponíveis não trabalharam como esperado, ou criaram problemas adicionais. Esta é, contudo, a única solução que permite a granularidade extrema quando você desabilita IPDT, porque você pode desligar somente as características IPDT-relacionadas que causam problemas e saem de tudo outro não afetado.

No Cisco IOS o mais recente, Versions15.2(2)E e mais tarde, você vê uma saída similar a esta:

```
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
```

As duas linhas em todos os tampões na parte inferior da saída são aquelas que usam IPDT a fim trabalhar. A maioria dos problemas criados quando você desabilita o seguimento do dispositivo podem ser evitados se você desabilita os únicos serviços que são executado na relação.

Nas versões anterior do Cisco IOS, esta maneira “fácil” de saber que módulos são permitidos sob uma relação não está disponível ainda, assim que você deve atravessar um processo mais involvido a fim obter os mesmos resultados. Você deve girar sobre **debuga a relação da trilha do dispositivo IP**, que é um log de baixa frequência que deva ser seguro na maioria de instalações. Seja cuidadoso não girar sobre **debugam o dispositivo IP que segue tudo** porque isto, pelo contrário, inunda o console em situações da escala.

Uma vez debugar está ligada, traz uma relação de volta ao padrão, e então adiciona e remove um serviço IPDT da configuração da interface. Os resultados do debugam dizem-lhe que serviço foi permitido/desabilitado com o comando que você se usou.

Aqui está um exemplo:

```
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)#
```

O que a saída revela é que você permitiu a característica **00000008**, e que a máscara dos novos recursos é **0000004C**.

Agora, remova a configuração que você apenas adicionou:

```
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)#
```

Uma vez que você remove a característica **00000008**, você pode ver a máscara **00000044**, que deve ter sido o original, máscara padrão. Este valor de **00000044** é esperado desde que AIM é **0x00000004** e S é **0x00000040**, que conduzem junto a **0x00000044**.

Há diversos serviços IPDT que podem ser executado sob uma relação:

Serviço IPDT	Interface
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

No exemplo, os módulos HOST_TRACK_CLIENT_SM (GERENTE DE SESSÃO) e HOST_TRACK_CLIENT_ATTACHMENT (igualmente conhecido como AIM/NMSP) são configurados para IPDT. A fim desligar IPDT nesta relação, você deve desabilitar ambos, porque IPDT está desabilitado SOMENTE quando todas as funções que o usam são desabilitadas também.

Depois que você desabilita aquelas características, você tem uma saída similar a esta:

```
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
-----------------------------------------
```

Desta maneira, IPDT é desabilitado com mais granularidade.

Está aqui algum exemplo dos comandos usados a fim desabilitar algumas das funções discutidas previamente:

- **o anexo do nmsp suprime**
- **nenhum auto monitor macro**

  Nota: A característica a mais atrasada deve estar disponível somente nas Plataformas que apoiam as portas espertas (apresentação instantânea de SmartPort), que são usadas a fim permitir as características e os ajustes baseados no lugar de um interruptor na rede e para distribuições de configuração maciças através da rede.

Verifique a operação IPDT

Use estes comandos a fim verificar o estado IPDT em seu dispositivo:

- **mostre o seguimento do dispositivo IP…**

  Este comando indica as relações onde IPDT é permitido e onde as associações MAC/IP/interface são seguidas atualmente.

- **cancele o seguimento do dispositivo IP…**

  Este comando cancela entradas IPDT-relacionadas.

  Nota: O interruptor envia pontas de prova ARP aos anfitriões que foram removidos. Se um host esta presente, responde à ponta de prova ARP e o interruptor adiciona uma entrada IPDT para o host. Você deve desabilitar pontas de prova ARP antes do comando claro IPDT; nessa maneira, todas as entradas de ARP devem ser idas. Se as pontas de prova ARP são permitidas após o comando de **seguimento do dispositivo claro IP**, todas as entradas voltam outra vez.

- **debugar o seguimento do dispositivo IP…**

  Este comando permite que você recolha debuga a fim indicar a atividade IPDT no realtime.