# Verificar operações do dispositivo IPDT

## Contents



## Introduction

Este documento descreve como verificar as operações do IP Device Tracking (IPDT) e como desativar essas ações.

## Prerequisites

### Requirements

Não existem requisitos específicos para este documento.

### Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas. No entanto, as saídas neste documento foram baseadas nestas versões de software e hardware:

- Cisco WS-C2960X
- Cisco IOS® 15.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

# Visão geral do IPDT

## Definição e uso

A principal tarefa do IPDT é rastrear os hosts conectados (associação de endereços MAC e IP). Para fazer isso, ele envia sondas de Protocolo de Resolução de Endereços (ARP) unicast com um intervalo padrão de 30 segundos; esses testadores são enviados para o endereço MAC do host conectado no outro lado do link e usam a camada 2 (L2) como a origem padrão do endereço MAC da interface física a partir da qual o ARP vai e um endereço IP do remetente de 0.0.0.0, com base na definição do testador ARP listada no RFC 5227.

## Trecho

Neste documento, o termo 'Prova ARP' é usado para se referir a um pacote de solicitação ARP, transmitido no link local, com um 'endereço IP do remetente' totalmente zero. O 'endereço de hardware do remetente' DEVE conter o endereço de hardware da interface que envia o pacote. O campo 'endereço IP do remetente' DEVE ser definido como zero, para evitar que os caches ARP sejam corrompidos em outros hosts no mesmo link, caso o endereço já esteja em uso por outro host. O campo 'endereço IP de destino' DEVE ser definido para o endereço que é investigado. Uma Sonda ARP transmite tanto uma pergunta (*Alguém usa este endereço?*) quanto uma instrução implícita (*Este é o endereço que espero usar*.).

A finalidade do IPDT é que o switch obtenha e mantenha uma lista de dispositivos conectados ao switch por meio de um endereço IP. A sonda não preenche a entrada de rastreamento; ele é simplesmente usado para manter a entrada na tabela depois de ser aprendida através de uma solicitação/resposta ARP do host.

A Inspeção ARP IP é ativada automaticamente quando o IPDT é ativado; detecta a presença de novos hosts quando monitora pacotes ARP. Se a inspeção ARP dinâmica estiver habilitada, somente os pacotes ARP que ela validar serão usados para detectar novos hosts para a tabela de Rastreamento de Dispositivos.

O rastreamento de DHCP IP, se habilitado, detecta a presença ou remoção de novos hosts quando o DHCP designa ou revoga seus endereços IP.  Quando o tráfego DHCP é visto para um determinado host, o temporizador de intervalo de prova ARP IPDT é redefinido.

O IPDT é um recurso que sempre esteve disponível. No entanto, em versões mais recentes do Cisco IOS®, suas interdependências são habilitadas por padrão (consulte 'ID de bug Cisco CSCuj04986'). Ele pode ser extremamente útil quando seu banco de dados de associações de hosts IP/MAC é usado para preencher o IP de origem de ACLs (Access Control Lists, listas de controle de acesso) dinâmicas ou para manter uma ligação de um endereço IP a uma tag de grupo de segurança.

A prova ARP é enviada sob duas circunstâncias:

- O link associado a uma entrada atual no banco de dados IPDT move-se de um estado DOWN para um UP e a entrada ARP foi preenchida.
- Um link já no estado UP associado a uma entrada no banco de dados IPDT tem um intervalo de sondagem expirado.

## Problema

O teste "keepalive" enviado pelo switch é uma verificação L2. Como tal, do ponto de vista do switch, os endereços IP usados como origem nos ARPs não são importantes: esse recurso pode ser usado em dispositivos sem nenhum endereço IP configurado, portanto a origem IP de 0.0.0.0 não é relevante.

Quando o host recebe essas mensagens, ele responde e preenche o campo IP de destino com o único endereço IP disponível no pacote recebido, que é seu próprio endereço IP. Isso pode causar alertas falsos de endereço IP duplicado, pois o host que responde vê seu próprio endereço IP como origem e destino do pacote; consulte o artigo Duplicate IP Address 0.0.0.0. Error Message Troubleshoot para obter mais informações sobre o cenário de endereço IP duplicado.

## Estado e operação padrão

A configuração global ativada/desativada para IPDT é um comportamento antigo que causou problemas no campo, pois os clientes nem sempre sabiam que precisavam ativar o IPDT para que determinados recursos funcionassem. Nas versões atuais, o IPDT é controlado unicamente em um nível de interface quando habilita um recurso que exige IPDT.

O IPDT está ativado globalmente por padrão com nessas versões; ou seja, nenhum comando de configuração global devido ao 'bug da Cisco ID CSCua85383':

- Catalyst 2k/3k 15.2(1)E
- Catalyst 3850: 3.2.0SE
- Catalyst 4k: 15.2(1)E/3.5.0E

Éimportante observar que, mesmo que o IPDT esteja ativado globalmente, isso não implica necessariamente que ele monitore ativamente uma determinada porta.

Nas versões em que o IPDT está sempre ativo e onde ele pode ser globalmente desligado/ligado, quando o IPDT está ativado globalmente, outros recursos realmente determinam se ele está ativo em uma interface específica (consulte a seção Áreas de funcionalidade).

## Áreas de funcionalidade

O IPDT e seus testadores ARP enviados de uma determinada interface são usados para estes recursos:

- Network Mobility Services Protocol (NMSP), versões 3.2.0E, 15.2(1)E, 3.5.0E e posteriores
- Sensor de dispositivo, versões 15.2(1)E, 3.5.0E e posteriores
- 1X, desvio de autenticação MAC (MAB), gerenciador de sessão
- Autenticação baseada na Web
- Auth-proxy
- Proteção de origem IP (IPSG) para hosts estáticos

- Netflow flexível
- Cisco TrustSec (CTS)
- Rastreamento de mídia
- Redirecionamentos de HTTP

## Matriz de recursos

| Platform | Recurso | Padrão ativado (Iniciar em) | Desabilitar método | Desabilitar CLI |
|---|---|---|---|---|
| Cat 2960/3750 (Cisco IOS) | IPDT | 15.2(1)E * | CLI global (versões mais antigas) * por interface | no ip device tracking * ip device tracking maxim *** |
| Cat 2960/3750 (Cisco IOS) | NMSP | não | CLI global ou CLI por interface | no nmsp enable **** de supressão de an nmsp |
| Cat 2960/3750 (Cisco IOS) | Sensor de dispositivo | 15.0(1)SE | CLI global | no macro auto monitor |
| Cat 2960/3750 (Cisco IOS) | Rastreamento ARP | 15.2(1)E ** | n/a | n/a |
| CAT 3850 | IPDT | todas as versões * | per-interface * | ip device tracking maxim *** |
| CAT 3850 | NMSP | todas as versões | por interface | supressão de anexo nm |
| CAT 3850 | Sensor de dispositivo | não | n/a | n/a |
| CAT 3850 | Rastreamento ARP | todas as versões ** | n/a | n/a |
| CAT 4500 | IPDT | 15.2(1)E / 3.5.0E * | CLI global (versões mais antigas) * por interface | no ip device tracking * ip device tracking maxim *** |
| CAT 4500 | NMSP | não | CLI global ou CLI por interface | no nmsp enable **** de supressão de an nmsp |
| CAT 4500 | Sensor de dispositivo | 15.1(1)SG/3.3.0SG | CLI global | no macro auto monitor |
| CAT 4500 | Rastreamento ARP | ** 15.2(1)E / 3.5.0E | n/a | n/a |

## Recursos

- O IPDT não pode ser desativado globalmente em versões mais recentes, mas ele só estará ativo em portas se os recursos que o exigem estiverem ativos.
- O rastreamento ARP só estará ativo se as combinações de recursos específicos o habilitarem.
- Se você desabilitar o IPDT em uma base por interface, o rastreamento ARP não será interrompido. Isso impede o rastreamento IPDT. Está disponível em i3.3.0SE, 15.2(1)E, 3.5.0E e posterior.
- A supressão NMSP por interface só estará disponível se o NMSP estiver habilitado

globalmente.

# Desabilitar IPDT

Nas versões em que o IPDT não está ativado por padrão, ele pode ser desativado globalmente com este comando:

```
Switch(config)#no ip device tracking
```

Nas versões em que o IPDT está sempre ativo, o comando anterior não está disponível ou não permite desativar o IPDT ('Cisco bug ID CSCuj04986'). Nesse caso, há várias maneiras de garantir que o IPDT não monitore uma porta específica ou não gere alertas IP duplicados.

## Digite o ip device tracking probe delay 10 Comando

Esse comando não permite que um switch envie uma sonda por 10 segundos quando detecta um link UP/flap, o que minimiza a possibilidade de que a sonda seja enviada enquanto o host no outro lado do link verifica se há endereços IP duplicados. O RFC especifica uma janela de 10 segundos para detecção de endereço duplicado, portanto, se você atrasar a prova de rastreamento de dispositivo, o problema poderá ser resolvido na maioria dos casos.

Se o switch enviar uma Prova ARP para o cliente enquanto o host (por exemplo, um PC com Microsoft Windows) estiver em sua fase de Detecção de Endereço Duplicado, o host detectará a prova como um endereço IP duplicado e apresentará ao usuário uma mensagem de que um endereço IP duplicado foi encontrado na rede. Se o PC não obtiver um endereço e o usuário precisar liberar/renovar manualmente o endereço, desconectar e reconectar à rede ou reinicializar o PC para obter acesso à rede.

Além do retardo de sonda, o retardo também é redefinido quando o switch detecta uma sonda do PC/host. Por exemplo, se o temporizador da sonda for contado até cinco segundos e detectar uma Sonda ARP do PC/host, o temporizador será redefinido para 10 segundos.

Essa configuração foi disponibilizada através da 'ID de bug Cisco CSCtn27420'.

## Digite o ip device tracking probe use-svi Comando

Com esse comando, você pode configurar o switch para enviar um Probe ARP não compatível com RFC; a origem IP não é 0.0.0.0, mas é a interface virtual do switch (SVI) na VLAN onde o host reside. As máquinas Microsoft Windows não veem mais a sonda como uma sonda conforme definido pelo RFC 5227 e não sinalizam um IP duplicado potencial.

## Digite o ip device tracking probe auto-source [fallback Comando

Para clientes que não têm dispositivos finais previsíveis/controláveis ou para aqueles que têm muitos switches em uma função apenas de L2, a configuração de um SVI, que introduz uma variável de Camada 3 no design, não é uma solução adequada. Um aprimoramento introduziu, na versão 15.2(2)E e posterior, a possibilidade de permitir a atribuição arbitrária de um endereço IP que não precisa pertencer ao switch para uso como o endereço origem em testes ARP gerados por IPDT. Este aprimoramento introduz a chance de modificar o comportamento automático do sistema destas maneiras (esta lista mostra como o sistema se comporta automaticamente após

cada comando ser usado):

### Digite o ip device tracking probe auto-source Comando

1. Defina a origem como VLAN SVI, se houver.
2. Procure um par origem/MAC na tabela de hosts IP para a mesma sub-rede.
3. Envie a origem IP zero como no caso padrão.

### Digite o ip device tracking probe auto-source fallback 0.0.0.1 255.255.255.0 Comando

1. Defina a origem como VLAN SVI, se houver.
2. Procure um par origem/MAC na tabela de hosts IP para a mesma sub-rede.
3. Calcule o IP de origem a partir do IP de destino com o bit e a máscara de host fornecidos.

### Digite o ip device tracking probe auto-source fallback 0.0.0.1 255.255.255.0 override Comando

1. Defina a origem como VLAN SVI, se houver.
2. Calcule o IP de origem a partir do IP de destino com o bit e a máscara de host fornecidos.

**Note**: Uma substituição faz com que você ignore a pesquisa de uma entrada na tabela. Como exemplo dos cálculos anteriores, suponha que você investigue o host 192.168.1.200. Com a máscara e os bits de host fornecidos, você gera um endereço de origem de 192.168.1.1. Se você investigar a entrada 10.5.5.20, poderá gerar um teste ARP com o endereço de origem 10.5.5.1 e assim por diante.

### Digite o ip device tracking maximum 0 Comando

Esse comando não desabilita verdadeiramente o IPDT, mas limita o número de hosts rastreados a zero. Essa não é uma solução recomendada e deve ser usada com cuidado, pois afeta todos os outros recursos que dependem do IPDT, o que inclui a configuração dos canais de porta conforme descrito na 'ID de bug Cisco CSCun81556'.

## Desativar Recursos Ativos que Disparam o IPDT

Alguns recursos que podem disparar o IPDT incluem NMSP, sensor de dispositivo, dot1x/MAB, WebAuth e IPSG. Não é recomendável habilitar esses recursos em portas de tronco. Essa solução é reservada para as situações mais difíceis ou complexas, em que nem todas as soluções disponíveis anteriormente funcionavam conforme o esperado ou criavam problemas adicionais. Esta é, no entanto, a única solução que permite extrema granularidade quando você desabilita o IPDT, porque você pode desativar apenas os recursos relacionados ao IPDT que causam problemas e deixar tudo o resto não afetado.

No Cisco IOS mais recente, versões 15.2(2)E e posteriores, você vê uma saída semelhante a esta:

```
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
```

As duas linhas em todas as letras maiúsculas na parte inferior da saída são aquelas que usam IPDT para funcionar. A maioria dos problemas criados quando você desabilita o rastreamento de dispositivo pode ser evitada se você desabilitar os serviços únicos executados na interface.

Em versões anteriores do Cisco IOS, essa maneira fácil de saber quais módulos estão ativados em uma interface ainda não está disponível, portanto, você deve passar por um processo mais envolvido para obter os mesmos resultados. Você deve ativar **debug ip device track interface**, que é um log de baixa frequência que deve ser seguro na maioria das configurações. Tome cuidado para não ativar o **debug ip device tracking all** porque, ao contrário, ele inunda o console em situações de escala.

Quando a depuração estiver ativada, coloque uma interface de volta ao padrão e adicione e remova um serviço IPDT da configuração da interface. Os resultados das depurações informam qual serviço foi ativado/desativado com o comando usado.

### Exemplo

```
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)#
```

O que a saída revela é que você ativou o recurso **00000008** e que a nova máscara de recurso é **0000004C**.

Agora, remova a configuração que acabou de adicionar:

```
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)#
```

Depois de remover o recurso **00000008**, você pode ver a máscara **0000044**, que deve ter sido a máscara padrão original. Esse valor de **00000044** é esperado, pois o AIM é **0x0000004** e o SM é **0x00000040**, que juntos resultam em **0x0000044**.

Há vários serviços IPDT que podem ser executados sob uma interface:

| Serviço IPT | 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 (SESSION-MANAGER) e HOST_TRACK_CLIENT_ATTACHMENT (também conhecido como AIM/NMSP) são configurados para IPDT. Para desativar o IPDT nesta interface, você deve desabilitar ambos, pois o IPDT é desabilitado SOMENTE quando todas as funções que o utilizam também são desabilitadas.

Depois de desativar esses recursos, você terá uma saída semelhante a esta:

```
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:
ßNo active features
----------------------------------------
```

Dessa forma, o IPDT é desativado com mais granularidade.

Aqui estão alguns exemplos de comandos usados para desativar algumas das funções discutidas anteriormente:

- supressão de anexo nmsp
- no macro auto monitor

**Note**: O recurso mais recente deve estar disponível apenas em plataformas que suportam Smart Ports (apresentação SmartPort Flash), que são usadas para ativar recursos com base no local de um switch na rede e para implantações de configuração em massa na rede.

# Verificar a operação do IPDT

Use estes comandos para verificar o status IPDT no seu dispositivo:

- show ip device tracking
  Esse comando exibe as interfaces onde o IPDT está habilitado e onde as associações MAC/IP/interface estão atualmente rastreadas.
- clear ip device tracking
- Esse comando limpa as entradas relacionadas ao IPDT.

**Note**: O switch envia testes ARP aos hosts que foram removidos. Se um host estiver presente, ele responde à prova ARP e o switch adiciona uma entrada IPDT para o host.

Você deve desativar os testes ARP antes do comando clear IPDT; dessa forma, todas as entradas ARP serão perdidas. Se as provas ARP forem ativadas após o comando **clear ip device tracking**, todas as entradas voltarão novamente.

- **debug ip device tracking**
  Esse comando permite coletar depurações para exibir a atividade IPDT em tempo real.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.