

# Verifique a configuração pós-MAB de rastreamento de dispositivo IP no switch

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Diagrama](#)

[Informações de Apoio](#)

[Configuração](#)

[Configuração no C1000](#)

[Configuração no ISE](#)

[Etapa 1. Adicionar dispositivo](#)

[Etapa 2. Adicionar Ponto de Extremidade](#)

[Etapa 3. Adicionar conjunto de políticas](#)

[Etapa 4. Adicionar política de autenticação](#)

[Etapa 5. Adicionar Política de Autorização](#)

[Verificar](#)

[Antes da configuração do MAB](#)

[Após a configuração do MAB](#)

[Etapa 1. Antes da autenticação MAB](#)

[Etapa 2. Após a autenticação MAB](#)

[Etapa 3. Confirmar sessão de autenticação](#)

[Etapa 4. Confirmar registro ao vivo do Radius](#)

[Etapa 5. Confirmar detalhes do pacote de rastreamento de dispositivo IP](#)

[Problema](#)

[Soluções possíveis](#)

[1. Atrasar o envio de provas ARP](#)

[2. Origem Automática de Configuração para Sondas ARP](#)

[Padrão 1. O IP do SVI está configurado](#)

[Padrão 2. O IP do SVI não está configurado](#)

[3. Desabilite Forçadamente o Rastreamento de Dispositivos IP](#)

[Referência](#)

---

## Introdução

Este documento descreve o comportamento do rastreamento de dispositivo IP após a configuração MAB e possíveis soluções para problemas de comunicação após a autenticação MAB.

# Pré-requisitos

## Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do Cisco Identity Services Engine
- Configuração do Cisco Catalyst

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Identity Services Engine Virtual 3.3 Patch 1
- C1000-48FP-4G-L 15.2(7)E9

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Diagrama

Este documento apresenta a configuração e a verificação da autenticação MAB neste diagrama.

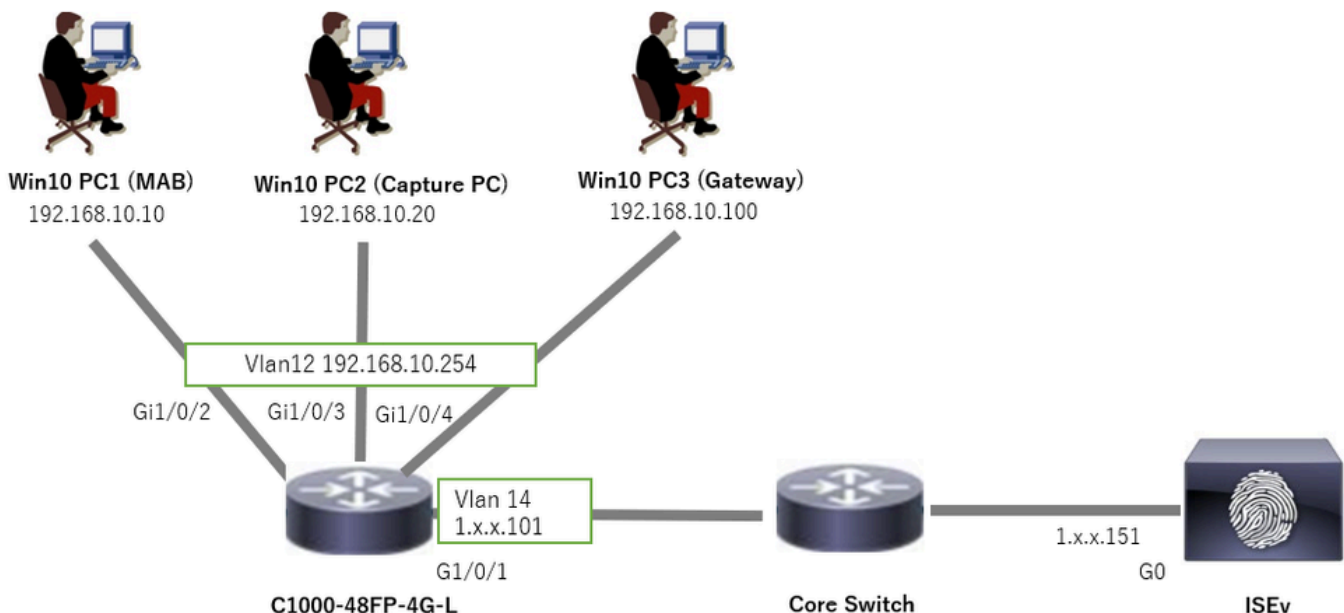


Diagrama de Rede

## Informações de Apoio

Mesmo que a autenticação MAB tenha êxito, após reinicializar (ou desconectar e reconectar o cabo) o Win10 PC1, ele não poderá fazer ping no gateway (Win10 PC3) com êxito. Este

comportamento inesperado é devido a um conflito de endereço IP no Win10 PC1. O rastreamento de dispositivo IP e suas sondas ARP são ativados por padrão na interface que está configurada como MAB. Quando o PC com Windows está conectado a um Switch Catalyst com rastreamento de dispositivo IP ativado, há uma possibilidade de que o lado do Windows detecte um conflito de endereço IP. Isso ocorre porque uma prova ARP (com um endereço IP do remetente de 0.0.0.0) é recebida durante a janela de detecção desse mecanismo, ela é tratada como um conflito de endereço IP.

## Configuração

Este exemplo de configuração demonstra o comportamento do rastreamento do dispositivo IP após a configuração MAB.

### Configuração no C1000

Essa é a configuração mínima na CLI do C1000.

```
aaa new-model

radius server ISE33
address ipv4 1.x.x.191
key cisco123

aaa group server radius AAASERVER
server name ISE33

aaa authentication dot1x default group AAASERVER
aaa authorization network default group AAASERVER
aaa accounting dot1x default start-stop group AAASERVER
dot1x system-auth-control

interface Vlan12
ip address 192.168.10.254 255.255.255.0

interface Vlan14
ip address 1.x.x.101 255.0.0.0

interface GigabitEthernet1/0/1
Switch port access vlan 14
Switch port mode access

interface GigabitEthernet1/0/3
Switch port access vlan 12
Switch port mode access

interface GigabitEthernet1/0/4
Switch port access vlan 12
Switch port mode access

interface GigabitEthernet1/0/2
Switch port access vlan 12
Switch port mode access
authentication host-mode multi-auth
authentication port-control auto
```

```
spanning-tree portfast edge
mab
```

```
// for packet capture
monitor session 1 source interface Gi1/0/2
monitor session 1 destination interface Gi1/0/3
```

## Configuração no ISE

### Etapa 1. Adicionar dispositivo

Navegue até Administração > Dispositivos de rede, clique no botão Adicionar para adicionar o dispositivo C1000.

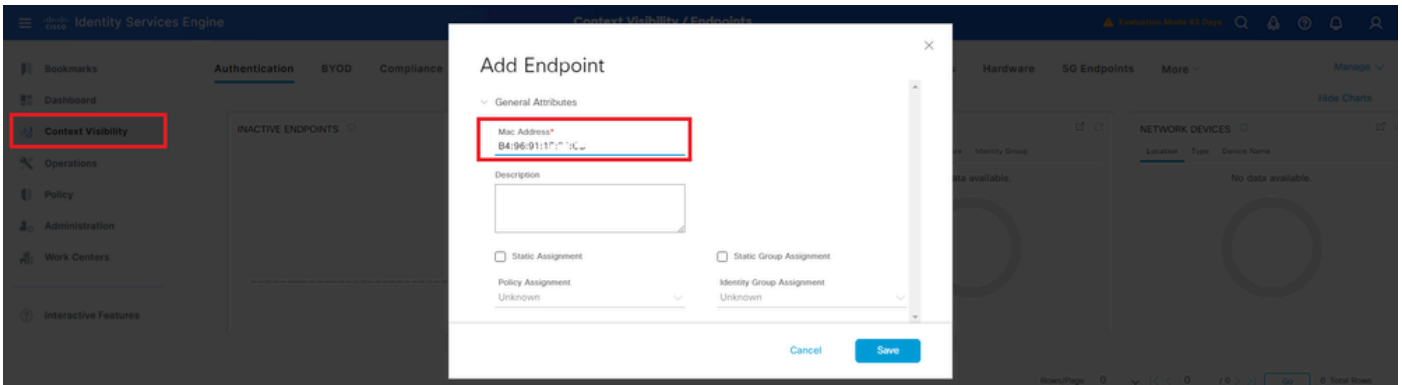
- Nome: C1000
- Endereço IP: 1.x.x.101

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The main navigation bar is blue with the Cisco logo and 'Identity Services Engine' text. The current page is 'Administration / Network Resources' and 'Network Devices'. The left sidebar contains various navigation options like 'Bookmarks', 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration', 'Work Centers', and 'Interactive Features'. The main content area is titled 'Network Devices' and 'New Network Device'. The 'Name' field is set to 'C1000'. The 'IP Address' field is set to '1.1.1.101 / 32'. The 'RADIUS Authentication Settings' section is expanded, showing 'RADIUS UDP Settings' with 'Protocol' set to 'RADIUS' and 'Shared Secret' set to 'cisco123'.

Adicionar dispositivo

### Etapa 2. Adicionar Ponto de Extremidade

Navegue até Visibilidade de contexto > Pontos finais, clique no botão Adicionar para adicionar o MAC do Ponto final.

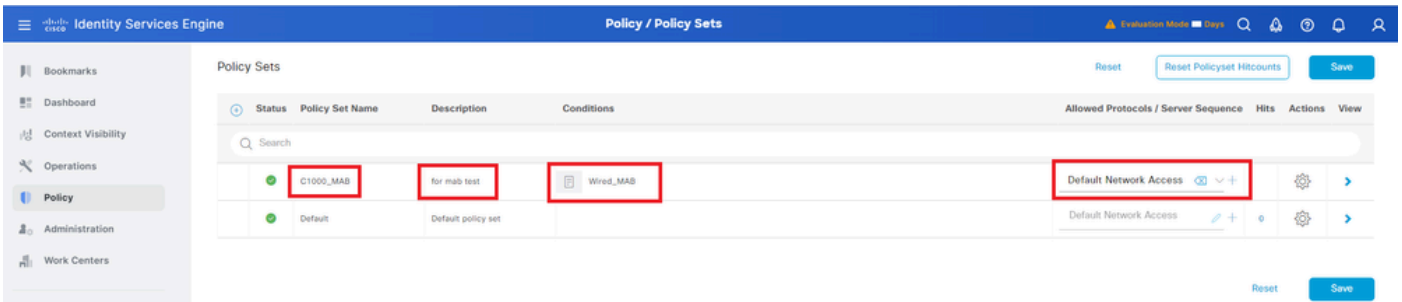


Adicionar Ponto de Extremidade

### Etapa 3. Adicionar conjunto de políticas

Navegue para Política > Conjuntos de políticas, clique em + para adicionar um conjunto de políticas.

- Nome do conjunto de políticas : C1000\_MAB
- Descrição : para teste mab
- Condições : Wired\_MAB
- Protocolos Permitidos/Sequência de Servidores: Acesso Padrão à Rede

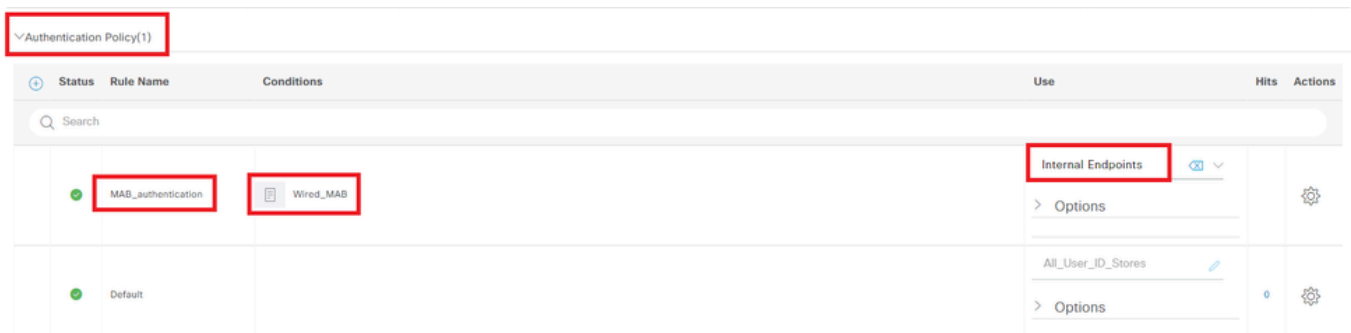


Adicionar conjunto de políticas

### Etapa 4. Adicionar política de autenticação

Navegue até Policy Sets, clique em C1000\_MAB para adicionar uma política de autenticação.

- Nome da regra : MAB\_authentication
- Condições : Wired\_MAB
- Uso: endpoints internos



Adicionar política de autenticação

## Etapa 5. Adicionar Diretiva de Autorização

Navegue até Policy Sets, clique em C1000\_MAB para adicionar uma política de autorização.

- Nome da Regra : MAB\_authorization
- Condições : Network\_Access\_Authentication\_Passed
- Resultados: PermitAccess

Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions
●	MAB_authorization	Network_Access_Authentication_Passed	PermitAccess	+	Select from list	+	⚙️
●	Default		DenyAccess	+	Select from list	+	⚙️

Adicionar Política de Autorização

## Verificar

### Antes da configuração do MAB

Execute `show ip device tracking all` o comando para confirmar se o recurso de rastreamento de dispositivo IP está desabilitado.

```
<#root>
```

```
Switch #
```

```
show ip device tracking all
```

```
Global IP Device Tracking for clients =
```

```
Disabled
```

```
-----  
IP Address MAC Address Vlan Interface Probe-Timeout State Source  
-----
```

Após a configuração do MAB

Etapa 1. Antes da autenticação MAB

Execute `show ip device tracking all` o comando para confirmar se o recurso de rastreamento de dispositivo IP está habilitado.

```
<#root>
```

```
Switch #
```

```
show ip device tracking all
```

Global IP Device Tracking for clients =

**Enabled**

Global IP Device Tracking Probe Count = 3

Global IP Device Tracking Probe Interval = 30

Global IP Device Tracking Probe Delay Interval = 0

-----  
IP Address MAC Address Vlan Interface Probe-Timeout State Source  
-----

Total number interfaces enabled: 1

Enabled interfaces:

Gi1/0/2

Etapa 2. Após a autenticação MAB

Inicialize a autenticação MAB do Win10 PC1 e execute o comando `show ip device tracking all` para confirmar o status do rastreamento do dispositivo IP em GigabitEthernet1/0/2.

<#root>

Switch #

`show ip device tracking all`

Global IP Device Tracking for clients =

**Enabled**

Global IP Device Tracking Probe Count = 3

Global IP Device Tracking Probe Interval = 30

Global IP Device Tracking Probe Delay Interval = 0

-----  
IP Address MAC Address Vlan Interface Probe-Timeout State Source  
-----

192.168.10.10

b496.9115.84cb 12 GigabitEthernet1/0/2 30

**ACTIVE**

ARP

Total number interfaces enabled: 1

Enabled interfaces:

Gi1/0/2

Etapa 3. Confirmar sessão de autenticação

Execute `show authentication sessions interface GigabitEthernet1/0/2 details` o comando para confirmar a sessão de autenticação MAB.

<#root>

Switch #

show authentication sessions interface GigabitEthernet1/0/2 details

Interface: GigabitEthernet1/0/2  
MAC Address: b496.9115.84cb  
IPv6 Address: Unknown  
IPv4 Address: 192.168.10.10  
User-Name: B4-96-91-15-84-CB  
Status: Authorized  
Domain: DATA  
Oper host mode: multi-auth  
Oper control dir: both  
Session timeout: N/A  
Restart timeout: N/A  
Periodic Acct timeout: N/A  
Session Uptime: 114s  
Common Session ID: 01C200650000001D62945338  
Acct Session ID: 0x0000000F  
Handle: 0xBE000007  
Current Policy: POLICY\_Gi1/0/2

Local Policies:  
Service Template: DEFAULT\_LINKSEC\_POLICY\_SHOULD\_SECURE (priority 150)

Server Policies:

Method status list:  
Method State

mab Authc Success

Etapa 4. Confirmar registro ao vivo do Radius

Navegue até **Operations > RADIUS > Live Logons** na GUI do ISE, confirme o registro ao vivo para autenticação MAB.

The screenshot shows the 'Live Sessions' page in the ISE GUI. At the top, there are several summary cards: 'Misconfigured Supplicants' (0), 'Misconfigured Network Devices' (0), 'RADIUS Drops' (0), 'Client Stopped Responding' (1), and 'Repeat Counter' (0). Below these cards is a table with columns: Time, Status, Details, Repea..., Identity, Endpoint ID, Endpoint Profile, Authentication Policy, Authorization Policy, Authorization Profiles, IP Address, and Network De... The table contains two rows of session data. The second row is highlighted with red boxes around the Identity, Authentication Policy, Authorization Policy, and IP Address columns. The Identity column contains 'B4-96-91-15-84-CB', the Authentication Policy column contains 'C1000\_MAB ==> MAB\_authentication', the Authorization Policy column contains 'C1000\_MAB ==> MAB\_authorizati...', and the IP Address column contains '192.168.10.10'.

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address	Network De...
Feb 25, 2024 04:32:06.437 PM	●		0	B4-96-91-15-84-CB	B4-96-91-15-84-CB	Intel-Device	C1000_MAB ==> MAB_authentication	C1000_MAB ==> MAB_authorizati...	PermitAccess	192.168.10.10	
Feb 25, 2024 04:32:05.396 PM	●		0	B4-96-91-15-84-CB	B4-96-91-15-84-CB	Intel-Device	C1000_MAB ==> MAB_authentication	C1000_MAB ==> MAB_authorizati...	PermitAccess	192.168.10.10	C1000

Etapa 5. Confirmar detalhes do pacote de rastreamento de dispositivo IP

Execute show interfaces GigabitEthernet1/0/2 o comando para confirmar o endereço MAC de GigabitEthernet1/0/2.

<#root>



Switch #

```
show interfaces GigabitEthernet1/0/2
```

```
GigabitEthernet1/0/2 is up, line protocol is up (connected)
Hardware is Gigabit Ethernet, address is 3c41.0e4f.1782 (bia 3c41.0e4f.1782)
```

Na captura de pacotes, confirme se as sondas ARP são enviadas por GigabitEthernet1/0/2 a cada 30s.

74	01:26:01.357866	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60	Who has 192.168.10.10? Tell 0.0.0.0
75	01:26:01.357988	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60	192.168.10.10 is at b4:96:91:15:84:cb
113	01:26:30.825787	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60	Who has 192.168.10.10? Tell 0.0.0.0
114	01:26:30.825919	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60	192.168.10.10 is at b4:96:91:15:84:cb
138	01:26:59.688695	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60	Who has 192.168.10.10? Tell 0.0.0.0
139	01:26:59.688876	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60	192.168.10.10 is at b4:96:91:15:84:cb
158	01:27:28.392691	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60	Who has 192.168.10.10? Tell 0.0.0.0
159	01:27:28.392910	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60	192.168.10.10 is at b4:96:91:15:84:cb
179	01:27:57.827636	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60	Who has 192.168.10.10? Tell 0.0.0.0
180	01:27:57.827784	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60	192.168.10.10 is at b4:96:91:15:84:cb

Testadores ARP

Na captura do pacote, confirme se o endereço IP do remetente dos testes ARP é 0.0.0.0.

Wireshark · Packet 74 · pciPassthru0

```
> Frame 74: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: 3c:41:0e:4f:17:82 (3c:41:0e:4f:17:82), Dst: IntelCor_15:84:cb (b4:96:91:15:84:cb)
  Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 3c:41:0e:4f:17:82 (3c:41:0e:4f:17:82)
    Sender IP address: 0.0.0.0
    Target MAC address: IntelCor_15:84:cb (b4:96:91:15:84:cb)
    Target IP address: 192.168.10.10
```

Detalhe dos Testes ARP

Problema

Há uma possibilidade de que o recurso de rastreamento de dispositivo IP do Switch Catalyst possa causar um conflito de endereço IP em um PC com Windows quando ele envia uma Prova ARP com um endereço IP de remetente de 0.0.0.0.

Soluções possíveis

Consulte [Troubleshoot Duplicate IP Address 0.0.0.0 Error Messages](#) para obter soluções possíveis.

Aqui estão exemplos de cada solução testada em um laboratório da Cisco para obter mais detalhes.

### 1. Atrasar o envio de provas ARP

Execute `ip device tracking probe delay <1-120>` o comando para atrasar o envio de provas ARP do Switch. Esse comando não permite que um Switch envie uma sonda por <1-120> 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.

Este é um exemplo para configurar o atraso da prova ARP para 10s.

```
Switch (config)#ip device tracking probe delay 10
```

Execute show ip device tracking all o comando para confirmar a configuração do atraso.

```
<#root>
```

```
Switch #show ip device tracking all
Global IP Device Tracking for clients = Enabled
Global IP Device Tracking Probe Count = 3
Global IP Device Tracking Probe Interval = 30

Global IP Device Tracking Probe Delay Interval = 10
```

```
-----
IP Address MAC Address Vlan Interface Probe-Timeout State Source
-----
192.168.10.10 b496.9115.84cb 12 GigabitEthernet1/0/2 30 ACTIVE ARP
```

```
Total number interfaces enabled: 1
Enabled interfaces:
Gi1/0/2
```

## 2. Origem Automática de Configuração para Sondas ARP

Execute ip device tracking probe auto-source fallback <host-ip> <mask> [override] o comando para alterar o endereço IP origem para Probes ARP. Com esse comando, a origem IP dos testadores ARP não é 0.0.0.0, mas é o endereço IP da interface virtual do switch (SVI) na VLAN onde o host reside ou será automaticamente calculada se a SVI não tiver um endereço IP definido.

Este é um exemplo para configurar o <host-ip> para 0.0.0.200.

```
Switch (config)#ip device tracking probe auto-source fallback 0.0.0.200 255.255.255.0 override
```

Padrão 1. O IP do SVI está configurado

Neste documento, como o endereço IP da SVI (o endereço IP da vlan12) está definido para a interface (GigabitEthernet1/0/2) que executa a autenticação MAB, o endereço IP origem para a prova ARP é alterado para 192.168.10.254.

Execute show ip device tracking all o comando para confirmar a configuração da fonte automática.

<#root>

```
Switch #show ip device tracking all
Global IP Device Tracking for clients = Enabled
Global IP Device Tracking Probe Count = 3
Global IP Device Tracking Probe Interval = 30
Global IP Device Tracking Probe Delay Interval = 0
IP Device Tracking Probe Auto Source = Enabled
```

Probe source IP selection order: SVI,Fallback 0.0.0.200 255.255.255.0

```
-----
IP Address MAC Address Vlan Interface Probe-Timeout State Source
-----
192.168.10.10 b496.9115.84cb 12 GigabitEthernet1/0/2 30 ACTIVE ARP
```


Total number interfaces enabled: 1  
Enabled interfaces:  
Gi1/0/2

Na captura de pacotes, confirme se as sondas ARP são enviadas por GigabitEthernet1/0/2 a cada 30s.

```
102 13:31:03.121397 3c:41:0e:4f:17:c1 IntelCor_15:84:cb ARP 60 Who has 192.168.10.10? Tell 192.168.10.254
103 13:31:03.121608 IntelCor_15:84:cb 3c:41:0e:4f:17:c1 ARP 60 192.168.10.10 is at b4:96:91:15:84:cb
123 13:31:33.006355 3c:41:0e:4f:17:c1 IntelCor_15:84:cb ARP 60 Who has 192.168.10.10? Tell 192.168.10.254
124 13:31:33.006502 IntelCor_15:84:cb 3c:41:0e:4f:17:c1 ARP 60 192.168.10.10 is at b4:96:91:15:84:cb
144 13:32:01.534263 3c:41:0e:4f:17:c1 IntelCor_15:84:cb ARP 60 Who has 192.168.10.10? Tell 192.168.10.254
145 13:32:01.534377 IntelCor_15:84:cb 3c:41:0e:4f:17:c1 ARP 60 192.168.10.10 is at b4:96:91:15:84:cb
163 13:32:30.386323 3c:41:0e:4f:17:c1 IntelCor_15:84:cb ARP 60 Who has 192.168.10.10? Tell 192.168.10.254
164 13:32:30.386325 IntelCor_15:84:cb 3c:41:0e:4f:17:c1 ARP 60 192.168.10.10 is at b4:96:91:15:84:cb
182 13:32:59.104148 3c:41:0e:4f:17:c1 IntelCor_15:84:cb ARP 60 Who has 192.168.10.10? Tell 192.168.10.254
183 13:32:59.104318 IntelCor_15:84:cb 3c:41:0e:4f:17:c1 ARP 60 192.168.10.10 is at b4:96:91:15:84:cb
```

Testadores ARP

Na captura de pacotes, confirme se o endereço IP do remetente dos testes ARP é 192.168.10.254, que é o IP do SVI (vlan 12).

 Wireshark · Packet 102 · pciPassthru0

```
> Frame 102: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: 3c:41:0e:4f:17:c1 (3c:41:0e:4f:17:c1), Dst: IntelCor_15:84:cb (b4:96:91:15:84:cb)
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: 3c:41:0e:4f:17:c1 (3c:41:0e:4f:17:c1)
  Sender IP address: 192.168.10.254
  Target MAC address: IntelCor_15:84:cb (b4:96:91:15:84:cb)
  Target IP address: 192.168.10.10
```

Detalhe dos Testes ARP

Padrão 2. O IP do SVI não está configurado

Neste documento, como o destino da prova ARP é 192.168.10.10/24, se o endereço IP da SVI não estiver configurado, o endereço IP origem é 192.168.10.200.

Exclua o endereço IP do SVI.

```
Switch (config)#int vlan 12  
Switch (config-if)#no ip address
```

Execute show ip device tracking all o comando para confirmar a configuração da fonte automática.

<#root>

```
Switch #show ip device tracking all  
Global IP Device Tracking for clients = Enabled  
Global IP Device Tracking Probe Count = 3  
Global IP Device Tracking Probe Interval = 30  
Global IP Device Tracking Probe Delay Interval = 0  
IP Device Tracking Probe Auto Source = Enabled
```

**Probe source IP selection order: SVI,Fallback 0.0.0.200 255.255.255.0**

```
-----  
IP Address MAC Address Vlan Interface Probe-Timeout State Source  
-----  
192.168.10.10 b496.9115.84cb 12 GigabitEthernet1/0/2 30 ACTIVE ARP
```

```
Total number interfaces enabled: 1  
Enabled interfaces:  
Gi1/0/2
```

Na captura de pacotes, confirme se as sondas ARP são enviadas por GigabitEthernet1/0/2 a cada 30s.

176	13:39:00.167788	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60	Who has 192.168.10.10? Tell 192.168.10.200
177	13:39:00.167975	IntelCor_15:84:cb	3c:41:0e:4f:17:82	ARP	60	192.168.10.10 is at b4:96:91:15:84:cb
196	13:39:29.131512	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60	Who has 192.168.10.10? Tell 192.168.10.200
197	13:39:29.131616	IntelCor_15:84:cb	3c:41:0e:4f:17:82	ARP	60	192.168.10.10 is at b4:96:91:15:84:cb
217	13:39:58.724683	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60	Who has 192.168.10.10? Tell 192.168.10.200
218	13:39:58.724858	IntelCor_15:84:cb	3c:41:0e:4f:17:82	ARP	60	192.168.10.10 is at b4:96:91:15:84:cb
238	13:40:27.746620	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60	Who has 192.168.10.10? Tell 192.168.10.200
239	13:40:27.746784	IntelCor_15:84:cb	3c:41:0e:4f:17:82	ARP	60	192.168.10.10 is at b4:96:91:15:84:cb
257	13:40:57.240571	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60	Who has 192.168.10.10? Tell 192.168.10.200
258	13:40:57.240702	IntelCor_15:84:cb	3c:41:0e:4f:17:82	ARP	60	192.168.10.10 is at b4:96:91:15:84:cb
278	13:41:27.193284	3c:41:0e:4f:17:82	IntelCor_15:84:cb	ARP	60	Who has 192.168.10.10? Tell 192.168.10.200
279	13:41:27.193419	IntelCor_15:84:cb	3c:41:0e:4f:17:82	ARP	60	192.168.10.10 is at b4:96:91:15:84:cb

*Testadores ARP*

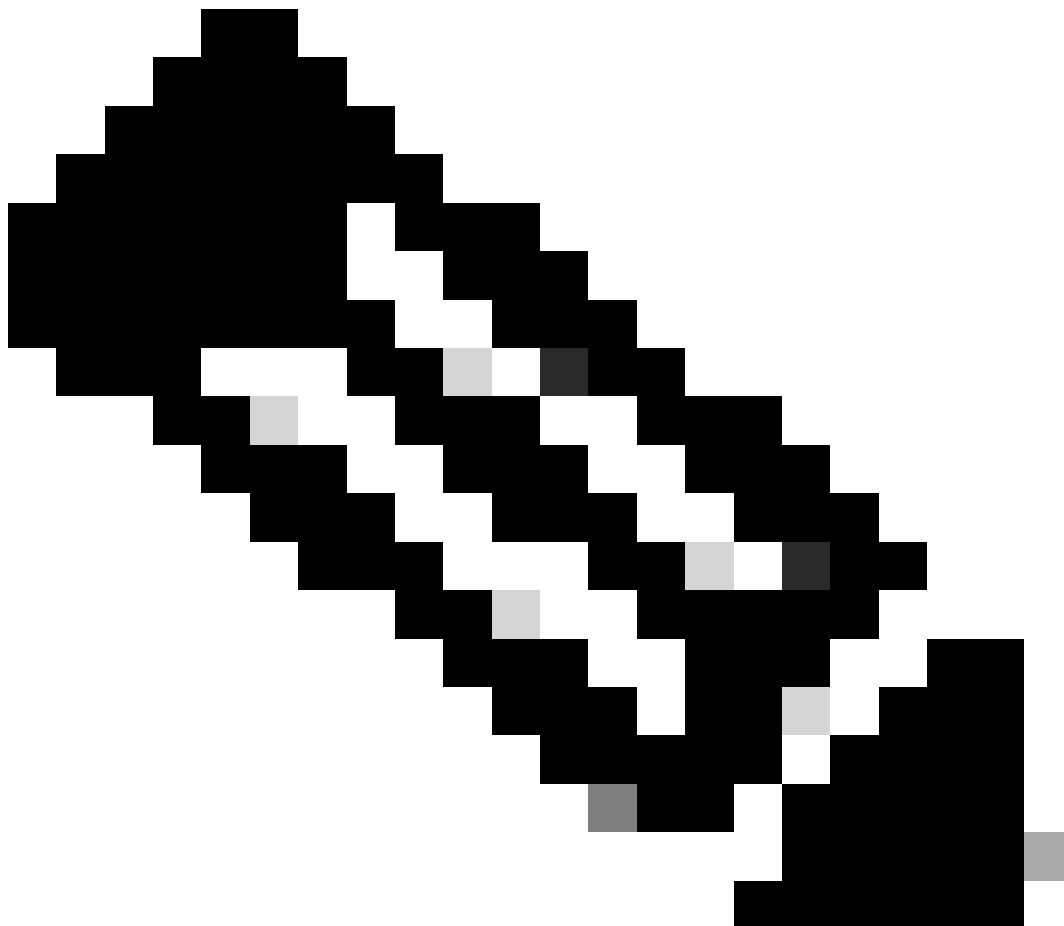
Na captura de pacotes, confirme se o endereço IP do remetente dos testes ARP foi alterado para 192.168.10.200.

```
> Frame 176: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: 3c:41:0e:4f:17:82 (3c:41:0e:4f:17:82), Dst: IntelCor_15:84:cb (b4:96:91:15:84:cb)
  Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 3c:41:0e:4f:17:82 (3c:41:0e:4f:17:82)
    Sender IP address: 192.168.10.200
    Target MAC address: IntelCor_15:84:cb (b4:96:91:15:84:cb)
    Target IP address: 192.168.10.10
```

*Detalhe dos Testes ARP*

### 3. Desabilite Forçadamente o Rastreamento de Dispositivos IP

Execute o **ip device tracking maximum 0** comando para desabilitar o rastreamento de dispositivo IP.



---

**Observação:** esse comando não desabilita realmente o rastreamento de dispositivos IP, mas limita o número de hosts rastreados a zero.

---

```
Switch (config)#int g1/0/2
Switch (config-if)#ip device tracking maximum 0
```

Execute show ip device tracking all o comando para confirmar o status do rastreamento do dispositivo IP em GigabitEthernet1/0/2.

```
Switch #show ip device tracking all
Global IP Device Tracking for clients = Enabled
Global IP Device Tracking Probe Count = 3
Global IP Device Tracking Probe Interval = 30
Global IP Device Tracking Probe Delay Interval = 0
```

```
-----
IP Address MAC Address Vlan Interface Probe-Timeout State Source
-----
```

```
Total number interfaces enabled: 1
Enabled interfaces:
Gi1/0/2
```

Referência

[Solucionar problemas de mensagens de erro de endereço IP duplicado 0.0.0.0](#)

[Verificar as operações do dispositivo IPDT](#)

## 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.