Überprüfung der IP-Geräte-Nachverfolgung nach MAB-Konfiguration auf dem Switch

Inhalt

Einleitung

In diesem Dokument wird das Verhalten der IP-Geräteverfolgung nach der MAB-Konfiguration und mögliche Lösungen für Kommunikationsprobleme nach der MAB-Authentifizierung beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfiguration der Cisco Identity Services Engine
- Konfiguration des Cisco Catalyst

Verwendete Komponenten

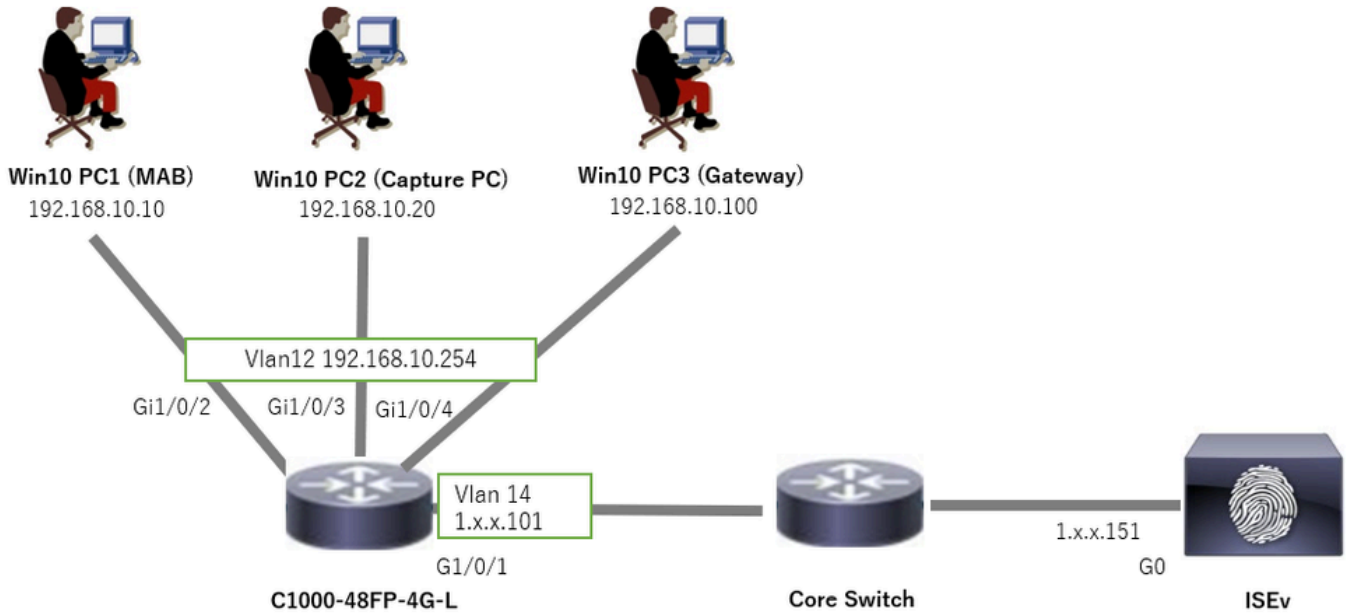
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Identity Services Engine Virtual 3.3 Patch 1
- C1000-48FP-4G-L 15,2(7)E9

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Diagramm

In diesem Dokument wird die Konfiguration und Verifizierung für die MAB-Authentifizierung in diesem Diagramm vorgestellt.



Netzwerkdiagramm

Hintergrundinformationen

Obwohl die MAB-Authentifizierung erfolgreich war, kann das Gateway (Win10 PC3) nach dem Neustart (oder dem Trennen und Neuanschließen des Kabels) von Win10 PC1 nicht erfolgreich

gepingt werden. Dieses unerwartete Verhalten ist auf einen IP-Adresskonflikt auf Win10 PC1 zurückzuführen.
Die IP-Geräteverfolgung und ihre ARP-Tests sind auf der Schnittstelle, die als MAB konfiguriert ist, standardmäßig aktiviert. Wenn Windows-PCs mit einem Catalyst Switch verbunden sind und die IP-Geräteverfolgung aktiviert ist, besteht die Möglichkeit, dass die Windows-Seite einen IP-Adresskonflikt erkennt. Dies tritt auf, da ein ARP-Prüfpunkt (mit der Absender-IP-Adresse 0.0.0.0) während des Erkennungsfensters dieses Mechanismus empfangen wird und als IP-Adresskonflikt behandelt wird.

Konfiguration

Dieses Konfigurationsbeispiel veranschaulicht das Verhalten der IP-Geräteverfolgung nach der MAB-Konfiguration.

Konfiguration in C1000

Dies ist die minimale Konfiguration in C1000 CLI.

```
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
```

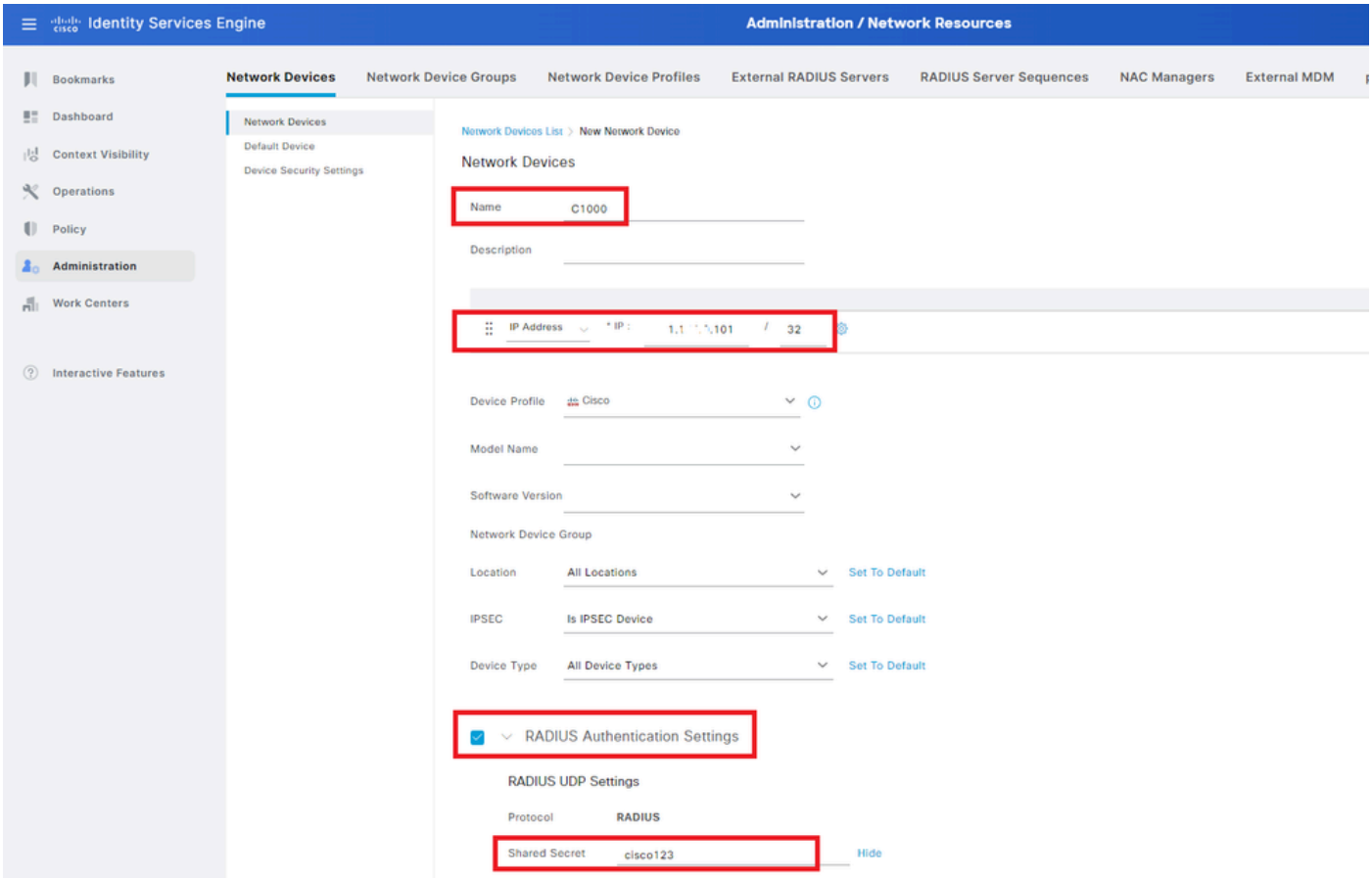
```
authentication port-control auto
spanning-tree portfast edge
mab

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

Konfiguration in der ISE

Schritt 1: Gerät hinzufügen

Navigieren Sie zu Administration > Network Devices, und klicken Sie auf die Schaltfläche Add, um ein C1000-Gerät hinzuzufügen.

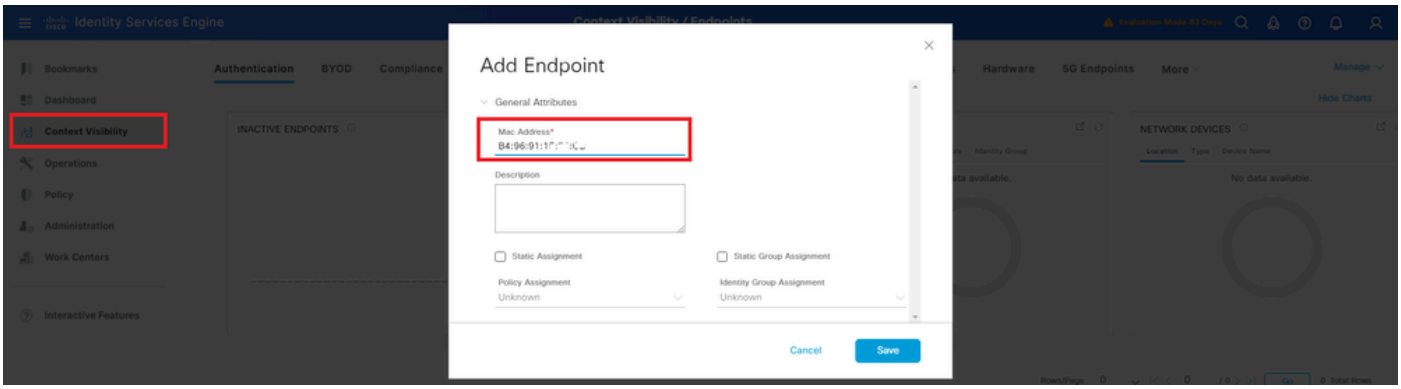
- Name: C1000
- IP-Adresse: 1.x.x.101



Gerät hinzufügen

Schritt 2: Endpunkt hinzufügen

Navigieren Sie zu Context Visibility > Endpoints, und klicken Sie auf die Schaltfläche Add (Hinzufügen), um MAC of Endpoint hinzuzufügen.

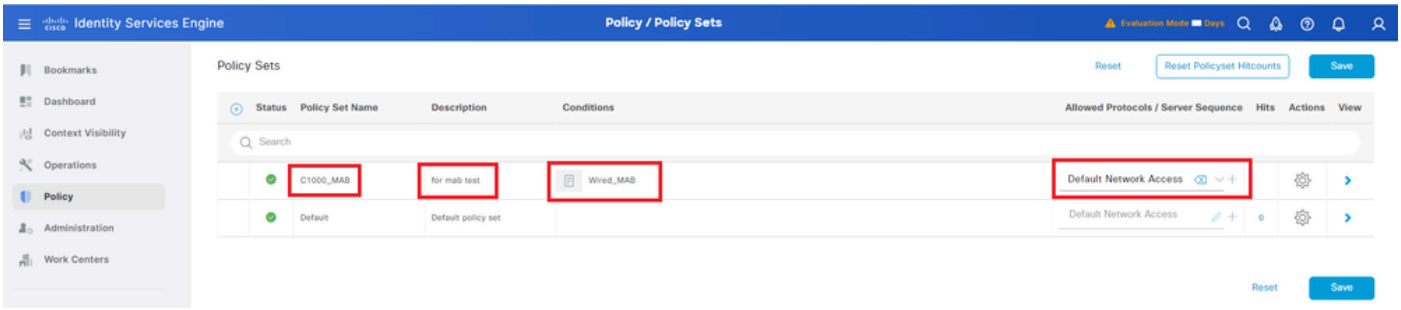


Endpunkt hinzufügen

Schritt 3: Policy Set hinzufügen

Navigieren Sie zu Policy > Policy Sets, und klicken Sie auf +, um einen Policy Set hinzuzufügen.

- Richtliniensatzname: C1000_MAB
- Beschreibung : for mab test
- Bedingungen: Wired_MAB
- Zulässige Protokolle/Serversequenz: Standard-Netzwerkzugriff

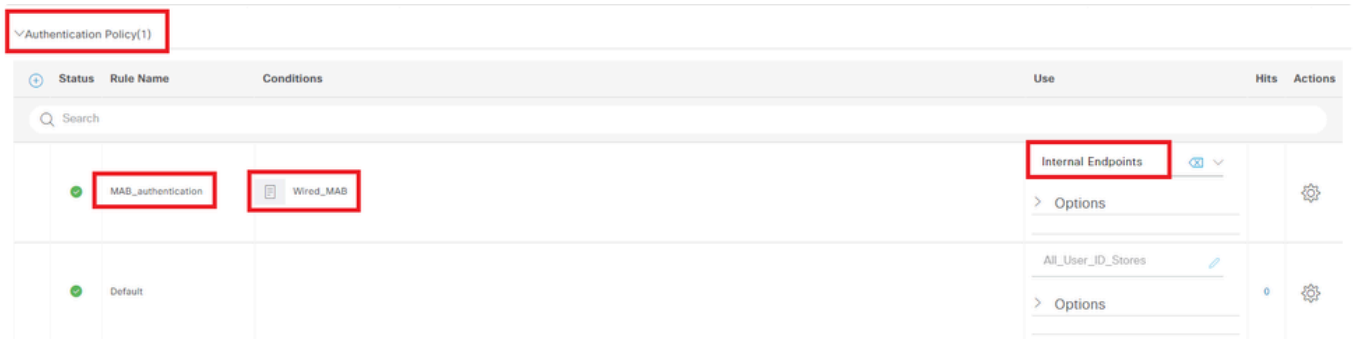


Policy Set hinzufügen

Schritt 4: Authentifizierungsrichtlinie hinzufügen

Navigieren Sie zu Policy Sets, und klicken Sie auf C1000_MAB, um eine Authentifizierungsrichtlinie hinzuzufügen.

- Regelname: MAB_authentication
- Bedingungen: Wired_MAB
- Verwendung: Interne Endgeräte

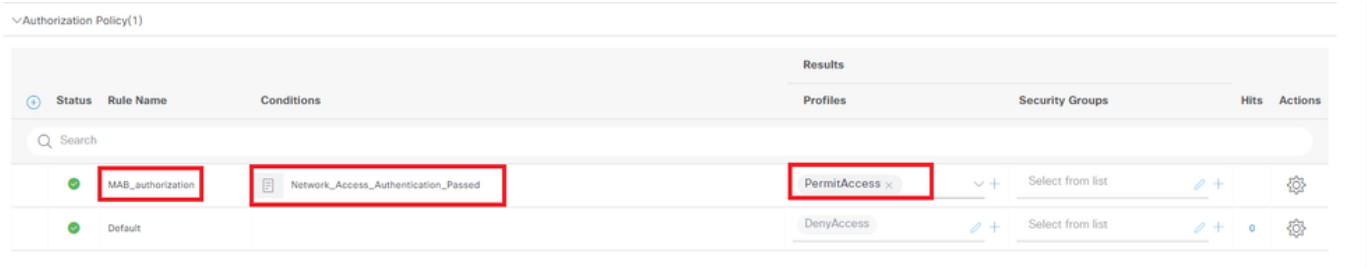


Authentifizierungsrichtlinie hinzufügen

Schritt 5: Autorisierungsrichtlinie hinzufügen

Navigieren Sie zu Policy Sets, und klicken Sie auf C1000_MAB, um eine Autorisierungsrichtlinie hinzuzufügen.

- Regelname: MAB_Authorization
- Bedingungen: Network_Access_Authentication_Passed
- Ergebnisse : PermitAccess



Autorisierungsrichtlinie hinzufügen

Überprüfung

Vor der Konfiguration von MAB

Führen Sie den Befehl ausshow ip device tracking all, um zu bestätigen, dass die Funktion zur IP-Geräteverfolgung deaktiviert ist.

<#root>

Switch #

show ip device tracking all

Global IP Device Tracking for clients =

Disabled

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

Nach der Konfiguration von MAB

Schritt 1: Vor MAB-Authentifizierung

Führen Sie den Befehl ausshow ip device tracking all, um zu bestätigen, dass die IP-Geräteverfolgungsfunktion aktiviert ist.

<#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
```

Schritt 2: Nach MAB-Authentifizierung

Initialisieren Sie die MAB-Authentifizierung von Win10 PC1, und führen Sie den Befehl aus, um den Status der IP-Geräteverfolgung auf GigabitEthernet1/0/2 zu bestätigenshow ip device tracking all.

```
<#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
```

Schritt 3: Authentifizierungssitzung bestätigen

Führen Sie den Befehl ausshow authentication sessions interface GigabitEthernet1/0/2 details, um die MAB-Authentifizierungssitzung zu bestätigen.

<#root>

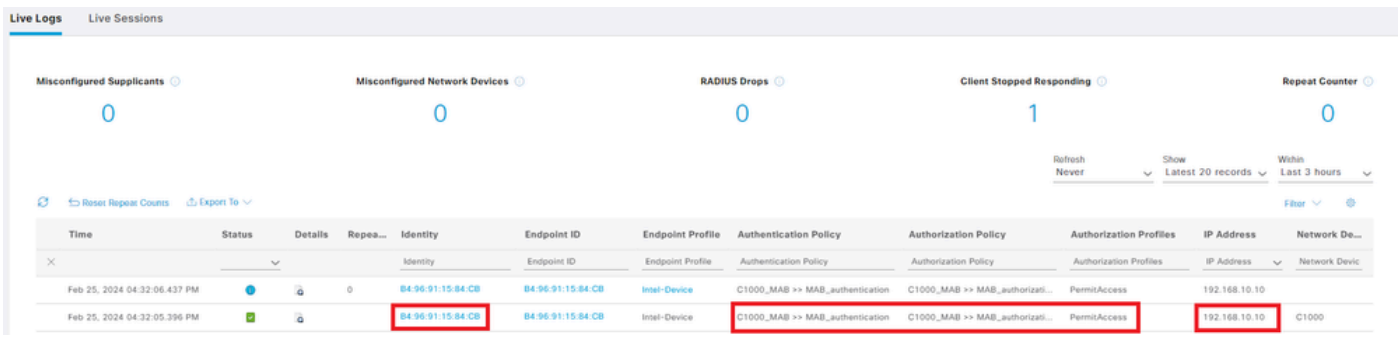
Switch #

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: 01C2006500000001D62945338
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
```

Schritt 4: RADIUS-Live-Protokoll bestätigen

Navigieren Sie zu **Operations > RADIUS > Live Logs (Vorgänge > RADIUS > Live**-Protokolle) in der ISE-GUI, und bestätigen Sie das Live-Protokoll für die MAB-Authentifizierung.



Schritt 5: Paketdetails der IP-Geräteverfolgung bestätigen

Führen Sie show interfaces GigabitEthernet1/0/2 command aus, um die MAC-Adresse von GigabitEthernet1/0/2 zu bestätigen.

<#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)
```

Überprüfen Sie bei der Paketerfassung, ob alle 30 Sekunden ARP-Tests von GigabitEthernet1/0/2 gesendet werden.

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	IntelCor_15:84:cb	3c:41:0e:4f:17:82	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	IntelCor_15:84:cb	3c:41:0e:4f:17:82	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	IntelCor_15:84:cb	3c:41:0e:4f:17:82	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	IntelCor_15:84:cb	3c:41:0e:4f:17:82	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	IntelCor_15:84:cb	3c:41:0e:4f:17:82	ARP	60 192.168.10.10 is at b4:96:91:15:84:cb

ARP-Tests

Bestätigen Sie in der Paketerfassung, dass die Absender-IP-Adresse von ARP Probes 0.0.0.0 lautet.

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)
v 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
```

Details zu ARP-Tests

Problem

Es besteht die Möglichkeit, dass die IP-Geräteverfolgungsfunktion des Catalyst Switches einen IP-Adressenkonflikt auf einem Windows-PC verursachen kann, wenn ein ARP-Prüfpunkt mit der Absender-IP-Adresse 0.0.0.0 gesendet wird.

Mögliche Lösungen

Informationen zu möglichen Lösungen finden Sie unter Fehlerbehebung bei doppelten IP-Adressen 0.0.0.0.
Hier finden Sie Beispiele für jede Lösung, die in einem Cisco Lab getestet wurde, um weitere Details zu erhalten.

1. Verzögern des Sendens von ARP-Datensammlungen

Führen Sie den Befehl ausip device tracking probe delay <1-120>, um das Senden von ARP-Tests von Switch zu verzögern. Mit diesem Befehl kann ein Switch bei Erkennung eines Verbindungs-UP/Flaps <1-120> Sekunden lang keinen Prüfpunkt senden. Dadurch wird die Wahrscheinlichkeit minimiert, dass der Prüfpunkt gesendet wird, während der Host auf der anderen Seite des Links nach doppelten IP-Adressen sucht.

Dies ist ein Beispiel zur Konfiguration der Verzögerung des ARP-Tests für 10 Sekunden.

Switch (config)#ip device tracking probe delay 10

Führen Sie den Befehl ausshow ip device tracking all, um die Einstellung der Verzögerung zu bestätigen.

<#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. Automatische Konfigurationsquelle für ARP-Tests

Führen Sie den Befehl ausip device tracking probe auto-source fallback <host-ip> <mask> [override], um die Quell-IP-Adresse für ARP-Tests zu ändern. Mit diesem Befehl ist die IP-Quelle von ARP Probes nicht 0.0.0.0, sondern die IP-Adresse von Switch Virtual Interface (SVI) im VLAN, in dem sich der Host befindet. Andernfalls wird sie automatisch berechnet, wenn für die SVI keine IP-Adresse festgelegt ist.

Dies ist ein Beispiel für die Konfiguration von <host-ip> in 0.0.0.200.

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

Muster 1. IP der SVI ist konfiguriert

Da in diesem Dokument die SVI-IP-Adresse (die IP-Adresse von vlan12) für die Schnittstelle (GigabitEthernet1/0/2) festgelegt ist, die die MAB-Authentifizierung durchführt, wird die Quell-IP-Adresse für den ARP-Test in 192.168.10.254 geändert.

Führen Sie den Befehl ausshow ip device tracking all, um die Einstellung der automatischen Quelle zu bestätigen.

<#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

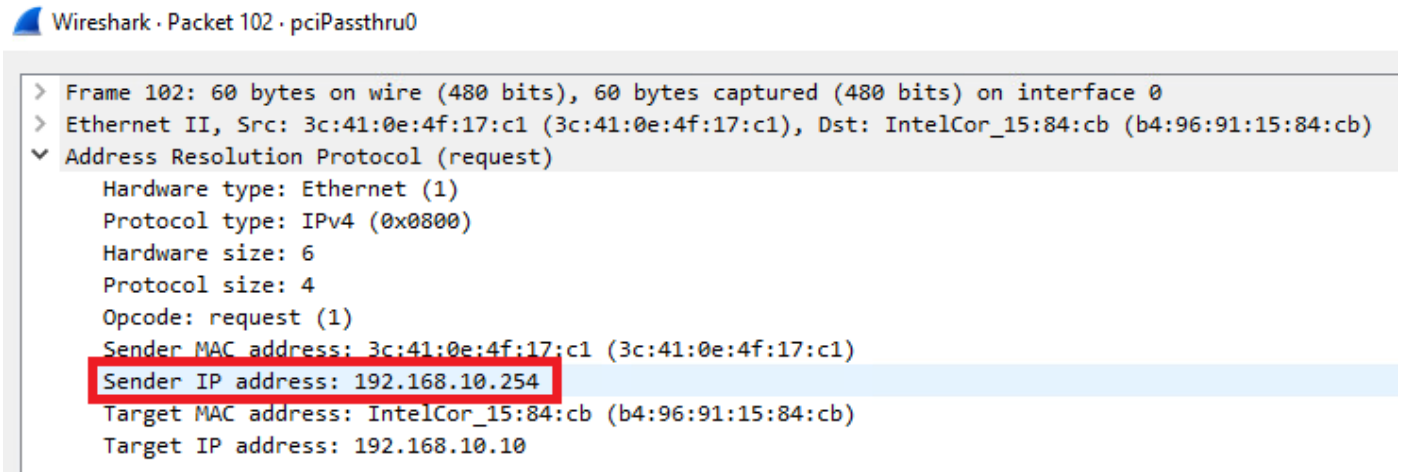
```
-------------------------------------------------------------------------------------------
IP Address MAC Address Vlan Interface Probe-Timeout State Source
-------------------------------------------------------------------------------------------
192.168.10.10 b496.9115.84cb 12 GigabitEthernet1/0/2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

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

Überprüfen Sie bei der Paketerfassung, ob alle 30 Sekunden ARP-Tests von GigabitEthernet1/0/2 gesendet werden.

```
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
```

ARP-Tests

Stellen Sie bei der Paketerfassung sicher, dass die Absender-IP-Adresse von ARP Probes 192.168.10.254 ist. Dies ist die IP von SVI (VLAN 12).



Details zu ARP-Tests

Muster 2. IP der SVI ist nicht konfiguriert

Da das Ziel für den ARP-Test in diesem Dokument 192.168.10.10/24 lautet, ist die Quell-IP-Adresse 192.168.10.200, wenn die SVI-IP-Adresse nicht konfiguriert ist.

Löschen Sie die IP-Adresse von SVI.

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

Führen Sie den Befehl ausshow ip device tracking all, um die Einstellung der automatischen Quelle zu bestätigen.

<#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

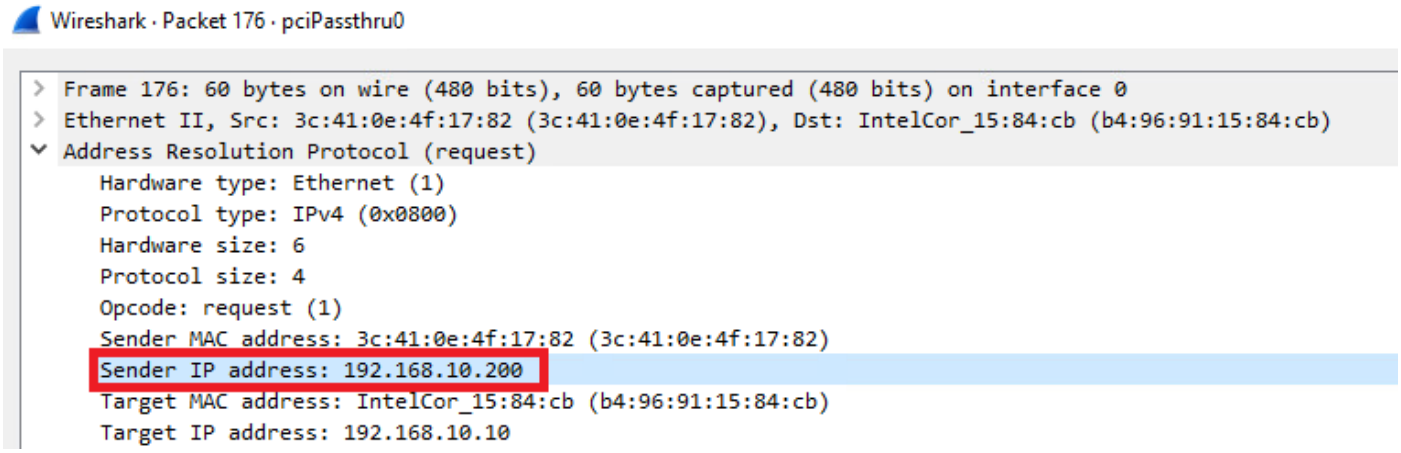
```
---------------------------------------------------------------------------------------------
IP Address MAC Address Vlan Interface Probe-Timeout State Source
---------------------------------------------------------------------------------------------
192.168.10.10 b496.9115.84cb 12 GigabitEthernet1/0/2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

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

Überprüfen Sie bei der Paketerfassung, ob alle 30 Sekunden ARP-Tests von GigabitEthernet1/0/2 gesendet werden.

```
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
```

ARP-Tests

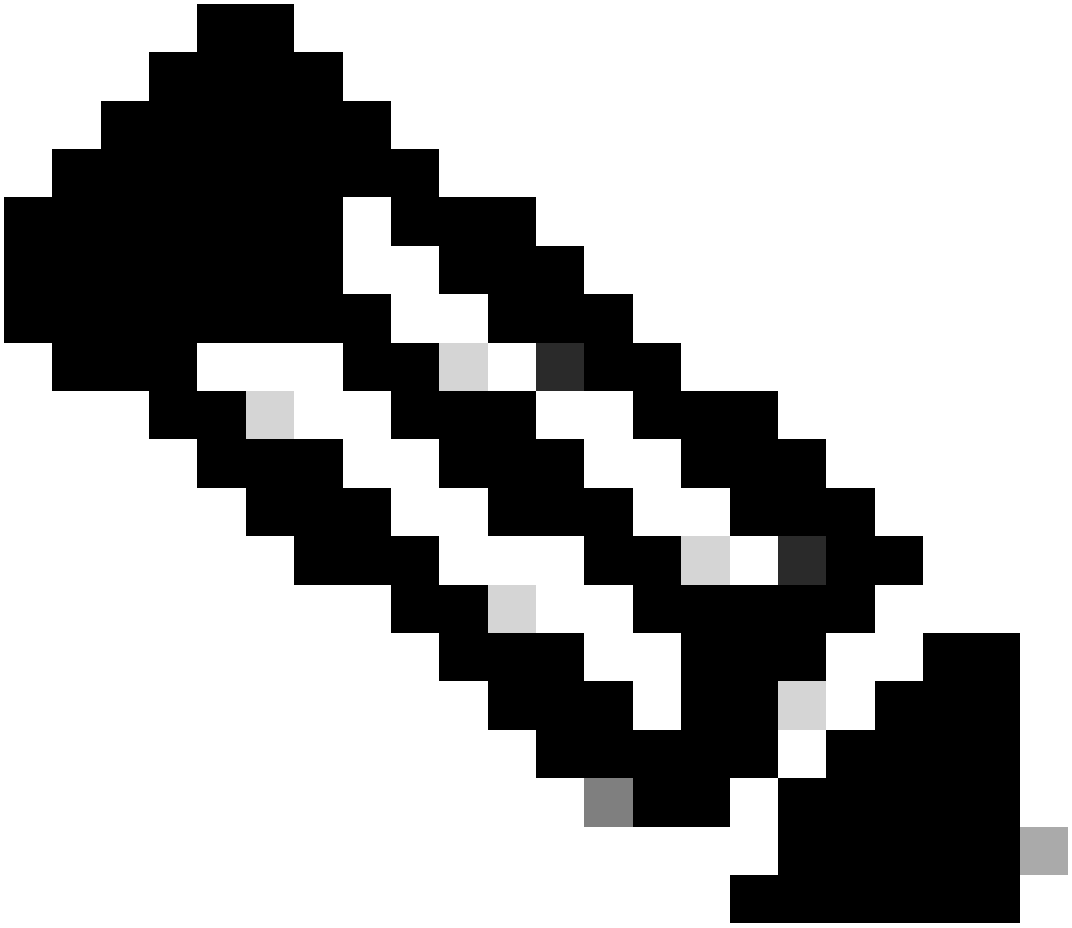
Überprüfen Sie in der Paketerfassung, ob die Absender-IP-Adresse von ARP Probes in 192.168.10.200 geändert wurde.



Details zu ARP-Tests

3. IP-Geräteverfolgung zwangsweise deaktivieren

Führen Sie einen **ip device tracking maximum 0** Befehl aus, um die IP-Geräteverfolgung zu deaktivieren.



Hinweis: Mit diesem Befehl wird die IP-Geräteverfolgung nicht wirklich deaktiviert, die Anzahl der verfolgten Hosts wird jedoch auf Null beschränkt.

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

Führen Sie show ip device tracking all command aus, um den Status der IP-Geräteverfolgung auf GigabitEthernet1/0/2 zu bestätigen.

```
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

Referenz

Fehlerbehebung bei doppelten IP-Adressen 0.0.0.0-Fehlermeldungen

Überprüfung des Betriebs des IPDT-Geräts

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.