Verify IP Device Tracking Post-MAB Configuration on Switch

Contents

Introduction
<u>Prerequisites</u>
Requirements
Components Used
<u>Diagram</u>
Background Information
<u>Configuration</u>
Configuration in C1000
Configuration in ISE
Step 1. Add Device
Step 2. Add Endpoint
Step 3. Add Policy Set
Step 4. Add Authentication Policy
Step 5. Add Authorization Policy
<u>Verify</u>
Before Configuration of MAB
After Configuration of MAB
Step 1. Before MAB Authentication
Step 2. After MAB Authentication
Step 3. Confirm Authentication Session
Step 4. Confirm Radius Live Log
Step 5. Confirm Packet Detail of IP Device Tracking
Problem
Possible Solutions
1. Delay the Sending of ARP Probes
2. Config Auto-Source for ARP Probes
Pattern 1. IP of SVI is Configured
Pattern 2. IP of SVI is Not Configured
3. Forcibly Disable IP Device Tracking
<u>Reference</u>

Introduction

This document describes the behavior of IP device tracking after MAB config and possible solutions for communication issue after MAB authentication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Configuration of Cisco Identity Services Engine
- Configuration of Cisco Catalyst

Components Used

The information in this document is based on these software and hardware versions:

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

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. If your network is live, ensure that you understand the potential impact of any command.

Diagram

This document introduces the configuration and verification for MAB authentication on this diagram.



Network Diagram

Background Information

Even though MAB authentication succeeds, after rebooting (or unplugging and replugging the cable) Win10 PC1, it cannot ping the gateway (Win10 PC3) successfully. This unexpected behavior is due to an IP address conflict on Win10 PC1.

IP device tracking and its ARP probes is enabled by default on the interface which is configured MAB. When Windows PC are connected to a Catalyst Switch with IP device tracking enabled, there is a possibility that the Windows side detects an IP address conflict. This occurs because an ARP Probe (with a sender IP address of 0.0.0.0) is received during the detection window of this mechanism, it is treated as an IP address conflict.

Configuration

This configuration example demonstrates the behavior of IP device tracking after MAB configuration.

Configuration in C1000

This is the minimal configuration 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

Configuration in ISE

Step 1. Add Device

Navigate to Administration > Network Devices, click Add button to add C1000 device.

- Name : C1000
- **IP Address** : 1.x.x.101

≡	dentity Services E	Engine		Administration / Network Resources						
Щ	Bookmarks	Network Devices	Network Devic	e Groups N	etwork Device Profiles	External RADIUS S	Servers	RADIUS Server Sequences	NAC Managers	External MDM
11	Dashboard	Network Devices		Network Devices Lis	st > New Network Device					
11	Context Visibility	Default Device Device Security Settin	105	Network Devic	ces					
*	Operations		Ĩ	Name	C1000					
0	Policy			Description						
20	Administration			- Janihoan						
ń	Work Centers			IP Addres	s tip:	101 / 22	8			
(I			52 0	Ŷ			
(3)	Interactive Features			Device Profile	tte Cisco	× ()				
				Model Name		~				
				Software Versio	n	~				
				Network Device	Group					
				Location	All Locations	~	Set To Defau	ult		
				IPSEC	Is IPSEC Device	~	Set To Defau	ult		
				Device Type	All Device Types	~	Set To Defau	ult		
				🗹 🗸 RAD	IUS Authentication Setti	ngs				
				RADIUS	UDP Settings					
				Protocol	RADIUS					
				Shared S	iecret cisco123		Hide			

Add Device

Step 2. Add Endpoint

Navigate to **Context Visibility > Endpoints**, click **Add** button to add MAC of Endpoint.

\equiv $ ightarrow$ Identity Services Engine	Context Visibility / Endnoints	🛦 transmissi tanan 20 part Q 🛕 🛞 Q
Ecokmarks Authentication BYOD Compilat	Add Endpoint	× Hardware SG Endpoints More - Manage -
2 Dashboard	 General Attributes 	Hide Charts
Context Visibility	Mac Address* B4:96:91:17:17:00	C NETWORK DEVICES C
* Operations	Description	ata available. No data available.
Policy		
Administration		
AII Work Centers	Static Assignment Static Group Assignment	
	Policy Assignment Identity Group Assignment	
Interactive Features	Unknown Unknown U	
	Cancel	

Add Endpoint

Step 3. Add Policy Set

Navigate to **Policy > Policy Sets**, click + to add a policy set.

- Policy Set Name : C1000_MAB
- **Description** : for mab test
- Conditions : Wired_MAB

• Allowed Protocols / Server Sequence : Default Network Access

≡	admite Identity Services En	gine					Policy / Policy Sets		A Evan	ation Mode	🔲 Days	۹	۵	0	۵	۹
н	Bookmarks	Policy	Sets						Reset	Rese	t Policyset	Hitcou	unts		Save	
51	Dashboard	۲	Status	Policy Set Name	Description		Conditions	Allowe	d Protoco	ls / Serve	r Sequend	e Hi	its A	ctions	View	
명	Context Visibility	Q	Search													
*	Operations		•	C1000 MAB	for main text	- 1	E Wred MAR	Defau	It Networl	Access	a v4			<i>1</i> 83		
0	Policy		- 1											181	· ·	
8.	Administration		٥	Default	Default policy set			Defau	lt Network	Access	+	0		¢۶	>	
d.	Work Centers															
												Ret	set		Save	

Add Policy Set

r

Step 4. Add Authentication Policy

Navigate to Policy Sets, click C1000_MAB to add an authentication policy.

- Rule Name : MAB_authentication
- Conditions : Wired_MAB
- Use : Internal Endpoints

٦

Hits Actio	ions
403	¢
• \$}	-
	• 40

Add Authentication Policy

Step 5. Add Authorization Policy

Navigate to Policy Sets, click C1000_MAB to add an authorization policy.

- **Rule Name** : MAB_authorization
- Conditions : Network_Access_Authentication_Passed
- **Results** : PermitAccess

		Results			
(+) Status Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Q Search					
MAB_authorization	Network_Access_Authentication_Passed	PermitAccess ×	V + Select from list	0+	¢۵
O Default		DenyAccess	Select from list		(2)

Add Authorization Policy

Verify

Before Configuration of MAB

Run show ip device tracking all command to confirm that IP device tracking feature is disabled.

<#root>
Switch #
show ip device tracking all
Global IP Device Tracking for clients =
Disabled
IP Address MAC Address Vlan Interface Probe-Timeout State Source

After Configuration of MAB

Step 1. Before MAB Authentication

Run show ip device tracking all command to confirm that IP device tracking feature is enabled.

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

Step 2. After MAB Authentication

Initialize MAB authentication from Win10 PC1 and run show ip device tracking all command to confirm the status of IP device tracking on 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

Step 3. Confirm Authentication Session

Run show authentication sessions interface GigabitEthernet1/0/2 details command to confirm the MAB authentication session.

<#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: 0x000000F
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
```

Step 4. Confirm Radius Live Log

Navigate to **Operations > RADIUS > Live Logs**in ISE GUI, confirm the live log for MAB authentication.

velogs Live Sessions												
Misconfigured Supplicants 🕓		Misconfigured Network Devices ()				RADIU	IS Drops 🕕	Client Stopped Resp		Repeat Counter 🕕		
0			0	0 0			1			0		
හි 🖯 Reset Repear Counts රැගින	iori To 🗸								Never V Latest	20 records 🧹	Within Last 3 hours Filter	
Time	Status	Details	Repea	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address	Network De	
×	~			Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address	Network Devic	
Feb 25, 2024 04:32:06.437 PM	•	à	0	84:96:91:15:84:CB	84:96:91:15:84:CB	Intel-Device	C1000_MAB >> MAB_authentication	C1000_MAB >> MAB_authorizati	PermitAccess	192.168.10.10		
Feb 25, 2024 04:32:05.396 PM		à		84:96:91:15:84:C8	84:96:91:15:84:CB	Intel-Device	C1000_MAB >> MAB_authentication	C1000_MAB >> MAB_authorizati	PermitAccess	192.168.10.10	C1000	

Step 5. Confirm Packet Detail of IP Device Tracking

Run show interfaces GigabitEthernet1/0/2 command to confirm the MAC address of 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)

In the packet capture, confirm that ARP probes are sent by GigabitEthernet1/0/2 every 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	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 Probes

In the packet capture, confirm that the sender IP address of ARP Probes are 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: 0.0.00
    Target MAC address: IntelCor_15:84:cb (b4:96:91:15:84:cb)
    Target IP address: 192.168.10.10
```

Detail of ARP Probes

Problem

There is a possibility that the IP device tracking feature of the Catalyst Switch could cause an IP address conflict on a Windows PC when it sends an ARP Probe with a sender IP address of 0.0.0.0.

Possible Solutions

Please refer to <u>Troubleshoot Duplicate IP Address 0.0.0.0 Error Messages</u> for possible solutions. Here are examples of each solution tested in a Cisco lab for further details.

1. Delay the Sending of ARP Probes

Run ip device tracking probe delay <1-120> command to delay the sending of ARP probes from Switch. This command does not allow a Switch to send a probe for <1-120> seconds when it detects a link UP/flap, which minimizes the possibility to have the probe sent while the host on the other side of the link checks for duplicate IP addresses.

This is an example to config the delay of ARP probe for 10s.

Switch (config)#ip device tracking probe delay 10

Run show ip device tracking all command to confirm the setting of delay.

<#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
```

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

2. Config Auto-Source for ARP Probes

Run ip device tracking probe auto-source fallback <host-ip> <mask> [override] command to change the source IP address for ARP Probes. With this command, the IP source of ARP Probes is not be 0.0.0.0, but it is the IP address of Switch Virtual Interface (SVI) in the VLAN where the host resides, or it is automatically calculated if the SVI does not have an IP address set.

This is an example to config the $\langle \text{host-ip} \rangle$ to 0.0.0200.

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

Pattern 1. IP of SVI is Configured

In this document, since the SVI IP address (the IP address of vlan12) is set for the interface (GigabitEthernet1/0/2) performing MAB authentication, the source IP address for the ARP probe is changed to 192.168.10.254.

Run show ip device tracking all command to confirm the setting of auto source.

<#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
```

In the packet capture, confirm that ARP probes are sent by GigabitEthernet1/0/2 every 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

ARP Probes

In the packet capture, confirm that the sender IP address of ARP Probes are 192.168.10.254 which is the IP of 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 IP address: 3c:41:0e:4f:17:c1 (3c:41:0e:4f:17:c1)
Sender IP address: 192.168.10.254
Target IP address: IntelCor_15:84:cb (b4:96:91:15:84:cb)
Target IP address: 192.168.10.10
```

Detail of ARP Probes

Pattern 2. IP of SVI is Not Configured

In this document, as the destination for the ARP probe is 192.168.10.10/24, if the SVI IP address is not configured, the source IP address is 192.168.10.200.

Delete the IP address of SVI.

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

Run show ip device tracking all command to confirm the setting of auto source.

<#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

In the packet capture, confirm that ARP probes are sent by GigabitEthernet1/0/2 every 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

ARP Probes

In the packet capture, confirm that the sender IP address of ARP Probes are changed to 192.168.10.200.

Wireshark · Packet 176 · pciPassthru0

```
> 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
```

Detail of ARP Probes

3. Forcibly Disable IP Device Tracking

Run ip device tracking maximum 0 command to disable IP device tracking.



Note: This command does not truly disable IP device tracking, but it does limit the number of tracked hosts to zero.

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

Run show ip device tracking all command to confirm the status of IP device tracking on GigabitEthernet1/0/2.

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

Reference

Troubleshoot Duplicate IP Address 0.0.0.0 Error Messages

Verify IPDT Device Operations