验证交换机上的IP设备跟踪MAB后配置

目录 <u>简介</u> 先决条件 要求 使用的组件 <u>图解</u> <u>背景信息</u> 配置 <u>C1000中的配置</u> <u>ISE中的配置</u> <u>步骤1:添加设备</u> <u>第二步:添加终端</u> <u>第三步:添加策略集</u> <u>第四步:添加身份验证策略</u> <u>第五步:添加授权策略</u> 验证 配置MAB之前 配置MAB之后 步骤1:在MAB身份验证之前 <u>第二步:在MAB身份验证之后</u> <u>第三步:确认身份验证会话</u> <u>第四步:确认Radius实时日志</u> <u>第五步:确认IP设备跟踪的数据包详细信息</u> 问题 可能的解决方案 <u>1. 延迟ARP探测的发送</u> 2. ARP探测的配置自动源 模式1。已配置SVI的IP <u>模式2.未配置SVI的IP</u> 3. 强制禁用IP设备跟踪

<u>参考</u>

简介

本文档介绍在MAB配置后IP设备跟踪的行为以及MAB身份验证后通信问题的可能解决方案。

先决条件

要求

Cisco 建议您了解以下主题:

- 思科身份服务引擎的配置
- Cisco Catalyst的配置

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 身份服务引擎虚拟3.3补丁1
- C1000-48FP-4G-L 15.2(7)E9

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

图解

本文档介绍此图中的MAB身份验证配置和验证。



网络图

背景信息

即使MAB身份验证成功,但在重新启动(或拔掉并重新插入电缆)Win10 PC1后,它仍然无法成功 ping通网关(Win10 PC3)。此意外行为是由于Win10 PC1上的IP地址冲突引起的。 默认情况下,在已配置MAB的接口上启用IP设备跟踪及其ARP探测。当Windows PC连接到启用了 IP设备跟踪的Catalyst交换机时,Windows端可能会检测到IP地址冲突。 出现这种情况是因为在此 机制的检测窗口期间收到ARP探测(发送方IP地址为0.0.00),将其视为IP地址冲突。

配置

此配置示例演示了MAB配置后IP设备跟踪的行为。

C1000中的配置

这是C1000 CLI中的最低配置。

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

ISE中的配置

步骤1:添加设备

导航到管理>网络设备,点击添加按钮以添加C1000设备。

- 名称:C1000
- IP地址:1.x.x.101

≡	dentity Services	Engine		Administration / Network Resources							
Щ	Bookmarks	Network Devices	Network Dev	ice Groups	Network Device Profiles	External RADIUS S	Servers R	RADIUS Server Sequences	NAC Managers	External MDM	
	Dashboard	Network Devices		Network Devices L	ist > New Network Device						
14	Context Visibility	Default Device Device Security Setting	as	Network Dev	ices						
×	Operations			Name	C1000						
	Policy			Description							
20	Administration			Description							
d.	Work Centers										
				IP Addre	Here 1.1 1.1 1.1 1	101 / 32	>				
?	Interactive Features										
				Device Profile	dia Cisco	()					
				Model Name		~					
				Software Versi	on	~					
				Network Devic	e Group						
				Location	All Locations	~	Set To Default				
				IPSEC	Is IPSEC Device	~	Set To Default				
				Device Type	All Device Types	~	Set To Default				
				RADIUS	DIUS Authentication Settin	ngs					
				Protoco	RADIUS						
				Shared	Secret cisco123		Hide				

添加设备

第二步:添加终端

导航到情景可视性>终端,点击添加按钮添加终端的MAC。

\equiv $\frac{1}{10000}$ Identity Services Eng	gine	Context Visibility / E	ndooints				
]] Bookmarks	Authentication BYOD Compliance	Add Endpoint		×	Hardware	More ~	
EE Dashboard		 General Attributes 		^			
Context Visibility	INACTIVE ENDPOINTS	Mac Address* B4:96:91:17:11:Cu			re Identity Group		
Operations Policy		Description			ata available.		
Administration							
Work Centers		Static Assignment Policy Assignment	Static Group Assignment				
Interactive Features		Unknown	Unknown	<u> </u>			
			Cancel	Save			

添加终端

第三步:添加策略集

导航到策略>策略集,点击+添加策略集。

- 策略集名称: C1000_MAB
- 说明:用于mab测试

- 条件:Wired_MAB
- 允许的协议/服务器序列:默认网络访问

≡	admite Identity Services Eng	igine Policy / Policy Sets	🔺 Evaluation Mode 🗖 Days 📿	۵.	0	<u>م</u> ۶	٩
н	Bookmarks	Policy Sets	Reset Policyset H	tcounts		Save	
	Dashboard	Status Policy Set Name Description Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View	
명	Context Visibility	Q, Search					
~	Operations	C1000_MAB for mabitest	Default Network Access 🛛 🗸 +		<i>{</i> 6}	,	
0	Policy				-	_	
8.	Administration	Default Default policy set	Default Network Access 0 +	•	¢۶	*	
-fil	Work Centers						
				Reset		Save	

添加策略集

第四步:添加身份验证策略

导航到策略集,点击C1000_MAB添加身份验证策略。

- 规则名称: MAB_authentication
- 条件:Wired_MAB
- 使用:内部终端

∨Authenticatic	n Policy(1)				
+ Status	Rule Name	Conditions	Use	Hits	Actions
Q Searc	h				
		Wired_MAB	Internal Endpoints 🛛 🛇 🗸		
٥	MAB_authentication		> Options		¢
			All_User_ID_Stores		
0	Default		> Options	0	¢

添加身份验证策略

第五步:添加授权策略

导航到策略集,点击C1000_MAB添加授权策略。

- 规则名称: MAB_authorization
- 条件: Network_Access_Authentication_Passed
- 结果:PermitAccess

VAuthorization Policy(1)		Results			
Status Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Q Search					
MAB_authorization	Network_Access_Authentication_Passed	PermitAccess ×	✓ + Select from list	F	¢۵
O Default		DenyAccess	+ Select from list	F o	

添加授权策略

配置MAB之前

运行show ip device tracking all命令以确认IP设备跟踪功能已禁用。

<#root>

Switch #

show ip device tracking all

Global IP Device Tracking for clients =

Disabled

IP Address MAC Address Vlan Interface Probe-Timeout State Source

配置MAB之后

步骤1:在MAB身份验证之前

运行show ip device tracking all命令以确认IP设备跟踪功能已启用。

<#root>

Switch #

show ip device tracking all

Global IP Device Tracking for clients =

Enabled

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

第二步:在MAB身份验证之后

从Win10 PC1初始化MAB身份验证并运行show ip device tracking all命令,以确认GigabitEthernet1/0/2上IP设备跟踪的状态。

<#root>

Switch #

show ip device tracking all

Global IP Device Tracking for clients =

Enabled

192.168.10.10

b496.9115.84cb 12 GigabitEthernet1/0/2 30

ACTIVE

ARP

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

第三步:确认身份验证会话

运行show authentication sessions interface GigabitEthernet1/0/2 details命令以确认MAB身份验证会话。

<#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

第四步:确认Radius实时日志

在ISE GUI中导航到操作> RADIUS >实时日志,确认MAB身份验证的实时日志。

Live Logs L	ive Sessions											
Misconfigure	ed Supplicants 🕕			Miscon	figured Network Devices		RADIU	S Drops 🕕	Client Stopped Res	ponding 🕕		Repeat Counter 🕕
	0				0			0	1			0
										Never Show Latest	20 records 🥪	Within Last 3 hours 🗸
Ø t∋ Res	eet Repeat Counts 🛛 🖞 Exp	oon To \sim										Filtor 🗸 🛛 🕀
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	Vetwork Devic
Feb 25	i, 2024 04:32:06.437 PM	٠	à	0	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	
Feb 25	. 2024 04:32:05.396 PM		0		84:96:91:15:84:CB	B4:96:91:15:84:CB	Intel-Device	C1000_MAB >> MAB_authentication	C1000_MAB >> MAB_authorizati	PermitAccess	192.168.10.10	C1000

第五步:确认IP设备跟踪的数据包详细信息

运行show interfaces GigabitEthernet1/0/2命令以确认GigabitEthernet1/0/2的MAC地址。

<#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)

在数据包捕获中,确认GigabitEthernet1/0/2每30秒发送一次ARP探测。

		-			
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探测功能

在数据包捕获中,确认ARP探测的发送方IP地址为0.0.0.0。

📕 Wireshark · Packet 74 · pciPassthru0

ARP探测的详细信息

问题

当Catalyst交换机发送带有发送方IP地址0.0.0.0的ARP探测时,该交换机的IP设备跟踪功能可能会导致Windows PC上的IP地址冲突。

可能的解决方案

有关可能的解决方案,请参阅<u>IP地址重复0.0.00的错误消息故障排除</u>。 以下是思科实验室中测试的每种解决方案的示例,以了解更多详细信息。

1. 延迟ARP探测的发送

运行ip device tracking probe delay <1-120>命令以延迟从交换机发送ARP探报。此命令不允许交换机在检测到链路UP/抖动时发送<1-120>秒的探测,这样可以最大程度地降低在链路另一端的主机检查重复IP地址时发送探测的可能性。

这是为10配置ARP探测延迟的示例。

Switch (config)#ip device tracking probe delay 10

运行show ip device tracking all命令以确认延迟设置。

<#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. ARP探测的配置自动源

运行ip device tracking probe auto-source fallback <host-ip> <mask> [override]命令以更改ARP探测的源IP地址。使用此命令,ARP探测功能的IP源不是0.0.0.0,而是主机所在VLAN中的交换机虚拟接口(SVI)的IP地址,或者如果SVI未设置IP地址,则会自动计算该IP地址。

这是将<host-ip>配置为0.0.0.200的示例。

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

模式1。已配置SVI的IP

在本文档中,由于为执行MAB身份验证的接口(GigabitEthernet1/0/2)设置了SVI IP地址(vlan12的IP地址),因此ARP探测的源IP地址 更改为192.168.10.254。

运行show ip device tracking all命令以确认自动源的设置。

<#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

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探测功能

在数据包捕获中,确认ARP探测的发送方IP地址为192.168.10.254,这是SVI (vlan 12)的IP。

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
```

ARP探测的详细信息

模式2.未配置SVI的IP

在本文档中,由于ARP探测的目的地是192.168.10.10/24,如果未配置SVI IP地址,则源IP地址为192.168.10.200。

删除SVI的IP地址

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

运行show ip device tracking all命令以确认自动源的设置。

<#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

在数据包捕获中,确认GigabitEthernet1/0/2每30秒发送一次ARP探测。

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探测功能

在数据包捕获中,确认ARP探测的发送方IP地址已更改为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
```

ARP探测的详细信息

3. 强制禁用IP设备跟踪

运行 ip device tracking maximum 0 命令以禁用IP设备跟踪。



注意:此命令并不是真正禁用IP设备跟踪,而是将跟踪的主机数量限制为零。

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

运行show ip device tracking all命令以确认GigabitEthernet1/0/2上IP设备跟踪的状态。

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

参考

排除IP地址为0.0.0.0的重复错误消息故障

<u>验证IPDT设备操作</u>

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。