

交換機上採用MAB/802.1x身份驗證的UCS實施

目錄

[簡介](#)

[背景](#)

[問題](#)

[拓撲](#)

[工作場景](#)

[非工作方案](#)

[解決方案](#)

簡介

本文檔介紹如何在思科交換機上實施帶有MAB/802.1x身份驗證的UCS C系列。

背景

思科提供的其中一項存取控制技術是MAC驗證略過(MAB)。MAB使用裝置的MAC地址來確定提供何種網路訪問。

在既包括支援IEEE 802.1X的裝置也包括不支援IEEE 802.1X裝置的網路中，MAB可以部署為IEEE 802.1X的回退機制或補充機制。如果網路沒有任何支援IEEE 802.1X的裝置，則可以將MAB部署為獨立身份驗證機制。

要瞭解有關解決方案級使用案例、設計和分階段部署方法的詳細資訊，請參閱 [MAC身份驗證繞行部署指南](#)。

問題

拓撲

```
UCS (C220)mgnt interface — gig 1/0/1[3750-X] — ISE (configured for MAB)
```

不同的UCS和不同的交換機會發生這種情況。在4500交換器上也觀察到了相同的情況。

UCS裝置(UCS-C210-M2:問題)：使用**access-session closed**或**no authentication open**命令時，MAB無法使用。

工作場景

UCS管理介面在交換機埠上連線。這是組態(工作)：

```
interface GigabitEthernet1/0/1
description DVR-UCS-dot1x-issue
switchport access vlan 300
switchport mode access
```

```
switchport voice vlan 400
ip arp inspection trust
ipv6 nd raguard
dot1x timeout quiet-period 300
dot1x timeout tx-period 5
dot1x timeout supp-timeout 5
dot1x timeout ratelimit-period 300
no mdix auto
source template ENT-TEMPLATE
spanning-tree portfast
spanning-tree guard root
end
3750# show access-sess int g1/0/1 details

Interface: GigabitEthernet1/0/1
IIF-ID: 0x102AEC0000003D7
MAC Address: 30f7.0d08.7ace
IPv6 Address: Unknown
IPv4 Address: 10.141.49.205
User-Name: 30-F7-0D-08-7A-CE
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: 65535s (local), Remaining: 11282s
Timeout action: Reauthenticate
Common Session ID: 0A8D31C7000017BD723AF6C2
Acct Session ID: 0x0000287D
Handle: 0x980002D5
Current Policy: ENT-IDENTITY-POL Server Policies:
ACS ACL: xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
SGT Value: 12 Method status list:
Method State
dot1x Stopped
mab Authc Success
```

非工作方案

但是，在**access-session closed**的情況下，您無法對它執行ping操作且無法看到訪問會話資訊。

```
3750(config)#int g1/0/1
3750(config-if)#access-session closed
3750(config-if)#shutdown
3750(config-if)#no shutdown

May 11 16:33:14.311 JST: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to down
May 11 16:33:15.312 JST: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1,
changed state to down
May 11 16:33:17.891 JST: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
May 11 16:33:18.891 JST: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1,
changed state to up
```

```
Sending 5, 100-byte ICMP Echos to 10.141.49.205, timeout is 2 seconds:
```

```
.....
Success rate is 0 percent (0/5)
3750#do sh access-sess int g1/0/1 details
No sessions match supplied criteria.
```

解決方案

Debug(**debug MAB all** 命令)顯示交換機上未獲知的UCS的MAC條目，這是使用後端進行身份驗證所必需的。

```
3750 (config)# interface GigabitEthernet1/0/37
3750(config-if)#access-session control-direction in
```

輸入**access-session control-direction in** 命令(之前稱為**authentication control-direction in** 命令)，使交換機能夠傳送輸出到主機的流量，但不能反過來。此命令通常用於印表機/裝置等客戶端，這些客戶端不會持續傳送流量以啟動通訊(也用於Wake on Lan)。實質上是由交換器傳送封包，使用者端會加以回應。響應將包含隨後用於MAB的MAC地址。在已建立的設定中，未收到來自客戶端的MAC地址。