UCS Implementation with MAB/802.1x Authentication on Switches

Contents

Introduction

This document describes how to implement UCS C-Series with MAB/802.1x authentication on Cisco switches.

Background

One of the access control techniques that Cisco provides is MAC Authentication Bypass (MAB). MAB uses the MAC address of a device in order to determine what kind of network access to provide.

In a network that includes both devices that support and devices that do not support IEEE 802.1X, MAB can be deployed as a fallback, or complementary, mechanism to IEEE 802.1X. If the network does not have any IEEE 802.1X-capable devices, MAB can be deployed as a standalone authentication mechanism.

In order to learn more about solution-level uses cases, design, and a phased deployment methodology, see MAC Authentication Bypass Deployment Guide.

Problem

Topology

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

This happens with different UCS and on different switches. The same is observed on the 4500 switch.

UCS devices (UCS-C210-M2: problem observed) does not work with MAB with **access-session closed** or **no authentication open** command.

Working Scenario

The UCS management interface is connected on switchport. This is the configuration (working):

```
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
```

Non-working Scenario

However, with **access-session closed**, you cannot ping it and cannot see access-session information.

```
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.
```

Solution

Debug (**debug MAB all** command) shows the MAC entry of UCS not learned on the switch, which is required to authenticate with the backend.

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

Enter the **access-session control-direction in** command (previously the **authentication control-direction in** command) in order to enable the switch to send traffic in egress to the host, but not the other way around. The command is usually used on clients such as printers/devices which do not continually send traffic as a way to initiate communication (also used for Wake on Lan). Essentially a packet is sent from the switch and the client responds. The response will contain the MAC address which is then used for MAB. In the already established setup, the MAC address from the client was not being received.