Contents

Introduction

This document describes specific scenario of implementing UCS C-series with MAB/802.1x authentication on Cisco switches.

Background

One of the access control technique that Cisco provides is called MAC Authentication Bypass (MAB). MAB uses the MAC address of a device 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.

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

Problem

Topology:

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

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

Working scenario:

UCS management interface is connected on switchport and this is the configuration (working):

Non-working scenario:

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

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) show the MAC entry of UCS not learnt on switch which is required to authenticate with backend.

Enable access-session control-direction in (previously authentication control-direction in), we 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 don't 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.