スイッチでのMAB/802.1x認証を使用したUCSの実装

内容

概要

このドキュメントでは、CiscoスイッチでMAB/802.1x認証を使用するUCS Cシリーズを実装する方法について説明します。

背景

シスコが提供するアクセス制御技術の1つに、MAC認証バイパス(MAB)があります。MABは、デバイスのMACアドレスを使用して、提供するネットワークアクセスの種類を決定します。

IEEE 802.1Xをサポートするデバイスと IEEE 802.1Xをサポートしないデバイスの両方を含むネットワークでは、MABをIEEE 802.1Xに対するフォールバック（補完的）メカニズムとして導入できます。ネットワークにIEEE 802.1X対応デバイスがない場合、MABをスタンドアロン認証メカニズムとして導入できます。

ソリューションレベルの使用例、設計、段階的な展開方法の詳細については、『 MAC Authentication Bypass Deployment Guide』を参照 してください。

問題

トポロジ

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

これは、異なるUCSと異なるスイッチで発生します。4500スイッチでも同様です。

UCSデバイス(UCS-C210-M2:問題が見つかりました)は、**access-session closed**または**no authentication open**コマンドで**MAB**と**は動作**しません。

正常動作シナリオ

UCS管理インターフェイスはスイッチポートに接続されています。次の設定（動作）です。

```
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
```

動作しないシナリオ

ただし、access-session closedの場合は、pingを実行できず、access-session情報を表示できません。

```
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.
```

解決方法

Debug(**debug MAB allコマンド)**は、バックエンドで認証するために必要な、スイッチで学習されなかったUCSのMACエントリを示します。

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

access-session control-direction inコマンド(以前は**authentication control-direction inコマンド)を入力し**て、スイッチがトラフィックをホストに出力で送信できるようにします。逆の方法は送信しません。このコマンドは通常、通信を開始する手段としてトラフィックを継続的に送信しないプリンタ/デバイスなどのクライアントで使用されます（Wake on Lanにも使用されます）。 基本的に、パケットがスイッチから送信され、クライアントが応答します。応答にはMACアドレスが含まれ、MACアドレスはMABに使用されます。すでに確立されているセットアップでは、クライアントからのMACアドレスが受信されませんでした。