Improving Security with MAC Authentication Bypass

by Bilal Ibrahim, Senior Network Engineer, UncommonX

Securing network access is critical and MAC authentication bypass (MAB) can help. These days, contractors and visitors require access to network resources over the same network as employees, but that means the possibility that unauthorized people or devices will gain access to controlled or confidential information also increases.

One of the solutions is to enable MAB. MAB will use the MAC address of the device to determine the level of the network access to provide. MAB offers visibility and identity-based access control at the network edge of endpoints that do not support IEEE 802.1X.

Other cases where you can use the MAC authentication bypass are:

1. Network environments in which a supplicant code is not available for a given client platform.
2. Network environments in which the end client configuration is not under administrative control; that is, the IEEE 802.1X requests are not supported on these networks.

MAB is the process of a nonauthenticating device (a device without an 802.1X supplicant running on it like network printers, cameras, and sensors) connecting to a network with 802.1X enabled. Enable the MAB option on the port so that the system will use the device MAC address as the user's name and password for authentication. Once the switch learns the MAC address, it contacts an authentication server (RADIUS) to check if it permits the MAC address.

MAB can operate in two states:

- Standalone: It only uses MAB for authentication.
- Fallback: It only uses MAB as a fallback for 802.1X. The switch will first attempt 802.1X and, when it fails, it uses MAB for authentication.

By default, MAB can support only one device (MAC address), and when it detects multiple source MAC addresses, it will trigger a security violation. You can change this default behavior to one of these:

- **Single-host mode**: This is the default setting. It will trigger a security violation when the switch detects another source MAC address after authentication.

- **Multi-domain authentication host mode**: We use this mode to authenticate two MAC addresses — one for the voice VLAN and another one for the data VLAN. This is typically seen when we have a PC and phone on a single port. The third MAC address will trigger a security violation.
- **Multi-authentication host mode**: This is to authenticate multiple source MAC addresses. This mode can be used in case we have another switch connected to our local switch. Each source MAC address is separately authenticated.
- **Multi-host mode**: The switch allows multiple source MAC addresses. It will only authenticate the first source MAC address. All others will be permitted automatically.

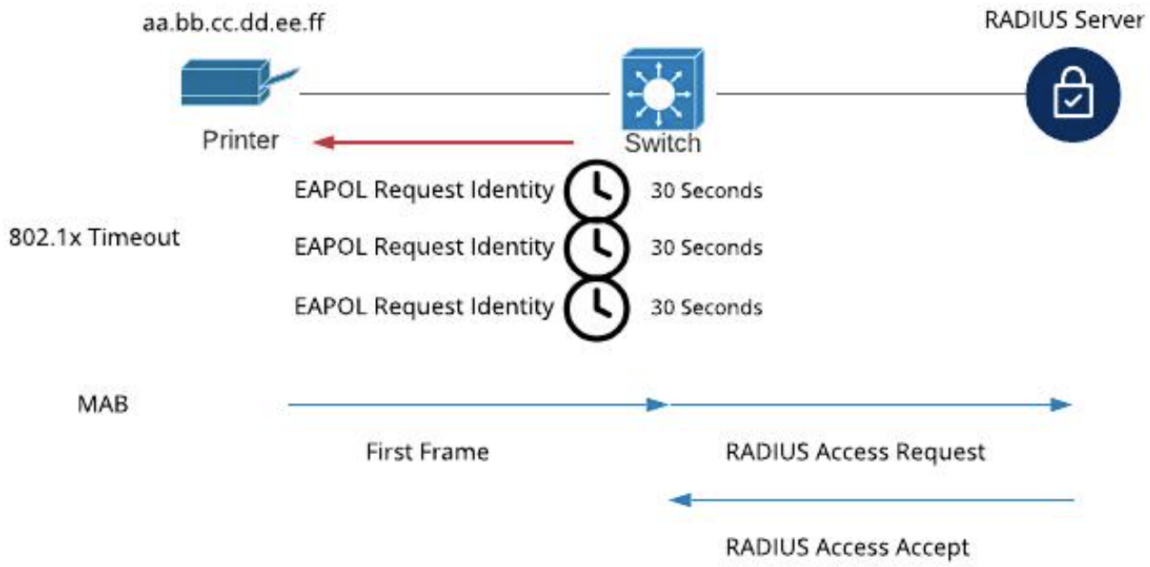
When MAB is enabled on switch port, the switch will forward each new detected MAC address and send it to RADIUS for authentication. Then it will use the MAC address to fill RADIUS attributes (username and password or calling station ID). ISE can authenticate the end device either based upon calling station ID or username and password.

ISE acts differently when the process host lookup is enabled versus disabled:

- Process host lookup is enabled: This option is recommended. It takes the calling station ID as the MAC address and checks in the internal endpoints database.
- Process host lookup is disabled: It takes the username and password as the MAC address and checks in the internal user database.

Authentication Time-out in 802.1X

This can be used to let the switch determine if the end device is 802.1X compatible or not. By default, the switch sends extensible authentication protocol (EAP) over LAN (EAPoL) to the end device every 30 seconds. If the switch does not receive any response for three EAPoL identity requests (total of three missing requests over 90 seconds) then it will assume that the endpoint is not 802.1X supplicant and start MAB. The recommendation is to decrease the default time-out period to make it faster.



MAC Authentication Bypass Configuration

1. We must enable **aaa** then configure the default authentication list as below:

Switch (config)#**aaa new-model**
Switch (config)#**aaa authentication dot1x default group radius**

2. Add the RADIUS authentication server along with the key:

Switch (config)#**radius server Test**
Switch (config)#**address ipv4 x.x.x.x auth-port 1812**
Switch (config-radius-server)#**key test**

3. Finally, we configure the switch port. We will have to set the default port control. If we choose force-authorized then the port is automatically authorized. The second option is force-unauthorized then the interface is not authorized. We can automatically set it so the switch can determine if the port is authorized or not.

Switch (config)# **interface GigabitEthernet2/1**
Switch (config-if)#**switchport mode access**
Switch (config-if)#**authentication port-control auto**
Switch (config-if)# **mab**

You can use a couple of useful commands to give us more details on MAB and the authenticated interfaces:

SW1#**show authentication sessions**
Interface MAC Address Method Domain Status Session ID
Gi2/1 aaaa.bbbb.cccc mab DATA Authz Success 0A38641F0000003500450DCF

Switch # **show authentication sessions interface GigabitEthernet2/1 details**:

Interface: GigabitEthernet2/1
MAC Address: aaaa.bbbb.cccc
IP Address: Unknown
Username: aaaabbbbcccc
Status: Authz Success
Domain: DATA
Security Policy: Should Secure
Security Status: Unsecure
Oper host mode: single-host
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: N/A
Session Time-out: N/A
Idle Time-out: N/A
Common Session ID: C0A8FE0100000271FEF432A8
Acct Session ID: 0x000003AE
Handle: 0xBF000272

Runnable methods list:
Method State
mab Authc Success

With MAB, we can't use advance authorization options for ISE like:

- Downloadable ACLs
- Dynamic VLAN*
- URL Redirection
- Secure Group Tags (SGTs)
- Smart Port Macros

*Implementing Dynamic VLANs on the devices that do not have 802.1X supplicant is not recommended.

About the author

Bilal Ibrahim is an IT professional with more than 16 years of experience in the vast area of networking technologies. His background has largely been in financial services with hands-on experience in enterprise networks specializing in Cisco LAN/WAN/backbone/data center and security environments. Bilal leads the internal network design and automation for UncommonX.