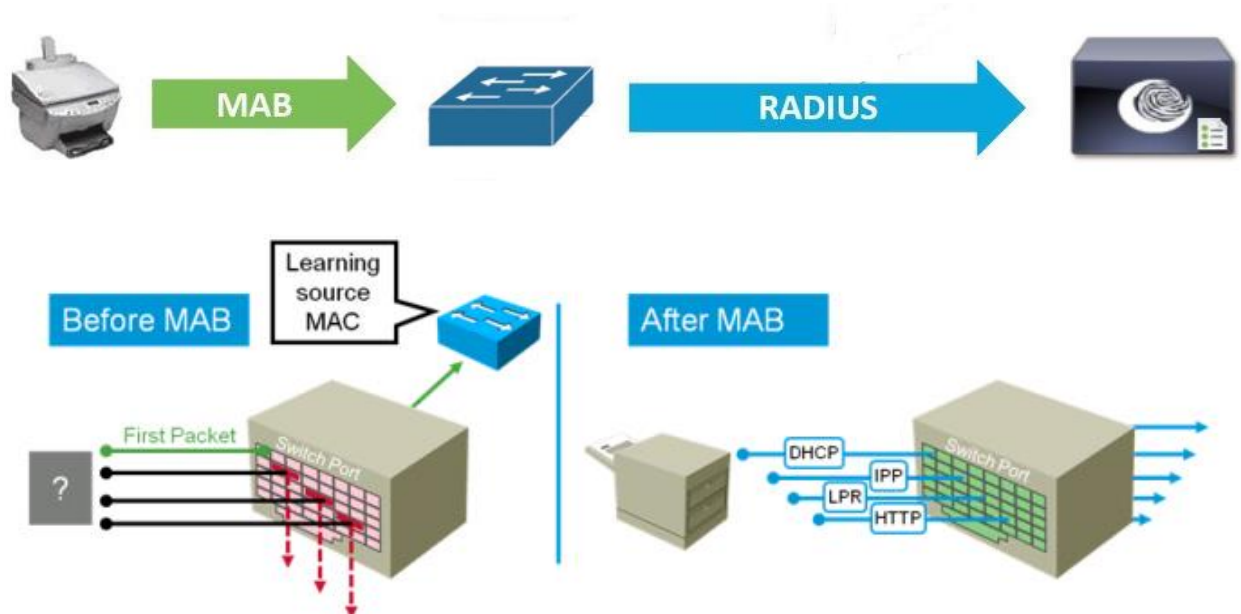
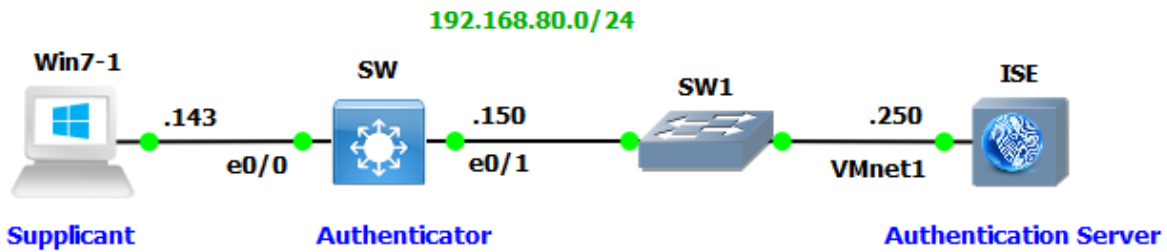


## Implement MAB:

- o MAB stands for Media Access Control Authentication Bypass.
- o MAB allow controlling devices to access the Network at Layer 2.
- o Authentication server performs authentication lookup using MAC address as a credential.
- o MAC Authentication Bypass feature is a MAC-address-based authentication mechanism.
- o MAB can be implemented over devices, which do not support 802.1x authentication.
- o MAB is used to authenticate non-802.1x capable devices such as printers, IP phones.
- o MAB is working over MAC address it is independent of Usernames and passwords.
- o MAB can also be implemented over the 802.1x supported devices.
- o MAB is not secure authentication method compared to other authentication methods.
- o MAB is not a strong authentication process it can be overcome by MAC address spoofing.
- o When enable MAB on switchport, switch drops all frames except first frame to learn MAC.
- o Once the switch has learned the MAC address of the connected device.
- o Switch contacts an authentication server to check if it permits the MAC address.
- o ISE authenticate MAB devices either based on Calling Station ID or Username & Password.
- o If Process Host Lookup is enabled, then Authentication is done based on Calling Station ID.
- o If Process Host Lookup is disabled, then Authentication is done on username & password.
- o By default, MAB only supports a single endpoint (device) per switchport.
- o MAB also supports dynamic values from your RADIUS server such as ACL or VLAN.
- o MAB can be deployed as standalone authentication.



## Lab Topology:



## MAB Configuration:

MAB Configuration on SW
SW(config)#interface vlan 1
SW(config-if)#ip address 192.168.80.150 255.255.255.0
SW(config-if)#no shutdown
SW(config-if)#exit
SW(config)#aaa new-model
SW(config)#aaa authentication dot1x default group radius
SW(config)#radius server ISE
SW(config-radius-server)#address ipv4 192.168.80.250 auth-port 1812 acct-port 1813
SW(config-radius-server)#key test123
SW(config)#interface ethernet 0/0
SW(config-if)#switchport host
SW(config-if)#authentication port-control auto
SW(config-if)#mab
SW(config-if)#authentication order mab dot1x
SW(config-if)#authentication priority dot1x mab
SW# debug radius authentication
SW# show mab all
SW# show authentication sessions interface ethernet 0/0
SW# show authentication sessions interface ethernet 0/0 details
SW# show authentication sessions

## Add Network Device:

Go to **Administration > Network Resources > Network Devices** to add the Device (SW), which will request to authenticate Dot1x Client.

Administration Work Centers 0

System  
Deployment  
Licensing  
Certificates  
Logging  
Maintenance  
Upgrade  
Backup & Restore  
Admin Access

**Network Resources**  
Network Devices  
Network Device Groups  
Network Device Profiles  
External RADIUS Servers  
RADIUS Server Sequences  
NAC Managers  
External MDM  
Location Services

pxGrid Services  
Feed Service Profiler  
Identity Mapping  
AD Domain Controllers  
Mapping Filters

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences

Network devices  
Default Device

Network Devices

Edit Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location
------	---------	--------------	----------

Click on Add button to add Device, Configure **Name** of the device, **IP address** configured.

Network Devices List > **New Network Device**

Network Devices

\* Name SW

Description SWITCH NAD

\* IP Address: 192.168.80.150 / 32

\* Device Profile Cisco

Model Name Unknown

Software Version Unknown

\* Network Device Group

Device Type All Device Types Set To Default

Location All Locations Set To Default

Scroll down to set Authentication settings. Set Password configured as Server key on Switch device “test123” and save settings.

**RADIUS Authentication Settings**

Enable Authentication Settings

Protocol **RADIUS**

\* Shared Secret

Enable KeyWrap  ⓘ

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

CoA Port

### Add MAC to Identity Store:

To add Windows 7 MAC address in ISE database, navigate to **Administration > Identities > End Points > Add**. Type Windows 7 MAC Address and click **“Save”** to save the setting.

Identity Services Engine | Home | Operations | Policy | Guest Access | **Administration** | Work Centers

System | **Identity Management** | Network Resources | Device Portal Management | pxGrid Services | Feed Service | Identity Mapping

**Identities** | Groups | External Identity Sources | Identity Source Sequences | Settings

**EndPoints**

Users

Latest Manual Network Scan Results

Endpoint List > New

Mac Address \*

Description

Static Assignment

Policy Assignment

Static Group Assignment

Identity Group Assignment

## Verify:

To verify navigate to **Operations > RADIUS Livelog**.

The live logs show the given MAC address has verified and allowed.

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy
2019-06-07 11:19:59.786	i		0	00:0c:29:55:68:e0	00:0c:29:55:68:e0	VMWare-Device	Default >> MAB >> D...	Default >> Basic_Aut...
2019-06-07 11:19:59.786	c		0	00:0c:29:55:68:e0	00:0c:29:55:68:e0	VMWare-Device	Default >> MAB >> D...	Default >> Basic_Aut...

Verify on Switch it show the method is MAB and authenticated.

```
SW#show authentication sessions
```

```
Interface Identifier Method Domain Status Fg Session ID
Et0/0 000c.2955.68e0 mab DATA Auth C0A850960000001000458959
```

Verify on Switch it show more details about MAB configured interface.

```
SW#show authentication sessions interface ethernet 0/0 details
```

```
Interface: Ethernet0/0
MAC Address: 000c.2955.68e0
IPv6 Address: Unknown
IPv4 Address: 192.168.80.143
User-Name: 00-0c-29-55-68-E0
Status: Authorized
Domain: DATA
Oper host mode: single-host
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 4526s
Common Session ID: C0A850960000001000458959
Acct Session ID: Unknown
Handle: 0xAD000005
Current Policy: POLICY_Et0/0
```

Local Policies:

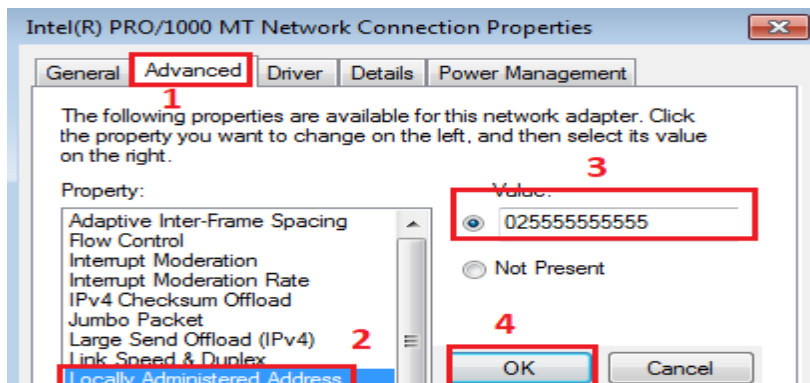
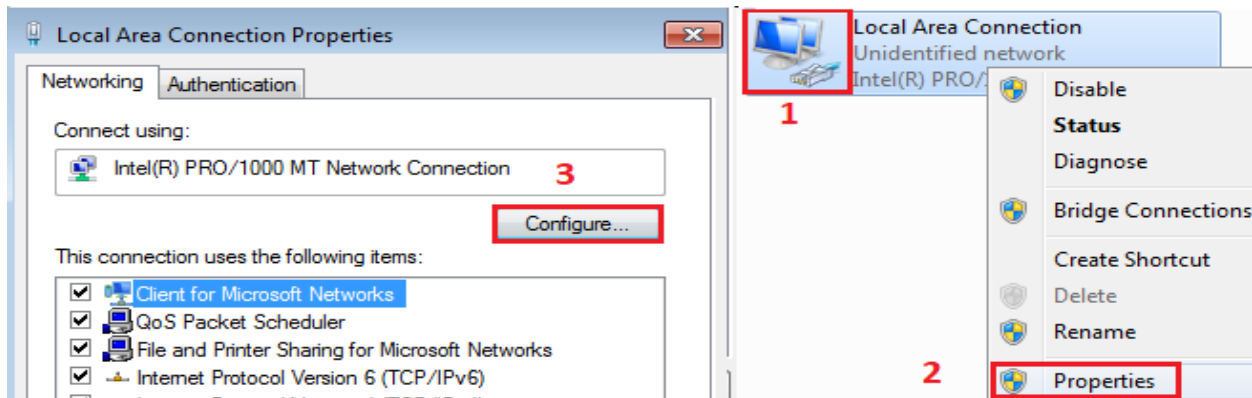
```
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure
Security Status: Link Unsecure
```

Server Policies:

Method status list:

```
Method State
mab Authc Success
```

Let us change the MAC Address of Windows 7.



Switch deducted the security violation and shutdown the interface.

```

SW#
*Jun 7 11:25:57.862: %PM-4-ERR_DISABLE: security-violation error detected on Et
0/0, putting Et0/0 in err-disable state
SW#
*Jun 7 11:25:57.863: %AUTHMGR-5-SECURITY_VIOLATION: Security violation on the i
nterface Ethernet0/0, new MAC address (0255.5555.5555) is seen.AuditSessionID U
nassigned
*Jun 7 11:25:58.862: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
0, changed state to down
..

```

Let us bring up the interface of switch.

```

SW(config)#interface ethernet 0/0
SW(config-if)#shutdown
SW(config-if)#no shutdown

```

Let us verify again from **Operations > RADIUS Livelog**. The new MAC address is not in local database that why it has been denied by cisco ISE.

