# CCNP Security - SISAS
# Layer 2 Authentication - MAB

# Network Access Authentication

- Layer 2
  - Supplicant does not need an IP address
  - MAB and 802.1x (EAP methods)
- Layer 3
  - Supplicant requires an IP address
  - Local Web Authentication (web portal on the NAD)
  - Central Web Authentication (web portal on the authentication server)

# MAB – MAC Authentication Bypass

- MAB (MAC Authentication Bypass) is used to…
  - Authenticate non 802.1x capable devices
  - Trigger CWA and BYOD enrollment
  - Technically is NOT an authentication method…just bypasses authentication
- If MAB is enabled on the switch interface
  - Switch takes each new MAC address and sends it to RADIUS for authentication
    - RADIUS User- Name and RADIUS User-Password equals to the MAC address
    - RADIUS Calling-Station-ID equals to the MAC address
    - RADIUS Service Type is Call-Check (10) for MAB

# MAB – MAC Authentication Bypass

- If “Process Host Lookup” is enabled on RADIUS server
  - Authentication is done based on the RADIUS Calling-Station-ID attribute value
- If “Process Host Lookup” is disabled on RADIUS server
  - Authentication is done based on the RADIUS User-Name and User-Password attributes value

# MAB Configuration Steps on Supplicant

- None
  - Because MAB is not a authentication protocol
  - It is authentication bypass
  - There is no negotiation between supplicant and NAD

# MAB Configuration Steps on NAD

- Enable AAA
  - `aaa new-model`
- Configure dot1x default authentication list
  - `aaa authentication dot1x default group`
- Enable MAB on switch port facing the supplicant
  - `mab [eap]`
- Enforce authentication on switch port facing the supplicant
  - `authentication port-control auto`
- Define RADIUS server settings
  - `radius-server host <IP> key <radius key>`
- Optionally configure other global/interface level settings
  - `radius-server attribute 31 mac format`

# MAB Configuration Steps on ISE

- Configure MAB authentication policy
  - Optionally use a default one
- Configure authorization policy
  - Optionally use a default one
- Add supplicant's MAC address into Internal Endpoints Store
  - Authentication performed based on RADIUS Calling Station-ID attribute value

# MAB Verification and Troubleshooting

- Verification
  - `show mab all`
  - `show authentication session`
  - `show aaa servers`
- Troubleshooting
  - `show authentication session interface <if_number>`
  - `debug mab all`
  - `debug radius authentication`

# MAB and 802.1x Common Authorizations

## VLAN

- Data VLAN (by name or number)
  - Optional, it overrides the VLAN locally configured on NAD switch port
- Voice VLAN permission
  - Mandatory for voice domain, allows Phone to join the voice VLAN as configured locally on NAD

# MAB and EAP Common Authorizations

- Access-Lists
  - dACL (Cisco Proprietary, uses AV pairs)
    - Before 12.2(55)SE code, switch port required a pre-auth ACL to be applied
    - ACL configured on ISE
  - Filter-ID ACL (IETF standard)
    - ACL configured on NAD
  - Per-user ACL (Cisco proprietary, uses AV pairs)
    - ACL configured on ISE and ACE's pushed through authorization by ISE
    - ACL configured on NAD and ACL name pushed through authorization by ISE
- ACL Common configuration requirements on NAD
  - `aaa authorization network default group`
  - dACL also needs `radius-server vsa send authentication`
  - `ip device tracking`

# Authorization Verification Troubleshooting

- Verification
  - `show ip access-list interface <if_number>`
  - `show ip interface <if_number>`
  - `show epm session interface <if_number>`
  - `show authentication interface <if_number>`
  - `show authentication session interface <if_number>`
- Troubleshooting
  - `show ip device tracking all`
  - `show aaa method-lists authorization`
  - `debug radius authentication`
  - `debug ip device tracking events`

# Q&A