CISCO ISE Configuration

On Switch :

1. Assign IP Address for the Switch

This step sets the management IP address of the switch, enabling remote management.

```
interface Vlan1
 ip address 192.168.43.230 255.255.255.0
 no shut
```

- **interface Vlan1**: The management interface for the switch.
- **ip address 192.168.43.230 255.255.255.0**: Assigns the IP address `192.168.43.230` with a subnet mask of `255.255.255.0` to VLAN 1.
- **no shut**: Ensures the VLAN interface is active (not shut down).

---

2. Enable AAA (Authentication, Authorization, Accounting)

AAA is a framework for configuring access control. In this case, it enables authentication, authorization, and accounting services.

```
aaa new-model
```

- **aaa new-model**: Enables AAA services on the switch.

---

3. AAA Configuration for 802.1x Authentication

This block configures the switch to use Cisco Identity Services Engine (ISE) for 802.1x authentication, authorization, and accounting.

```
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE
```

- **aaa authentication dot1x default group ISE**: Configures 802.1x authentication to use the ISE group for authentication.
- **aaa authorization network default group ISE**: Configures network authorization to use the ISE group for authorization.
- **aaa accounting dot1x default start-stop group ISE**: Configures 802.1x accounting to use the ISE group, tracking session start and stop events.

---

4. Configure Cisco ISE (Identity Services Engine) as the Authentication Server

This section defines the ISE as the RADIUS server for authentication and accounting.

```
radius server ISE1
 address ipv4 192.168.43.200 auth-port 1812 acct-port 1813
 key cisco
```

- **radius server ISE1**: Creates a RADIUS server profile called `ISE1`.
- **address ipv4 192.168.43.200 auth-port 1812 acct-port 1813**: Specifies the IP address (`192.168.43.200`), authentication port (`1812`), and accounting port (`1813`) for the RADIUS server.
- **key cisco**: Defines the shared secret used for secure communication between the switch and ISE (`cisco`).

---

5. Create AAA Group for RADIUS Servers

This step groups RADIUS servers for AAA authentication.

```
aaa group server radius ISE
 server name ISE1
```

- **aaa group server radius ISE**: Creates a group named `ISE` for RADIUS servers.
- **server name ISE1**: Adds the RADIUS server `ISE1` to the `ISE` group.

---

6. Configure CoA (Change of Authorization)

Change of Authorization allows dynamic changes to an authenticated session.

```
aaa server radius dynamic-author
 client 192.168.43.200 server-key cisco
```

- **aaa server radius dynamic-author**: Enables dynamic authorization (CoA).
- **client 192.168.43.200 server-key cisco**: Specifies that the client with IP `192.168.43.200` can send CoA requests, using the key `cisco` for communication.

---

7. Enable 802.1x Globally on the Switch

This command enables 802.1x authentication for the entire switch.

```
dot1x system-auth-control
```

- **dot1x system-auth-control**: Globally enables 802.1x port-based authentication on the switch.

---

8. Define Permitted Traffic Before Authentication (Low-Impact Mode)

This Access Control List (ACL) allows specific traffic types (DHCP, DNS, etc.) before the port is authenticated. This is part of a low-impact mode configuration.

```
ip access-list extended PRE-AUTH
 remark DHCP
 permit udp any eq bootpc any eq bootps
 remark DNS
 permit udp any any eq domain
 remark PING
 permit icmp any any echo
 remark TFTP
 permit udp any any eq tftp
 remark DROP AND LOG THE REST
 deny ip any any log
```

- **ip access-list extended PRE-AUTH**: Creates an ACL named `PRE-AUTH` to control traffic before authentication.
- **permit**: Allows traffic for specific services like DHCP (bootpc, bootps), DNS, PING (ICMP), and TFTP.
- **deny ip any any log**: Denies all other traffic and logs any packets that match this rule.

---

9. Configure 802.1x on a Specific Interface (Ethernet0/0)

This step configures 802.1x authentication for a particular client interface.

```
interface Ethernet0/0
 description Client-1
 switchport mode access
 authentication open
 authentication port-control auto
 authentication periodic
 dot1x pae authenticator
 spanning-tree portfast
 ip access-group PRE-AUTH in
```

- **interface Ethernet0/0**: Refers to interface `Ethernet0/0`.
- **description Client-1**: Adds a description for documentation purposes (`Client-1`).
- **switchport mode access**: Configures the port as an access port (for a single VLAN).
- **authentication open**: Allows limited access for non-authenticated users.
- **authentication port-control auto**: Automatically enables 802.1x port control.
- **authentication periodic**: Periodically re-authenticates the client.
- **dot1x pae authenticator**: Configures the switch to act as an 802.1x authenticator.
- **spanning-tree portfast**: Enables PortFast for faster transition to the forwarding state.
- **ip access-group PRE-AUTH in**: Applies the `PRE-AUTH` ACL for inbound traffic.

---

10. Configure MAB (MAC Authentication Bypass) on a Specific Interface (Ethernet0/2)

MAB is used when devices do not support 802.1x; it allows authentication based on the MAC address.

```
interface Ethernet0/2
 description Client-2
 switchport mode access
 authentication open
 authentication port-control auto
 mab
 spanning-tree portfast
 ip access-group PRE-AUTH in
```

- **interface Ethernet0/2**: Refers to interface `Ethernet0/2`.
- **description Client-2**: Adds a description for documentation purposes (`Client-2`).
- **switchport mode access**: Configures the port as an access port.
- **authentication open**: Allows limited access for non-authenticated users.
- **authentication port-control auto**: Automatically enables port control for 802.1x or MAB.
- **mab**: Enables MAC Authentication Bypass for devices without 802.1x support.
- **spanning-tree portfast**: Enables PortFast for faster transition to the forwarding state.
- **ip access-group PRE-AUTH in**: Applies the `PRE-AUTH` ACL for inbound traffic.

On CISCO ISE :

1. Add the Switch as a Network Device

In Cisco ISE, the switch must be added as a network device to allow ISE to communicate with it using RADIUS.

- **Navigate to**: `Administration` > `Network Resources` > `Network Devices`
- **Add New Network Device**:
  - **Name**: Provide a descriptive name (e.g., Switch1)
  - **IP Address**: Enter the IP address of the switch (`192.168.43.230`)
  - **Shared Secret**: Enter the same RADIUS shared secret as configured on the switch (`cisco`)
  - **Enable RADIUS Authentication**: Check this option
  - **Authentication Settings**: Select RADIUS

---

2. Configure RADIUS Server Settings

Cisco ISE will authenticate clients using the RADIUS protocol, so you need to verify that your RADIUS settings are correct.

- **Navigate to**: `Administration` > `System` > `Settings` > `RADIUS`
  - Ensure that the **authentication ports** are set to `1812` and **accounting ports** to `1813` (as configured in the switch).

---

3. Create a New Identity Source Sequence (For 802.1x and MAB)

To support both 802.1x and MAB, create an Identity Source Sequence. This sequence will first attempt to authenticate a device using 802.1x and fall back to MAB if needed.

- **Navigate to**: `Administration` > `Identity Management` > `Identity Source Sequences`
- **Add New Identity Source Sequence**:
  - **Name**: (e.g., Dot1x_MAB_Sequence)

    - **Authentication Methods**:
        - Include the **Internal Users** for 802.1x
        - Include **Internal Endpoints** for MAB
    - **Drop Down Menu for Options**:
        - **Authentication failed**: Move to the next identity source
        - **User not found**: Move to the next identity source

---

4. Create Authentication Policy

This step defines the authentication mechanisms and rules for both 802.1x and MAB.

- **Navigate to**: `Policy` > `Authentication`
- **Create New Rule**:
    - **Condition**: Select **Wired_802.1X** for ports using 802.1x
    - **Action**: Choose the **Dot1x_MAB_Sequence** created above
    - **MAB Rule**: Create a similar rule for **Wired_MAB** if the device doesn't support 802.1x. This rule will use the same Identity Source Sequence.

---

5. Configure Authorization Policy

Define authorization rules to specify what access is granted based on the authentication result.

- **Navigate to**: `Policy` > `Authorization`
- **Create a New Rule**:
    - **Condition**: Select **EndPoints Identity Group Equals RegisteredDevices** (for authorized devices)
    - **Action**: Permit Access (e.g., `PermitAccess`)
- **MAB Authorization Rule**: Create an additional rule for MAB, granting limited network access (e.g., `Guest Access` or `Restricted VLAN`) until full authentication occurs.

---

6. Configure Profiling Policies (Optional)

Cisco ISE can dynamically profile devices and classify them, allowing for more granular policy enforcement. You can configure the profiling service if needed for specific device types.

- **Navigate to**: `Policy` > `Profiling`
- Create profiles for common device types (e.g., printers, phones) that may use MAB authentication.

7. Configure Posture Policies (Optional)

If you want to enforce endpoint compliance (e.g., checking for antivirus, OS patches), configure posture policies.

- **Navigate to**: `Policy` > `Policy Elements` > `Results` > `Posture`
- Create new posture requirements based on the security posture of endpoints.

8. Enable Change of Authorization (CoA)

To allow Cisco ISE to dynamically change authorization for devices (e.g., move them to a different VLAN after successful posture assessment), CoA must be enabled.

- **Navigate to**: `Administration` > `System` > `Settings` > `RADIUS` > `CoA Settings`
  - Ensure **RADIUS Change of Authorization (CoA)** is enabled.

9. Endpoint Device Registration

For MAB to work, devices using MAC addresses for authentication need to be registered in the Cisco ISE database.

- **Navigate to**: `Work Centers` > `Endpoints` > `Add Endpoint`
  - Add devices using their MAC address.

10. Verify Accounting Settings

Ensure that accounting for tracking session activity is enabled.

- **Navigate to**: `Administration` > `System` > `Settings` > `RADIUS` > `Accounting`
  - Enable **Start-Stop Accounting** to track the beginning and end of sessions.