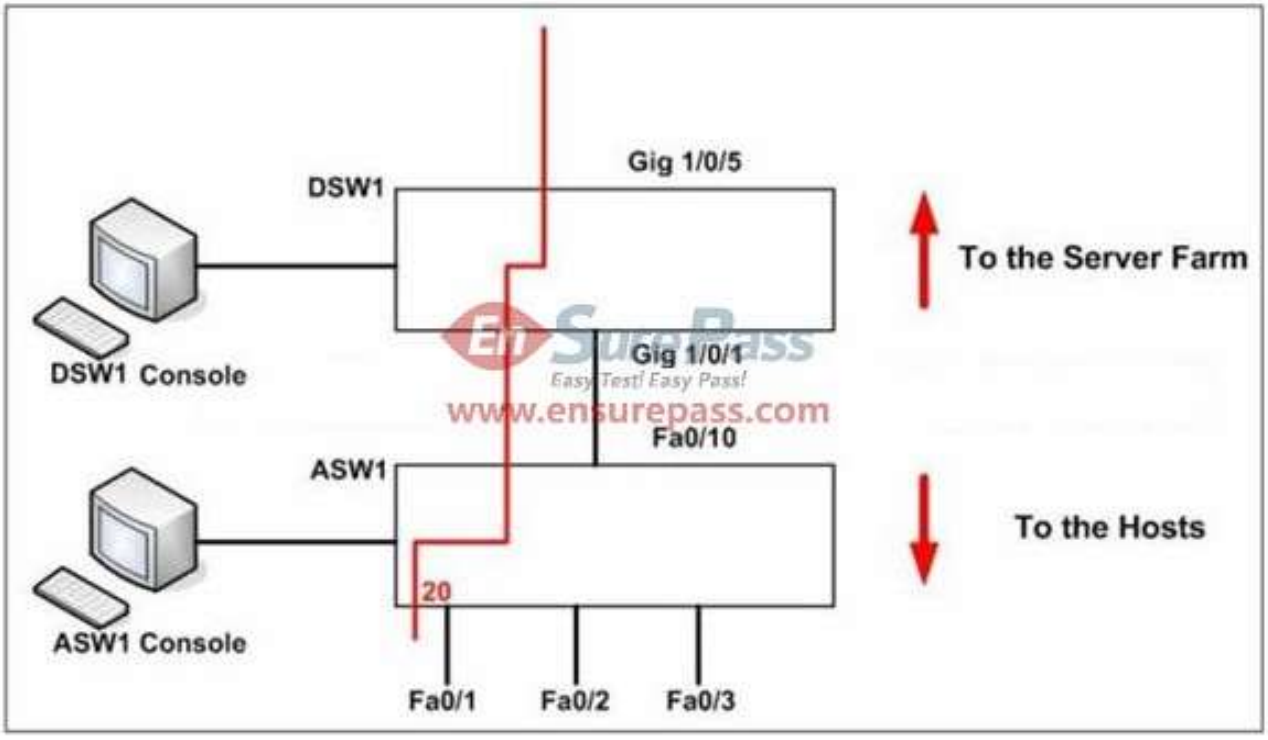
In computer security,**AAA stands for Authentication, Authorization and Accounting**:

- **Authentication:** Verify the identity of the user, who are you?
- **Authorization:** What is the user allowed to do? what resources can he/she access?
- **Accounting:** Used for billing and auditing.

AAA is used in a scenario where a user has to authenticate before getting access to the network.
Before authentication user wont even get an IP address. The only thing the user is allowed to do is send his/her credentials which will be forwarded to the AAA server. If user credentials are OK the port will be unblocked and user will be granted access to the network.

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

Check out the below example



Acme is a small shipping company that has an existing enterprise network comprised of 2 switches DSW1 and ASW1. The topology diagram indicates their layer 2 mapping. VLAN 40 is a new VLAN that will be used to provide the shipping personnel access to the server.

For security reasons, it is necessary to restrict access to VLAN 20 in the following manner:
- Users connecting to ASW1′s port must be authenticate before they are given access to the network.
- Authentication is to be done via a Radius server:
- Radius server host: 172.120.39.46
- Radius key: rad123
- Authentication should be implemented as close to the host device possible.
- Devices on VLAN 20 are restricted to in the address range of 172.120.40.0/24.
- Packets from devices in the address range of 172.120.40.0/24 should be passed on VLAN 20.
- Packets from devices in any other address range should be dropped on VLAN 20.
- Filtering should be implemented as close to the server farm as possible.

The Radius server and application servers will be installed at a future date. You have been tasked with implementing the above access control as a pre-condition to installing the servers.
You must use the available IOS switch features.

Solution

NOTE : Authentication should be Implemented as close to the host device as possible in this case “ASW1″. VLAN filtering should be Implemented as close to the server farm as possible in this case “DSW1″.

This scenario in particular mentions that there is a new VLAN 40 added to the network, however, it does not tell you to configure anything using VLAN 40 so you can ignore it.
Only ports on VLAN 20 are required to be secured using dot1x authentication and the only port configured on VLAN 20 is fa0/1 (this is why ports Fa0/2 and Fa0/3 are not configured with authentication).

Only 172.120.40.0/24 network should be passed on VLAN 20 and packets from devices in any other address range should be dropped on VLAN 20. This suggests that vlan 20 is the only vlan where you need to configure on access-map

First we have to enable aaa authentication on ASW1

1. **ASW1(config)#aaa new-model**
2. **ASW1(config)#radius-server host 172.120.39.46 key rad123**
3. **ASW1(config)#aaa authentication dot1x default group radius**
4. **ASW1(config)#dot1x system-auth-control**

Explanation

1. This is an important command.it enable AAA on the switch globally
2. We configure ASW1 with the IP address of RADIUS server given and given the radius key "rad123" as per requirement.
3. This is how we configure ASW1 to use the RADIUS server for authentication for 802.1X enabled interfaces. You can create multiple groups with RADIUS servers if you want.here we have one RADIUS server which is in the default group.
4. We need to use the dot1x system-auth-control command globally before 802.1X works

Configure Fa0/1 to use 802.1x:

1. **ASW1(config)#interface fastEthernet 0/1**
2. **ASW1(config-if)#switchport mode access (Optional)**
3. **ASW1(config-if)#switchport access vlan 20(Optional)**
4. **ASW1(config-if)#dot1x port-control auto**
5. **ASW1(config-If)#no shut**
6. **ASW1(config-If)#exit**

On the interface level we need to use the "**dot1x port-control auto"** command.In auto mode no client connected to that port will be allowed to pass user traffic until the port has been authorized by the authorization server.

NOTE :Verify configuration using "Show run" command and save the configuration using "copy run start"

Configuring DSW1 Switch

We need to configure VLAN ACL here.Creating of VLAN ACL includes 3 step

1. **Create Access-List**
2. **Create Access MAP**
3. **Applying to a VLAN**

Configuring Access list

1. **DSW1#conf terminal**
2. **DSW1(config)#ip access-list standard 10**
3. **DSW1(config-std-nacl)#permit 172.120.40.0 0.0.0.255**
4. **DSW1(config-std-nacl)#exit**

Create Access MAP

1. **DSW1(config)#vlan access-map MYMAP 1**
2. **DSW1(config-access-map)#match ip address 10**
3. **DSW1(config-access-map)#action forward**
4. **DSW1(config-access-map)#exit**
5. **DSW1(config)# vlan access-map MYMAP 2**
6. **DSW1(config-access-map)# action drop**
7. **DSW1(config-access-map)# exit**

Explanation

1. ”1″ is the line number 1 of the access-map named “MYMAP”
2. ”10″ is the access-list number used to identify the ACL
3. This is the action that will be applied to the traffic matched on ACL “10″ .Here we need to allow traffic so we give "action forward"
4. Even there is a implicit deny at the end like normal ACL,here we giving "action drop" statement to deny other traffic

Apply on VLAN

1. **DSW1(config)#vlan filter MYMAP vlan-list 20**
2. **DSW1(config)#exit**

NOTE : Applies the VLAN access-map named “MYMAP” to vlan 20 DSW1.Verify and save the configuration