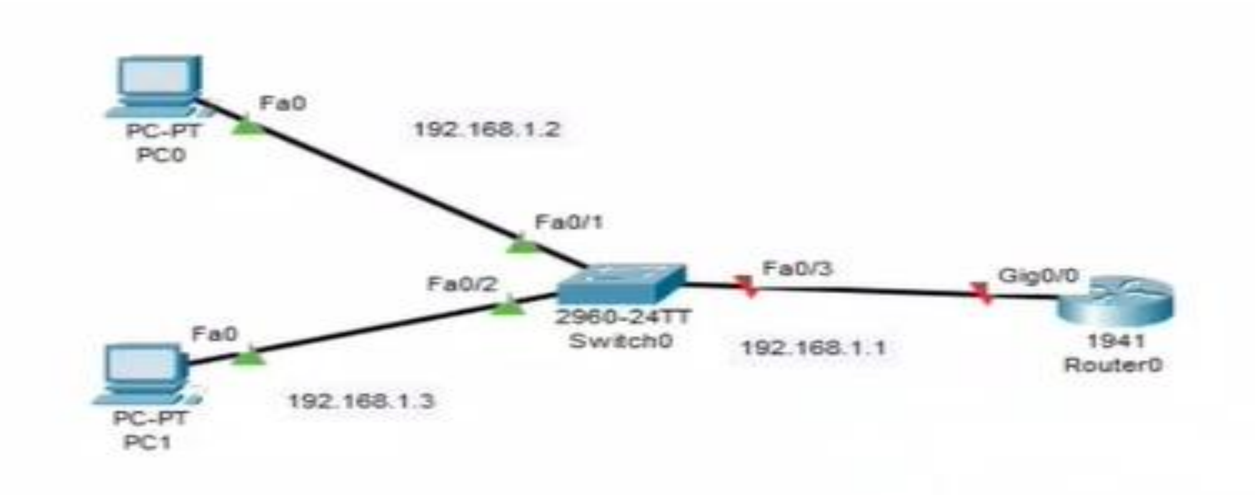
Security In Computing Practical’s

Practical 2: Configure AAA Authentication on Cisco routers

Topology:



Addressing Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	gig0/0	192.168.1.1	255.255.255.0	N/A
PC0	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC1	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives:

- Configure a local user account on R1 and configure authenticate on the console and vty lines using local AAA.
- Verify local AAA authentication from the R1 console and the PC0 client and PC1 Client.

■ Configure Router:

Step 1: Configure password for vty lines

```
R1(config) # line vty 0 4

R1(config-line) #password vtypa55

R1(config-line) #login
```

Step 2: Configure secret on router

```
R1(config) # enable secret enpa55
```

Step 3: Configure OSPF on routers

```
R1(config) #router ospf 1
R1(config-router) #network 192.168.1.0 0.0.0.255 area 0
```

Step 4: Configure OSPF MD5 authentication for all router in area 0

```
R1(config) #router ospf 1
R1(config-router)# area 0 authentication message-digest
```

Step 5: Configure MD5 key for all routers in area 0

```
R1(config)# int gig0/0
R1(config-if)# ip ospf message-digest-key 1 md5 pa55
```

Step 6: Verify configurations.

a. Verify the MD5 authentication configurations using the commands show ip ospf interface.

b. Verify end-to-end connectivity.

Output should be shown in all the routers :

```
R1# show ip ospf interface
Message-digest Authentication Enabled
Youngest key ID is 1
```

Security In Computing Practical’s

Part 1: Configure Local AAA Authentication for Console Access on R1

Step 1: Test Connectivity

```
PC0 > ping 192.168.1.3
Successful
PC1 > ping 192.168.1.2
Successful
```

Step 2: Configure Local username on R1

```
R1(config)# username admin secret adminpa55
```

Step 3: Configure local AAA authentication for console access on R1.

```
R1(config)# aaa new-model
R1(config)# aaa authentication login default local
```

Step 4: Configure the line console to use the defined AAA authentication method.

```
R1(config)# line console 0
R1(config-line)# login authentication default
```

Step 5: Verify the AAA authentication method.

```
R1(config-line)# end
User Access Verification
Username: admin
Password: adminpa55
R1>
```

Part 2: Configure Local AAA Authentication for vty Lines on R1

Step 1: Configure domain name and crypto key for use with SSH.

```
R1(config)# ip domain-name ccnasecurity.com

R1(config)# crypto key generate rsa

How many bits in the modulus [512]: 1024
```

Step 2: Configure a named list AAA authentication method for the vty lines on R1.

```
R1(config)# aaa authentication login SSH-LOGIN local
```

Step 3: Configure the vty lines to use the defined AAA authentication method.

```
R1(config)# line vty 0 4

R1(config-line)# login authentication SSH-LOGIN

R1(config-line)# transport input ssh

R1(config-line)# end
```

Step 4: Verify the AAA authentication method.

```
PC0> ssh –l Admin 192.168.1.1

Password: adminpa55

R1>

PC1> ssh –l Admin 192.168.1.1

Password: adminpa55

R1>
```