Practical 2

- Configure AAA Authentication on Cisco Routers - Packet Tracer Configure a local user account on Router and configure authenticate on the console and vty lines using local AAA.

Addressing Table

Device	Interface	IP addresses	Subnet Mask	Default Gateway	Switch Port
R1	G 0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
R2	G 0/0	192.168.2.1	255.255.255.0	N/A	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
R3	G 0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
TACACS +Server	NIC	192.168.2.2	255.255.255.0	192.168.2.1	S2 F0/6
RADIUS Server	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 F0/1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/8

Part1: Configure Local AAA Authentication for console Access on R1

Step1: Test Connectivity

```
PC > ping 192.168.1.3
PC > ping 192.168.2.3
PC > ping 192.168.3.3
```

Step 2: Configure a local username on R1

```
R1 (config) # username Admin1 secret admin1pa55
```

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) #~~ (config-line)# login authentication default
```

Step 5: Verify the AAA authentication method.

```
R1 (config-line) # end
R1 # exit
```

Part 2 : Configure local AAA authentication for vty lines on R1

Step1: Configure domain name and crypto key for use with SSH

```
R1(config)# ip domain-name ccnasecurity.com
R1(config)# crypto key generate rsa
```

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

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

Step3: 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

```
PC> ssh -l Admin1 192.168.1.1.
Open
Password: admin1pa55
```

Part 3: Configure server-based AAA authentication using TACACS+ on R2

Step1: Configure a backup local database entry called Admin

```
R2(config)# username Admin2 secret admin2pass
```

Step 2: Verify the TACACS+ Server Configuration

Click the TACACS+ Server. On the services tab, click AAA. Notice that there is a network configuration entry for R2 and a user setup entry for Admin2

step3: Configure the TACACS+ Server specifics on R2

```
R2 (config)# tacacs-server host 192.168.2.2
R2 (config)# tacacs-server key tacacspass
```

Step4: Configure AAA login authentication for console access on R2

```
R2 (config)# aaa new-model
R2 (config)# aaa authentication login default group
                tacacs+ local
```

Step5: Configure the line console to ~~be~~ use the defined AAA authentication model.

```
R2 (config)# line console 0
```

R2 (config- line)# login authentication default

Step 6: Verify the AAA authentication method.

R2 (config-line)# end
R2 # exit

PART 4: Configure server based AAA Authentication using Radius on R3.

Step 1: Configure a backup local database entry called Admin

```
R3 (config)# username Admin3 secret admin3pa55
```

Step 2: Verify the RADIUS server configuration

click the RADIUS server
On the services tab, click AAA.
Notice that there is a Network configuration entry for R3 and a user setup entry for Admin3

Step 3: Configure Radius server specifies on R3

```
R3 (config) # radius-server host 192.168.3.2
R3 (config) # radius-server key radiuspa55
```

Step 4: Configure AAA login authentication for console acess on R3.

```
R3 (config) # aaa new-model
R3 (config) # aaa authentication login default
            group radius local.
```

Step 5: Configure the line console to use the defined AAA authentication method.

```
R3(config)# line console 0
R3(config-line)# login authentication default
```

Step 6: verify the AAA authentication method

```
R3(config-line)#end.
R3#exit
```