Practical 2: Configure AAA authentication

IP Addressing Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Gig0/0	192.168.1.1	255.255.255.0	-
	Se0/1/0	10.1.1.1	255.255.255.252	-
R2	Gig0/0	192.168.2.1	255.255.255.0	-
	Se0/1/0	10.1.1.2	255.255.255.252	-
	Se0/1/1	10.2.2.2	255.255.255.252	-
R3	Gig0/0	192.168.3.1	255.255.255.0	-
	Se0/1/0	10.2.2.1	255.255.255.252	-
TACACS+	Fa0	192.168.2.2	255.255.255.0	192.168.2.1
RADIUS	Fa0	192.168.3.2	255.255.255.0	192.168.3.1
PC1	Fa0	192.168.1.3	255.255.255.0	192.168.1.1
PC2	Fa0	192.168.2.3	255.255.255.0	192.168.2.1
PC3	Fa0	192.168.3.3	255.255.255.0	192.168.3.1

Router OSPF:

R1:

R1(config)#router ospf 1

R1(config-router)#network 192.168.1.1 0.0.0.255 area 0

R1(config-router)#network 10.1.1.2 0.255.255.255 area 0

R1(config-router)#exit

R2:

R2(config)#router ospf 1

R2(config-router)#network 192.168.2.1 0.0.0.255 area 0

R2(config-router)#network 10.1.1.1 0.255.255.255 area 0

R2(config-router)#network 10.2.2.1 0.255.255.255 area 0

R2(config-router)#exit

R3:

R3(config)#router ospf 1

R3(config-router)#network 192.168.3.1 0.0.0.255 area 0

R3(config-router)#network 10.2.2.2 0.255.255.255 area 0

R3(config-router)#exit

a. Configure Local AAA authentication for R1

1. Check Connectivity from all PCs

2. Configure AAA

R1(config)#username admin1 secret admin1pa55

R1(config)#aaa new-model

R1(config)#aaa authentication login default local

R1(config)#line console 0

R1(config-line)#login authentication default

R1(config-line)#end

R1#exit

User Access Verification

Username: admin1

Password: admin1pa55

R1>

b. Configure Local AAA Authentication for vty lines on R1

R1(config)#ip domain-name tyit.com

R1(config)#crypto key generate rsa.

How many bits in the modulus [512]: 1024

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

R1(config)#line vty 0 4

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

R1(config-line)#transport input ssh

R1(config-line)#end

Verify the AAA Authentication

In PC1, open command prompt

C:\ > ssh -l admin1 192.168.1.1

Password: admin1pa55

This should be successful.

c. Configure server-based AAA authentication using TACACS+ on R2

1. In TACACS+

Go to services and under AAA section make Service On

In **Network Configuration**, enter

Client Name: R2, Client IP: 192.168.2.1, Secret tacacspa55 and ServerType Tacacs and Click Add

In **User Setup**, enter

Username: admin2 and Password: admin2pa55 and Click Add

2. In R2

R2(config)#username admin2 secret admin2pa55

R2(config)#tacacs-server host 192.168.2.2

R2(config)#tacacs-server key tacacspa55

R2(config)#aaa new-model

R2(config)#aaa authentication login default group tacacs+ local

R2(config)#line console 0

R2(config-line)#login authentication default

R2(config-line)#end

R2#exit

User Access Verification

Username: admin2

Password: admin2pa55

R2>

This should be successful

d. Configure server-based AAA authentication RADIUS on R3

1. In RADIUS

Go to services and under AAA section make Service On

In **Network Configuration**, enter

Client Name: R3, Client IP: 192.168.3.1, Secret radiuspa55 and ServerType Radius and Click Add

In **User Setup**, enter

Username: admin3 and Password: admin3pa55 and Click Add

R3(config)#username admin3 secret admin3pa55

R3(config)#radius-server host 192.168.3.2

R3(config)#radius-server key radiuspa55

R3(config)#aaa new-model

R3(config)#aaa authentication login default group radius local

R3(config)#line console 0

R3(config-line)#login authentication default

R3(config-line)#end

R3#exit

User Access Verification

Username: admin3

Password: admin3pa55

R3>

This should be successful