Practical 3 : configure AAA Authentication

Step 3: Configure local database authentication on console

```
R1: R1>en
    R1# conf t
    R1(Config)# username Admin1 secret admin1 pass
              # aaa new-model (Applying AAA security...
              # aaa authentication login dyfault local
```

aaa authentication login → configure authentication for login to the device

dyfault → this method should be made dyfault

local → routers should use locally config data

```
# line console 0 (console port 0 configⁿ)
# login authentication dyfault
```

login authentication → specifies that login authentication should be done

dyfault → apply whatever setting you made default above

```
# end
# exit
```

→ Enter username & password.

Step 4: Configure local AAA Authenticatⁿ for vty lines on R1.

(Configure domain Name & crypto key for SSH)

```
R1(config)# ip domain-name ccnasecurity.com
           # crypto key generate ~~RSA~~ rsa
             1024
```

Step 5: Configure a named list AAA method for vty lines.

Named list means a group that contains specific methods here, we use SSH-LOGIN as named list containing all local AAA ~~(i.e. local, TACACS+ & RADIUS login)~~ (local creds)

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

aaa authentication login → specific that settings are being configed for ~~local~~ login attemps

SSH-LOGIN → named list

local → The local creds database should be used for authentication.

Step 6: Config vty lines

```
(config)# line vty 0 4
         # login authentication SSH-LOGIN
         # transport input ssh
```

Step 7: verify the AAA method

PC-A > Cmd > ssh -l Admin1 192.168.1.1
password adminpa55

Part 2: Configure Server based AAA using TACACS+ R2

R2(config)# username Admin2 secret admin2pa55

a backup local DB entry for ensuring that user can login even if TACACS+ server is down.

→ Go to TACACS+ server → services → AAA
On → client name R2, IP: 192.168.2.1
secret - tacacspa55, server Type: TACACS+ > Add
username - Admin2 password: admin2pa55 > Add

→ Configure AAA login for console on R2

```
R2(config)# tacacs-server host 192.168.2.2 # tacacs-server key tacacspa55
R2(config)# aaa new-model
            # aaa authentication login default group tacacs+ local
```

authenticatn should be attempted using Tacacs+ server group if it fails fall to local. dB.

```
# line console 0   # login authentication default
# end   # exit → login using username & pass
```

Repeat the same for RADIUS server

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

→ RADIUS server → Services → AAA → On → Client Name: R3
IP: 192.168.3.1, secret - radiuspa55, server Type: Radius > Add
UN: Admin3 password: admin3pa55 > Add

```
# radius-server host 192.168.3.2 # radius-server key radiuspa55
R3(config)# aaa ...
# "       "        group radius local
# line console 0
# login authenticatn default
# end
# exit
```

To verify try to login using the UN & Pass.