PRACTICAL NO 3: Configure AAA Authentication on Cisco Routers

To provide a centralized management system for the authentication, authorization and accounting (AAA framework), Access Control Server (ACS) is used. For the communication between the client and the ACS server, two protocols are used namely TACACS+ and RADIUS.

TACACS+
Terminal Access Controller Access Control System (TACACS+) is Cisco proprietary protocol which is used for the communication of the Cisco client and Cisco ACS server. It uses TCP port number 49 which makes it reliable.

RADIUS –
Remote Access Dial In User Service (RADIUS) is an open standard protocol used for the communication between any vendor AAA client and ACS server. If one of the client or server is from any other vendor (other than Cisco) then we have to use RADIUS. It uses port number 1812 for authentication and authorization and 1813 for accounting.

TACACS+	RADIUS
Cisco proprietary protocol	open standard protocol
It uses TCP as transmission protocol	It uses UDP as transmission protocol
It uses TCP port number 49.	It uses UDP port number 1812 for authentication and authorization and 1813 for accounting.
Authentication, Authorization and Accounting is separated in TACACS+.	Authentication and Authorization is combined in RADIUS.
All the AAA packets are encrypted.	Only the passwords are encrypted while the other information such as username, accounting information etc are not encrypted.
Preferably used for ACS.	used when ISE is used
It provides more granular control i.e can specify the particular command for authorization.	No external authorization of commands supported.
TACACS+ offers multiprotocol support	No multiprotocol support.

Used for device administration.	used for network access

Similarities –

The process is start by Network Access Device (NAD – client of TACACS+ or RADIUS). NAD contact the TACACS+ or RADIUS server and transmit the request for authentication (username and password) to the server. First, NAD obtain username prompt and transmit the username to the server and then again the server is contact by NAD to obtain password prompt and then the password is send to the server.

The server replies with access-accept message if the credentials are valid otherwise send an access-reject message to the client. Further authorisation and accounting is different in both protocols as authentication and authorisation is combined in RADIUS

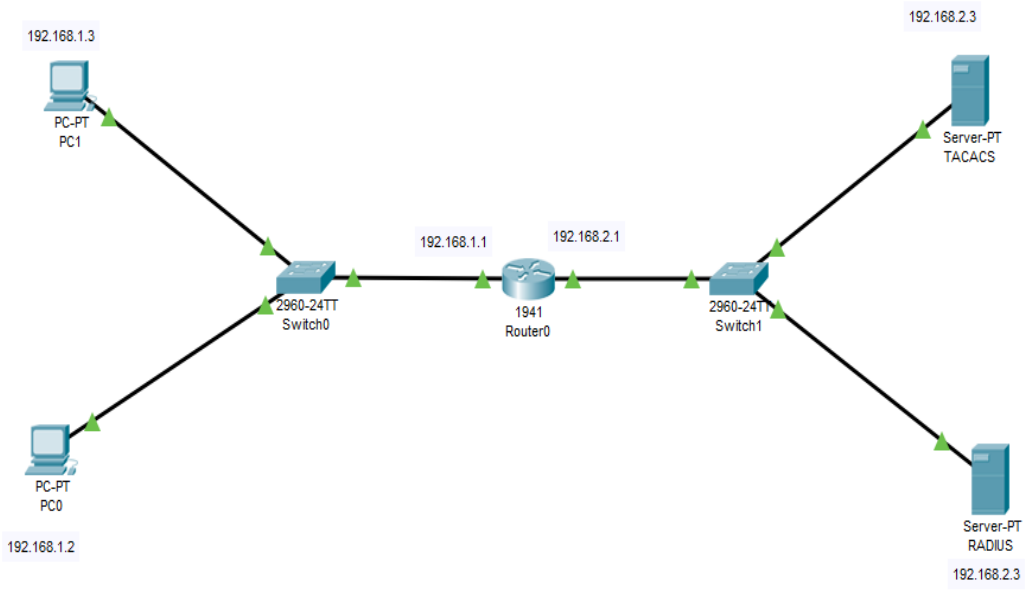
Advantages (TACACS+ over RADIUS) –

1. As TACACS+ uses TCP therefore more reliable than RADIUS.
2. TACACS+ provides more control over the authorization of commands while in RADIUS, no external authorization of commands is supported.
3. All the AAA packets are encrypted in TACACS+ while only the passwords are encrypted in RADIUS i.e more secure.

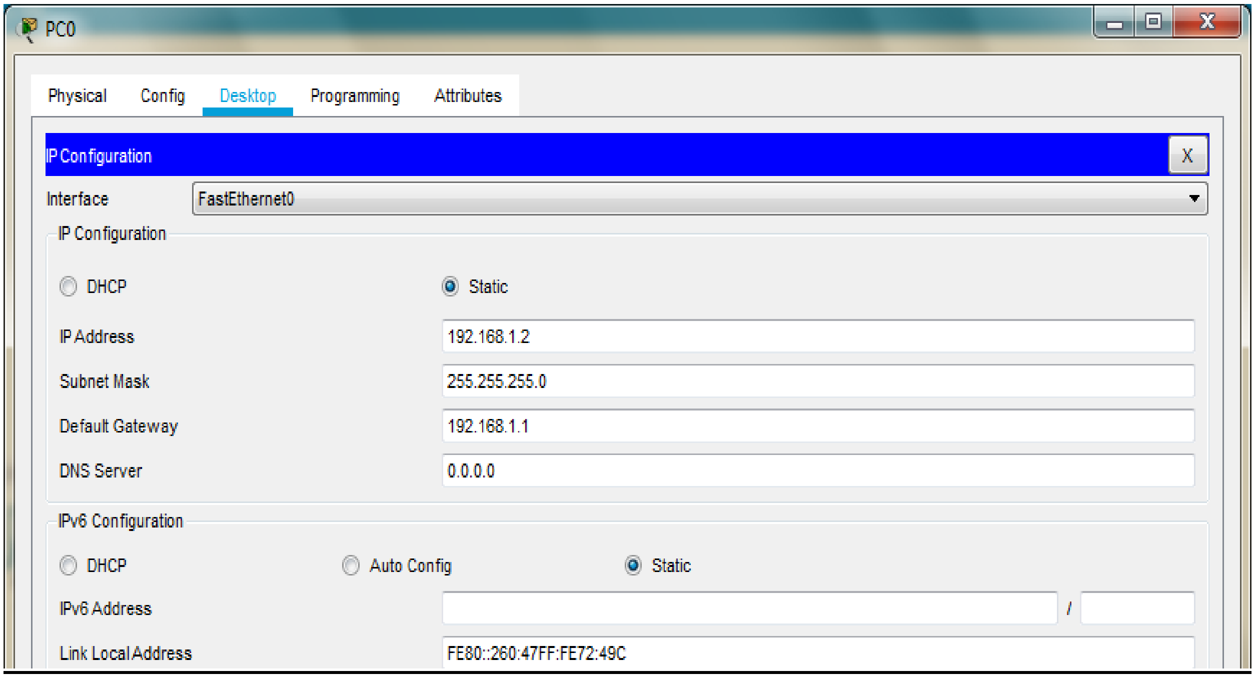
Advantage (RADIUS over TACACS+) –

1. As it is open standard therefore RADIUS can be used with other vendors device while because TACACS+ is Cisco proprietary, it can be used with Cisco devices only.
2. It has more extensive accounting support than TACACS+.

We use the following Topology for the present case



Configuring PC0



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IP Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 0.0.0.0

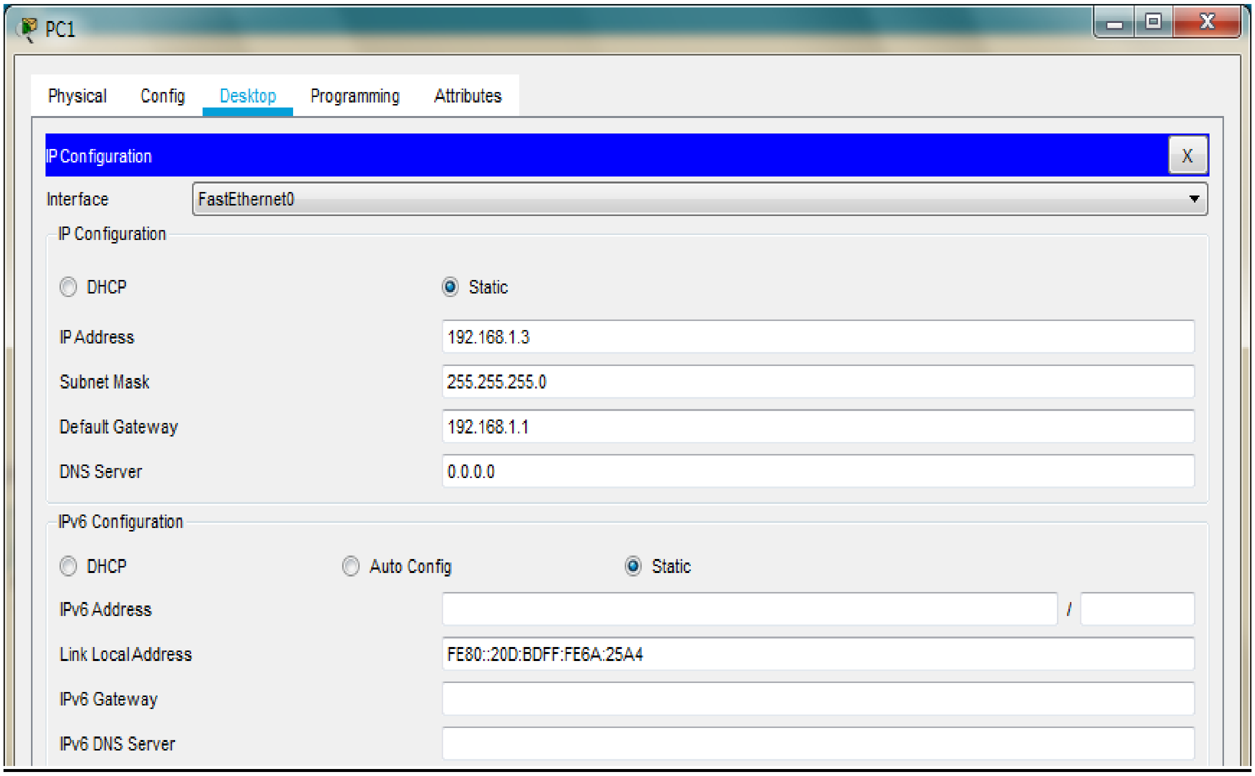
IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address: /

Link Local Address: FE80::260:47FF:FE72:49C

Configuring PC1



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IP Address: 192.168.1.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

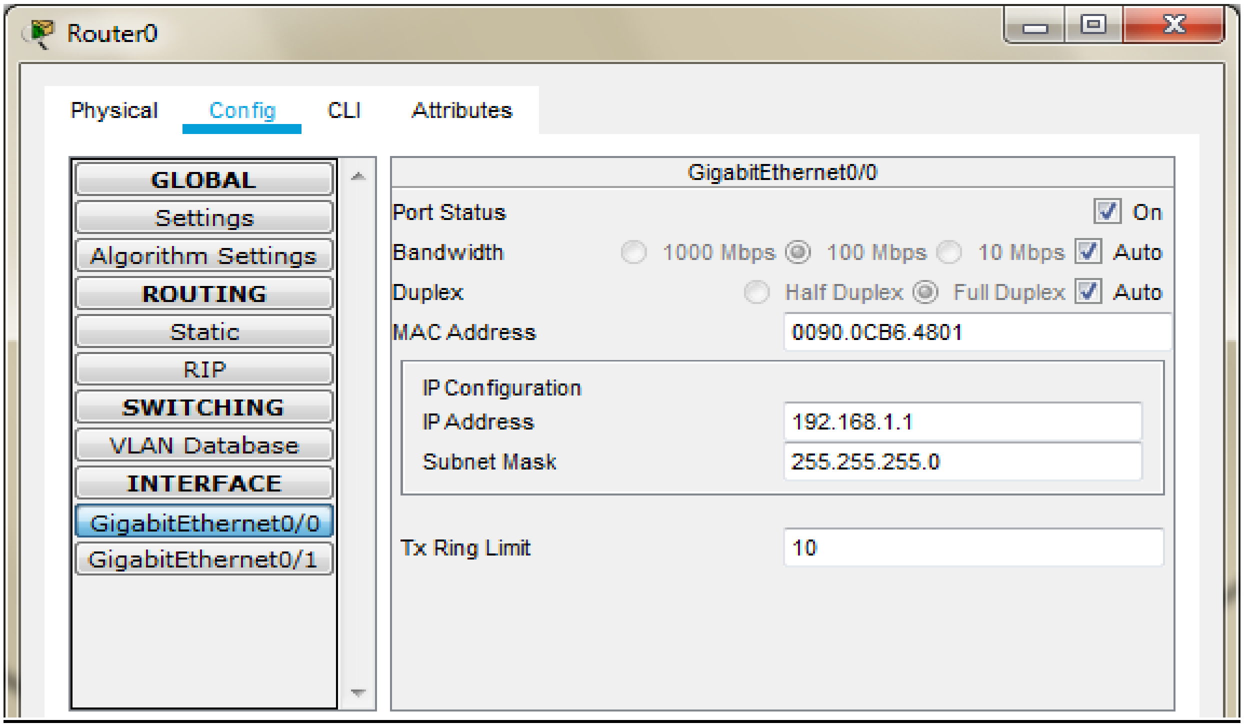
IPv6 Address: /

Link Local Address: FE80::20D:BDFF:FE6A:25A4

IPv6 Gateway:

IPv6 DNS Server:

Configuring Router0

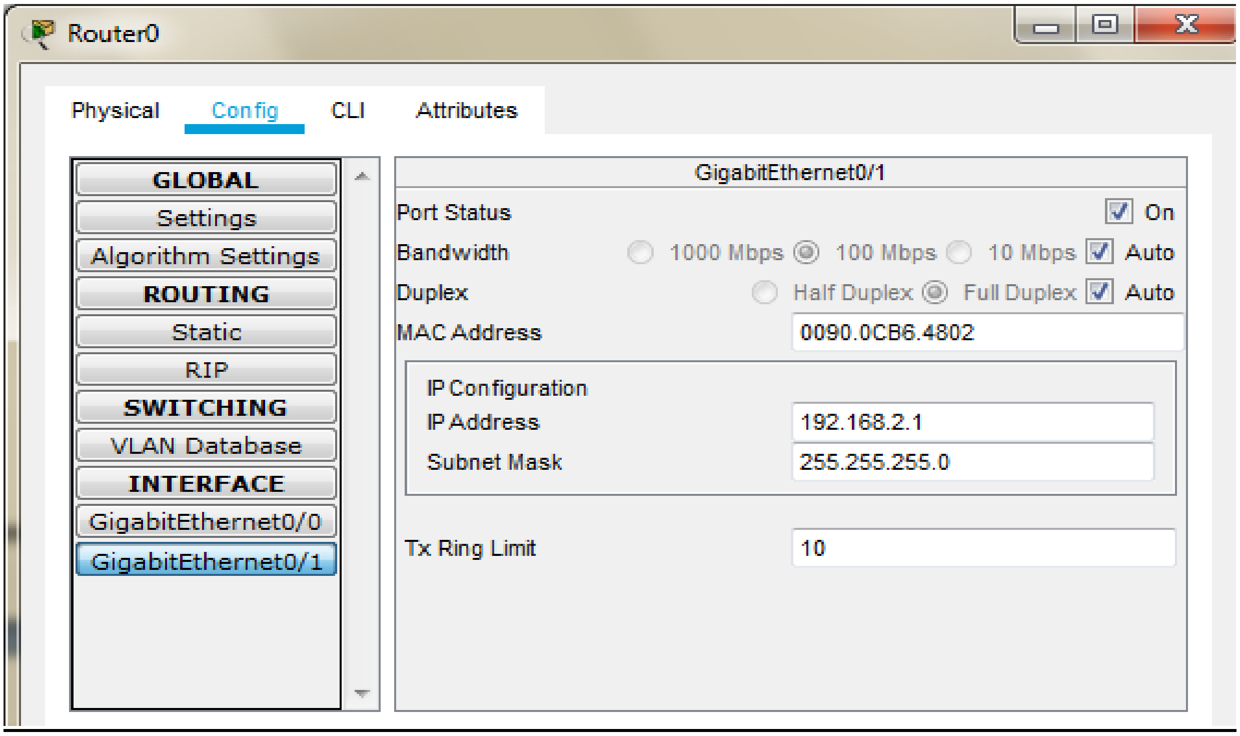


GigabitEthernet0/0

Port Status	☑ On
Bandwidth	○ 1000 Mbps ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex	○ Half Duplex ● Full Duplex ☑ Auto
MAC Address	0090.0CB6.4801

IP Configuration

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Tx Ring Limit	10



GigabitEthernet0/1

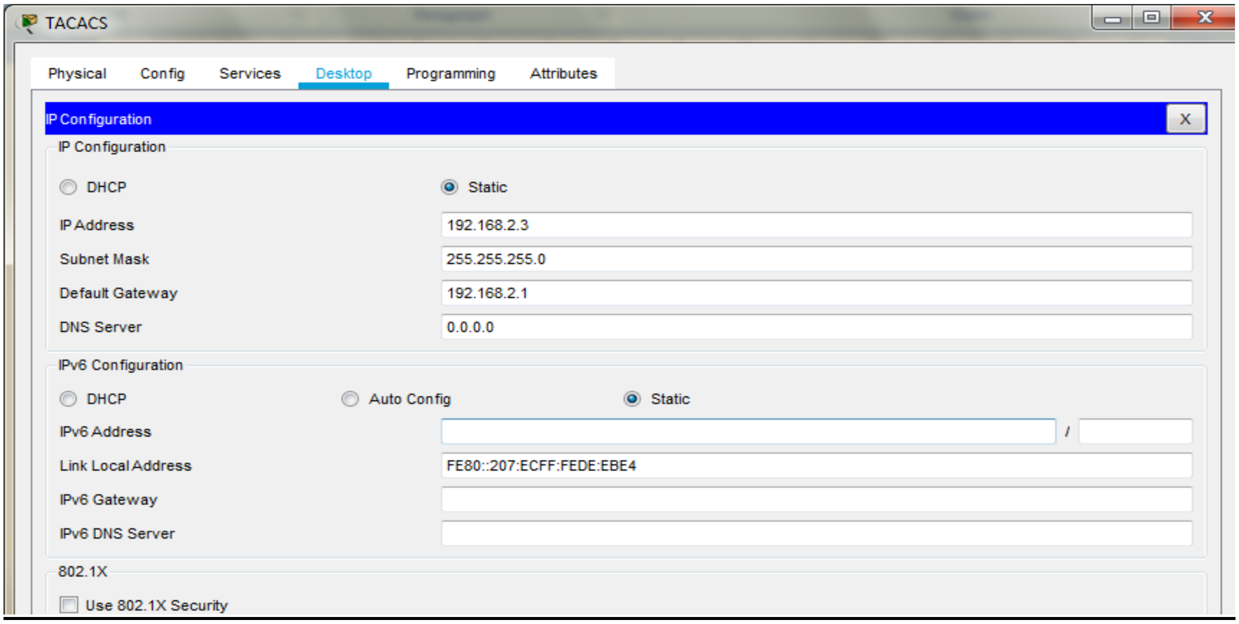
Port Status	☑ On
Bandwidth	○ 1000 Mbps ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex	○ Half Duplex ● Full Duplex ☑ Auto
MAC Address	0090.0CB6.4802

IP Configuration

IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Tx Ring Limit	10

Configuring Server0 (As TACACS)

While configuring the TACACS/RADIUS server the Client IP address must be the Router IP



IP Configuration

IP Configuration

○ DHCP ● Static

IP Address	192.168.2.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server	0.0.0.0

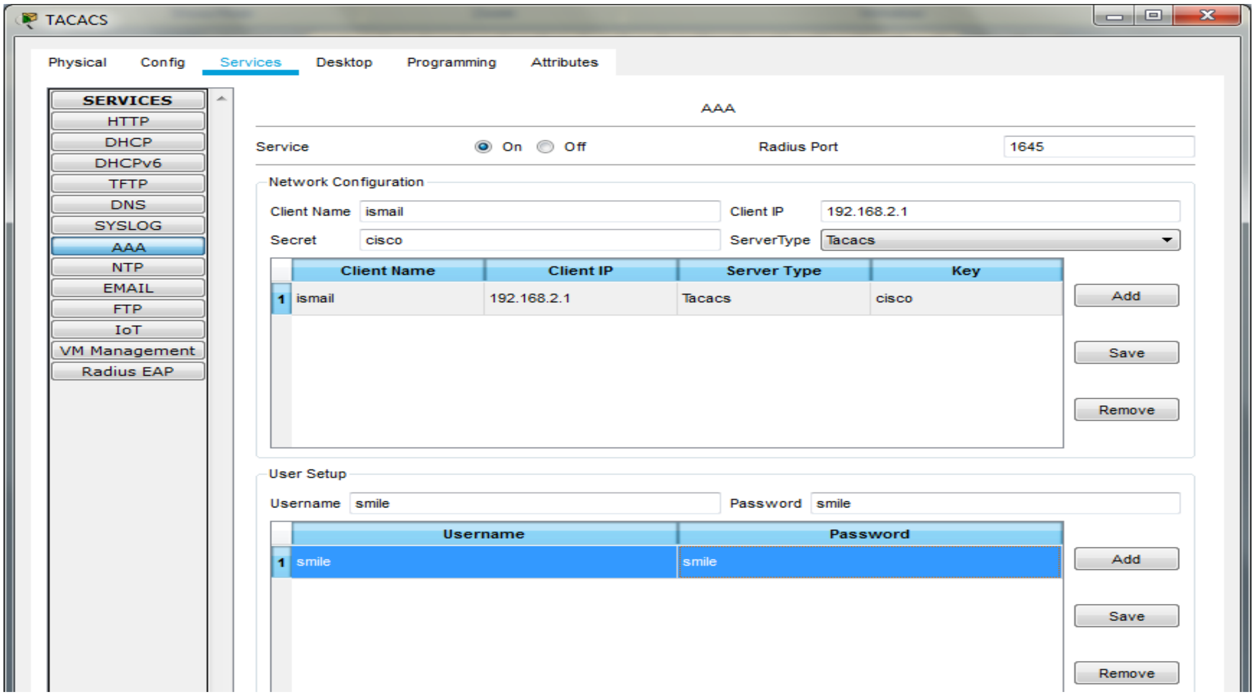
IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address	/
Link Local Address	FE80::207:ECFF:FEDE:EBE4
IPv6 Gateway	
IPv6 DNS Server	

802.1X

□ Use 802.1X Security



AAA

Service ● On ○ Off Radius Port 1645

Network Configuration

Client Name ismail Client IP 192.168.2.1

Secret cisco ServerType Tacacs

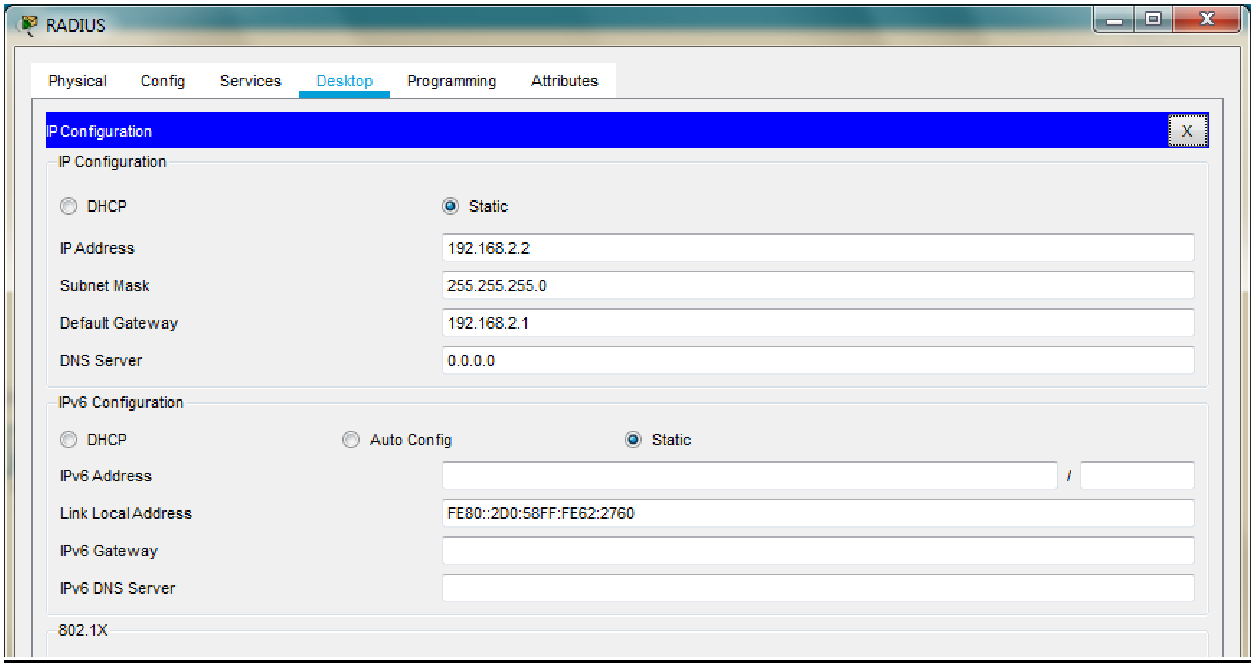
	Client Name	Client IP	Server Type	Key
1	ismail	192.168.2.1	Tacacs	cisco

User Setup

Username smile Password smile

	Username	Password
1	smile	smile

Configuring Server1 (As RADIUS)



IP Configuration

IP Configuration

○ DHCP ● Static

IP Address: 192.168.2.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

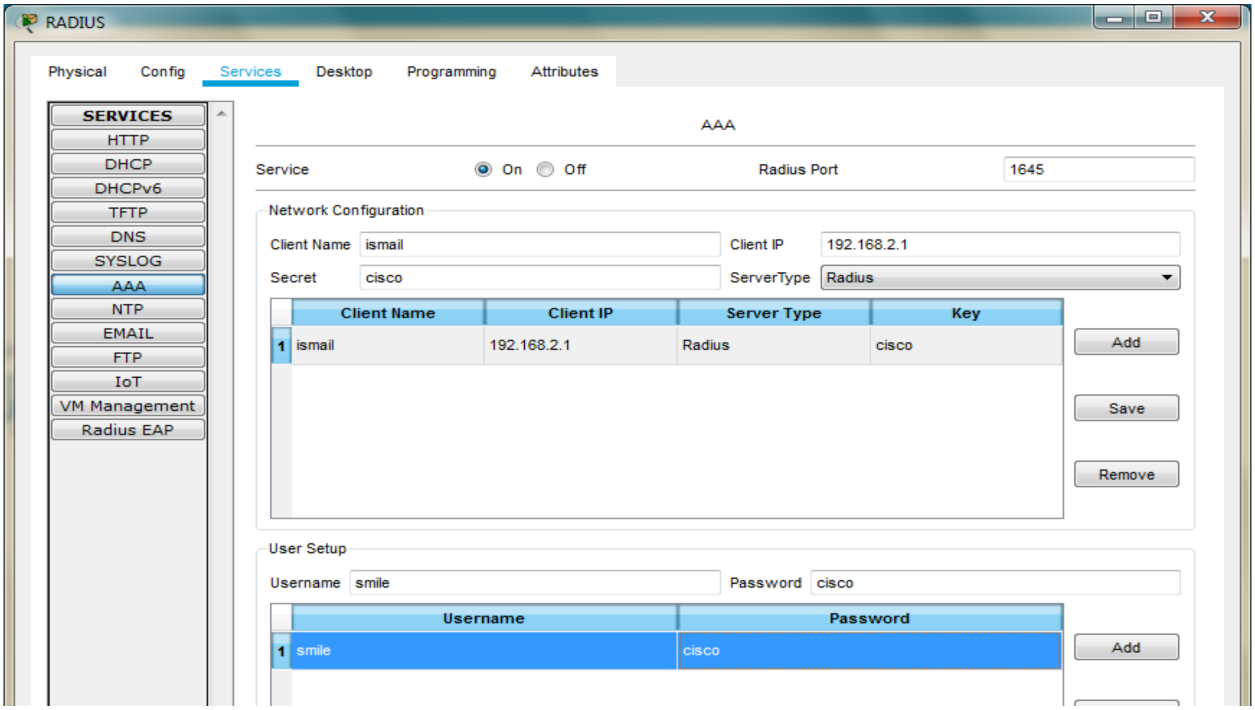
IPv6 Address: /

Link Local Address: FE80::2D0:58FF:FE62:2760

IPv6 Gateway:

IPv6 DNS Server:

802.1X



AAA

Service ● On ○ Off Radius Port 1645

Network Configuration

Client Name: ismail Client IP: 192.168.2.1

Secret: cisco ServerType: Radius

	Client Name	Client IP	Server Type	Key
1	ismail	192.168.2.1	Radius	cisco

User Setup

Username: smile Password: cisco

	Username	Password
1	smile	cisco

Type the following commands in the CLI mode of the Router0

```
Router>enable
Router#configure terminal
Router(config)#aaa new-model
Router(config)#tacacs-server host 192.168.2.3 key cisco
Router(config)#radius-server host 192.168.2.2 key cisco
Router(config)#aaa authentication login ismail group tacacs+ group radius local
Router(config)#line vty 0 4
Router(config-line)#login authentication ismail
Router(config-line)#exit
Router(config)#
```

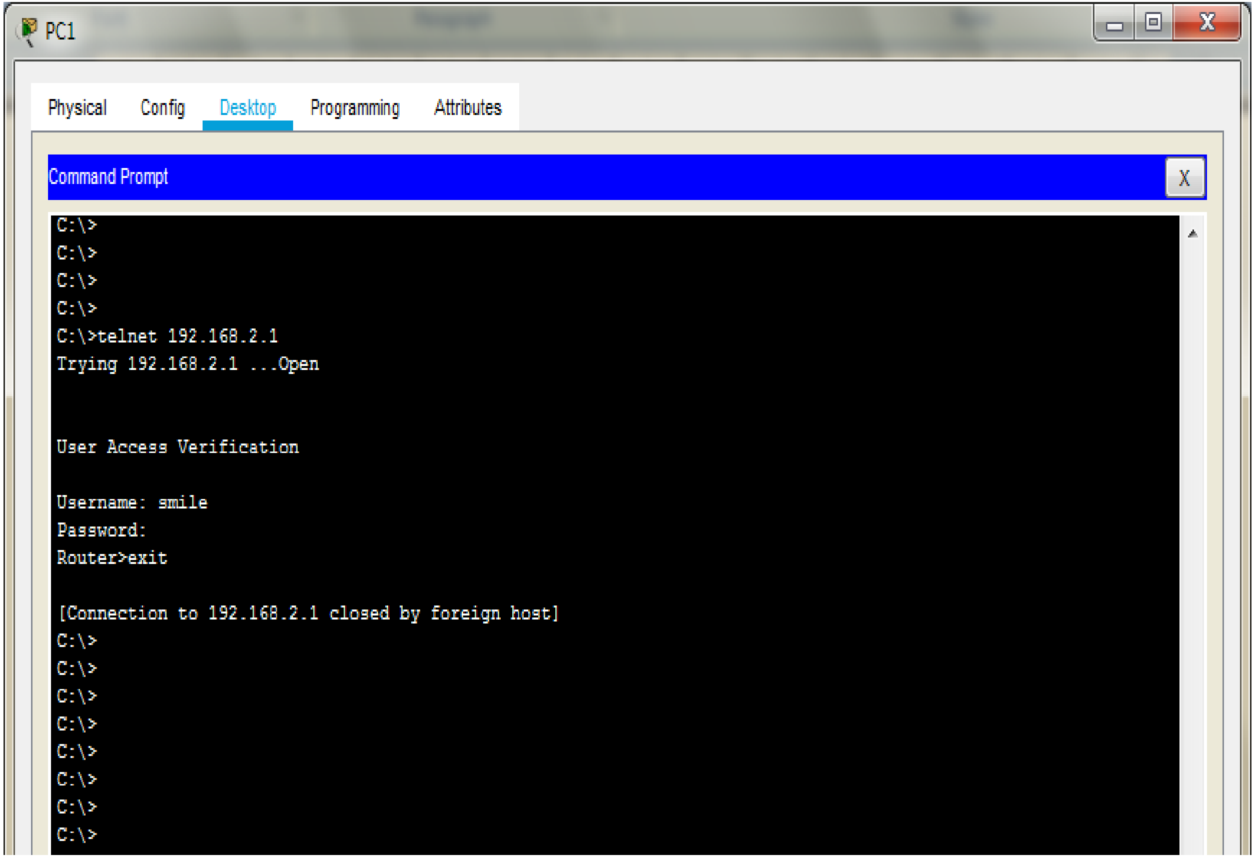
The Authentication can be done by typing the command **telnet 192.168.2.1 (**the Router IP**)** in any of the PCs

We get a prompt to type the username and password, the username and password set in TACACS are entered

Username: smile

Password: smile

We get the following



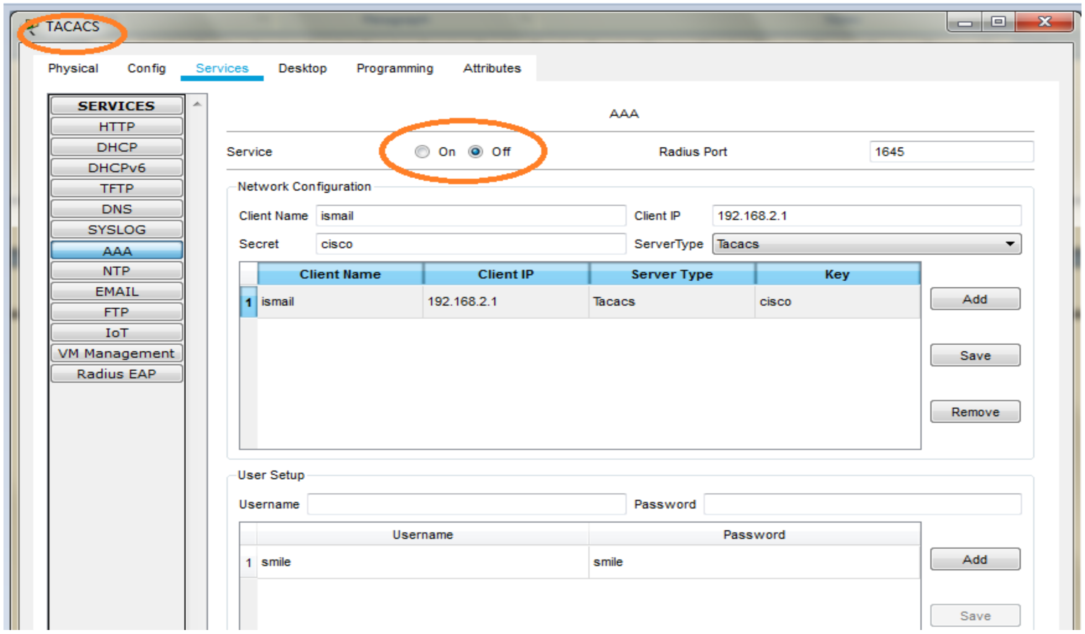
```
C:\>
C:\>
C:\>
C:\>
C:\>telnet 192.168.2.1
Trying 192.168.2.1 ...Open


User Access Verification

Username: smile
Password:
Router>exit

[Connection to 192.168.2.1 closed by foreign host]
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
```

In order to authenticate the RADIUS server we need to turn OFF the TACACS service



AAA

Service ○ On ● Off Radius Port 1645

Network Configuration

Client Name ismail Client IP 192.168.2.1

Secret cisco ServerType Tacacs

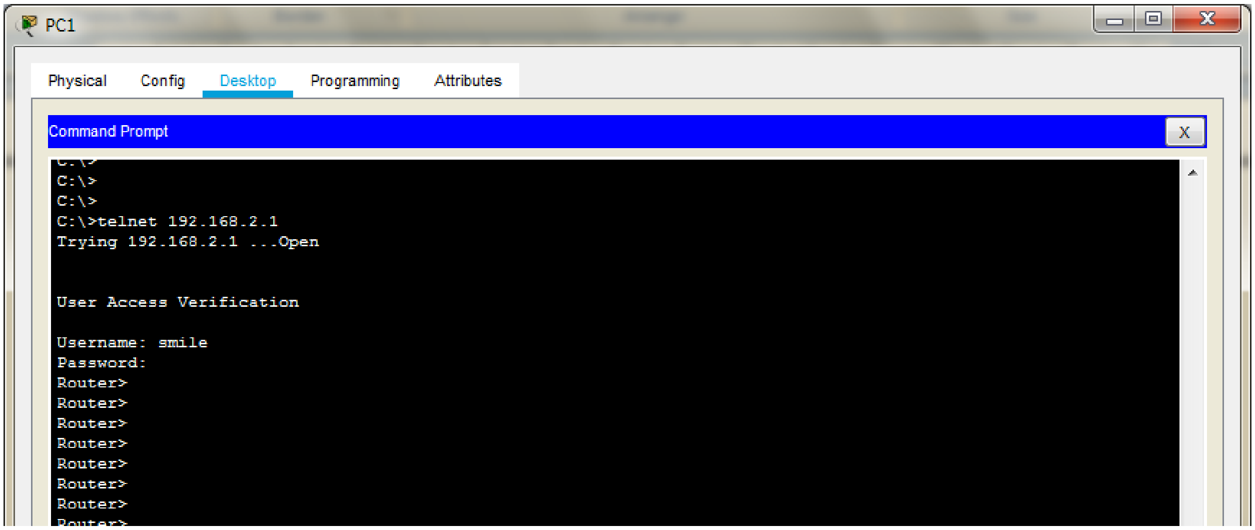
	Client Name	Client IP	Server Type	Key
1	ismail	192.168.2.1	Tacacs	cisco

User Setup

Username Password

	Username	Password
1	smile	smile

We again enter the command **telnet 192.168.2.1 (**the Router IP**)** and enter the username and password of the RADIUS server (Username: smile , Password: cisco)
We get the following



```
C:\>
C:\>
C:\>
C:\>telnet 192.168.2.1
Trying 192.168.2.1 ...Open


User Access Verification

Username: smile
Password:
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
```

The local login can also be verified by turning OFF both TACACS and RADIUS service. The username and Password are both cisco (by default)
Hence the authentication through both TACACS and RADIUS