PRACTICAL NO 2: 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 servers 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	Authentication, Authorization and Accounting is combined
All the AAA packets are encrypted	Only the passwords are encrypted while the other information such as username, accounting information 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
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 sent 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.

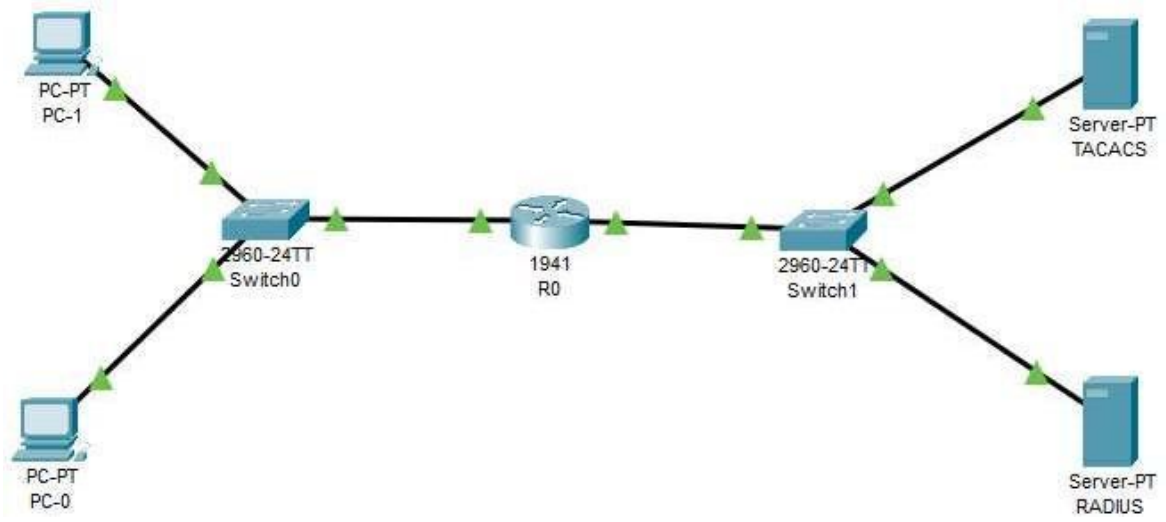
Advantages (TACACS+ over RADIUS) –

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+.

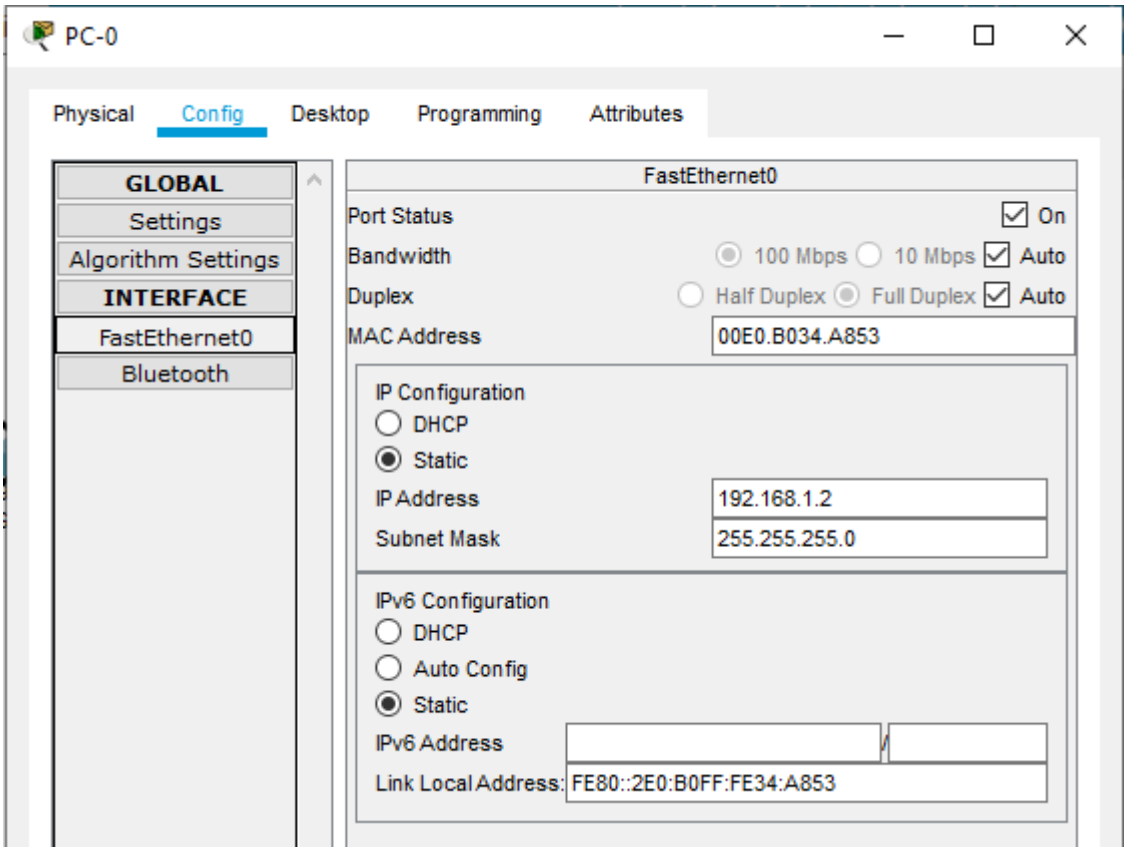
Let us consider the following Topology to understand the above AAA authentication.



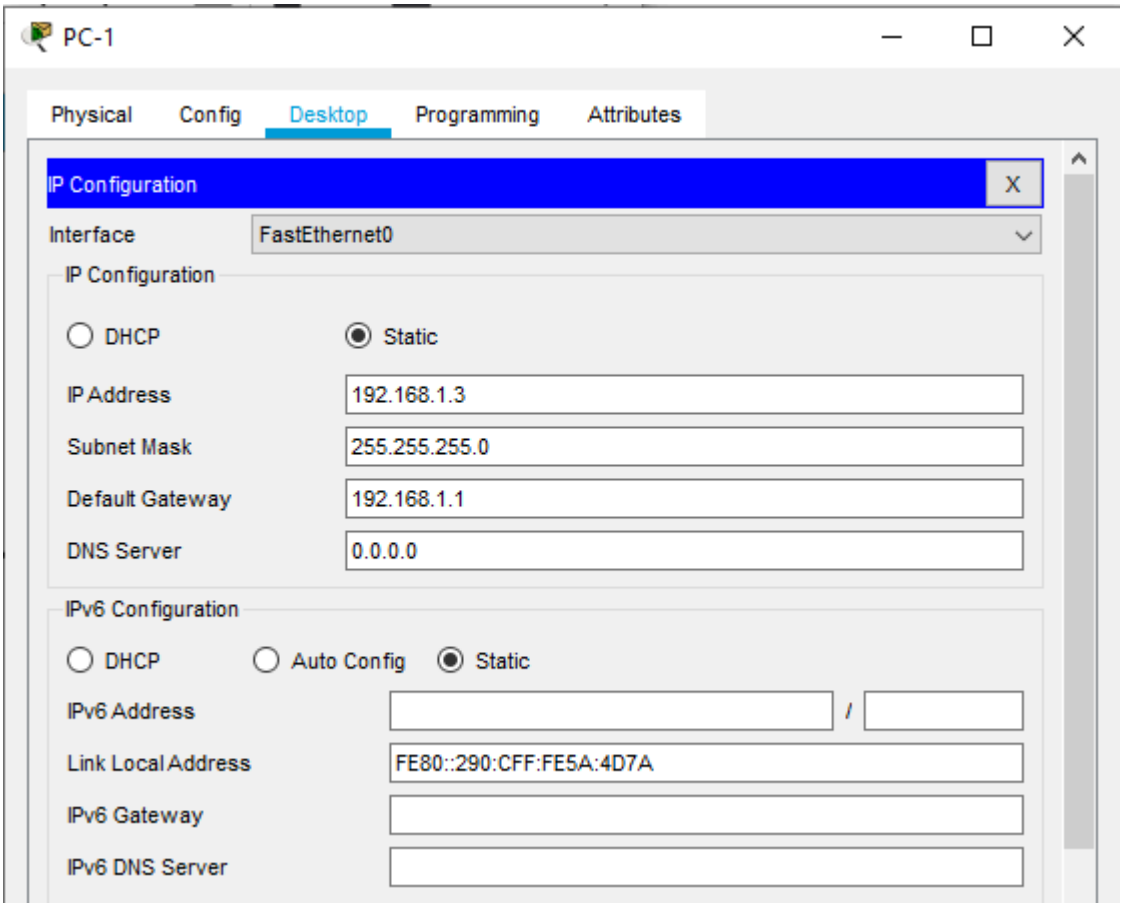
Let us consider the following Address table to configure the network devices:

Device	Interface	IP Address	Subnet Mask	Default gatewa y	Switch Port
TACACS	NIL	192.168.2.3	255.255.255.0	192.168.2.1	S1 F0/6
RADIUS	NIL	192.168.2.2	255.255.255.0	192.168.2.1	S1 F0/1
PC-0	NIL	192.168.1.2	255.255.255.0	192.168.1.1	S0 F0/6
PC-1	NIL	192.168.1.3	255.255.255.0	192.168.1.1	S0 F0/1
R0	GE0/0	192.168.1.1	255.255.255.0	NA	S0 F0/5
	GE0/1	192.168.2.1	255.255.255.0	NA	S1 F0/5

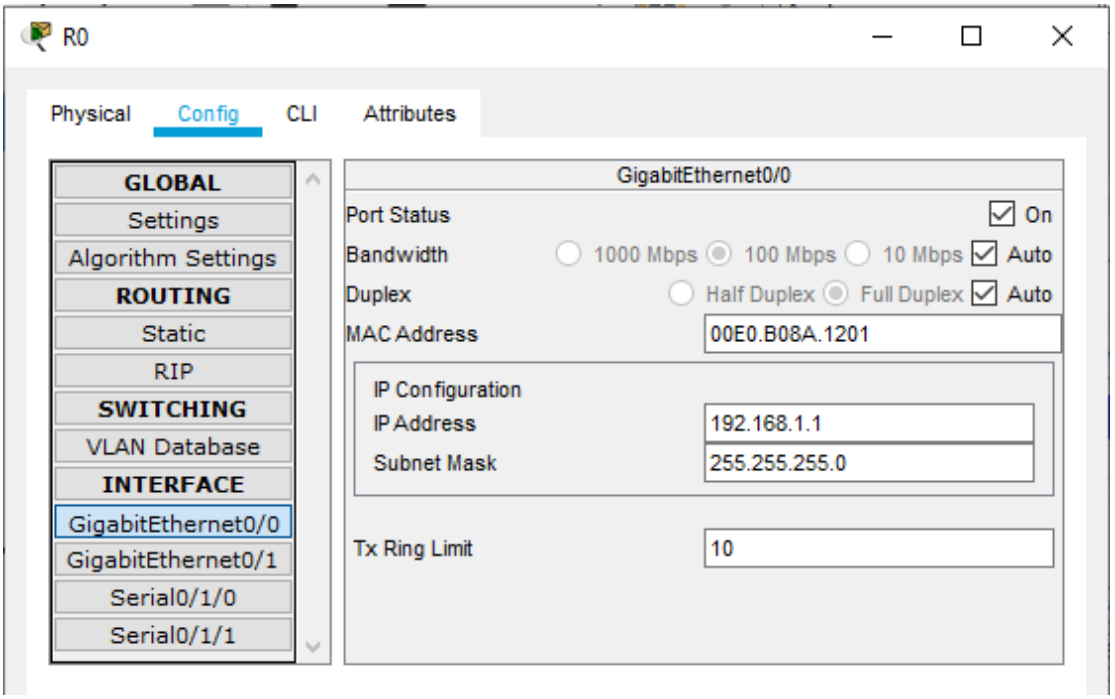
Configuring PC-0

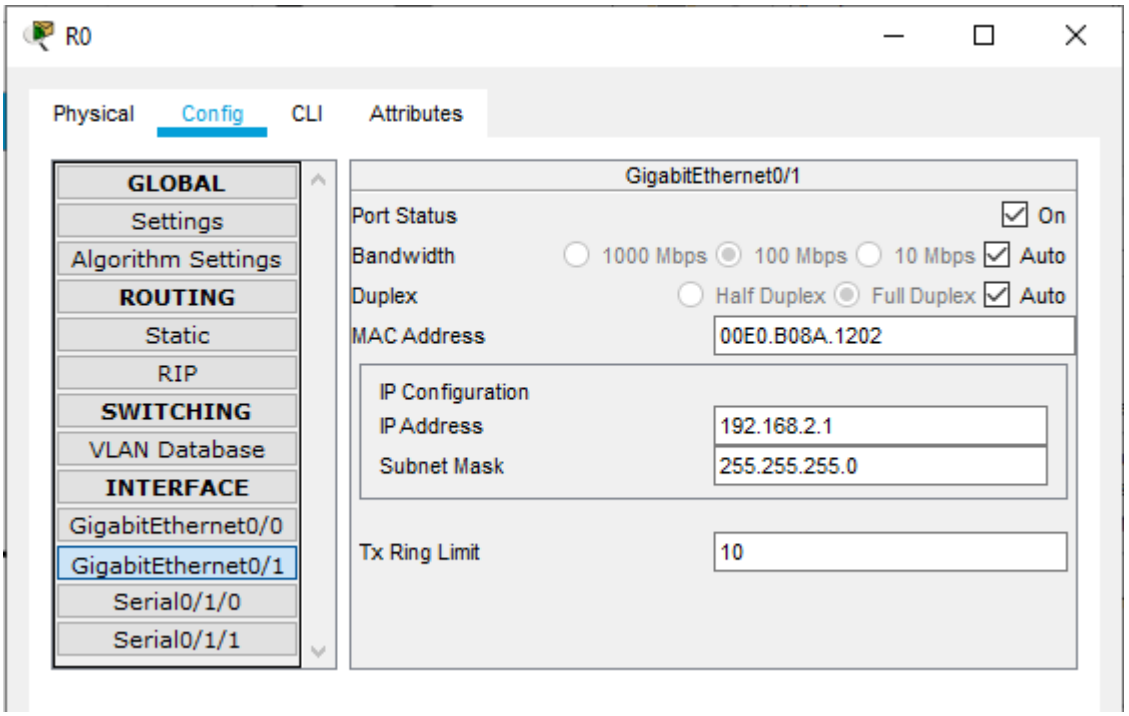


Configuring PC-1

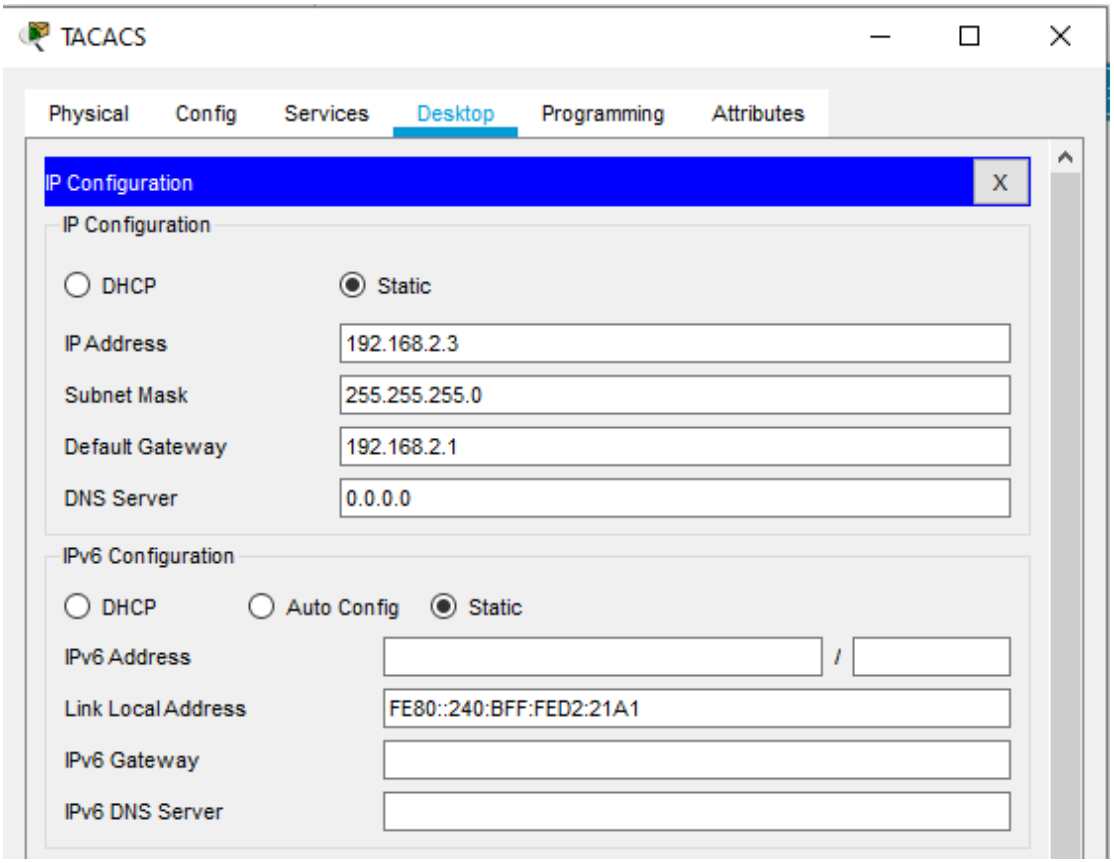


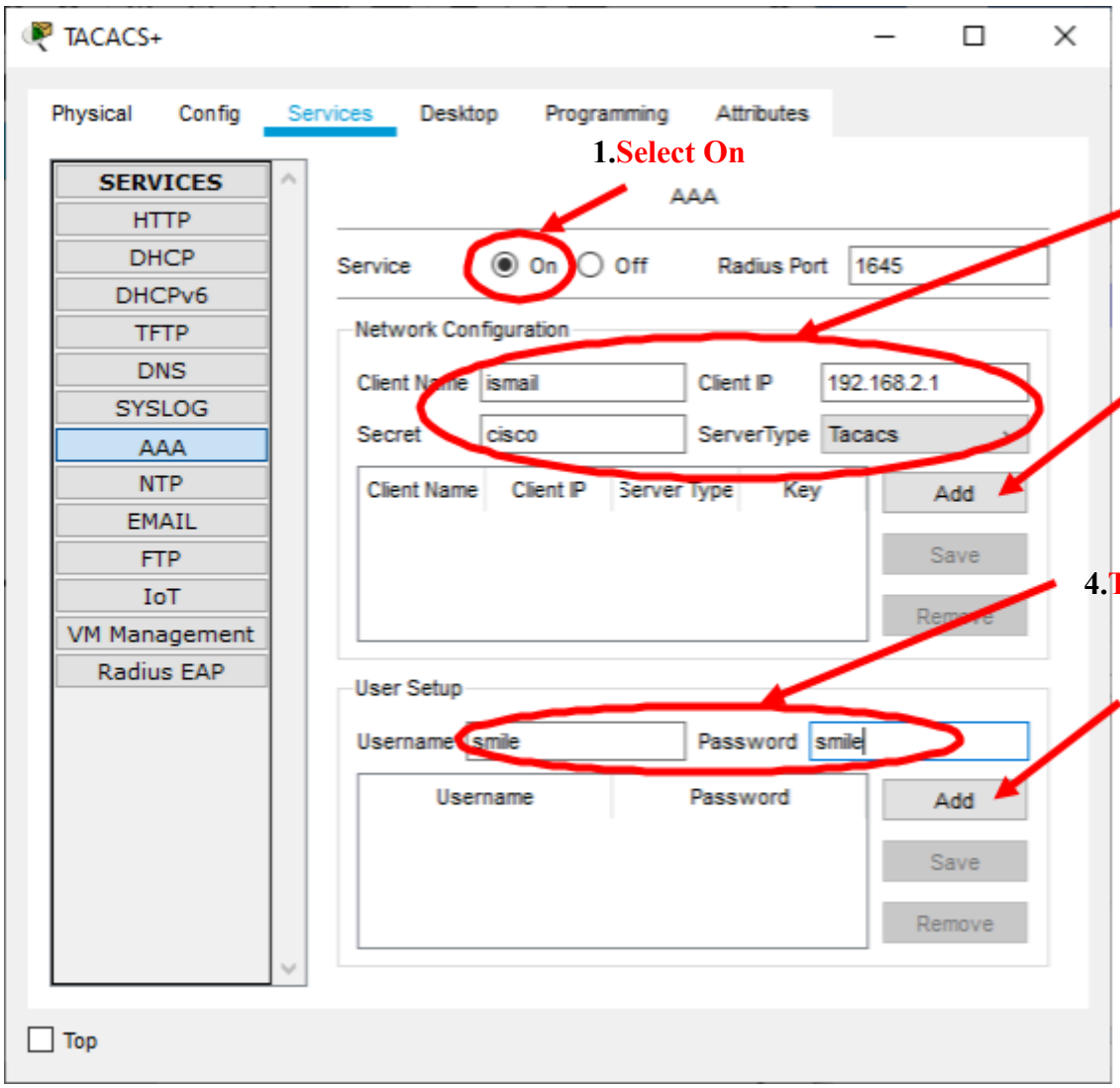
Configuring Router R0



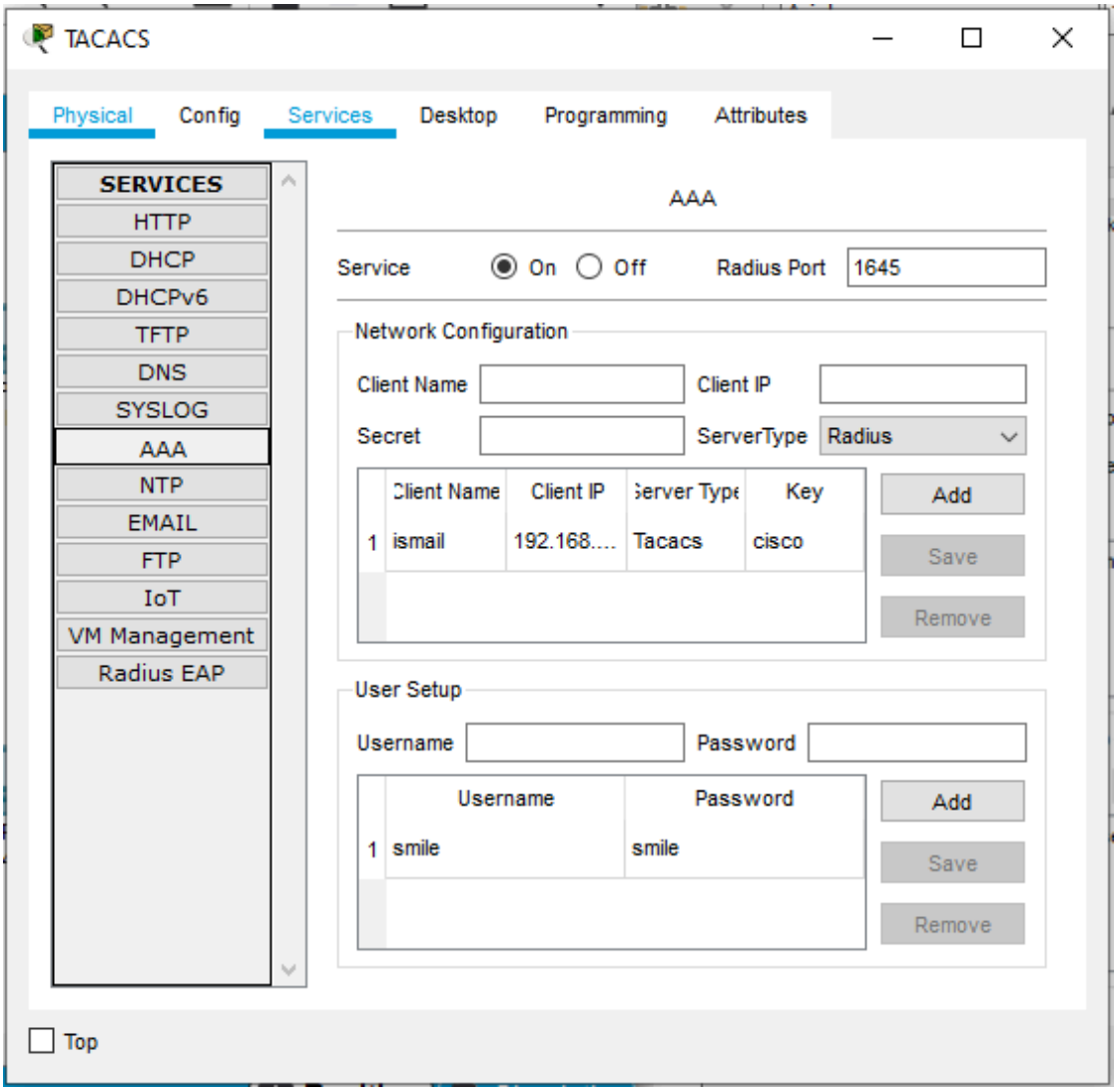


Configuring TACACS

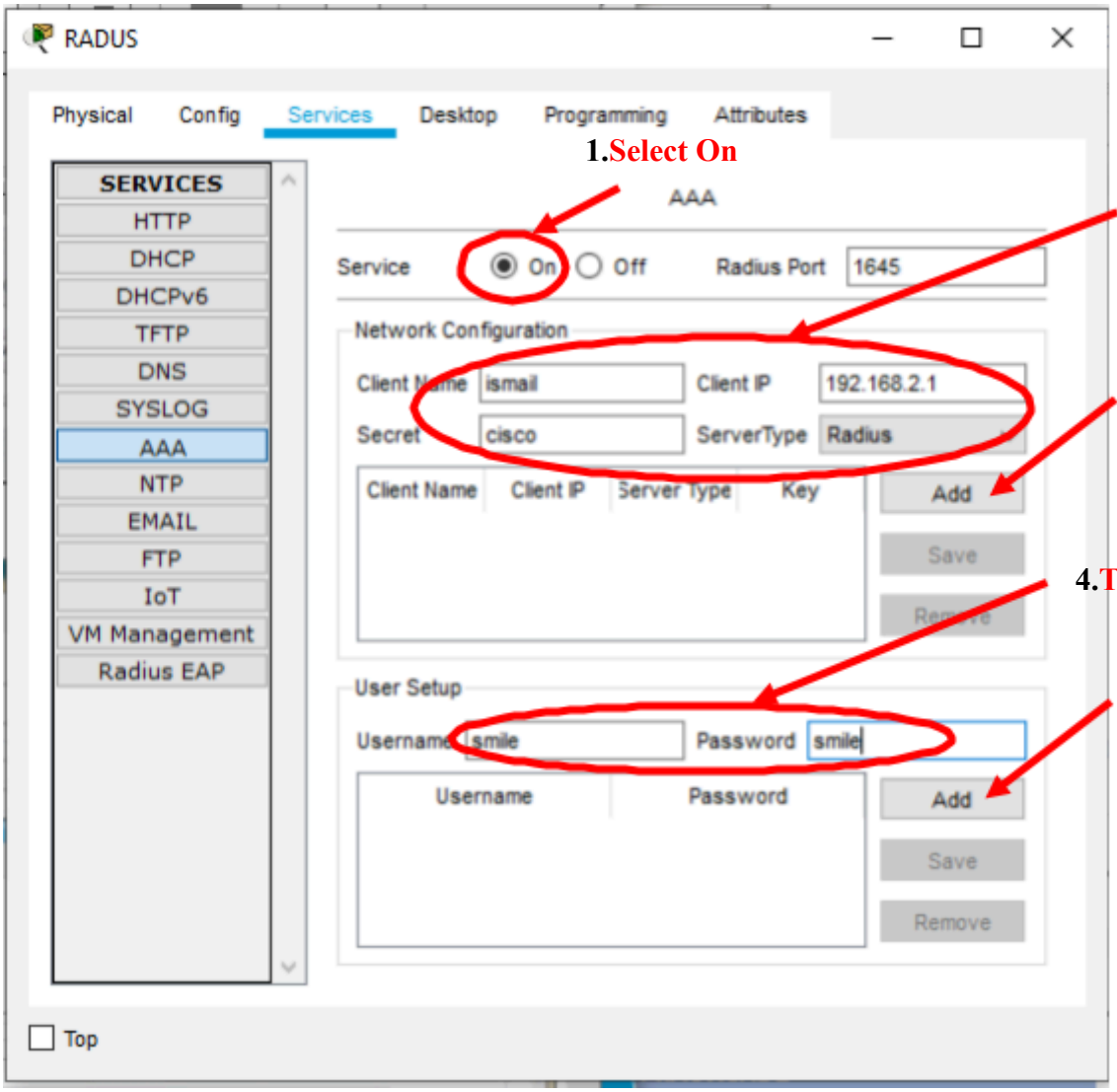



TACACS+
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
1.Select On
AAA
Service
On
Off
Radius Port
1645
Network Configuration
Client Name
ismail
Client IP
192.168.2.1
Secret
cisco
ServerType
Tacacs
Client Name
Client IP
Server Type
Key
Add
Save
Remove
2.Type this
3.Click Add
4.Type this
User Setup
Username
smile
Password
smile
Username
Password
Add
Save
Remove
5.Click Add
Top

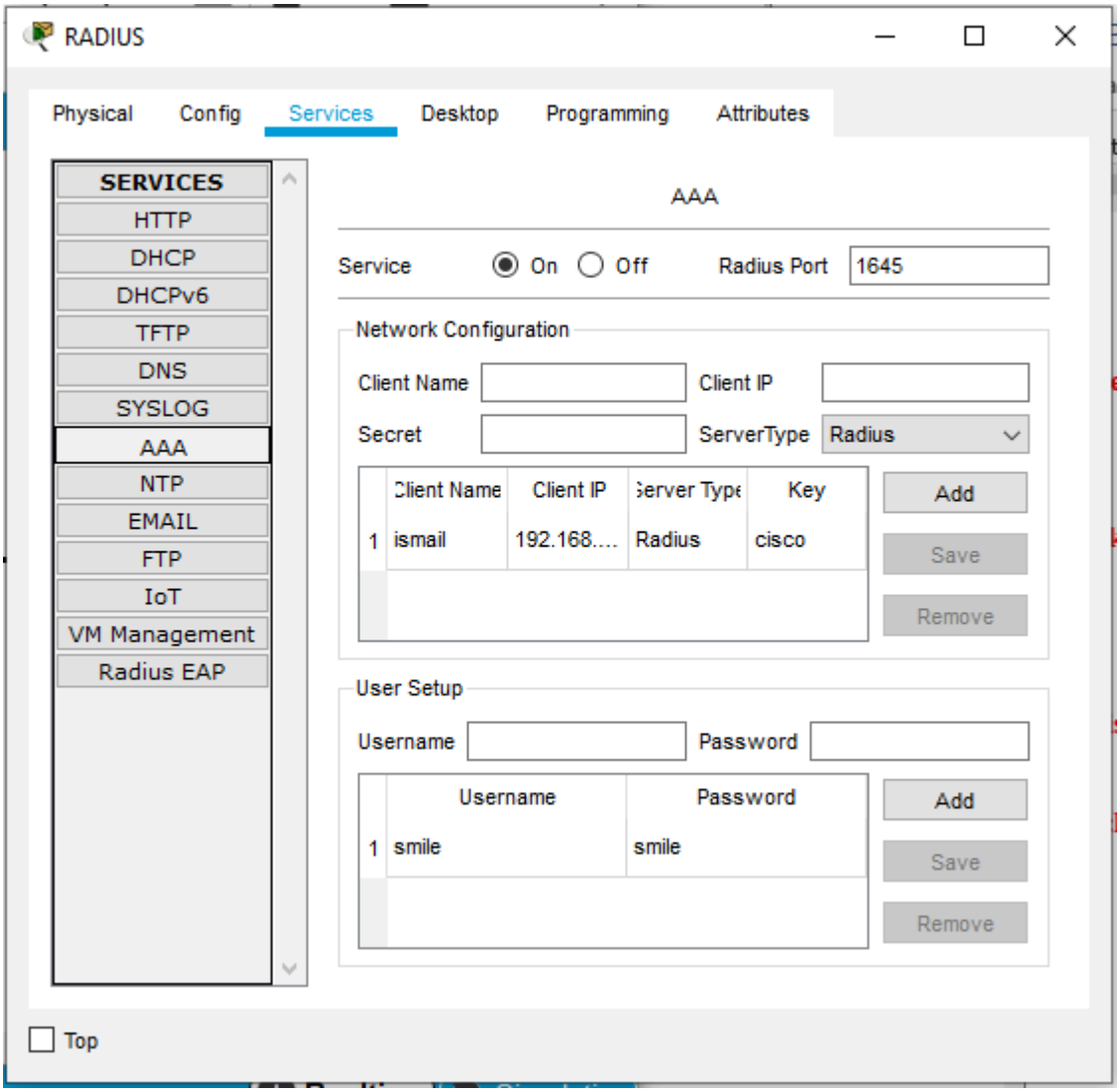
Your window should look like below image after you click Add button



Configuring RADIUS



Your window should look like below image after you click Add button

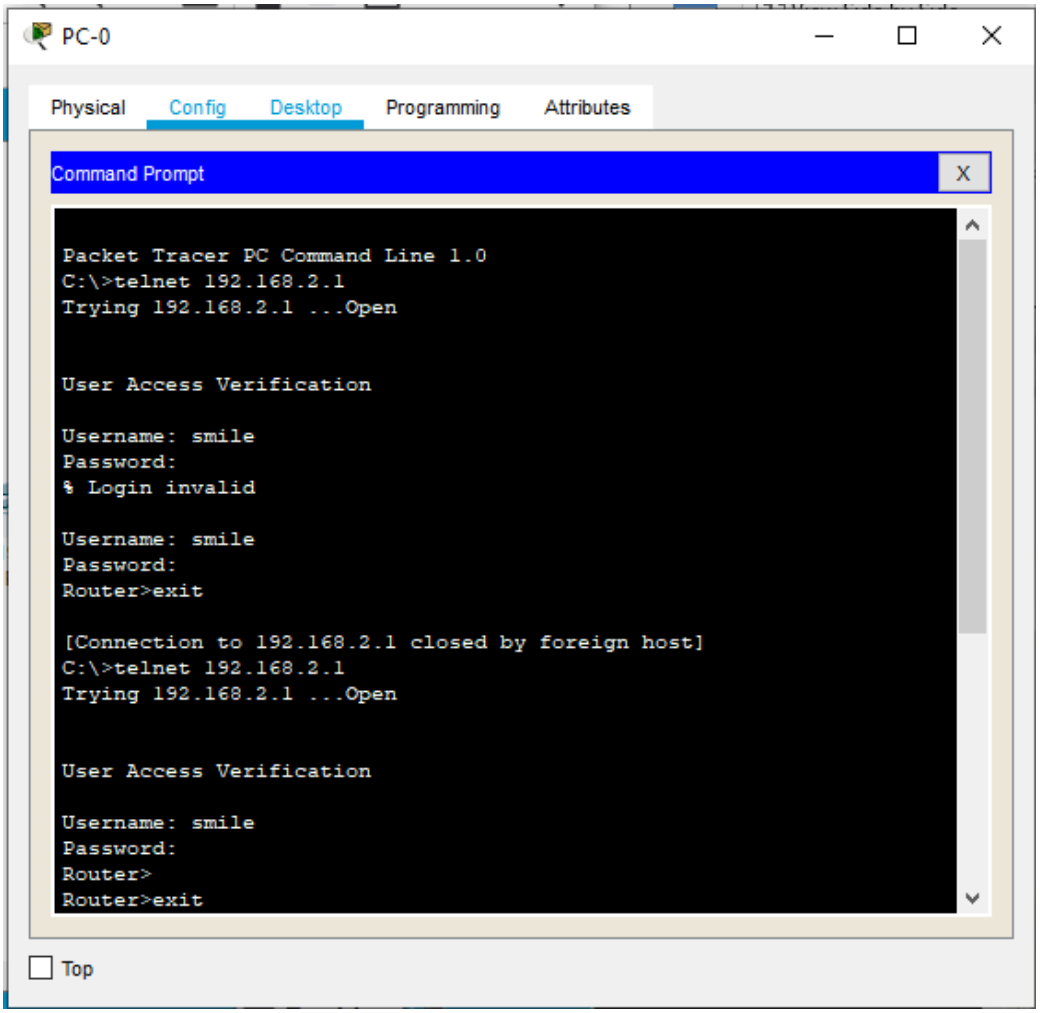


Type the following commands in the CLI mode of the Router0

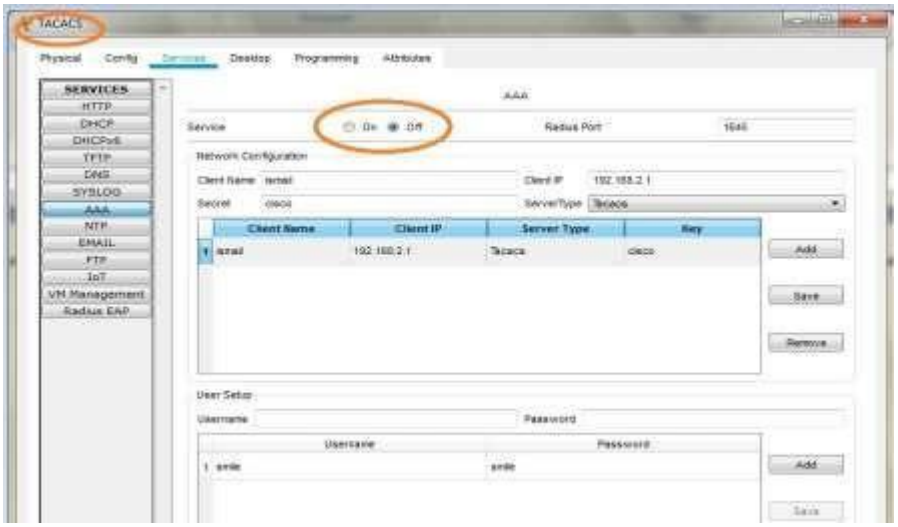
Router>enable
Router#configure terminal
Router(config)#aaa new-model
Router(config)#tacacs-server host 192.168.2.3 key cisco
Router(config)#radius-server host 192.168.2.2 key cisco
Router(config)#aaa authentication login ismail group tacacs+ group radius local
Router(config)#line vty 0 4
Router(config-line)#login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

To get check the output:

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



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



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: smile) We get the following