

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.

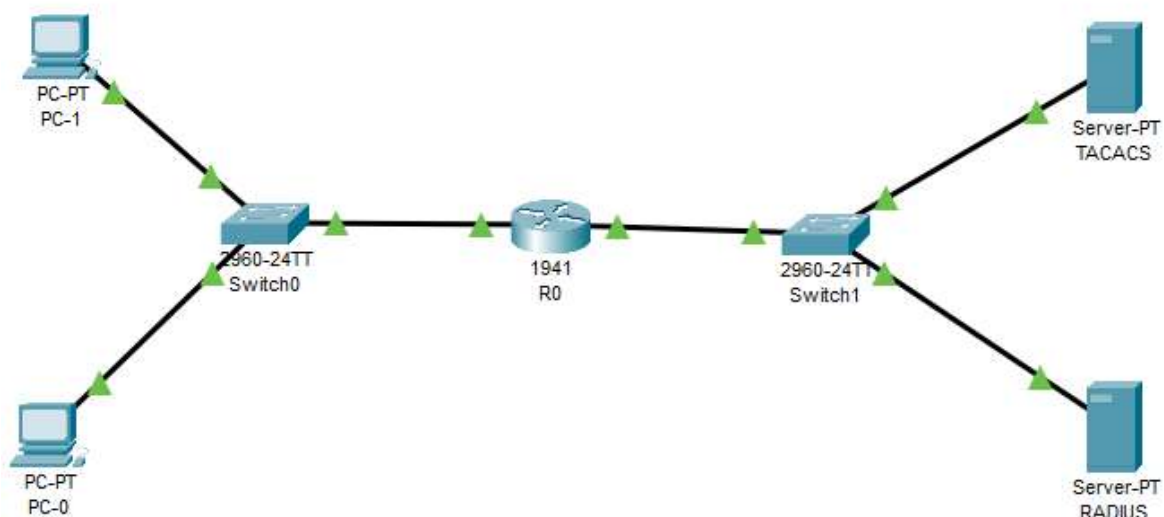
Advantages (TACACS+ over RADIUS) –

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+.

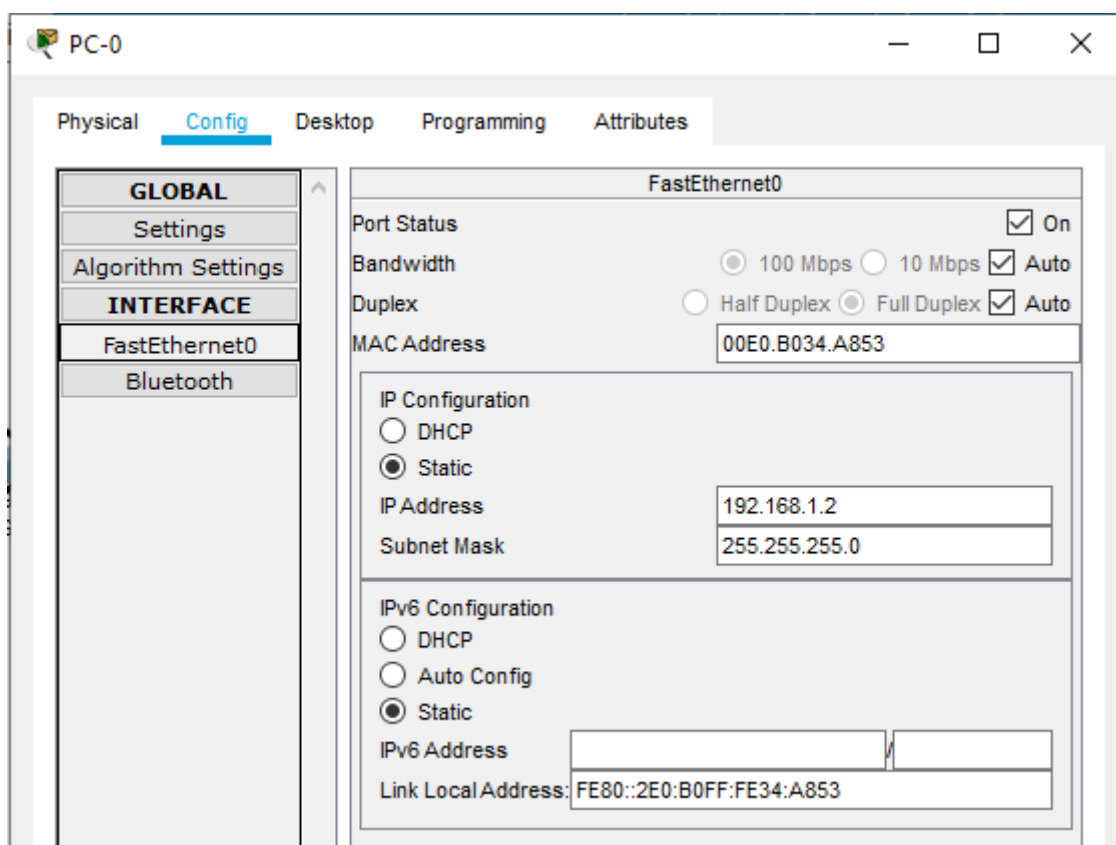
Let us consider the following Topology to understand the above AAA authentication.



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

Device	Interface	IP Address	Subnet Mask	Default gateway	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

PC-1

Physical Config **Desktop** Programming Attributes

IP Configuration X

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::290:CFF:FE5A:4D7A

IPv6 Gateway:

IPv6 DNS Server:

Configuring Router R0

R0

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

GigabitEthernet0/0

Port Status: ☒ On

Bandwidth: ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex: ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address: 00E0.B08A.1201

IP Configuration

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Tx Ring Limit: 10

The screenshot shows the configuration window for interface GigabitEthernet0/1 on router R0. The 'Config' tab is selected. The left sidebar shows a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under INTERFACE, GigabitEthernet0/1 is selected. The main area displays the following settings:

GigabitEthernet0/1	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input type="radio"/> 1000 Mbps <input checked="" type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input type="radio"/> Half Duplex <input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
MAC Address	00E0.B08A.1202
IP Configuration	
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Tx Ring Limit	10

Configuring TACACS

The screenshot shows the configuration window for TACACS. The 'Desktop' tab is selected. The left sidebar shows a tree view with categories: Physical, Config, Services, Desktop, Programming, and Attributes. Under Desktop, IP Configuration is selected. The main area displays the following settings:

IP Configuration	
<input type="radio"/> DHCP <input checked="" type="radio"/> 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	
<input type="radio"/> DHCP <input type="radio"/> Auto Config <input checked="" type="radio"/> Static	
IPv6 Address	<input type="text"/> / <input type="text"/>
Link Local Address	FE80::240:BFF:FED2:21A1
IPv6 Gateway	<input type="text"/>
IPv6 DNS Server	<input type="text"/>

The screenshot shows the TACACS+ configuration window with the 'Services' tab selected. The left sidebar lists various services, with 'AAA' highlighted. The main configuration area is divided into 'Network Configuration' and 'User Setup' sections.

1. Select On: A red circle highlights the 'On' radio button under the 'Service' section.

2. Type this: A red circle highlights the 'Client Name' field in the 'Network Configuration' section, containing the text 'ismail'.

3. Click Add: A red circle highlights the 'Add' button in the 'Network Configuration' section.

4. Type this: A red circle highlights the 'Password' field in the 'User Setup' section, containing the text 'smile'.

5. Click Add: A red circle highlights the 'Add' button in the 'User Setup' section.

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

The screenshot shows the TACACS configuration window with the 'Services' tab selected. The left sidebar lists various services, with 'AAA' highlighted. The main area displays the AAA configuration, including a 'Service' status (On/Off), 'Radius Port' (1645), and sections for 'Network Configuration' and 'User Setup'.

Services List:

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA**
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

AAA Configuration:

Service: ☒ On ☐ Off Radius Port:

Network Configuration:

Client Name: Client IP:
 Secret: ServerType:

	Client Name	Client IP	Server Type	Key
1	ismail	192.168....	Tacacs	cisco

Buttons: Add, Save, Remove

User Setup:

Username: Password:

	Username	Password
1	smile	smile

Buttons: Add, Save, Remove

☐ Top

Configuring RADIUS

The screenshot shows the RADUS configuration window with the **Services** tab selected. The **AAA** service is highlighted in the left sidebar. The main configuration area shows the **Service** set to **On** (radio button selected) and the **Radius Port** set to **1645**. The **Network Configuration** section contains fields for **Client Name** (ismail), **Client IP** (192.168.2.1), **Secret** (cisco), and **ServerType** (Radius). Below these fields is a table with columns **Client Name**, **Client IP**, **Server Type**, and **Key**, and an **Add** button. The **User Setup** section contains fields for **Username** (smile) and **Password** (smile), and an **Add** button. Red arrows and text annotations provide step-by-step instructions: 1. Select On, 2. Type this (pointing to the Network Configuration fields), 3. Click Add (pointing to the Add button in the Network Configuration section), 4. Type this (pointing to the User Setup fields), and 5. Click Add (pointing to the Add button in the User Setup section).

1. Select On

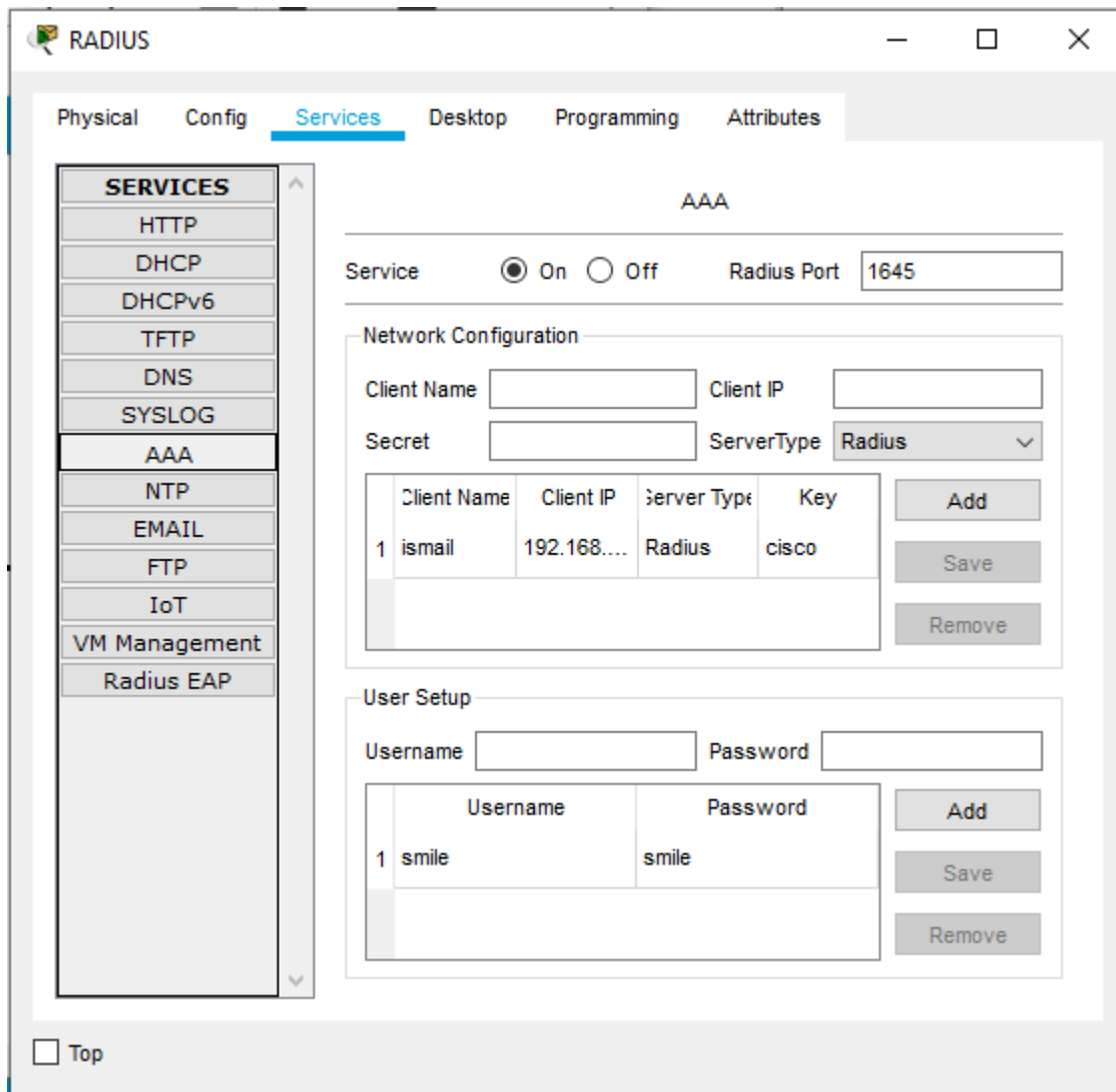
2. Type this

3. Click Add

4. Type this

5. Click Add

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:

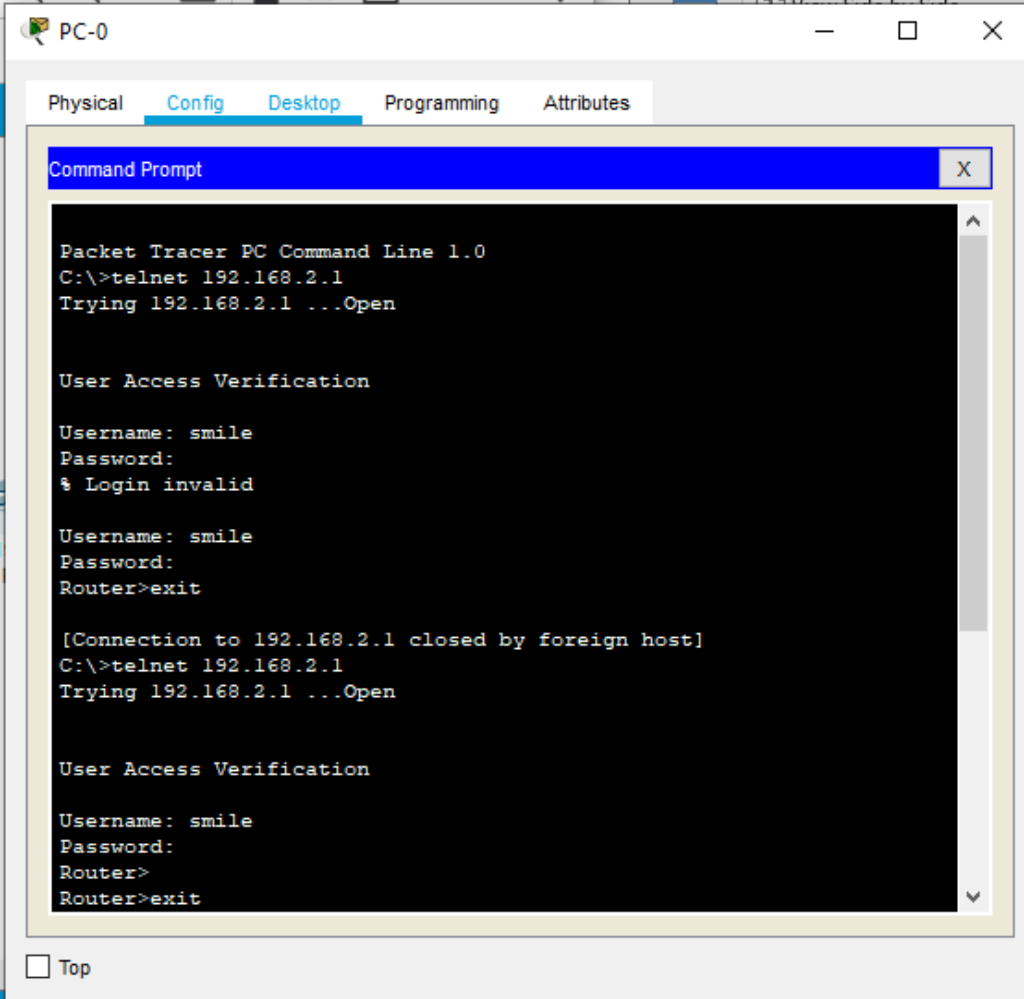
The Authentication can be done by typing the command **telnet 192.168.2.1** (the Router IP) in any of the PCs

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



The screenshot shows a Packet Tracer PC Command Line window for PC-0. The window has tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, showing a Command Prompt window. The Command Prompt displays the following text:

```
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.2.1
Trying 192.168.2.1 ...Open

User Access Verification

Username: smile
Password:
% Login invalid

Username: smile
Password:
Router>exit

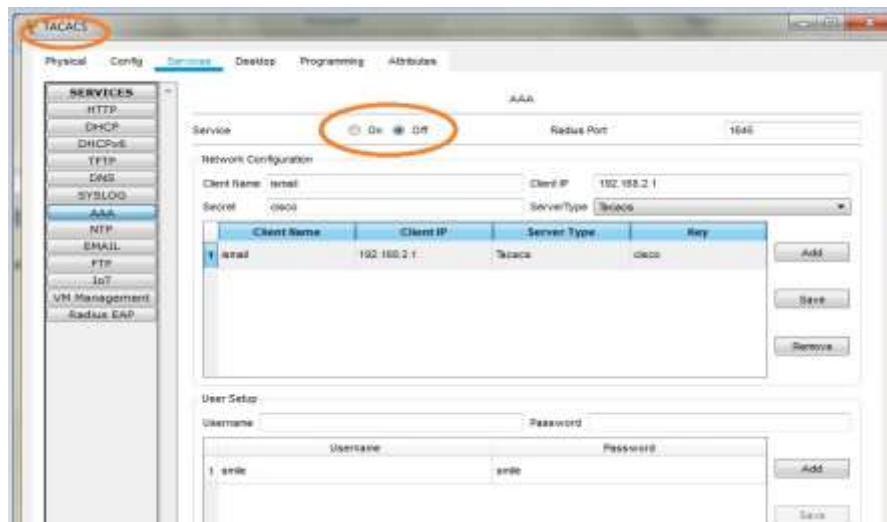
[Connection to 192.168.2.1 closed by foreign host]
C:\>telnet 192.168.2.1
Trying 192.168.2.1 ...Open

User Access Verification

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

At the bottom of the Command Prompt window, there is a checkbox labeled "Top" which is currently unchecked.

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

