

**Practical 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 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**

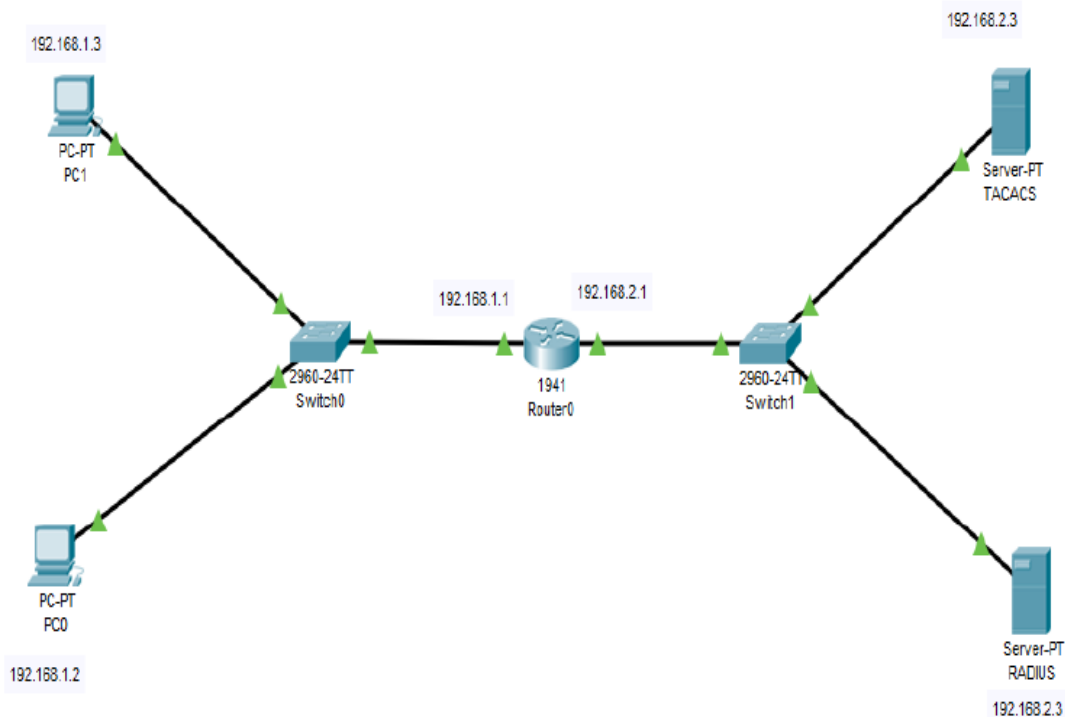
The process is start by Network Access Device (NAD – client of TACACS+ or RADIUS). NAD contact the TACACS+ or RADIUS server and transmit the request for authentication (username and password) to the server. First, NAD obtain username prompt and transmit the username to the server and then again, the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

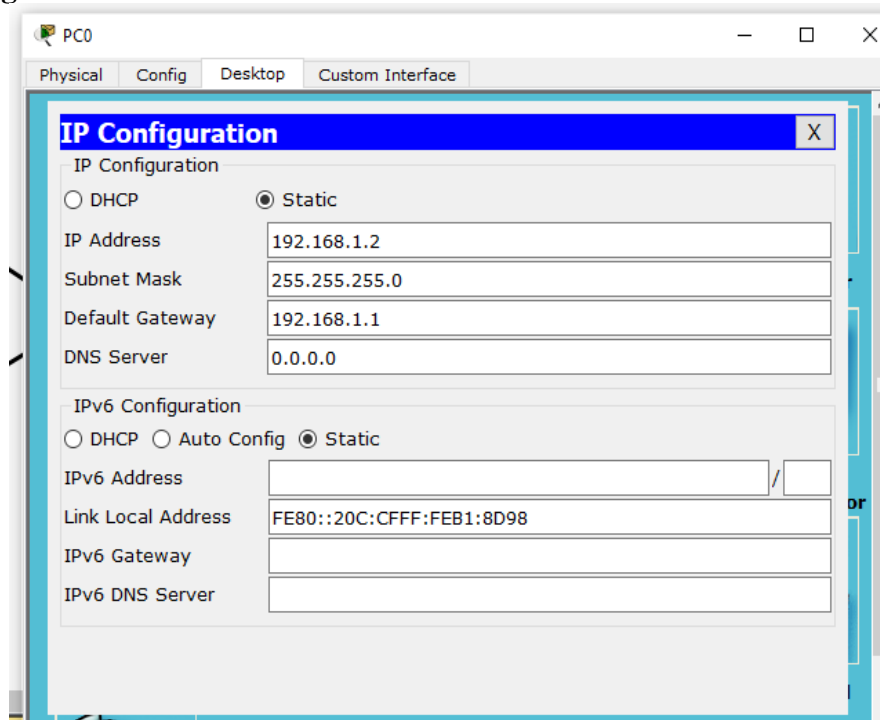
**Advantages (TACACS+ over RADIUS)**

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.

**Advantages (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+.



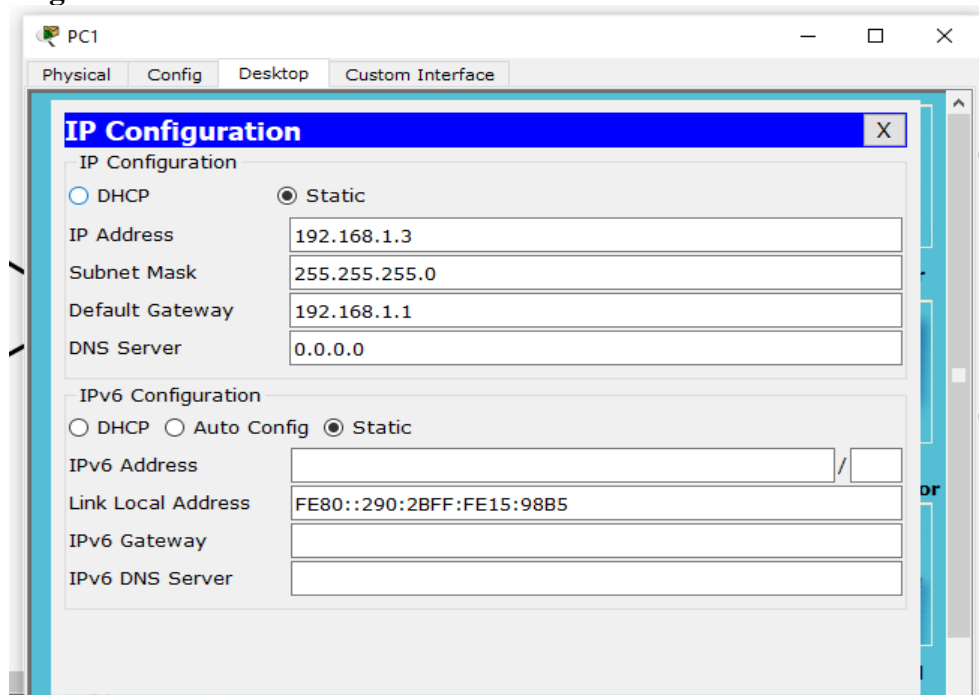
**Configuring PC0**

The screenshot shows the 'PC0' configuration window with the 'Config' tab selected. The 'IP Configuration' dialog is open, showing the following settings:

IP Configuration	
<input type="radio"/> DHCP <input checked="" type="radio"/> 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	
<input type="radio"/> DHCP <input type="radio"/> Auto Config <input checked="" type="radio"/> Static	
IPv6 Address	
Link Local Address	FE80::20C:CFFF:FEB1:8D98
IPv6 Gateway	
IPv6 DNS Server	

**Configuring PC1**

The screenshot shows the 'PC1' configuration window with the 'Config' tab selected. The 'IP Configuration' dialog is open, showing the following settings:

IP Configuration	
<input type="radio"/> DHCP <input checked="" type="radio"/> 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	
<input type="radio"/> DHCP <input type="radio"/> Auto Config <input checked="" type="radio"/> Static	
IPv6 Address	
Link Local Address	FE80::290:2BFF:FE15:98B5
IPv6 Gateway	
IPv6 DNS Server	

## Configuring Router0

The screenshot shows the 'Router0' configuration window with the 'Config' tab selected. The left sidebar contains a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under the INTERFACE category, 'GigabitEthernet0/0' is selected. The main panel displays the configuration for 'GigabitEthernet0/0'. The 'Port Status' is set to 'On'. The 'Bandwidth' is set to '100 Mbps' (selected with a radio button). The 'Duplex' is set to 'Full Duplex' (selected with a radio button). The 'MAC Address' is '0090.0CB6.4801'. The 'IP Configuration' section shows 'IP Address' as '192.168.1.1' and 'Subnet Mask' as '255.255.255.0'. The 'Tx Ring Limit' is set to '10'.

Category	Sub-category	Value
GLOBAL	Settings	
ROUTING	Static	
ROUTING	RIP	
SWITCHING	VLAN Database	
INTERFACE	GigabitEthernet0/0	
INTERFACE	GigabitEthernet0/1	

GigabitEthernet0/0	
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	0090.0CB6.4801
IP Configuration	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Tx Ring Limit	10

The screenshot shows the 'Router0' configuration window with the 'Config' tab selected. The left sidebar contains a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under the INTERFACE category, 'GigabitEthernet0/1' is selected. The main panel displays the configuration for 'GigabitEthernet0/1'. The 'Port Status' is set to 'On'. The 'Bandwidth' is set to '100 Mbps' (selected with a radio button). The 'Duplex' is set to 'Full Duplex' (selected with a radio button). The 'MAC Address' is '0090.0CB6.4802'. The 'IP Configuration' section shows 'IP Address' as '192.168.2.1' and 'Subnet Mask' as '255.255.255.0'. The 'Tx Ring Limit' is set to '10'.

Category	Sub-category	Value
GLOBAL	Settings	
ROUTING	Static	
ROUTING	RIP	
SWITCHING	VLAN Database	
INTERFACE	GigabitEthernet0/0	
INTERFACE	GigabitEthernet0/1	

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	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.

The screenshot shows the 'IP Configuration' window in the TACACS+ application. The 'Interface' is set to 'FastEthernet0'. Under 'IP Configuration', 'Static' is selected. The fields are filled with: IP Address: 192.168.2.3, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.2.1, and DNS Server: 0.0.0.0. Under 'IPv6 Configuration', 'Static' is also selected, with fields for IPv6 Address, Link Local Address (FE80::290:CFF:FE89:3846), IPv6 Gateway, and IPv6 DNS Server.

The screenshot shows the 'Services' window in the TACACS+ application. The 'AAA' service is selected in the left sidebar. The 'Service' is set to 'On' and the 'Radius Port' is 1645. Under 'Network Configuration', the 'Client Name' is 'dalmia', 'Client IP' is '192.168.2.1', 'Secret' is 'cisco', and 'ServerType' is 'Tacacs'. A table lists the configuration:

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

Buttons for 'Add', 'Save', and 'Remove' are present. Under 'User Setup', the 'Username' is 'dalmia' and 'Password' is 'dalmia'. A table lists the user:

	Username	Password
1	dalmia	dalmia

Buttons for 'Add', 'Save', and 'Remove' are present.

## Configuring Server1(As RADIUS)

RADIUS

Physical Config Services Desktop Custom Interface

### IP Configuration

Interface: FastEthernet0

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::210:11FF:FE25:CBBA

IPv6 Gateway:

IPv6 DNS Server:

RADIUS

Physical Config Services Desktop Custom Interface

### AAA

Service: ☐ On ☒ Off Radius Port: 1645

Network Configuration

Client Name: dalmia Client IP: 192.168.2.1

Secret: cisco ServerType: Radius

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

Add Save Remove

User Setup

Username: dalmia Password: dalmia

	Username	Password
1	dalmia	dalmia

Add Save Remove

Click on Router 0 go to CLI tab and press enter and enter the following commands: -

```
Router>en
Router#conf t
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 dalmia group tacacs+ group radius local
Router(config)#line vty 0 4
Router(config-line)#login authentication dalmia
Router(config-line)#exit
Router(config)#
```

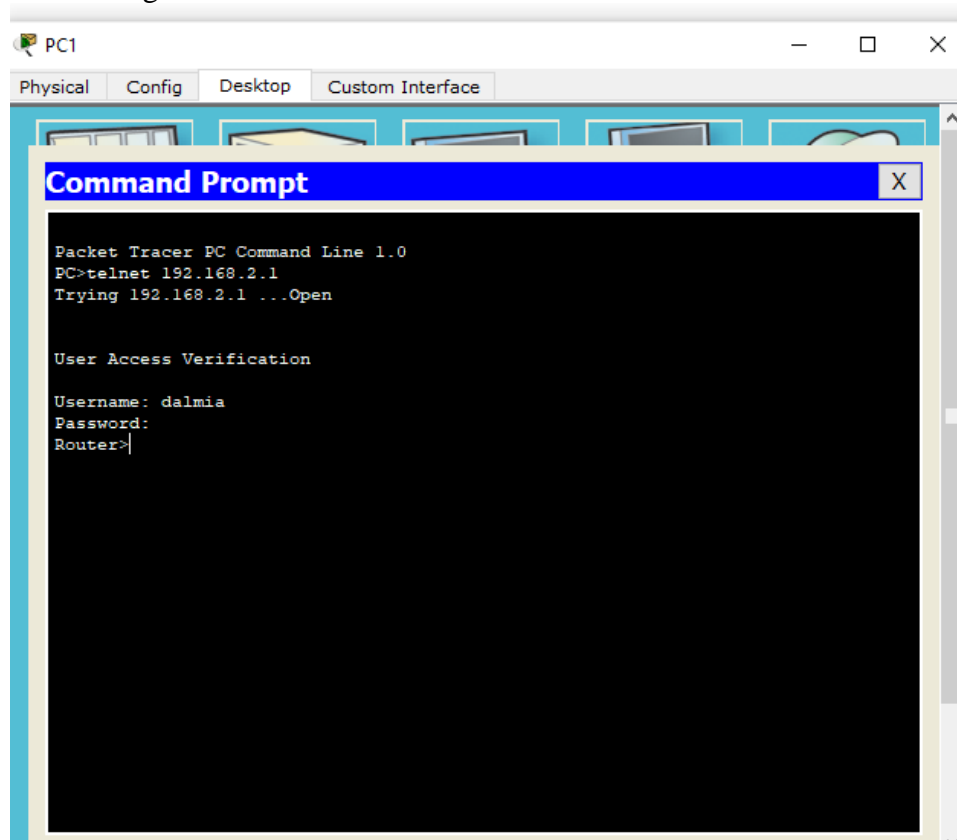
The Authentication can be done by typing the command **telnet 192.168.2.1** (the Router IP) in any of the PCs

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

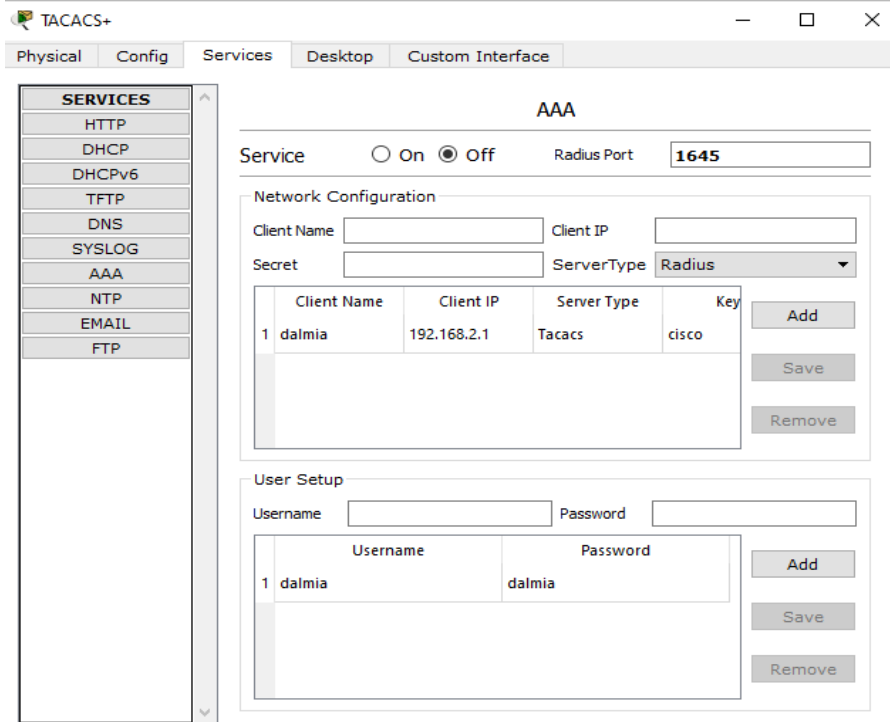
Username: dalmia

Password: dalmia

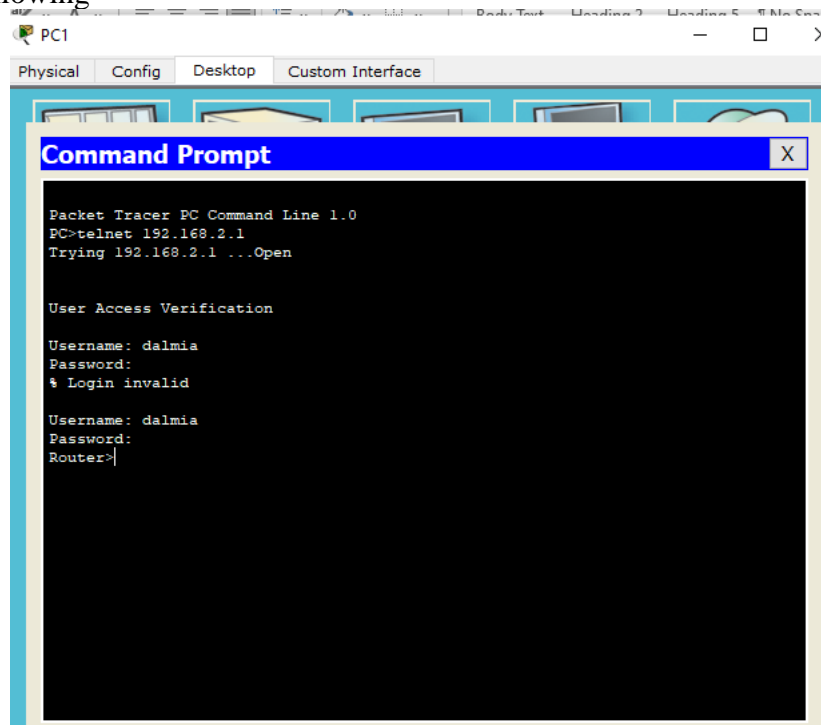
We get the following



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: dalmia , Password: dalmia)  
We get the following



The local login can also be verified by turning OFF both TACACS and RADIUS service.  
Hence the authentication through both TACACS and RADIUS.

\*\*\*\*\*