

**GURU NANAK COLLEGE OF ARTS, SCIENCE & COMMERCE**  
**GTB NAGAR, MUMBAI-37**

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**TYBSc(IT), SEMESTER VI**

Practical Journal

for

the subject

**SECURITY IN COMPUTING**

Submitted by

NAME- Mohit Sulendra Rajbhar

ROLL NO-22

for the academic year

2021-2022



Guru Nanak College of Arts, Science & Commerce

G.T.B.Nagar, Mumbai – 400 037.

Department of Information Technology

**CERTIFICATE**

This is to certify that Mr. Mohit Sulendra Rajbhar of TYBSc [Information Technology] Semester VI, Roll No. 22 has successfully completed the practicals for the subject of SECURITY IN COMPUTING as a partial fulfillment of the degree B.Sc(IT) during the academic year 2021-22.

Mr. Shahid Ansari  
Mrs. Harpreet Kaur  
Faculty-in-charge

BScIT-in-charge

Internal Examiner

External Examiner

Date : / /2022      College Seal

<b>Practical no</b>	<b>Title</b>	<b>Date</b>	<b>Sign</b>
<b>1</b>	<b>Configure Cisco Routers for Syslog, NTP, and SSH Operations</b>		
<b>2</b>	<b>Configure AAA Authentication</b>		
<b>3</b>	<b>Configuring Extended ACLs</b>		
<b>4</b>	<b>Configure IP ACLs to Mitigate Attacks</b>		
<b>5</b>	<b>Configuring IPv6 ACLs</b>		
<b>6</b>	<b>Configuring a Zone-Based Policy Firewall (ZPF)</b>		
<b>7</b>	<b>Configure IOS Intrusion Prevention System (IPS) Using the CLI</b>		
<b>8</b>	<b>Packet Tracer - Layer 2 Security</b>		
<b>9</b>	<b>Layer 2 VLAN Security</b>		

## PRACTICAL NO 1:

### Configure Cisco Routers for Syslog, NTP, and SSH Operations

#### OSPF, MD5 Authentication

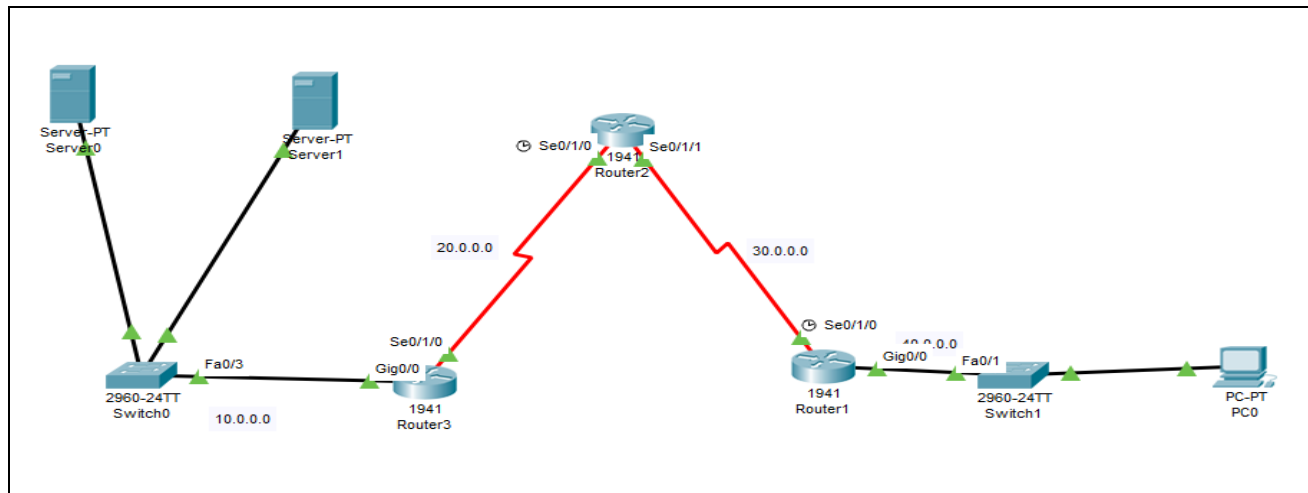
- OSPF is a routing protocol. Two routers speaking OSPF to each other exchange information about the routes they know about and the cost for them to get there.
- When many OSPF routers are part of the same network, information about all of the routes in a network are learned by all of the OSPF routers within that network—technically called an **area**. (We'll talk more about area as we go on).
- Each OSPF router passes along information about the routes and costs they've heard about to all of their adjacent OSPF routers, called **neighbors**.
- OSPF routers rely on **cost** to compute the shortest path through the network between themselves and a remote router or network destination.
- The shortest path computation is done using Dijkstra's algorithm. This algorithm isn't unique to OSPF. Rather, it's a mathematical algorithm that happens to have an obvious application to networking.

#### MD5 Authentication

- MD5 authentication provides higher security than plain text authentication.
- This method uses the MD5 algorithm to compute a hash value from the contents of the OSPF packet and a password (or key).
- This hash value is transmitted in the packet, along with a key ID and a non-decreasing sequence number.
- The receiver, which knows the same password, calculates its own hash value.
- If nothing in the message changes, the hash value of the receiver should match the hash value of the sender which is transmitted with the message.
- The key ID allows the routers to reference multiple passwords.
- This makes password migration easier and more secure.
- For example, to migrate from one password to another, configure a password under a different key ID and remove the first key.
- The sequence number prevents replay attacks, in which OSPF packets are captured, modified, and retransmitted to a router.
- As with plain text authentication, MD5 authentication passwords do not have to be the same throughout an area. However, they do need to be the same between neighbors.

## Example

### Consider the following topology



### Configuring PC0

PC0

Physical Config **Desktop** Programming Attributes

☐ DHCP ☒ Static

IP Address: 40.0.0.2

Subnet Mask: 255.0.0.0

Default Gateway: 40.0.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

### Configuring NTP Server

NTP Server

Physical Config **Services** **Desktop** Programming Attributes

☐ DHCP ☒ Static

IP Address: 10.0.0.2

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

### Configuring SYSLOG Server

SYSLOG Server

Physical Config **Services** **Desktop** Programming Attributes

☐ DHCP ☒ Static

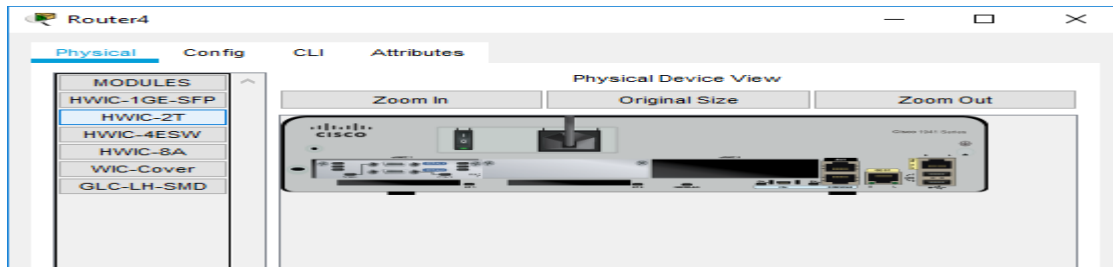
IP Address: 10.0.0.3

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

**Note : Adding Serial interface to all Routers****Part 1: Configure OSPF MD5 Authentication**

**ROUTER 3: Type the following command in the CLI mode**

```
Router>enable
Router#
Router#configure terminal
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#ip address 20.0.0.1 255.0.0.0
Router(config-if)# no shutdown
Router(config-if)#exit
```

**The following Command is for setting the OSPF configuration**

```
Router(config)#router ospf 1
Router(config-router)#network 10.0.0.0 0.255.255.255 area 1
Router(config-router)#network 20.0.0.0 0.255.255.255 area 1
Router(config-router)#exit
Router(config)#exit
Router#
```

**ROUTER 2: Type the following command in the CLI mode**

```
Router>enable
Router#
Router#configure terminal
Router(config)#interface GigabitEthernet0/0
```

```
Router(config-if)#ip address 20.0.0.2 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#ip address 30.0.0.1 255.0.0.0
Router(config-if)# no shutdown
Router(config-if)#exit
```

The following Command is for setting the OSPF configuration

```
Router(config)#router ospf 1
Router(config-router)#network 30.0.0.0 0.255.255.255 area 1
Router(config-router)#network 20.0.0.0 0.255.255.255 area 1
Router(config-router)#exit
Router(config)#exit
Router#
```

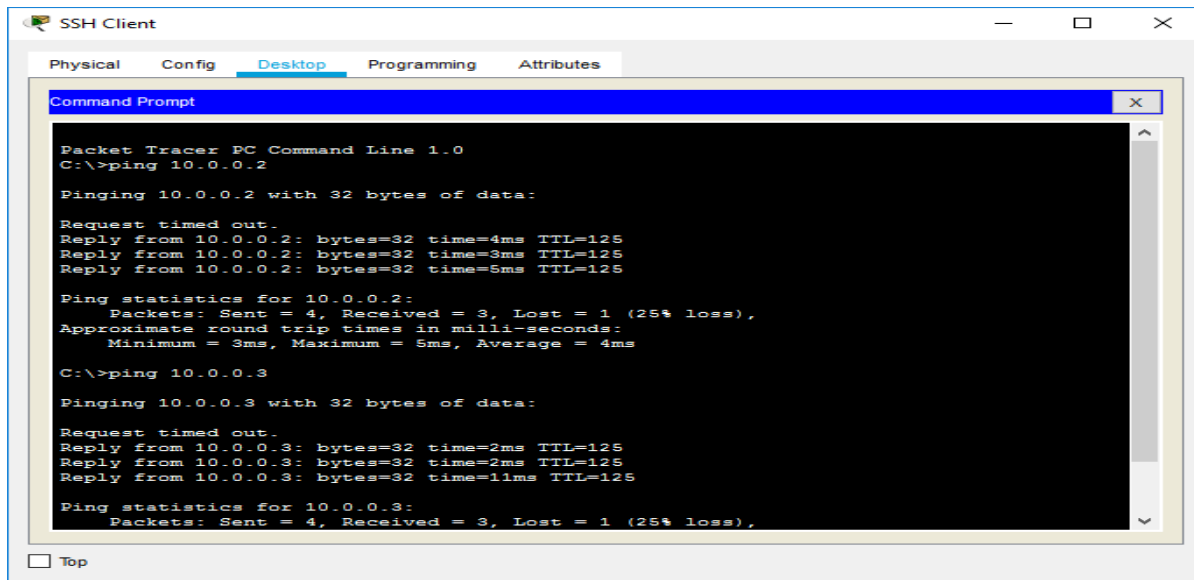
**ROUTER 1 : Type the following command in the CLI mode**

```
Router>enable
Router#
Router#configure terminal
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 40.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#ip address 30.0.0.2 255.0.0.0
Router(config-if)# no shutdown
Router(config-if)#exit
```

The following Command is for setting the OSPF configuration

```
Router(config)#router ospf 1
Router(config-router)#network 30.0.0.0 0.255.255.255 area 1
Router(config-router)#network 40.0.0.0 0.255.255.255 area 1
Router(config-router)#exit
Router(config)#exit
Router#
```

Now we verify the connectivity by using the following



## MD5 Authentication

### For Router 3

```
Router(config)#router ospf 1
Router(config-router)#area 1 authentication message-digest
Router(config-router)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#ip ospf message-digest-key 1 md5 admin
Router(config-if)#exit
```

### For Router 2

```
Router(config)#router ospf 1
Router(config-router)#area 1 authentication message-digest
Router(config-router)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#ip ospf message-digest-key 1 md5 admin
Router(config-if)#exit
```

```
Router(config)#router ospf 1
Router(config-router)#area 1 authentication message-digest
Router(config-router)#exit
Router(config)#interface Serial0/1/1
Router(config-if)#ip ospf message-digest-key 1 md5 admin
Router(config-if)#exit
```

### For Router 1

```
Router(config)#router ospf 1
Router(config-router)#area 0 authentication message-digest
```



```
Router(config-router)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#ip ospf message-digest-key 1 md5 admin
Router(config-if)#exit
```

Verify the authentication using the following command on any Router

**Router#show ip ospf interface**

**The following output is obtained**

```
Router1SSH
Physical Config CLI Attributes
IOS Command Line Interface
Router#
Router#sho
Router#show ip os
Router#show ip ospf in
Router#show ip ospf interface

Serial0/1/0 is up, line protocol is up
Internet address is 30.0.0.2/8, Area 1
Process ID 1, Router ID 40.0.0.1, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:03
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
Youngest key id is 1
GigabitEthernet0/0 is up, line protocol is up
Internet address is 40.0.0.1/8, Area 1
Process ID 1, Router ID 40.0.0.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 40.0.0.1, Interface address 40.0.0.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:08
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
No key configured, using default key id 0
Router#
Router#
```

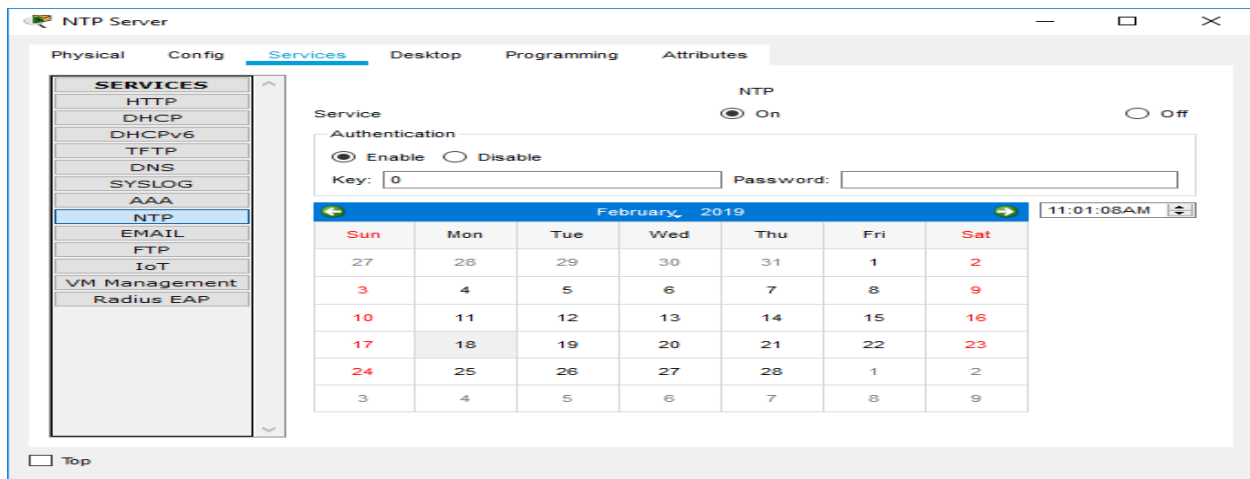
## b) NTP

- Network Time Protocol (NTP) is a TCP/IP protocol used to synchronize computer clocks across data networks.

- NTP was developed in the 1980s by D.L. Mills at the University of Delaware to achieve highly accurate time synchronization and to sustain the effects of variable latency over packet-switched data networks through a jitter buffer.

We use the same topology to study the given protocol

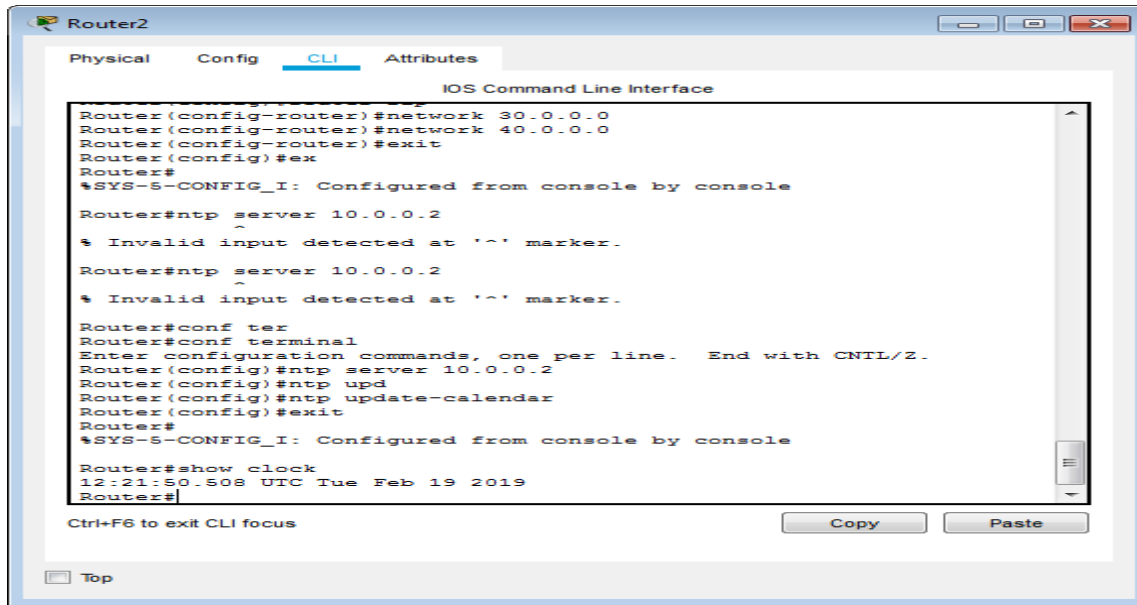
### Configure NTP Server and enable the NTP service



### Now Go to CLI Mode of Router4 and type the following commands on all Routers

```
Router>en
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ntp server 10.0.0.2
Router(config)#ntp update-calendar
Router(config)#exit
Router#show clock
16:14:55.13 UTC Fri Dec 7 2018
```

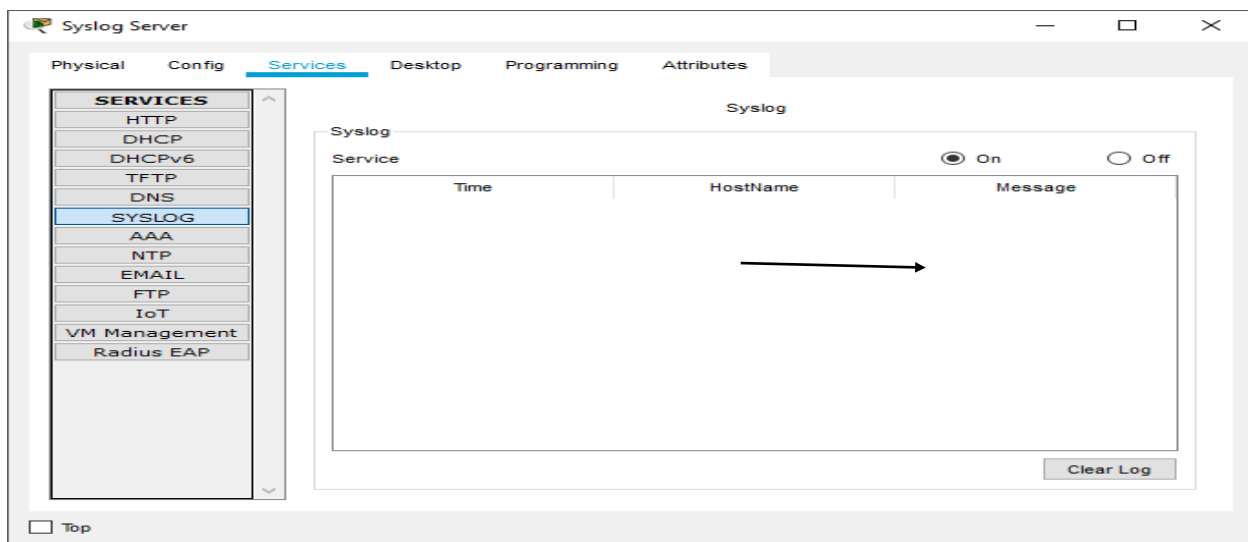
### Output



### c) To log messages to the syslog server

#### Configure SYSLOG Server and enable the service

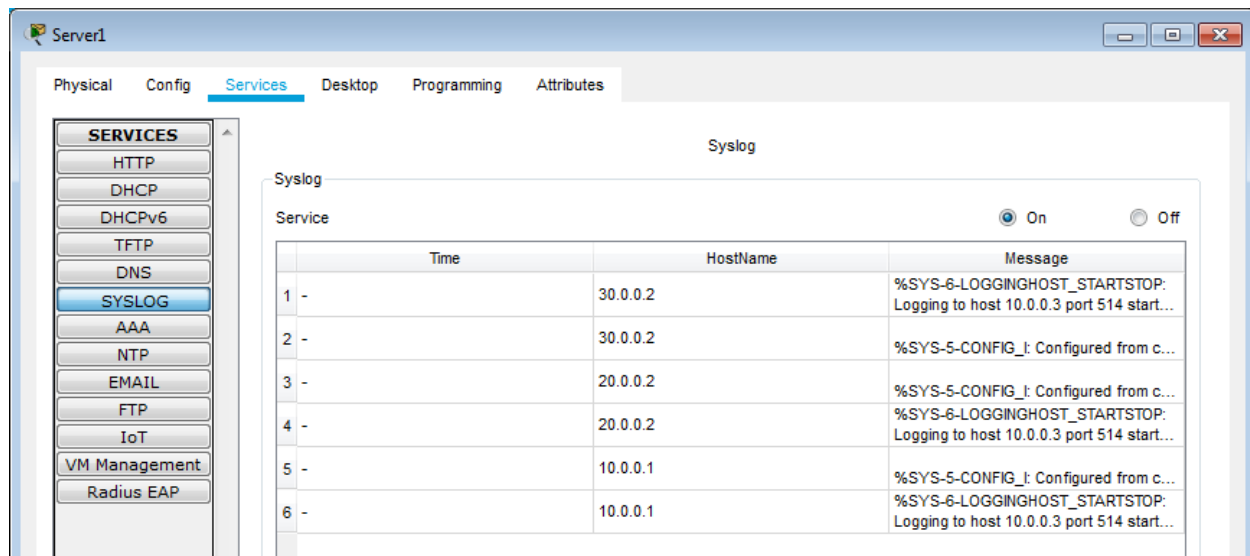
- Syslog is a way for network devices to send event messages to a logging server – usually known as a Syslog server.
- The Syslog **protocol** is supported by a wide range of devices and can be used to log different types of events.
- For example, a router might send messages about users logging on to console sessions, while a web-server might log access-denied events.
- **Start the syslog service on the server (10.0.0.3)**



**Now Go to CLI Mode of Router0 and type the following commands in all the Routers.**

```
Router>enable
Router#ping 10.0.0.3
Router#configure terminal
Router(config)#logging 10.0.0.3
```

**Output:**



**d) To support SSH connections.**

- An **SSH server** is a software program which uses the secure shell protocol to accept connections from remote computers.
- The way **SSH works** is by making use of a client-server model to allow for authentication of two remote systems and encryption of the data that passes between them.
- It organizes the secure connection by authenticating the client and opening the correct shell environment if the verification is successful.

**Now Go to CLI Mode of Router0 and type the following commands.**

```
Router#configure terminal
Router(config)#ip domain-name admin.com
```

```
Router(config)#hostname admin
```

```
admin(config)#crypto key generate rsa
```

The name for the keys will be: admin.admin.com

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

```
admin(config)#line vty 0
```

```
*Feb 19 12:58:22.61: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

```
admin(config)#line vty 0 4
```

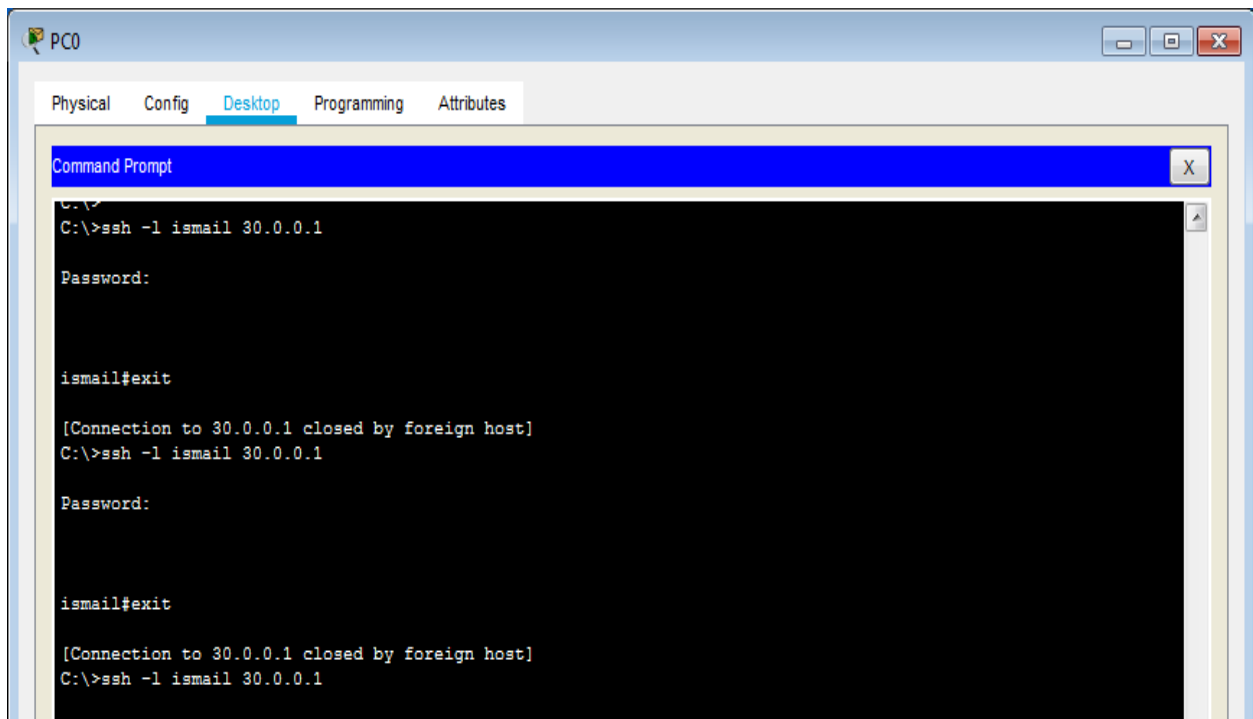
```
admin(config-line)# transport input ssh
```

```
admin(config-line)#ip ssh ver 2
```

```
admin(config-line)#login local
```

```
admin(config)#username admin privilege 15 password rollno
```

### Output: Go to cmd of PC0



The screenshot shows a window titled 'PC0' with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The Command Prompt shows the following sequence of commands and output:

```
C:\>ssh -l ismail 30.0.0.1
Password:
ismail#exit
[Connection to 30.0.0.1 closed by foreign host]
C:\>ssh -l ismail 30.0.0.1
Password:
ismail#exit
[Connection to 30.0.0.1 closed by foreign host]
C:\>ssh -l ismail 30.0.0.1
```

## Practical No. 2: Configure AAA Authentication

Access control is the way you control who is allowed access to the network server and what services the security services provide the primary framework through which you set up access control on your device or access server.

AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing the following services:

- Authentication—Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you select, encryption.

Authorization—Provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP and Telnet.

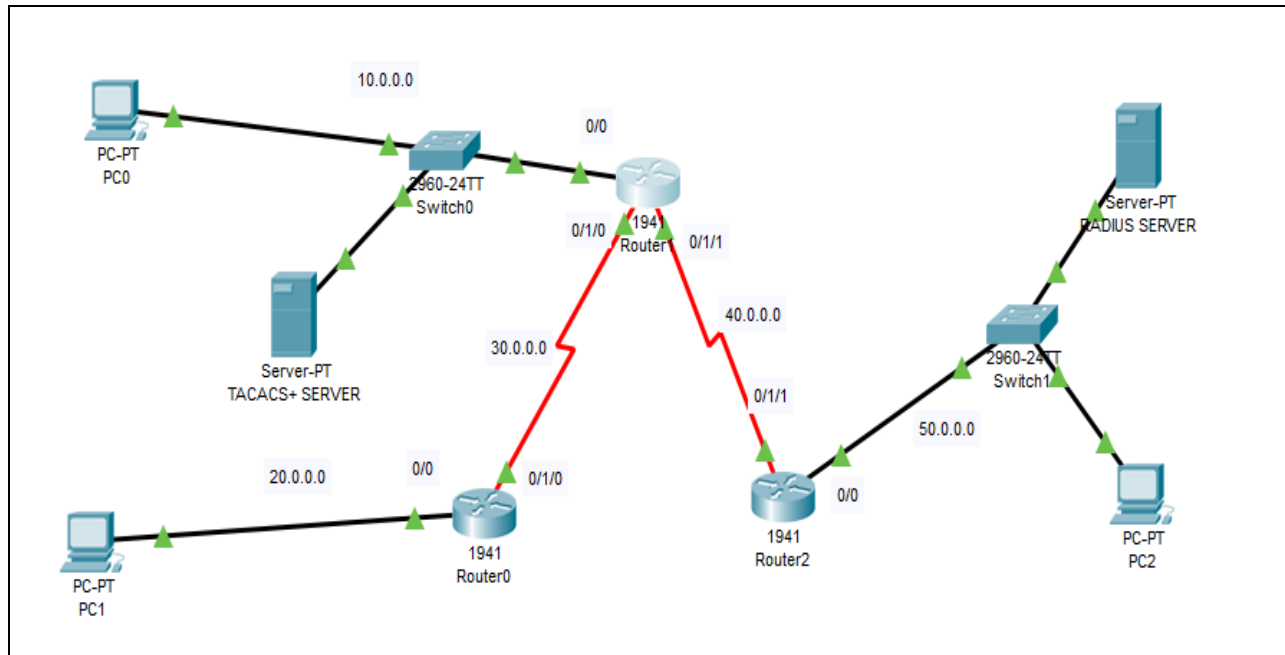
Accounting—Provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times.

AAA provides the following benefits:

- Increased flexibility and control of access configuration
- Scalability
- Standardized authentication methods, such as RADIUS and TACACS+
- Multiple backup systems

- a) Configure a local user account on Router and configure authentication on the console and vty lines using local AAA

We use the following topology for the present case.



### Configure Router0

```

Router>enable
Router#
Router#configure terminal
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 20.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#ip address 30.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit

```

```

Router(config)#router rip
Router(config-router)#network 20.0.0.0
Router(config-router)#network 30.0.0.0
Router(config-router)#

```

### Configure Router1

```

Router>enable
Router#
Router#configure terminal
Router(config)#interface GigabitEthernet0/0

```

```
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#ip address 30.0.0.2 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface Serial0/1/1
Router(config-if)#ip address 40.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

```
Router(config)#router rip
Router(config-router)#network 10.0.0.0
Router(config-router)#network 30.0.0.0
Router(config-router)#network 40.0.0.0
Router(config-router)#
```

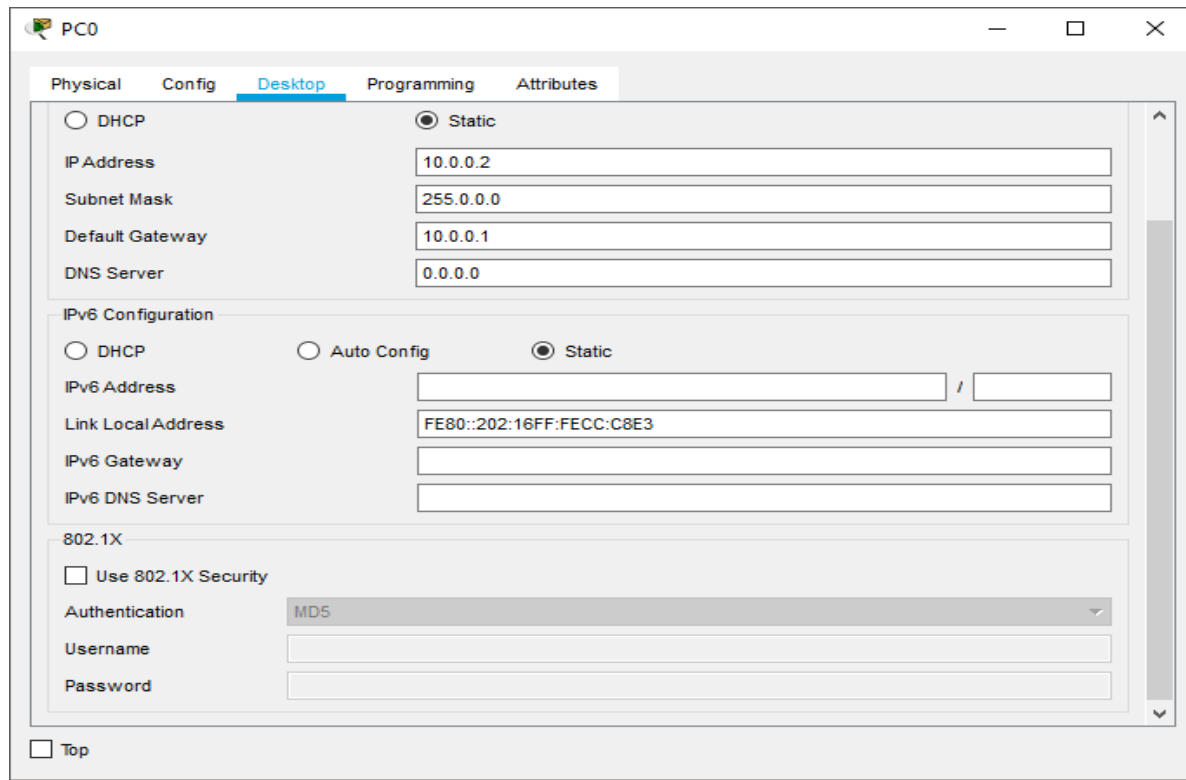
### Configure Router2

```
Router>enable
Router#
Router#configure terminal
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 50.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#ip address 40.0.0.2 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

```
Router(config)#router rip
Router(config-router)#network 40.0.0.0
Router(config-router)#network 50.0.0.0
Router(config-router)#
```

### Configure PC0





The screenshot shows the configuration window for PC0. The 'Desktop' tab is selected. Under the 'Static' radio button, the IP Address is 10.0.0.2, Subnet Mask is 255.0.0.0, Default Gateway is 10.0.0.1, and DNS Server is 0.0.0.0. The IPv6 Configuration section has the 'Static' radio button selected, with an empty IPv6 Address field, a Link Local Address of FE80::202:16FF:FECC:C8E3, and empty fields for IPv6 Gateway and IPv6 DNS Server. The 802.1X section has 'Use 802.1X Security' unchecked, 'Authentication' set to MD5, and empty fields for Username and Password. A 'Top' button is at the bottom left.

PC0

Physical Config **Desktop** Programming Attributes

☐ DHCP ☒ Static

IP Address 10.0.0.2

Subnet Mask 255.0.0.0

Default Gateway 10.0.0.1

DNS Server 0.0.0.0

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address /

Link Local Address FE80::202:16FF:FECC:C8E3

IPv6 Gateway

IPv6 DNS Server

802.1X

☐ Use 802.1X Security

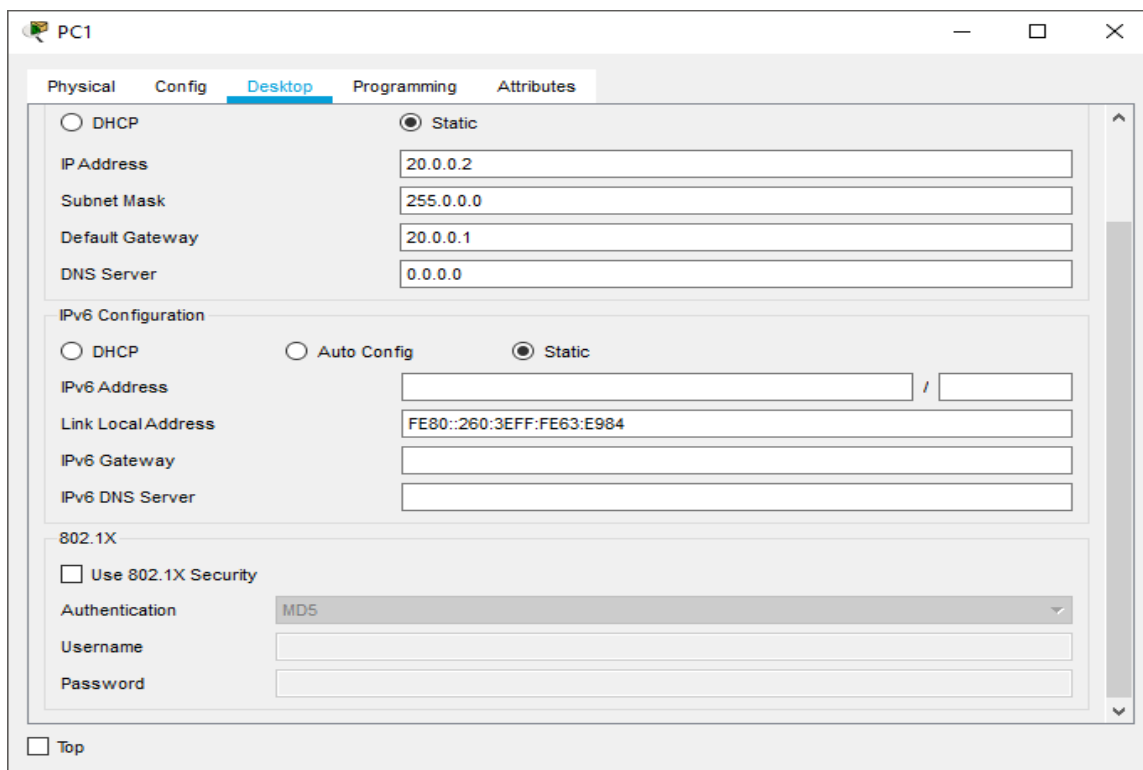
Authentication MD5

Username

Password

☐ Top

## Configure PC1



The screenshot shows the configuration window for PC1. The 'Desktop' tab is selected. Under the 'Static' radio button, the IP Address is 20.0.0.2, Subnet Mask is 255.0.0.0, Default Gateway is 20.0.0.1, and DNS Server is 0.0.0.0. The IPv6 Configuration section has the 'Static' radio button selected, with an empty IPv6 Address field, a Link Local Address of FE80::260:3EFF:FE63:E984, and empty fields for IPv6 Gateway and IPv6 DNS Server. The 802.1X section has 'Use 802.1X Security' unchecked, 'Authentication' set to MD5, and empty fields for Username and Password. A 'Top' button is at the bottom left.

PC1

Physical Config **Desktop** Programming Attributes

☐ DHCP ☒ Static

IP Address 20.0.0.2

Subnet Mask 255.0.0.0

Default Gateway 20.0.0.1

DNS Server 0.0.0.0

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address /

Link Local Address FE80::260:3EFF:FE63:E984

IPv6 Gateway

IPv6 DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

☐ Top

## Configure PC2

PC2

Physical Config **Desktop** Programming Attributes

☐ DHCP ☒ Static

IP Address 50.0.0.3

Subnet Mask 255.0.0.0

Default Gateway 50.0.0.1

DNS Server 0.0.0.0

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address /

Link Local Address FE80::230:F2FF:FE18:7D38

IPv6 Gateway

IPv6 DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

☐ Top

## Configure RADIUS SERVER

RADIUS SERVER

Physical Config Services **Desktop** Programming Attributes

☐ DHCP ☒ Static

IP Address 50.0.0.2

Subnet Mask 255.0.0.0

Default Gateway 50.0.0.1

DNS Server 0.0.0.0

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address /

Link Local Address FE80::20C:85FF:FE3E:840E

IPv6 Gateway

IPv6 DNS Server

802.1X

☐ Use 802.1X Security

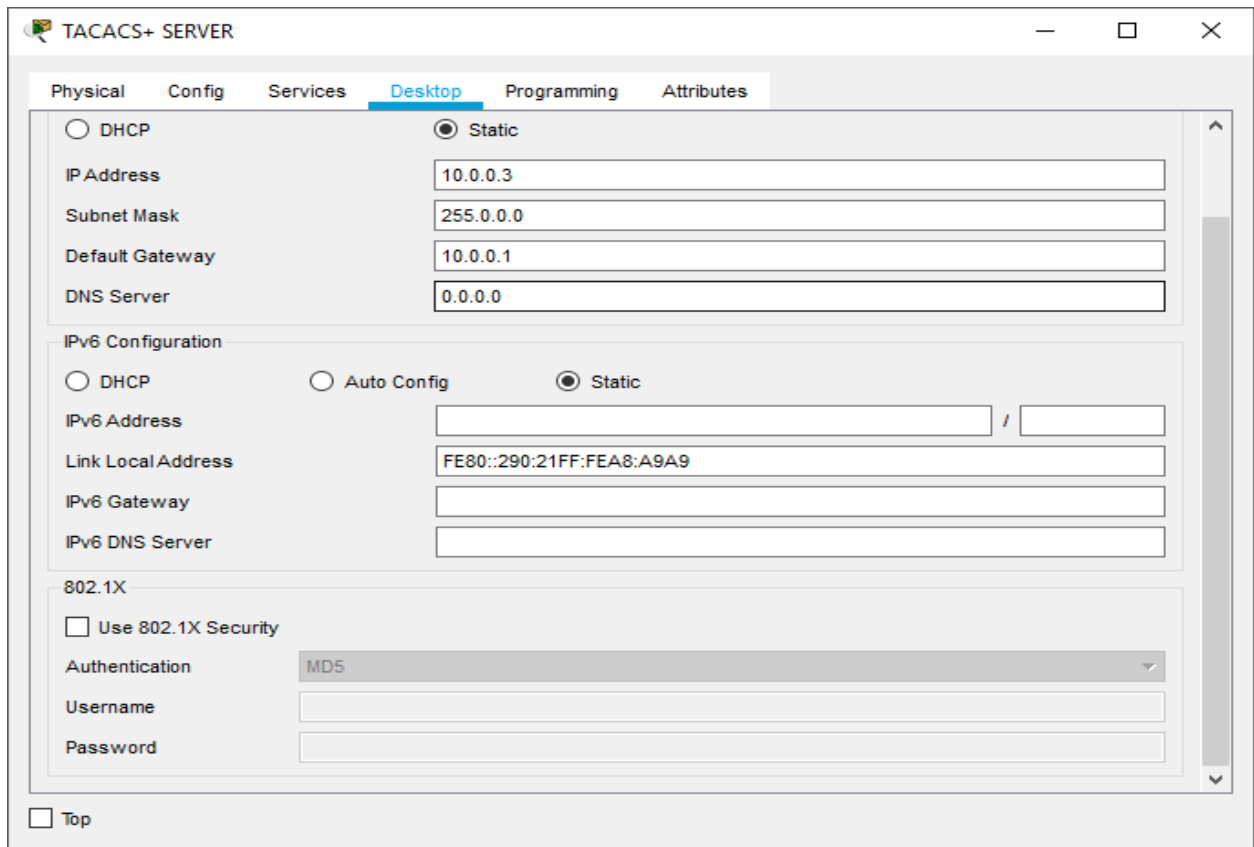
Authentication MD5

Username

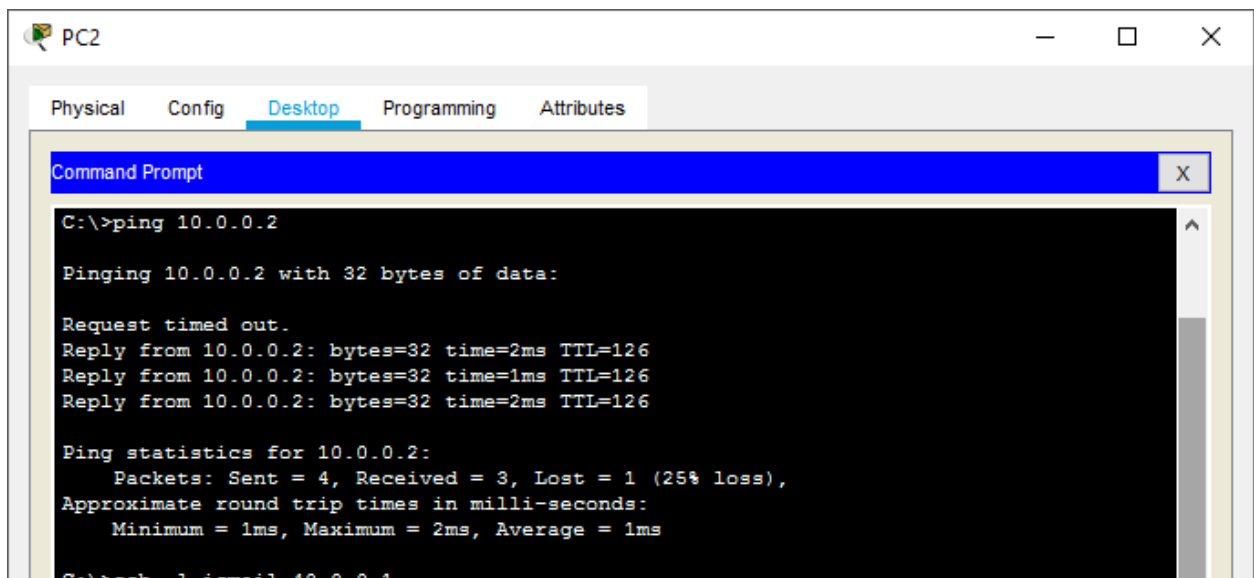
Password

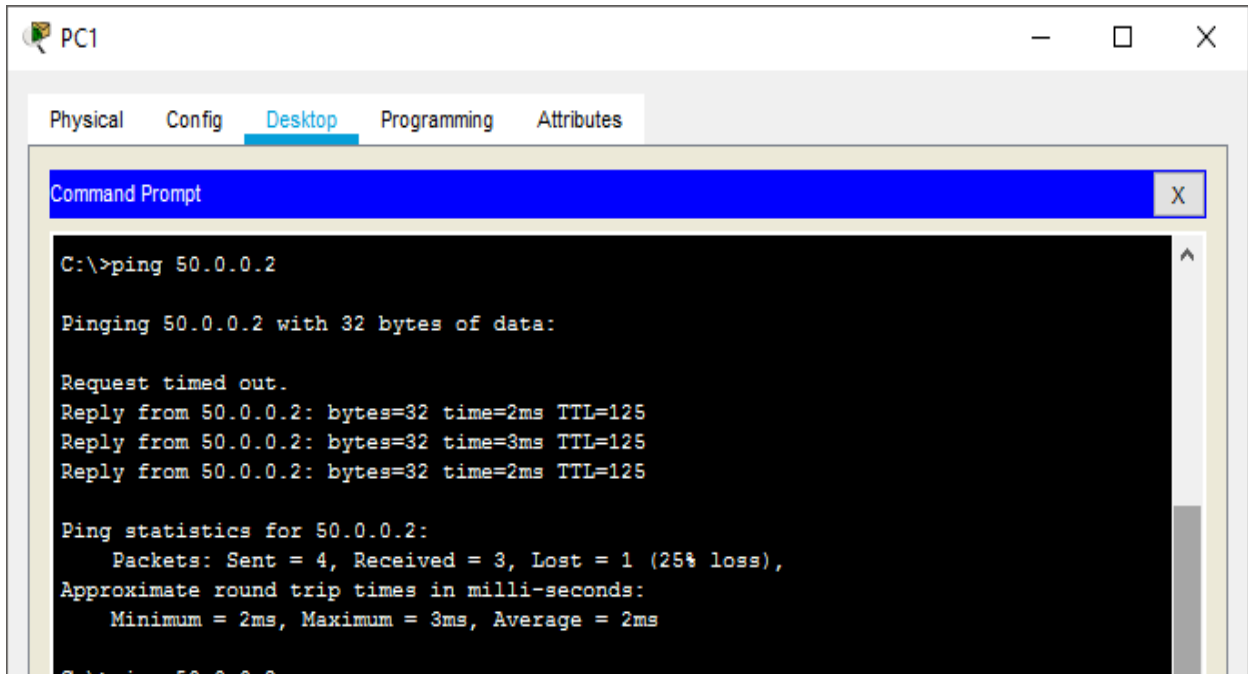
☐ Top

## Configure TACACS+ SERVER



We verify the connectivity by using the following commands





**Configure the Local AAA Authentication for Console Access on Router0 (type the following commands in the CLI mode of Router0)**

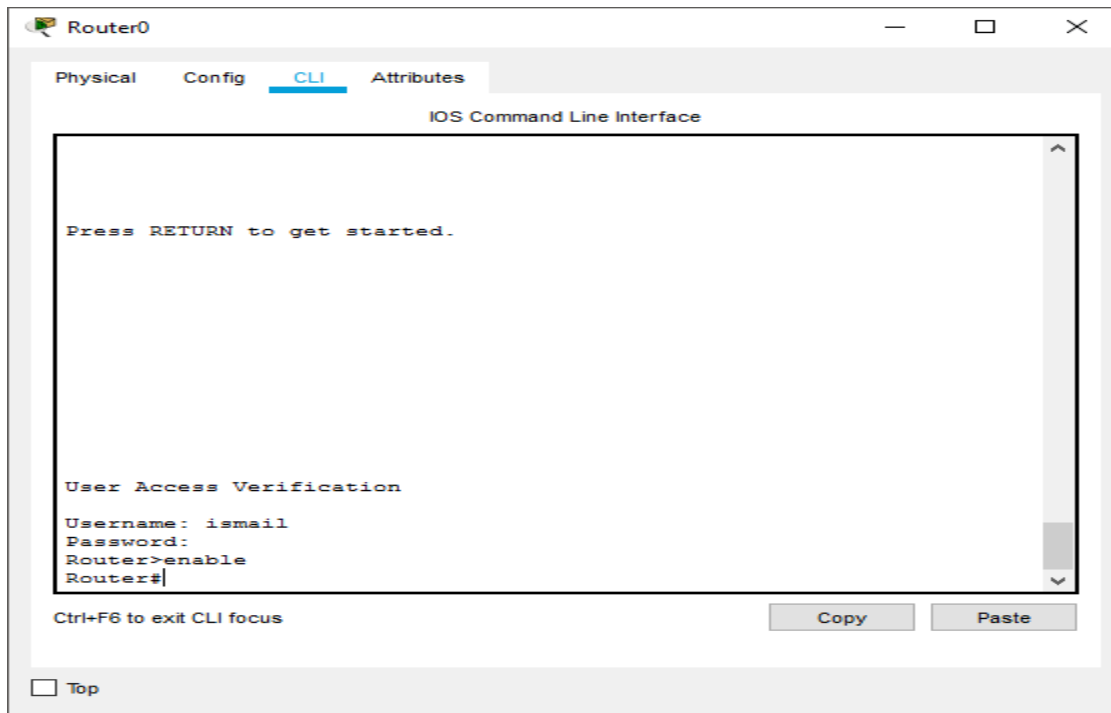
```
Router>
Router>en
Router#configure terminal
Router(config)#username admin secret abcd
Router(config)#aaa new-model
Router(config)#aaa authentication login default local
Router(config)#line console 0
Router(config-line)#login authentication default
Router(config-line)#end
Router#exit
```

**Press ENTER to get started.**

**User Access Verification**

Username: admin  
Password:  
Router>enable  
Router#

Hence the Authentication is done



Configure the vty lines to use the defined AAA authentication method( type the following command in Router0)

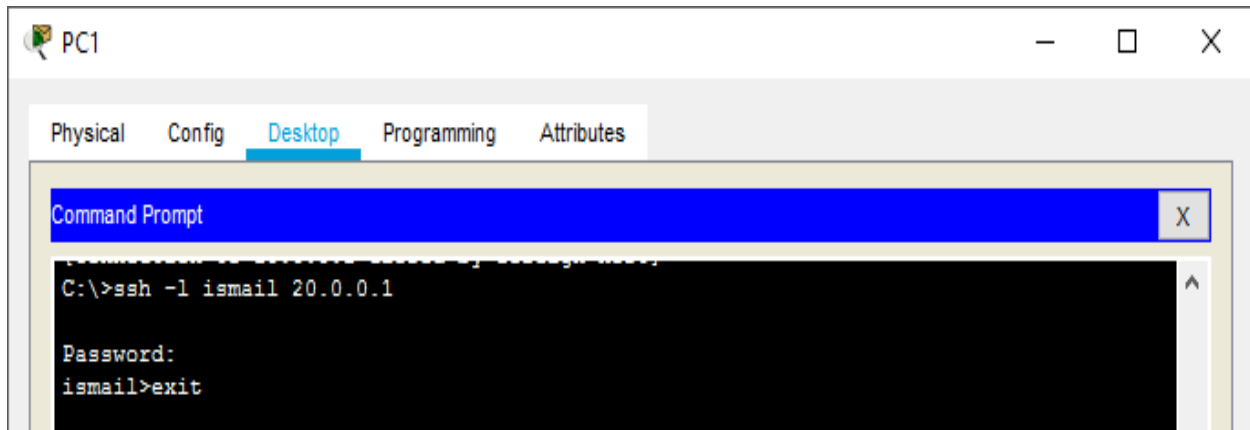
```
Router>enable
Router#configure terminal
Router(config)#ip domain-name admin.com
Router(config)#hostname admin
admin(config)#crypto key generate rsa
The name for the keys will be: admin.admin.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
```

```
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

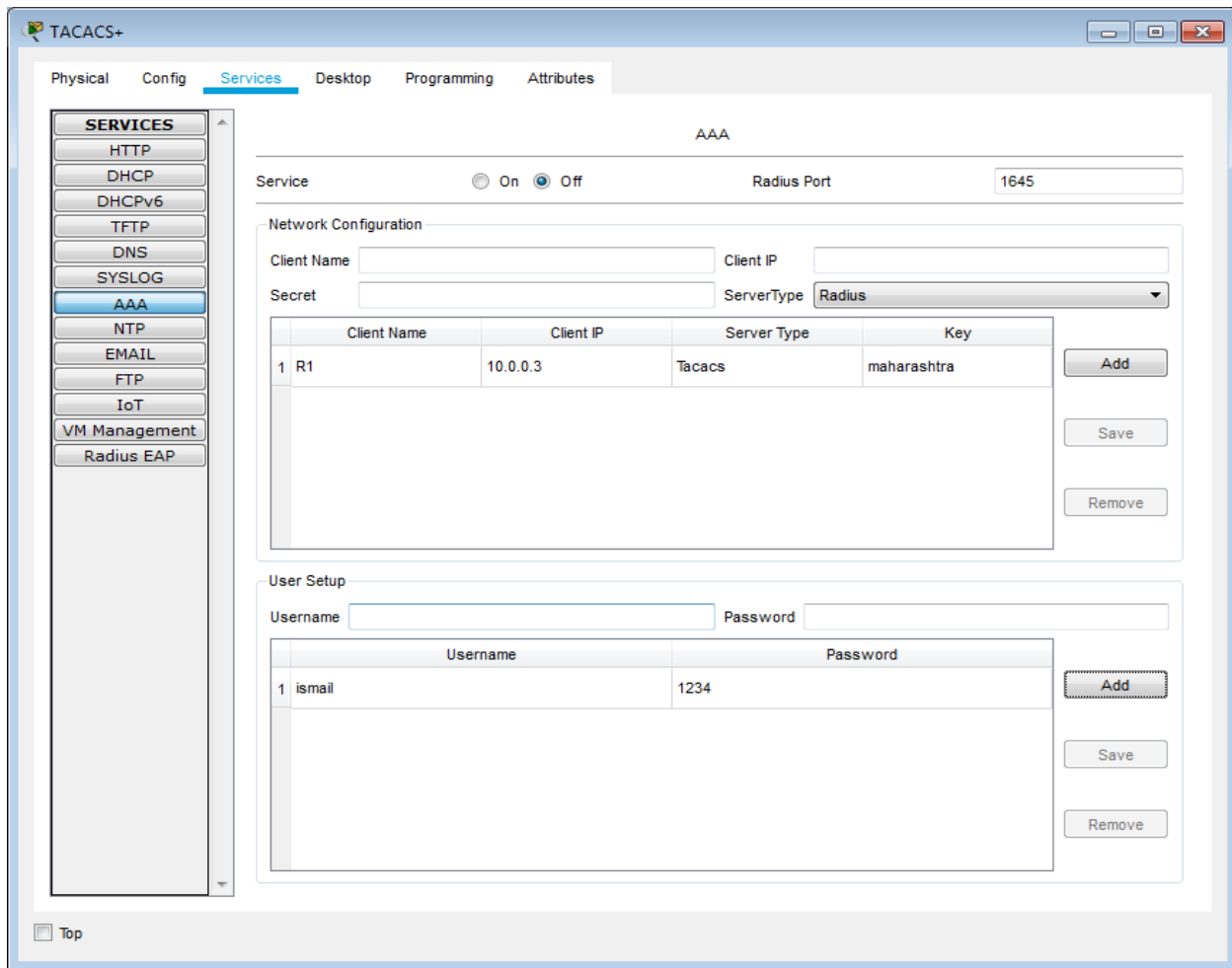
```
admin(config)#aaa authentication login ssh-admin local
admin(config)#line vty 0 4
admin(config-line)#login authentication ssh-admin
```

```
admin(config-line)#transport input ssh
admin(config-line)#end
admin#
```

Now verify the configuration using the following



## TACACS+ Server configuration



## Configure Server-Based AAA Authentication Using TACACS+ on Router1 (type the following commands in the CLI mode of Router1)

```
Router#configure terminal
Router(config)#username admin secret 12345
Router(config)#tacacs-server host 10.0.0.3
Router(config)#tacacs-server key 1234
Router(config)#hostname R1
R1(config)#aaa new-model
R1(config)#aaa authentication login default group tacacs+ local
R1(config)#line console 0
R1(config-line)#login authentication default
R1(config-line)#end
R1#

R1#exit
```

Press Enter to get started.

## User Access Verification

Username: admin

Password:

R1>en

R1#exit

## Configure Server-Based AAA Authentication Using RADIUS on R3

### RADIUS Server configuration

**RADIUS**

Physical Config **Services** Desktop Programming Attributes

**SERVICES**

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

**AAA**

Service ☐ On ☒ Off Radius Port 1645

**Network Configuration**

Client Name  Client IP

Secret  ServerType Radius

	Client Name	Client IP	Server Type	Key	
1	R3	50.0.0.3	Radius	maharashtra	<input type="button" value="Add"/>

**User Setup**

Username ismail Password 1234

	Username	Password	
1	ismail	1234	<input type="button" value="Add"/>

☐ Top



## **Configure Server-Based AAA Authentication Using RADIUS Server on Router3( type the following commands in the CLI mode of Router1)**

```
Router#configure terminal
Router(config)#username admin secret 12345
Router(config)#radius-server host 50.0.0.3
Router(config)#radius-server key 1234
Router(config)#hostname R3
R3(config)#aaa new-model
R3(config)#aaa authentication login default group tacacs+ local
R3(config)#line console 0
R3(config-line)#login authentication default
R3(config-line)#end
R3#

R3#exit
```

**Press Enter to get started.**

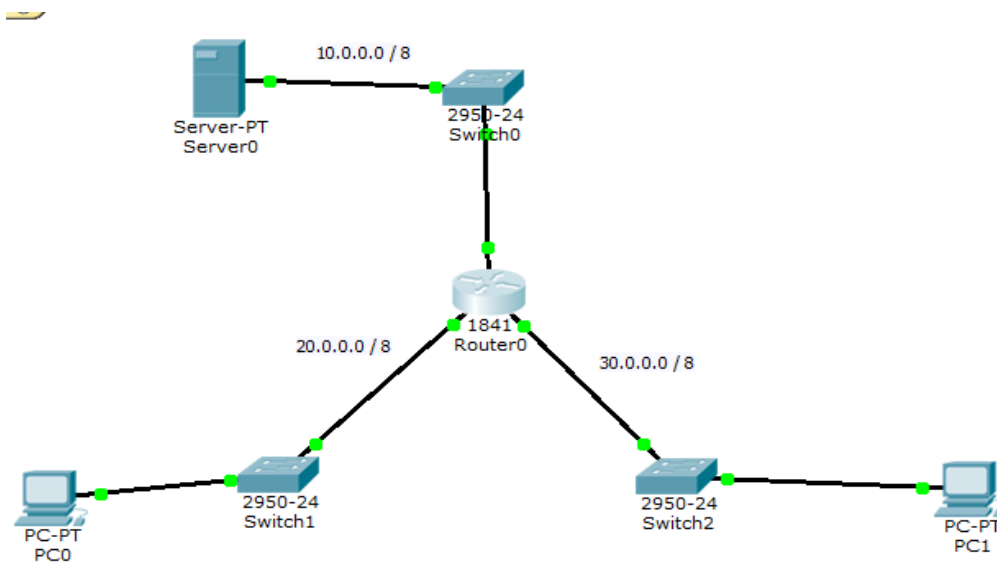
### **User Access Verification**

```
Username: admin
Password:
R3>en
R3#exit
```

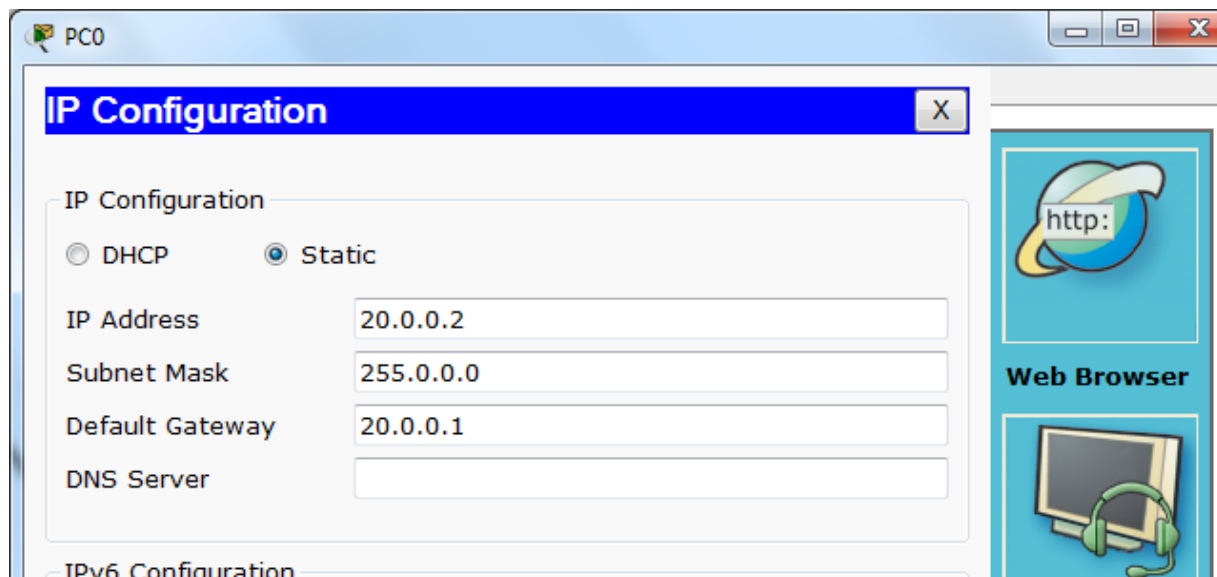
## PRACTICAL NO 3: Configuring Extended ACLs

ACLs are used to control network access or to specify traffic for many features to act upon. An extended ACL is made up of one or more access control entries (ACEs). Each ACE specifies a source and destination for matching traffic. You can identify parameters within the access-list command, or you can create objects or object groups for use in the ACL.

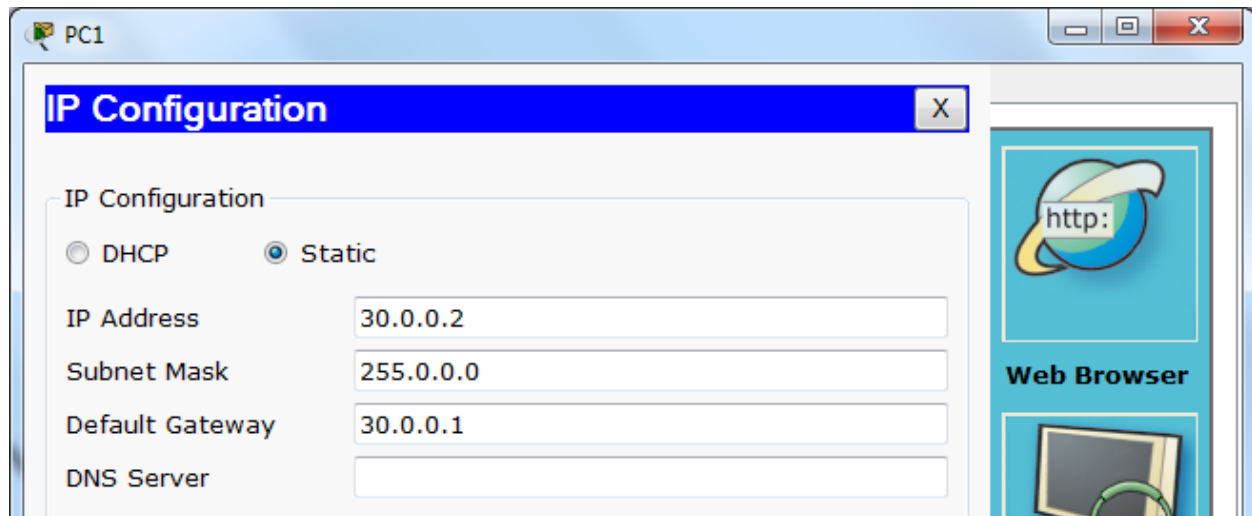
We use the following topology to study ACL configuration



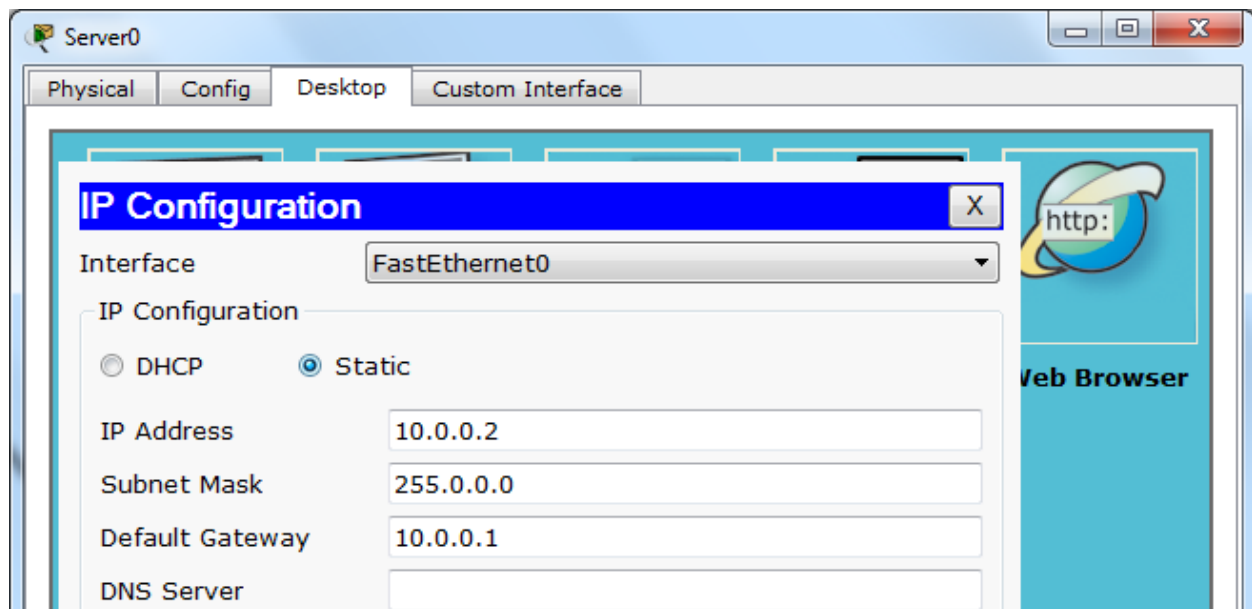
### Configuring PC0



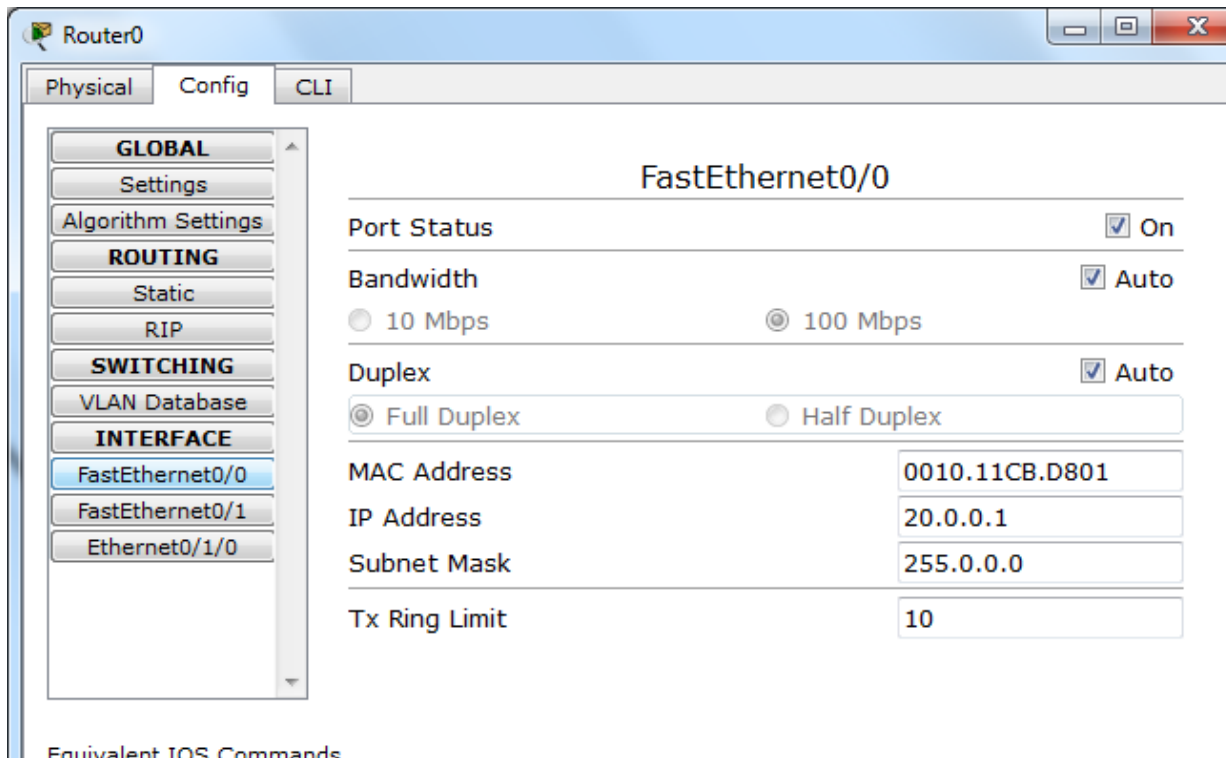
## Configuring PC1



## Configuring Server



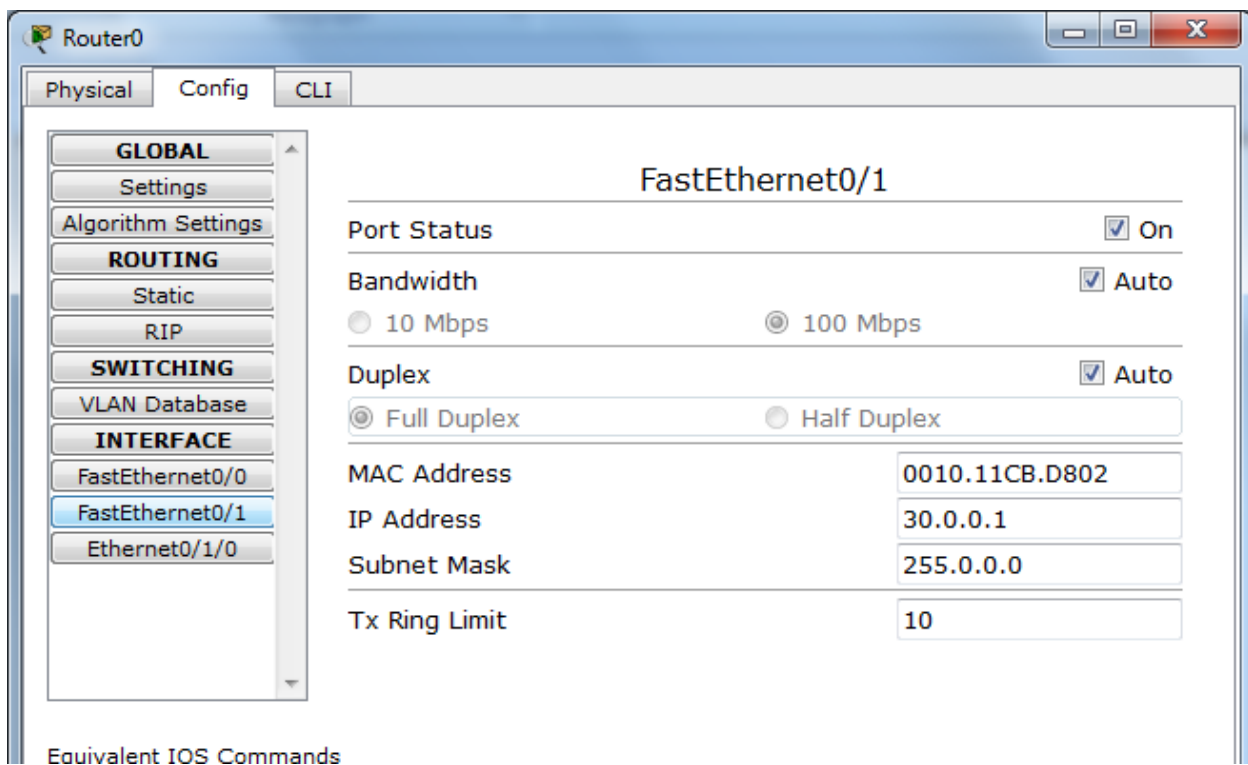
## Configuring Router



The screenshot shows the Router0 configuration window with the 'Config' tab selected. The left sidebar has a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under INTERFACE, 'FastEthernet0/0' is selected. The main area displays the configuration for 'FastEthernet0/0' with the following settings:

Parameter	Value
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="checkbox"/> Auto <input type="radio"/> 10 Mbps <input checked="" type="radio"/> 100 Mbps
Duplex	<input checked="" type="checkbox"/> Auto <input checked="" type="radio"/> Full Duplex <input type="radio"/> Half Duplex
MAC Address	0010.11CB.D801
IP Address	20.0.0.1
Subnet Mask	255.0.0.0
Tx Ring Limit	10

Equivalent IOS Commands



The screenshot shows the Router0 configuration window with the 'Config' tab selected. The left sidebar has a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under INTERFACE, 'FastEthernet0/1' is selected. The main area displays the configuration for 'FastEthernet0/1' with the following settings:

Parameter	Value
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="checkbox"/> Auto <input type="radio"/> 10 Mbps <input checked="" type="radio"/> 100 Mbps
Duplex	<input checked="" type="checkbox"/> Auto <input checked="" type="radio"/> Full Duplex <input type="radio"/> Half Duplex
MAC Address	0010.11CB.D802
IP Address	30.0.0.1
Subnet Mask	255.0.0.0
Tx Ring Limit	10

Equivalent IOS Commands

The screenshot shows the 'Router0' configuration window with the 'Config' tab selected. The left sidebar has a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under 'INTERFACE', 'Ethernet0/1/0' is selected. The main area displays the configuration for 'Ethernet0/1/0' with the following fields:

Ethernet0/1/0	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="checkbox"/> Auto
<input checked="" type="radio"/> 10 Mbps	
Duplex	<input checked="" type="checkbox"/> Auto
<input checked="" type="radio"/> Full Duplex <input type="radio"/> Half Duplex	
MAC Address	00D0.5865.031E
IP Address	10.0.0.1
Subnet Mask	255.0.0.0
Tx Ring Limit	10

Equivalent IOS Commands

### RIP Configuration for the Router

The screenshot shows the 'Router0' configuration window with the 'Config' tab selected. The left sidebar has a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under 'ROUTING', 'RIP' is selected. The main area displays the 'RIP Routing' configuration with the following fields:

RIP Routing	
Network	<input type="text"/>
<input type="button" value="Add"/>	
Network Address	
10.0.0.0	
20.0.0.0	
30.0.0.0	
<input type="button" value="Remove"/>	

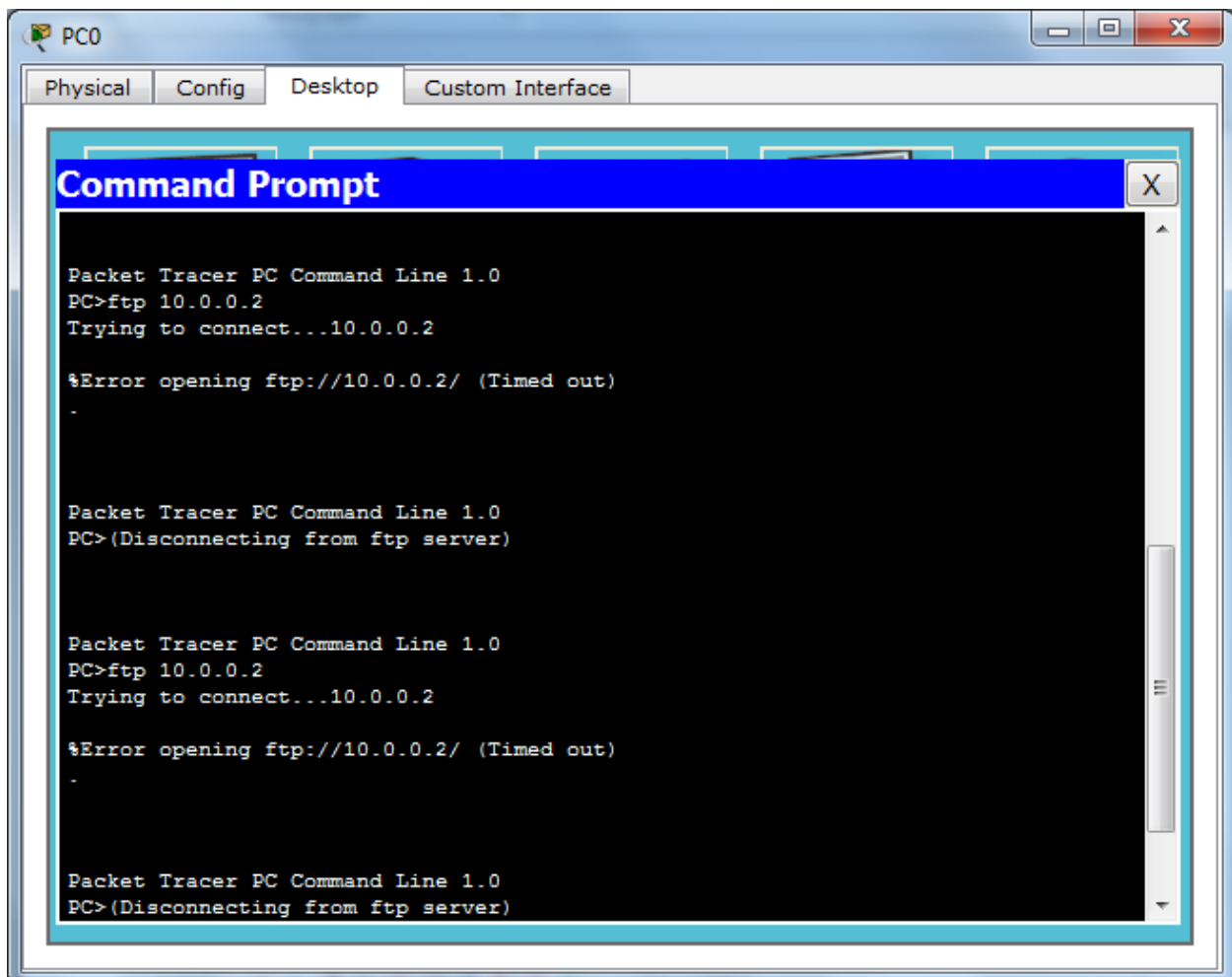
```
Router(config)#access-list ?
<1-99>   IP standard access list
<100-199> IP extended access list
Router(config)#access-list 100 ?
deny     Specify packets to reject
permit   Specify packets to forward
remark   Access list entry comment
Router(config)#access-list 100 permit ?
ahp      Authentication Header Protocol
eigrp    Cisco's EIGRP routing protocol
esp      Encapsulation Security Payload
gre      Cisco's GRE tunneling
icmp     Internet Control Message Protocol
ip       Any Internet Protocol
ospf     OSPF routing protocol
tcp      Transmission Control Protocol
udp      User Datagram Protocol
Router(config)#access-list 100 permit tcp ?
A.B.C.D  Source address
any      Any source host
host     A single source host
Router(config)#access-list 100 permit tcp 10.0.0.2 ?
A.B.C.D  Source wildcard bits
Router(config)#access-list 100 permit tcp 10.0.0.2 0.255.255.255 ?
A.B.C.D  Destination address
any      Any destination host
eq       Match only packets on a given port number
gt       Match only packets with a greater port number
host     A single destination host
lt       Match only packets with a lower port number
neq      Match only packets not on a given port number
range    Match only packets in the range of port numbers
Router(config)#access-list 100 permit tcp 10.0.0.2 0.255.255.255 host ?
A.B.C.D  Destination address
Router(config)#access-list 100 permit tcp 10.0.0.2 0.255.255.255 host 20.0.0.2 ?
dscp     Match packets with given dscp value
eq       Match only packets on a given port number
established established
gt       Match only packets with a greater port number
lt       Match only packets with a lower port number
neq      Match only packets not on a given port number
precedence Match packets with given precedence value
range    Match only packets in the range of port numbers
<cr>
Router(config)#access-list 100 permit tcp 10.0.0.2 0.255.255.255 host 20.0.0.2 eq ?
<0-65535> Port number
```

```
ftp      File Transfer Protocol (21)
pop3     Post Office Protocol v3 (110)
smtp     Simple Mail Transport Protocol (25)
telnet   Telnet (23)
www      World Wide Web (HTTP, 80)
Router(config)#access-list 100 permit tcp 10.0.0.2 0.255.255.255 host 20.0.0.2 eq ftp
Router(config)#interface FastEthernet0/0
Router(config-if)#ip access-group 100 in
```

Verifying the output by typing the following command from PC0

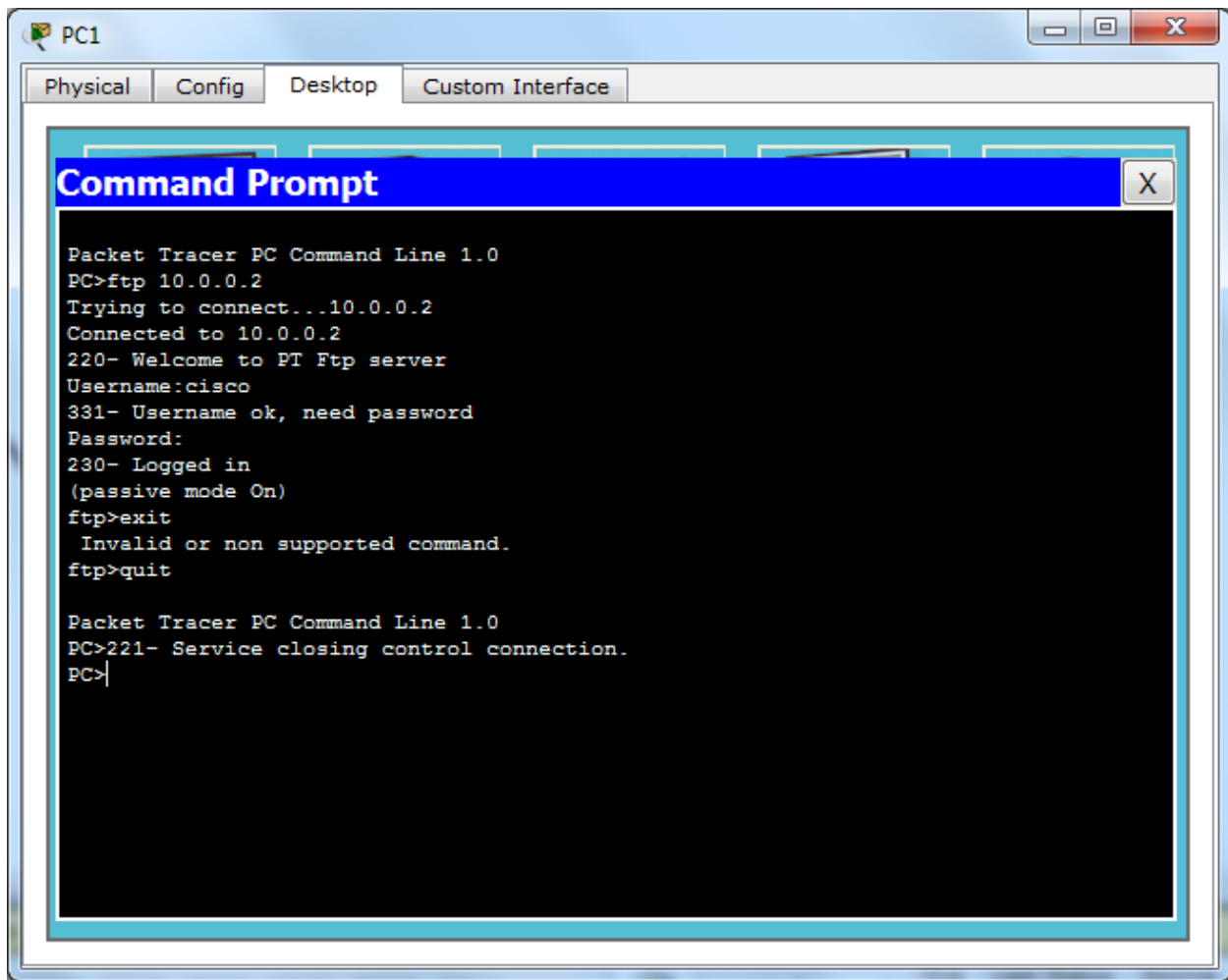
PC> [ftp 10.0.0.2](#)

We get the following output output



Now verifying the output by typing the following command from PC1

PC> [ftp 10.0.0.2](#)



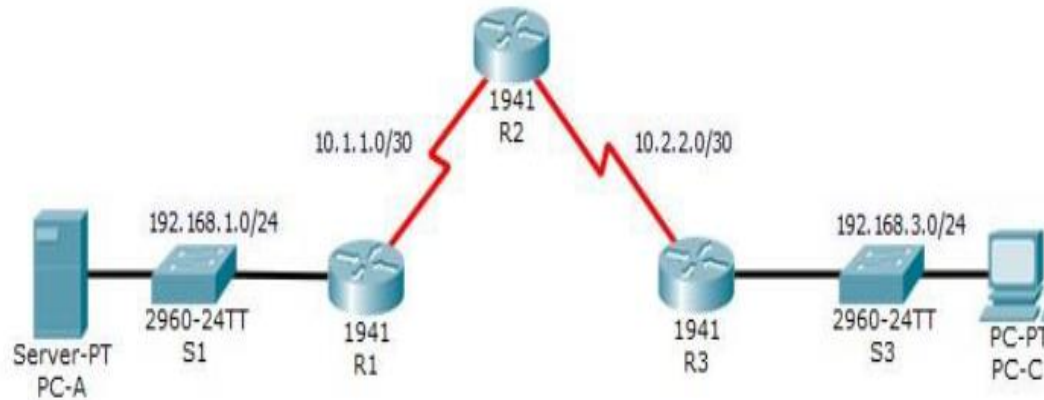
The screenshot shows a Packet Tracer PC Command Line window for PC1. The window has tabs for Physical, Config, Desktop, and Custom Interface. The Command Prompt window is open, displaying the following text:

```
Packet Tracer PC Command Line 1.0
PC>ftp 10.0.0.2
Trying to connect...10.0.0.2
Connected to 10.0.0.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>exit
Invalid or non supported command.
ftp>quit

Packet Tracer PC Command Line 1.0
PC>221- Service closing control connection.
PC>
```



## Practical 4: Configure IP ACLs to Mitigate Attacks.



**Addressing Table**

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
	Lo0	192.168.2.1	255.255.255.0	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

We configure the PCs, Server and Routers as follows

Server2

Physical Config Services **Desktop** Programming Attributes

☐ DHCP ☒ Static

IP Address

Subnet Mask

Default Gateway

DNS Server

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

Router4

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

IP Configuration

IP Address

Subnet Mask

Tx Ring Limit

Router4

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

**Serial0/1/0**

Port Status ☒ On

Duplex ☒ Full Duplex

Clock Rate

IP Configuration

IP Address

Subnet Mask

Tx Ring Limit

The image displays two screenshots of the Router6 configuration interface, showing the configuration for two serial interfaces: Serial0/1/0 and Serial0/1/1.

**Router6 - Serial0/1/0 Configuration:**

- Physical:** Config, CLI, Attributes
- Left Panel (Tree View):**
  - GLOBAL
    - Settings
    - Algorithm Settings
  - ROUTING
    - Static
    - RIP
  - SWITCHING
    - VLAN Database
  - INTERFACE
    - GigabitEthernet0/0
    - GigabitEthernet0/1
    - Serial0/1/0 (Selected)
    - Serial0/1/1
- Right Panel (Serial0/1/0):**
  - Port Status: ☒ On
  - Duplex: ☐ Full Duplex
  - Clock Rate: 2000000
  - IP Configuration:
    - IP Address: 10.1.1.2
    - Subnet Mask: 255.255.255.252
  - Tx Ring Limit: 10

**Router6 - Serial0/1/1 Configuration:**

- Physical:** Config, CLI, Attributes
- Left Panel (Tree View):**
  - GLOBAL
    - Settings
    - Algorithm Settings
  - ROUTING
    - Static
    - RIP
  - SWITCHING
    - VLAN Database
  - INTERFACE
    - GigabitEthernet0/0
    - GigabitEthernet0/1
    - Serial0/1/0
    - Serial0/1/1 (Selected)
- Right Panel (Serial0/1/1):**
  - Port Status: ☒ On
  - Duplex: ☐ Full Duplex
  - Clock Rate: 1200
  - IP Configuration:
    - IP Address: 10.2.2.1
    - Subnet Mask: 255.255.255.252
  - Tx Ring Limit: 10

Router5

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

**Serial0/1/0**

Port Status ☒ On

Duplex ☐ Full Duplex

Clock Rate 2000000

IP Configuration

IP Address 10.2.2.2

Subnet Mask 255.255.255.252

Tx Ring Limit 10

Router5

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

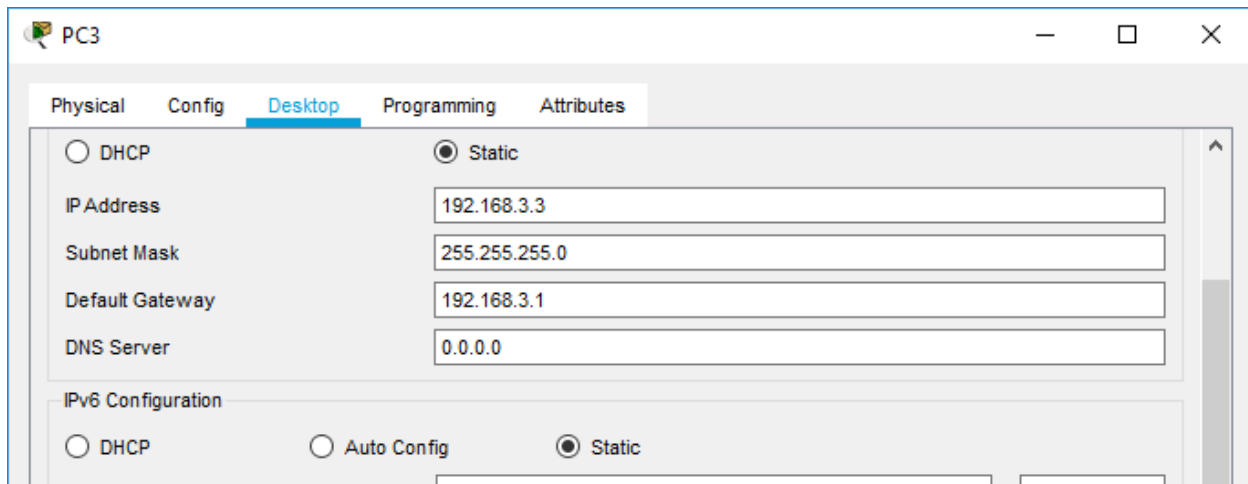
MAC Address 000B.BE67.E801

IP Configuration

IP Address 192.168.3.1

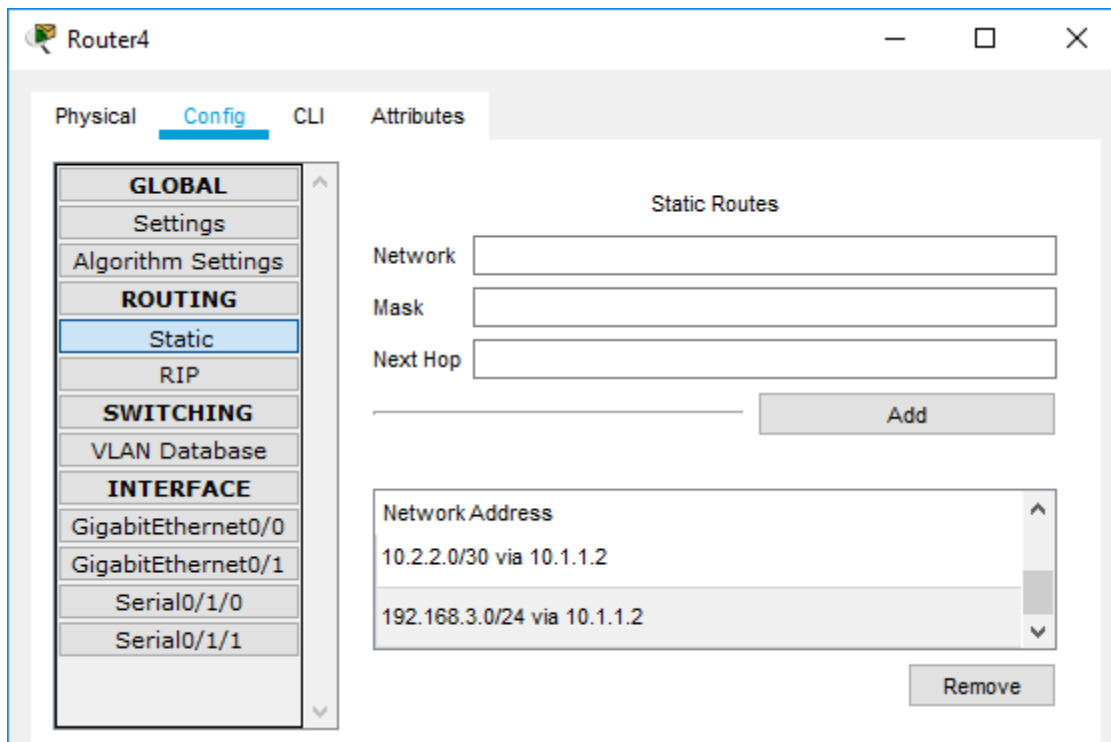
Subnet Mask 255.255.255.0

Tx Ring Limit 10



## STATIC ROUTING :

Now we do the Static Routing on all the Routers as follows



Router6

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

Static Routes

Network

Mask

Next Hop

Network Address

192.168.1.0/24 via 10.1.1.1

192.168.3.0/24 via 10.2.2.2

Router5

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

Static Routes

Network

Mask

Next Hop

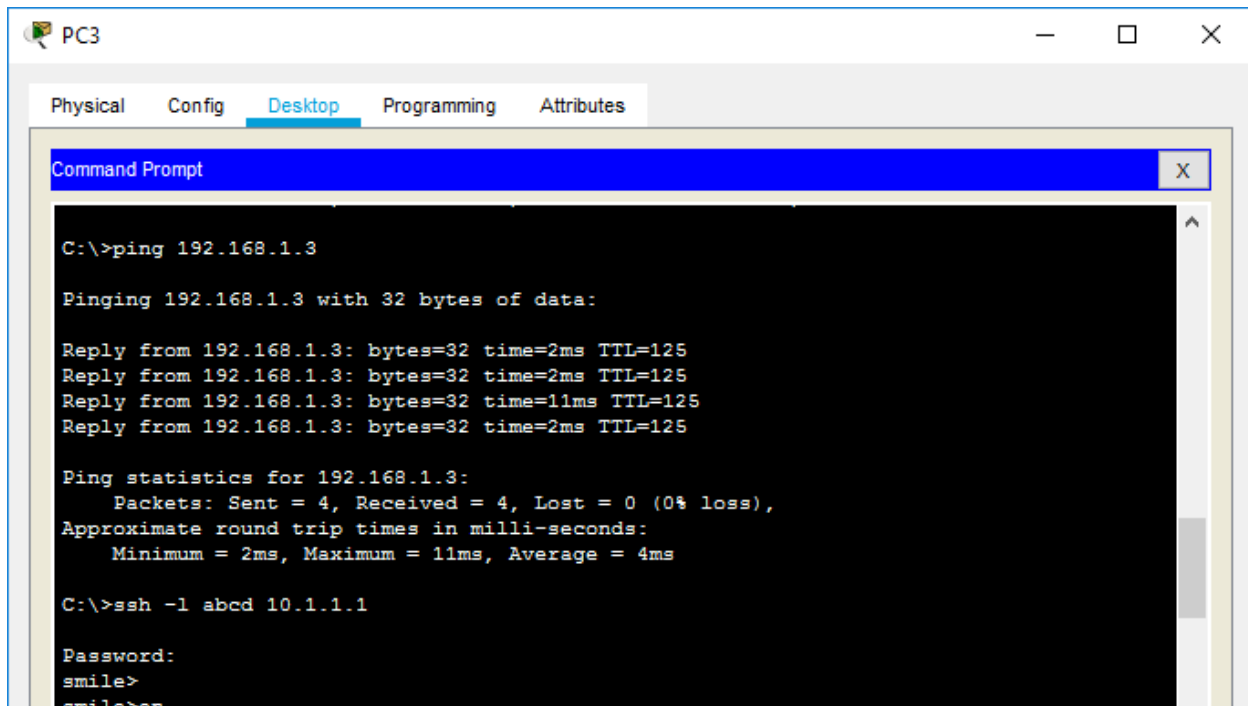
Network Address

192.168.1.0/24 via 10.2.2.1

10.1.1.0/30 via 10.2.2.1

## PART 1 : Verify the basic network connectivity

Now we check the connectivity by pinging the server (192.168.1.3) from the PC (192.168.3.3)

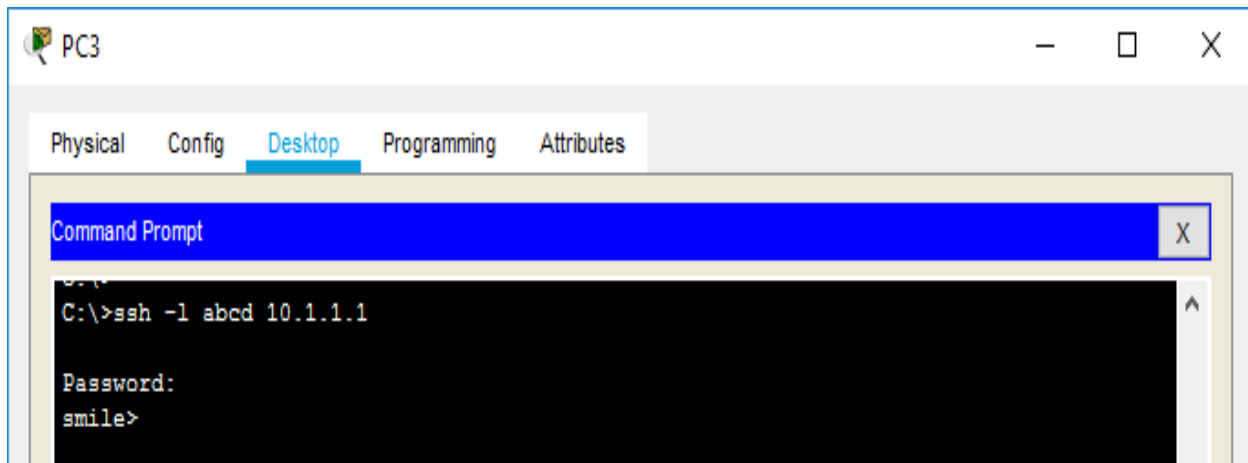


Setting the SSH on Router 4 using the following commands in the CLI mode

```
Router(config)#username abcd secret xyz
Router(config)#aaa new-model
Router(config)#aaa authentication login default local
Router(config)#ip domain-name smile.com
Router(config)#hostname smile
smile(config)#crypto
smile(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
```

```
smile(config)#aaa authentication login abcd local
smile(config)#line vty 0 4
smile(config-line)#login authentication abcd
smile(config-line)#transport input ssh
smile(config-line)#end
```

Now verifying the same using the following commands on the PC



## PART 2: Secure Access to Routers

Configure the Router 4 to block any access to the routers except the PC (192.168.3.3)

```
smile#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
smile(config)#access-list 10 permit host 192.168.3.3
```

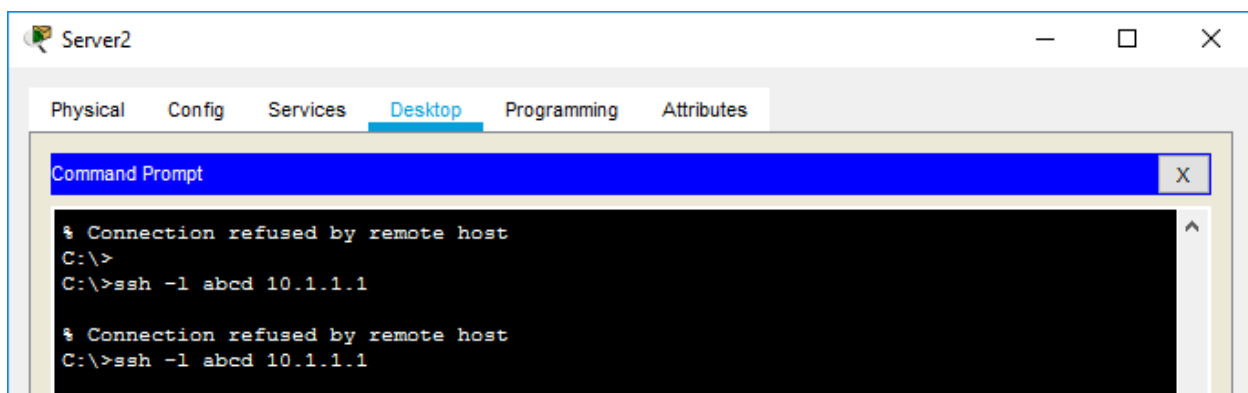
```
smile(config)#line vty 0 4
```

```
smile(config-line)#access-class 10 in
```

```
smile(config-line)#exit
```

From the above commands we deny any host other than PC (192.168.3.3) to get access to the router 4

We check it by accessing the Router 4 through the Server (192.168.1.3) as follows





### PART 3: Create a Numbered IP ACL 120 on Router 4

We type the following command in the CLI mode for the Router 4  
smile#

smile#configure terminal

smile(config)#access-list 120 permit tcp any host 192.168.1.3 eq smtp

smile(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp

smile(config)#access-list 120 deny tcp any host 192.168.1.3 eq 443

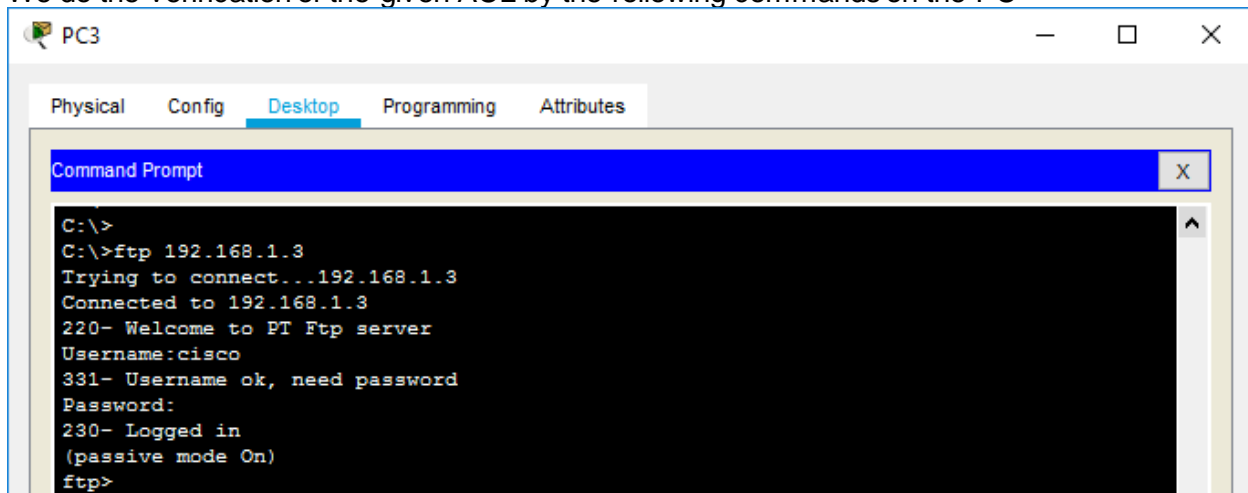
smile(config)#access-list 120 permit tcp any host 192.168.1.3 eq 22

smile(config)#interface Serial0/1/0

smile(config-if)#ip access-group 120 in

smile(config-if)#exit

We do the verification of the given ACL by the following commands on the PC



### PART 4: Modify an Existing ACL on Router 4

Smile(config)# access-list 120 permit icmp any any echo-reply

Smile(config)# access-list 120 permit icmp any any unreachable

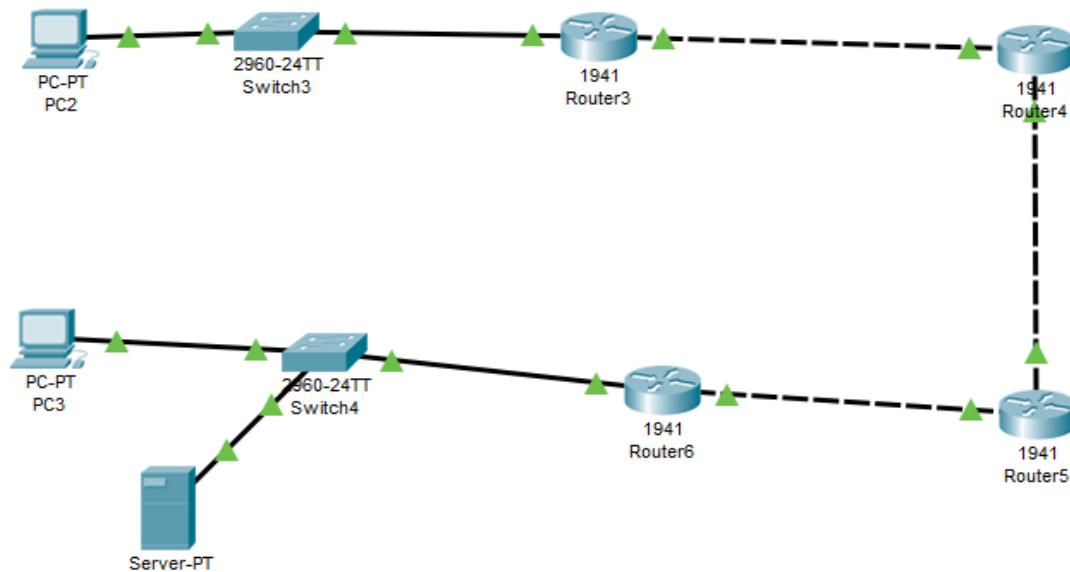
Smile(config)# access-list 120 deny icmp any any

Smile(config)# access-list 120 permit ip any any

Similarly we can create and modify the ACLs for all the Routers

## Practical 5: Configuring IPv6 ACLs

We use the following topology to configure the IPv6 ACLs



We configure the Hosts and Routers as follows (only add ipv6 address and gateway, don't touch the link local address)

The screenshot shows the configuration window for PC2, specifically the Desktop tab. The configuration is set to Static. The IPv6 Configuration section is also set to Static. The IPv6 Address is configured as 2004::2 / 64. The Link Local Address is FE80::20D:BDFF:FE5E:E164. The IPv6 Gateway is 2004::1. The IPv6 DNS Server is left blank. The 802.1X section is also visible.

Field	Value
IP Address	
Subnet Mask	
Default Gateway	0.0.0.0
DNS Server	0.0.0.0
IPv6 Configuration	
IPv6 Address	2004::2 / 64
Link Local Address	FE80::20D:BDFF:FE5E:E164
IPv6 Gateway	2004::1
IPv6 DNS Server	
802.1X	

PC3

Physical Config **Desktop** Programming Attributes

☐ DHCP ☒ Static

IP Address

Subnet Mask

Default Gateway

DNS Server

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address  /

Link Local Address

IPv6 Gateway

IPv6 DNS Server

Server1

Physical Config Services **Desktop** Programming Attributes

☐ DHCP ☒ Static

IP Address

Subnet Mask

Default Gateway

DNS Server

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address  /

Link Local Address

IPv6 Gateway

IPv6 DNS Server

**For router 3 type the following commands**

```
Router>enable
Router#
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ipv6 address 2001::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ipv6 address 2002::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
```

**For router 4 type the following commands**

```
Router>en
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ipv6 address 2002::2/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ipv6 address 2003::1/64
Router(config-if)#ipv6 rip a enable
```

**For router 5 type the following commands**

```
Router>
Router>enable
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ipv6 address 2003::2/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ipv6 address 2004::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#exit
Router(config)#
```

**For router 6 type the following commands**

```
Router>
Router>enable
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ipv6 address 2004::2/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ipv6 address 2005::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#exit
Router(config)#
```

**Now we configure, apply and verify the IPv6 ACL on Router 6**

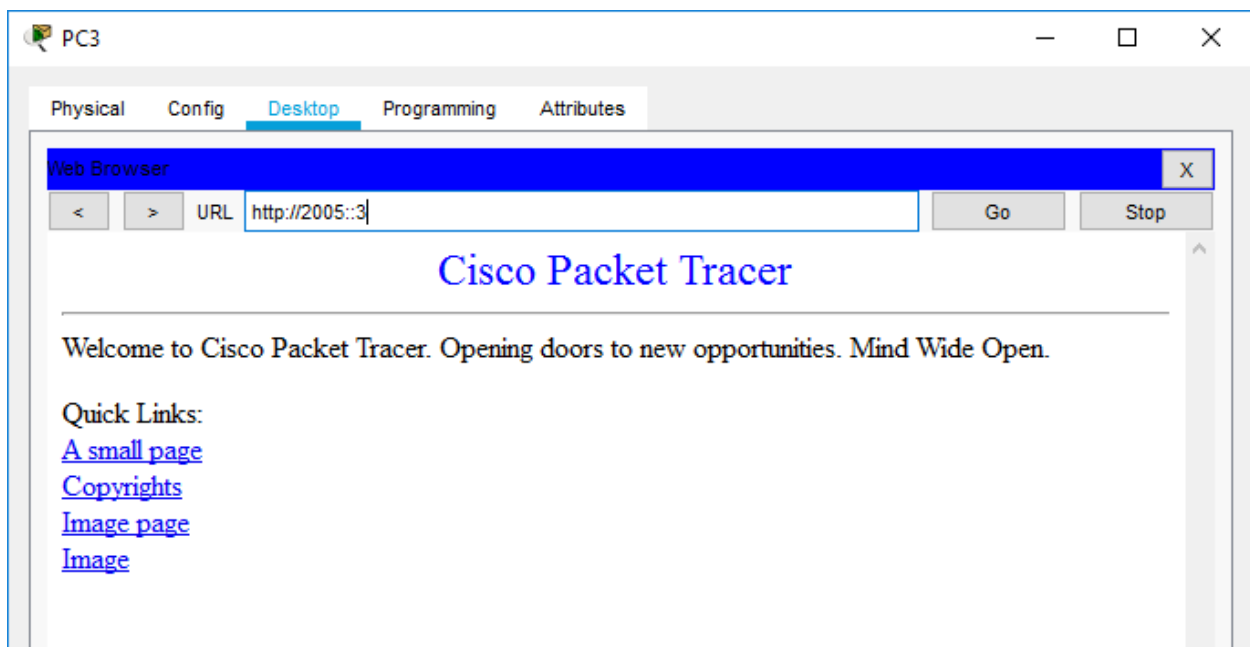
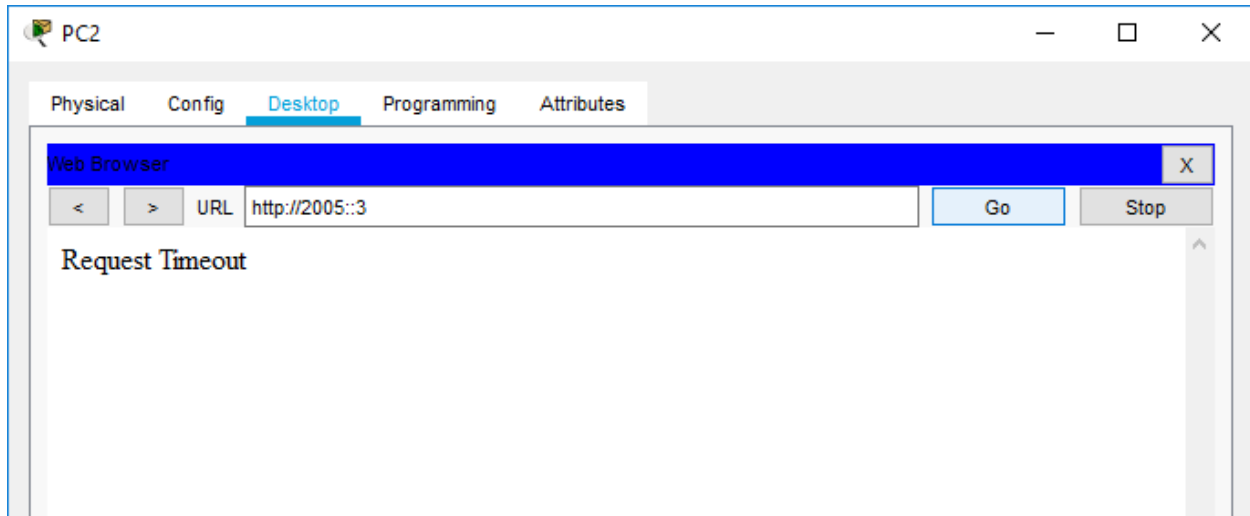
Type the following command in the CLI mode of Router 6

```
Router(config)#ipv6 acc
Router(config)#ipv6 access-list smile
Router(config-ipv6-acl)#
Router(config-ipv6-acl)#deny tcp any host 2005::3 eq www
Router(config-ipv6-acl)#deny tcp any host 2005::3 eq 443
Router(config-ipv6-acl)#exit
```

**WE apply the ACL list to the proper interface as follows**

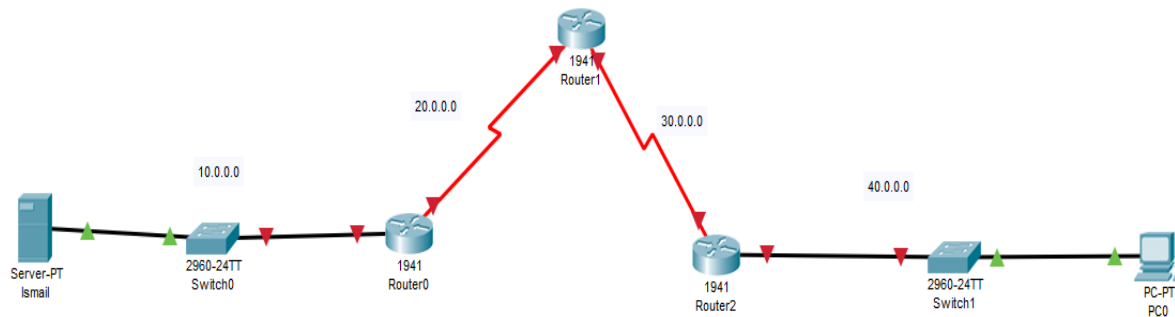
```
Router(config)#
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ipv6 traffic-filter smile in
Router(config-if)#
```

We verify the services www on PC2 and PC3 and get the following output

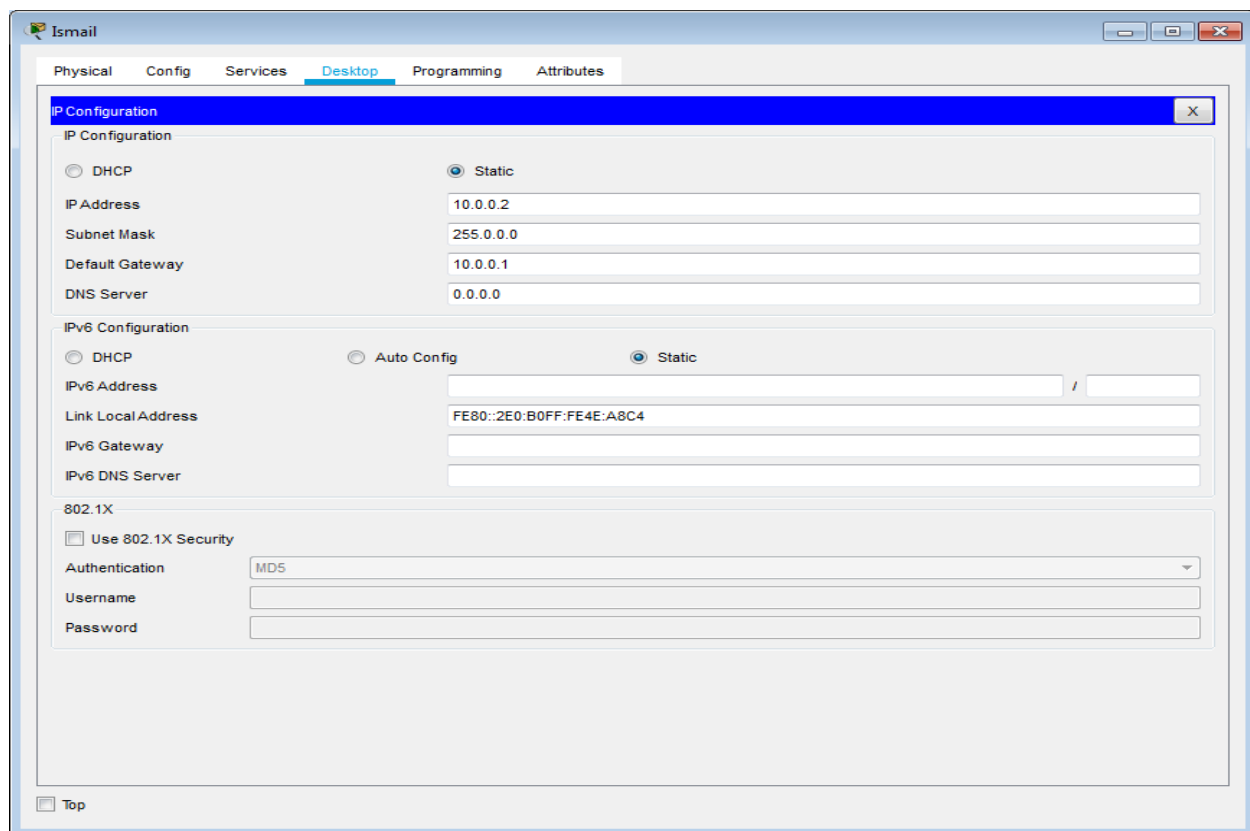


## Practical 6: Configuring a Zone-Based Policy Firewall (ZPF)

**Consider the following topology**



## Configuring Server



**(Note: The SERIAL interface must be added on each Router before configuring them)**

**Configuring the Router0:**

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#ip address 20.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#
Router(config-if)#exit

Router(config)#router rip
Router(config-router)#network 10.0.0.0
Router(config-router)#network 20.0.0.0
Router(config-router)#
```

**Configuring the Router1:**

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Serial0/1/0
Router(config-if)#ip address 20.0.0.2 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface Serial0/1/1
Router(config-if)#ip address 30.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#

Router(config)#router rip
Router(config-router)#network 30.0.0.0
Router(config-router)#network 20.0.0.0
Router(config-router)#
```

**Configuring the Router2:**

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Serial0/1/1
```



```
Router(config-if)#ip address 30.0.0.2 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 40.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

```
Router(config)#router rip
Router(config-router)#network 30.0.0.0
Router(config-router)#network 40.0.0.0
Router(config-router)#
```

## Configure the PC

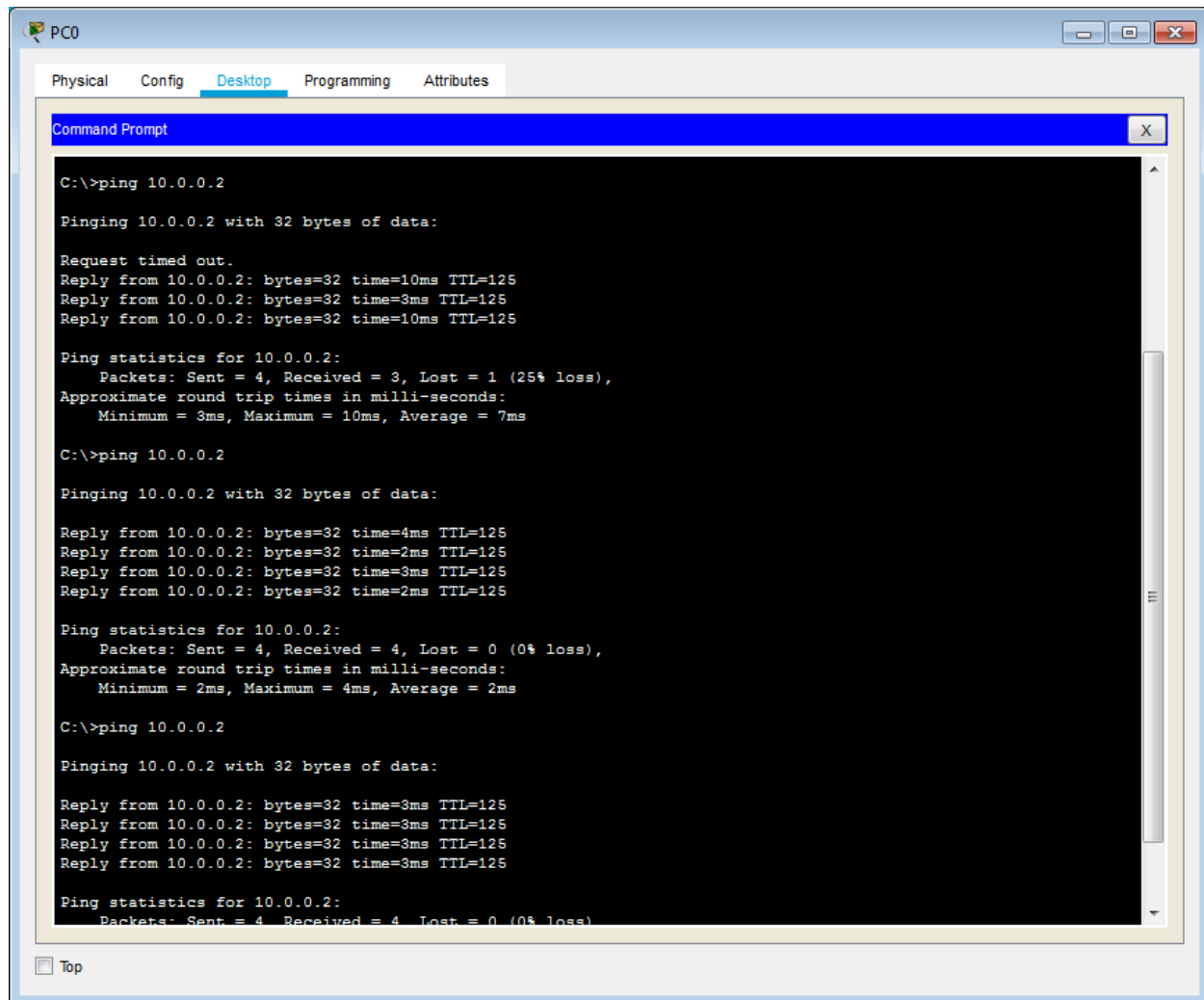
The screenshot shows the configuration window for PC0 in a network simulator. The 'Desktop' tab is selected, and the 'IP Configuration' section is expanded. The interface is 'FastEthernet0'. The IP Configuration section has two radio buttons: 'DHCP' (unselected) and 'Static' (selected). The Static configuration fields are filled with the following values:

Field	Value
IP Address	40.0.0.2
Subnet Mask	255.0.0.0
Default Gateway	40.0.0.1
DNS Server	0.0.0.0

Below the IP Configuration section is the 'IPv6 Configuration' section, which has three radio buttons: 'DHCP' (unselected), 'Auto Config' (unselected), and 'Static' (selected). The Static configuration fields are empty.

At the bottom of the window is the '802.1X' section, which has a checkbox for 'Use 802.1X Security' (unchecked). Below this are fields for 'Authentication' (set to 'MD5'), 'Username', and 'Password'.

The Basic connectivity must be verified by using the ping command:



```
PC0
Physical Config Desktop Programming Attributes

Command Prompt

C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Request timed out.
Reply from 10.0.0.2: bytes=32 time=10ms TTL=125
Reply from 10.0.0.2: bytes=32 time=3ms TTL=125
Reply from 10.0.0.2: bytes=32 time=10ms TTL=125

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 10ms, Average = 7ms

C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=4ms TTL=125
Reply from 10.0.0.2: bytes=32 time=2ms TTL=125
Reply from 10.0.0.2: bytes=32 time=3ms TTL=125
Reply from 10.0.0.2: bytes=32 time=2ms TTL=125

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 2ms

C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=3ms TTL=125
Reply from 10.0.0.2: bytes=32 time=3ms TTL=125
Reply from 10.0.0.2: bytes=32 time=3ms TTL=125
Reply from 10.0.0.2: bytes=32 time=3ms TTL=125

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

Setting the SSH on Router 1 using the following commands in the CLI mode

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#username smile secret 1234

Router(config)#aaa new-model

Router(config)#aaa authentication login default local

Router(config)#ip domain-name smile.com

Router(config)#hostname smile

smile(config)#crypto key generate rsa

The name for the keys will be: smile.smile.com

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

\*Mar 1 0:30:13.877: %SSH-5-ENABLED: SSH 1.99 has been enabled

smile(config)#aaa authentication login smile local

smile(config)#line vty 0 4

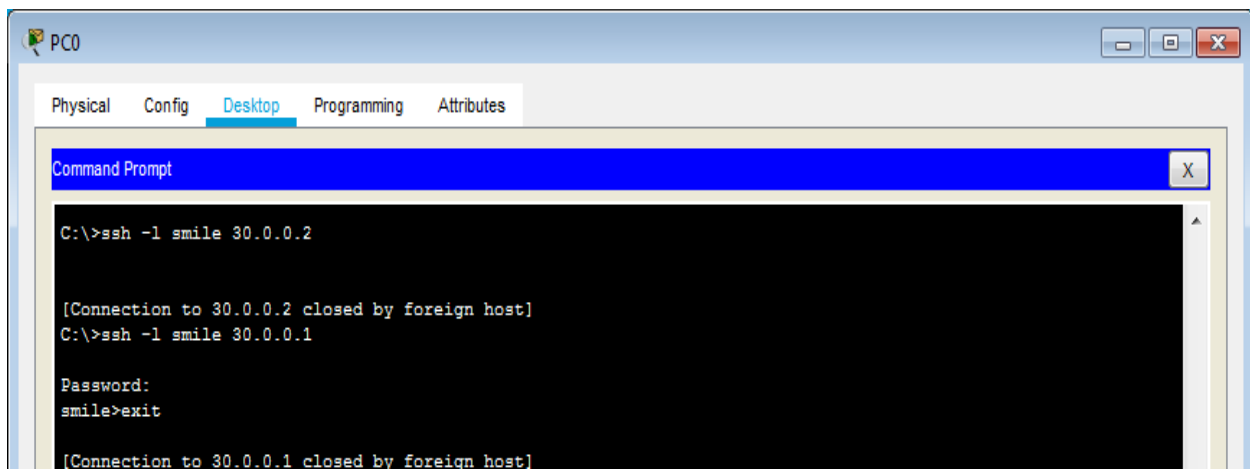
smile(config-line)#login authentication smile

smile(config-line)#transport input ssh

smile(config-line)#end

smile#

Now verifying the same using the following commands on the PC



Checking the connectivity from Pc to Server by opening the Web Browser



## Creating the FIREWALL ZONES ON Router2

**Enabling the Security technology package on the Router2 using the following command**

```
Router#
Router#conf
Router#configure ter
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#zone sec
Router(config)#zone security SMILE-ZONE
Router(config-sec-zone)#EXIT
Router(config)#
Router(config)#zone
Router(config)#zone se
Router(config)#zone security OUT-ZONE
Router(config-sec-zone)#EXIT
Router(config-sec-zone)#exit
Router(config)#
Router(config)#ac
Router(config)#access-list 101 permit 40.0.0.2 0.255.255.255 any
^
% Invalid input detected at '^' marker.
Router(config)#access-list 101 permit ip 40.0.0.2 0.255.255.255 any
Router(config)#class
Router(config)#class-map type
Router(config)#class-map type inspect match
Router(config)#class-map type inspect match-all IN-
Router(config)#class-map type inspect match-all IN-NET-
Router(config)#class-map type inspect match-all IN-NET-CLASS-MAP
Router(config-cmap)#
Router(config-cmap)#mat
Router(config-cmap)#match ac
Router(config-cmap)#match access-group 101
Router(config-cmap)#exit
Router(config)#pol
Router(config)#policy-map type in
Router(config)#policy-map type inspect IN-2
Router(config)#policy-map type inspect IN-2-OUT-PMAP
Router(config-pmap)#cl
Router(config-pmap)#class t
Router(config-pmap)#class type in
```

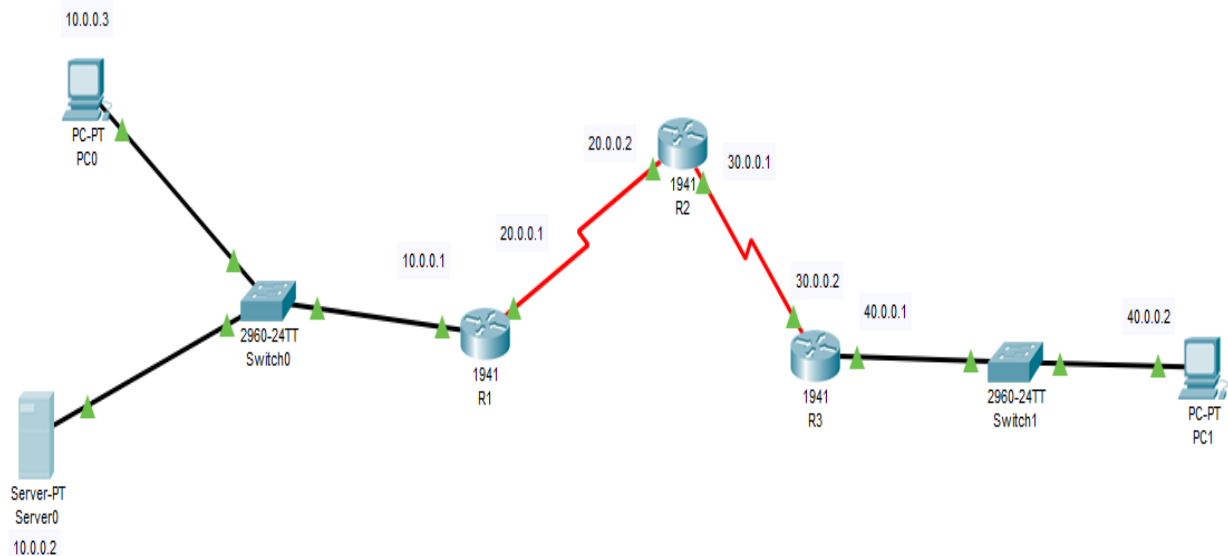
```
Router(config-pmap)#class type inspect IN-NET-CLASS-MAP
Router(config-pmap-c)#in
Router(config-pmap-c)#inspect
%No specific protocol configured in class IN-NET-CLASS-MAP for inspection. All protocols
will be inspected
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#
Router(config)#zone-pair security IN-2-OUT-ZPAIR
Router(config)#zone-pair security IN-2-OUT-ZPAIR ?
source Source zone
Router(config)#zone-pair security IN-2-OUT-ZPAIR SMILE-ZONE OUT-ZONE
^
% Invalid input detected at '^' marker.
Router(config)#zone-pair security IN-2-OUT-ZPAIR 40.0.0.1 30.0.0.2
^
% Invalid input detected at '^' marker.
Router(config)#zone-pair security IN-2-OUT-ZPAIR 40.0.0.1 SMILE-ZONE 30.0.0.2 OUT-
ZONE
^
% Invalid input detected at '^' marker.
Router(config)#zone-pair security IN-2-OUT-ZPAIR ?
source Source zone
Router(config)#zone-pair security IN-2-OUT-ZPAIR so
Router(config)#zone-pair security IN-2-OUT-ZPAIR source SMILE-ZONE de
Router(config)#zone-pair security IN-2-OUT-ZPAIR source SMILE-ZONE destination OUT-
ZONE
Router(config-sec-zone-pair)#ser
Router(config-sec-zone-pair)#service-policy type in
Router(config-sec-zone-pair)#service-policy type inspect IN
Router(config-sec-zone-pair)#service-policy type inspect IN-2-OUT-PMAP
Router(config-sec-zone-pair)#exit
Router(config)#
Router(config)#interface Serial0/1/1
Router(config-if)#zone
Router(config-if)#zone-member sec
Router(config-if)#zone-member security
Router(config-if)#zone-member security SMILE-ZONE
Router(config-if)#EXIT
Router(config)#
Router(config)#interface Serial0/1/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ZONE
Router(config-if)#
```

```
Router(config-if)#zone
Router(config-if)#zone-member se
Router(config-if)#zone-member security OUT-ZONE
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#exitt
^
% Invalid input detected at '^' marker.
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Router#copy
Router#copy ru
Router#copy running-config star
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

## Practical 7: Configure IOS Intrusion Prevention System (IPS) Using the CLI

Consider the following topology



Configure the PCs, Routers and the Server with the following addresses

PC0	10.0.0.3
SERVER	10.0.0.2
R1 G0/0	10.0.0.1
S0/1/0	20.0.0.1
R2 S0/1/0	20.0.0.2
S0/1/1	30.0.0.1
R3 S0/1/1	30.0.0.2
G0/0	40.0.0.1
PC1	40.0.0.2

Use RIP routing protocol and add the networks in the Routers as follows

R1	10.0.0.0	20.0.0.0
R2	20.0.0.0	30.0.0.0
R3	30.0.0.0.	40.0.0.0

Configure Server as the SYSLOG server

Ping the PC0 to PC1 and PC1 to PC0 and verify the connectivity

Type the following commands in R1

```
R1(config)# license boot module c1900 technology-package securityk9
```

Enable the security package and reload the router

```
R1(config)#exit
```

```
R1#write
```

```
R1#reload
```

```
R1# mkdir ipsdir
```

```
R1(config)# ip ips config location flash:ipsdir
```

```
R1(config)# ip ips name iosips
```

```
R1(config)# ip ips notify log
```

```
R1#set clock 11:12:23 5 APR 2019
```

```
R1#Show clock
```

```
R1(config)# service timestamps log datetime msec
```

```
R1(config)#logging host 10.0.0.2
```

```
R1(config)# ip ips signaturecategory
```

```
R1(config-ips-category)# category all
```

```
R1(config-ips-category-action)# retired true
```

```
R1(config-ips-category-action)# exit
```

```
R1(config-ips-category)# category ios_ips basic
```

```
R1(config-ips-category-action)# retired false
```

```
R1(config-ips-category-action)# exit
```

```
R1(config-ips-cateogry)# exit
```

```
Do you want to accept these changes? [confirm] <Enter>
```

```
R1(config)# interface g0/0
```

```
R1(config-if)# ip ips iosips out
```

```
R1(config)# ip ips signature-definition
```

```
R1(config-sigdef)# signature 2004 0
```

```
R1(config-sigdef-sig)# status
```

```
R1(config-sigdef-sig-status)# retired false
```

```
R1(config-sigdef-sig-status)# enabled true
```

```
R1(config-sigdef-sig-status)# exit
```

```
R1(config-sigdef-sig)# engine
```

```
R1(config-sigdef-sig-engine)# event-action produce-alert
```

```
R1(config-sigdefsig-engine)# event-action deny-packet-inline
```

```
R1(config-sigdef-sig-engine)# exit
```

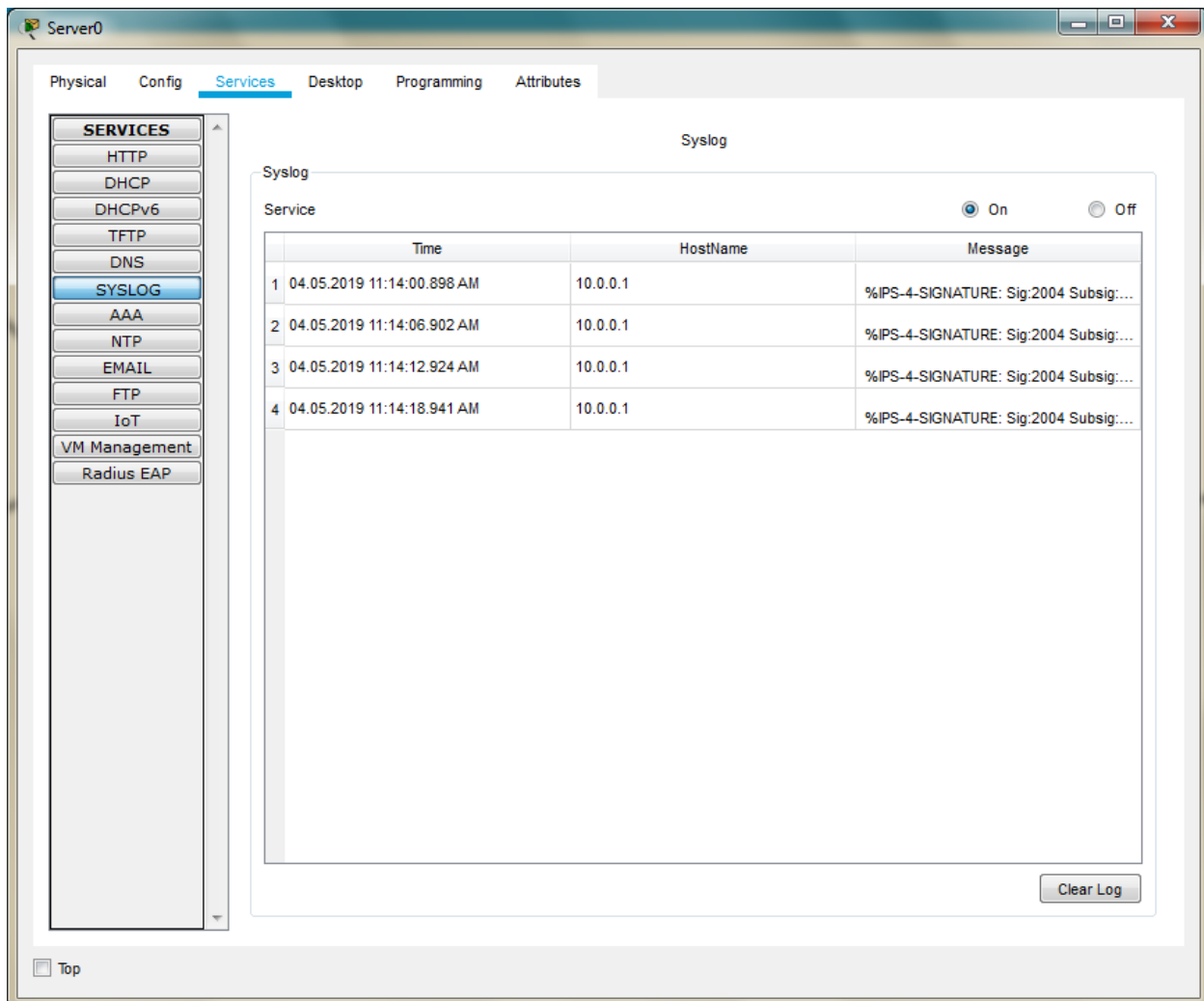
```
R1(config-sigdef-sig)# exit
```

```
R1(config-sigdef)# exit
```

```
Do you want to accept these changes? [confirm] <Enter>
```



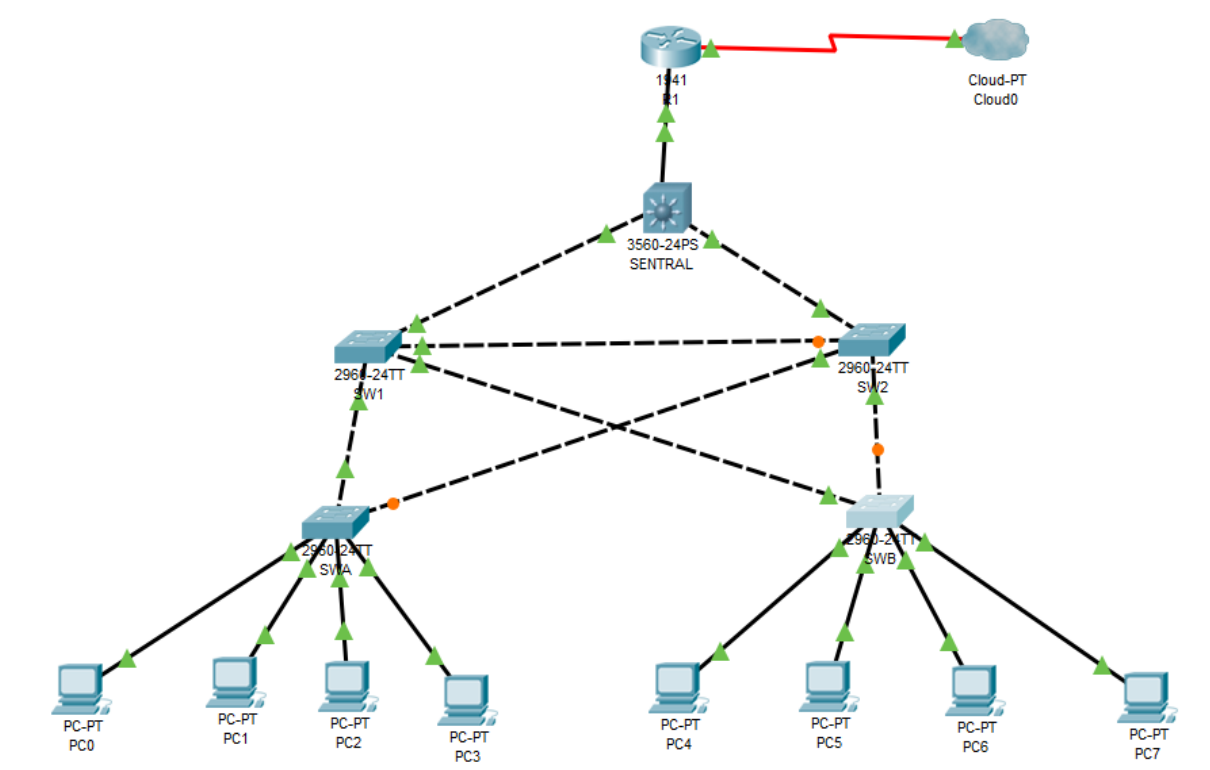
Now ping PC1 from PC0 and PC0 from PC1 and observe the output at the SYSLOG services of the Server



Only one ping is successful while the other fails

## Practical 8: Packet Tracer – Layer 2 Security

Consider the following topology



### Configure the Root Bridge

Type the following command in the CLI mode of CENTRAL switch

```
CENTRAL(config)#SPAnning-tree vlan 1 root primary
CENTRAL(config)#exit
```

Type the following command in the CLI mode of SW1 switch

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW1
SW1(config)#spanning-tree vlan 1 root secondary
```

Verify the spanning-tree configuration by using the following commands in the CENTRAL switch

```
CENTRAL#show spanning-tree
```

The following output is obtained  
VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 24577

Address 00E0.8F81.9573

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 24577 (priority 24576 sys-id-ext 1)

Address 00E0.8F81.9573

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

-----

Fa0/1 Desg FWD 19 128.1 P2p

Gi0/1 Desg FWD 4 128.25 P2p

Gi0/2 Desg FWD 4 128.26 P2p

## Protect against STP attacks

Type the following commands in the CLI modes of the Switches SWA and SWB

### Enable portfast on all access ports

```
Switch>enable
```

```
Switch#configure terminal
```

```
Switch(config)#hostname SWA
```

```
SWA(config)#interface range f0/1-4
```

```
SWA(config-if-range)#spanning-tree portfast
```

```
Switch>enable
```

```
Switch#configure terminal
```

```
Switch(config)#hostname SWB
```

```
SWB(config)#interface range f0/1-4
```

```
SWB(config-if-range)#spanning-tree portfast
```

### Enable BPDU guard on all access points

```
SWA(config-if-range)#spanning-tree bpduguard enable
```

```
SWA(config-if-range)#exit
```

```
SWB(config-if-range)#spanning-tree bpduguard enable
SWB(config-if-range)#exit
```

**Enable root guard**

```
SW1(config)#interface range f0/23-24
SW1(config-if-range)#spanning-tree guard root
```

```
SW2(config)#interface range f0/23-24
SW2(config-if-range)#spanning-tree guard root
```

## Configure Port Security and Disable Unused Ports

```
SWA(config-if-range)#exit
SWA(config)#interface range f0/1-22
SWA(config-if-range)#switchport port-security maximum 2
SWA(config-if-range)#switchport port-security violation shutdown
SWA(config-if-range)#switchport port-security mac-address sticky
```

```
SWB(config-if-range)#exit
SWB(config)#interface range f0/1-22
SWB(config-if-range)#switchport port-security maximum 2
SWB(config-if-range)#switchport port-security violation shutdown
SWB(config-if-range)#switchport port-security mac-address sticky
```

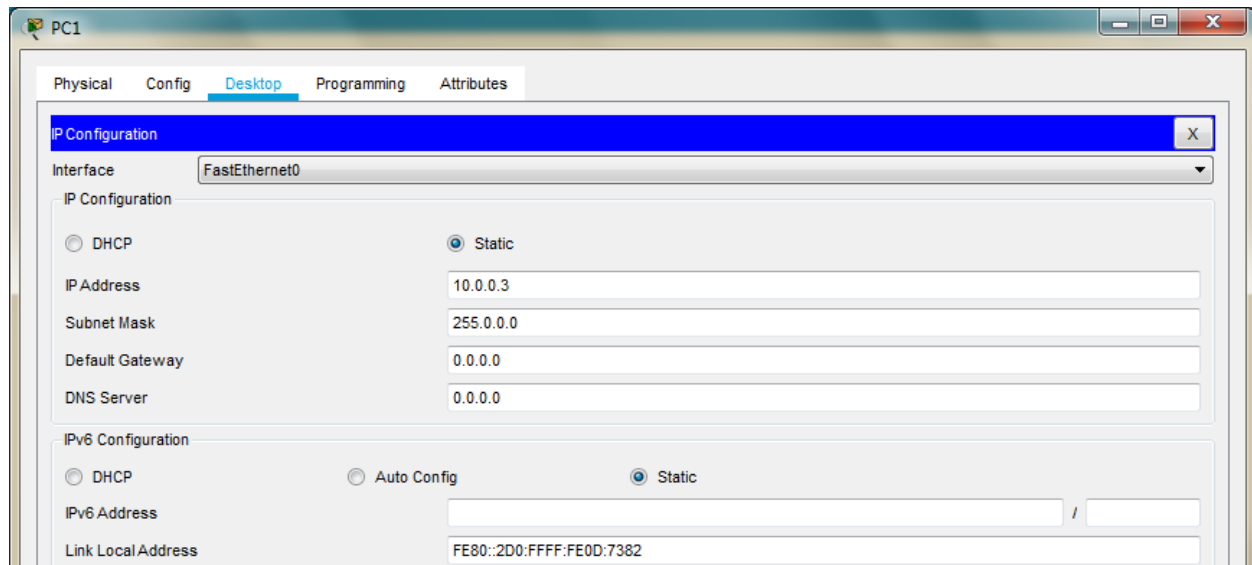
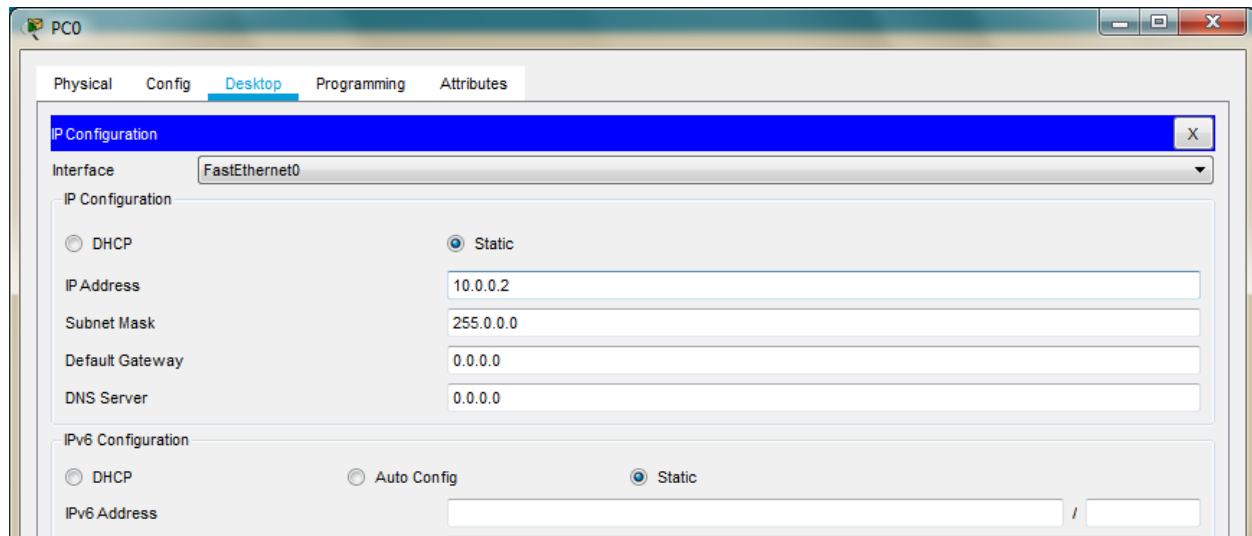
**Verify Port Security (type the commands in SWA) and observe the output**

```
SWA#show port-security interface f0/1
```

**We get the following output**

```
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 2
Total MAC Addresses : 0
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

Now we configure the PCs and Give assign IP address to any two PCs



Now we ping one of the PC from the other and then type the following command in SWA

SWA#show port-security interface f0/1

We get the following output

SWA#show port-security interface f0/1

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 2

Total MAC Addresses : 1

Configured MAC Addresses : 0

Sticky MAC Addresses : 1

**Last Source Address:Vlan : 0001.6406.2AAE:1**

Security Violation Count : 0

**Finally we disable the unused ports**

SWA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SWA(config)#interface range f0/5-22

SWA(config-if-range)#shutdown

SWB#configure terminal

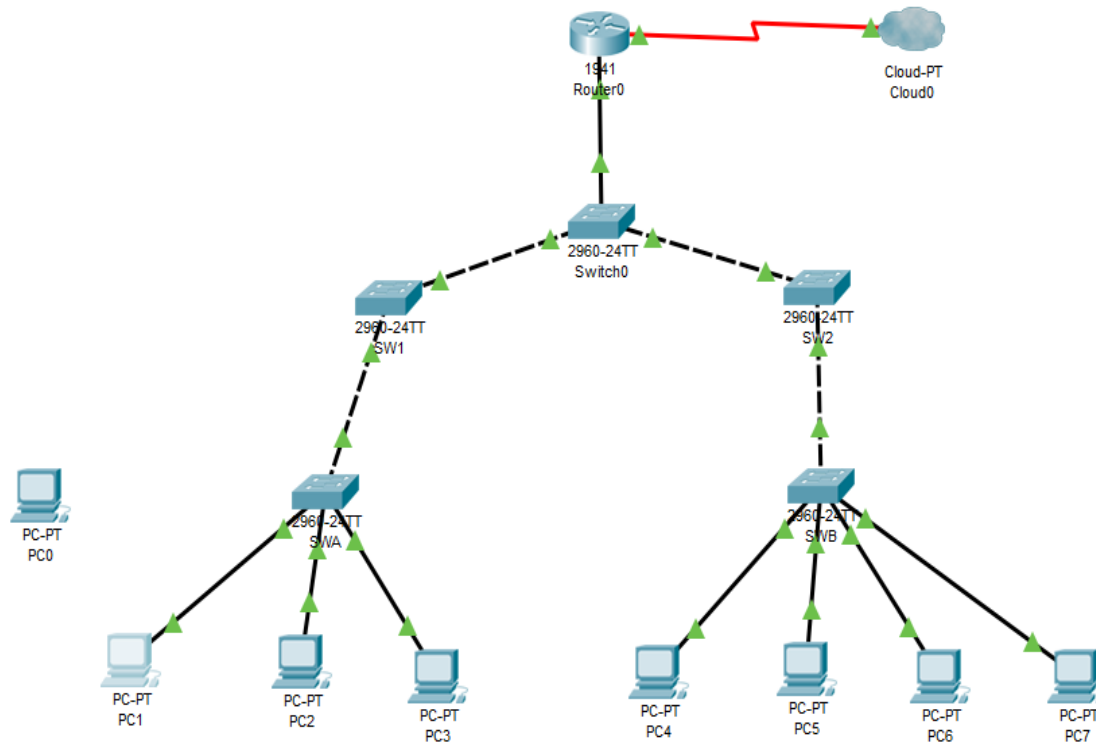
Enter configuration commands, one per line. End with CNTL/Z.

SWB(config)#interface range f0/5-22

SWB(config-if-range)#shutdown

## Practical 9: Layer 2 VLAN Security

We use the following topology

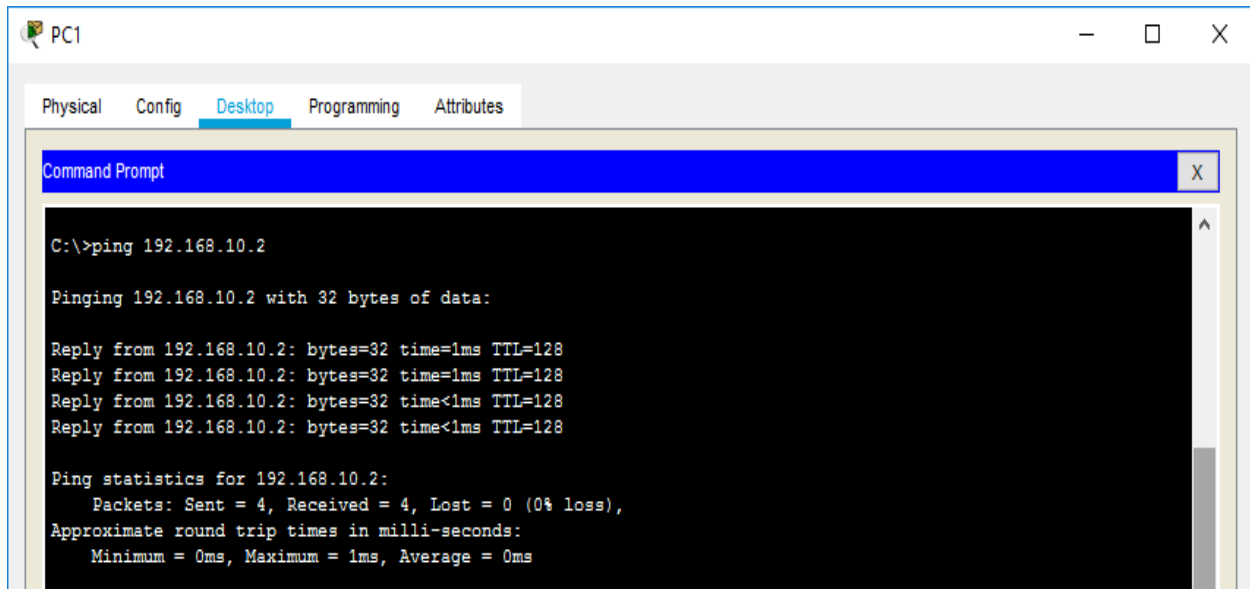


Assign IP addresses to the PCs

PC1	192.168.10.1
PC2	192.168.10.2
PC3	192.168.10.3
PC4	192.168.10.4
PC5	192.168.10.5
PC6	192.168.10.6
PC7	192.168.10.7
PC8	192.168.10.10

## VERIFY CONNECTIVITY

We Ping the PC2 from PC1



The screenshot shows a Packet Tracer PC1 window with the 'Desktop' tab selected. A Command Prompt window is open, displaying the results of a ping command to 192.168.10.2. The output shows four successful replies with 32 bytes of data, a time of 1ms, and a TTL of 128. The ping statistics indicate that all four packets were sent and received with 0% loss.

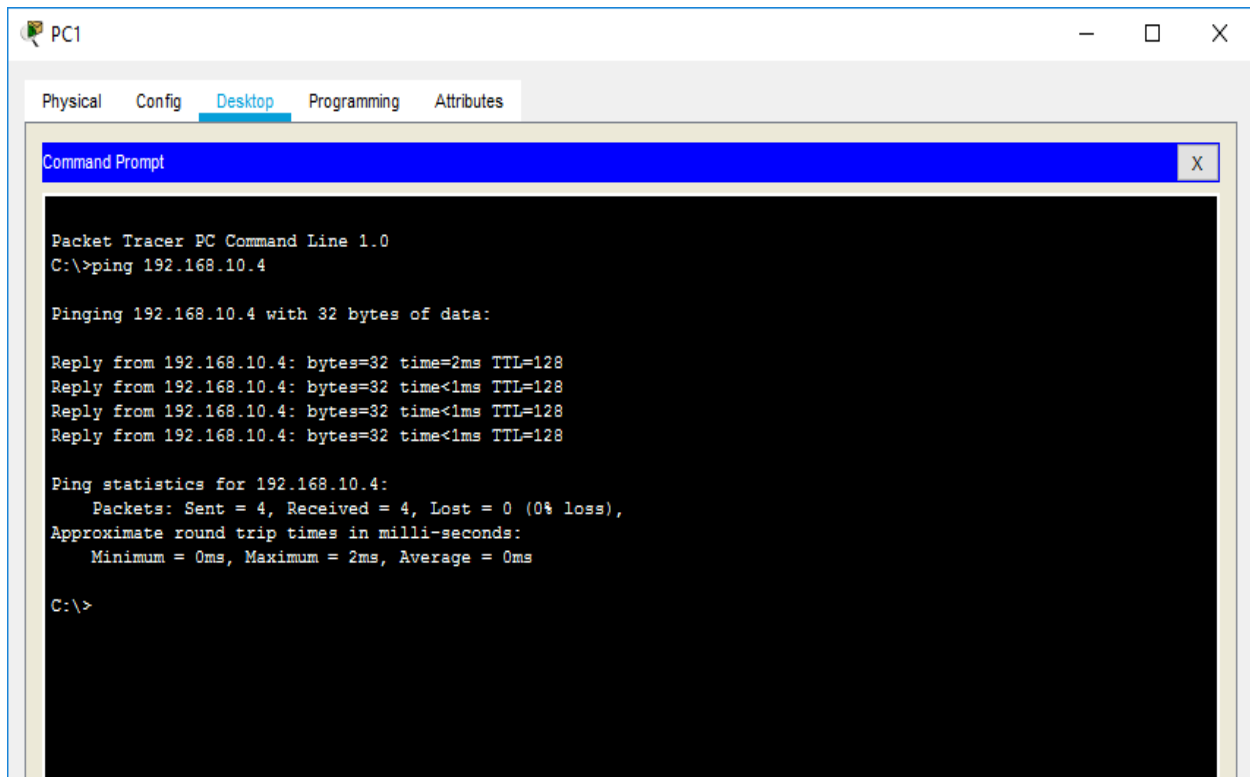
```
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=1ms TTL=128
Reply from 192.168.10.2: bytes=32 time=1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

We Ping the PC4 from PC1



The screenshot shows a Packet Tracer PC1 window with the 'Desktop' tab selected. A Command Prompt window is open, displaying the results of a ping command to 192.168.10.4. The output shows four successful replies with 32 bytes of data, a time of 2ms, and a TTL of 128. The ping statistics indicate that all four packets were sent and received with 0% loss.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.4

Pinging 192.168.10.4 with 32 bytes of data:

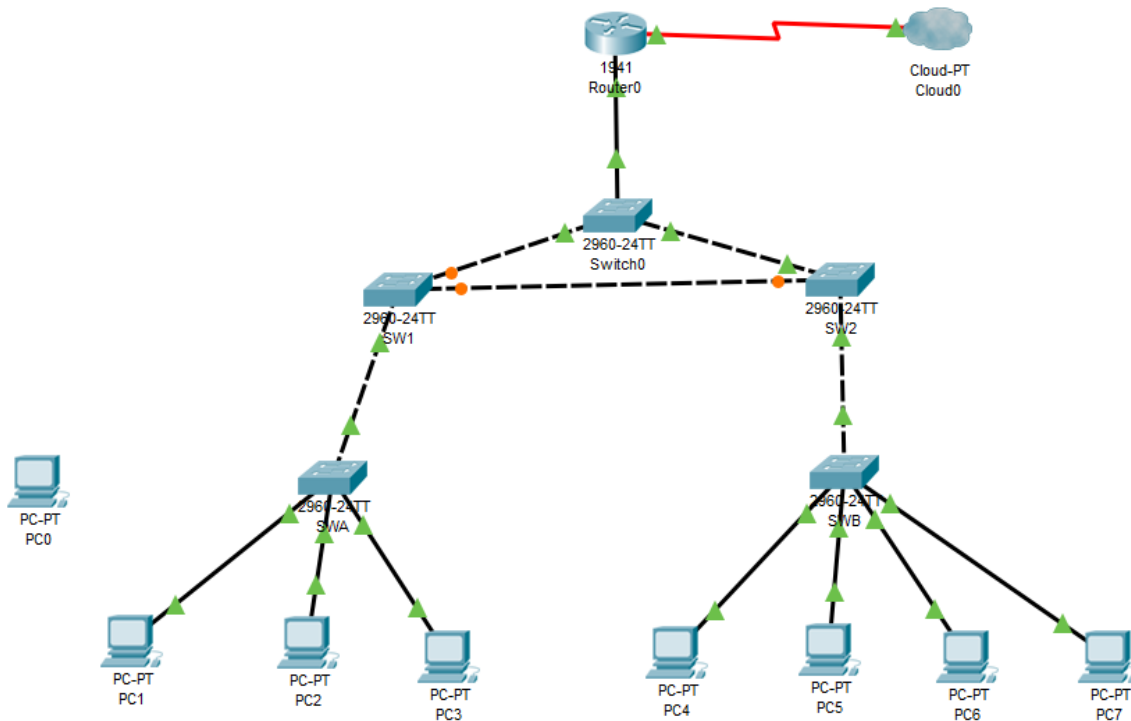
Reply from 192.168.10.4: bytes=32 time=2ms TTL=128
Reply from 192.168.10.4: bytes=32 time<1ms TTL=128
Reply from 192.168.10.4: bytes=32 time<1ms TTL=128
Reply from 192.168.10.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>
```



CREATE A REDUNDANT LINK BETWEEN SW1 and SW2 (f0/23 and f0/23)



**Enable trunking, including all trunk security mechanisms on the link between SW-1 and SW-2.**

Type the following commands in the CLI mode of SW1 and SW2

```
SW1(config)#interface f0/23
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk native vlan 15
SW1(config-if)#switchport nonegotiate
SW1(config-if)#no shutdown
```

```
SW2(config)#interface f0/23
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport trunk native vlan 15
SW2(config-if)#switchport nonegotiate
SW2(config-if)#no shutdown
```

**Enable VLAN 20 as a Management VLAN**

```
SWA>
SWA>enable
SWA#conf
SWA#configure ter
SWA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWA(config)#vlan 20
SWA(config-vlan)#exit
SWA(config-if)#ip address 192.168.20.1 255.255.255.0
SWA(config-if)#
```

```
SWB>enable
SWB#configure terminal
SWB(config)#vlan 20
SWB(config-vlan)#exit
SWB(config)#interface vlan 20
SWB(config-if)#ip address 192.168.20.2 255.255.255.0
```

```
SW1(config)#vlan 20
SW1(config-vlan)#exit
SW1(config)#interface vlan 20
SW1(config-if)#ip address 192.168.20.3 255.255.255.0
```

```
SW2(config)#vlan 20
SW2(config-vlan)#exit
SW2(config)#interface vlan 20
SW2(config-if)#ip address 192.168.20.4 255.255.255.0
```

```
Switch>
Switch>enable
Switch#configure terminal
Switch(config)#interface vlan 20
Switch(config-if)#ip address 192.168.20.5 255.255.255.0
```

**Connect and configure the management PC.**

Connect the management PC to **SW-A** port F0/5 and ensure that it is assigned an available IP address within the 192.168.10.10

Type the following commands in the Router  
Router>

```
Router>en
Router>enable
Router#confi
Router#configure ter
Router#configure terminal
Router(config)#interface g0/0.3
Router(config-subif)#
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#exit
Router(config)#interface g0/0.3
Router(config-subif)#ip address 192.168.20.100 255.255.255.0
Router(config-subif)#exit
Router(config)#
```

### **Enable security**

```
R1(config)# access-list 101 deny ip any 192.168.20.0 0.0.0.255 R1(config)# access-list 101  
permit ip any any  
R1(config)# access-list 102 permit ip host 192.168.20.50 any
```

```
R1(config)# interface g0/0.1  
R1(config-subif)# ip access-group 101 in  
R1(config-subif)# interface g0/0.2  
R1(config-subif)# ip access-group 101 in  
R1(config-subif)# line vty 0 4  
R1(config-line)# access-class 102 in
```

```
R1(config-line)# exit  
R1(config)#ip domain-name smile.com  
R1(config)#crypto key generate rsa  
The name for the keys will be:R1.smile.com  
Choose the size of the key modulus in the range of 360 to 2048 for your  
General Purpose Keys. Choosing a key modulus greater than 512 may take  
a few minutes.
```

How many bits in the modulus [512]: 1024  
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

```
R1(config)#aaa authentication login ssh-admin local  
R1(config)#line vty 0 4  
R1(config-line)#login authentication ssh-admin  
R1(config-line)#transport input ssh  
R1(config-line)#end
```

**Verify security.**

Verify only the Management PC can access the router. Use SSH to access R1 with username SSHAdmin

No password set

PC> ssh -l SSHAdmin 192.168.20.100

