VIKAS VIDYA EDUCATION TRUST'S

Lords Universal College

Department of Information Technology

Practical Journal

Of

USIT-602 : Information Security

Name :

Roll No :

Class : TYBSc.IT

Semester : VI

VIKAS VIDYA EDUCATION TRUST'S

Lords Universal College

Department of Information Technology

CERTIFICATE

Class: TYBSc.IT **Year:** 2024-2025

This is to certify that the work entered in this Journal is the work of

Shree / Kumari _____

Of TYBSc.IT Roll no:_____

University Exam No: _____ has satisfactorily completed the required number of practical and worked for the 5th term the term of the year 2024 2025 in the college laboratory as laid down by the university.

Head of the Department	**External Examiner**	**Internal Examiner**

Date: / / 20 **Department of Bsc.IT**

INDEX

Sr No.	Name	Date	Sign
1	**Configure Routers:** a. OSPF MD5 authentication. b. NTP. c. to log messages to the syslog server		
2	**Configure AAA Authentication** **a.** Configure a local user account on Router and configure authenticate on the console and vty lines using local AAA **b.** Verify local AAA authentication from the Router console and the PC-A client		
3	**Configuring Extended ACLs** **a.** Configure, Apply and Verify an Extended Numbered ACL		
4	**Configure IP ACLs to Mitigate Attacks and IPV6 ACLs** **a.** Verify connectivity among devices before firewall configuration. **b.** Use ACLs to ensure remote access to the routers is available only from management station PC-C. **c.** Configure ACLs on to mitigate attacks. **d.** Configuring IPv6 ACLs		

5	**Configuring a Zone-Based Policy Firewall**		
6	**Configure IOS Intrusion Prevention System (IPS) Using the CLI** a. Enable IOS IPS. b. Modify an IPS signature.		
7	**Layer 2 Security** a. Assign the Central switch as the root bridge. b. Secure spanning-tree parameters to prevent STP manipulation attacks. c. Enable port security to prevent CAM table overflow attacks.		
8	**Layer 2 VLAN Security**		
9	**Configure and Verify a Site-to-Site IPsec VPN Using CLI**		
10	**Configuring ASA Basic Settings and Firewall Using CLI** **a.** Configure basic ASA settings and interface security levels using CLI **b.** Configure routing, address translation, and inspection policy using CLI **c.** Configure DHCP, AAA, and SSH **d.** Configure a DMZ, Static NAT, and ACLs		

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 Djikstra'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

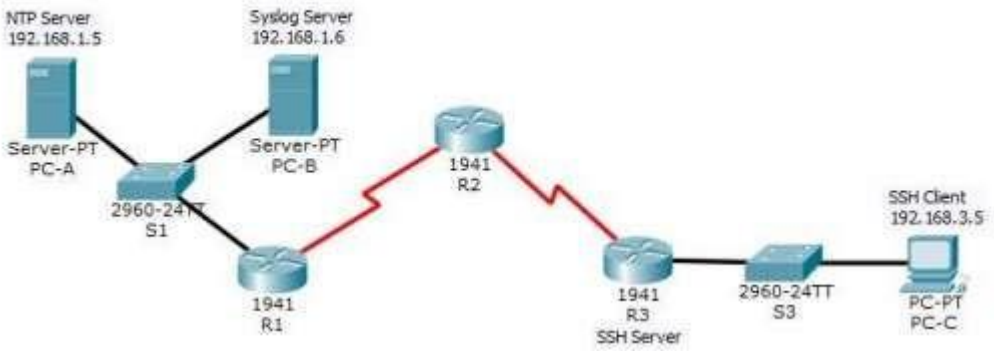
- MD5 authentication provides higher security than plain text authentication.
- This method uses the MD5 algorithm to compute a hash value from the contents of the OSPF packet and a password (or key).
- This hash value is transmitted in the packet, along with a key ID and a non-decreasing sequence number.
- 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

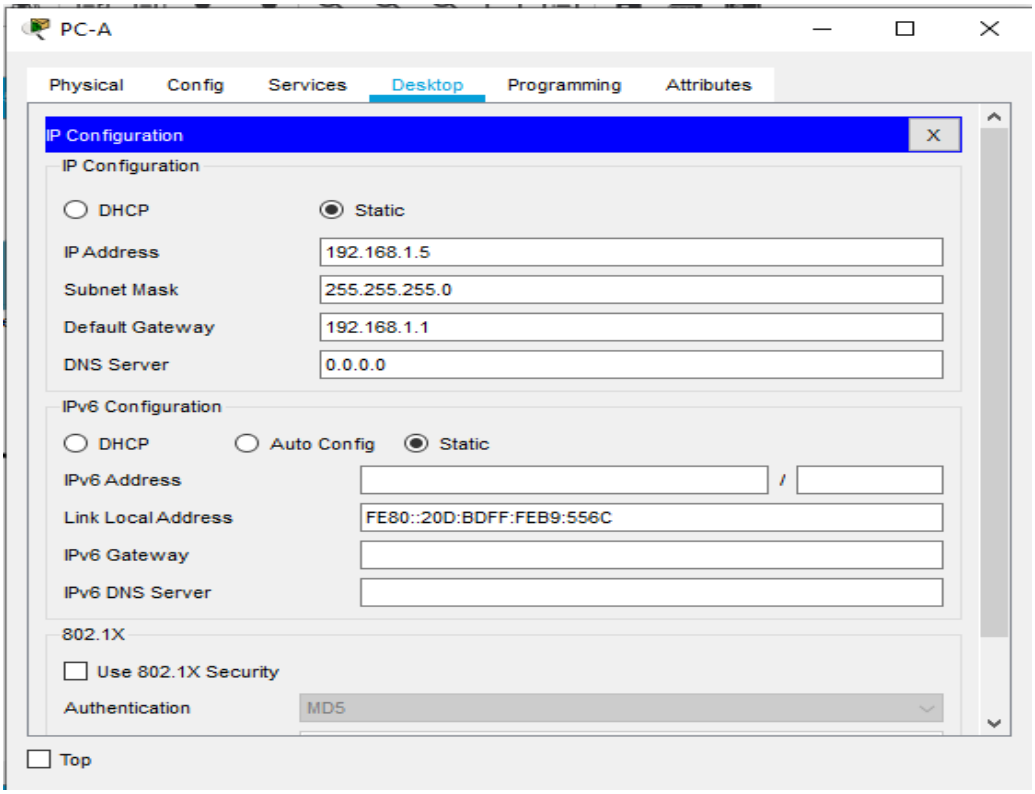
Topology



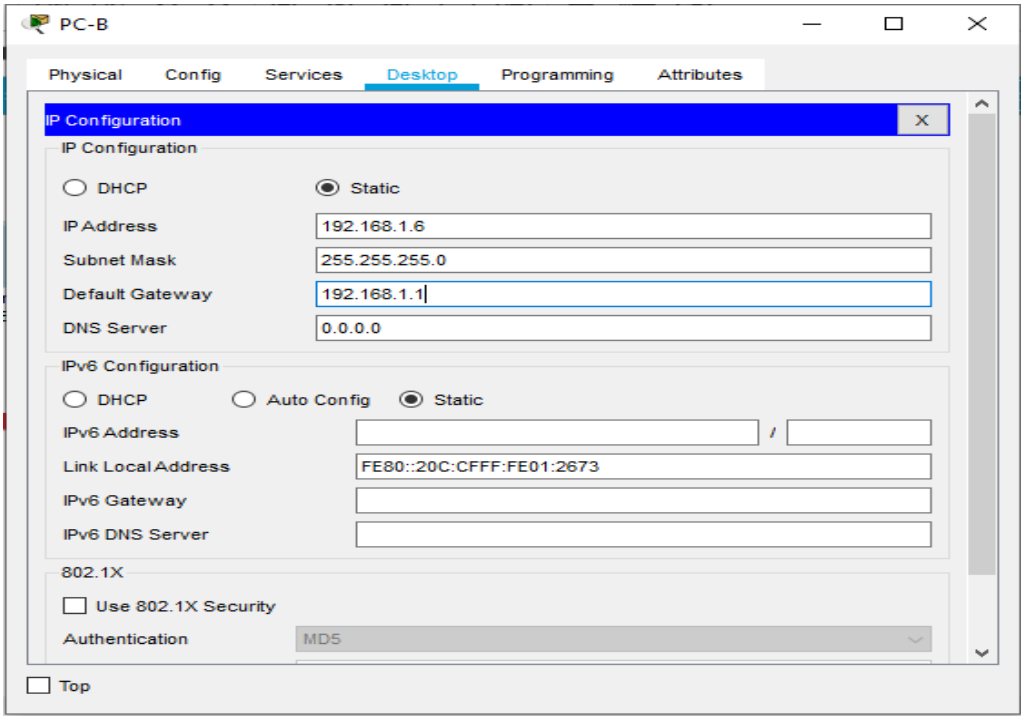
Addressing Table

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)	**100.2.2.2**	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	**100.2.2.1**	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.5	255.255.255.0	192.168.1.1	S1 F0/6
PC-B	NIC	192.168.1.6	255.255.255.0	192.168.1.1	**S1 F0/18**
PC-C	NIC	192.168.3.5	255.255.255.0	192.168.3.1	**S3 F0/18**

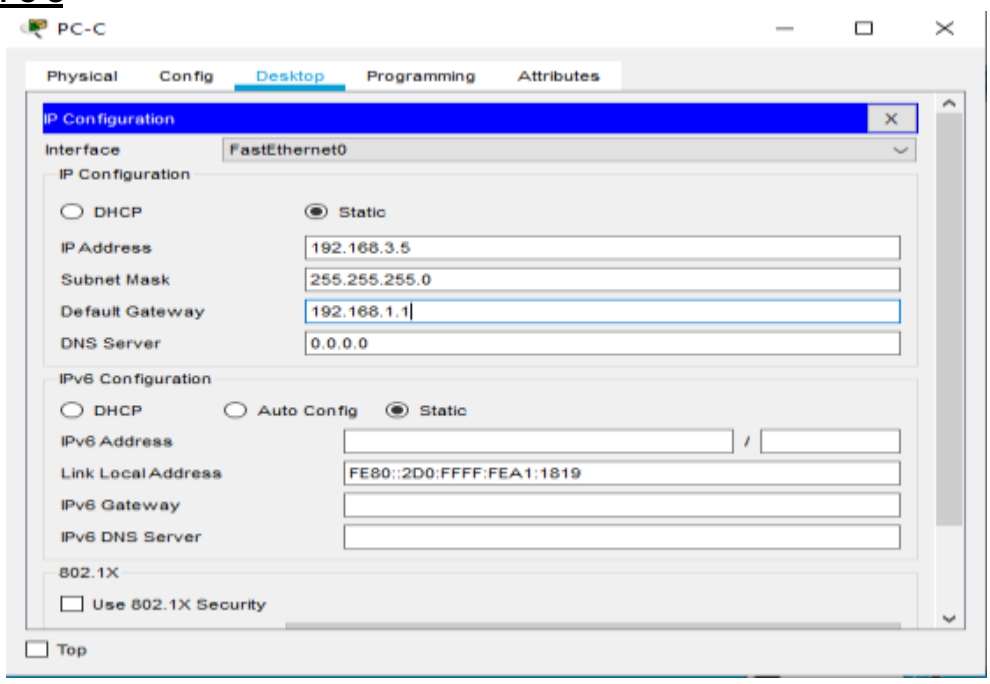
Configuring PC-A



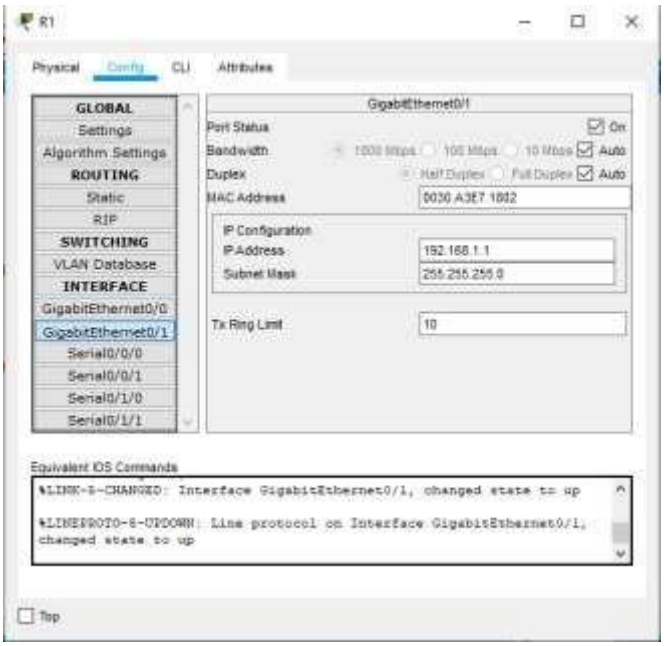
Configuring PC-B

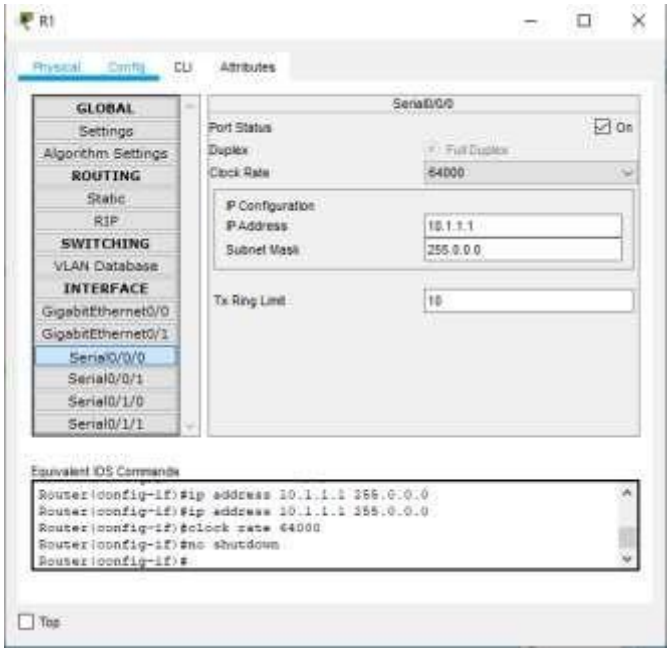


Configuring PC-C

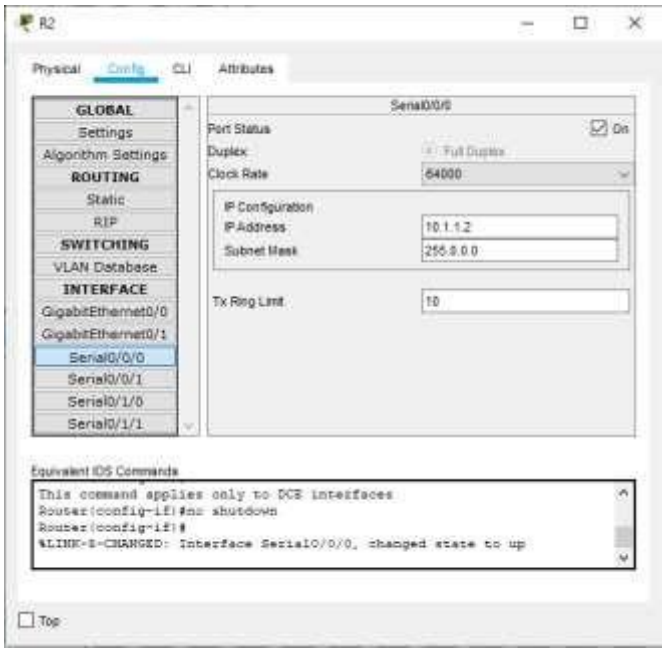


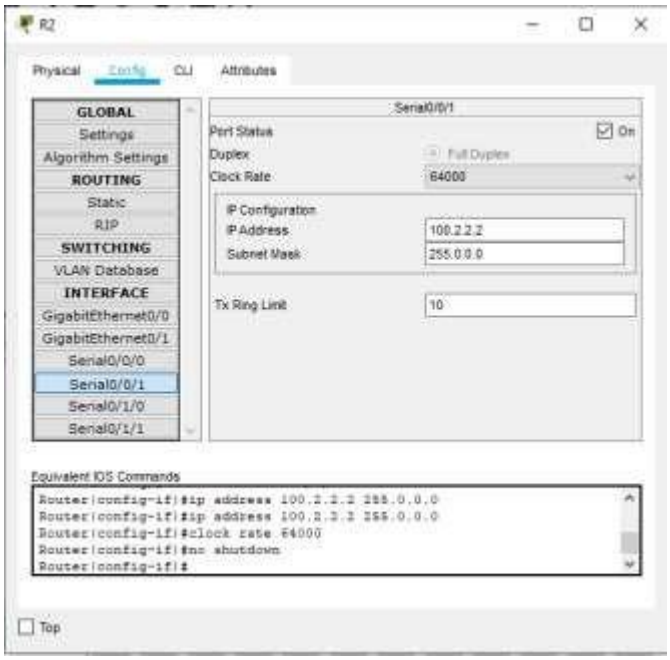
Configuring R1



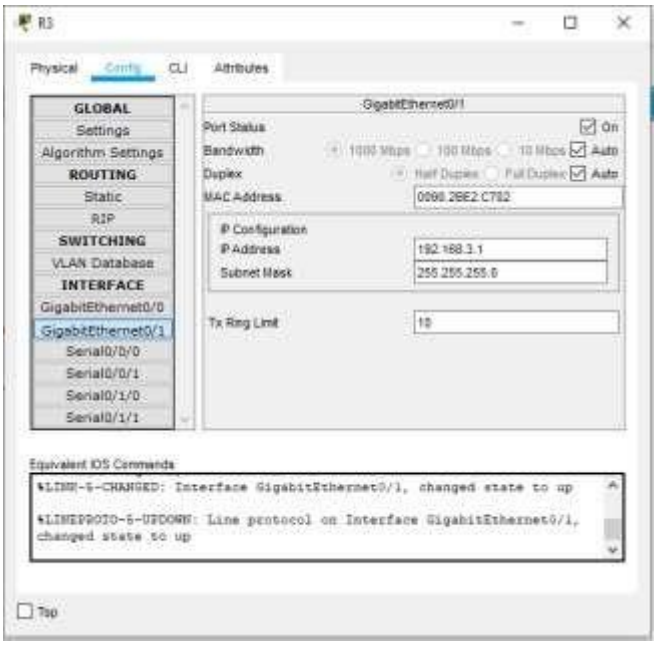


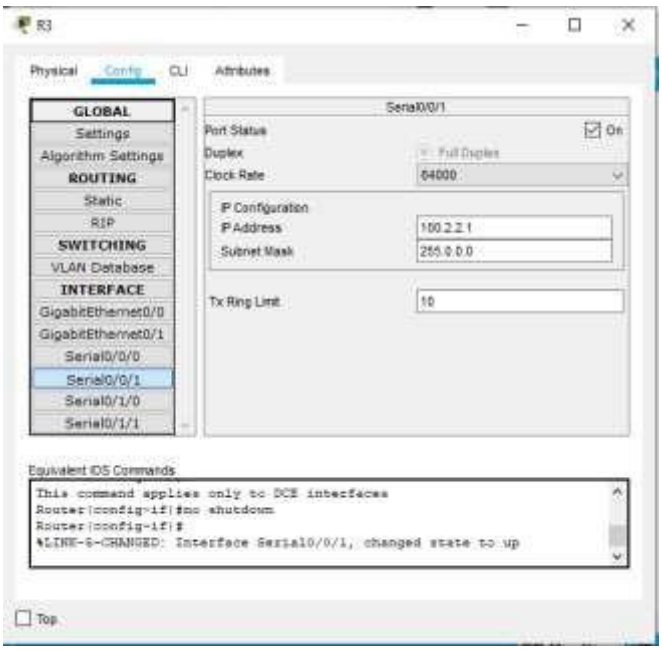
Configuring R2





Configuring R3





Part 1: Configure OSPF MD5 Authentication

ROUTER 1: Type the following command in the CLI mode

```
Router>enable
Router#configure terminal
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.255.255.255 area 1
Router(config-router)#network 10.1.1.0 0.255.255.255 area 1
Router(config-router)#exit
Router(config)#exit
Router#
```

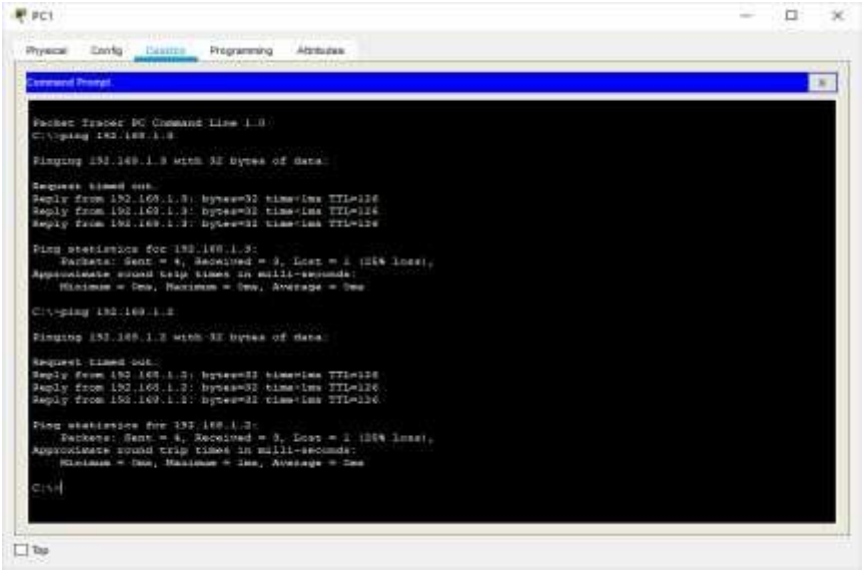
ROUTER 2: Type the following command in the CLI mode

```
Router>enable
Router#configure terminal
Router(config)#router ospf 1
Router(config-router)#network 10.1.1.0 0.255.255.255 area 1
Router(config-router)#network 100.2.2.0 0.255.255.255 area 1
Router(config-router)#exit
Router(config)#exit
Router#
```

ROUTER 3: Type the following command in the CLI mode

```
Router>enable
Router#configure terminal
Router(config)#router ospf 1
Router(config-router)#network 192.168.3.0 0.255.255.255 area 1
Router(config-router)#network 100.2.2.0 0.255.255.255 area 1
Router(config-router)#exit
Router(config)#exit
Router#
```

Now we verify the connectivity by using the following



Hence OSPF has been verified

MD5 Authentication

ROUTER 1: Type the following command in the CLI mode

Router>enable
Router#
Router#configure terminal
Router(config)#interface Serial0/0/0
Router(config-if)#ip ospf authentication message-digest
Router(config-if)#ip ospf message-digest-key 1 md5 smile
Router(config-if)#exit
Router(config)#exit

ROUTER 2: Type the following command in the CLI mode

Router>enable
Router#
Router#configure terminal
Router(config)#interface Serial0/0/0
Router(config-if)#ip ospf authentication message-digest
Router(config-if)#ip ospf message-digest-key 1 md5 smile
Router(config-if)#exit
Router(config)#exit

Verify the MD5 Authentication using the following command in the CLI mode of Router1

Router#show ip ospf interface gigabitEthernet 0/1

We get the following output:
GigabitEthernet0/1 is up, line protocol is up
Internet address is 192.168.2.1/24, Area 1
Process ID 1, Router ID 192.168.2.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 192.168.3.1, Interface address 192.168.2.2
Backup Designated Router (ID) 192.168.2.1, Interface address 192.168.2.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:06
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 1, Adjacent neighbor count is 1
Adjacent with neighbor 192.168.3.1 (Designated Router)
Suppress hello for 0 neighbor(s)

Message digest authentication enabled

Youngest key id is 1

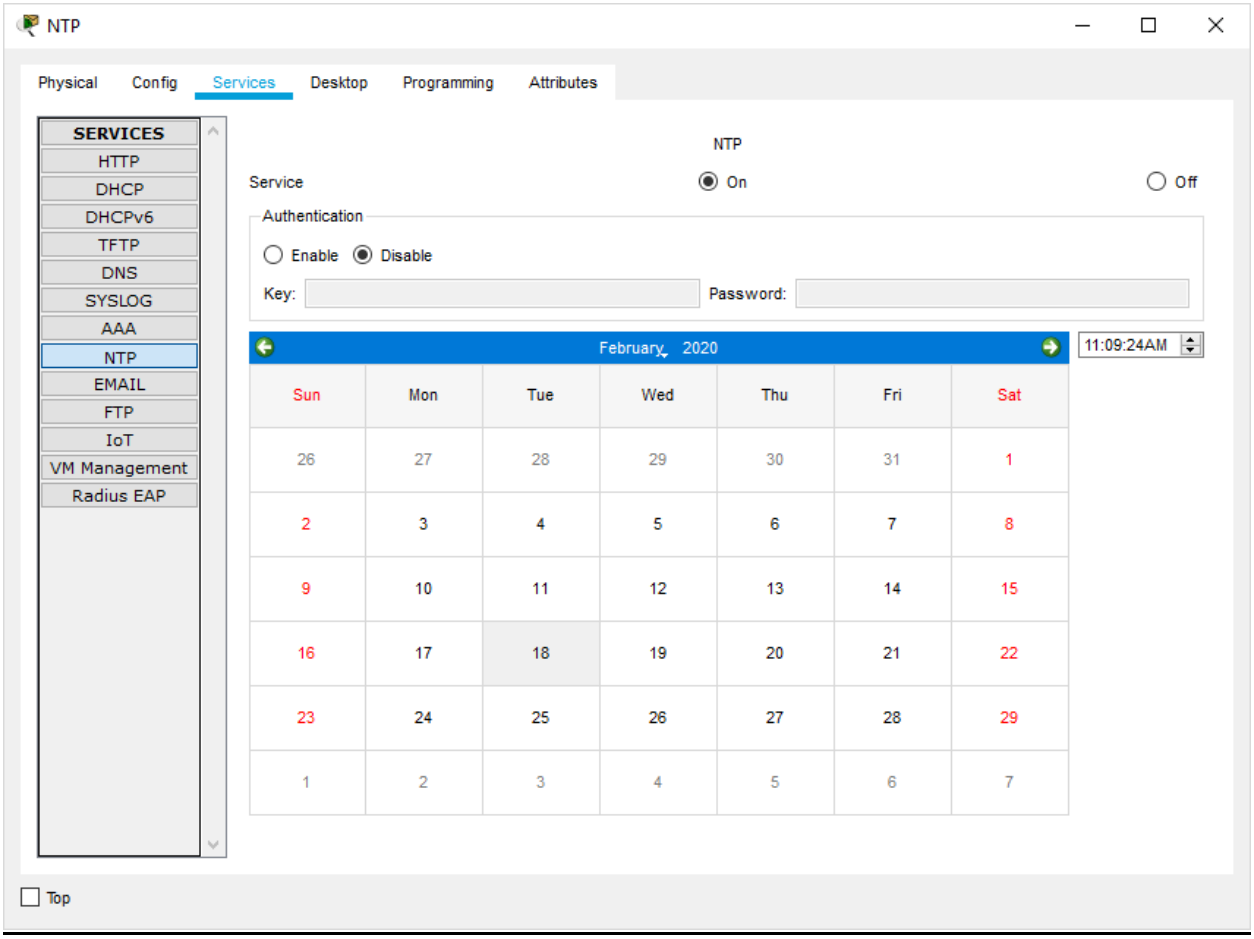
MD5 Authentication has been verified

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 Router1 and type the following commands on both the Routers

```
Router#enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ntp server 192.168.1.5
Router(config)#ntp update-calendar
Router(config)#exit
Router#
```

To verify the Output we use the following command

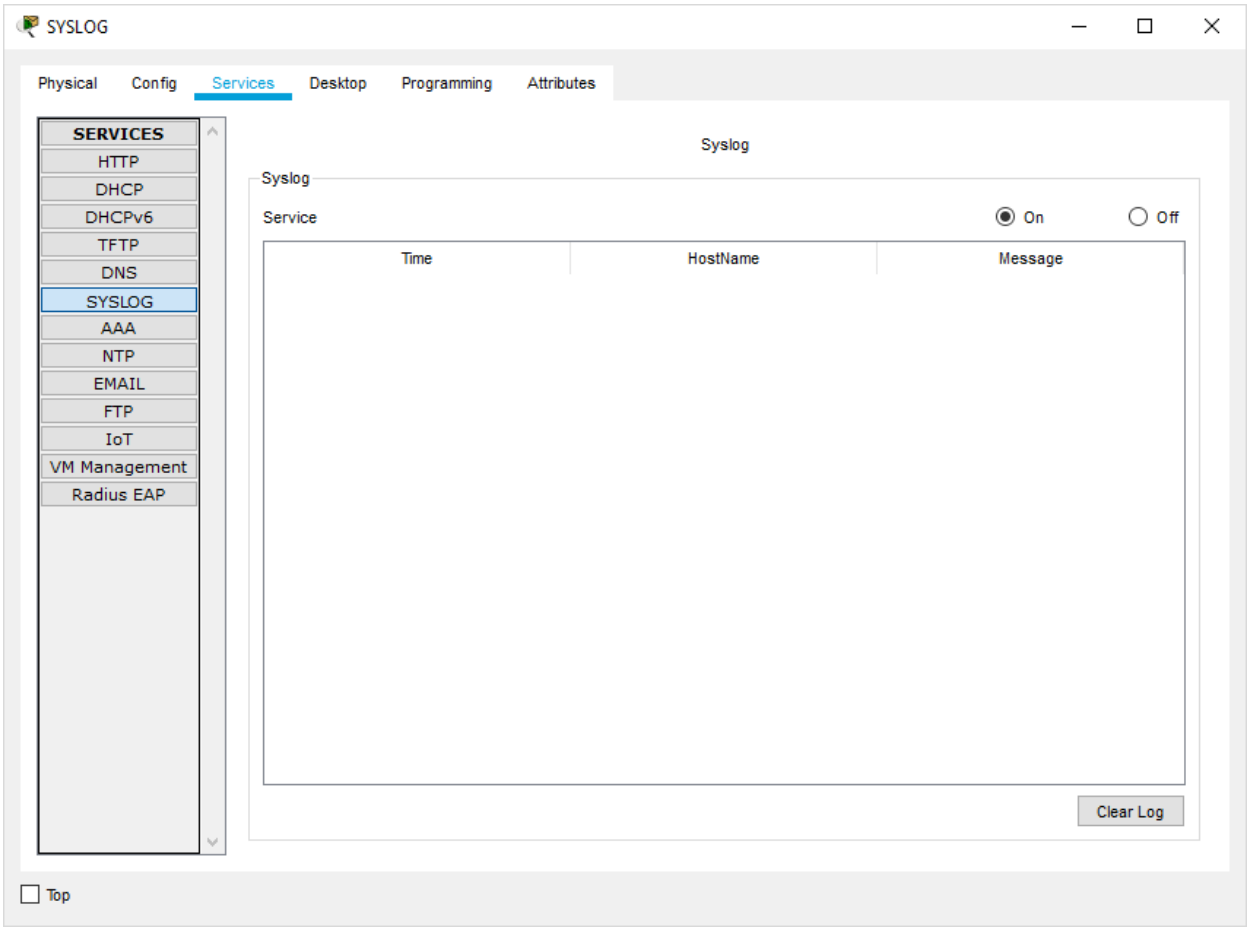
```
Router#show clock
18:12:43.760 UTC Fri Jan 14 2022
Router#
```

c) 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.

Turn ON the SYSLOG service on the server

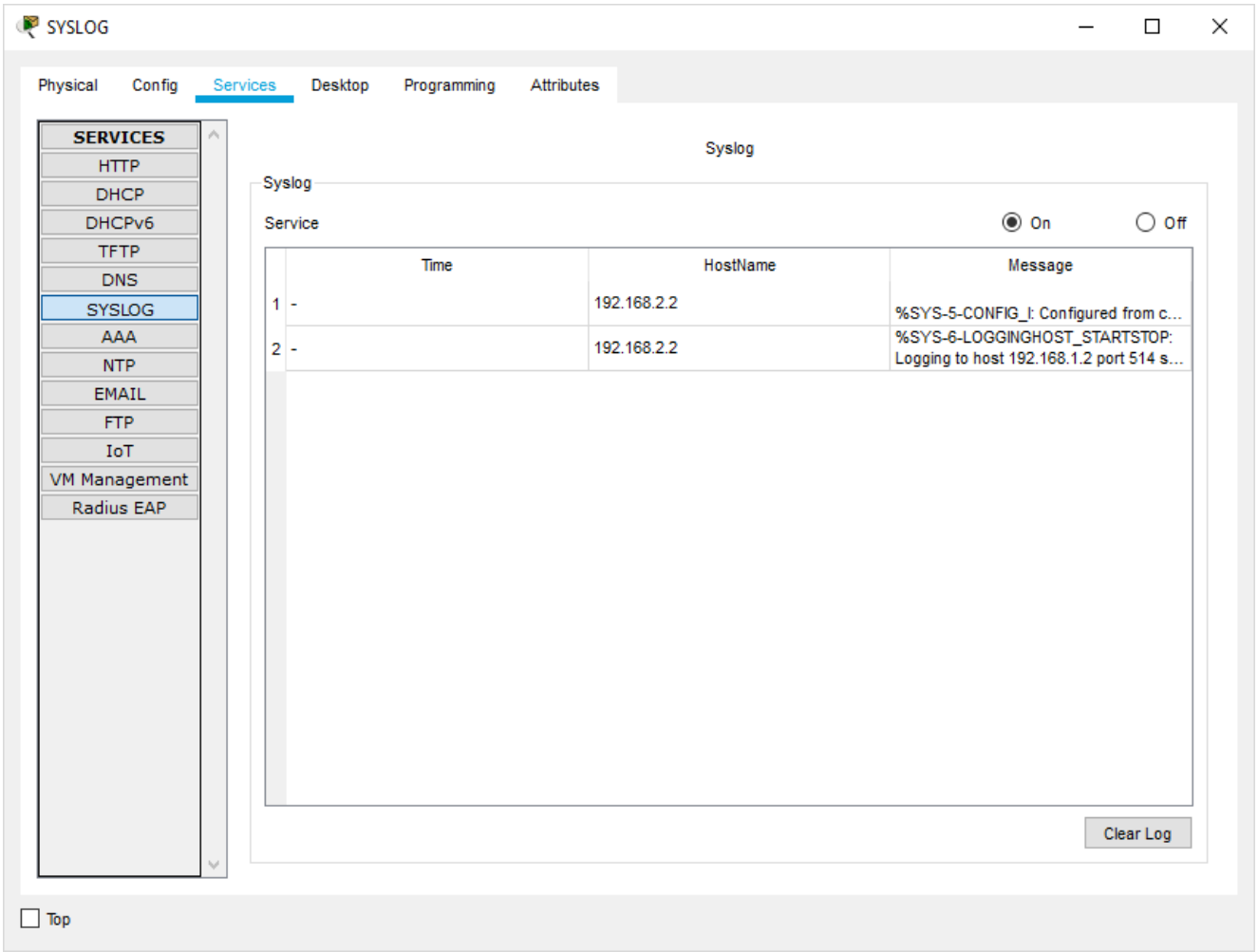


And Turn OFF on all other Servers

Now Go to CLI Mode of any Router and type the following commands in all the Routers.

```
Router#
Router#configure terminal
Router(config)#logging 192.168.1.6
Router(config)#exit
Router#
```

Output:



d) SSH

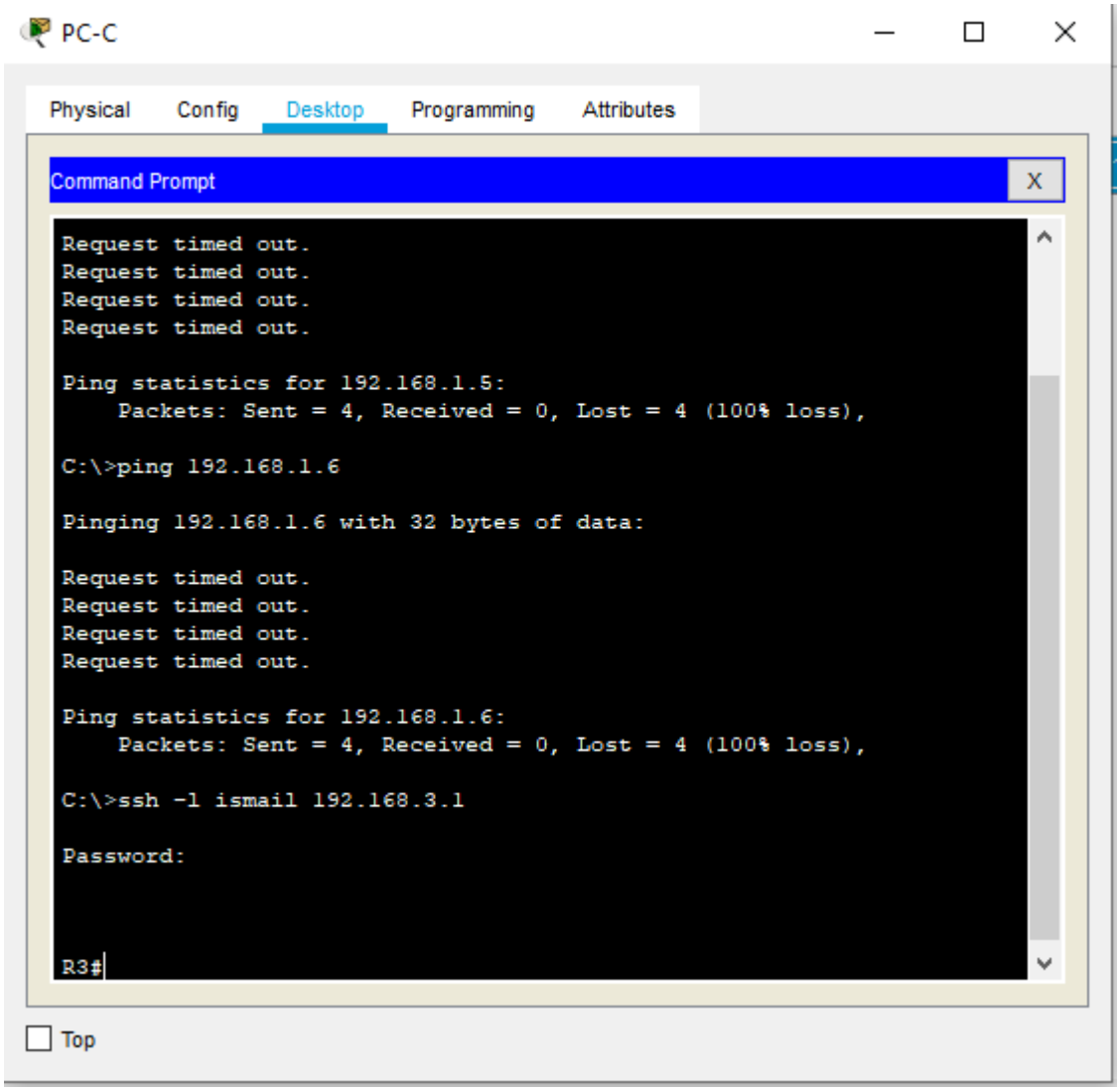
- An **SSH server** is a software program which uses the secure shell protocol to accept connections from remote computers.
- The way **SSH works** is by making use of a client-server model to allow for authentication of two remote systems and encryption of the data that passes between them.
- It organizes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

Now Go to CLI Mode of Router3 and type the following commands.

```
Router#configure terminal
Router(config)#ip domain-name ismail.com
Router(config)#hostname R3
R3(config)#
R3(config)#crypto key generate rsa


The name for the keys will be: R1.ismail.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.


R3(config)#line vty 0 4
R3(config-line)#transport input ssh
R3(config-line)#login local
R3(config-line)#exit
R3(config)#username ismail privilege 15 password cisco
R3(config)#
```

Output: Go to cmd of PC-C and type the command

ssh –l ismail 192.168.3.1 and type the password cisco



Hence SSH is also verified

PRACTICAL NO 2: Configure AAA Authentication

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.

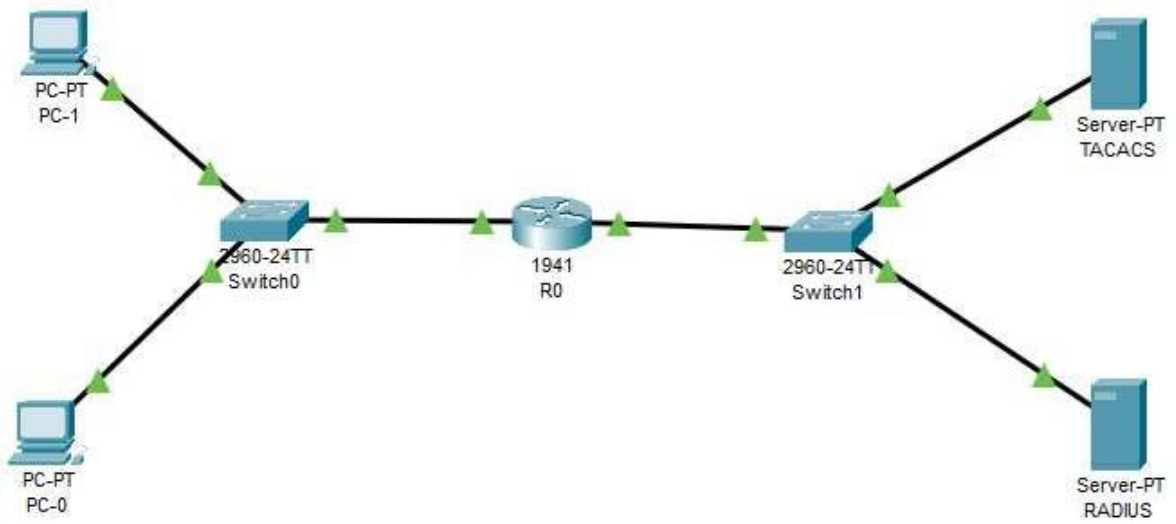
Advantages (TACACS+ over RADIUS) –

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+.

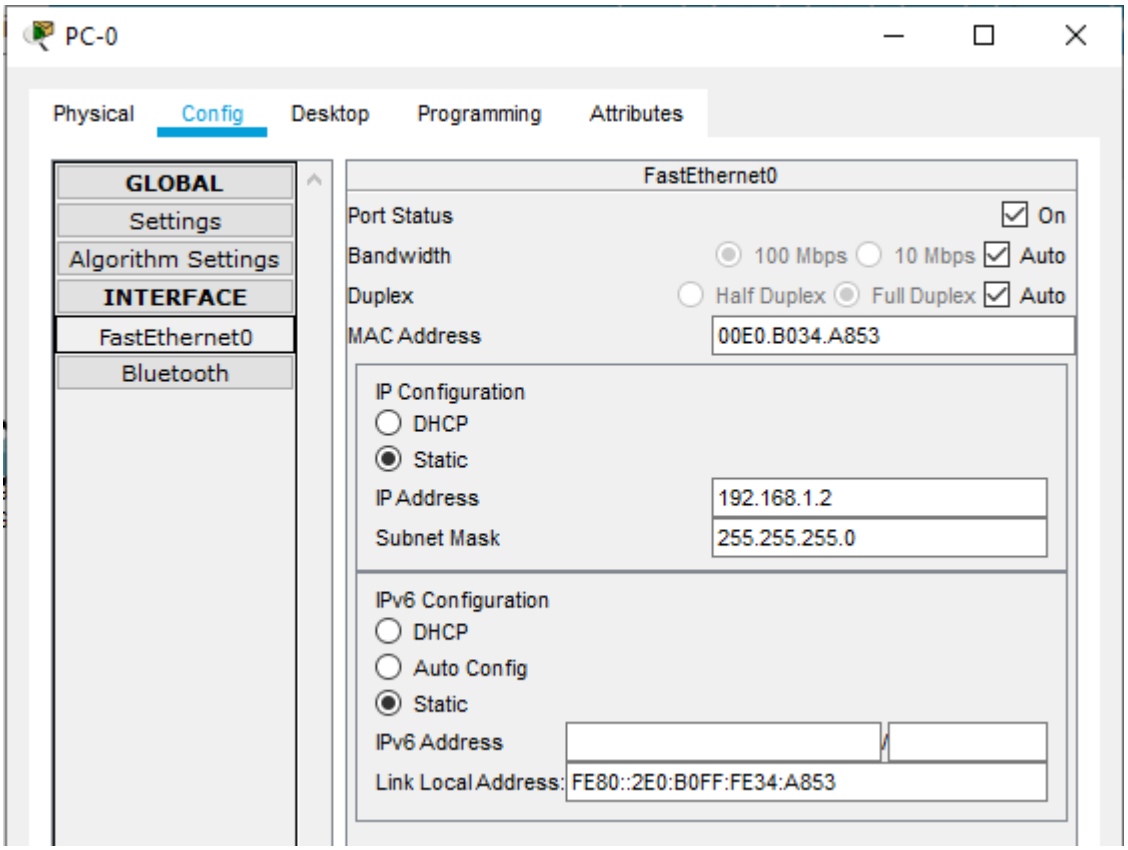
Let us consider the following Topology to understand the above AAA authentication.



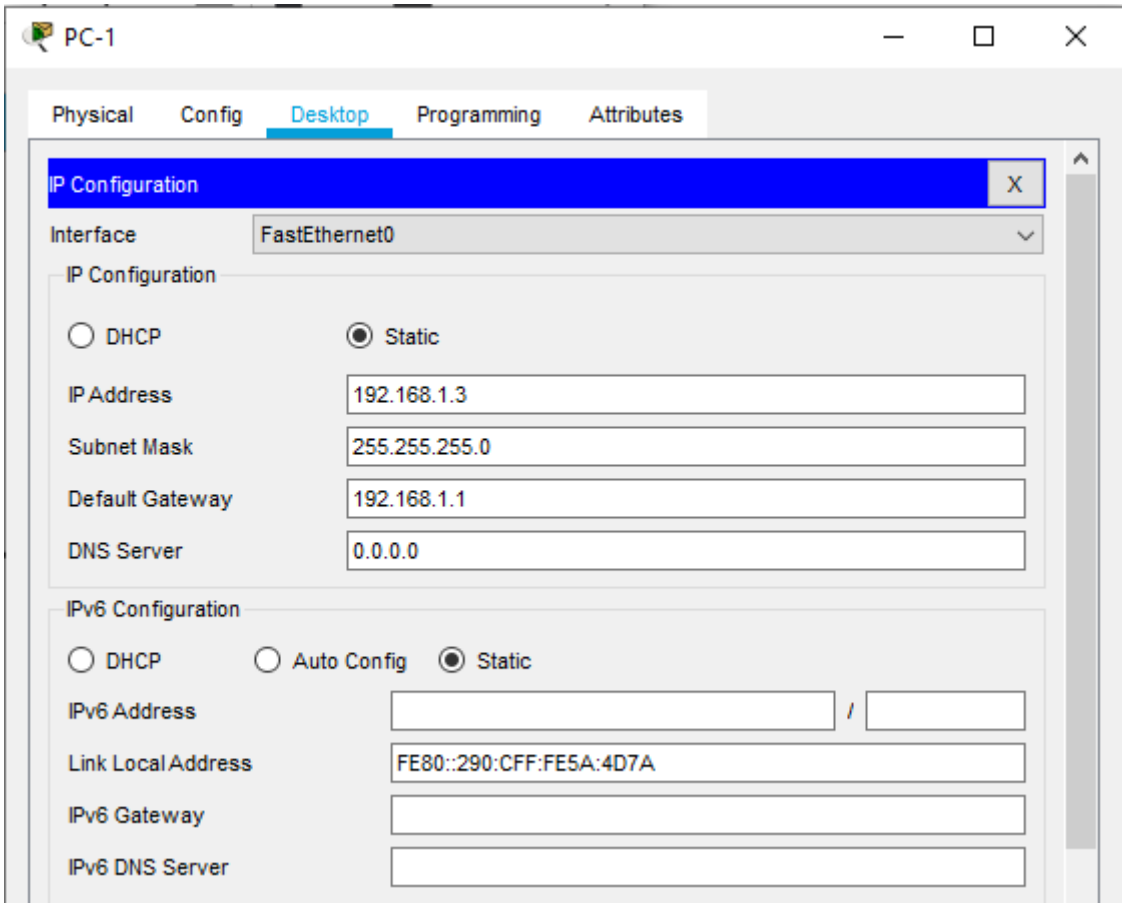
Let us consider the following Address table to configure the network devices:

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

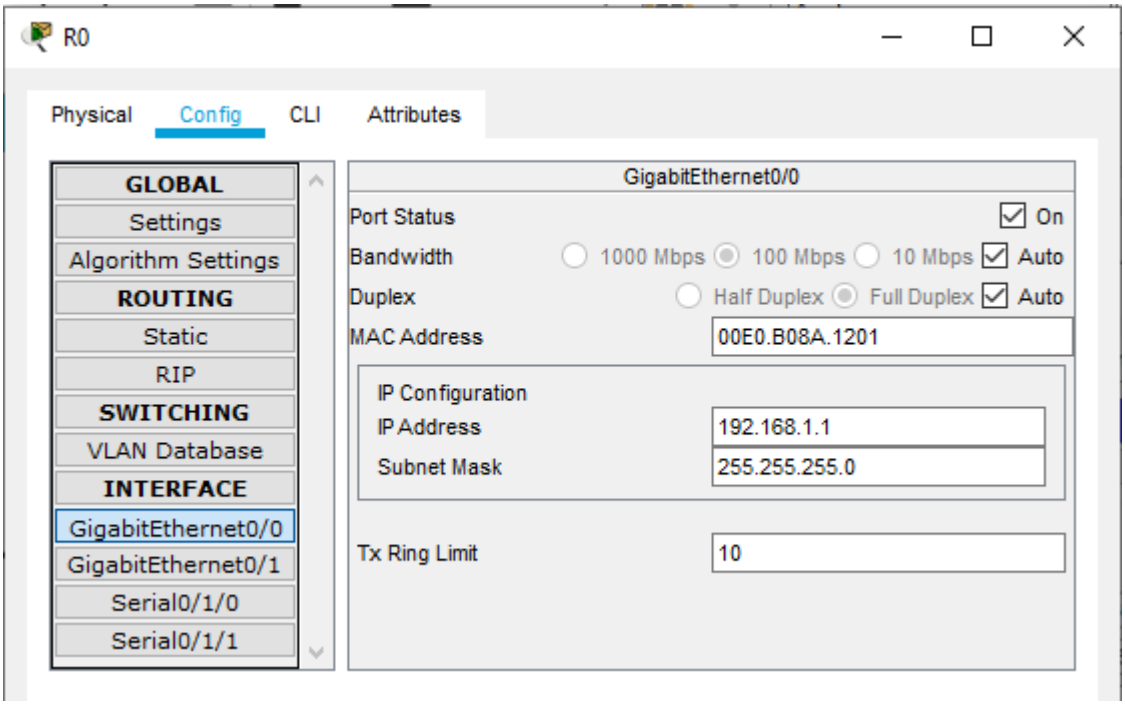
Configuring PC-0

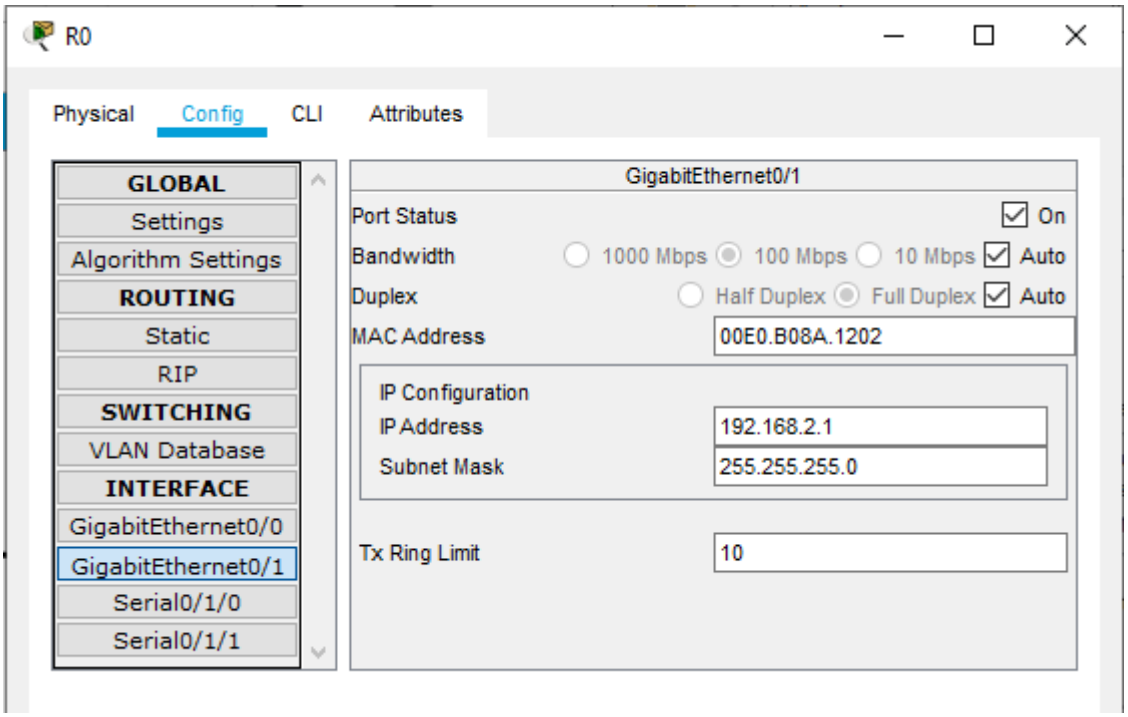


Configuring PC-1

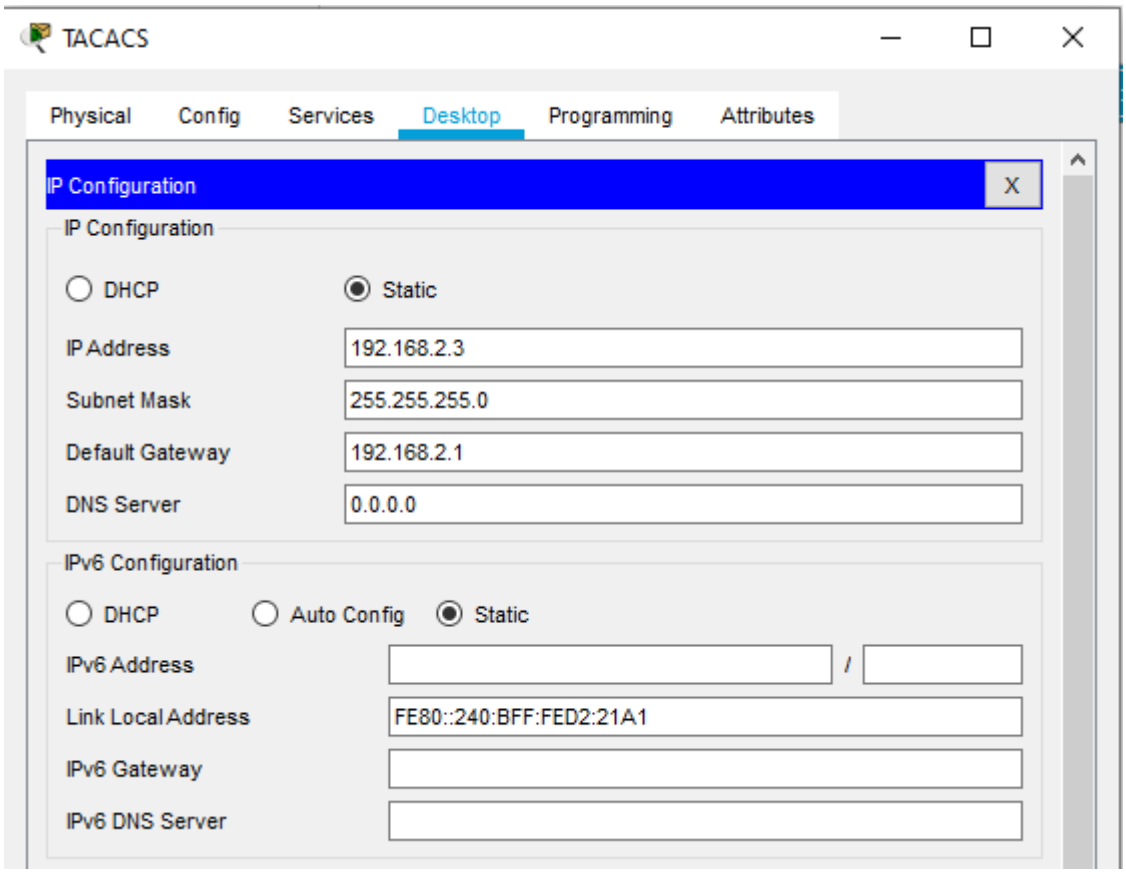


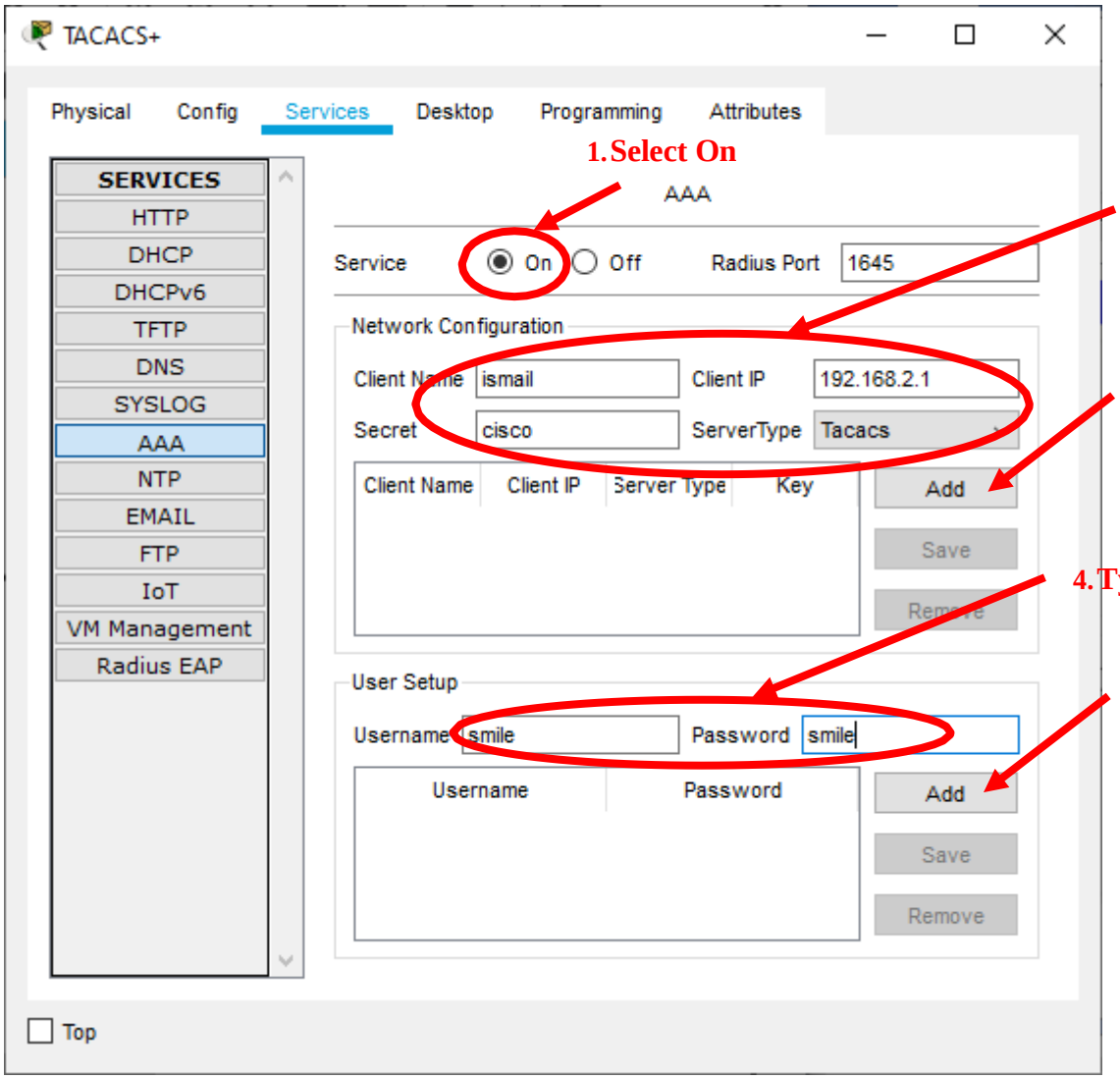
Configuring Router R0



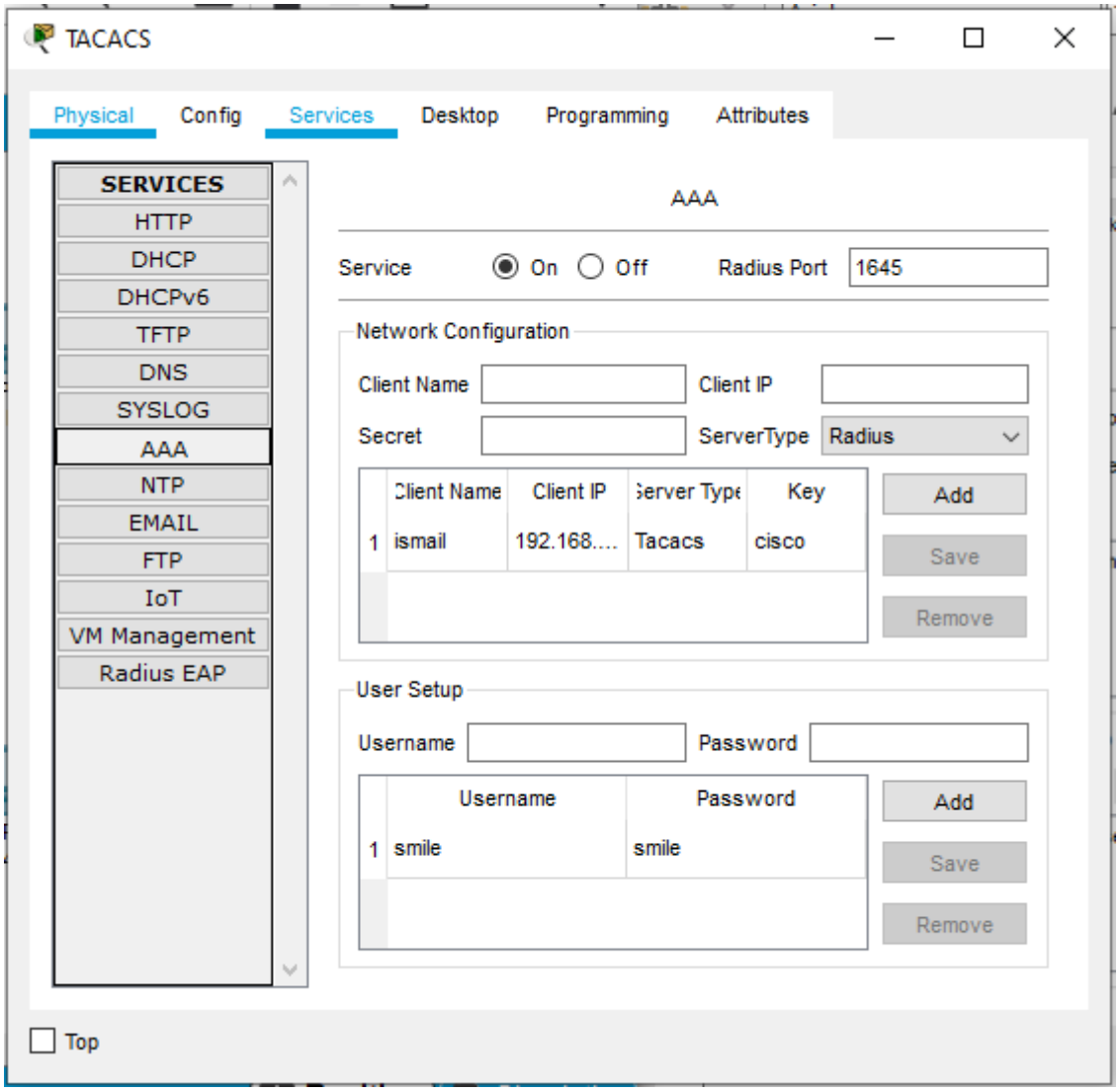


Configuring TACACS

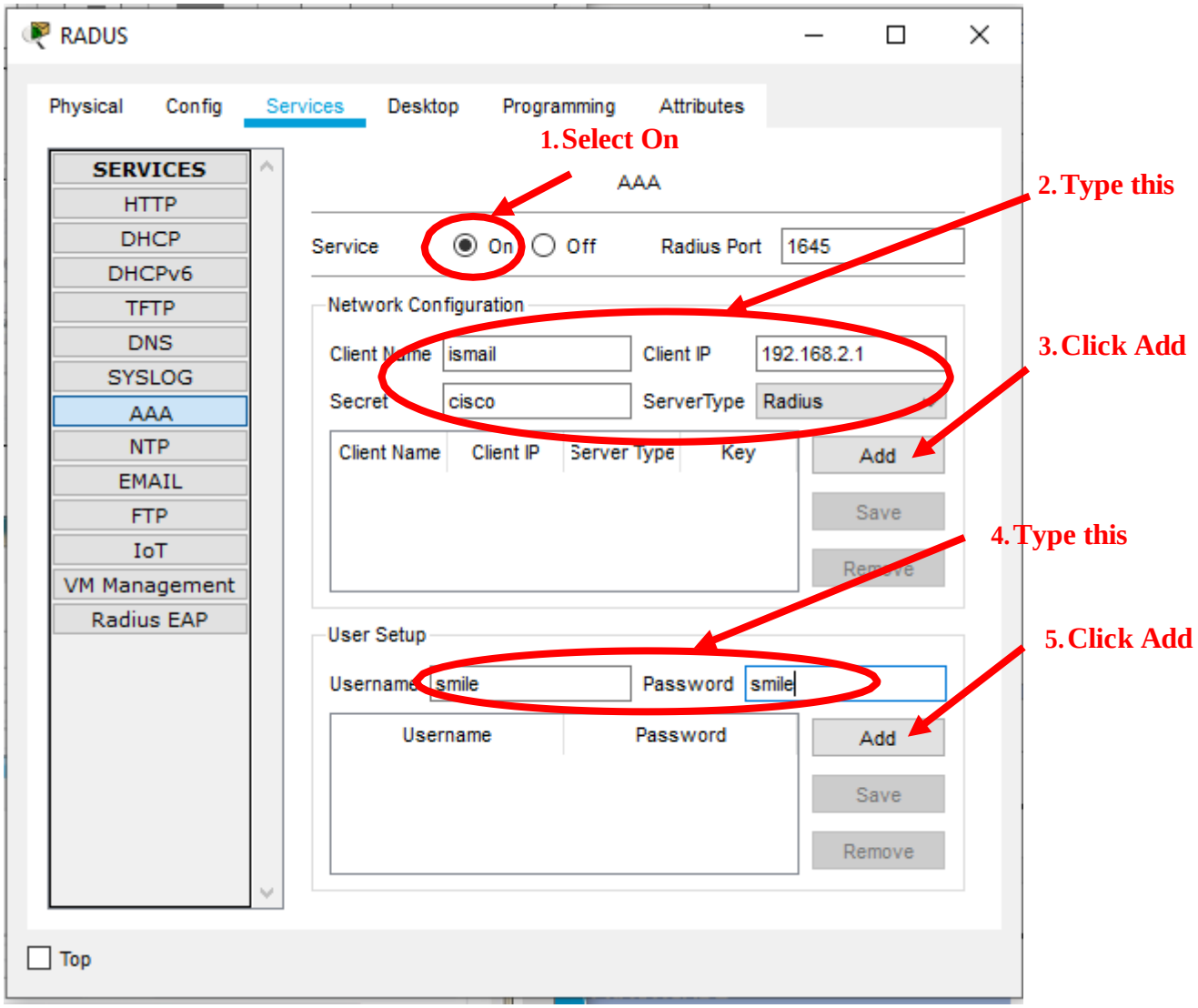



TACACS+
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
1. Select On
AAA
Service
On
Off
Radius Port
1645
2. Type this
Network Configuration
Client Name
ismail
Client IP
192.168.2.1
Secret
cisco
ServerType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

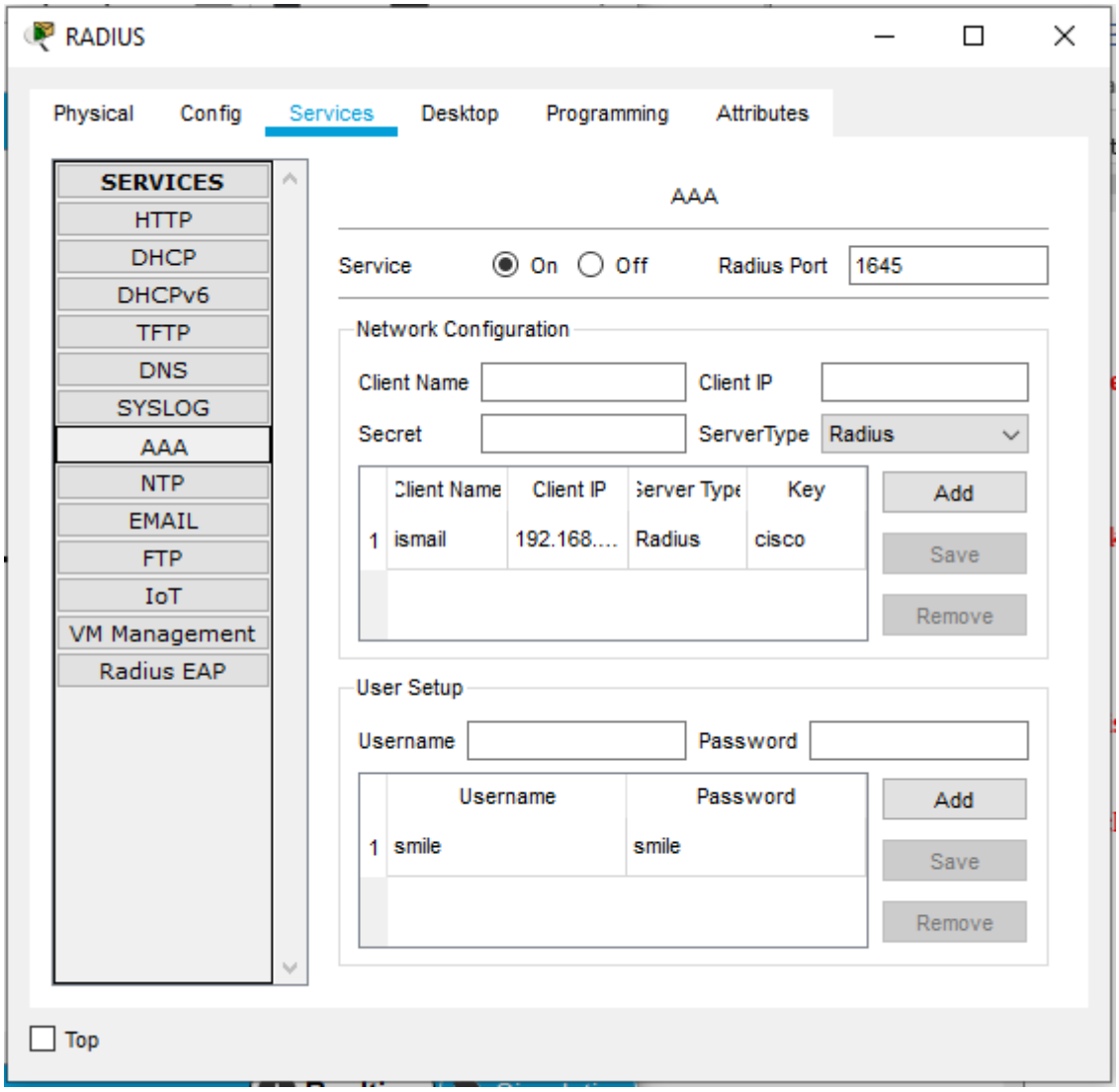
Your window should look like below image after you click Add button



Configuring RADIUS



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

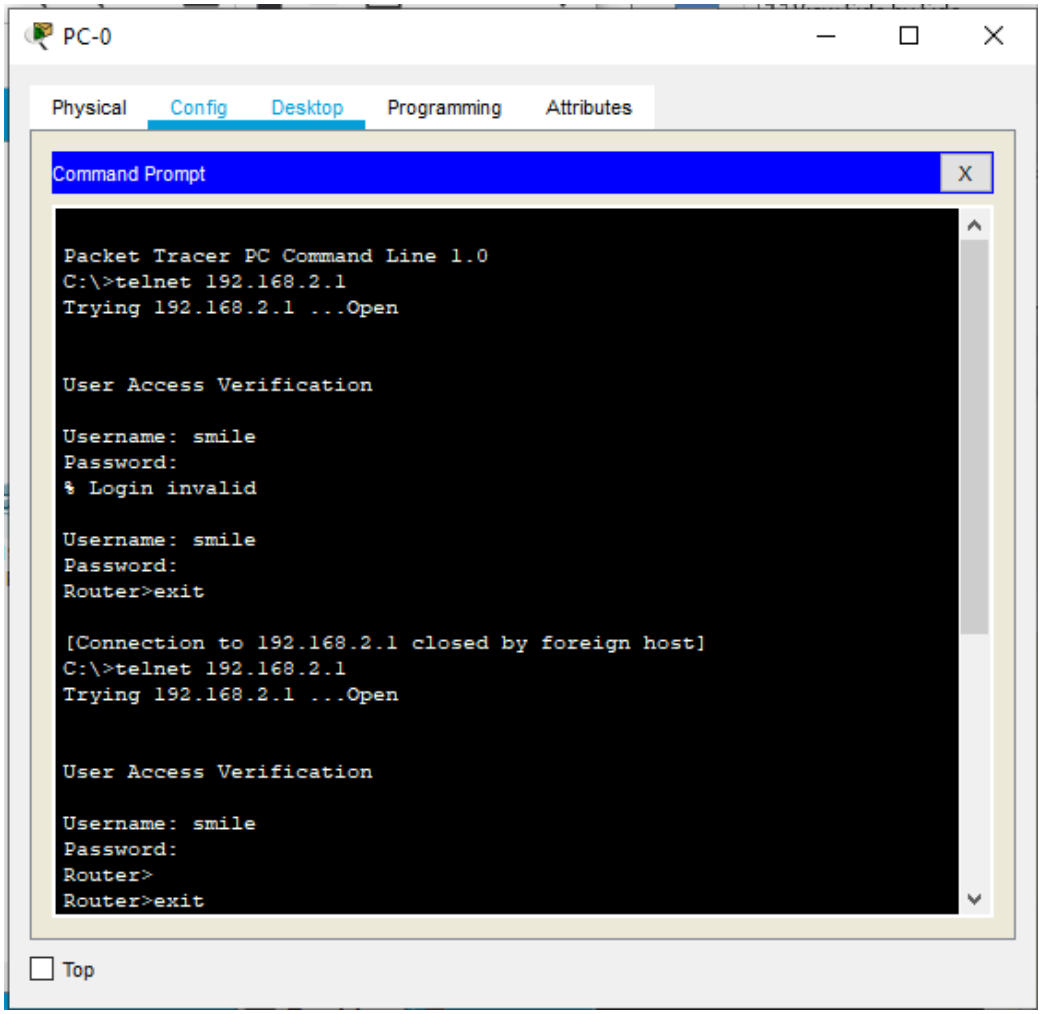


Type the following commands in the CLI mode of the Router0

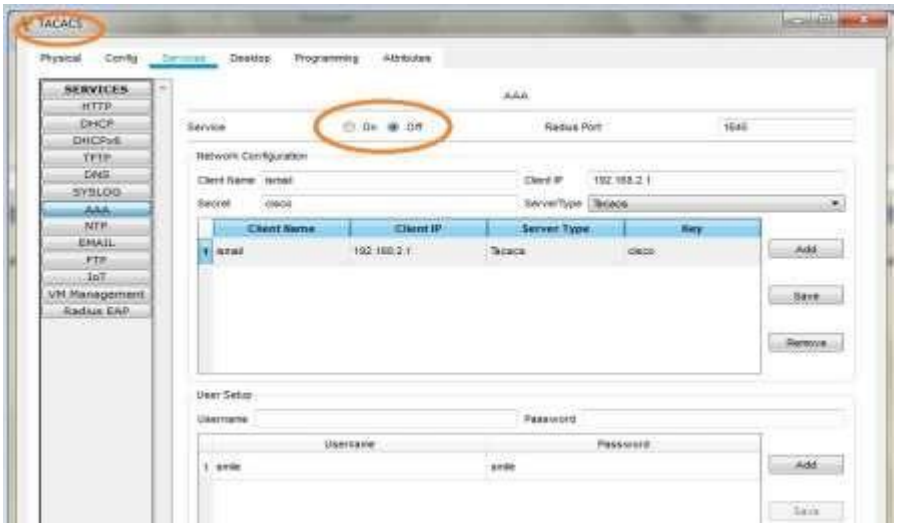
```
Router>enable
Router#configure terminal
Router(config)#aaa new-model
Router(config)#tacacs-server host 192.168.2.3 key cisco
Router(config)#radius-server host 192.168.2.2 key cisco
Router(config)#aaa authentication login ismail group tacacs+ group radius local
Router(config)#line vty 0 4
Router(config-line)#login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

To get check the output:

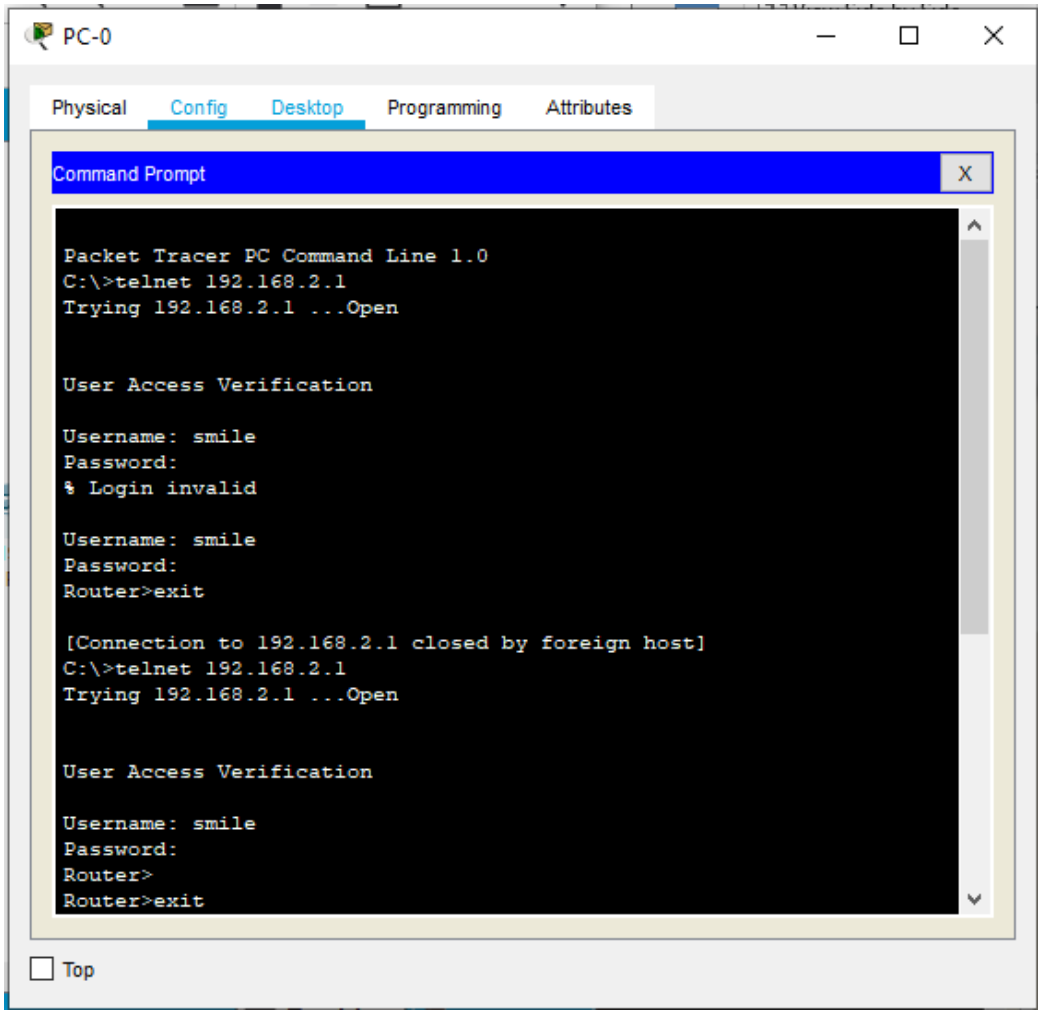
The Authentication can be done by typing the command **telnet 192.168.2.1 (**the Router IP**)** in any of the PCs
We get a prompt to type the username and password, the username and password set in TACACS are entered
Username: smile
Password: smile
We get the following



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



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



PRACTICAL NO 3: Configure extended ACLs

The Cisco Access Control List (ACL) are used for filtering traffic based on a given filtering criteria on a router or switch interface. Based on the conditions supplied by the ACL, a packet is allowed or blocked from further movement.

Cisco ACLs are available for several types of routed protocols including IP, IPX, AppleTalk, XNS, DECnet, and others. However, we will be discussing ACLs pertaining to TCP/IP protocol only.

ACLs for TCP/IP traffic filtering are primarily divided into two types:

1. Standard Access Lists, and
2. Extended Access Lists

Standard Access Control Lists:
Standard IP ACLs range from 1 to 99. A Standard Access List allows you to permit or deny traffic FROM
specific IP addresses. The destination of the packet and the ports involved can be anything. This is the command syntax format of a standard ACL.

access-list access-list-number {permit|deny}
{host|source source-wildcard|any} Standard ACL example:
access-list 10 permit 192.168.2.0 0.0.0.255

This list allows traffic from all addresses in the range 192.168.2.0 to 192.168.2.255

Note that when configuring access lists on a router, you must identify each access list uniquely by assigning either a name or a number to the protocol's access list.

There is an implicit deny added to every access list. If you entered the command:

show access-list 10

The output looks like:
access-list 10 permit 192.168.2.0 0.0.0.255 access-list 10 deny any

Standard Access Control Lists:

Standard IP ACLs range from 1 to 99. A Standard Access List allows you to permit or deny traffic FROM specific IP addresses. The destination of the packet and the ports involved can be anything. This is the command syntax format of a standard ACL.

access-list access-list-number {permit|deny}
{host|source source-wildcard|any} Standard ACL example:
access-list 10 permit 192.168.2.0 0.0.0.255

This list allows traffic from all addresses in the range 192.168.2.0 to 192.168.2.255

Note that when configuring access lists on a router, you must identify each access list uniquely by assigning either a name or a number to the protocol's access list.

There is an implicit deny added to every access list. If you entered the command:

show access-list 10

The output looks like:
access-list 10 permit 192.168.2.0 0.0.0.255 access-list 10 deny any

Extended Access Control Lists:
Extended IP ACLs allow you to permit or deny traffic from specific IP addresses to a specific destination IP address and port. It also allows you to have granular control by specifying controls for different types of protocols such as ICMP, TCP, UDP, etc within the ACL statements. Extended IP ACLs range from
100 to 199. In Cisco IOS Software Release 12.0.1, extended ACLs began to use additional numbers (2000 to 2699).

The syntax for IP Extended ACL is given below:

access-list access-list-number {deny | permit} protocol source source-wildcard destination destination-wildcard [precedence precedence]

Note that the above syntax is simplified, and given for general understanding only.

Extended ACL example:
access-list 110 - Applied to traffic leaving the office (outgoing)
access-list 110 permit tcp 92.128.2.0 0.0.0.255 any eq 80

ACL 110 permits traffic originating from any address on the 92.128.2.0 network. The 'any' statement means that the traffic is allowed to have any destination address with the limitation of going to port 80. The value of 0.0.0.0/255.255.255.255 can be specified as 'any'.

Applying an ACL to a router interface:

After the ACL is defined, it must be applied to the interface (inbound or outbound). The syntax for applying an ACL to a router interface is given below:

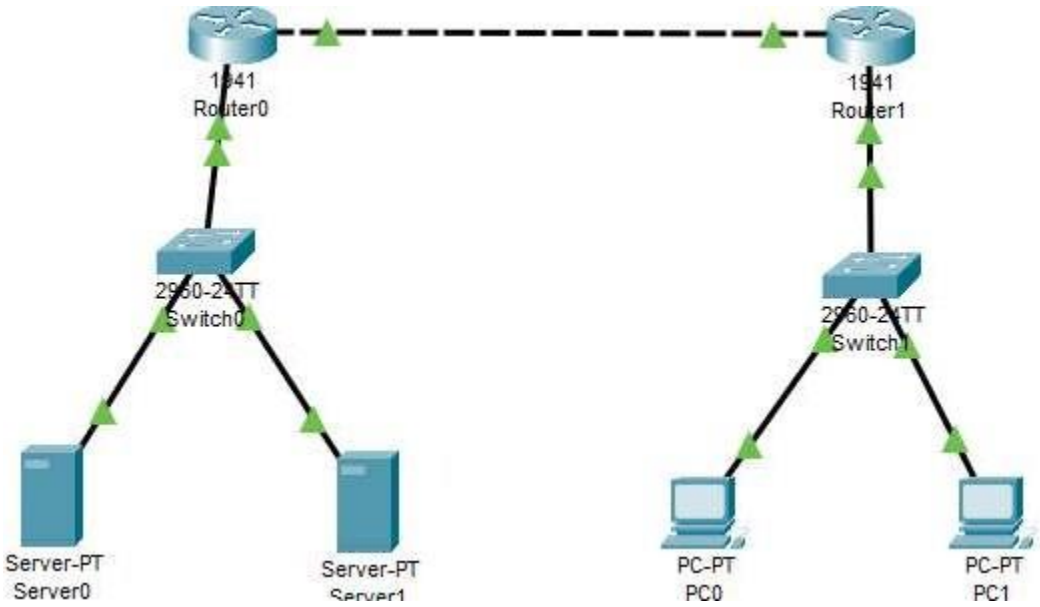
interface <interface>
ip access-group {number|name} {in|out}

An Access List may be specified by a name or a number. "in" applies the ACL to the inbound traffic, and "out" applies the ACL on the outbound traffic.

Example: To apply the standard ACL created in the previous example, use the following commands:

Rouer(config)#interface serial0
Rouer(config-if)#ip access-group 10 out

Consider the following topology

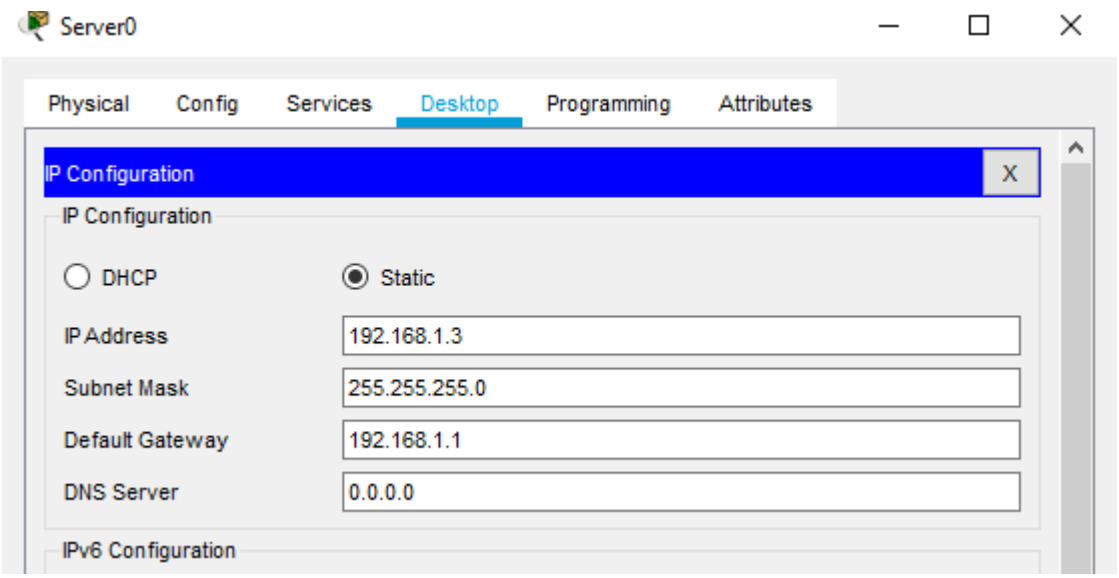


Let us consider the following Address table to configure the network devices:

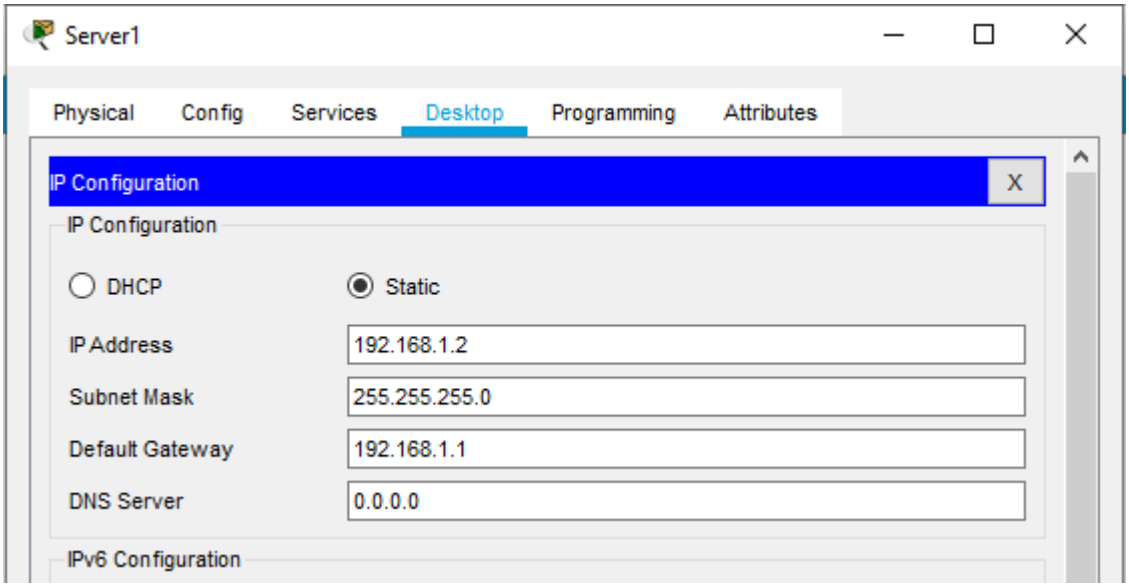
Device	Interface	IP Address	Subnet Mask	Default gateway	Switch Port
Server 0	NA	192.168.1.3	255.255.255.0	192.168.1.1	Switch 0 F/06
Server 1	NA	192.168.1.2	255.255.255.0	192.168.1.1	Switch 0 F0/1
PC 0	NA	192.168.3.2	255.255.255.0	192.168.3.1	Switch 1 F/06
PC 1	NA	192.168.3.3	255.255.255.0	192.168.3.1	Switch 1 F0/1
Router 0	GE0/0	192.168.1.1	255.255.255.0	NA	Switch 0 F0/5
	GE0/1	192.168.2.2	255.255.255.0	NA	GE0/1
Router 1	GE0/0	192.168.3.1	255.255.255.0	NA	Switch 1 F0/5
	GE0/1	192.168.2.2	255.255.255.0	NA	GE 0/1

Part 1: Configure, Apply and Verify an Extended Numbered ACL

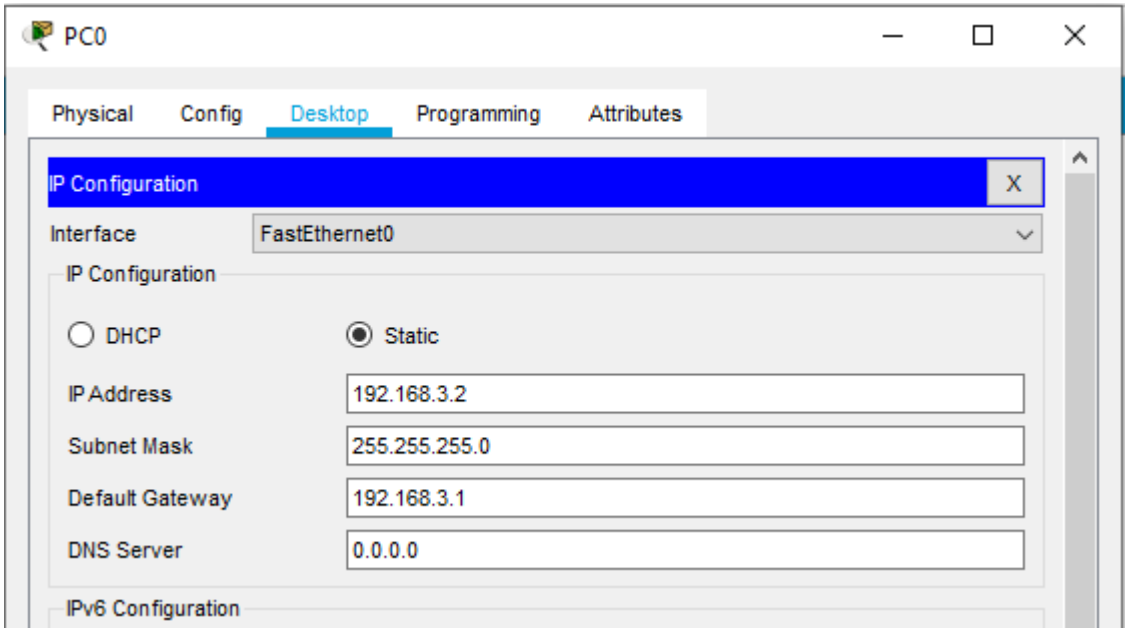
Configuring Server 0



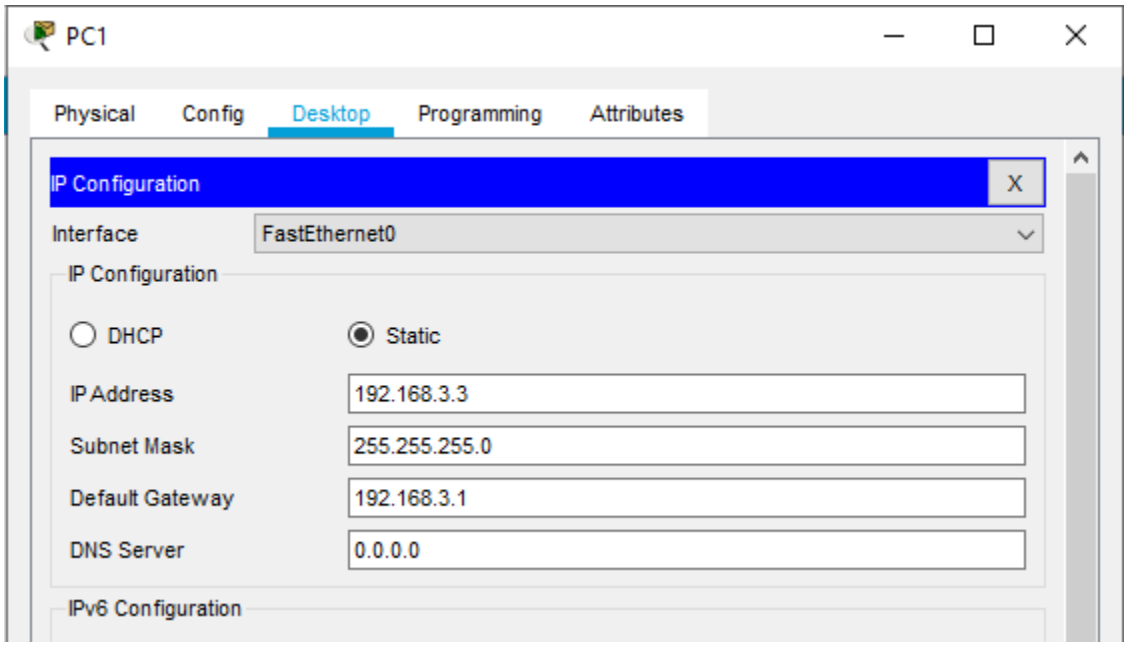
Configuring Server 1



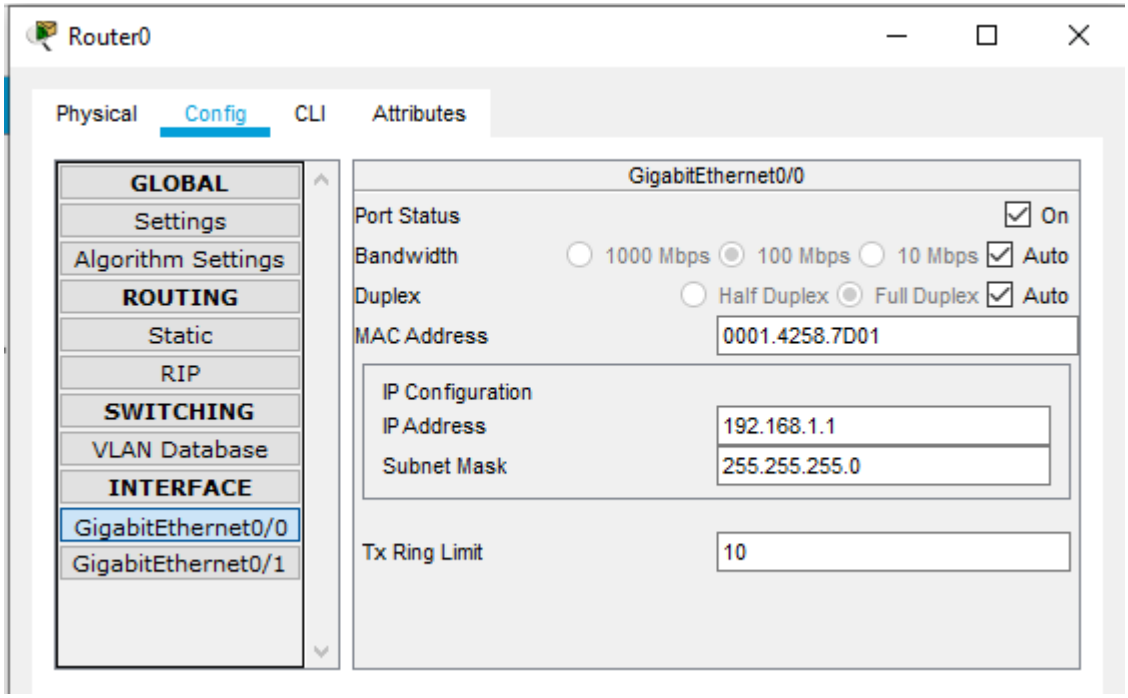
Configuring PC 0

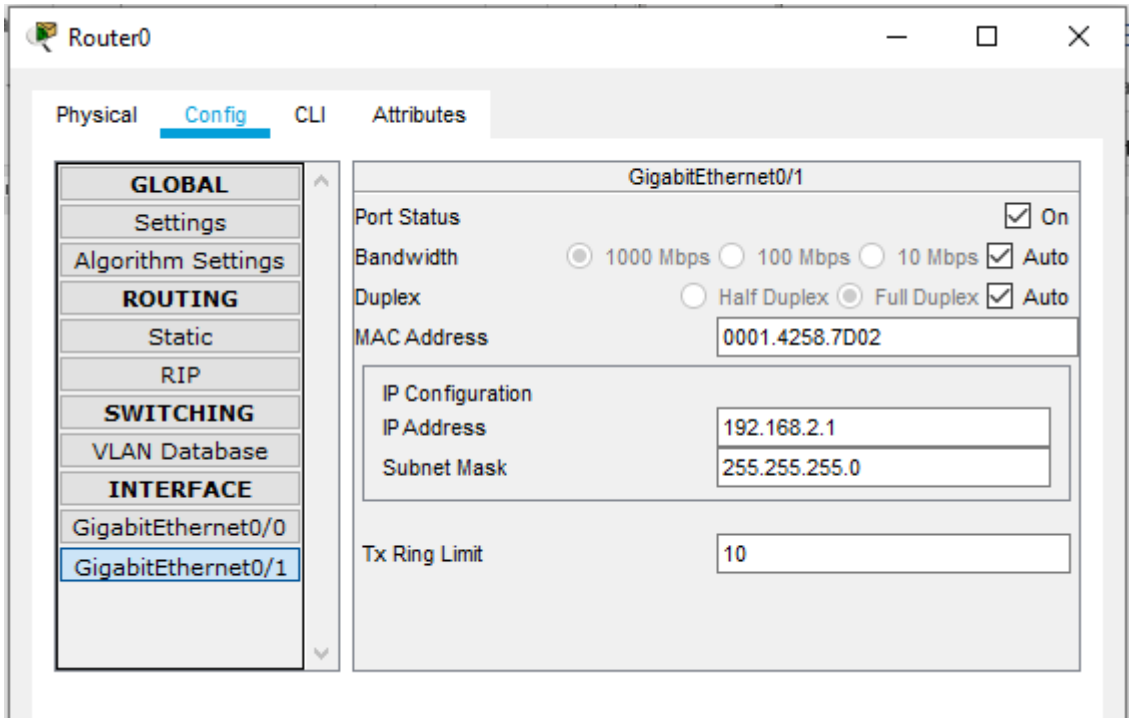


Configuring PC 1

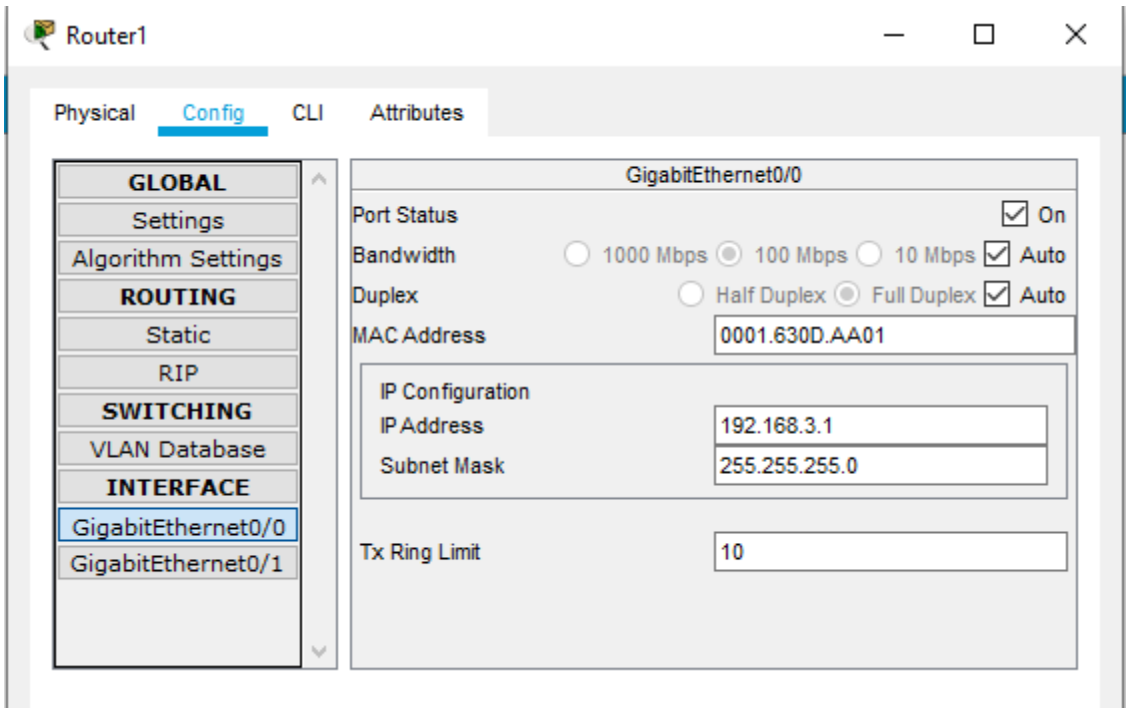


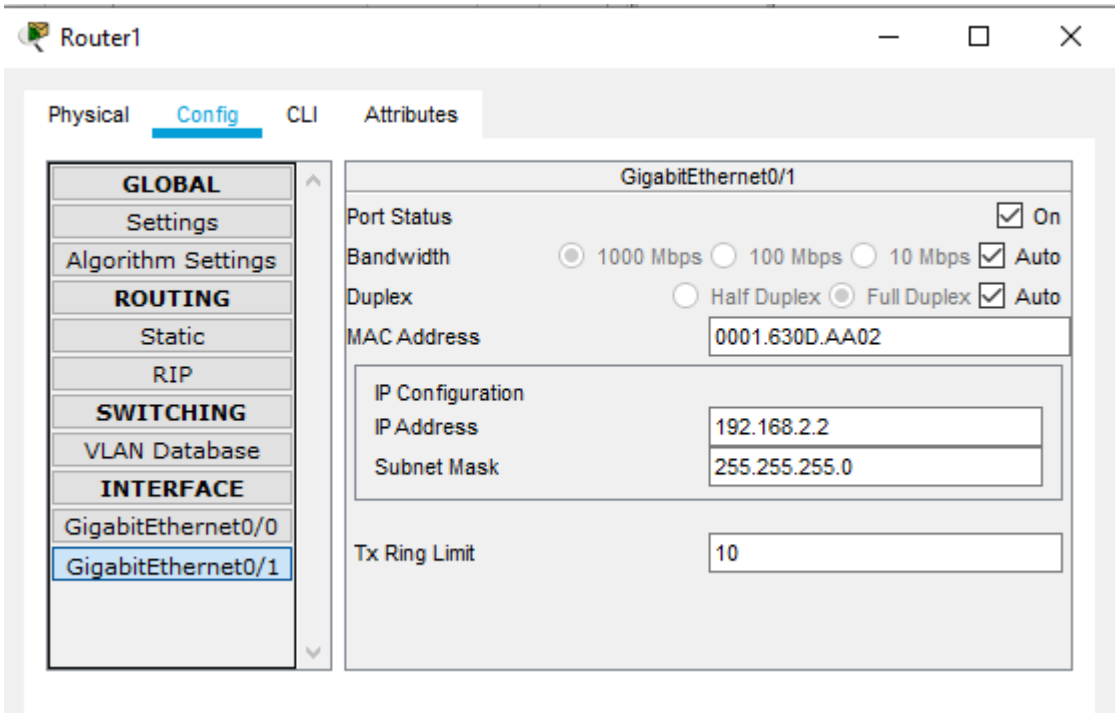
Configuring Router 0



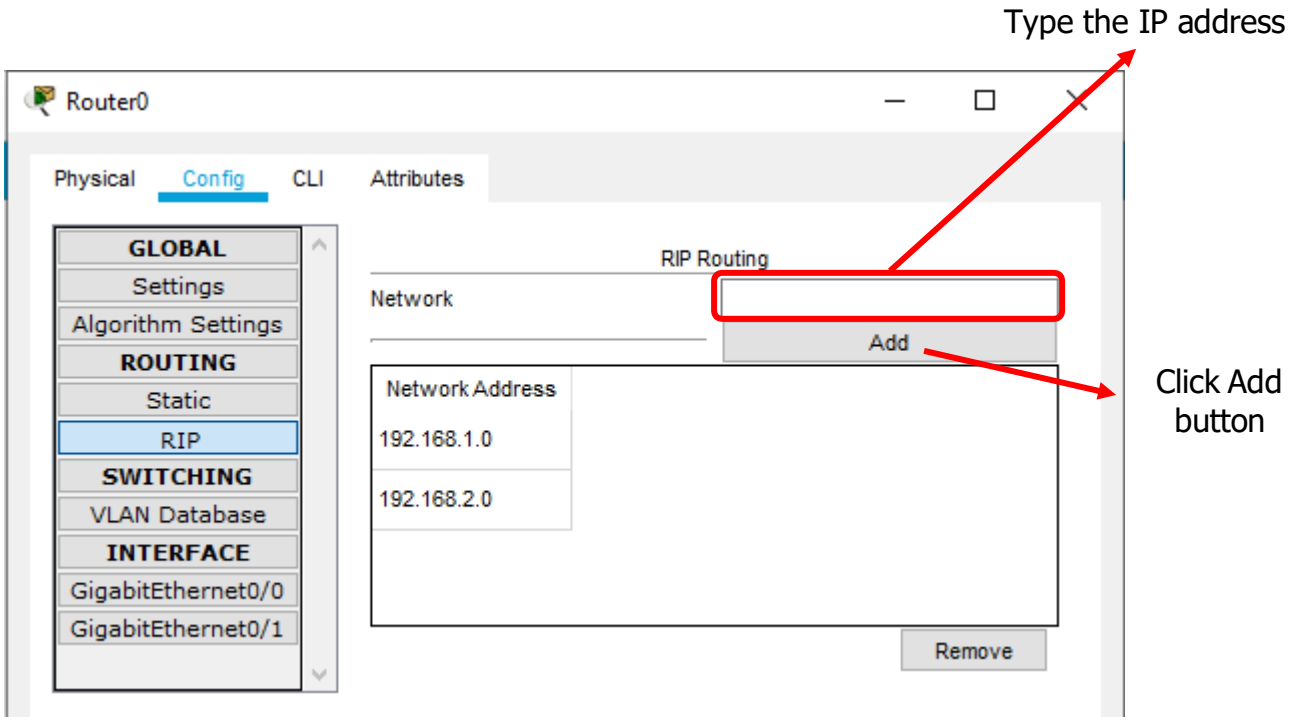


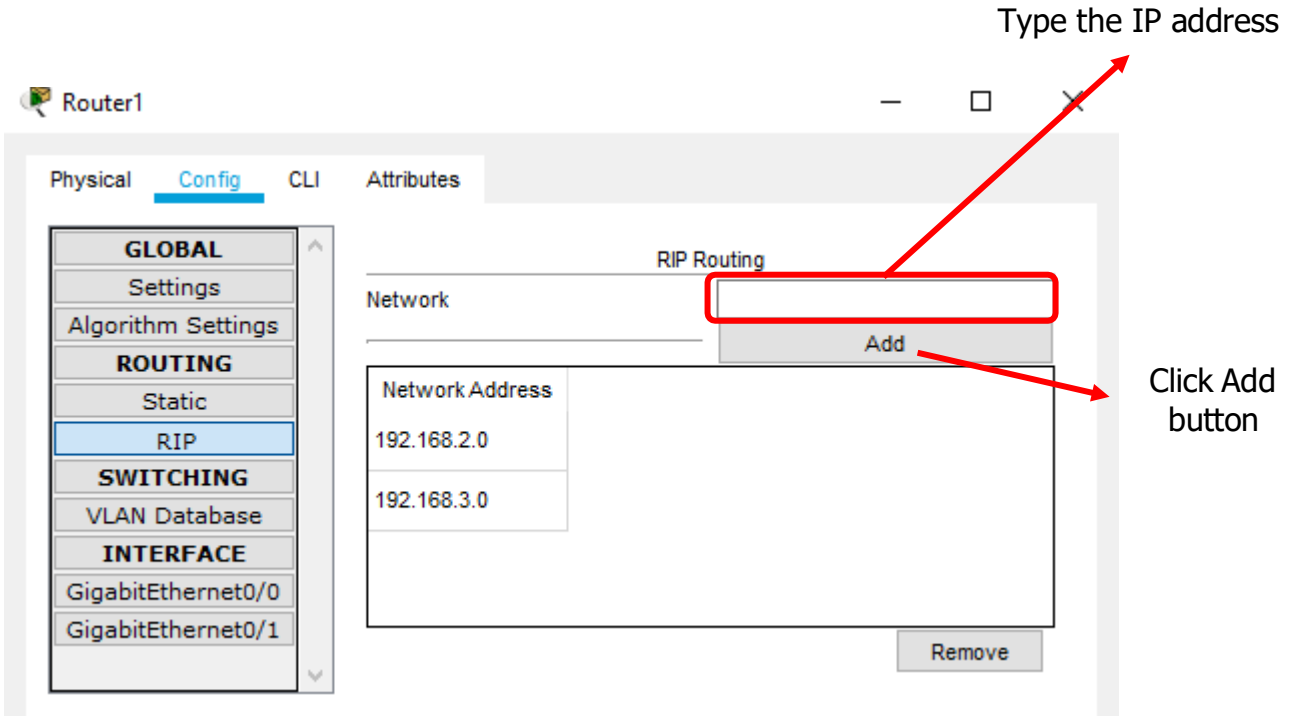
Configuring Router 1





Set the RIP protocol on both the Routers as follows



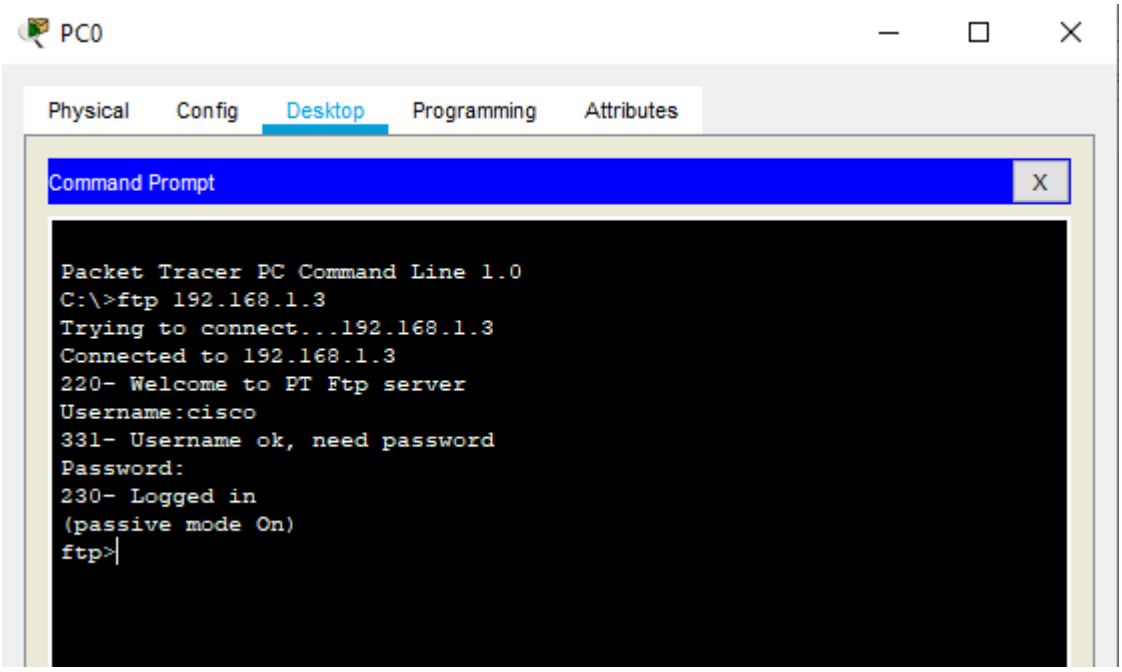


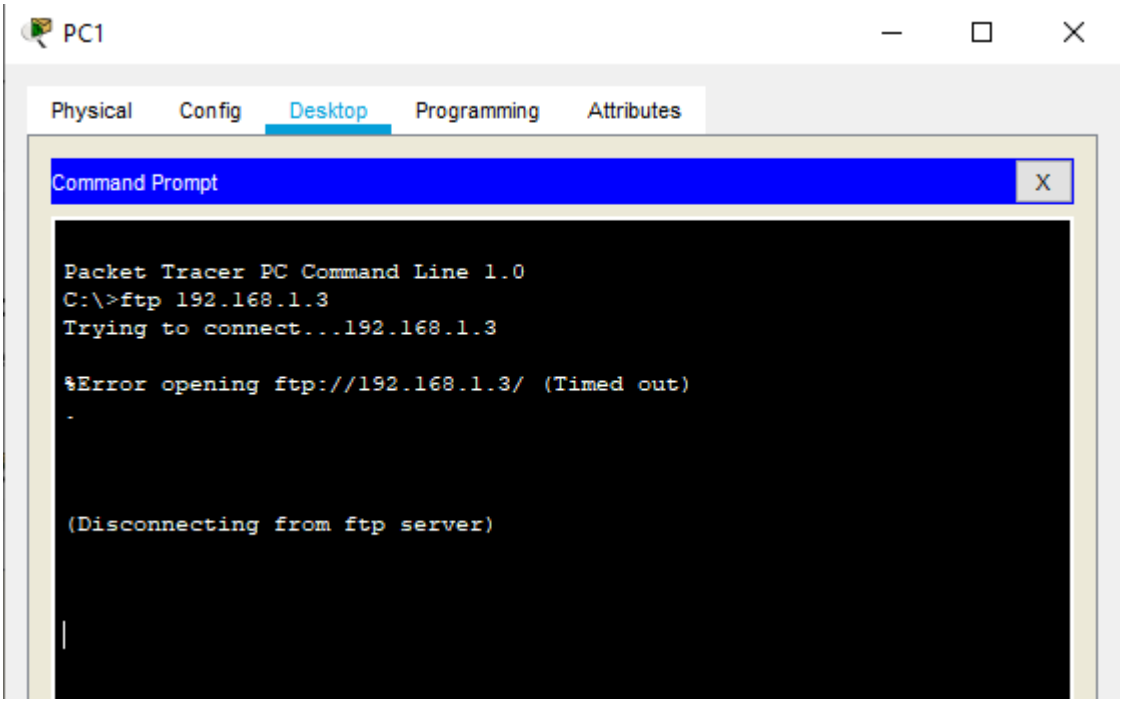
Check the connectivity between all the devices in the topology.

Type the following commands in Router1

```
Router#configure  terminal
Router(config)#access-list 100 permit tcp host 192.168.3.2 host 192.168.1.3 eq ftp
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip access-group 100 out
Router(config-if)#exit
Router(config)#
```

Now verify the ftp (ftp 192.168.1.3) command from both the PCs, one would be successful (PC0) and other (PC1) would fail



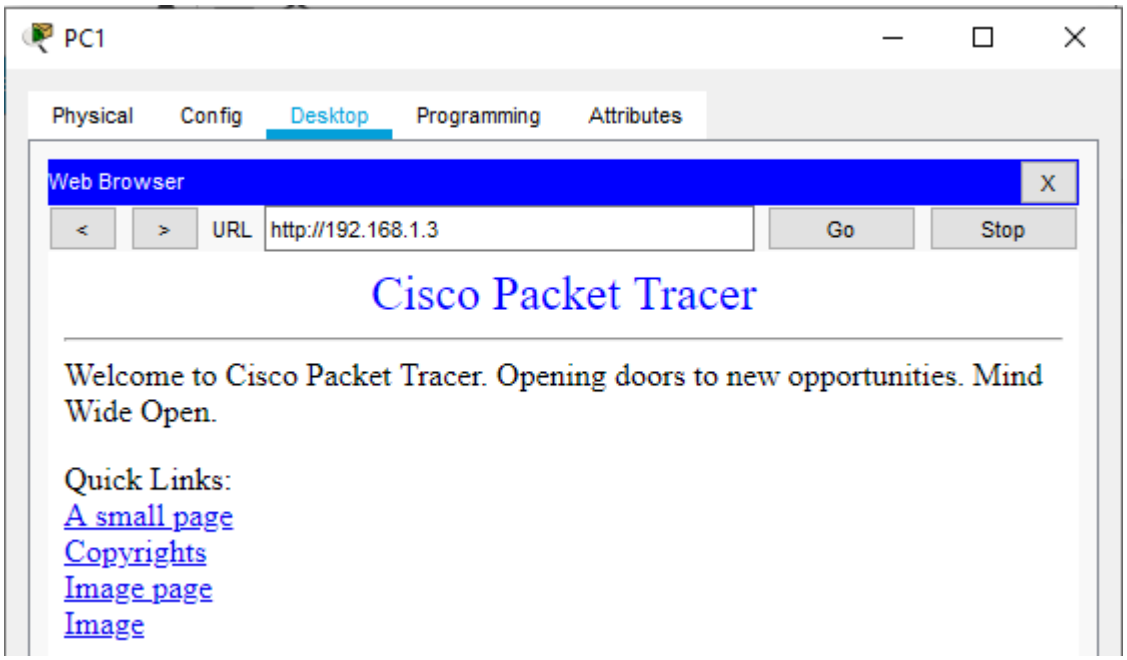


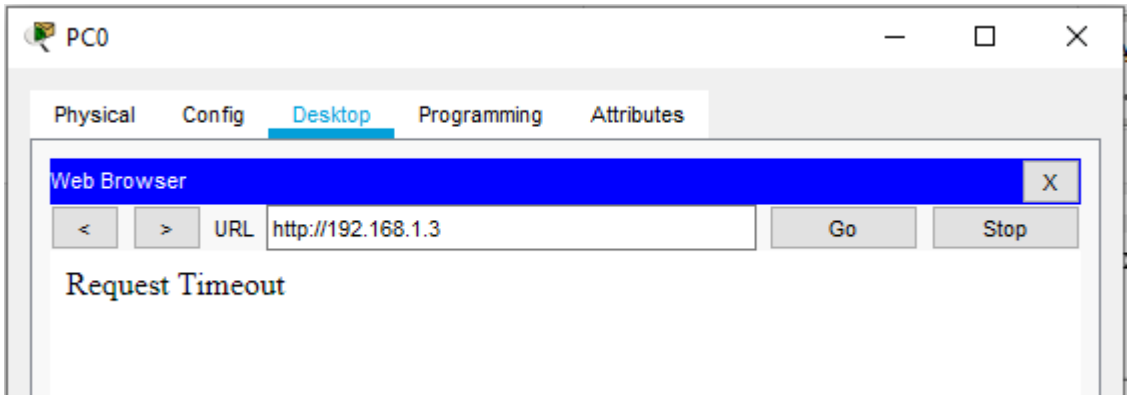
Part 2: Configure, Apply and Verify an Extended Named ACL

We use the same topology for this case
Type the following command in the CLI mode of Router1

```
Router> Router>enable router
Router#configure terminal
Router(config)#ip access-list extended SMILE
Router(config-ext-nacl)#permit tcp host 192.168.3.3 host 192.168.1.3 eq www
Router(config-ext-nacl)#exit
Router(config)#
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip access-group SMILE out
Router(config-if)#exit
Router(config)#
```

Now verify the www (192.168.1.3) command from both the PCs browser, one would be successful (PC1) and other (PC0) would fail





Hence Extended Numbered ACLs as well as Extended Named ACLs have been verified.

PRACTICAL NO 4: Configure IP ACLs to Mitigate Attacks and IPv6 ACLs

Access Control Lists (ACLs)

Network administrators must figure out how to deny unwanted access to the network while allowing internal users appropriate access to necessary services. Although security tools, such as passwords, callback equipment, and physical security devices are helpful, they often lack the flexibility of basic traffic filtering and the specific controls most administrators prefer.

For example, a network administrator may want to allow users access to the Internet, but not permit external users telnet access into the LAN.
Routers provide basic traffic filtering capabilities, such as blocking Internet traffic, with access control lists (ACLs).

An ACL is a sequential list of permit or deny statements that apply to addresses or upper-layer protocols.

The router examines each packet to determine whether to forward or drop it, based on the conditions specified in the ACL. Some ACL decision points are:
1) IP source address
2) IP destination addresses
3) UDP or TCP protocols
4) Upper-layer (TCP/UDP) port numbers

ACLs must be defined on a:
1) Per-protocol (IP, IPX, AppleTalk)
2) Per direction (in or out)
3) Per port (interface) basis.
4) ACLs control traffic in one direction at a time on an interface.
5) A separate ACL would need to be created for each direction, one for inbound and one for outbound traffic.
6) Finally every interface can have multiple protocols and directions defined.

An ACL is a group of statements that define whether packets are accepted or rejected coming into an interface or leaving an interface.
1) ACL statements operate in sequential, logical order (top down).
2) If a condition match is true, the packet is permitted or denied and the rest of the ACL statements are not checked.

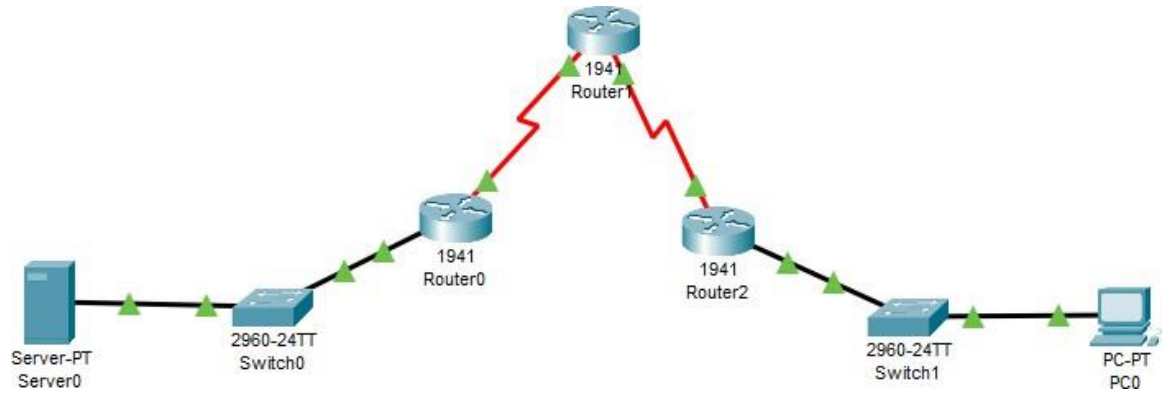
3) If all the ACL statements are unmatched, an implicit "deny any"
statement is placed at the end of the list by default. (not visible) When first learning how to create ACLs, it is a good idea to add the
implicit deny at the end of ACLs to reinforce the dynamic presence of the command line.

Standard IP ACLs
Can only filter on source IP addresses

Extended IP ACLs Can filter on:
1) Source IP address
2) Destination IP address
3) Protocol (TCP, UDP)
4) Port Numbers (Telnet – 23, http – 80, etc.) and other parameters

An access list is a sequential series of commands or filters. These lists tell the router what types of packets to: accept or deny Acceptance and denial can be based on specified conditions. ACLs applied on the router's interfaces

We use the following topology to study the present case

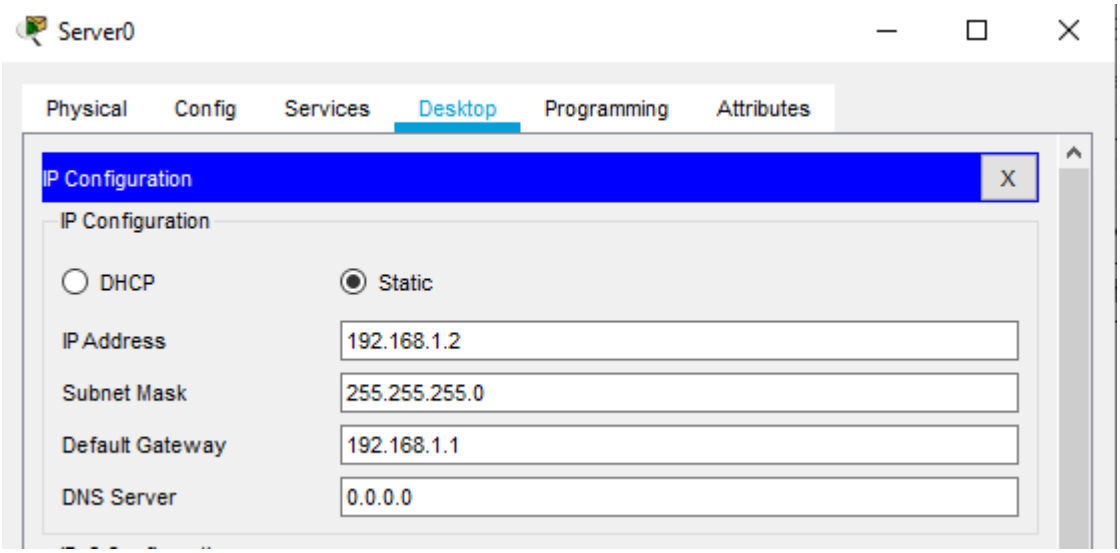


Let us consider the following Address table to configure the network devices:

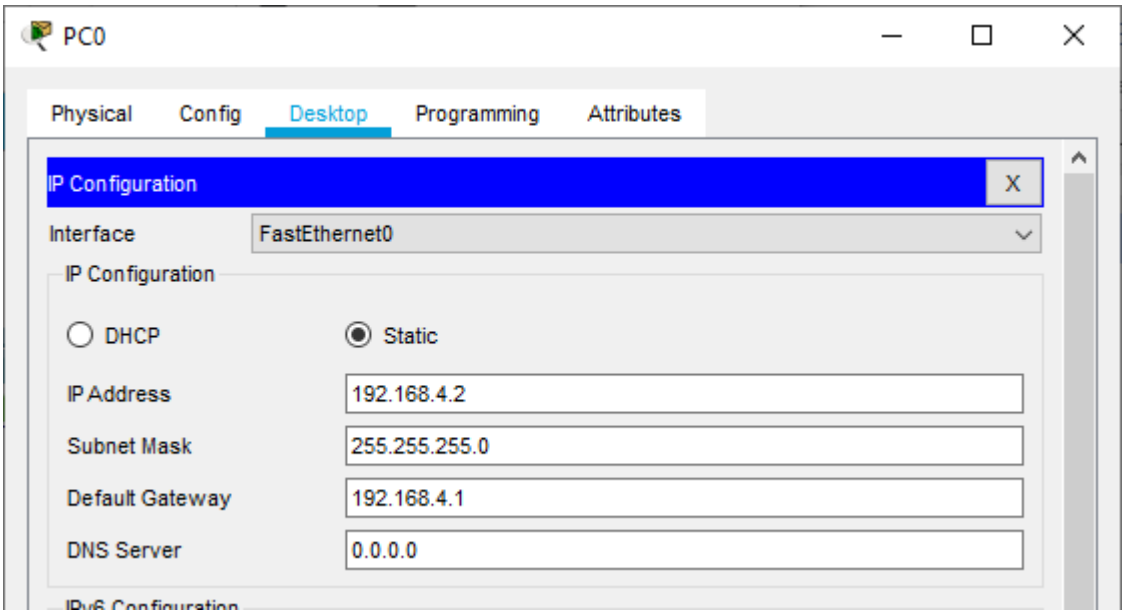
Device	Interface	IP Address	Subnet Mask	Default gateway	Switch Port
PC 0	NA	192.168.4.2	255.255.255.0	192.168.4.1	Switch1 F0/1
Server0	NA	192.168.1.2	255.255.255.0	192.168.1.1	Switch0 F0/1
Router0	GE0/0	192.168.1.1	255.255.255.0	NA	Switch0 F0/5
	S0/1/0	192.168.2.1	255.255.255.0	NA	NA
Router1	S0/1/0	192.168.2.2	255.255.255.0	NA	NA
	S0/1/1	192.168.3.1	255.255.255.0	NA	NA
Router2	S0/1/1	192.168.3.2	255.255.255.0	NA	NA
	GE0/0	192.168.4.1	255.255.255.0	NA	Switch1 F0/5

Part 1 - Verify connectivity among devices before firewall configuration

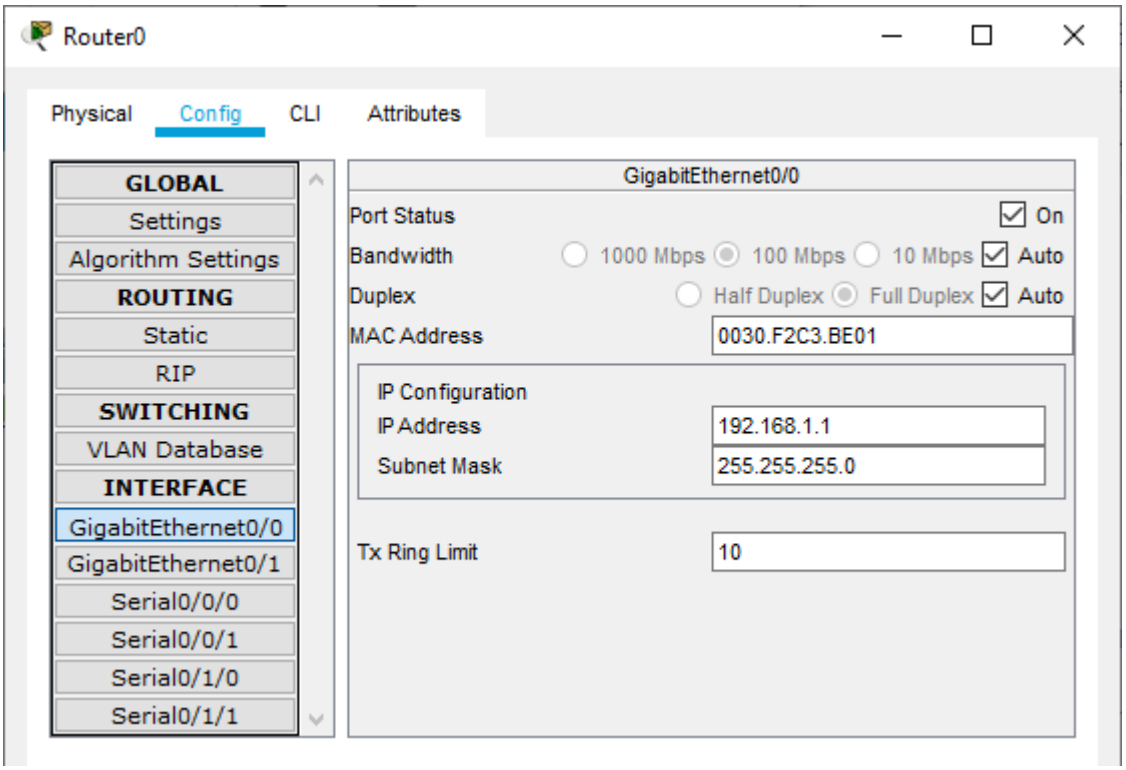
Configuring Server 0

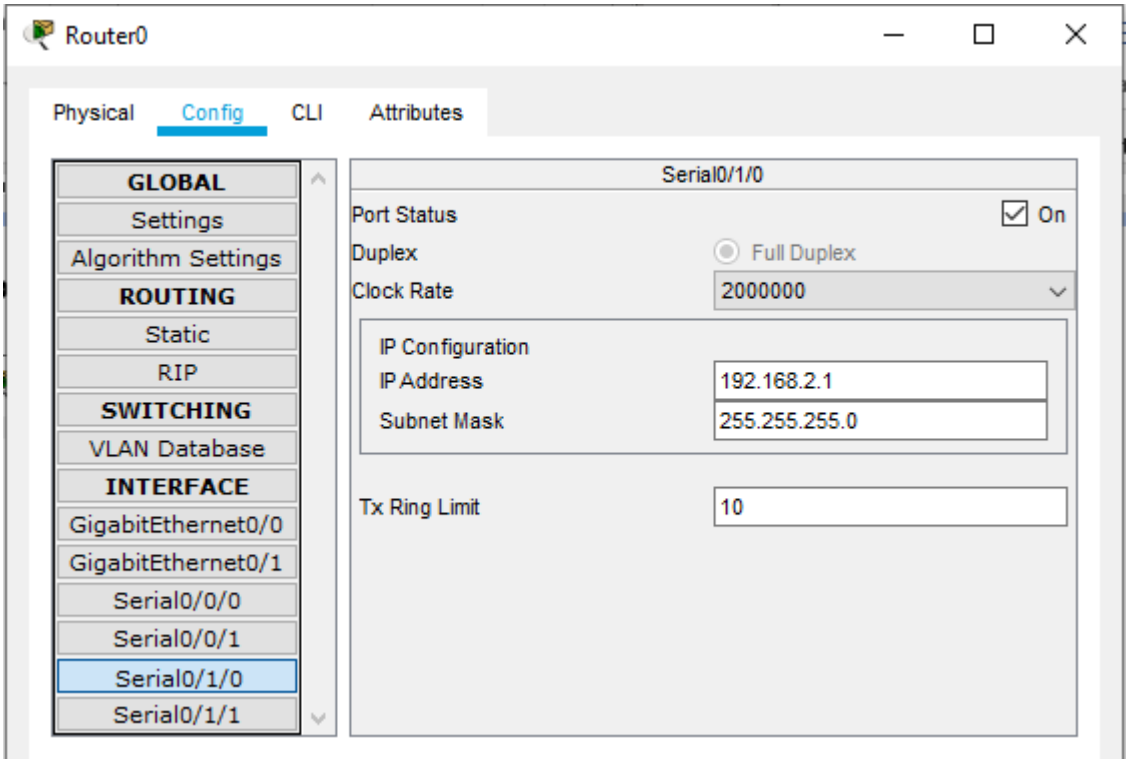


Configuring PC0

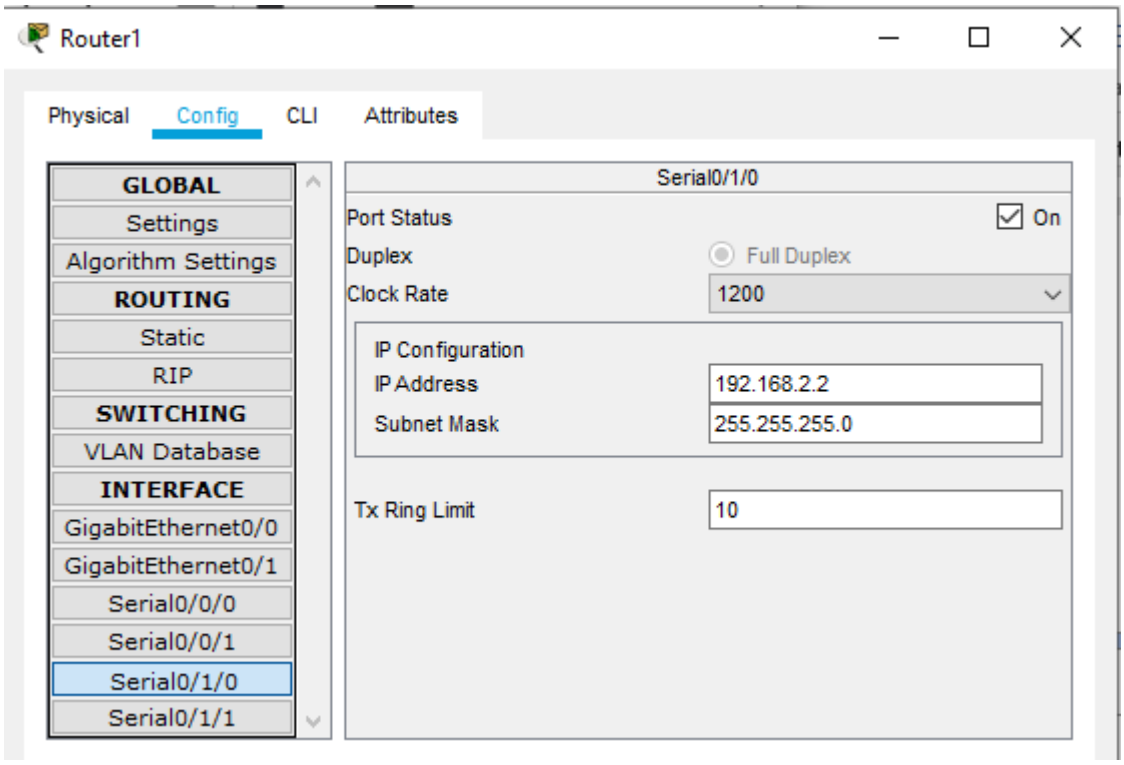


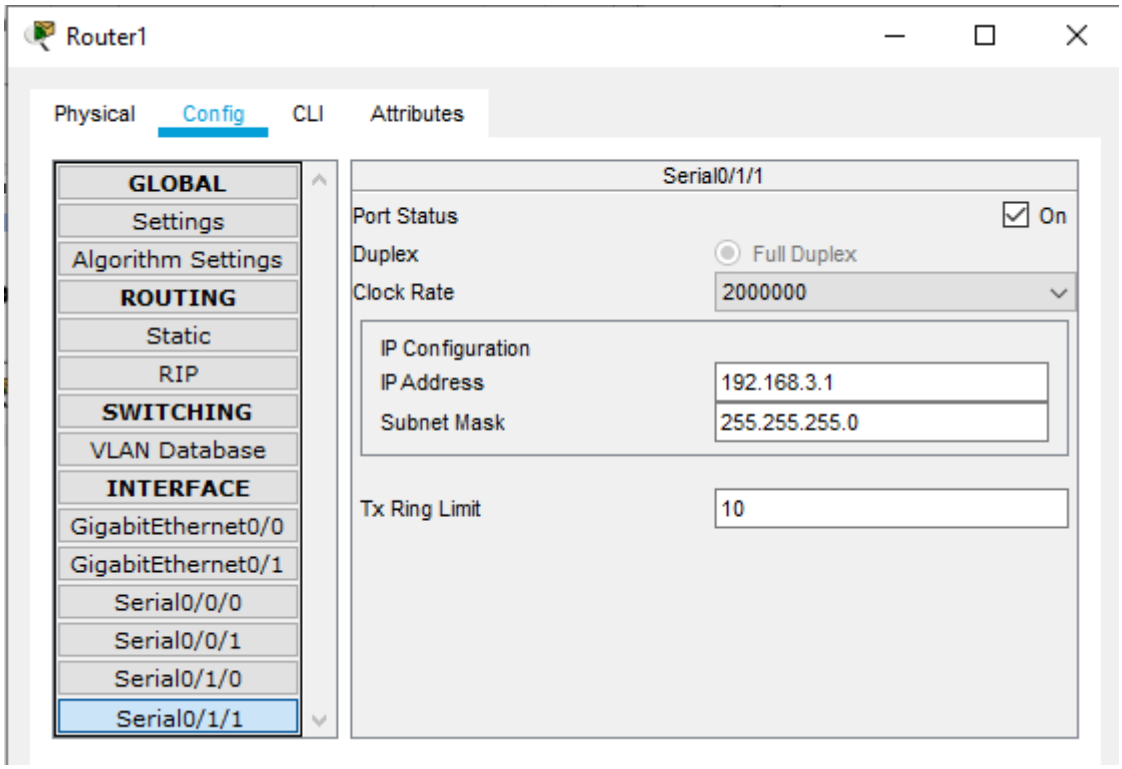
Configuring Router0



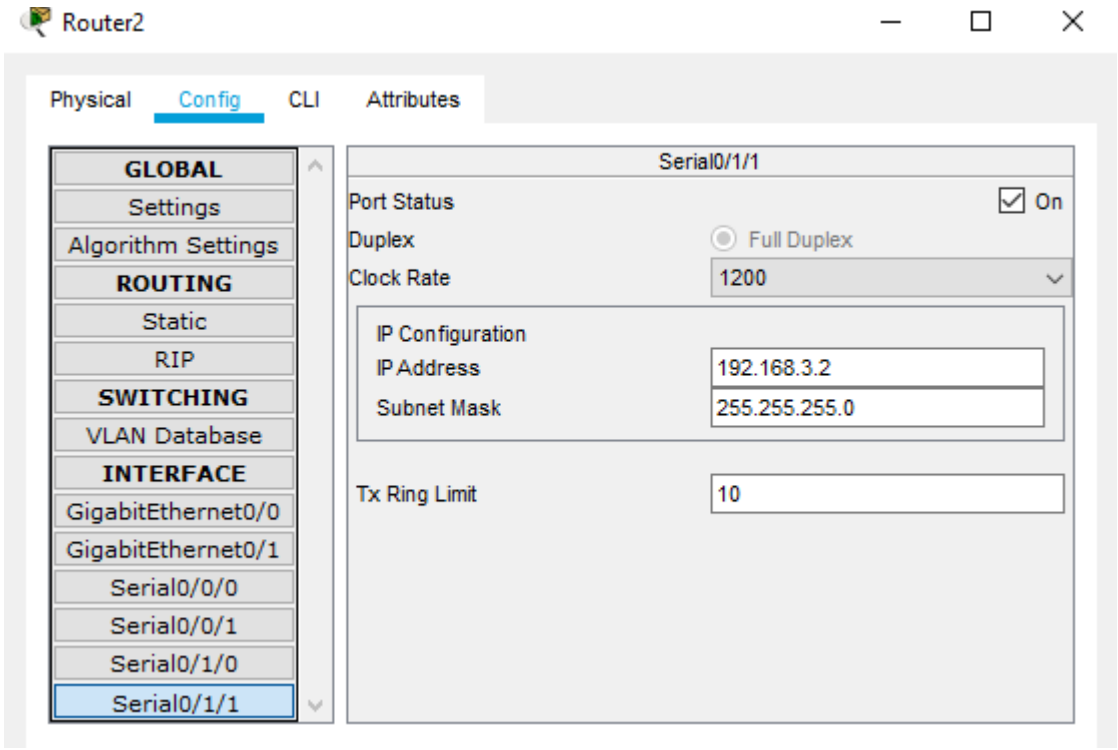


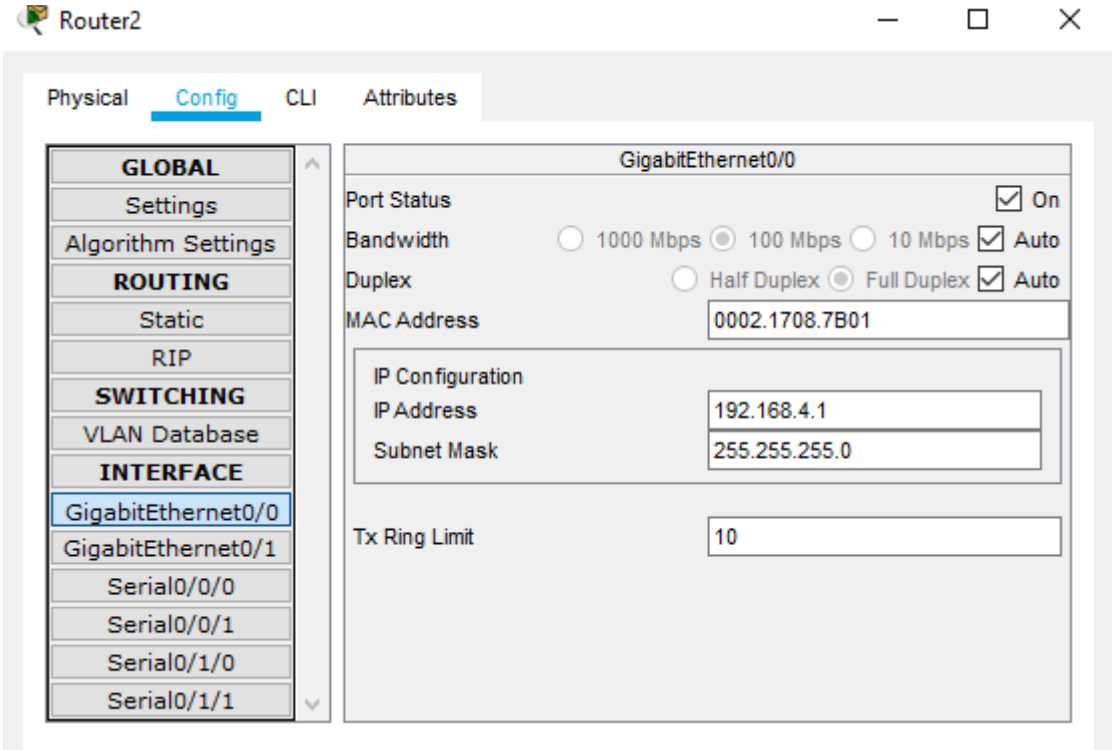
Configuring Router1



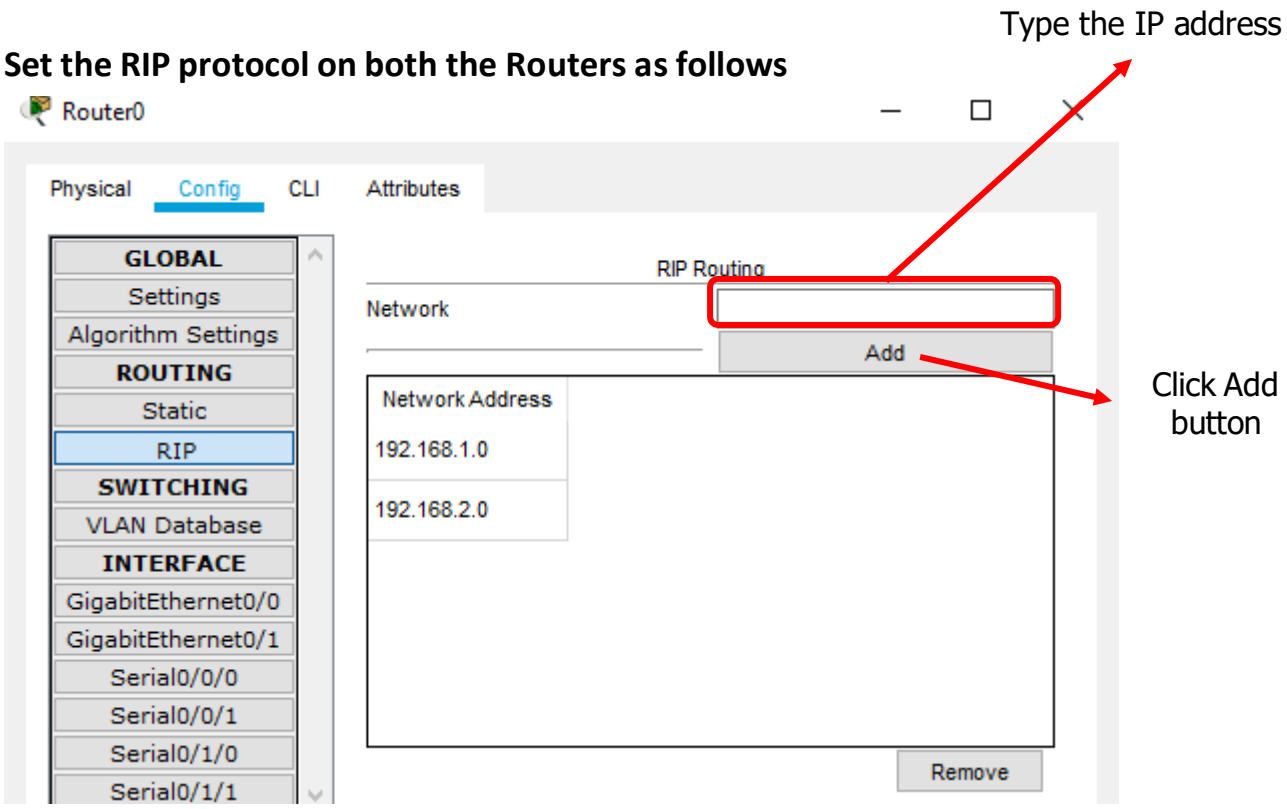


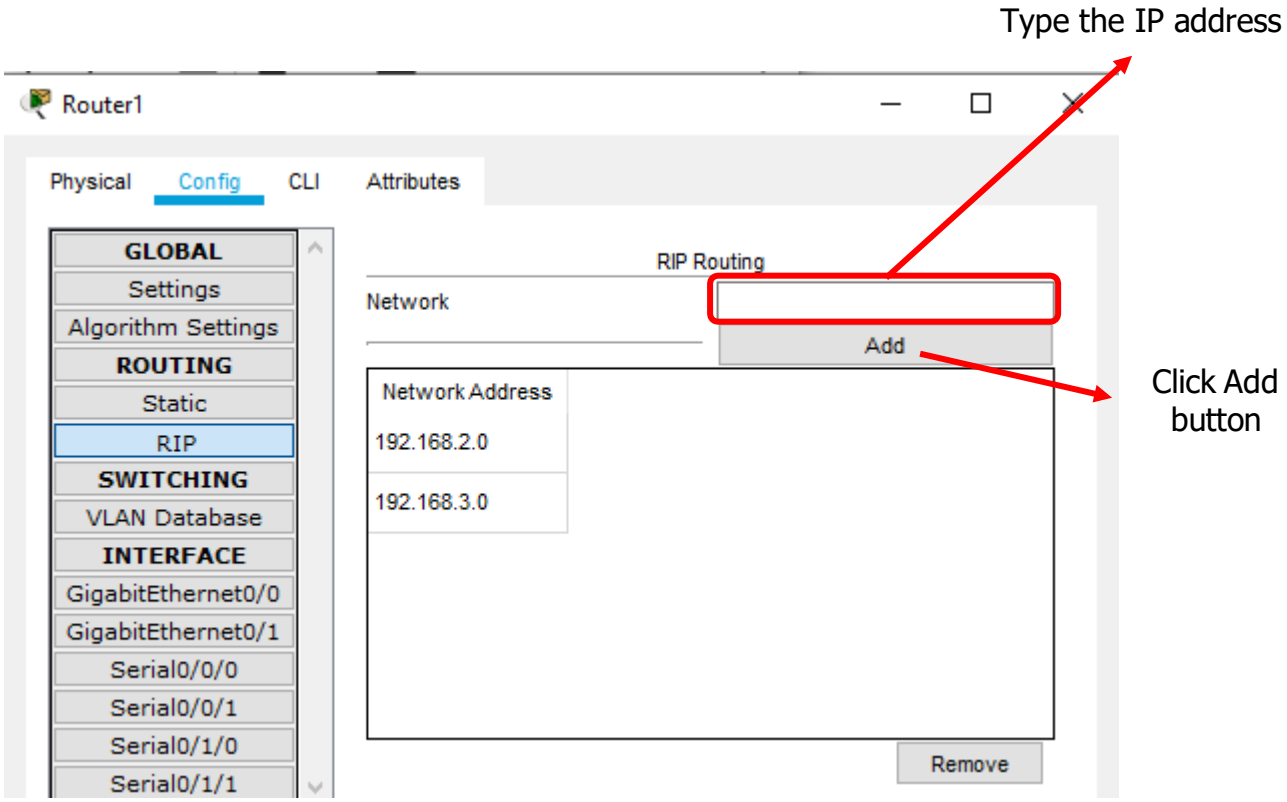
Configuring Router2

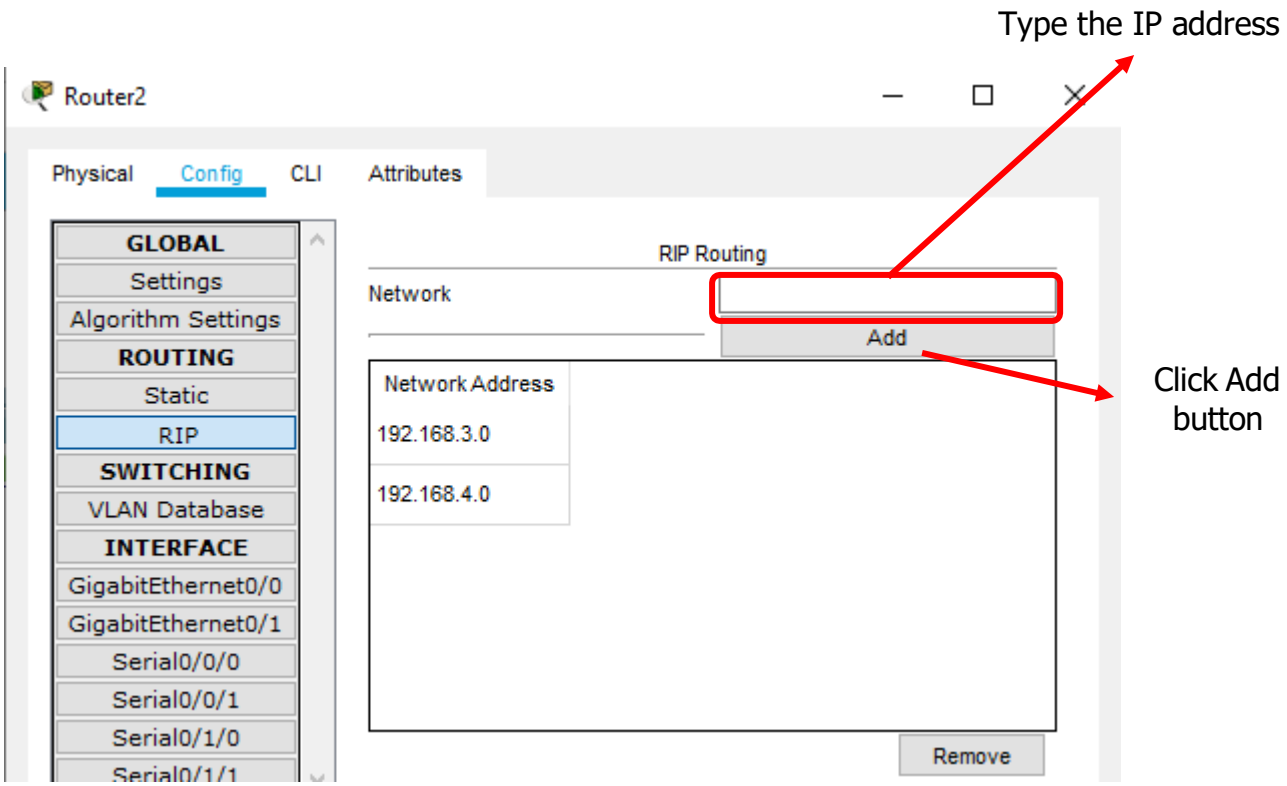




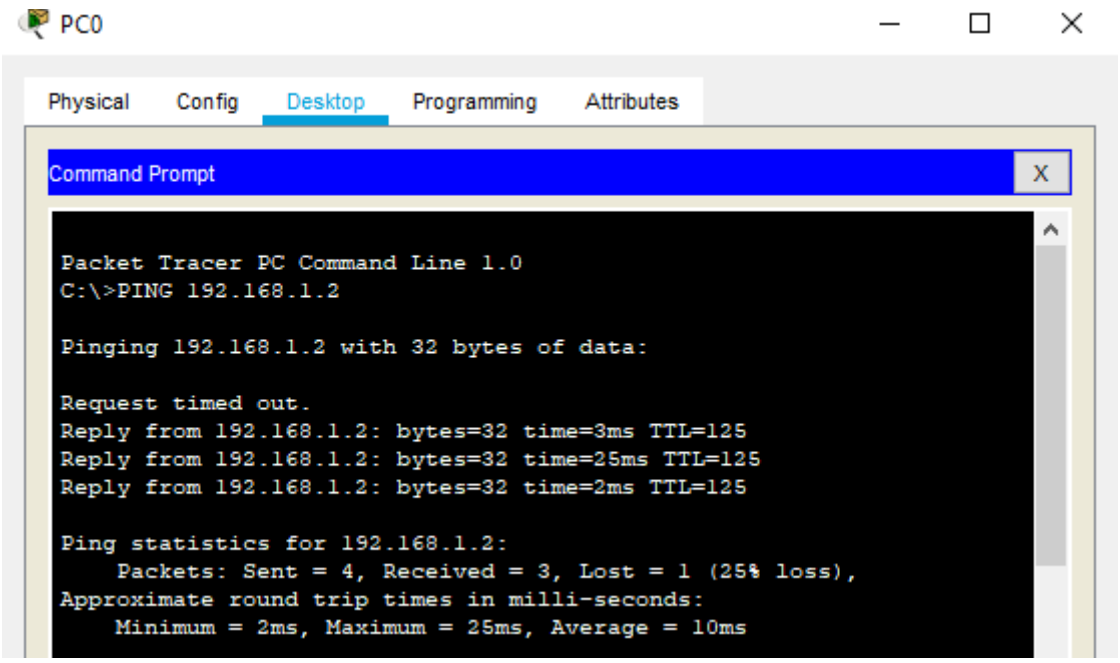
Set the RIP protocol on both the Routers as follows



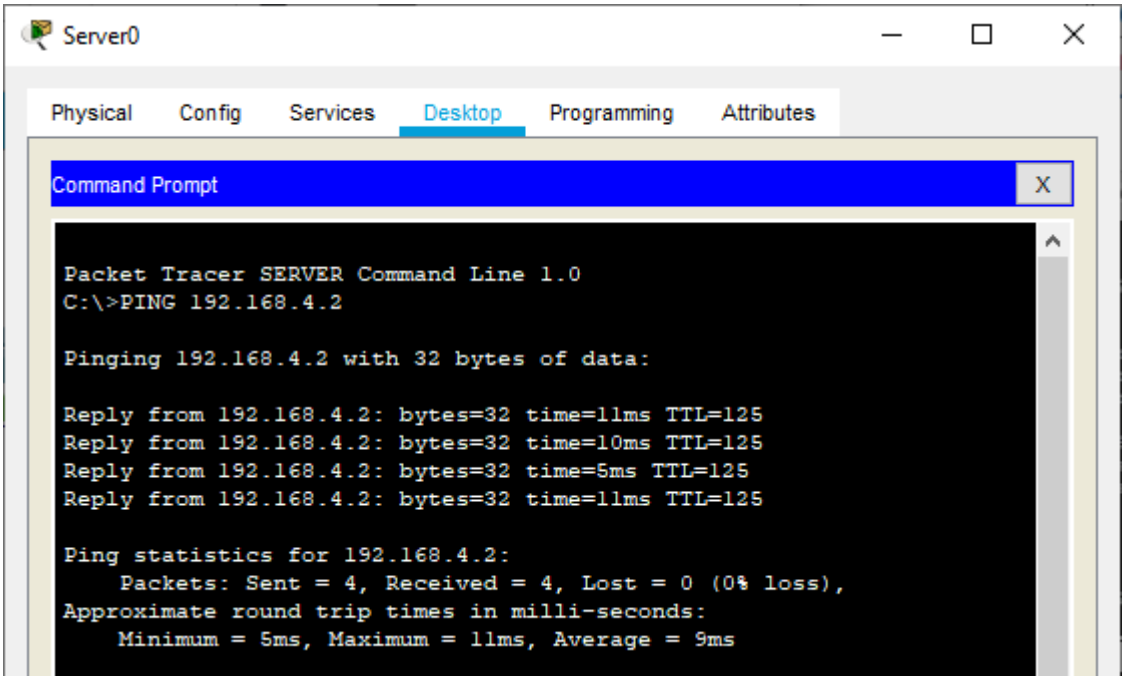




We can now verify the connectivity by pinging Server from PC



We can now verify the connectivity by pinging PC from Server



Part 2 – Secure Access to Routers

We configure ACL 10 to block all remote access to the Routers and allow remote access only from PC. We type the following commands in all the Routers (Router0, Router1, and Router2). This part is divided in 2 subparts

Set up the SSH protocol

Enter the following commands in CLI mode of Router0

```
Router>enable
Router#configure terminal
Router(config)#ip domain-name ismail.com
Router(config)#hostname Router0
Router0(config)#
Router0(config)#crypto key generate rsa
Router0(config)#line vty 0 4
Router0(config-line)#transport input ssh
Router0(config-line)#login local
Router0(config-line)#exit
Router0(config)#username SSHadmin privilege 15 password ismail
Router0(config)#exit
Router0#
```

Enter the following commands in CLI mode of Router1

```
Router>enable
Router#configure terminal
Router(config)#ip domain-name ismail.com
Router(config)#hostname Router1
Router1(config)#
Router1(config)#crypto key generate rsa
Router1(config)#line vty 0 4
Router1(config-line)#transport input ssh
Router1(config-line)#login local
Router1(config-line)#exit
Router1(config)#username SSHadmin privilege 15 password ismail
Router1(config)#exit
Router1#
```

Enter the following commands in CLI mode of Router2

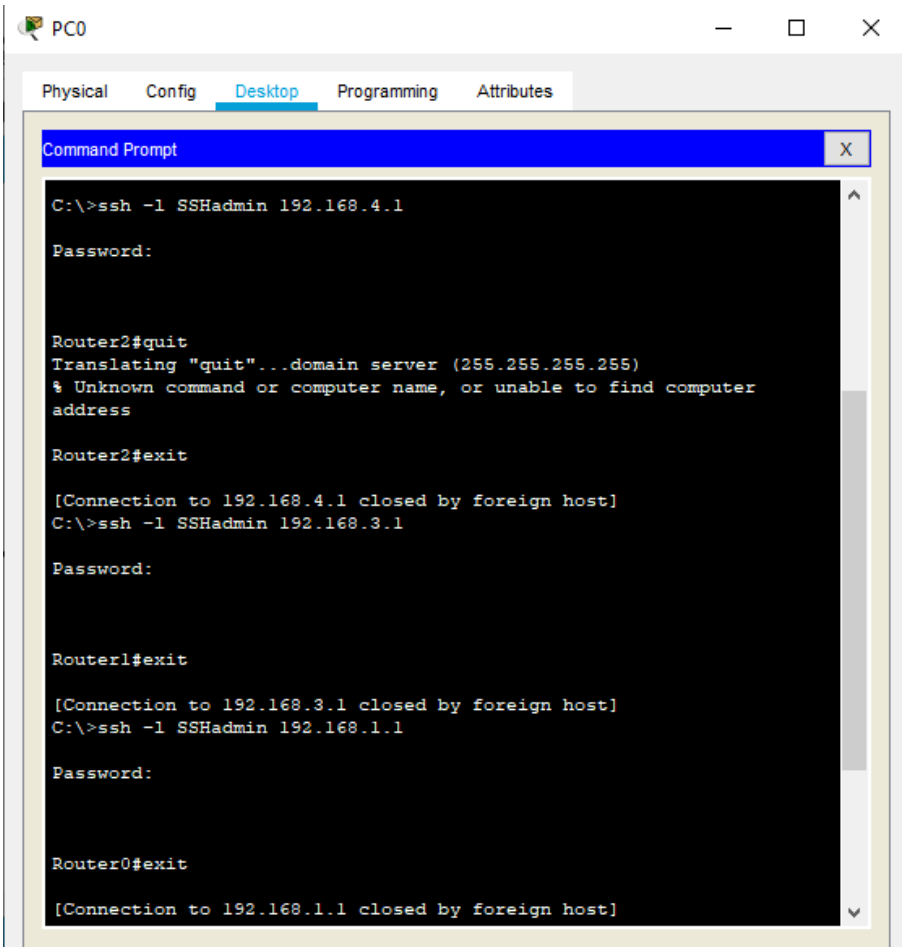
```
Router>enable
Router#configure terminal
```

```
Router(config)#ip domain-name ismail.com
Router(config)#hostname Router2
Router2(config)#
Router2(config)#crypto key generate rsa
Router2(config)#line vty 0 4
Router2(config-line)#transport input ssh
Router2(config-line)#login local
Router2(config-line)#exit
Router2(config)#username SSHadmin privilege 15 password ismail
Router2(config)#exit
Router2#
```

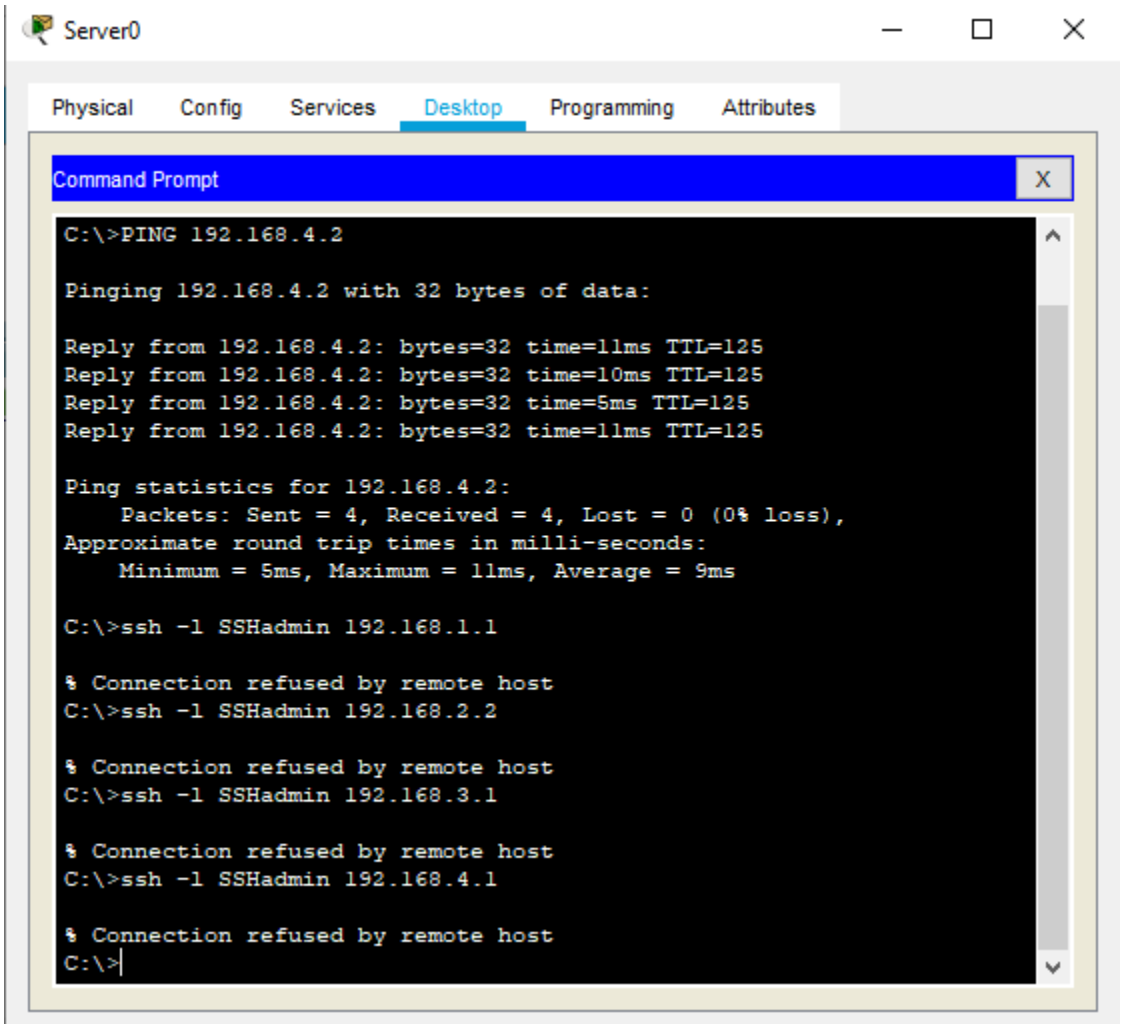
Create an ACL 10 to permit remote access to PC only
Enter the following commands in CLI mode of all Routers

```
Router>enable
Router#configure terminal
Router(config)#access-list 10 permit host 192.168.4.2
Router(config)#line vty 0 4
Router(config-line)#access-class 10 in
```

Now we verify the remote access from PC using the following and find it to be successful



Now we verify the remote access from Server using the following and find it to be failure


Server0
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
X
C:\>PING 192.168.4.2
Pinging 192.168.4.2 with 32 bytes of data:
Reply from 192.168.4.2: bytes=32 time=11ms TTL=125
Reply from 192.168.4.2: bytes=32 time=10ms TTL=125
Reply from 192.168.4.2: bytes=32 time=5ms TTL=125
Reply from 192.168.4.2: bytes=32 time=11ms TTL=125
Ping statistics for 192.168.4.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 5ms, Maximum = 11ms, Average = 9ms
C:\>ssh -l SSHadmin 192.168.1.1
% Connection refused by remote host
C:\>ssh -l SSHadmin 192.168.2.2
% Connection refused by remote host
C:\>ssh -l SSHadmin 192.168.3.1
% Connection refused by remote host
C:\>ssh -l SSHadmin 192.168.4.1
% Connection refused by remote host
C:\>

Part 3 - Create a Numbered IP ACL 120 on R1

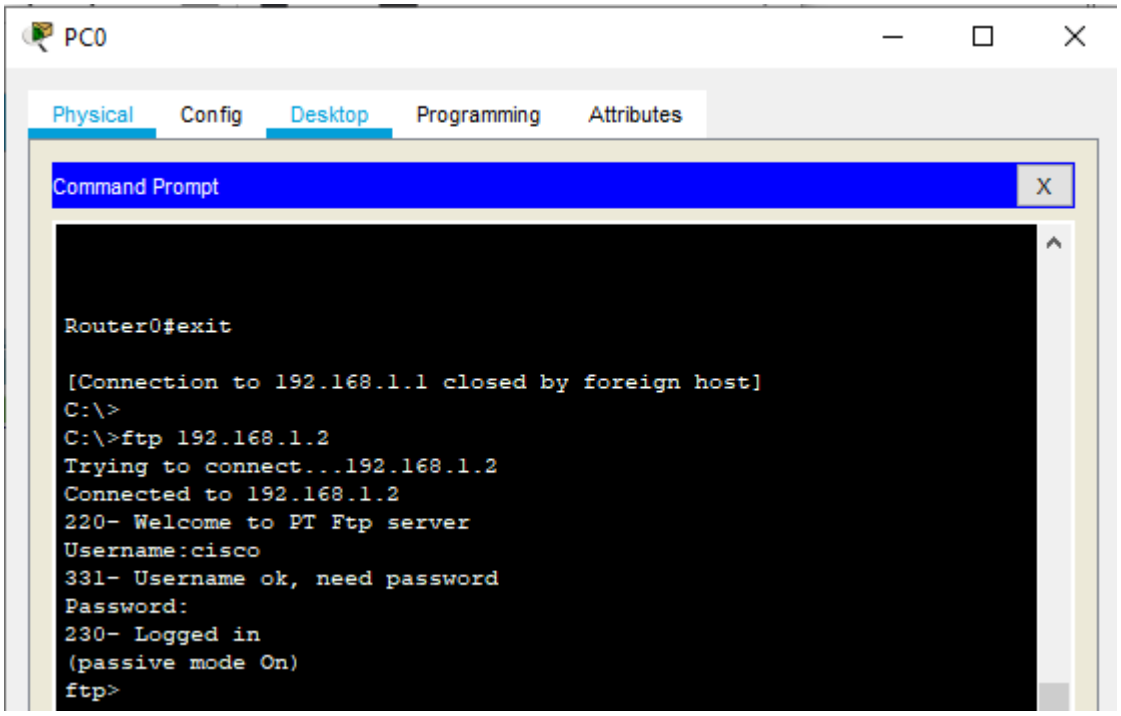
We need to perform the following in this part

1) Create an IP ACL numbered 120 on R1 using the following rules
2) Permit any outside host to access DNS, SMTP, and FTP services on server
3) Deny any outside host access to HTTPS services on **server**
4) Permit PC to access Router1 via SSH. (Done in previous part)

Enter the following commands in the CLI mode of Router1

```
Router1>enable
Router1#
Router1#configure terminal
Router1(config)#access-list 120 permit udp any host 192.168.1.2 eq domain
Router1(config)#access-list 120 permit tcp any host 192.168.1.2 eq smtp
Router1(config)#access-list 120 permit tcp any host 192.168.1.2 eq ftp
Router1(config)#access-list 120 deny tcp any host 192.168.1.2 eq 443
Router1(config)#exit
Router1#configure terminal
Router1(config)#interface Serial0/1/1
Router1(config-if)#ip access-group 120 in
```

Verify the above entering the following commands in the PC



Hence, we have applied and verified all the required ACLs

Configuring IPv6 ACLs

Access Control Lists for IPv6 Traffic Filtering

The standard ACL functionality in IPv6 is similar to standard ACLs in IPv4. Access lists determine what traffic is blocked and what traffic is forwarded at device interfaces and allow filtering based on source and destination addresses, inbound and outbound to a specific interface. Each access list has an implicit deny statement at the end. IPv6 ACLs are defined and their deny and permit conditions are set using the **ipv6 access-list** command with the deny and **permit** keywords in global configuration mode.

IPv6 extended ACLs augments standard IPv6 ACL functionality to support traffic filtering based on IPv6 option headers and optional, upper-layer protocol type information for finer granularity of control (functionality similar to extended ACLs in IPv4).

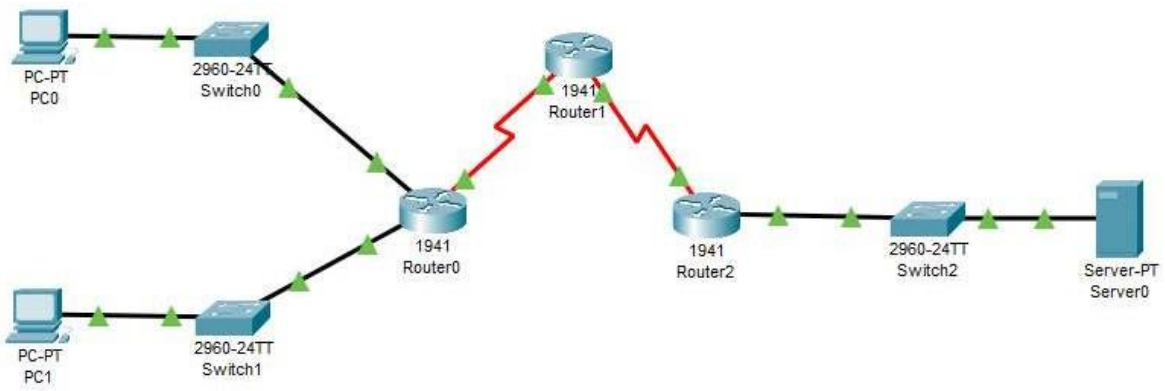
IPv6 Packet Inspection

The following header fields are used for IPv6 inspection: traffic class, flow label, payload length, next header, hop limit, and source or destination IP address. For further information on and descriptions of the IPv6 header fields, see RFC 2474.

Access Class Filtering in IPv6

Filtering incoming and outgoing connections to and from the device based on an IPv6 ACL is performed using the **ipv6 access-class** command in line configuration mode. The **ipv6 access- class** command is similar to the **access-class** command, except the IPv6 ACLs are defined by a name. If the IPv6 ACL is applied to inbound traffic, the source address in the ACL is matched against the incoming connection source address and the destination address in the ACL is matched against the local device address on the interface. If the IPv6 ACL is applied to outbound traffic, the source address in the ACL is matched against the local device address on the interface and the destination address in the ACL is matched against the outgoing connection source address. We recommend that identical restrictions are set on all the virtual terminal lines because a user can attempt to connect to any of them.

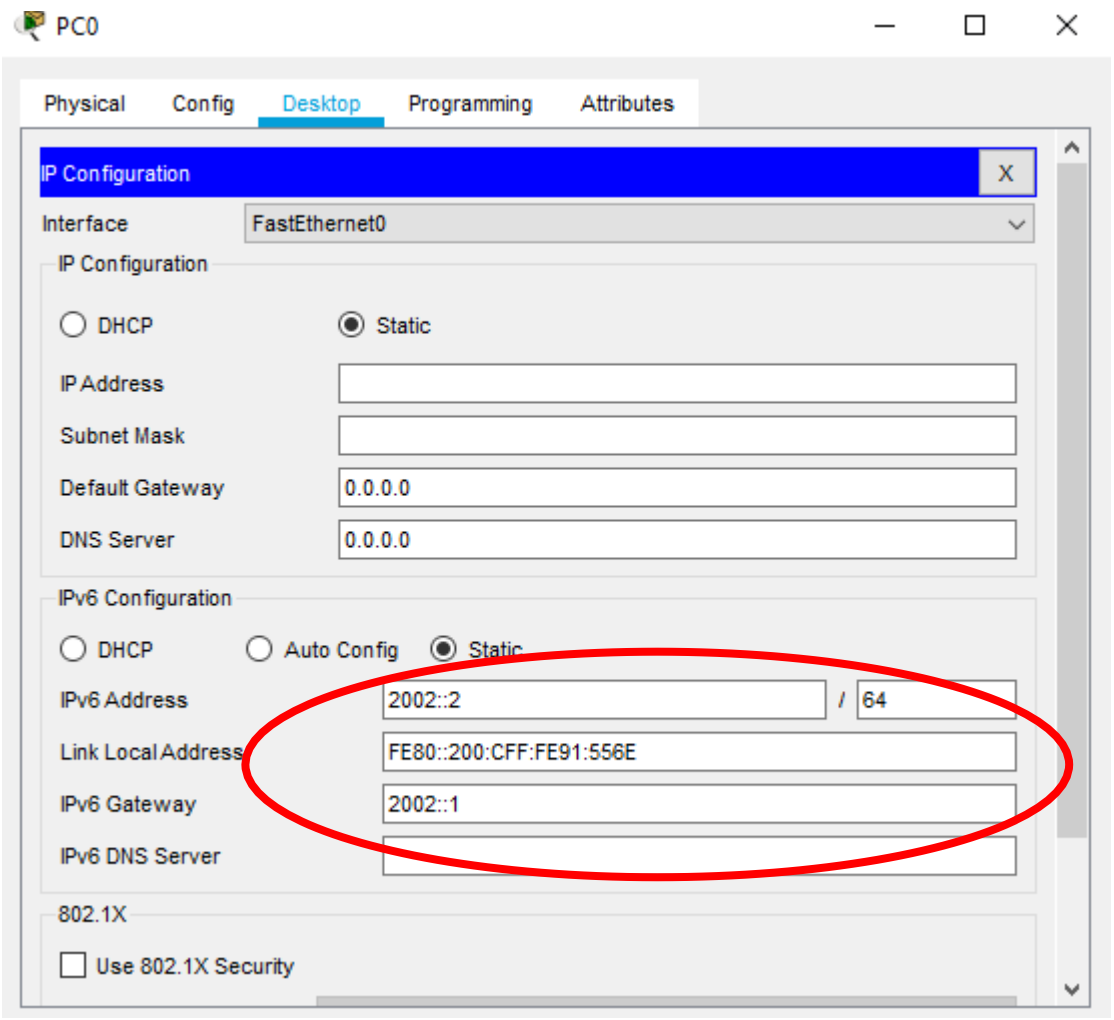
We use the following topology



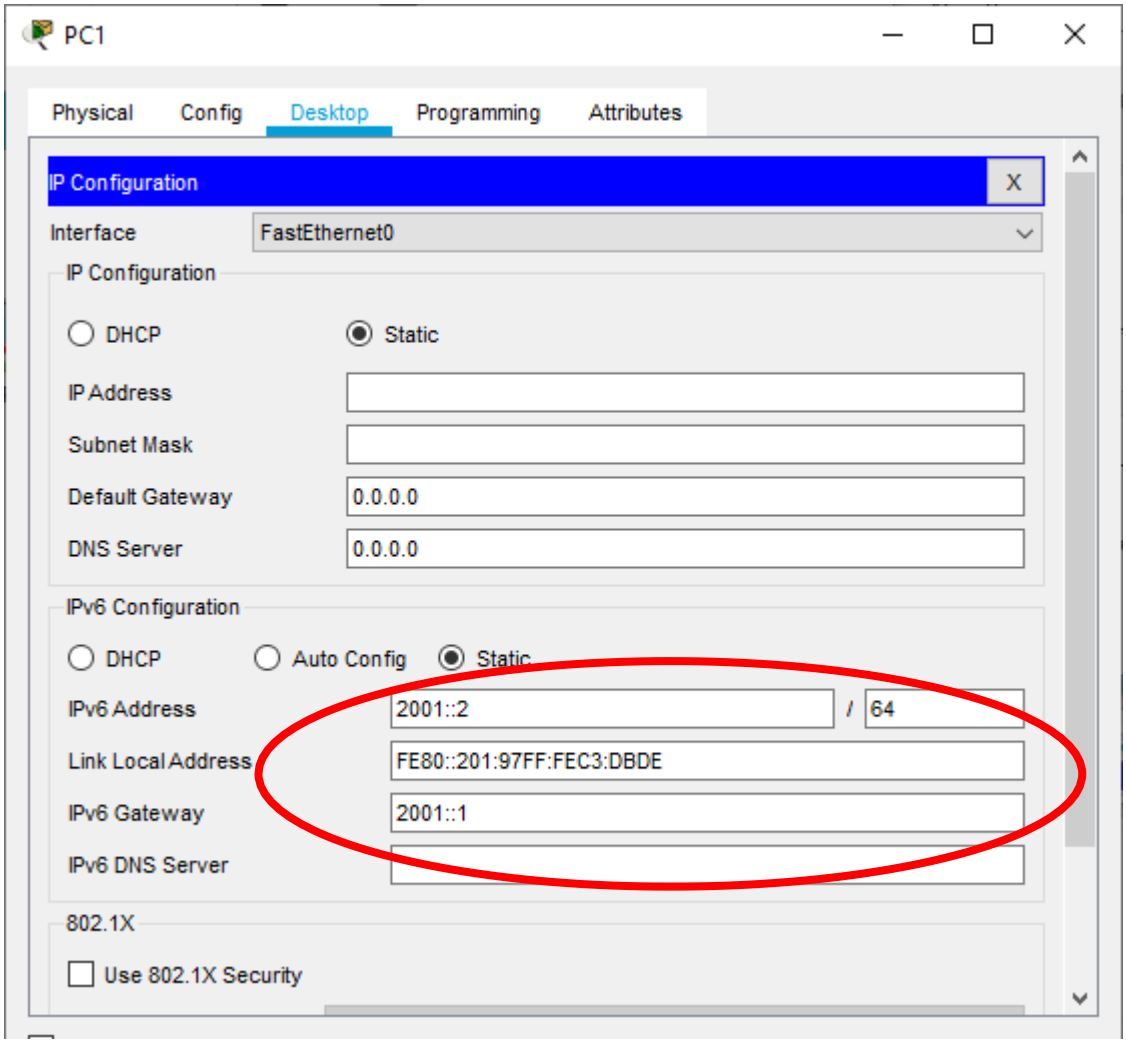
Let us consider the following Address table to configure the network devices:

Device	Interface	IPv6 Address	IPv6 gateway	Switch Port
PC 0	NA	2002::2 / 64	2002::1	Switch0 F0/1
PC 1	NA	2001::2 / 64	2001::1	Switch1 F0/1
Server0	NA	2005::2 / 64	2005::1	Switch2 F0/1
Router0	GE0/0	2002::1 / 64	NA	Switch0 F0/5
	GE0/1	2001::1 / 64	NA	Switch1 F0/5
	S0/1/0	2003::1 / 64	NA	NA
Router1	S0/1/0	2003::1 / 64	NA	NA
	S0/1/1	2004::1 / 64	NA	NA
Router2	S0/1/1	2004::2 / 64	NA	NA
	GE0/0	2005::1 / 64	NA	Switch2 F0/5

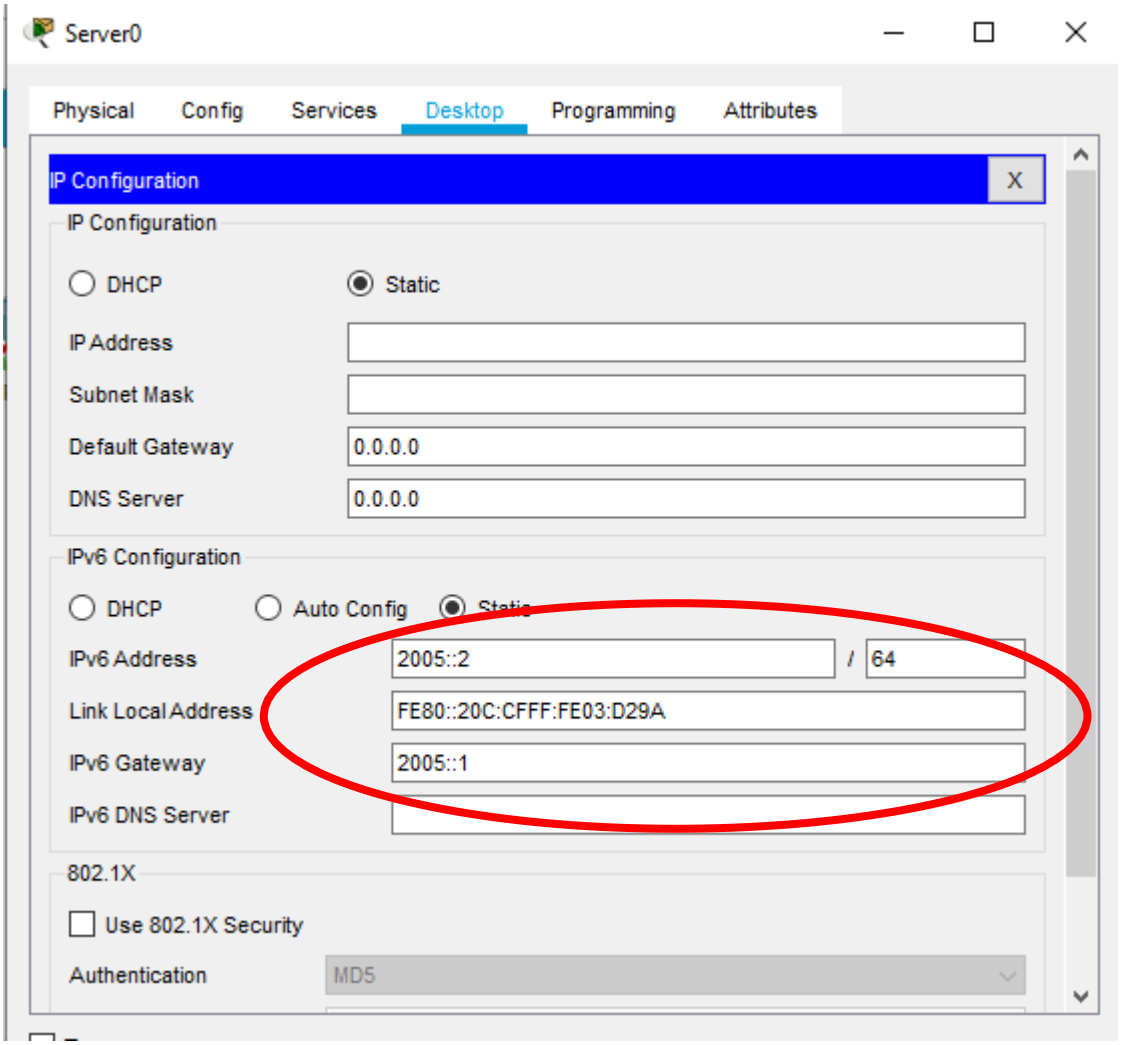
Configuring PC0



Configuring PC1



Configuring Server0



For setting the ipv6 addresses we need to use the CLI mode for each Router as follows

Configuring Router0

```
Router>
Router>enable
Router#
Router#configure terminal
Router(config)#ipv6 unicast-routing

Router(config)#interface GigabitEthernet0/0
Router(config-if)#ipv6 address 2002::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#

Router(config)#interface GigabitEthernet0/1
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)#

Router(config)#interface Serial0/1/0
Router(config-if)#ipv6 address 2003::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

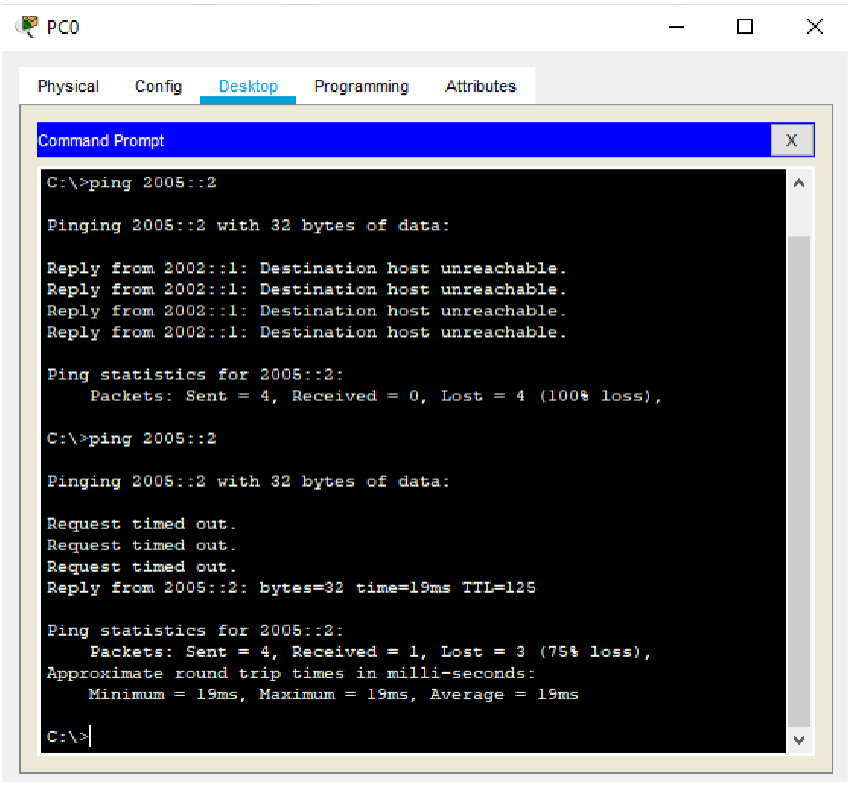
Configuring Router1

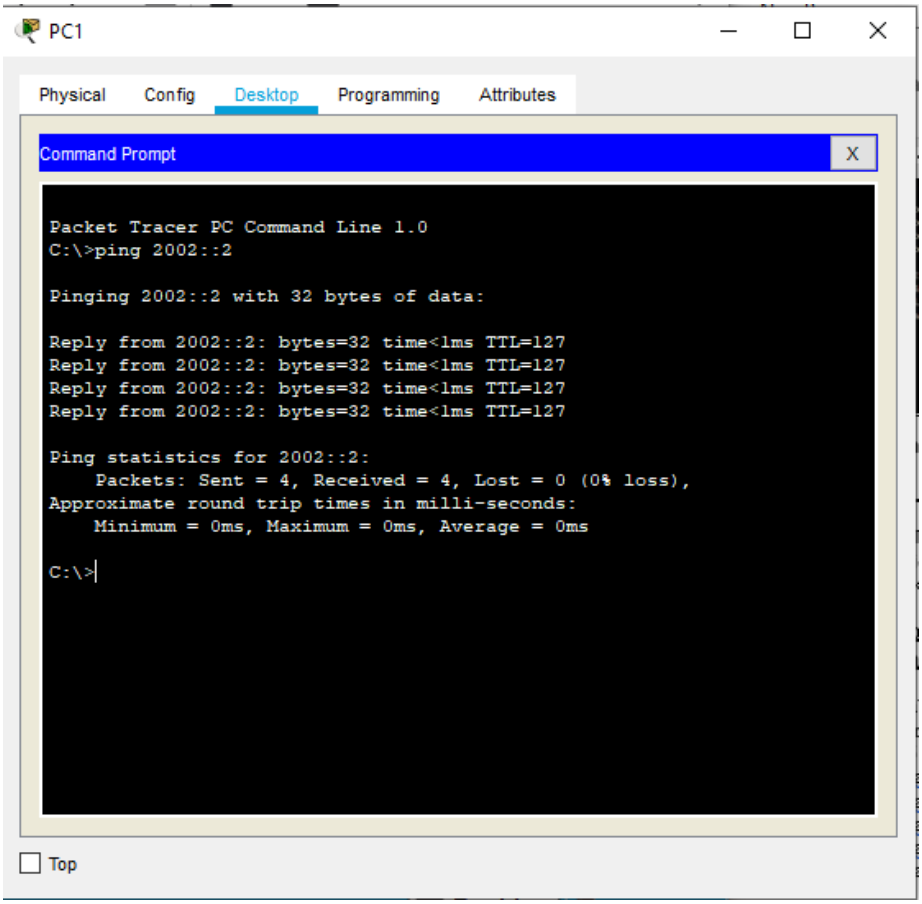
```
Router>enable
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)#

Router(config)#interface Serial0/1/0
Router(config-if)#ipv6 address 2003::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#
Router(config-if)#exit
Router(config)#

Router(config)#interface Serial0/1/1
Router(config-if)#ipv6 address 2004::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

Configuring Router2

```
Router>enable
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)#

Router(config)#interface Serial0/1/1
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 GigabitEthernet0/0
Router(config-if)#ipv6 address 2005::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

Check the connectivity by pinging from PCs to Server





And we see that the connectivity is established

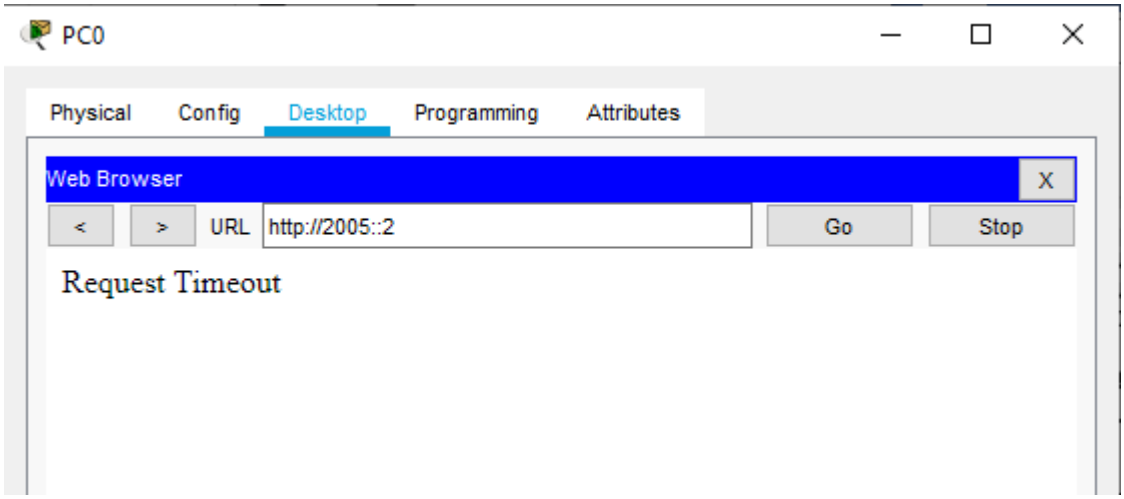
We configure the ACL and apply it to the Router1 with the following conditions

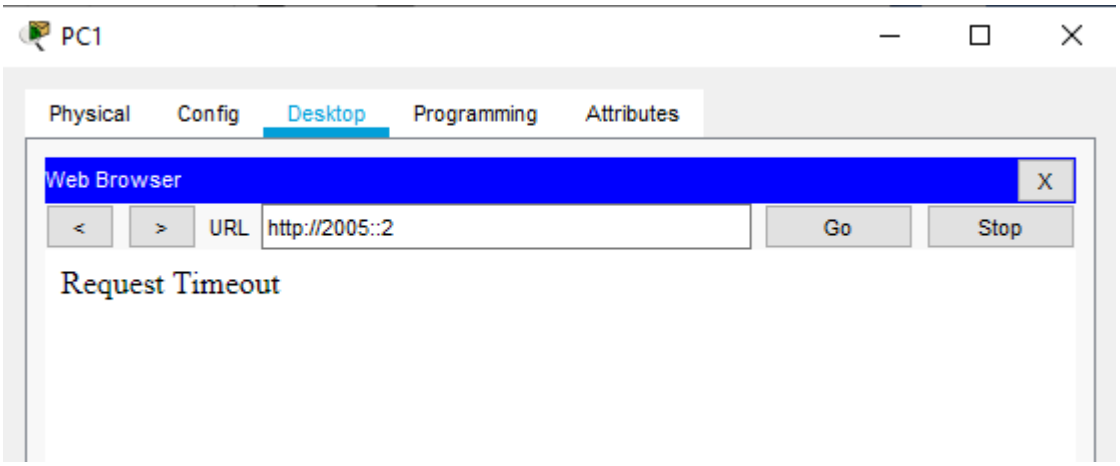
1) No HTTP or HTTPS allowed on server by any host
2) No www service accessible on the server by any host
3) Only ipv6 packets allowed towards the server

We enter the following commands in the CLI mode of the Router1 and Router2, apply it at the proper interface

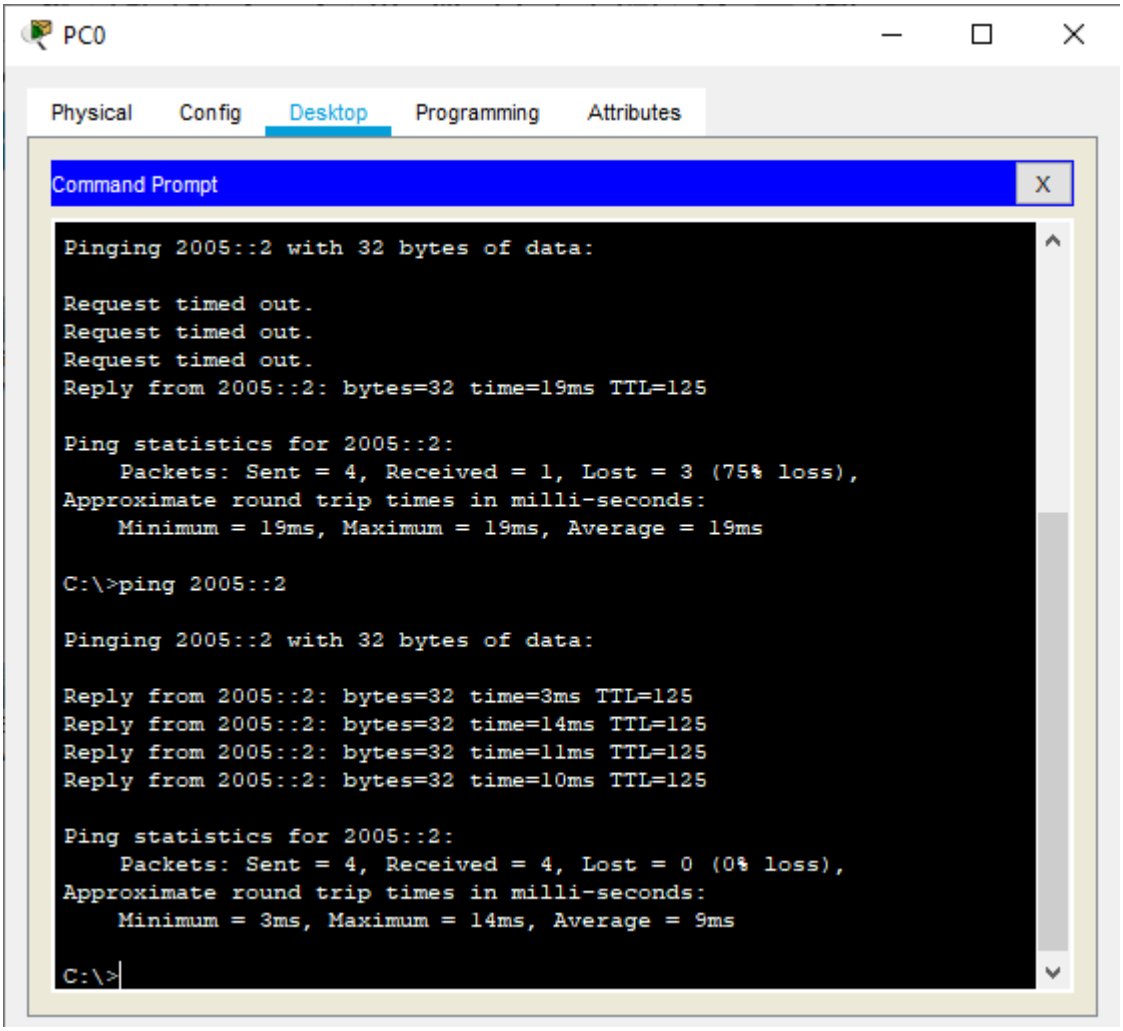
```
Router>
Router>enable
Router#configure terminal
Router(config)#ipv6 access-list smile
Router(config-ipv6-acl)#deny tcp any host 2005::2 eq www
Router(config-ipv6-acl)#deny tcp any host 2005::2 eq 443
Router(config-ipv6-acl)#permit ipv6 any any
Router(config-ipv6-acl)# Router(config-ipv6-acl)#exit

Router(config)# Router(config)#interface Serial0/1/1
Router(config-if)#ipv6 traffic-filter smile in
Router(config-if)#exit
Router(config)#
```

We verify the configuration by first accessing the www service from the browser of both PCs and get failure





Next we verify whether the ipv6 protocol works by pinging server from any of the PC (it must be successful)



Hence the given ACLs have been applied and verified on host running on ipv6 protocol.

\

PRACTICAL NO 5: Configuring a Zone-Based Policy Firewall (ZPF)

Cisco IOS® Software Release 12.4(6)T introduced Zone-Based Policy Firewall (ZFW), a new configuration model for the Cisco IOS Firewall feature set. This new configuration model offers intuitive policies for multiple-interface routers, increased granularity of firewall policy application, and a default deny-all policy that prohibits traffic between firewall security zones until an explicit policy is applied to allow desirable traffic.

Nearly all classic Cisco IOS Firewall features implemented before Cisco IOS Software Release 12.4(6)T are supported in the new zone-based policy inspection interface:

1) Stateful packet inspection
2) VRF-aware Cisco IOS Firewall
3) URL filtering
4) Denial-of-Service (DoS) mitigation

Cisco IOS Software Release 12.4(9)T added ZFW support for per-class session/connection and throughput limits, as well as application inspection and control:

1) HTTP
2) Post Office Protocol (POP3),
3) Internet Mail Access Protocol (IMAP),
4) Simple Mail Transfer Protocol / Enhanced Simple Mail Transfer Protocol (SMTP/ESMTP)
5) Sun Remote Procedure Call (RPC)
6) Instant Messaging (IM) applications:
    i) Microsoft Messenger
    ii) Yahoo! Messenger
    iii) AOL Instant Messenger
7) Peer-to-Peer (P2P) File Sharing:
    i) Bittorrent ii) KaZaA iii) Gnutella iv) eDonkey

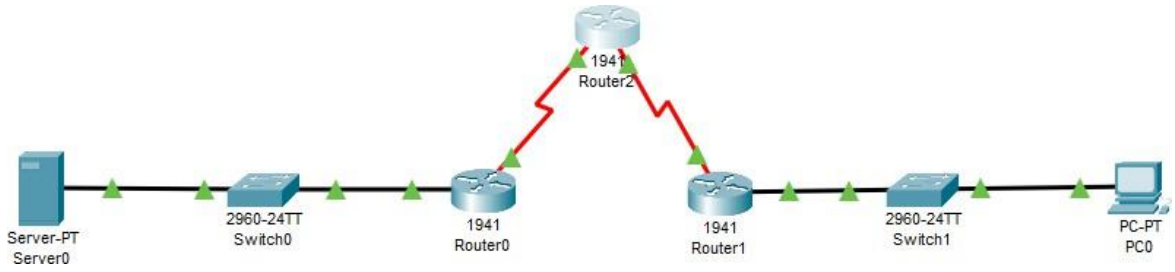
Cisco IOS Software Release 12.4(11)T added statistics for easier DoS protection tuning.

Some Cisco IOS Classic Firewall features and capabilities are not yet supported in a ZFW in Cisco IOS Software Release 12.4(15)T:

i) Authentication proxy
ii) Stateful firewall failover
iii) Unified firewall MIB
iv) IPv6 stateful inspection
v) TCP out-of-order support

ZFW generally improves Cisco IOS performance for most firewall inspection activities. Neither Cisco IOS ZFW or Classic Firewall include stateful inspection support for multicast traffic.

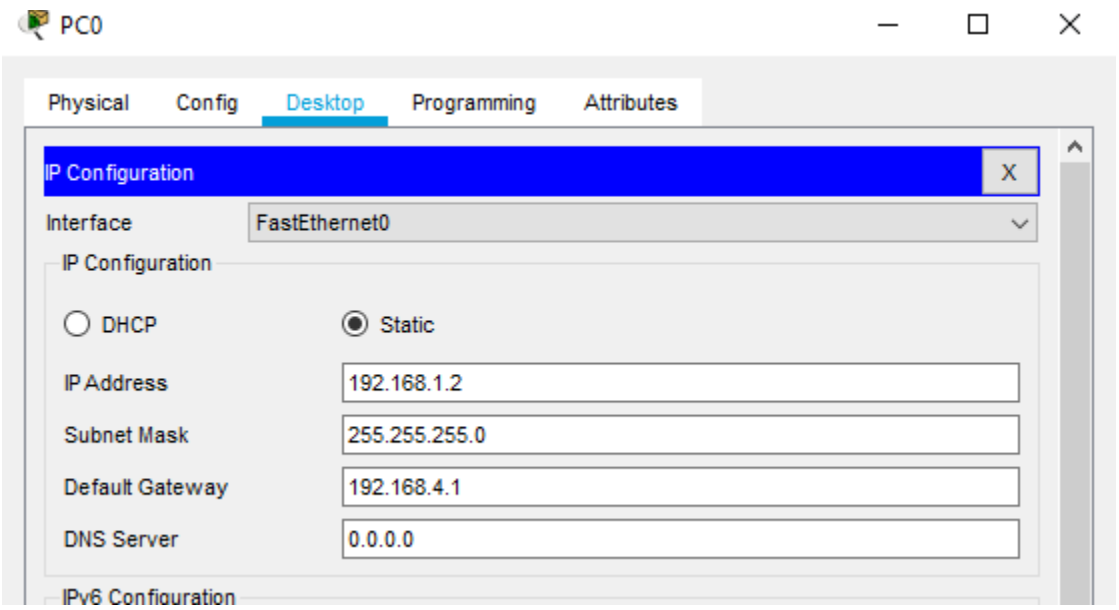
We use the following topology



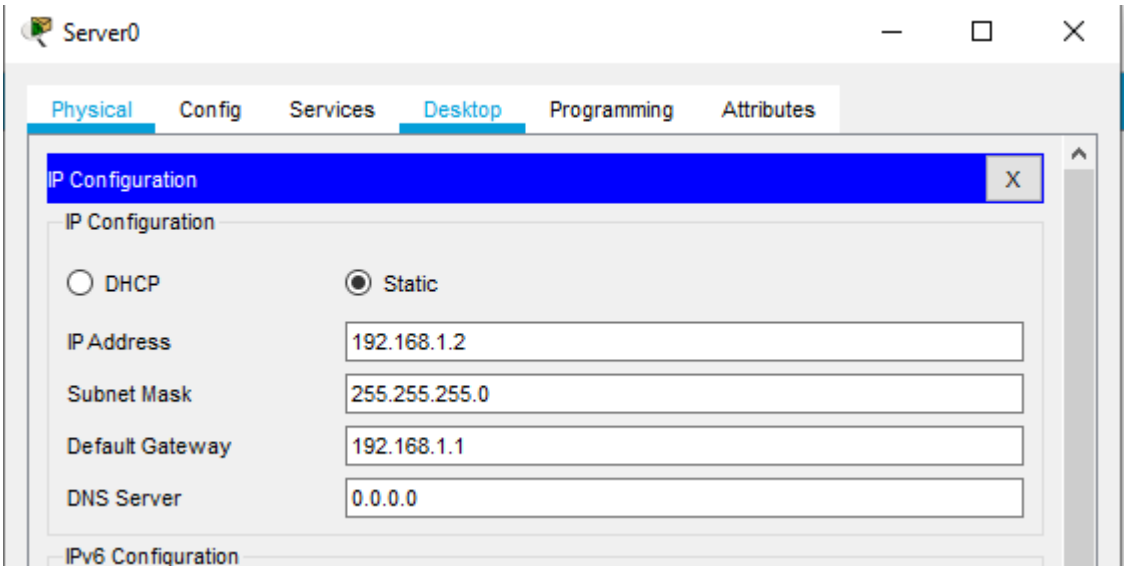
Let us consider the following Address table to configure the network devices:

Device	Interface	IP Address	Subnet Mask	Default gateway	Switch Port
PC 0	NA	192.168.4.2	255.255.255.0	192.168.4.1	Switch1 F0/1
Server0	NA	192.168.1.2	255.255.255.0	192.168.1.1	Switch0 F0/1
Router0	GE0/0	192.168.1.1	255.255.255.0	NA	Switch0 F0/5
	S0/1/0	192.168.2.1	255.255.255.0	NA	NA
Router2	S0/1/0	192.168.2.2	255.255.255.0	NA	NA
	S0/1/1	192.168.3.1	255.255.255.0	NA	NA
Router1	S0/1/1	192.168.3.2	255.255.255.0	NA	NA
	GE0/0	192.168.4.1	255.255.255.0	NA	Switch1 F0/5

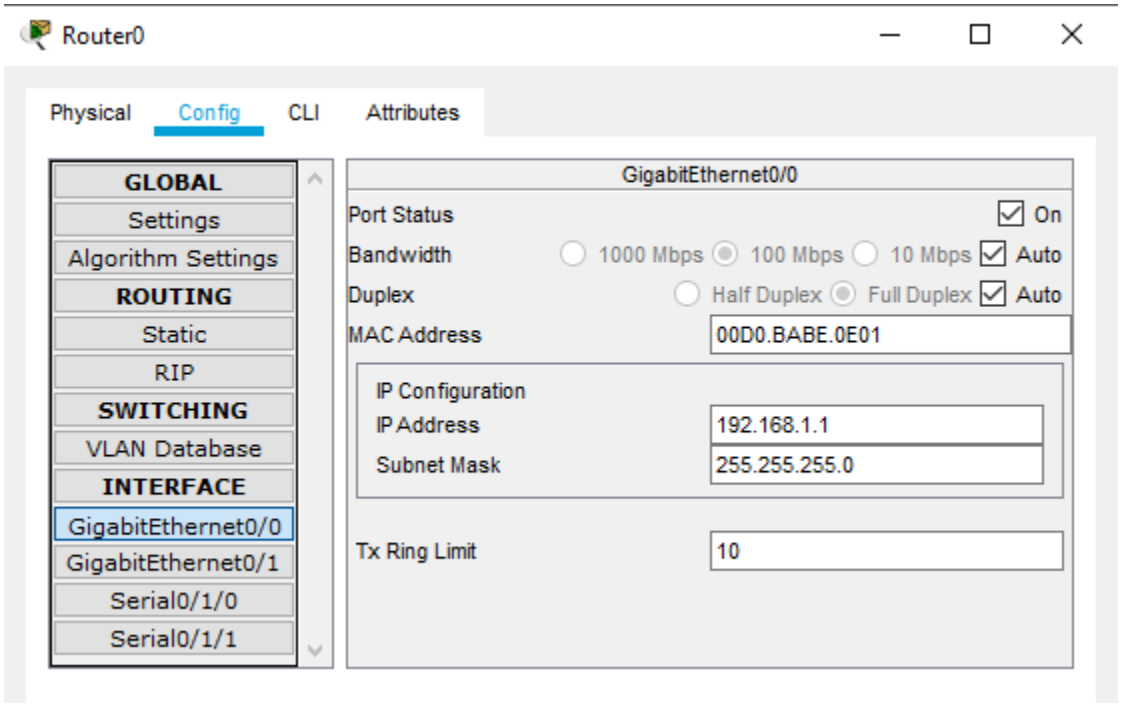
Configuring PC0

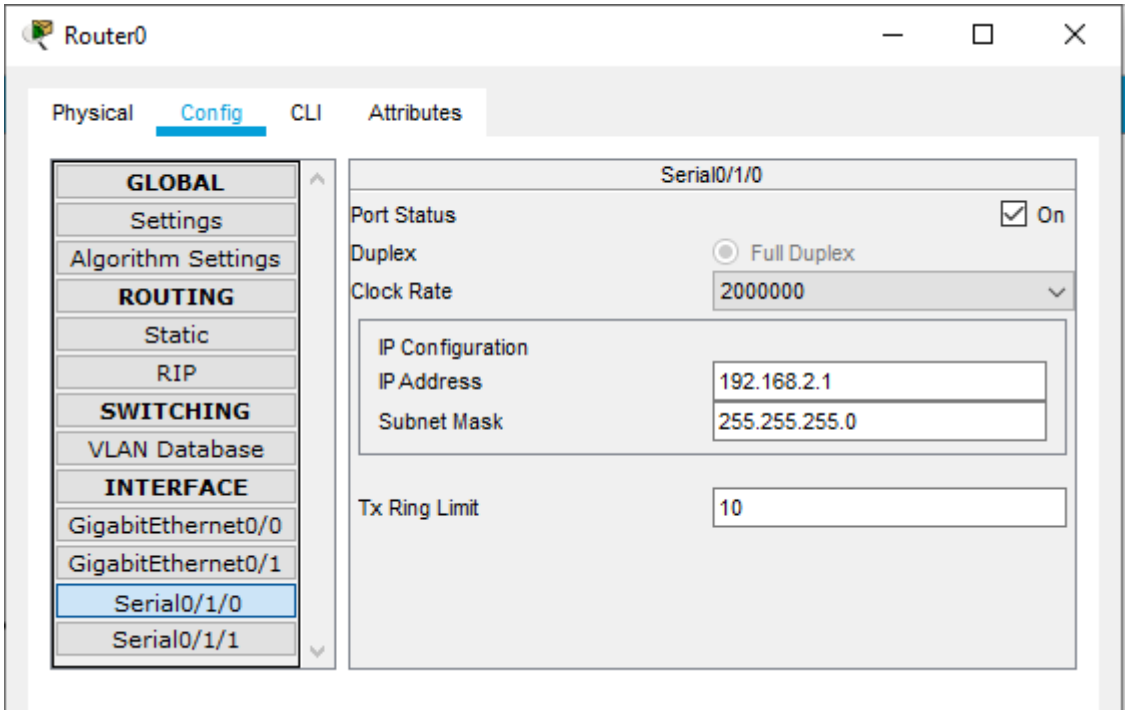


Configuring Server0

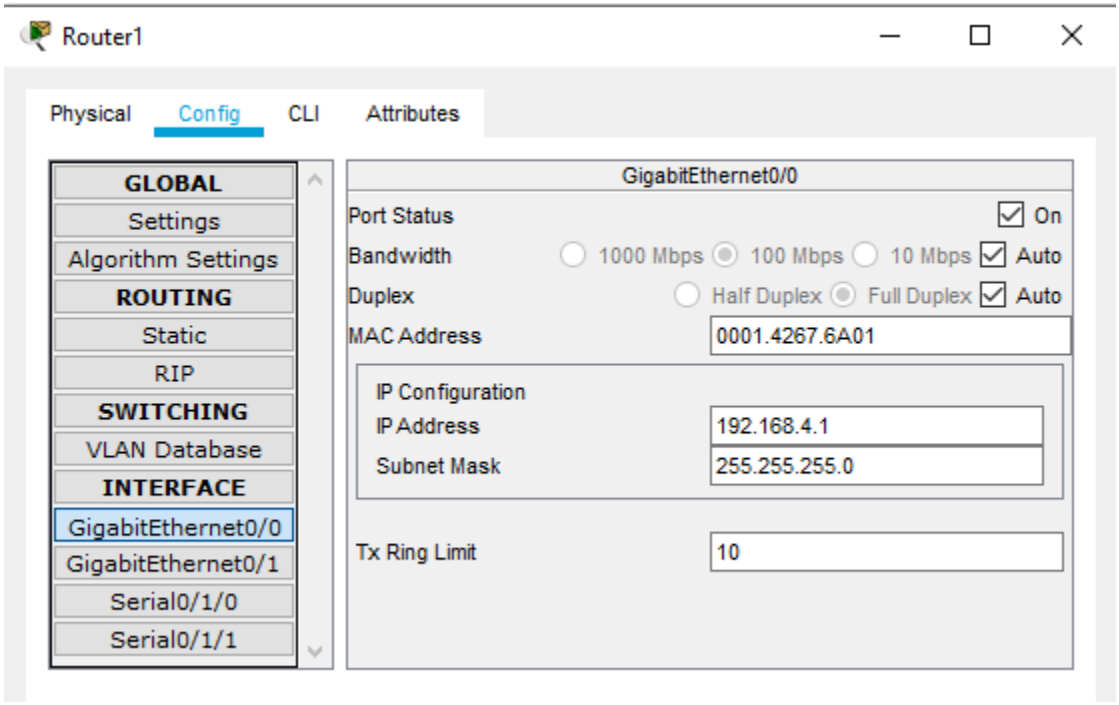


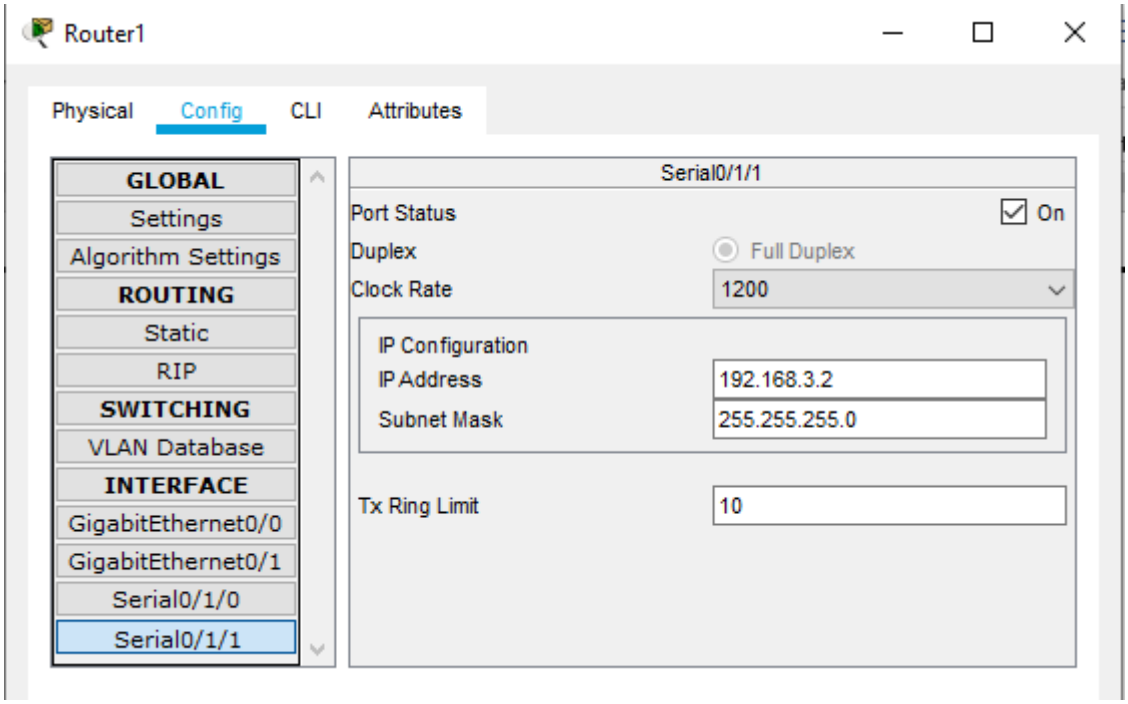
Configuring Router0



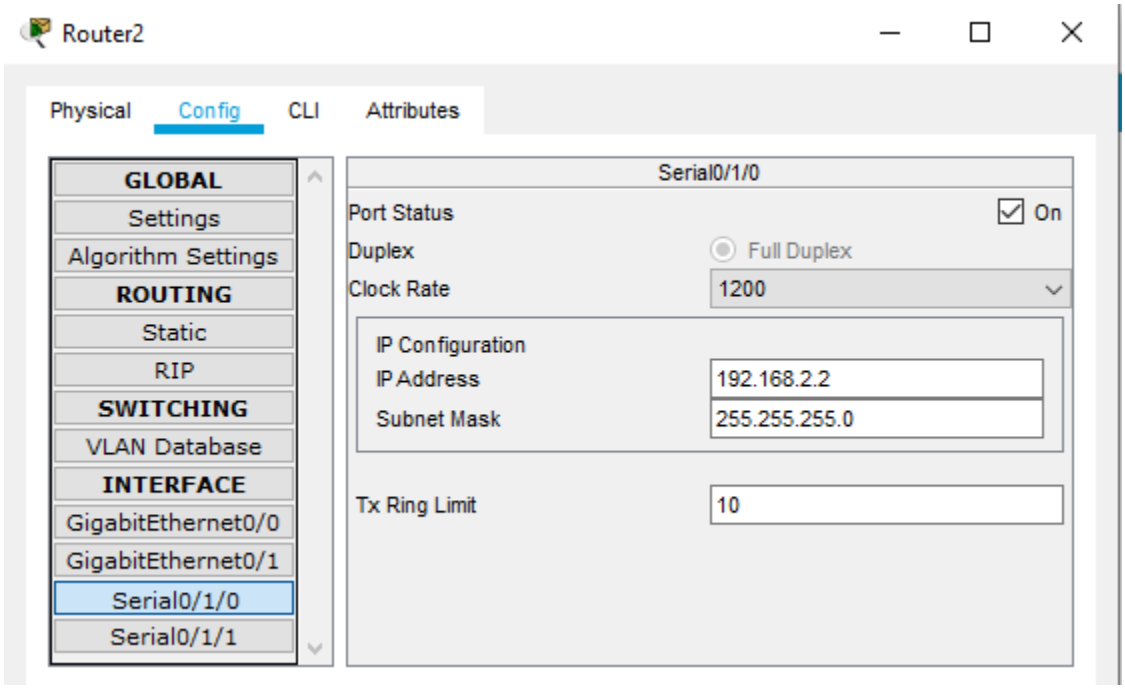


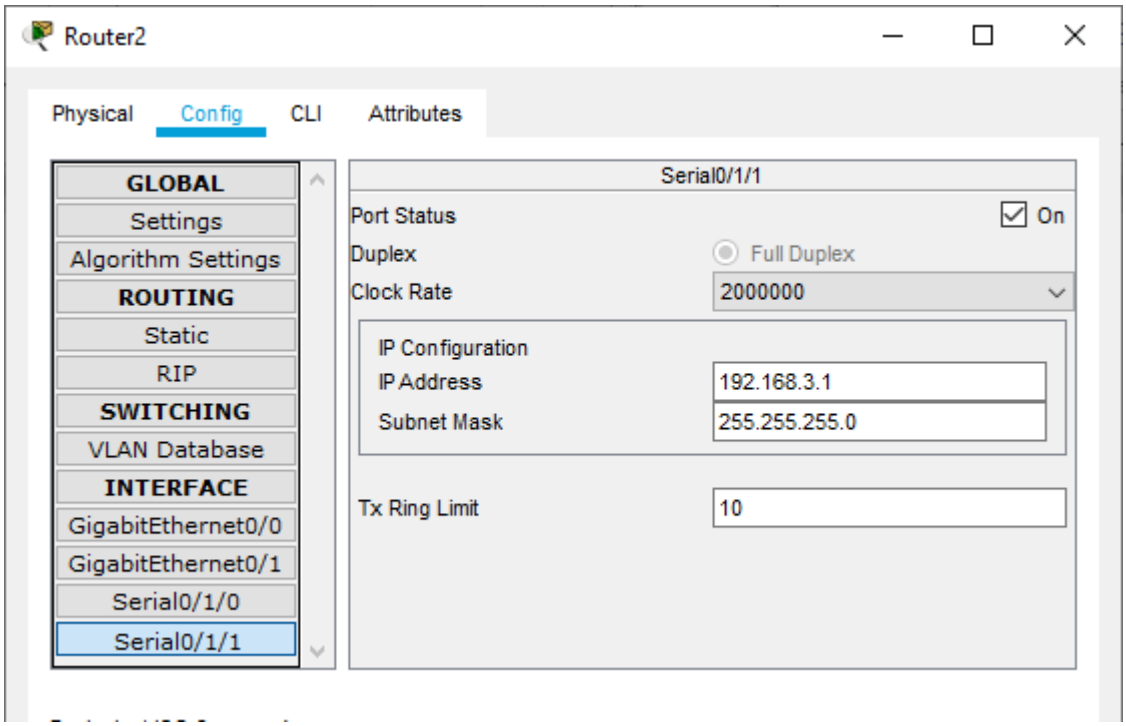
Configuring Router1





Configuring Router2

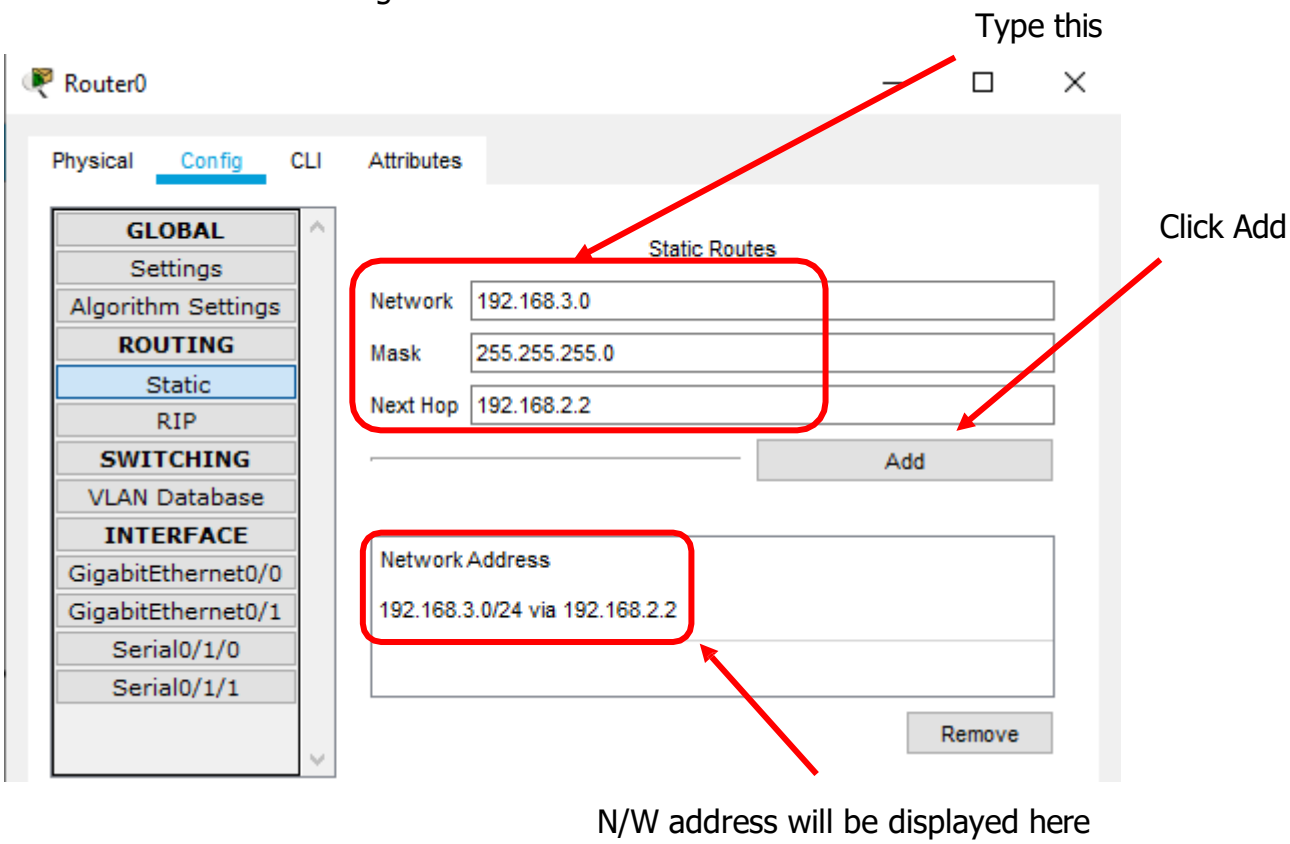


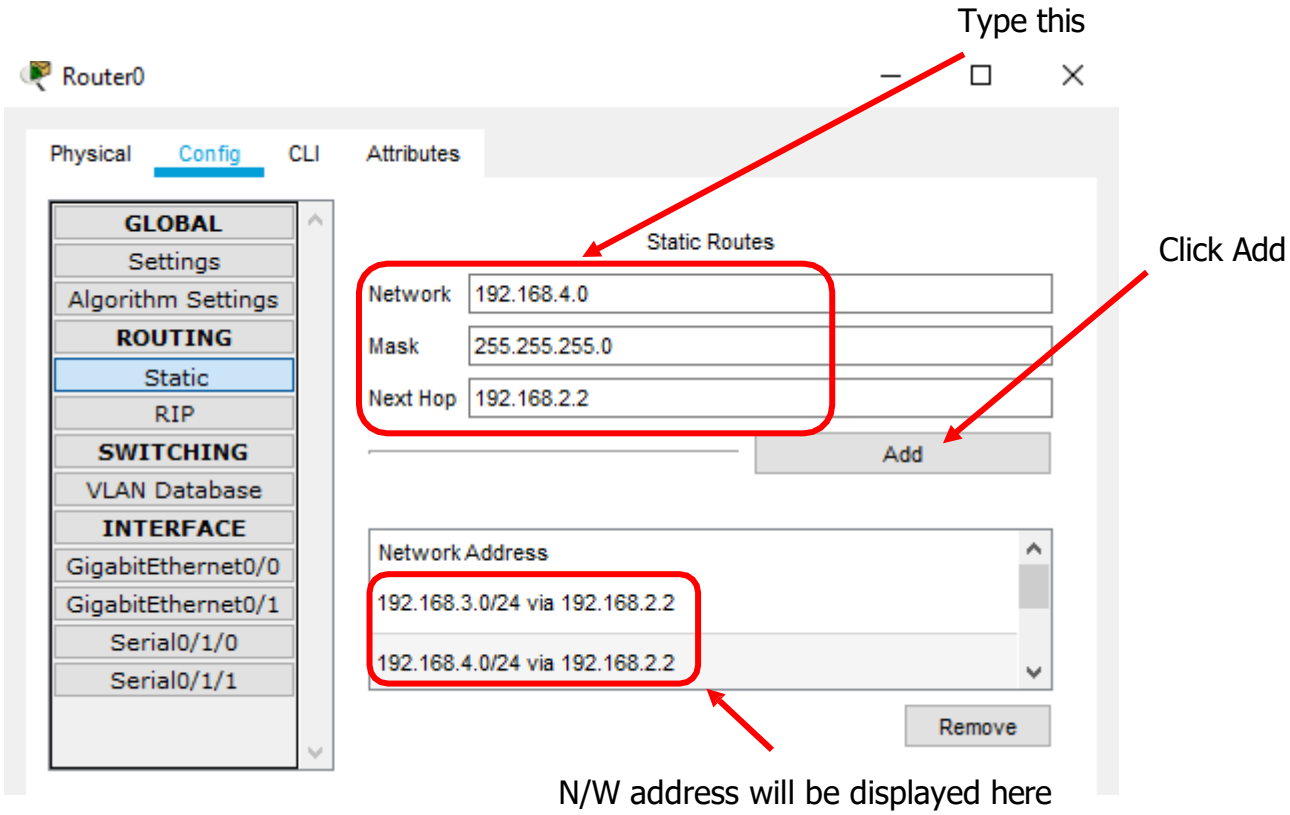


Part 1: Static Routing

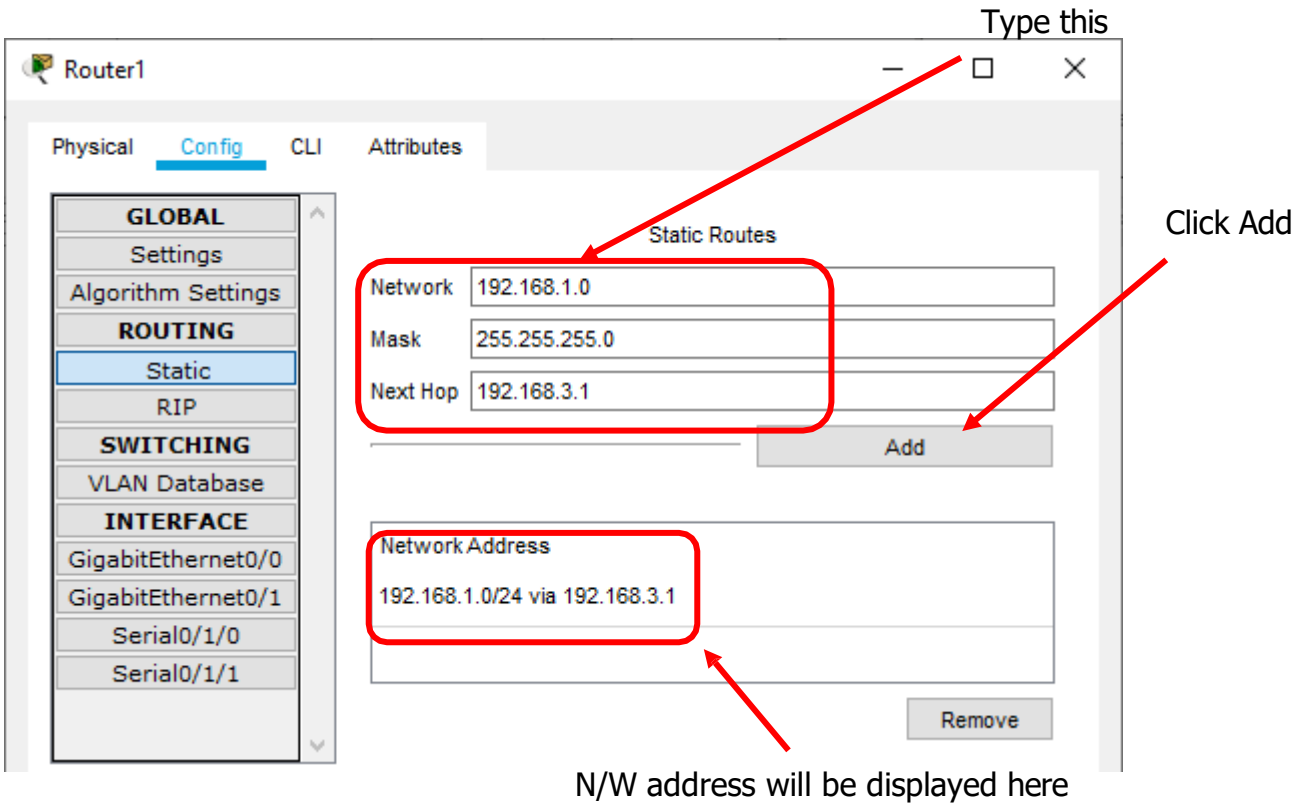
Static Routing is done using the following procedure for each Router

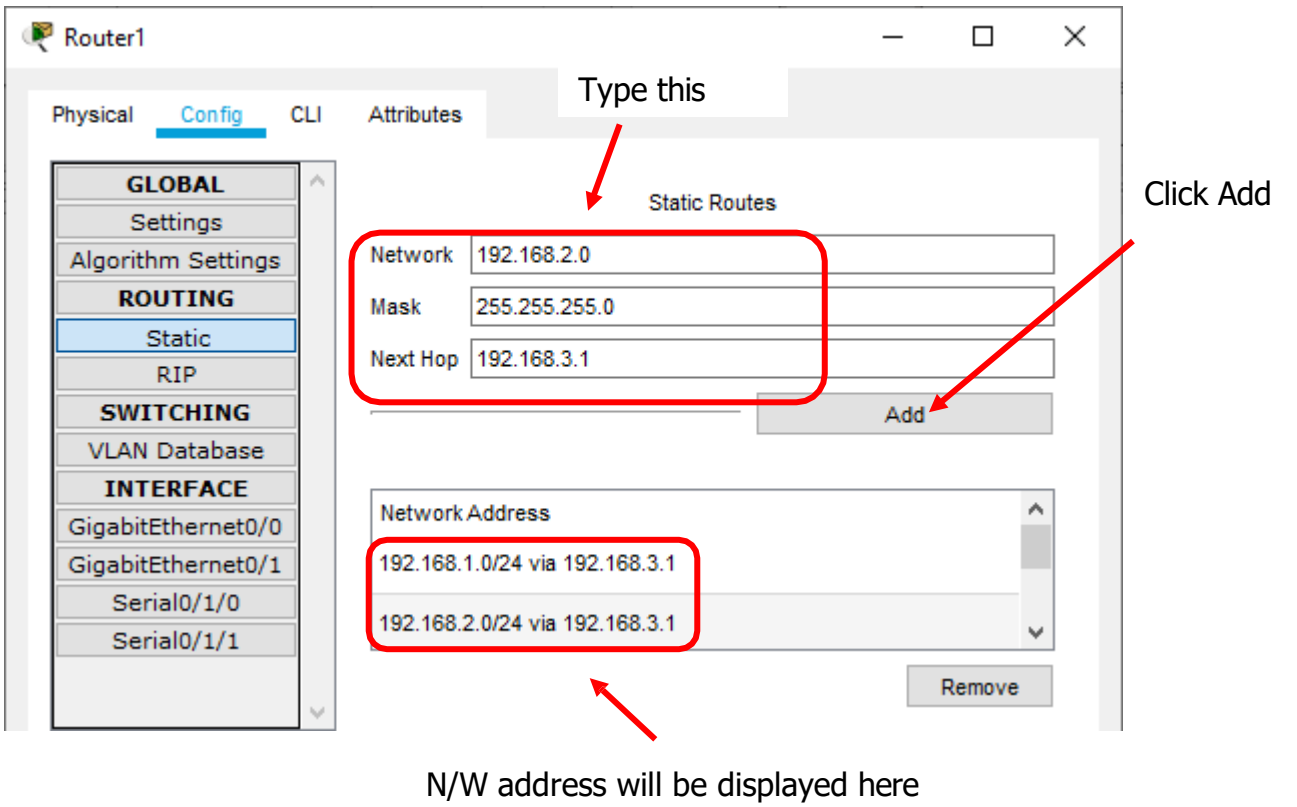
Router 0: Add the following in the Static mode of Router0



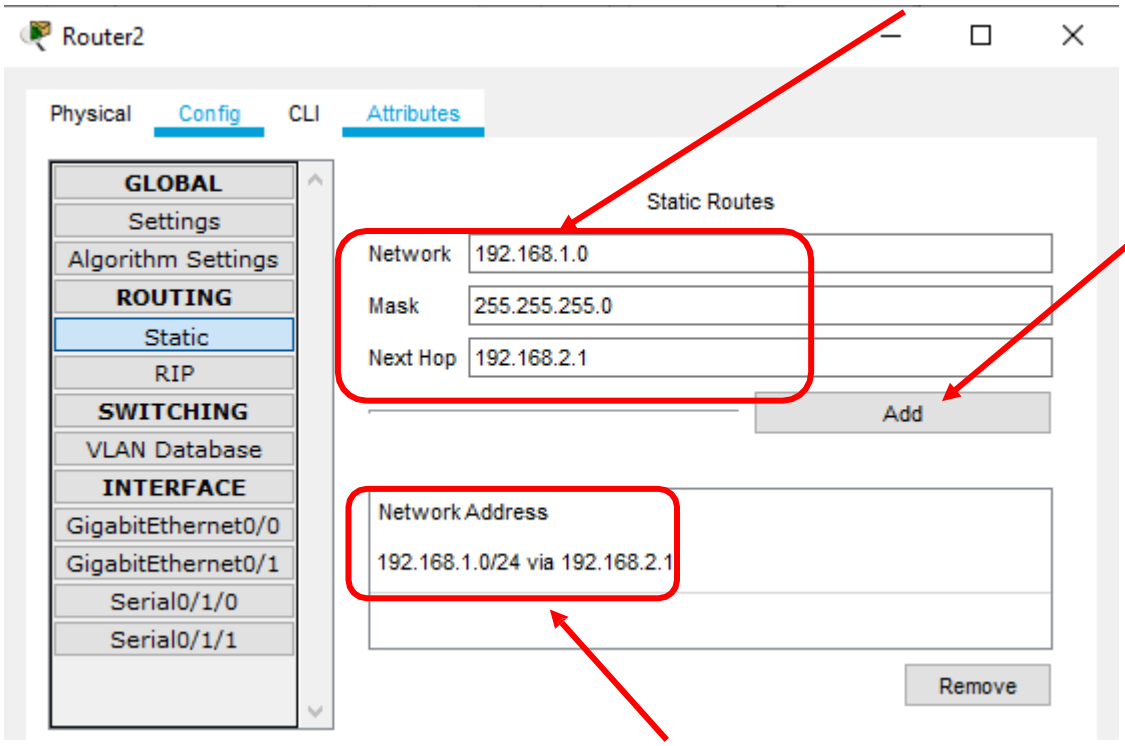


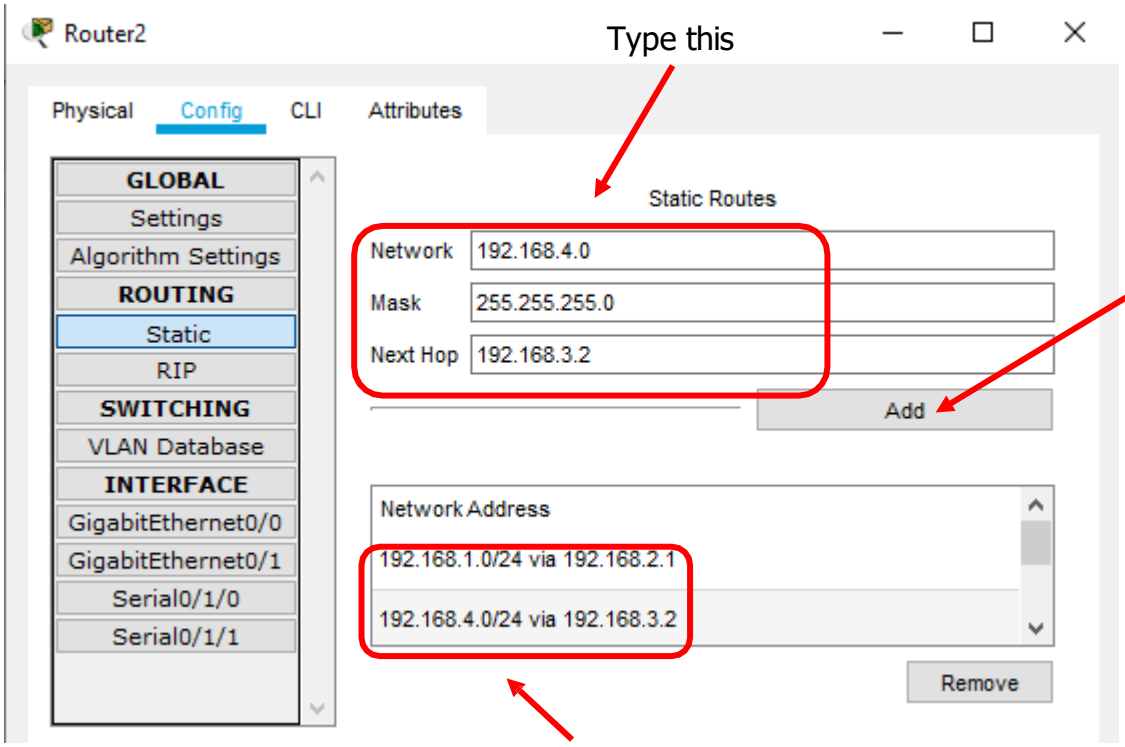
Router 1: Add the following in the Static mode of Router1



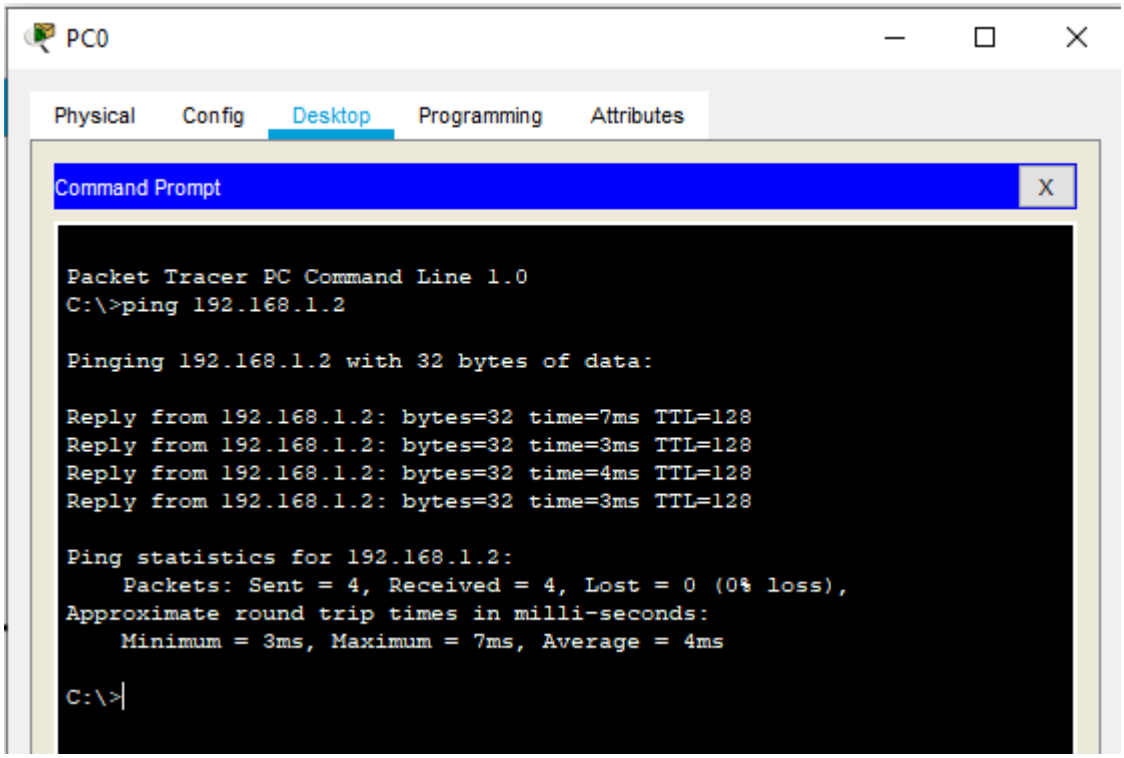


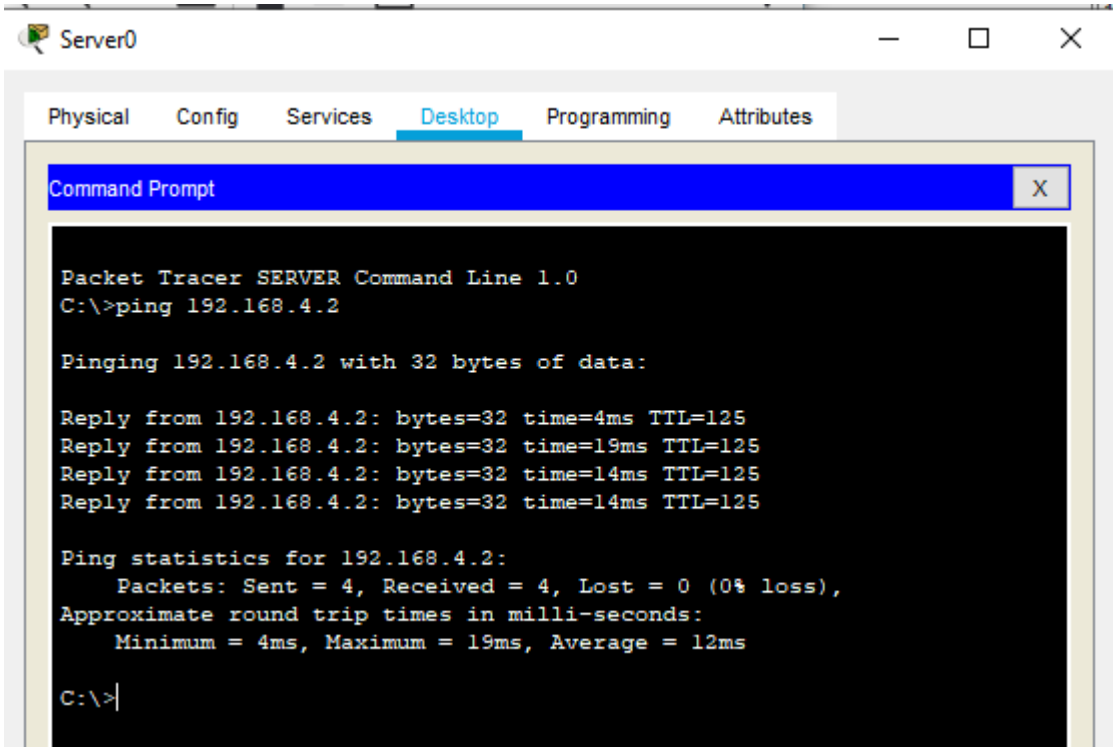
Router 2: Add the following in the Static mode of Router2





Now we check the connectivity by pinging the Server from the PC and from PC to Server





Part 2: Configuring SSH on Router 2

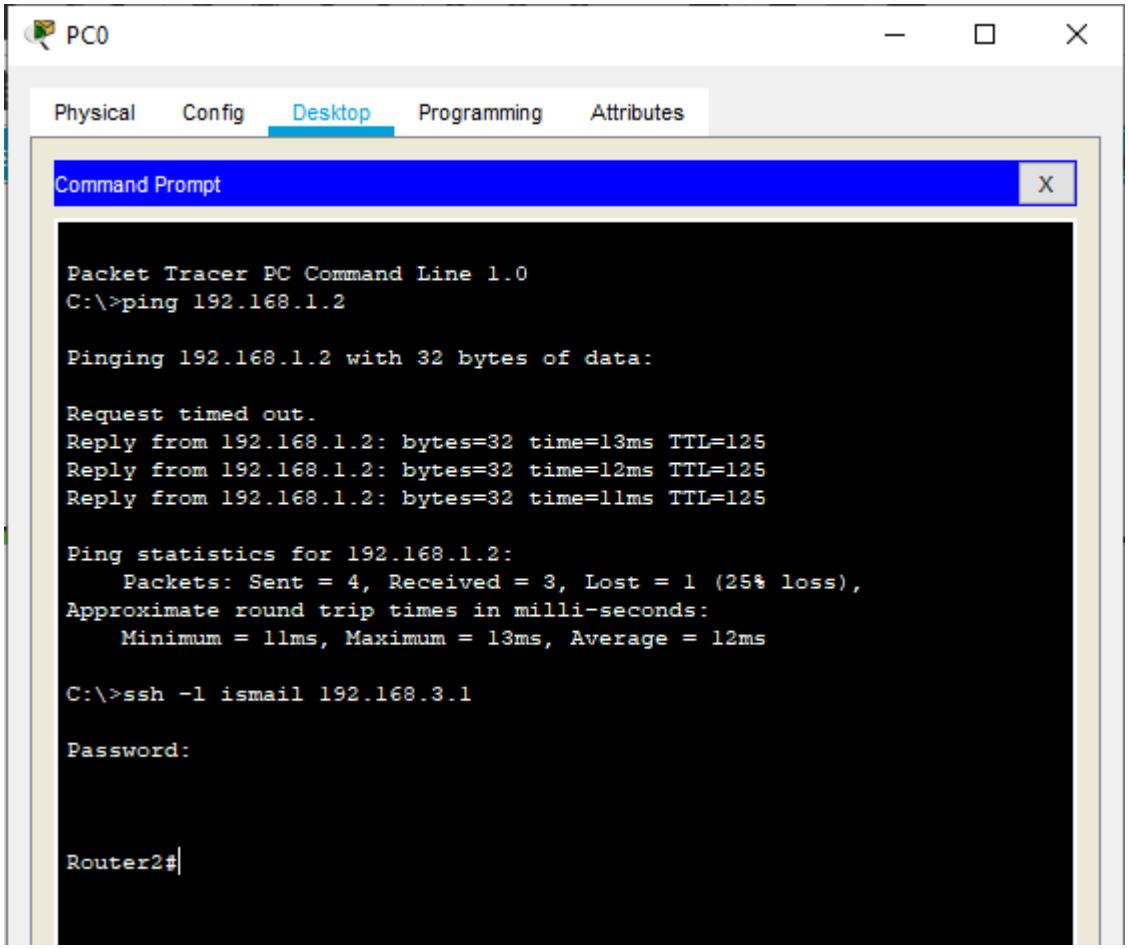
Type the following commands in the CLI mode of Router2

Router>enable
Router#configure terminal
Router(config)#ip domain-name .com
Router(config)#hostname Router2
Router2(config)#crypto key generate rsa

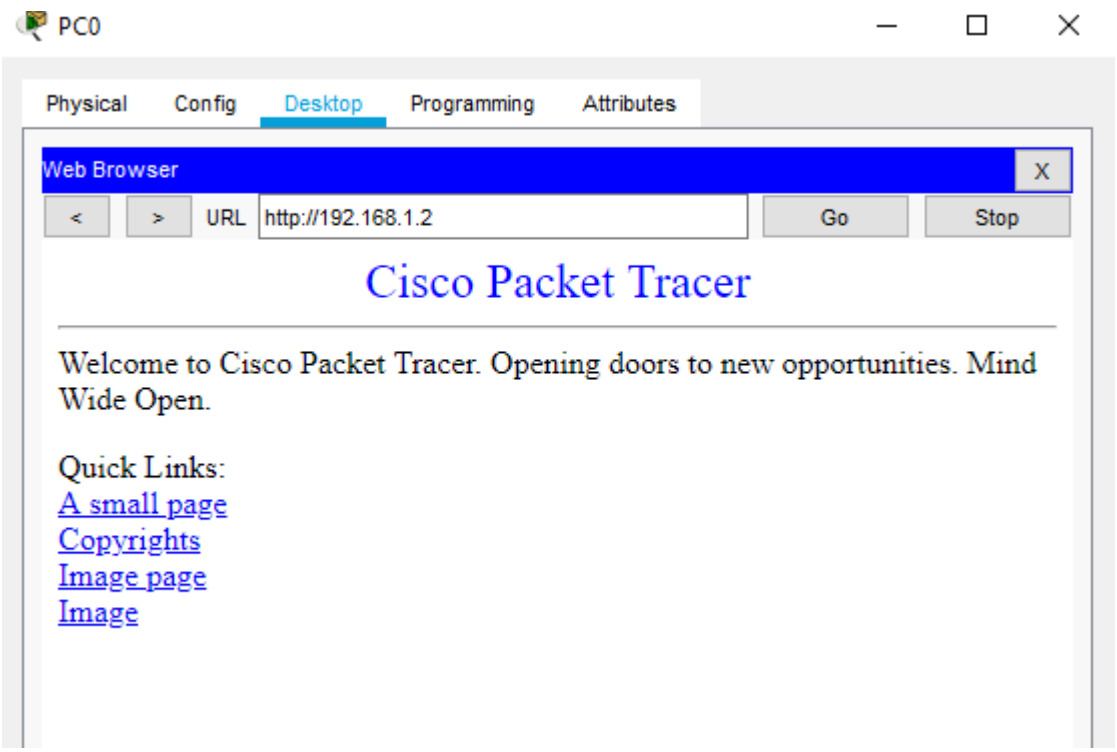
Router2 (config)#line vty 0 4
Router2 (config-line)#transport input ssh
Router2 (config-line)#login local
Router2 (config-line)#exit

Router2 (config)#username ismail privilege 15 password cisco

Now verify ssh from PC0 by typing the following command
ssh -l ismail 192.168.3.1



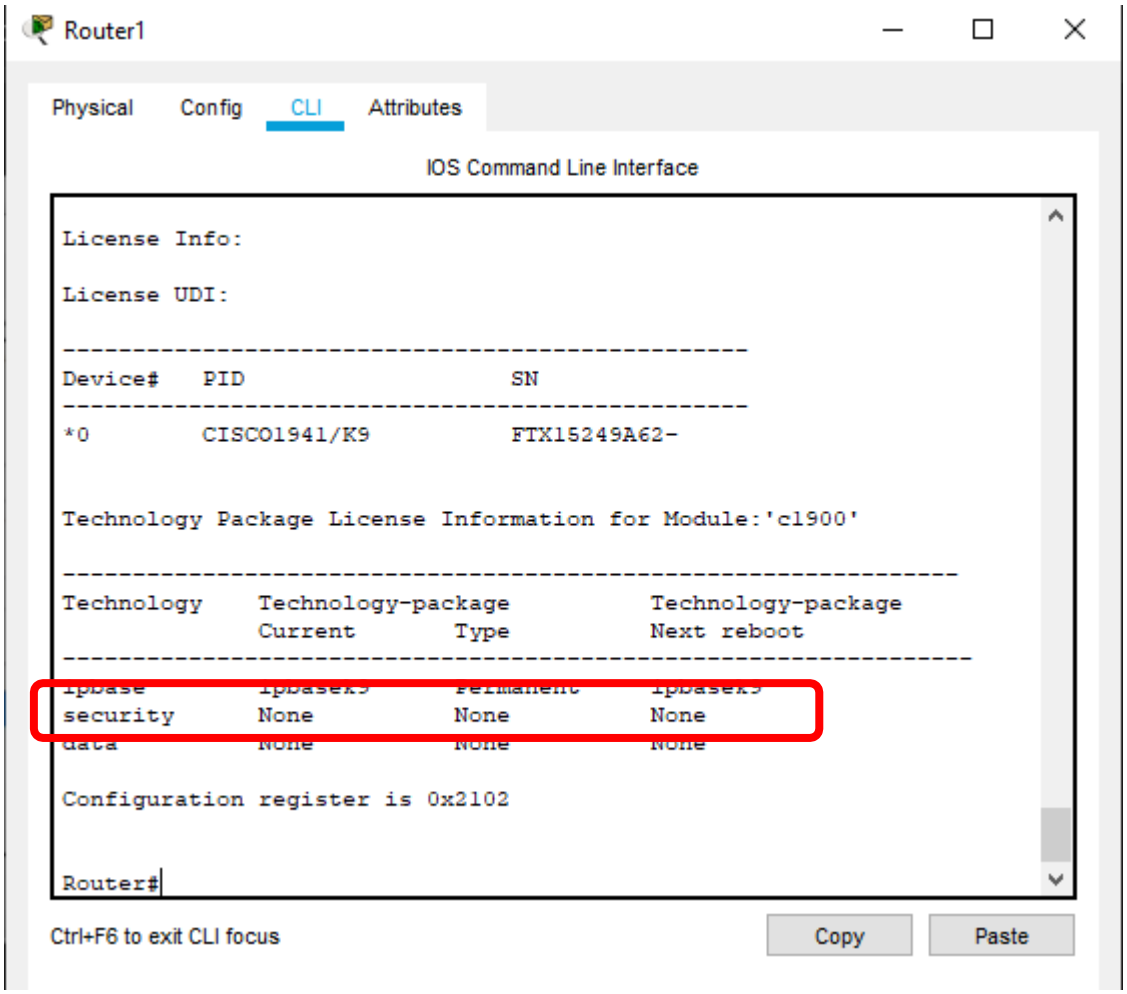
Next we access the web services of the Server using the web browser of PC using the following



Part 3: Create the Firewall Zones on Router1

Type the following commands in the CLI mode of Router1

Router>enable
Router#configure terminal
Router(config)#show version

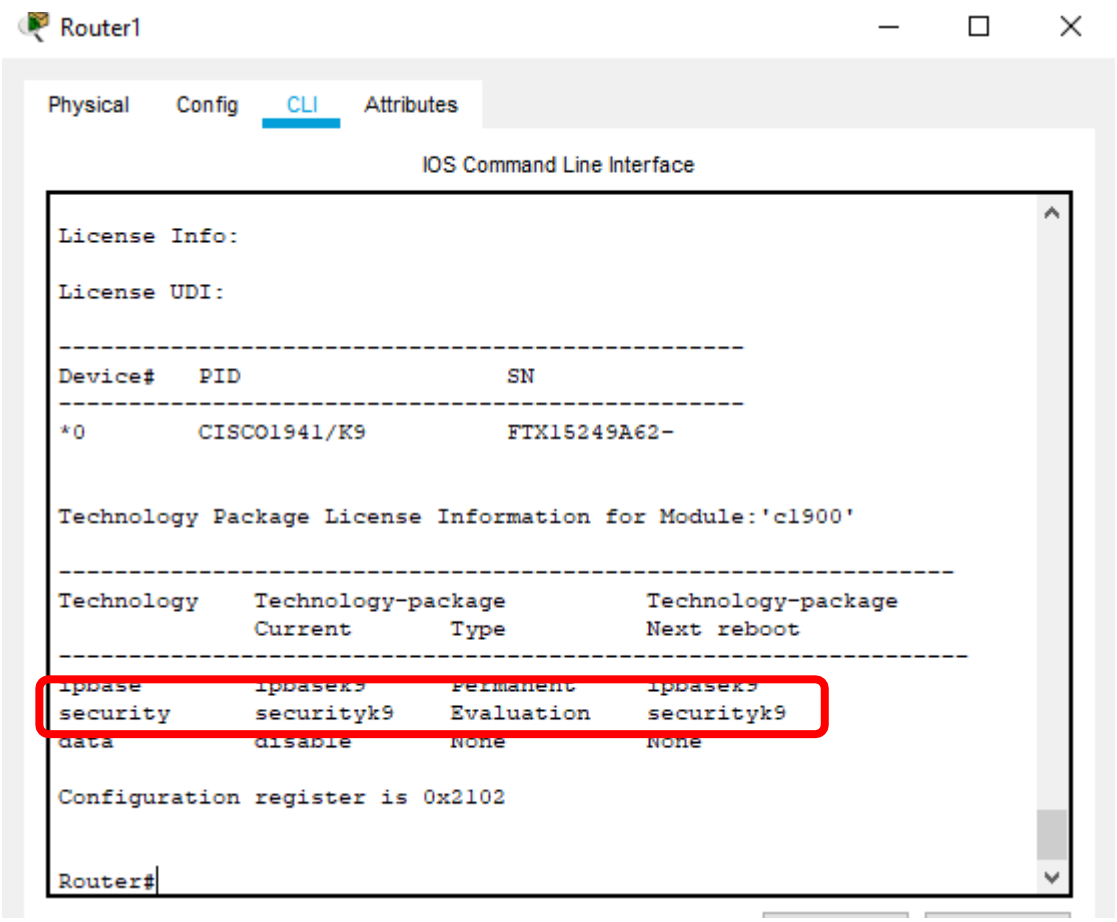


Router#configure terminal
Router (config)#license boot module c1900 technology-package securityk9
ACCEPT? [yes/no]: y

Router(config)#exit
Router>enable

Router#reload
Router>enable

Router#show version



Router#
Router#configure terminal

Router(config)#zone security in-zone
Router(config-sec-zone)#exit

Router(config)#zone security out-zone
Router(config-sec-zone)#exit

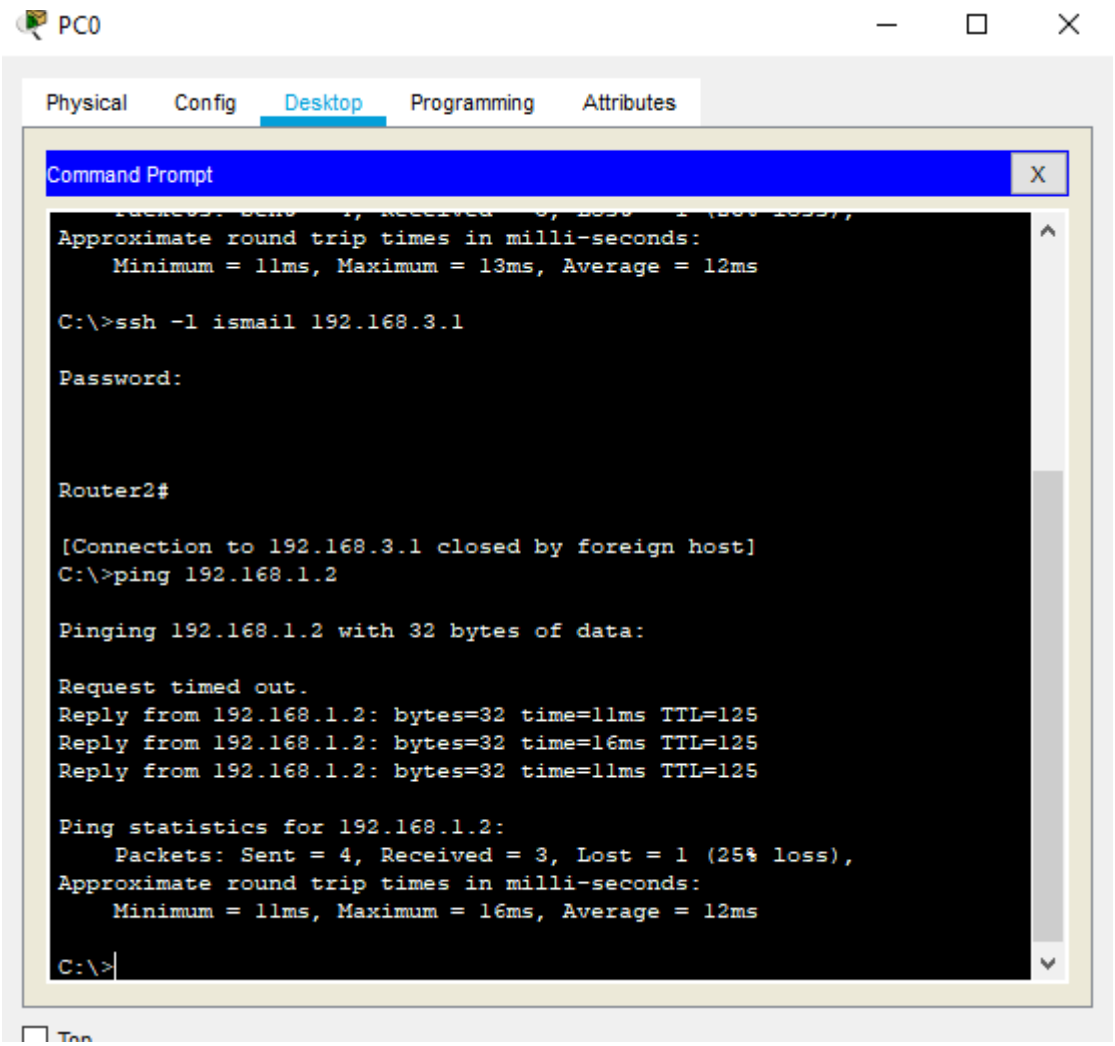
Router(config)#access-list 101 permit ip
192.168.4.0 0.0.0.255 any Router(config)#class-
map type inspect match-all in-map Router(config-
cmap)#match access-group 101
Router(config-cmap)#exit

Router(config)#policy-map type
inspect in-out Router(config-
pmap)#class type inspect in-

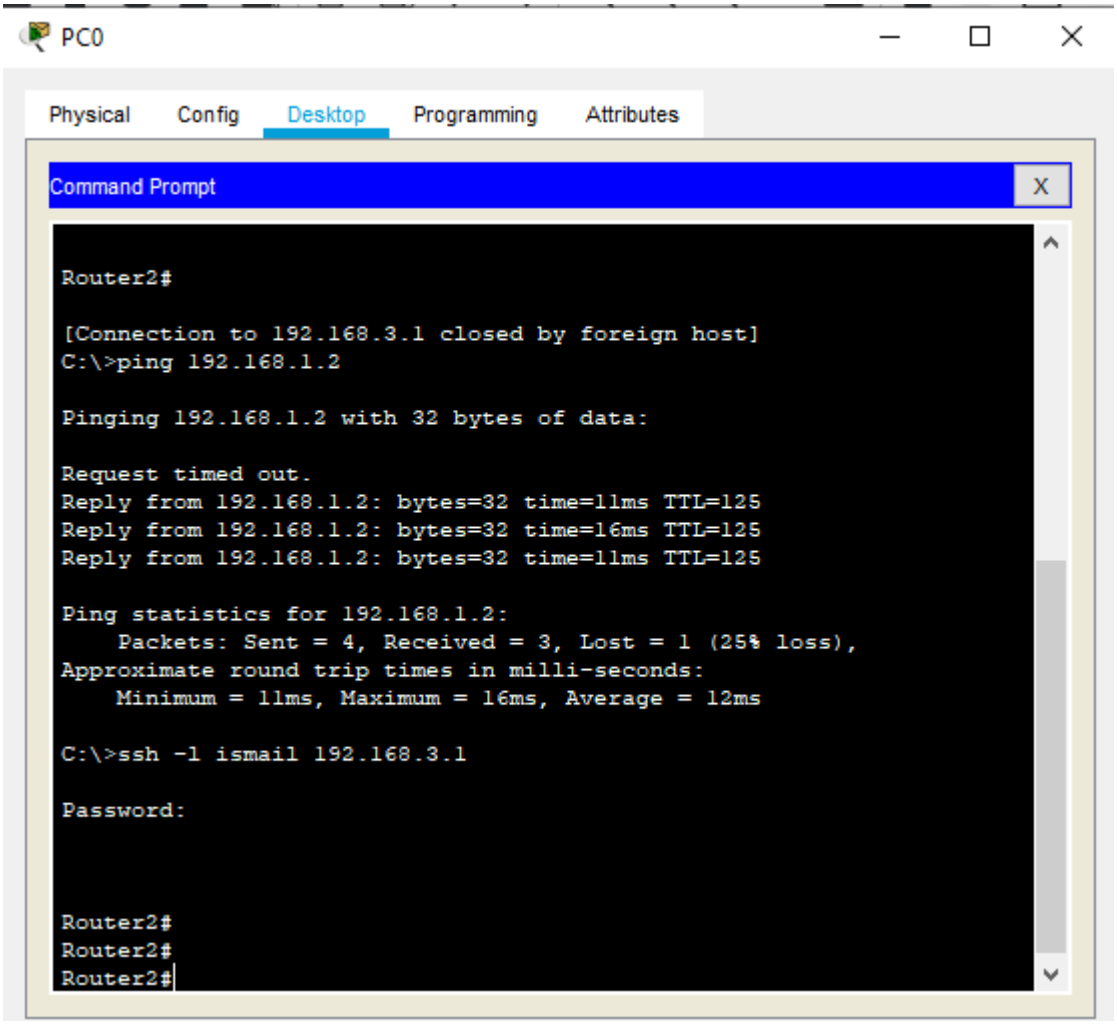
```
map Router(config-pmap-
c)#inspect
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#

Router(config)#zone-pair security in-out-zone source in-zone destination out-zone
Router(config-sec-zone-pair)#service-policy type inspect in-out
Router(config-sec-zone-pair)#exit
Router(config)#

Router(config)#interface GigabitEthernet0/0
Router(config-if)#zone-member security in-zone
Router(config-if)#exit
Router(config)#

Router(config)#interface Serial0/1/1
Router(config-if)#zone-member security out-zone
Router(config-if)#exit
Router(config)#exit

Router#copy running-config startup-config
```

Part 4: Testing the Firewall Functionality (from in-zone to out-zone) by the following steps

Step 1: Pinging SERVER from PC (it will succeed)



Step 2: Start an SSH session from PC to Router 2 (192.168.3.1)

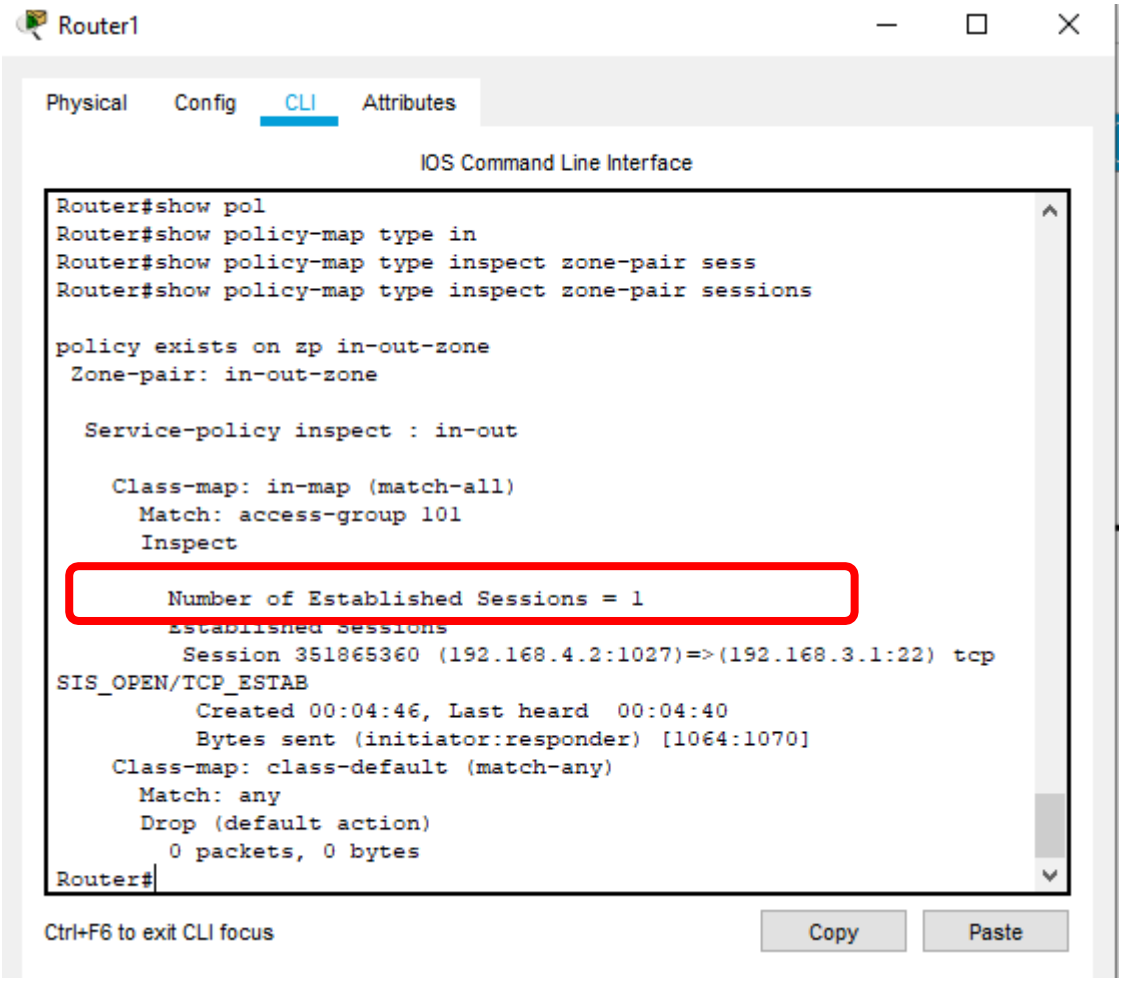


As seen above the session becomes active and we get access to Router2 (Do not exit and the session and continue to Step 3)

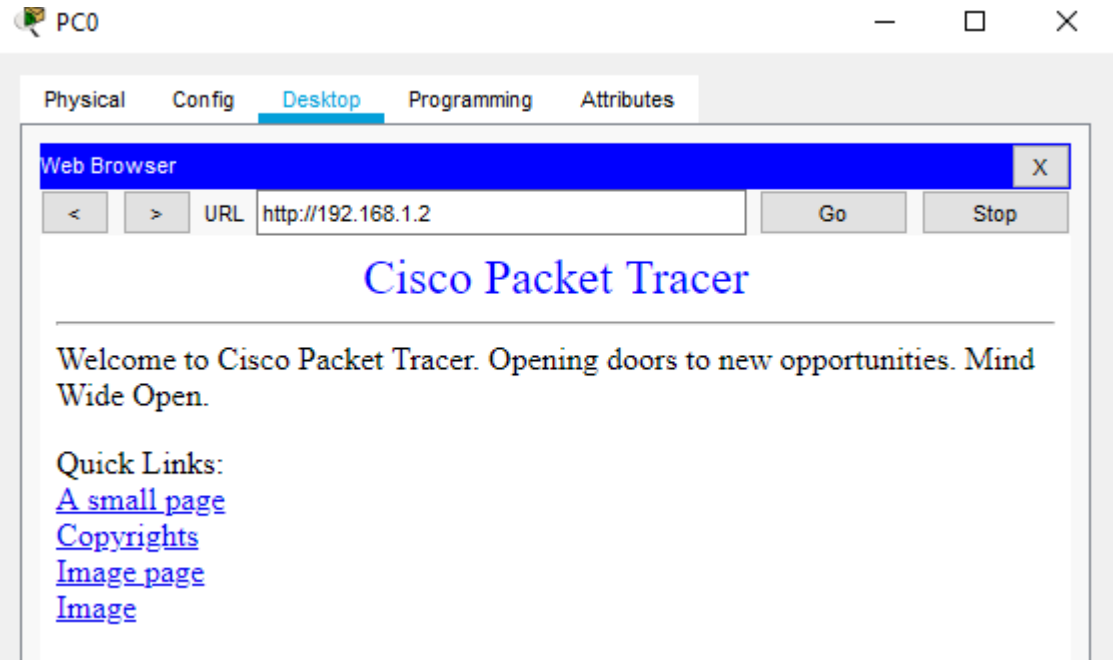
Step 3: Type the following command in the CLI mode of Router1

Router#show policy-map type inspect zone-pair sessions

We will get the following output

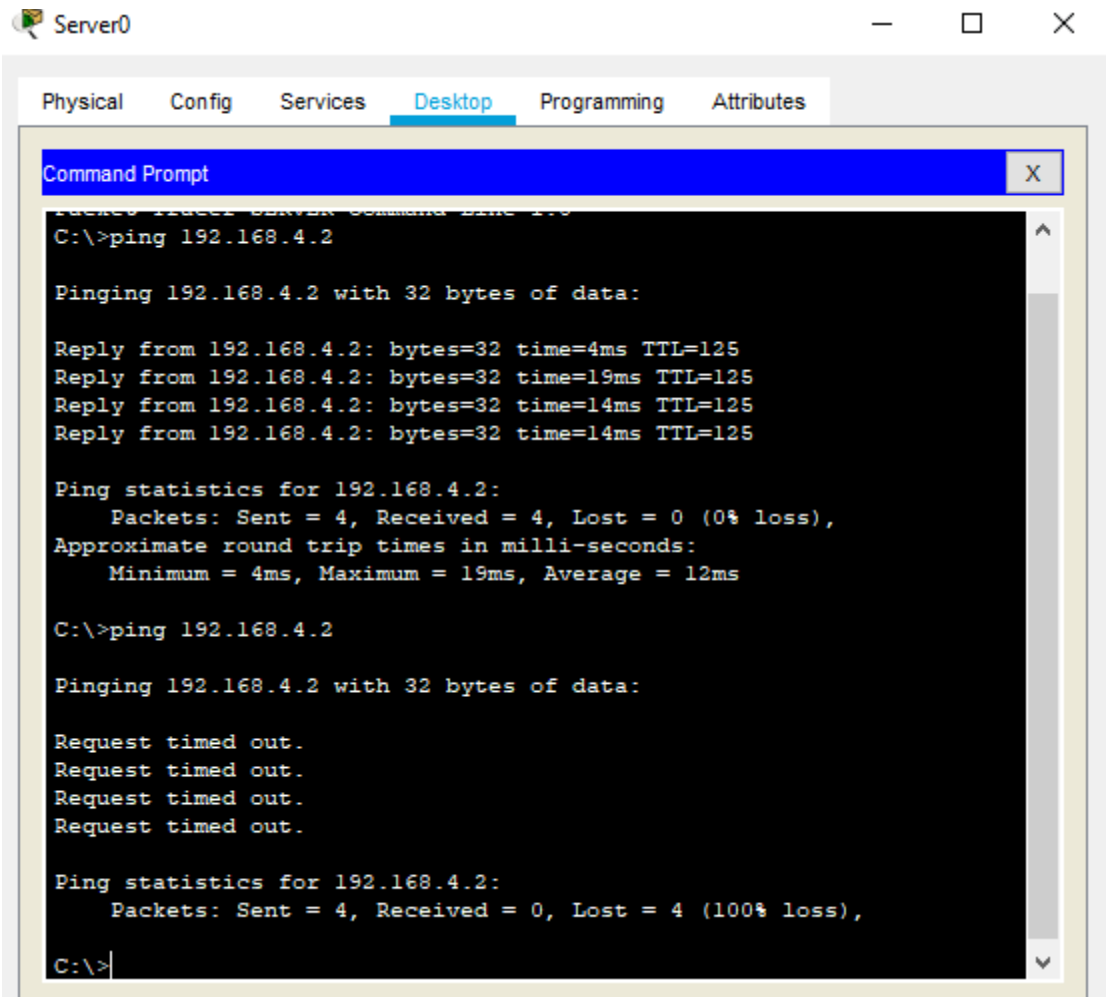


Step 4: We close the SSH connection and open the web browser and access the server address (192.168.1.2) and get the following



Part 5: Testing the Firewall Functionality (from out-zone to in-zone) by the following steps

Step 1: Ping PC0 from the SERVER (ip 192.168.4.2) (it will result in Failure)



Hence the Firewall functionality has been verified

PRACTICAL NO 6: Configure IOS Intrusion Prevention System (IPS) Using the CLI

The Cisco IOS IPS acts as an in-line intrusion prevention sensor, watching packets and sessions as they flow through the router and scanning each packet to match any of the Cisco IOS IPS signatures. When it detects suspicious activity, it responds before network security can be compromised and logs the event through Cisco IOS syslog messages or Security Device Event Exchange (SDEE). The network administrator can configure Cisco IOS IPS to choose the appropriate response to various threats. The Signature Event Action Processor (SEAP) can dynamically control actions that are to be taken by a signature event on the basis of parameters such as fidelity, severity, or target value rating. These parameters have default values but can also be configured through CLI. When packets in a session match a signature, Cisco IOS IPS can take any of the following actions, as appropriate:

1) Send an alarm to a syslog server or a centralized management interface

2) Drop the packet

3) Reset the connection

4) Deny traffic from the source IP address of the attacker for a specified amount of time 5) Deny traffic on the connection for which the signature was seen for a specified amount of time

Cisco developed its Cisco IOS software-based intrusion-prevention capabilities and Cisco IOS Firewall with flexibility in mind, so that individual signatures could be disabled in case of false positives. Generally, it is preferable to enable both the firewall and Cisco IOS IPS to support network security policies. However, each of these features may be enabled independently

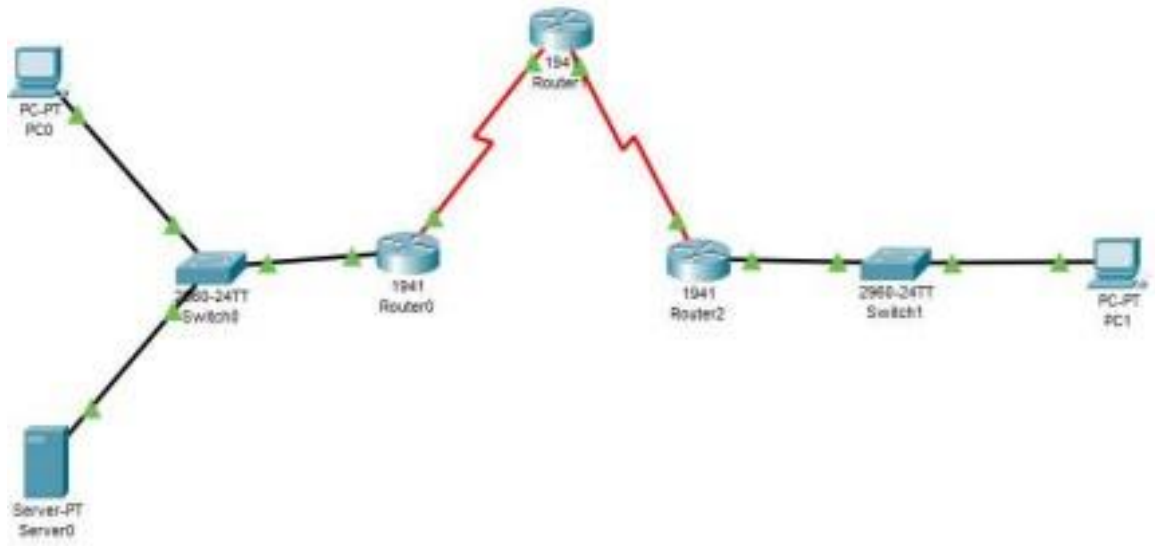
and on different router interfaces.

Signatures:

A signature is a set of rules that an IDS and an IPS use to detect typical intrusive activity, such as DoS attacks. We can easily install signatures using IDS and IPS management software such as Cisco IDM. Sensors enables us to modify existing signatures and define new ones. As sensors scan network packets, they use signatures to detect known attacks and respond with predefined actions. A malicious packet flow has a specific type of activity and signature, and an IDS or IPS sensor examines the data flow using many different signatures. When an IDS or IPS sensor matches a signature with a data flow, the sensor

takes action, such as logging the event or sending an alarm to IDS or IPS management software, such as the Cisco SDM

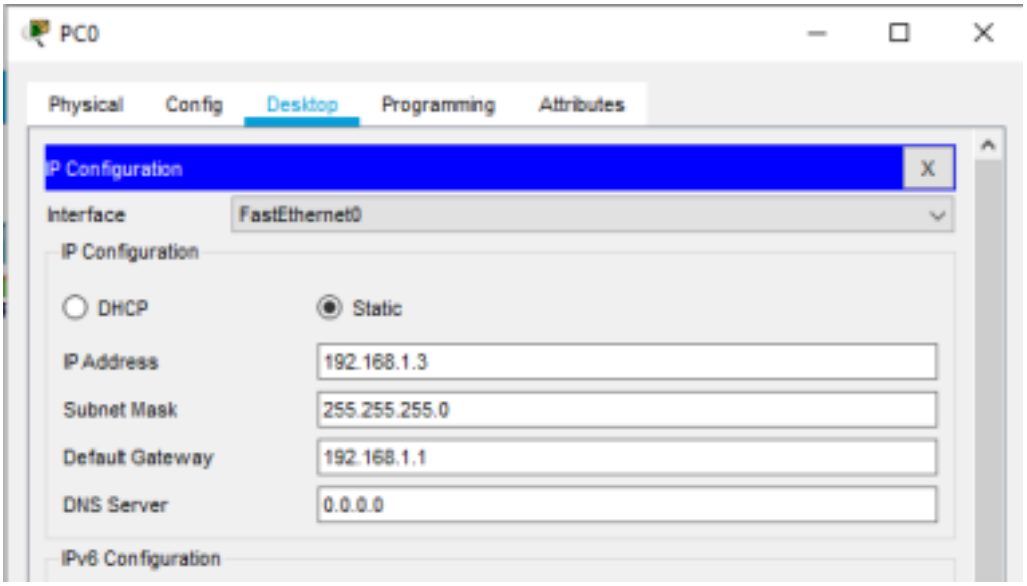
We us the following topology for the present case:



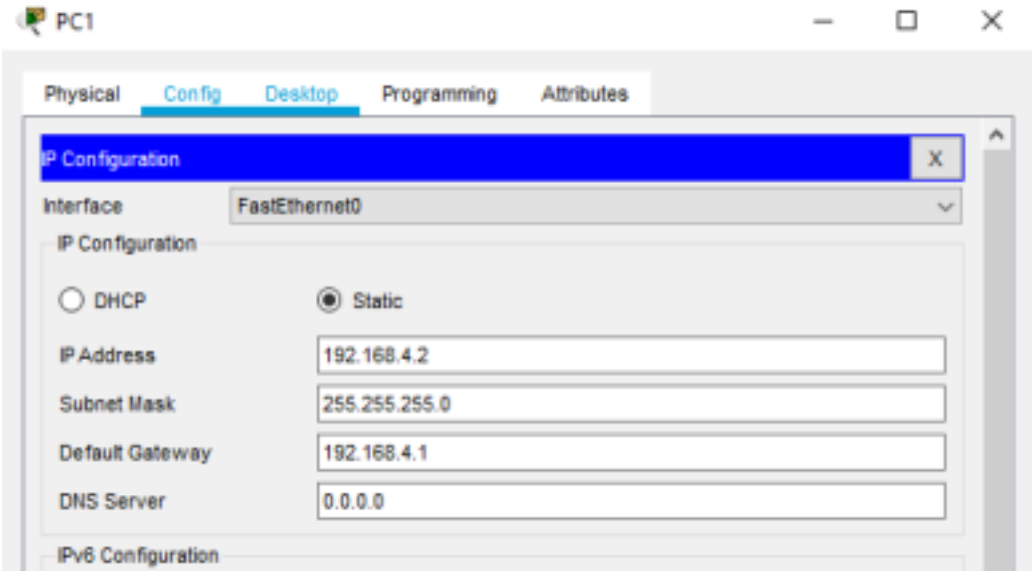
Let us consider the following Address table to configure the network devices:

Device	Interface	IP Address	Subnet Mask	Default gateway	Switch Port
PC 0	NA	192.168.1.3	255.255.255.0	192.168.1.1	Switch0 F0/1
PC 1	NA	192.168.4.2	255.255.255.0	192.168.4.1	Switch1 F0/1
Server0	NA	192.168.1.2	255.255.255.0	192.168.1.1	Switch0 F0/2
Router0	GE0/0	192.168.1.1	255.255.255.0	NA	Switch0 F0/5
	S0/1/0	192.168.2.1	255.255.255.0	NA	NA
Router1	S0/1/0	192.168.2.2	255.255.255.0	NA	NA
	S0/1/1	192.168.3.1	255.255.255.0	NA	NA
Router2	S0/1/1	192.168.3.2	255.255.255.0	NA	NA
	GE0/0	192.168.4.1	255.255.255.0	NA	Switch1 F0/5

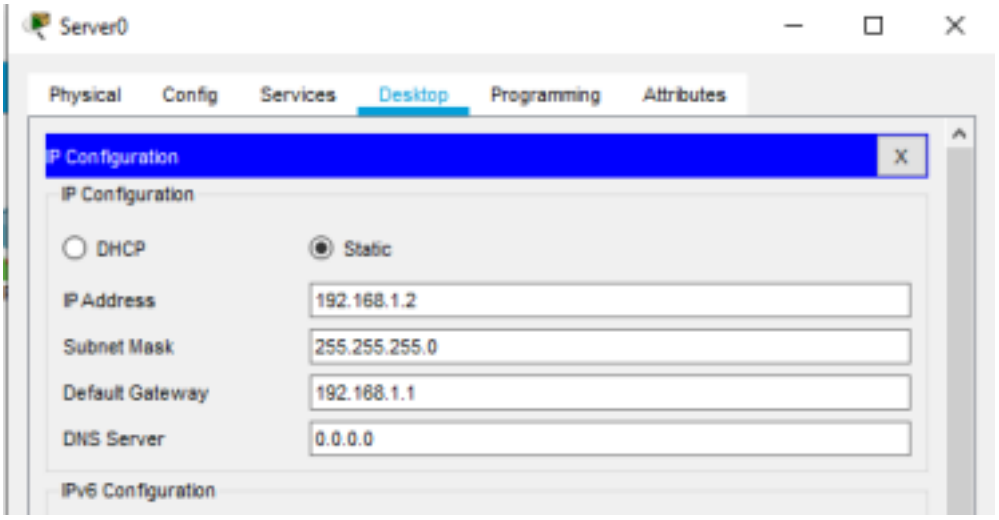
Configuring PC0



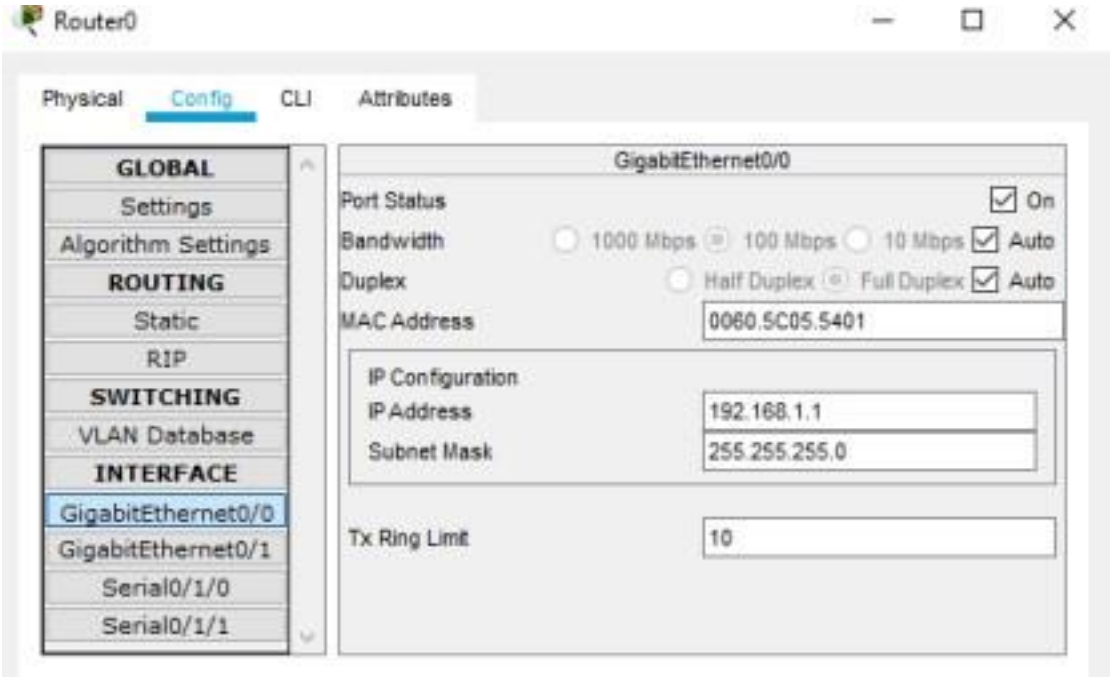
Configuring PC1

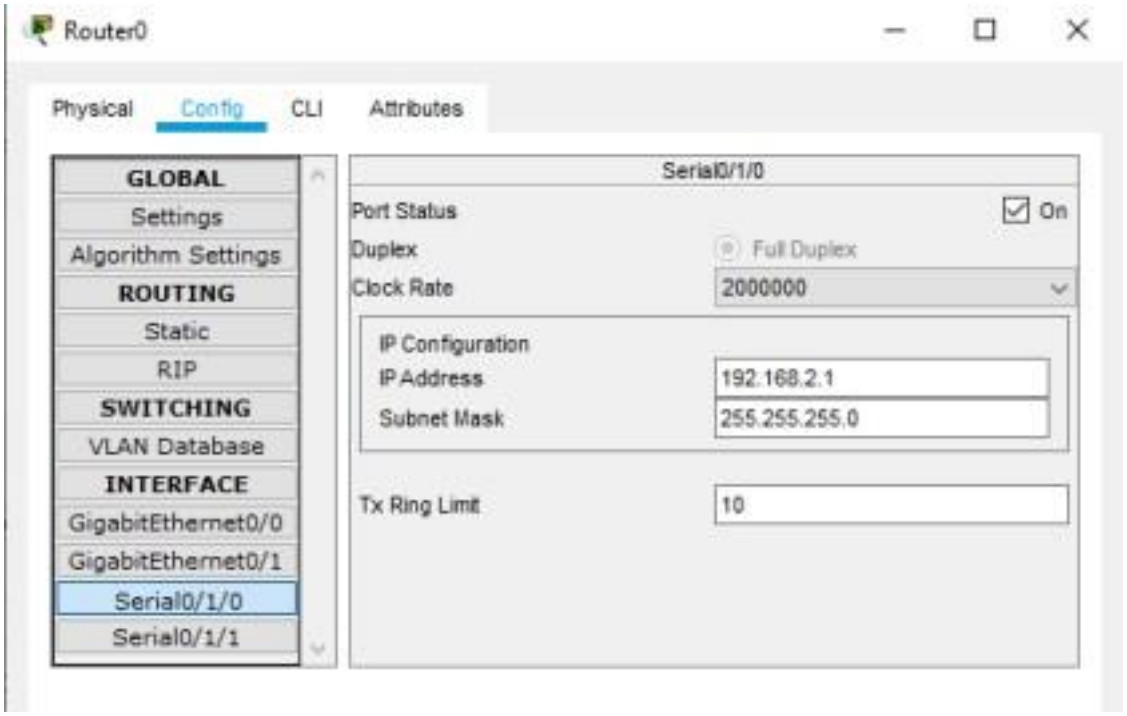


Configuring Server0

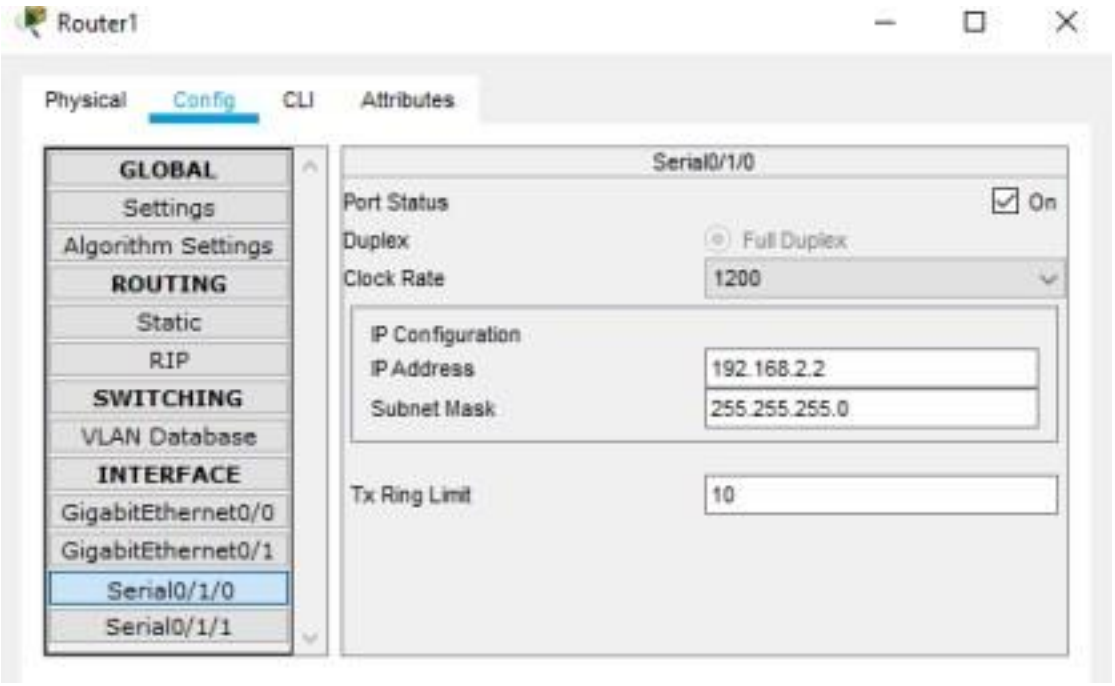


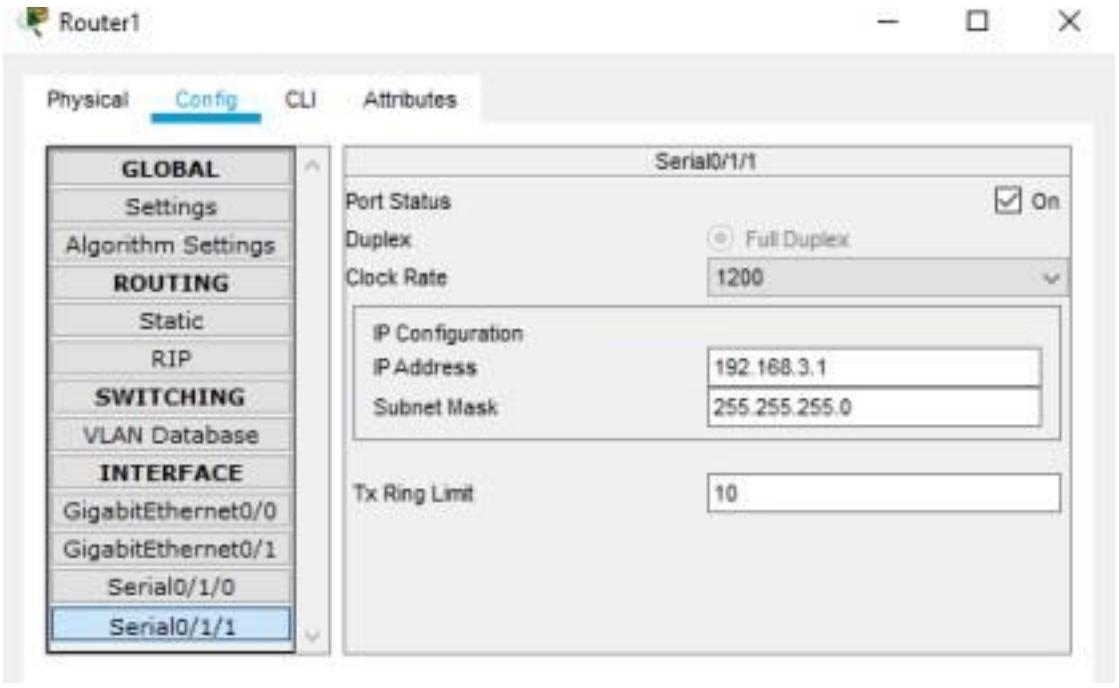
Configuring Router0



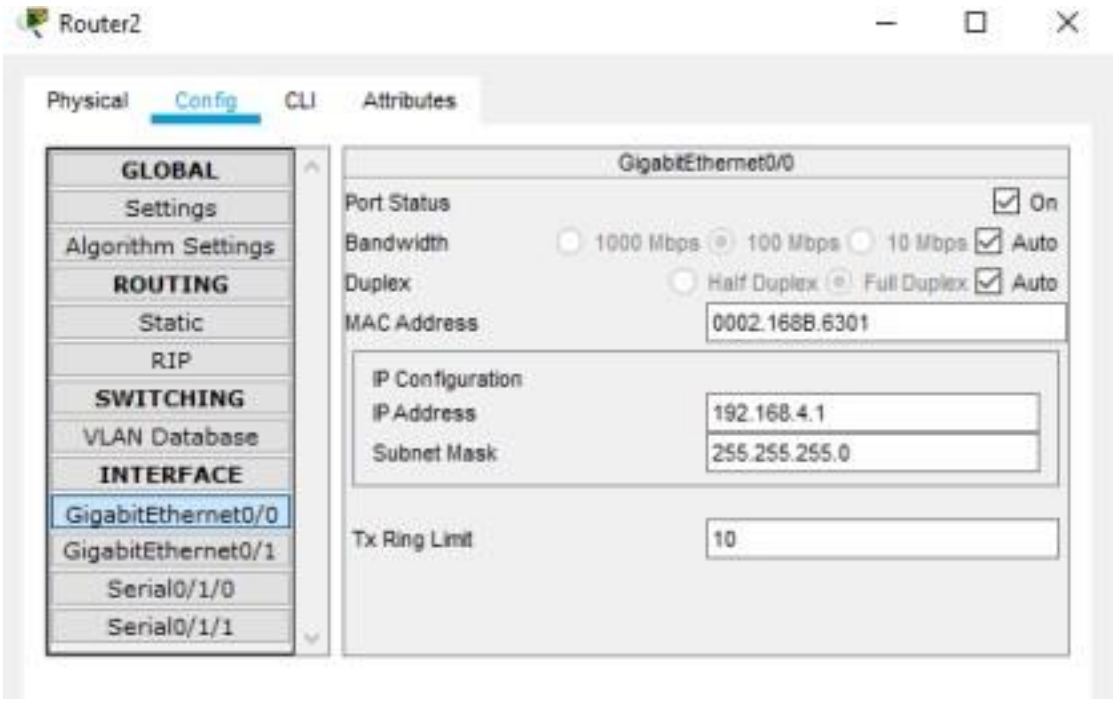


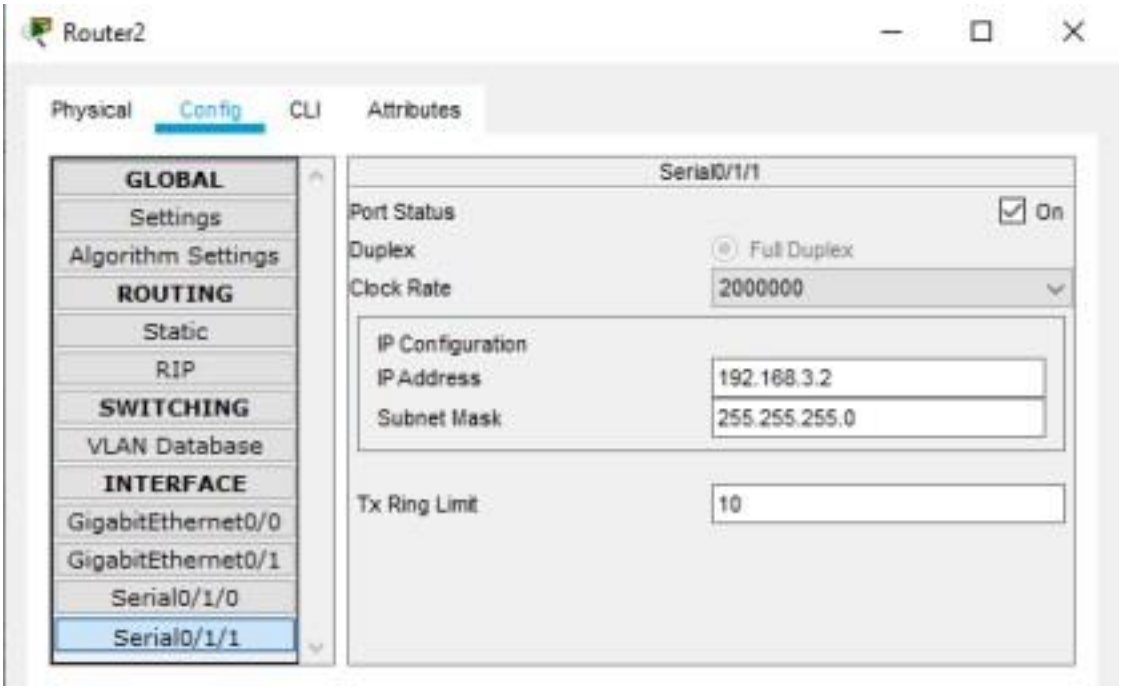
Configuring Router1



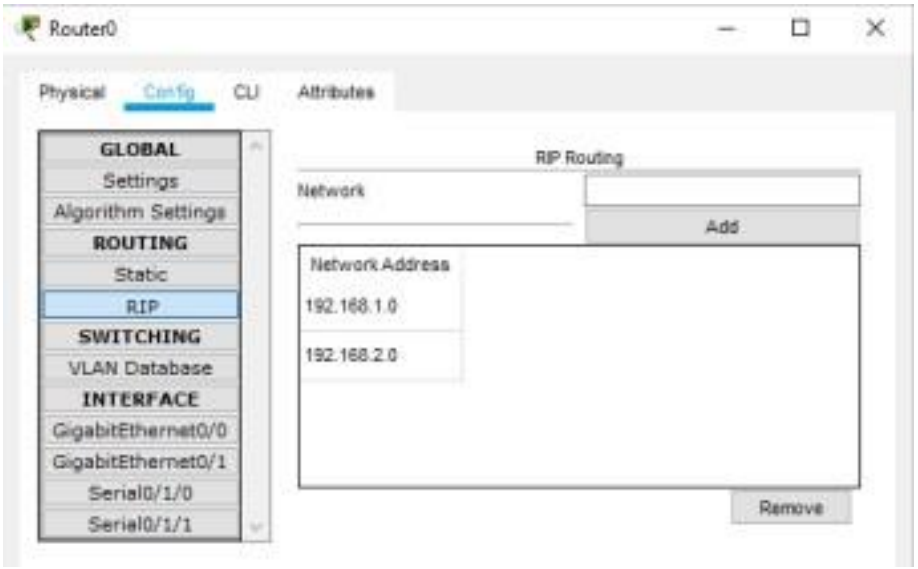


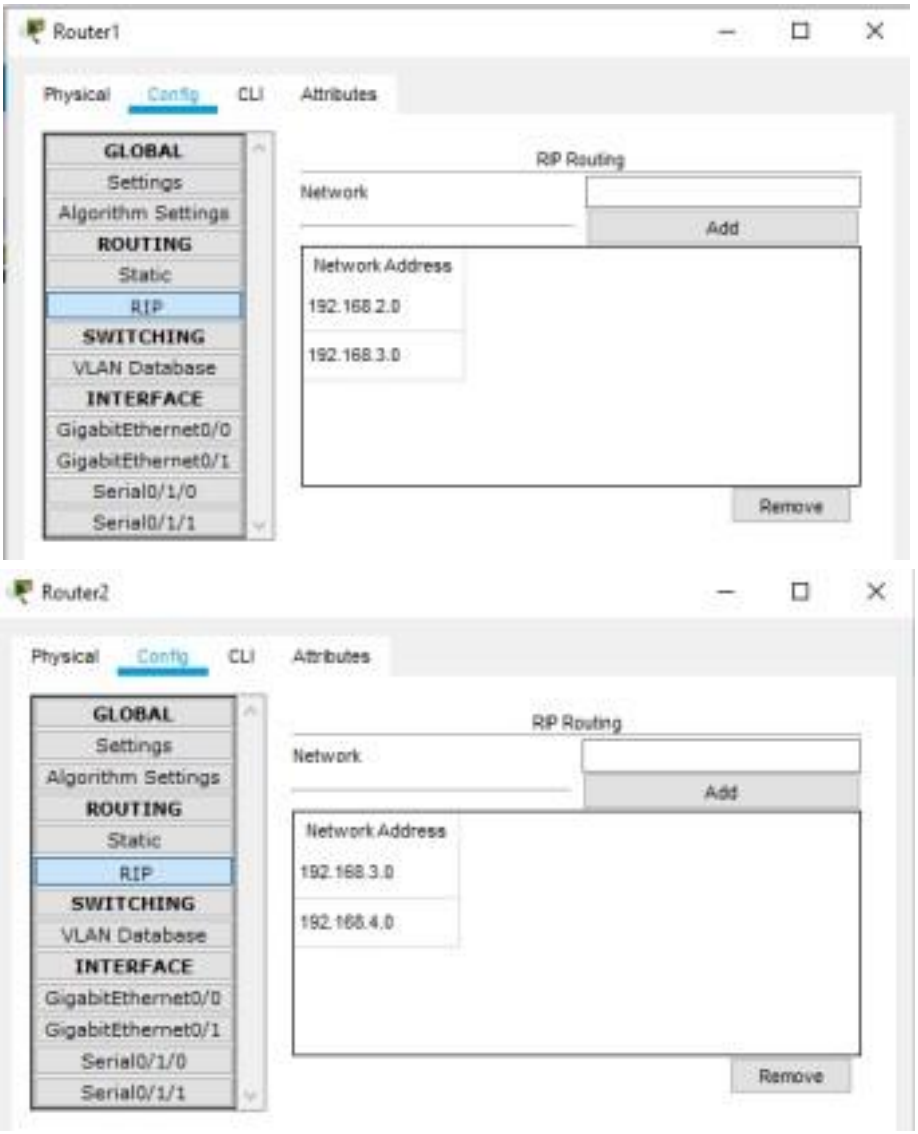
Configuring Router2



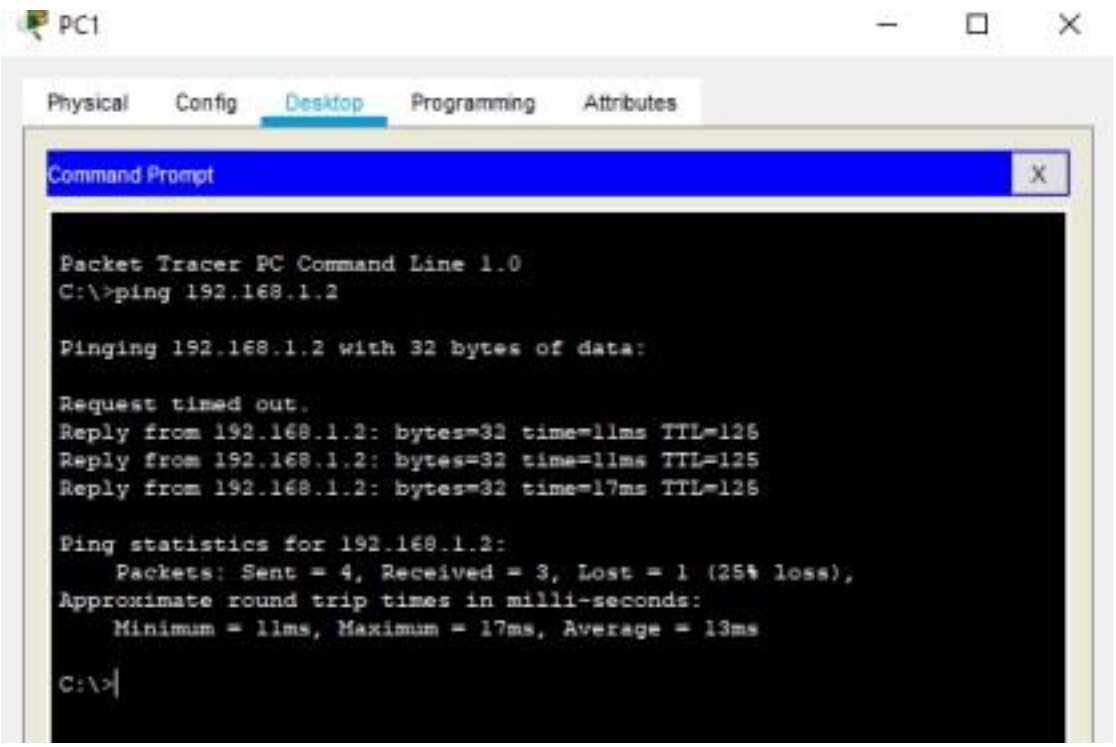


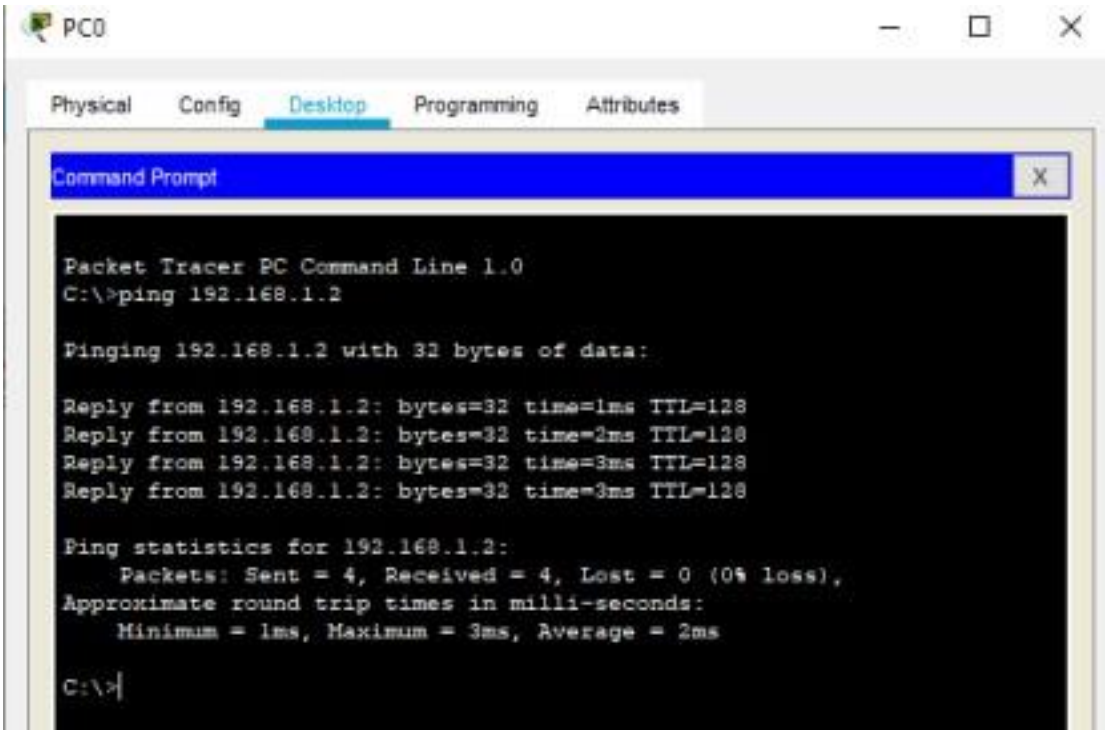
We need to set the Routing table in all the Routers so that each node could send and receive packets from others (RIP is set in all the Routers as follows)





Now we can check the connectivity by sending ping commands from any node to any other node





So, we conclude that the connectivity has been established

PART1: Enable the IOS IPS (on Router1)

Type the following command in the CLI mode of Router1

Router#show version

We will get a message informing whether the security Package is enabled or not

As seen above the security package is not enabled, to enable the security feature, type the following command in Router1

Router#configure terminal
Router(config)#license boot module c1900 technology-package securityk9 ACCEPT? [yes/no]: y

Press enter key

Router#
Router#reload
System configuration has been modified. Save? [yes/no]:y
Proceed with reload? [confirm] Press Enter key
Press RETURN to get started! Press Enter key

Router>enable
Router# Router#show version

We will get a message informing whether the security package is enabled or

not

As seen above now the security package has been enabled

Now type the following commands in the CLI mode of Router1

```
Router#
Router#clock set 10:30:45 march 3 2022
Router#mkdir smile
Create directory filename [smile]? Press enter key
Created dir flash:smile

Router#

Router#configure terminal
Router(config)#ip ips config location flash:smile
Router(config)#ip ips name iosips
Router(config)#ip ips notify log
Router(config)#ip ips signature-category
Router(config-ips-category)#category all



Router(config-ips-category-action)#retired true
Router(config-ips-category-action)#exit
```

```
Router(config-ips-category)#category ios_ips basic
Router(config-ips-category-action)#retired false
Router(config-ips-category-action)#exit
Router(config-ips-category)#exit
Do you want to accept these changes? [confirm]y

Router(config)#interface Serial0/1/0
Router(config-if)#ip ips iosips out
Router(config-if)#
Press enter key
Router(config-if)#exit
Router(config)#
```

Part 2: Modify the Signature

Type the following commands in the CLI mode of Router1

```
Router(config)#
Router(config)#ip ips signature-definition
Router(config-sigdef)#signature 2004 0
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#enabled true
Router(config-sigdef-sig-status)#exit
Router(config-sigdef-sig)#engine
Router(config-sigdef-sig-engine)#event-action produce-alert
Router(config-sigdef-sig-engine)#event-action deny-packet-inline
Router(config-sigdef-sig-engine)#exit
Router(config-sigdef-sig)#exit
Router(config-sigdef)#exit
Do you want to accept these changes? [confirm]y
Router(config)#
```

Now we need to verify the above IPS configuration, we do it first by pinging PC1 to SERVER and then from SERVER to PC1

PC1 to SERVER – The ping fails

Server to PC1 – The Ping is successful

We check the Syslog service on the server to check the logging activity, by typing the following commands in Router0

```
Router>enable
Router#configure terminal
Router(config)#logging 192.168.1.2
Router(config)#
Router(config)#
Router(config)#exit
Router#

Router#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/3 ms

Router#
```

Hence, we set the IPS and also verified it on Router1

Practical 7: Packet Tracer - Layer 2 Security Topology

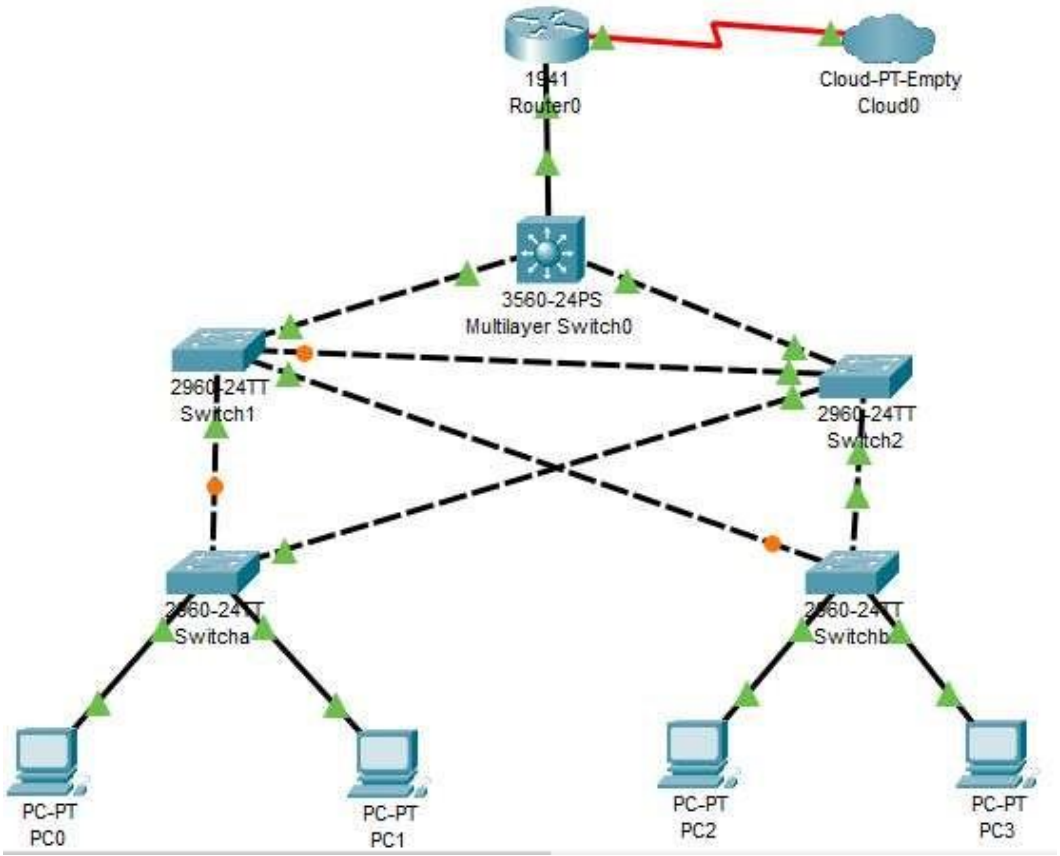
Objectives

- Assign the Central switch as the root bridge.
- Secure spanning-tree parameters to prevent STP manipulation attacks.
- Enable port security to prevent CAM table overflow attacks.

Background / Scenario

There have been a number of attacks on the network recently. For this reason, the network administrator has assigned you the task of configuring Layer 2 security. For optimum performance and security, the administrator would like to ensure that the root bridge is the 3560 Central switch. To prevent spanning-tree manipulation attacks, the administrator wants to ensure that the STP parameters are secure. To prevent against CAM table overflow attacks, the network administrator has decided to configure port security to limit the number of MAC addresses each switch port can learn. If the number of MAC addresses exceeds the set limit, the administrator would like the port to be shutdown.

Let us consider the following topology to present this case:



Let us consider the following interface table to connect the network devices:

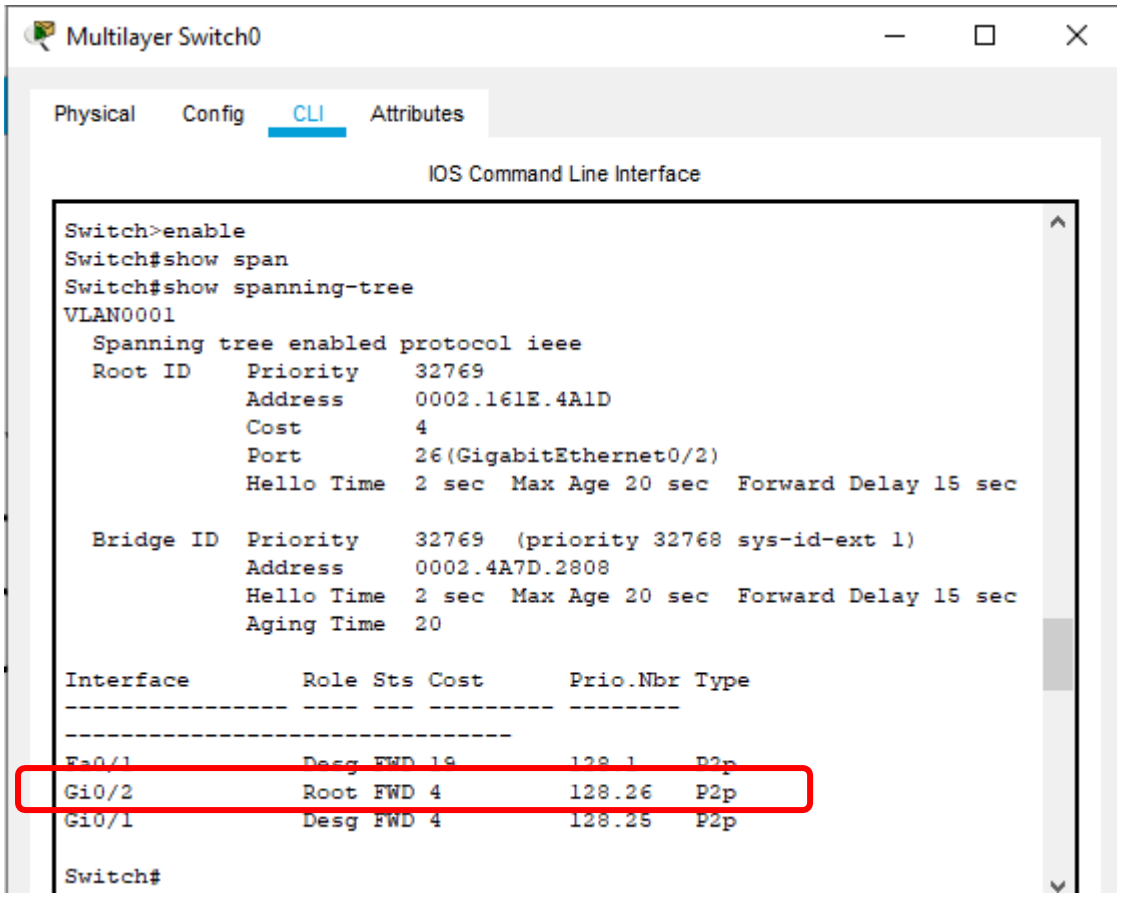
Note: Add one Serial Port in Router 0 and in Empty Cloud 0.

Device	Interface	Switch Port
PC 0	FastEthernet0	Switcha F0/1
PC 1	FastEthernet0	Switcha F0/2
PC 2	FastEthernet0	Switchb F0/1
PC 3	FastEthernet0	Switchb F0/2
Switch a	F0/23	Switch1 F0/23
	F0/24	Switch2 F0/1
Switch b	F0/23	Switch2 F0/23
	F0/24	Switch1 F0/1
Switch 1	F0/24	Switch2 F0/24
	GE 0/1	Multilayer Switch0 GE 0/1
Switch 2	GE 0/1	Multilayer Switch0 GE 0/2
Router 0	GE 0/1	Multilayer Switch0 F0/1
	S0/1/0	Cloud0 S4

Part 1: Configure Root Bridge

Type the following command in CLI mode of Multilayer Switch0, to check which is the Root bridge

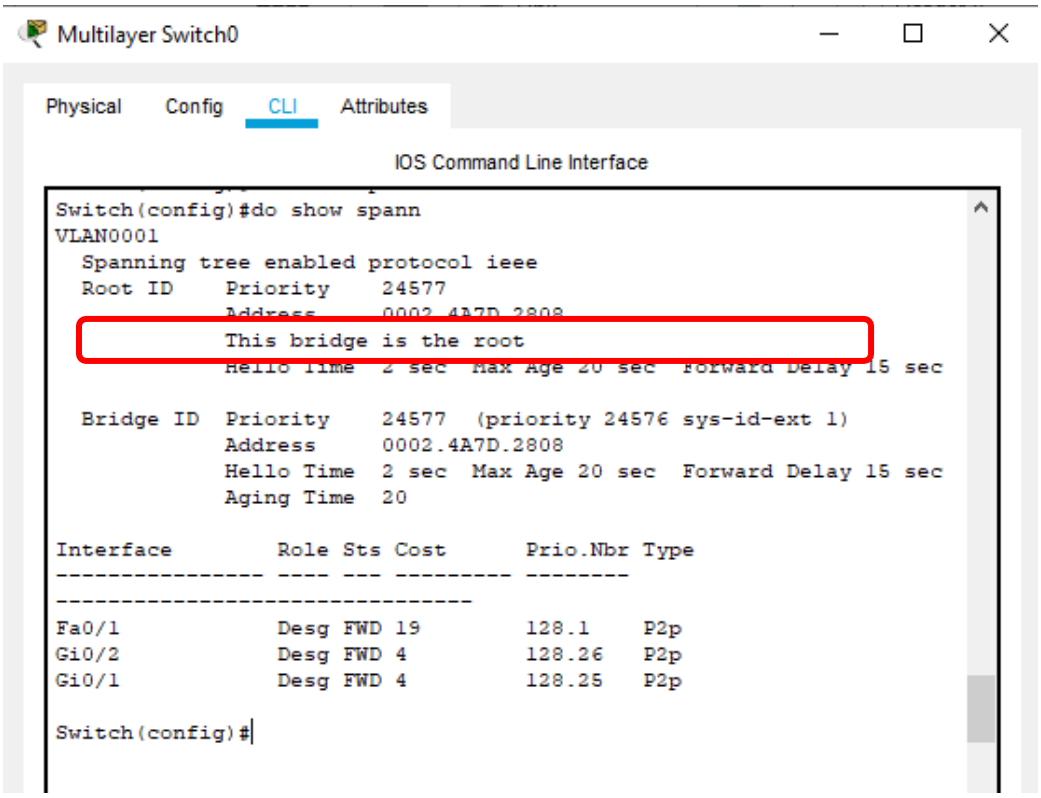
Switch>enable
Switch#show spanning-tree



The output shows that the bridge connected to GigabitEthernet 0/2 is the Root Bridge, i.e., Switch 2 is the Root Bridge in the above topology.

Now we need to make Multilayer Switch0 as the Root Bridge. Type the following commands in the CLI mode of Multilayer Switch0.

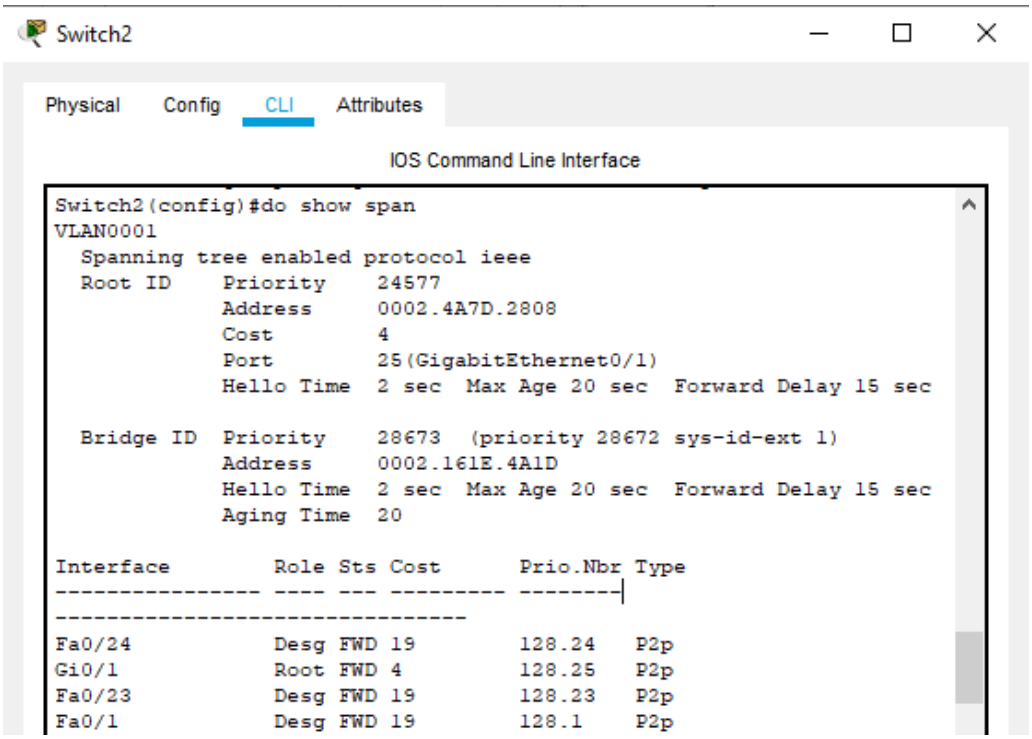
Switch#
Switch#configure terminal
Switch(config)#spanning-tree vlan 1 root primary
Switch(config)#do show spann



Now, we have made the Multilayer Switch0 as the Root Bridge.

But we also need to remove the Switch2 from Root Bridge. For that open the CLI mode of Switch2 and type the following code.

Switch2#configure terminal
Switch2(config)#spanning-tree vlan 1 root secondary
Switch2(config)#do show span



Thus, we have successfully made the central (Multilayer Switch0) as the Root Bridge.

Part 2: Protect Against STP Attacks
Open CLI mode of Switch a and type the following command

```
Switcha>enable
Switcha#configure termial
Switcha(config)#interface range fastEthernet 0/1-2
Switcha(config-if-range)#switchport mode access
Switcha(config-if-range)#spanning-tree portfast
Switcha(config-if-range)#spanning-tree bpduguard enable
```

Now minimize the Switch a window and open the Switch b CLI mode and type the same command

```
Switchb>enable
Switchb#configure termial
Switchb(config)#interface range fastEthernet 0/1-2
Switchb(config-if-range)#switchport mode access
Switchb(config-if-range)#spanning-tree portfast
Switchb(config-if-range)#spanning-tree bpduguard enable
```

Now minimize the Switch b window and open the Switch 1 CLI mode and type the following command

```
Switch1>enable
Switch1#configure terminal
Switch1(config)#interface range fastEthernet 0/23-24
Switch1(config-if-range)#spanning-tree guard root
```

Now minimize the Switch 1 window and open the Switch 2 CLI mode and type the same command

```
Switch2>enable
Switch2#configure terminal
Switch2(config)#interface range fastEthernet 0/23-24
Switch2(config-if-range)#spanning-tree guard root
```

Thus, we have Protected all the switch against STP Attacks.

Part 3: Configure Port Security and Disable unsed ports

Open CLI mode of Switch a and type the following command

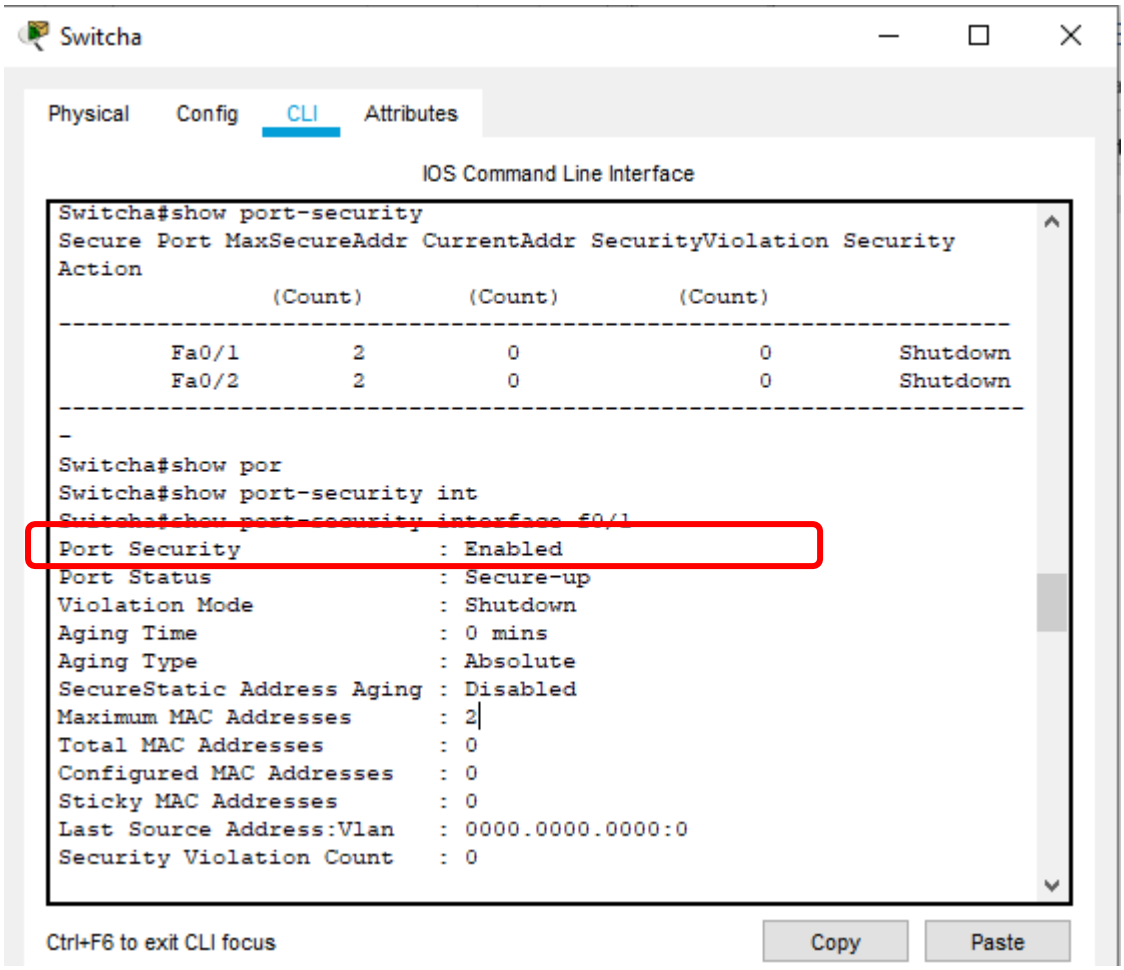
Switcha(config-if-range)#switchport port-security
Switcha(config-if-range)#switchport port-security maximum 2
Switcha(config-if-range)#switchport port-security mac-address sticky
Switcha(config-if-range)#switchport port-security violation shutdown

Now minimize the Switch a window and open the Switch b CLI mode and type the same command

Switchb(config-if-range)#switchport port-security
Switchb(config-if-range)#switchport port-security maximum 2
Switchb(config-if-range)#switchport port-security mac-address sticky
Switchb(config-if-range)#switchport port-security violation shutdown

Now let us check if the security is enabled or not. Open CLI mode of Switch a and type the following

Switcha(config-if-range)# CTRL Z
Switcha#show port-security interface f0/1



Let us now disable all the unused ports in switch a and switch b.

Open the CLI mode of Switch a and type the following command

```
Switcha#enable
Switcha#configure terminal
Switcha(config)#interface range fastEthernet 0/3-22
Switcha(config-if-range)#shutdown
```

Open the CLI mode of Switch b and type the following command

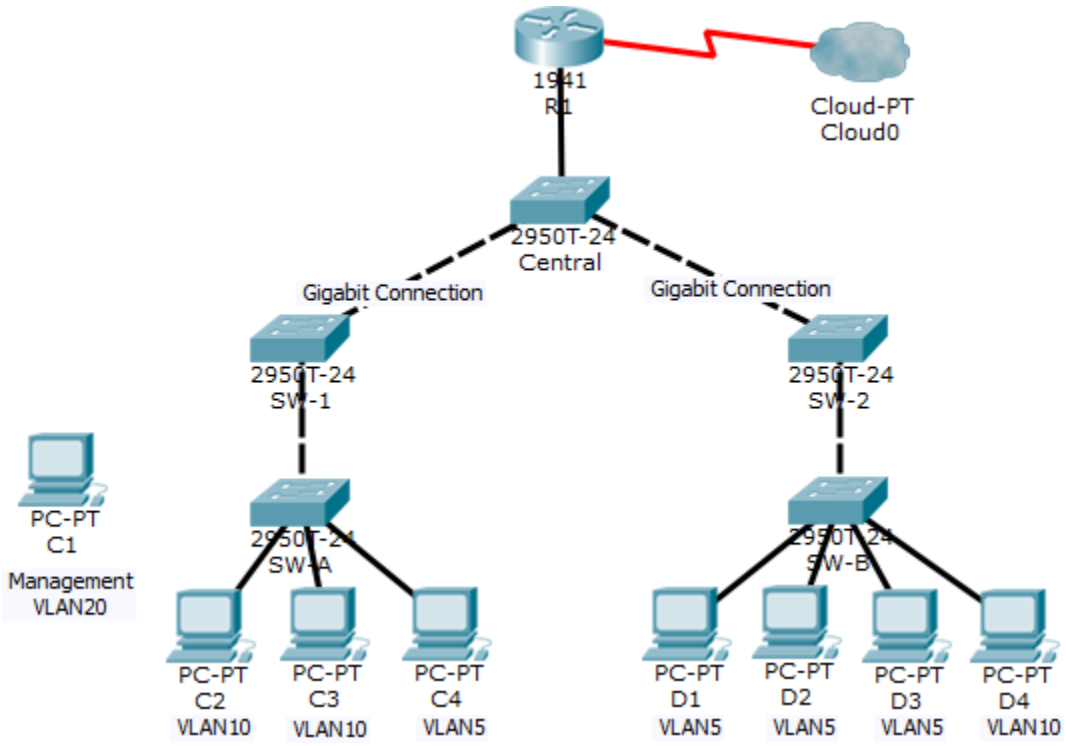
```
Switchb#enable
Switchb#configure terminal
Switchb(config)#interface range fastEthernet 0/3-22
Switchb(config-if-range)#shutdown
```

Thus, Port Security is enabled and all the unsed ports are disabled.

PRACTICAL - 8

Packet Tracer - Layer 2 VLAN Security

Topology



Objectives

- Connect a new redundant link between SW-1 and SW-2.
- Enable trunking and configure security on the new trunk link between SW-1 and SW-2.
- Create a new management VLAN (VLAN 20) and attach a management PC to that VLAN.
- Implement an ACL to prevent outside users from accessing the management VLAN.

Background / Scenario

A company's network is currently set up using two separate VLANs: VLAN 5 and VLAN 10. In addition, all trunk ports are configured with native VLAN 15. A network administrator wants to add a redundant link between switch SW-1 and SW-2. The link must have trunking enabled and all security requirements should be in place.

In addition, the network administrator wants to connect a management PC to switch SW-A. The administrator would like to enable the management PC to connect to all switches and the router, but does not want any other devices to connect to the management PC or the switches. The administrator would like to create a new VLAN 20 for management purposes.

All devices have been preconfigured with:

- Enable secret password: **ciscoenpa55**
- Console password: **ciscoconpa55**

- SSH username and password: **SSHadmin** / **ciscosshpa55**

Part 1: Verify Connectivity

Step 1: Verify connectivity between C2 (VLAN 10) and C3 (VLAN 10).

Step 2: Verify connectivity between C2 (VLAN 10) and D1 (VLAN 5).

Note: If using the simple PDU GUI packet, be sure to ping twice to allow for ARP.

Part 2: Create a Redundant Link Between SW-1 and SW-2

Step 1: Connect SW-1 and SW-2.

Using a crossover cable, connect port F0/23 on **SW-1** to port F0/23 on **SW-2**.

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

Trunking has already been configured on all pre-existing trunk interfaces. The new link must be configured for trunking, including all trunk security mechanisms. On both **SW-1** and **SW-2**, set the port to trunk, assign native VLAN 15 to the trunk port, and disable auto-negotiation.

```
SW-1(config)# interface f0/23
SW-1(config-if)# switchport mode trunk
SW-1(config-if)# switchport trunk native vlan 15
SW-1(config-if)# switchport nonegotiate
SW-1(config-if)# no shutdown

SW-2(config)# interface f0/23
SW-2(config-if)# switchport mode trunk
SW-2(config-if)# switchport trunk native vlan 15
SW-2(config-if)# switchport nonegotiate
SW-2(config-if)# no shutdown
```

Part 3: Enable VLAN 20 as a Management VLAN

The network administrator wants to access all switch and routing devices using a management PC. For security purposes, the administrator wants to ensure that all managed devices are on a separate VLAN.

Step 1: Enable a management VLAN (VLAN 20) on SW-A.

a. Enable VLAN 20 on **SW-A**.

```
SW-A(config)# vlan 20
SW-A(config-vlan)# exit
```

b. Create an interface VLAN 20 and assign an IP address within the 192.168.20.0/24 network.

```
SW-A(config)# interface vlan 20
SW-A(config-if)# ip address 192.168.20.1 255.255.255.0
```

Step 2: Enable the same management VLAN on all other switches.

a. Create the management VLAN on all switches: **SW-B**, **SW-1**, **SW-2**, and **Central**.

```
SW-B(config)# vlan 20
SW-B(config-vlan)# exit

SW-1(config)# vlan 20
SW-1(config-vlan)# exit

SW-2(config)# vlan 20
SW-2(config-vlan)# exit

Central(config)# vlan 20
Central(config-vlan)# exit
```

b. Create an interface VLAN 20 on all switches and assign an IP address within the 192.168.20.0/24 network.

```
SW-B(config)# interface vlan 20
SW-B(config-if)# ip address 192.168.20.2 255.255.255.0

SW-1(config)# interface vlan 20
SW-1(config-if)# ip address 192.168.20.3 255.255.255.0

SW-2(config)# interface vlan 20
SW-2(config-if)# ip address 192.168.20.4 255.255.255.0

Central(config)# interface vlan 20
Central(config-if)# ip address 192.168.20.5 255.255.255.0
```

Step 3: Connect and configure the management PC.

Connect the management PC to **SW-A** port F0/1 and ensure that it is assigned an available IP address within the 192.168.20.0/24 network.

Step 4: On SW-A, ensure the management PC is part of VLAN 20.

Interface F0/1 must be part of VLAN 20.

```
SW-A(config)# interface f0/1
SW-A(config-if)# switchport access vlan 20
SW-A(config-if)# no shutdown
```

Step 5: Verify connectivity of the management PC to all switches.

The management PC should be able to ping **SW-A**, **SW-B**, **SW-1**, **SW-2**, and **Central**.

Part 4: Enable the Management PC to Access Router R1

Step 1: Enable a new subinterface on router R1.

a. Create subinterface g0/0.3 and set encapsulation to dot1q 20 to account for VLAN 20.

```
R1(config)# interface g0/0.3
R1(config-subif)# encapsulation dot1q 20
```

b. Assign an IP address within the 192.168.20.0/24 network.

```
R1(config)# interface g0/0.3
R1(config-subif)# ip address 192.168.20.100 255.255.255.0
```

Step 2: Verify connectivity between the management PC and R1.

Be sure to configure the default gateway on the management PC to allow for connectivity.

Step 3: Enable security.

While the management PC must be able to access the router, no other PC should be able to access the management VLAN.

a. Create an ACL that allows only the Management PC to access the router.

Example: (may vary from student configuration)

```
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
```

b. Apply the ACL to the proper interface(s).

Example: (may vary from student configuration)

```
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
```

Note: Access list 102 is used to only allow the Management PC (192.168.20.50 in this example) to access the router. This prevents an IP address change to bypass the ACL.

Note: There are multiple ways in which an ACL can be created to accomplish the necessary security. For this reason, grading on this portion of the activity is based on the correct connectivity requirements. The management PC must be able to connect to all switches and the router. All other PCs should not be able to connect to any devices within the management VLAN.

Step 4: Verify security.

a. Verify only the Management PC can access the router. Use SSH to access **R1** with username **SSHadmin** and password **ciscosshpa55**.

```
PC> ssh -l SSHadmin 192.168.20.100
```

b. From the management PC, ping **SW-A**, **SW-B**, and **R1**. Were the pings successful? Explain.

_____

_____

_____

The pings should have been successful because all devices within the 192.168.20.0 network should be able to ping one another. Devices within VLAN20 are not required to route through the router.

c. From **D1**, ping the management PC. Were the pings successful? Explain.

_____

The ping should have failed because for a device within a different VLAN to successfully ping a device within VLAN20, it must be routed. The router has an ACL that prevents all packets from accessing the 192.168.20.0 network.

Step 5: Check results.

Your completion percentage should be 100%. Click **Check Results** to view feedback and verification of which required components have been completed.

If all components appear to be correct and the activity still shows incomplete, it could be due to the connectivity tests that verify the ACL operation.

!!! Script for SW-1

```
conf t
interface f0/23
 switchport mode trunk
 switchport trunk native vlan 15
 switchport nonegotiate
 no shutdown
vlan 20
 exit
interface vlan 20
 ip address 192.168.20.3 255.255.255.0
```

!!! Script for SW-2

```
conf t
interface f0/23
 switchport mode trunk
 switchport trunk native vlan 15
 switchport nonegotiate
 no shutdown
vlan 20
 exit
interface vlan 20
 ip address 192.168.20.4 255.255.255.0
```

!!! Script for SW-A

```
conf t
vlan 20
 exit
interface vlan 20
 ip address 192.168.20.1 255.255.255.0
interface f0/1
 switchport access vlan 20
 no shutdown
```

!!! Script for SW-B

```
conf t
vlan 20
 exit
interface vlan 20
 ip address 192.168.20.2 255.255.255.0
```

!!! Script for Central

```
conf t
vlan 20
 exit
interface vlan 20
 ip address 192.168.20.5 255.255.255.0
```

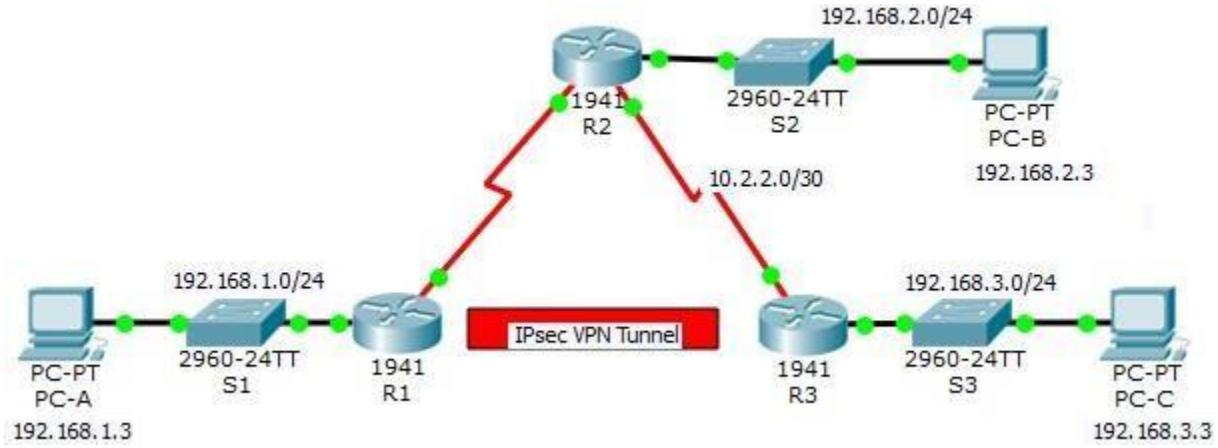
!!! Script for R1

```
conf t
interface GigabitEthernet0/0.1
 ip access-group 101 in
interface GigabitEthernet0/0.2
 ip access-group 101 in
interface g0/0.3
 encapsulation dot1q 20
 ip address 192.168.20.100 255.255.255.0
access-list 101 deny ip any 192.168.20.0 0.0.0.255
access-list 101 permit ip any any
access-list 102 permit ip host 192.168.20.50 any
line vty 0 4
 access-class 102 in
```

PRACTICAL - 9

Packet Tracer - Configure and Verify a Site-to-Site IPsec VPN Using CLI

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Objectives

- Verify connectivity throughout the network.
- Configure R1 to support a site-to-site IPsec VPN with R3.

Background / Scenario

The network topology shows three routers. Your task is to configure R1 and R3 to support a site-to-site IPsec VPN when traffic flows between their respective LANs. The IPsec VPN tunnel is from R1 to R3 via R2. R2

acts as a pass-through and has no knowledge of the VPN. IPsec provides secure transmission of sensitive information over unprotected networks, such as the Internet. IPsec operates at the network layer and protects and authenticates IP packets between participating IPsec devices (peers), such as Cisco routers.

ISAKMP Phase 1 Policy Parameters

Parameters		R1	R3
Key Distribution Method	Manual or **ISAKMP**	**ISAKMP**	**ISAKMP**
Encryption Algorithm	**DES**, 3DES, or AES	AES 256	AES 256
Hash Algorithm	MD5 or **SHA-1**	**SHA-1**	**SHA-1**
Authentication Method	Pre-shared keys or **RSA**	pre-share	pre-share
Key Exchange	DH Group 1, 2, or 5	DH 5	DH 5
IKE SA Lifetime	86400 seconds or less	**86400**	**86400**
ISAKMP Key		vpnpa55	vpnpa55

Note: Bolded parameters are defaults. Only unbolded parameters have to be explicitly configured.

IPsec Phase 2 Policy Parameters

Parameters	R1	R3
Transform Set Name	VPN-SET	VPN-SET
ESP Transform Encryption	esp-aes	esp-aes
ESP Transform Authentication	esp-sha-hmac	esp-sha-hmac
Peer IP Address	10.2.2.2	10.1.1.2
Traffic to be Encrypted	access-list 110 (source 192.168.1.0 dest 192.168.3.0)	access-list 110 (source 192.168.3.0 dest 192.168.1.0)
Crypto Map Name	VPN-MAP	VPN-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp

The routers have been pre-configured with the following:

- Password for console line: **ciscoconpa55**
- Password for vty lines: **ciscovtypa55**
- Enable password: **ciscoenpa55**
- SSH username and password: **SSHadmin** / **ciscosshpa55**
- OSPF 101

Part 1: Configure IPsec Parameters on R1

Step 1: Test connectivity.

Ping from PC-A to PC-C.

Step 2: Enable the Security Technology package.

a. On R1, issue the **show version** command to view the Security Technology package license information.

b. If the Security Technology package has not been enabled, use the following command to enable the package.

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

c. Accept the end-user license agreement.

d. Save the running-config and reload the router to enable the security license.

e. Verify that the Security Technology package has been enabled by using the **show version** command.

Step 3: Identify interesting traffic on R1.

Configure ACL 110 to identify the traffic from the LAN on R1 to the LAN on R3 as interesting. This interesting traffic will trigger the IPsec VPN to be implemented when there is traffic between the R1 to R3 LANs. All other traffic sourced from the LANs will not be encrypted. Because of the implicit **deny all**, there is no need to configure a **deny ip any any** statement.

```
R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255
```

Step 4: Configure the IKE Phase 1 ISAKMP policy on R1.

Configure the **crypto ISAKMP policy 10** properties on R1 along with the shared crypto key **vpnpa55**. Refer to the ISAKMP Phase 1 table for the specific parameters to configure. Default values do not have to be configured. Therefore, only the encryption method, key exchange method, and DH method must be configured.

Note: The highest DH group currently supported by Packet Tracer is group 5. In a production network, you would configure at least DH 14.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 5
R1(config-isakmp)# exit
R1(config)# crypto isakmp key vpnpa55 address 10.2.2.2
```

Step 5: Configure the IKE Phase 2 IPsec policy on R1.

a. Create the transform-set VPN-SET to use **esp-aes** and **esp-sha-hmac**.

```
R1(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
```

b. Create the crypto map VPN-MAP that binds all of the Phase 2 parameters together. Use sequence number 10 and identify it as an ipsec-isakmp map.

```
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 10.2.2.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit
```

Step 6: Configure the crypto map on the outgoing interface.

Bind the **VPN-MAP** crypto map to the outgoing Serial 0/0/0 interface.

```
R1(config)# interface s0/0/0
R1(config-if)# crypto map VPN-MAP
```

Part 2: Configure IPsec Parameters on R3

Step 1: Enable the Security Technology package.

a. On R3, issue the **show version** command to verify that the Security Technology package license information has been enabled.

b. If the Security Technology package has not been enabled, enable the package and reload R3.

Step 2: Configure router R3 to support a site-to-site VPN with R1.

Configure reciprocating parameters on R3. Configure ACL 110 identifying the traffic from the LAN on R3 to the LAN on R1 as interesting.

```
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255
```

Step 3: Configure the IKE Phase 1 ISAKMP properties on R3.

Configure the crypto ISAKMP policy 10 properties on R3 along with the shared crypto key vpnpa55.

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes 256
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 5
R3(config-isakmp)# exit
R3(config)# crypto isakmp key vpnpa55 address 10.1.1.2
```

Step 4: Configure the IKE Phase 2 IPsec policy on R3.

a. Create the transform-set VPN-SET to use **esp-aes** and **esp-sha-hmac**.

```
R3(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
```

b. Create the crypto map VPN-MAP that binds all of the Phase 2 parameters together. Use sequence number 10 and identify it as an ipsec-isakmp map.

```
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 10.1.1.2
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit
```

Step 5: Configure the crypto map on the outgoing interface.

Bind the VPN-MAP crypto map to the outgoing Serial 0/0/1 interface. **Note**: This is not graded.

```
R3(config)# interface s0/0/1
R3(config-if)# crypto map VPN-MAP
```

Part 3: Verify the IPsec VPN

Step 1: Verify the tunnel prior to interesting traffic.

Issue the **show crypto ipsec sa** command on R1. Notice that the number of packets encapsulated, encrypted, decapsulated, and decrypted are all set to 0.

Step 2: Create interesting traffic.

Ping PC-C from PC-A.

Step 3: Verify the tunnel after interesting traffic.

On R1, re-issue the **show crypto ipsec sa** command. Notice that the number of packets is more than 0, which indicates that the IPsec VPN tunnel is working.

Step 4: Create uninteresting traffic.

Ping PC-B from PC-A. **Note**: Issuing a ping from router R1 to PC-C or R3 to PC-A is not interesting traffic.

Step 5: Verify the tunnel.

On R1, re-issue the **show crypto ipsec sa** command. Notice that the number of packets has not changed, which verifies that uninteresting traffic is not encrypted.

Step 6: Check results.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

!!! Script for R1

```
config t
license boot module c1900 technology-package securityk9
yes
end
copy running-config startup-config

reload

config t
access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
crypto isakmp policy 10
 encryption aes 256
 authentication pre-share
 group 5
 exit
crypto isakmp key vpnpa55 address 10.2.2.2
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
 description VPN connection to R3
 set peer 10.2.2.2
 set transform-set VPN-SET
 match address 110
 exit
```

```
interface S0/0/0
 crypto map VPN-MAP
```

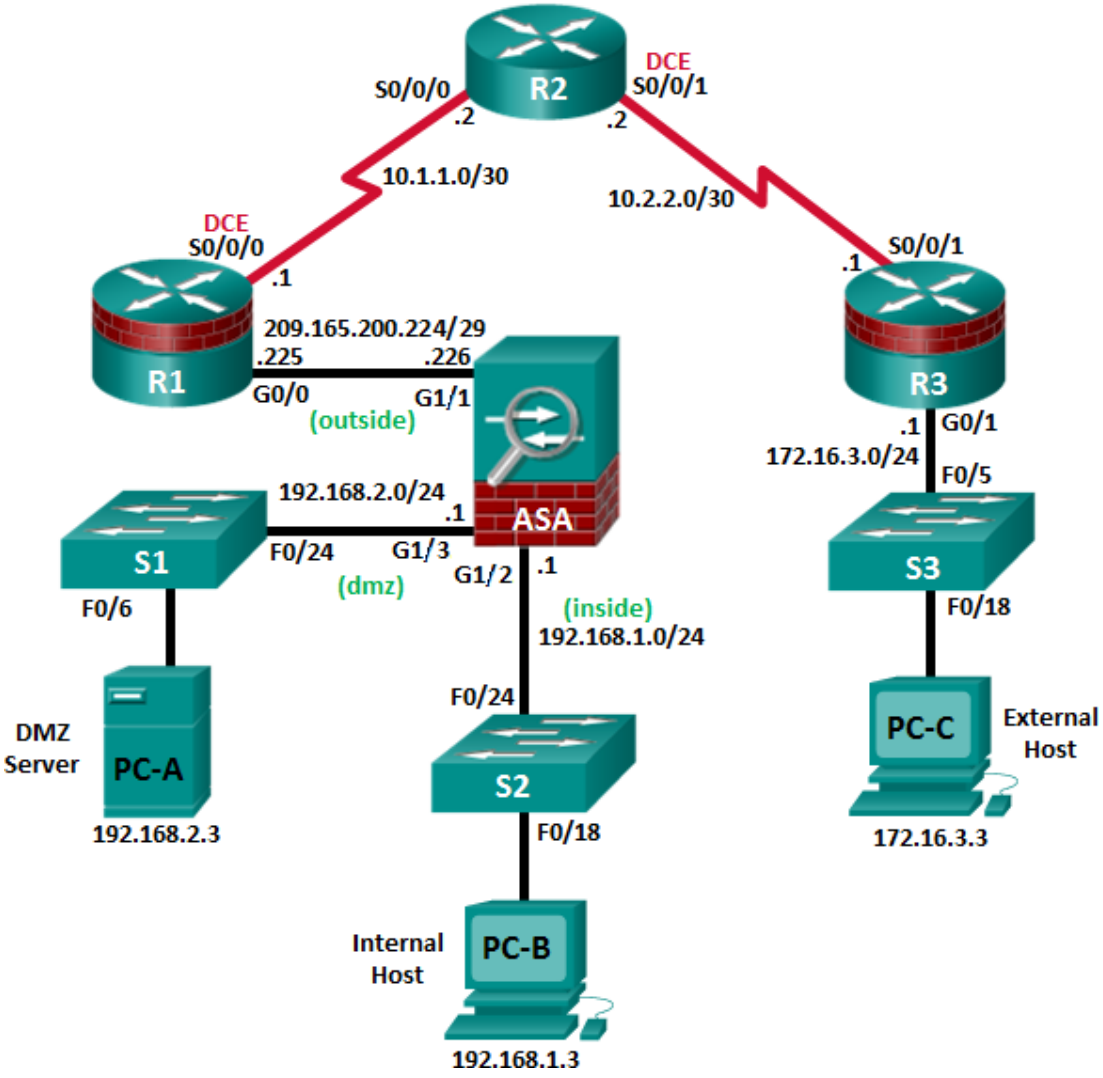
!!! Script for R3

```
config t
access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
crypto isakmp policy 10
 encryption aes 256
 authentication pre-share
 group 5
 exit
crypto isakmp key vpnpa55 address 10.1.1.2
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
 crypto map VPN-MAP 10 ipsec-isakmp
 description VPN connection to R1
 set peer 10.1.1.2
 set transform-set VPN-SET
 match address 110
 exit
interface S0/0/1
 crypto map VPN-MAP
```

PRACTICAL - 10

Configuring ASA Basic Settings and Firewall Using CLI

Topology



Note: ISR G2 devices use GigabitEthernet interfaces instead of FastEthernet interfaces.

IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0	209.165.200.225	255.255.255.248	N/A	ASA G1/1
	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
R3	G0/1	172.16.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
ASA	G1/2	192.168.1.1	255.255.255.0	NA	S2 F0/24
ASA	G1/1	209.165.200.226	255.255.255.248	NA	R1 G0/0
ASA	G1/3	192.168.2.1	255.255.255.0	NA	S1 F0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 F0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 F0/18

Objectives

Part 1: Basic Router/Switch/PC Configuration

- Configure hostnames and interface IP addresses for routers, switches, and PCs.
- Configure static routing, including default routes, between R1, R2, and R3.
- Enable HTTP and SSH access for R1.
- Configure PC host IP settings.
- Verify connectivity between hosts, switches, and routers.
- Save the basic running configuration for each router and switch.

Part 2: Accessing the ASA Console and Using CLI Setup Mode to Configure Basic Settings

- Access the ASA console and view hardware, software, and configuration settings.
- Determine the ASA version, interfaces, and license.
- Determine the file system and contents of flash memory.
- Use CLI Setup mode to configure basic settings (hostname, passwords, clock, etc.).

Part 3: Configuring Basic ASA Settings and Interface Security Levels Using the CLI.

- Configure the hostname and domain name.
- Configure the login and enable passwords.
- Set the date and time.
- Configure the inside and outside interfaces.
- Test connectivity to the ASA.
- Configure SSH access to the ASA.

- Configure HTTPS access on the ASA for ASDM.

Part 4: Configuring Routing, Address Translation, and Inspection Policy Using the CLI

- Configure a static default route for the ASA.
- Configure PAT and network objects.
- Modify the MPF application inspection global service policy.

Part 5: Configuring DHCP, AAA, and SSH

- Configure the ASA as a DHCP server/client.
- Configure Local AAA user authentication.
- Configure SSH remote access to the AAA.

Part 6: Configuring DMZ, Static NAT, and ACLs

- Configure the DMZ interface VLAN 3 on the ASA.
- Configure static NAT for the DMZ server using a network object.
- Configure an ACL to allow access to the DMZ for Internet users.
- Verify access to the DMZ server for external and internal users.

Part 1: Basic Router/Switch/PC Configuration

In Part 1 of this lab, you will configure basic settings on the routers, such as interface IP addresses and static routing.

Note: Do not configure ASA settings at this time.

Step 1: Configure basic settings for routers and switches.

a. Configure hostnames as shown in the topology for each router.

b. Configure router interface IP addresses as shown in the IP Addressing Table.

c. Configure a clock rate for routers with a DCE serial cable attached to their serial interface. R1 is shown here as an example.

```
R1(config)# interface S0/0/0
R1(config-if)# clock rate 64000
```

d. Configure the host name for the switches. Other than the host name, the switches can be left in their default configuration state. Configuring the VLAN management IP address for the switches is optional.

Step 2: Configure static routing on the routers.

a. Configure a static default route from R1 to R2 and from R3 to R2.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/0
R3(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/1
```

b. Configure a static route from R2 to the R1 G0/0 subnet (connected to ASA interface Gi1/1) and a static route from R2 to the R3 LAN.

```
R2(config)# ip route 209.165.200.224 255.255.255.248 Serial0/0/0
R2(config)# ip route 172.16.3.0 255.255.255.0 Serial0/0/1
```

Step 3: Enable the HTTP server and configure a user account, encrypted passwords, and crypto keys for SSH.

a. Enable HTTP access to R1 using the **ip http server** command in global config mode. Set the console and VTY passwords to cisco. This will provide web and SSH targets for testing later in the lab.

```
R1(config)# ip http server
```

b. Configure a minimum password length of 10 characters using the **security passwords** command.

```
R1(config)# security passwords min-length 10
```

c. Configure a domain name.

```
R1(config)# ip domain-name ccnasecurity.com
```

d. Configure crypto keys for SSH.

```
R1(config)# crypto key generate rsa general-keys modulus 1024
```

e. Configure an admin01 user account using algorithm-type scrypt for encryption and a password of admin01pass.

```
R1(config)# username admin01 algorithm-type scrypt secret admin01pass
```

f. Configure line console 0 to use the local user database for logins. For additional security, the **exec-timeout** command causes the line to log out after five minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.

Note: To avoid repetitive logins during this lab, the **exec-timeout** command can be set to 0 0, which prevents it from expiring. However, this is not considered to be a good security practice.

```
R1(config)# line console 0
R1(config-line)# login local
R1(config-line)# exec-timeout 5 0
R1(config-line)# logging synchronous
```

g. Configure line vty 0 4 to use the local user database for logins and restrict access to only SSH connections.

```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exec-timeout 5 0
```

h. Configure the enable password with strong encryption.

```
R1(config)# enable algorithm-type scrypt secret admin01pass
```

Step 4: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A, PC-B, and PC-C as shown in the IP Addressing Table.

Step 5: Verify connectivity.

Because the ASA is the focal point for the network zones, and it has not yet been configured, there will be no connectivity between devices that are connected to it. However, PC-C should be able to ping the R1 interface. From PC-C, ping the R1 G0/0 IP address (209.165.200.225). If these pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-C to R1 G0/0 and S0/0/0 you have demonstrated that static routing is configured and functioning correctly.

Step 6: Save the basic running configuration for each router and switch.

Part 2: Accessing the ASA Console and Using CLI Setup to Configure Basic Settings

In Part 2 of this lab, you will access the ASA via the console and use various **show** commands to determine hardware, software, and configuration settings. You will clear the current configuration and use the CLI interactive setup utility to configure basic ASA settings.

Note: Do not configure ASA settings at this time.

Step 1: Access the ASA console.

a. Enter privileged mode with the **enable** command and password (if a password has been set). The password is blank by default. Press **Enter**. If the password has been changed to what is specified in this lab, enter the word **class**. The default ASA hostname and prompt is *ciscoasa*>.

```
ciscoasa> enable
Password: class (or press Enter if none set)
```

Step 2: Determine the ASA version, interfaces, and license.

The ASA 5506 comes with eight Gigabit Ethernet ports.

Use the **show version** command to determine various aspects of this ASA device.

```
ciscoasa# show version

Cisco Adaptive Security Appliance Software Version 9.8(2)
Firepower Extensible Operating System Version 2.2(2.52)
Device Manager Version 7.8(1)

Compiled on Sun 27-Aug-17 13:06 PDT by builders
System image file is "disk0:/asa982-lfbff-k8.SPA"
Config file at boot was "startup-config"

ciscoasa up 10 mins 59 secs

Hardware:   ASA5506, 4096 MB RAM, CPU Atom C2000 series 1250 MHz, 1 CPU (4
cores)
Internal ATA Compact Flash, 8000MB
BIOS Flash M25P64 @ 0xfed01000, 16384KB

Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision
0x1)
                             Number of accelerators: 1

 1: Ext: GigabitEthernet1/1  : address is 00f2.8b8e.69ef, irq 255
 2: Ext: GigabitEthernet1/2  : address is 00f2.8b8e.69f0, irq 255
 3: Ext: GigabitEthernet1/3  : address is 00f2.8b8e.69f1, irq 255
 4: Ext: GigabitEthernet1/4  : address is 00f2.8b8e.69f2, irq 255
 5: Ext: GigabitEthernet1/5  : address is 00f2.8b8e.69f3, irq 255
 6: Ext: GigabitEthernet1/6  : address is 00f2.8b8e.69f4, irq 255
 7: Ext: GigabitEthernet1/7  : address is 00f2.8b8e.69f5, irq 255
 8: Ext: GigabitEthernet1/8  : address is 00f2.8b8e.69f6, irq 255
<output omitted>
```

Step 3: Determine the file system and contents of flash memory.

a. Display the ASA file system using the **show file system** command. Determine what prefixes are supported.

```
ciscoasa# show file system
File Systems:
     Size(b)      Free(b)      Type      Flags  Prefixes
* 7859437568    4465147904    disk      rw      disk0: flash:
              -             -  disk      rw      disk1:
              -             -  network   rw      tftp:
              -             -  opaque    rw      system:
              -             -  network   ro      http:
              -             -  network   ro      https:
              -             -  network   rw      scp:
              -             -  network   rw      ftp:
              -             -  network   wo
```

What is another name for flash:?_____

b. Display the contents of flash memory using one of these commands: **show flash**, **show disk0**, **dir flash:**, or **dir disk0:**.

c.

```
ciscoasa# show flash
--#--  --length--  -----date/time --------path
  103       33        Nov 29 2017 10:34:52  .boot_string
   11     4096        Jan 09 2016 19:43:02  log
```

```
      13    65486       Nov 29 2017 11:28:45  log/asa-appagent.log
      20    4096        Jan 09 2016 19:43:52  crypto_archive
      21    4096        Jan 09 2016 19:43:56  coredumpinfo
      22    59          Jan 09 2016 19:43:56  coredumpinfo/coredump.cfg
     104    08563072    Nov 24 2017 14:55:22  asa982-lfbff-k8.SPA
     105    5209829     Oct 17 2017 21:50:48  anyconnect-win-4.5.02033-
        webdeploy-k9.pkg
     106     26916068    Nov 24 2017 15:22:28  asdm-781.bin
7859437568 bytes total (4465147904 bytes free)
```

Step 4: Determine the current running configuration.

The ASA 5506 is commonly used as an edge security device that connects a small business or teleworker to an ISP device, such as a DSL or cable modem, for access to the Internet.

Display the current running configuration using the **show running-config** command.

```
ciscoasa# show running-config
: Saved
: Serial Number: JAD2002064E
: Hardware:   ASA5506, 4096 MB RAM, CPU Atom C2000 series 1250 MHz, 1 CPU (4
cores)
:
ASA Version 9.8(2)
!
hostname ciscoasa
enable password
$sha512$5000$ftqbmZLcP1yvT9in1bvjlg==$+GU2ZHobKrNifvyb45nWEQ== pbkdf2
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
names
!
interface GigabitEthernet1/1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/2
```

```
 shutdown
 no nameif
 no security-level
 no ip address
!
<output omitted>
```

Note: To stop the output from a command using the CLI, press **Q**.

You can restore the ASA to its factory default settings by using the **configure factory-default** command.

```
ciscoasa# conf t
ciscoasa(config)# configure factory-default

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
Executing command: …
Executing command: …
Executing command: …
Factory-default configuration is completed
<output omitted>
```

Note: If you receive a prompt for Anonymous Error reporting, proceed by answering **No**.

Review this output and pay attention to the VLAN interfaces, NAT-related, and DHCP-related sections. These will be configured later in this lab using the CLI.

You may want to capture and print the factory-default configuration as a reference. Use the terminal emulation program to copy it from the ASA and paste it into a text document. You can then edit this file if desired, so that it contains only valid commands. You should remove password commands and enter the **no shut** command to bring up the desired interfaces.

Step 5: Clear the previous ASA configuration settings.

Use the **write erase** command to remove the startup-config file from flash memory.

```
ciscoasa# write erase
Erase configuration in flash memory? [confirm]
[OK]
ciscoasa#

ciscoasa# show start
No Configuration
```

Note: The IOS command **erase startup-config** is not supported on the ASA.

Use the **reload** command to restart the ASA. This causes the ASA to come up in CLI Setup mode. If prompted that the config has been modified and needs to be saved, respond with **N**, and then press **Enter** to proceed with the reload.

```
ciscoasa# reload
Proceed with reload? [confirm]
ciscoasa#
*** --- START GRACEFUL SHUTDOWN ---
Shutting down isakmp
Shutting down webvpn
Shutting down sw-module
Shutting down License Controller
Shutting down File system
*** --- SHUTDOWN NOW ---
Process shutdown finished
Rebooting.....
CISCO SYSTEMS
Cisco Systems ROMMON, Version 1.1.8, RELEASE SOFTWARE<output omitted>
```

Step 6: Use the Setup interactive CLI mode to configure basic settings.

When the ASA completes the reload process, it should detect that the startup-config file is missing and present a series of interactive prompts to configure basic ASA settings. If it does not come up in this mode, repeat Step 5. As an alternative, you can run the **setup** command at the global configuration mode prompt,

Note: The interactive prompt mode does not configure the ASA with factory defaults as described in Step 4. This mode can be used to configure minimal basic settings, such as hostname, clock, and passwords. You can also go directly to the CLI to configure the ASA settings, as described in Part 3.

Respond to the Setup interactive prompts as shown here, after the ASA reloads.

```
Pre-configure Firewall now through interactive prompts [yes]? <Enter>
Firewall Mode [Routed]: <Enter>
Enable password [<use current password>]: class
Allow password recovery [yes]? <Enter>
Clock (UTC):
  Year [2017]: <Enter>
  Month [Oct]: <Enter>
  Day [4]: <Enter>
  Time [09:09:08]: <Enter>
Management IP address: 192.168.100.1
Management network mask: 255.255.255.0
Host name: ASA-Init
Domain name: generic.com
IP address of host running Device Manager: <Enter>

The following configuration will be used:
Enable password: class
Allow password recovery: yes
Clock (UTC): 09:09:08 Oct 4 2017
Firewall Mode: Routed
Management IP address: 192.168.1.1
```

```
Management network mask: 255.255.255.0
Host name: ASA-Init
Domain name: generic.com

Use this configuration and save to flash? [yes] <Enter>

INFO: Security level for "management" set to 0 by default.
Cryptochecksum: 83d45883 a8343ed5 68b4810c 6f60ef05

4047 bytes copied in 0.80 secs
ASA-Init>
```

Note: In the above configuration, the IP address of the host running ASDM was left blank. It is not necessary to install ASDM on a host. It can be run from the flash memory of the ASA device itself using the browser of the host.

Note: The responses to the prompts are automatically stored in the startup-config and the running config. However, additional security-related commands, such as a global default inspection service policy, are inserted into the running-config by the ASA OS.

a. Enter privileged EXEC mode with the **enable** command. Enter **class** for the password.

b. Issue the **show run** command to see the additional security-related configuration commands that are inserted by the ASA.

c. Issue the **copy run start** command to capture the additional security-related commands in the startup-config file.

Part 3: Configuring ASA Settings and Interface Security Using the CLI

In Part 3, you will configure basic settings by using the ASA CLI, even though some of them were already configured using the Setup mode interactive prompts in Part 2. In this part, you will start with the settings configured in Part 2 and then add to or modify them to create a complete basic configuration.

Tip: Many ASA CLI commands are similar to, if not the same, as those used with the Cisco IOS CLI. In addition, the process of moving between configuration modes and sub-modes is essentially the same.

Note: You must complete Part 2 before beginning Part 3.

Step 1: Configure the hostname and domain name.

a. Enter global configuration mode using the **config t** command. The first time you enter configuration mode after running Setup, you will be prompted to enable anonymous reporting. Respond with no.

```
ASA-Init# config t
ASA-Init(config)#

****************************** NOTICE ******************************

Help to improve the ASA platform by enabling anonymous reporting,
which allows Cisco to securely receive minimal error and health
information from the device. To learn more about this feature,
please visit: http://www.cisco.com/go/smartcall
```

```
Would you like to enable anonymous error reporting to help improve
the product? [Y]es, [N]o, [A]sk later: n

In the future, if you would like to enable this feature,
issue the command "call-home reporting anonymous".
```

b. Configure the ASA hostname using the **hostname** command.

```
ASA-Init(config)# hostname CCNAS-ASA
```

c. Configure the domain name using the **domain-name** command.

```
CCNAS-ASA(config)# domain-name ccnasecurity.com
```

Step 2: Configure the login and enable mode passwords.

a. The login password is used for Telnet connections (and SSH prior to ASA version 8.4). By default, it is set to cisco, but since the default startup configuration was erased you have the option to configure the login password using the **passwd** or **password** command. This command is optional because later in the lab we will configure the ASA for SSH, and not Telnet access.

```
CCNAS-ASA(config)# passwd cisco
```

b. Configure the privileged EXEC mode (enable) password using the **enable password** command.

```
CCNAS-ASA(config)# enable password class
```

Step 3: Set the date and time.

The date and time can be set manually using the **clock set** command. The syntax for the **clock set** command is **clock set** *hh:mm:ss {month day | day month} year*. The following example shows how to set the date and time using a 24-hour clock:

```
CCNAS-ASA(config)# clock set 11:14:00 November 20 2017
```

Step 4: Configure the inside and outside interfaces.

ASA 5506 interface notes:

The 5506 is different than the 5505 ASA model. With the 5506 ASA, the physical ports can be assigned a Layer 3 IP address directly, much like a Cisco router. In this step, you will configure internal and external interfaces, name them, assign IP addresses, and set the interface security level.

If you completed the initial configuration Setup utility, the MGMT interface is configured with an IP address of 192.168.100.1. You will configure another interface as the inside interface for this lab. You will only configure the inside and outside interfaces at this time. The dmz interface will be configured in Part 5 of the lab.

a. Configure the Gi1/2 interface for the inside network (192.168.1.0/24) and set the security level to the highest setting of 100.

```
CCNAS-ASA(config)# interface gi1/2
CCNAS-ASA(config-if)# nameif inside
CCNAS-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)# security-level 100
CCNAS-ASA(config-if)# no shutdown
```

b. Configure the G1/1 interface for the outside network (209.165.200.224/29), set the security level to the lowest setting of 0, and access the Gi1/1 interface.

```
CCNAS-ASA(config-if)# interface G1/1
CCNAS-ASA(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
CCNAS-ASA(config-if)# ip address 209.165.200.226 255.255.255.248
CCNAS-ASA(config-if)# no shutdown
```

Interface security-level notes:

You may receive a message that the security level for the inside interface was set automatically to 100, and the outside interface was set to 0. The ASA uses interface security levels from 0 to 100 to enforce the security policy. Security level 100 (inside) is the most secure and level 0 (outside) is the least secure.

By default, the ASA applies a policy where traffic from a higher security level interface to one with a lower level is permitted and traffic from a lower security level interface to one with a higher security level is denied. The ASA default security policy permits outbound traffic, which is inspected, by default. Returning traffic is allowed due to stateful packet inspection. This default "routed mode" firewall behavior of the ASA allows packets to be routed from the inside network to the outside network, but not vice-versa. In Part 4 of this lab, you will configure NAT to increase the firewall protection.

c. Use the **show interface** command to ensure that ASA ports Gi1/1 and Gi1/2 are both up. An example is shown for Gi1/1. If either port is shown as down/down, check the physical connections. If either port is administratively down, bring it up with the **no shutdown** command.

```
CCNAS-ASA# show interface gig1/1
Interface GigabitEthernet1/1 "outside", is up, line protocol is up
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec<output omitted>
```

d. Display the status for all ASA interfaces using the **show interface ip brief** command.

Note: This command is different from the **show ip interface brief** IOS command. If any of the physical or logical interfaces previously configured are not up/up, troubleshoot as necessary before continuing.

Tip: Most ASA **show** commands, as well as **ping**, **copy**, and others, can be issued from within any configuration mode prompt without the **do** command that is required with IOS.

```
CCNAS-ASA# show interface ip brief
Interface                  IP-Address      OK? Method Status
Protocol
Virtual0                   127.1.0.1       YES unset up
up
GigabitEthernet1/1         209.165.200.226 YES manual up
up
GigabitEthernet1/2         192.168.1.1     YES manual up
up GigabitEthernet1/3         unassigned      YES unset  administratively
down down
GigabitEthernet1/4         unassigned      YES unset  administratively down
down
GigabitEthernet1/5         unassigned      YES unset  administratively down
down
GigabitEthernet1/6         unassigned      YES unset  administratively down
down
GigabitEthernet1/7         unassigned      YES unset  administratively down
down
```

```
GigabitEthernet1/8          unassigned      YES unset administratively down
down
Internal-Control1/1         127.0.1.1       YES unset up
up
Internal-Data1/1            unassigned      YES unset up
down
Internal-Data1/2            unassigned      YES unset up
up
Internal-Data1/3            unassigned      YES unset up
up
Management1/1               192.168.100.1   YES manual down                down
```

e. Display the information for the Layer 3 interfaces using the **show ip address** command.

```
CCNAS-ASA# show ip address
System IP Addresses:
Interface                Name                   IP address      Subnet mask
Method
GigabitEthernet1/1       outside                209.165.200.226
255.255.255.248 manual
GigabitEthernet1/2       inside                 192.168.1.1     255.255.255.0
manual
Management1/1            management             192.168.100.1   255.255.255.0
manual
Current IP Addresses:
Interface                Name                   IP address      Subnet mask
Method
GigabitEthernet1/1       outside                209.165.200.226
255.255.255.248 manual
GigabitEthernet1/2       inside                 192.168.1.1     255.255.255.0
manual
```

Management1/1 management 192.168.100.1 255.255.255.0 manual

f. You may also use the **show running-config interface type/number** command to display the configuration for a particular interface from the running configuration.

```
CCNAS-ASA# show running-config interface gig1/1
!
interface GigabitEthernet1/1
 nameif outside
 security-level 0
ip address 209.165.200.226 255.255.255.248
```

Step 5: Test connectivity to the ASA.

a. Ensure that PC-B has a static IP address of 192.168.1.3, a subnet mask of 255.255.255.0, and a default gateway of 192.168.1.1 (the IP address of the Gi1/2 inside interface).

b. You should be able to ping from PC-B to the ASA inside interface address and ping from the ASA to PC-B. If the pings fail, troubleshoot the configuration as necessary.

```
CCNAS-ASA# ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

c. From PC-C, ping the Gi1/1 (outside) interface at IP address 209.165.200.226. You should **Not** be able to ping this address.

Part 4: Configuring Routing, Address Translation, and Inspection Policy Using the CLI

In Part 4 of this lab, you will provide a default route for the ASA to reach external networks. You will configure address translation using network objects to enhance firewall security. You will then modify the default application inspection policy to allow specific traffic.

Note: You must complete Part 3 before proceeding to Part 4.

Step 1: Configure a static default route for the ASA.

In Part 3, you configured the ASA outside interface with a static IP address and subnet mask. However, the ASA does not have a gateway of last resort defined. To enable the ASA to reach external networks, you will configure a default static route on the ASA outside interface.

Note: If the ASA outside interface was configured as a DHCP client, it could obtain a default gateway IP address from the ISP. However, in this lab, the outside interface is configured with a static address.

a. Ping from the ASA to R1 G0/0 at IP address 209.165.200.225. Was the ping successful?

_____

_____

b. Ping from the ASA to R1 S0/0/0 at IP address 10.1.1.1. Was the ping successful?

_____

_____

c. Create a “quad zero” default route using the **route** command, associate it with the ASA outside interface, and point to the R1 G0/0 at IP address 209.165.200.225 as the gateway of last resort. The default administrative distance is one by default.

```
CCNAS-ASA(config)# route outside 0.0.0.0 0.0.0.0 209.165.200.225
```

d. Issue the **show route** command to display the ASA routing table and the static default route you just created.

```
CCNAS-ASA# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, + - replicated route
```

```
Gateway of last resort is 209.165.200.225 to network 0.0.0.0

S*    0.0.0.0 0.0.0.0 [1/0] via 209.165.200.225, outside
C        192.168.1.0 255.255.255.0 is directly connected, inside
L        192.168.1.1 255.255.255.255 is directly connected, inside
C        209.165.200.224 255.255.255.248 is directly connected, outside
L        209.165.200.226 255.255.255.255 is directly connected, outside
```

e. Ping from the ASA to R1 S0/0/0 IP address 10.1.1.1.

Step 2: Configure address translation using PAT and network objects.

Note: Beginning with ASA version 8.3, network objects are used to configure all forms of NAT. A network object is created, and it is within this object that NAT is configured. In Step 2a, the network object **INSIDE-NET** is used to translate the inside network addresses (192.168.10.0/24) to the global address of the outside ASA interface. This type of object configuration is called Auto-NAT.

a. Create the network object **INSIDE-NET** and assign attributes to it using the **subnet** and **nat** commands.

```
CCNAS-ASA(config)# object network INSIDE-NET
CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.0
CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic interface
CCNAS-ASA(config-network-object)# end
```

b. The ASA splits the configuration into the object portion that defines the network to be translated and the actual **nat** command parameters. These appear in two different places in the running configuration. Display the NAT object configuration using the **show run object** and **show run nat** commands.

```
CCNAS-ASA# show run object
object network INSIDE-NET
 subnet 192.168.1.0 255.255.255.0

CCNAS-ASA# show run nat
!
object network INSIDE-NET
 nat (inside,outside) dynamic interface
```

c. From PC-B, attempt to ping the R1 G0/0 interface at IP address **209.165.200.225**. Notice the pings are not successful at this time as the default inspection policy does not allow ICMP to pass through the firewall.

d. Issue the **show nat** command on the ASA to see the translated and untranslated hits. Notice that, of the pings from PC-B, three were translated and three were not because ICMP is not being inspected by the global inspection policy. The outgoing pings (echoes) were translated, and the returning echo replies were blocked by the firewall policy. You will configure the default inspection policy to allow ICMP in the next step. **Note:** Depending on the processes and daemons running on the particular computer used as PC-B, you may see more translated and untranslated hits than the three echo requests and echo replies.

```
CCNAS-ASA# show nat

Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic INSIDE-NET interface
```

```
    translate_hits = 3, untranslate_hits = 3
```

e. Ping from PC-B to R1 again and quickly issue the **show xlate** command to see the addresses being translated.

```
CCNAS-ASA# show xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net

ICMP PAT from inside:192.168.1.3/1 to outside:209.165.200.226/1 flags ri idle 0:00:01
timeout 0:00:30
```

Note: The flags (r and i) indicate that the translation was based on a port map (r) and was done dynamically (i).

f. Open a browser on PC-B and enter the IP address of R1 G0/0 (209.165.200.225). In a pop-up window, you should be prompted by R1 that authentication is required. TCP-based HTTP traffic is permitted, by default, by the firewall inspection policy.

g. On the ASA, reissue the **show nat** and **show xlate** commands to see the hits and addresses being translated for the HTTP connection.

Step 3: Modify the default MPF application inspection global service policy.

For application layer inspection, as well as other advanced options, the Cisco MPF is available on ASAs. Cisco MPF uses three configuration objects to define modular, object-oriented, and hierarchical policies:

- **Class maps** - Define a match criterion.
- **Policy maps** - Associate actions to the match criteria.
- **Service policies** - Attach the policy map to an interface, or globally to all interfaces of the appliance.

a. Display the default MPF policy map that performs the inspection on inside-to-outside traffic. Only traffic that was initiated from the inside is allowed back in to the outside interface. Notice that the ICMP protocol is missing.

```
CCNA-ASA# show run | begin class
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
```

```
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
  inspect dns preset_dns_map
policy-map type inspect dns migrated_dns_map_2
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
!
service-policy global_policy global
<output omitted>
```

b. Add the inspection of ICMP traffic to the policy map list using the following commands:

```
CCNAS-ASA(config)# policy-map global_policy
CCNAS-ASA(config-pmap)# class inspection_default
CCNAS-ASA(config-pmap-c)# inspect icmp
```

c. Display the default MPF polich map to verify ICMP is now listed in the inspection rules.

```
CCNA-ASA(config-pmap-c)# show run policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
class inspection_default
inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect  rsh
  inspect rtsp
```

```
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc
 inspect tftp
 inspect sip
 inspect xdmcp
 inspect dns preset_dns_map
 inspect icmp
!
```

d. From PC-B, attempt to ping the R1 G0/0 interface at IP address 209.165.200.225. The pings should be successful this time because ICMP traffic is now being inspected and legitimate return traffic is being allowed.

Part 5: Configuring DHCP, AAA, and SSH

In Part 5, you will configure ASA features, such as DHCP and enhanced login security, using AAA and SSH.

Note: You must complete Part 4 before beginning Part 5.

Step 1: Configure the ASA as a DHCP server.

The ASA can be both a DHCP server and a DHCP client. In this step, you will configure the ASA as a DHCP server to dynamically assign IP addresses for DHCP clients on the inside network.

a. Configure a DHCP address pool and enable it on the ASA inside interface. This is the range of addresses to be assigned to inside DHCP clients. Attempt to set the range from 192.168.1.5 through 192.168.1.100.

```
CCNAS-ASA(config)# dhcpd address 192.168.1.5-192.168.1.100 inside
```

Were you able to do this on this ASA?

_____

_____

b. (Optional) Specify the IP address of the DNS server to be given to clients.

```
CCNAS-ASA(config)# dhcpd dns 209.165.201.2
```

Note: Other parameters can be specified for clients, such as WINS server, lease length, and domain name. By default, the ASA sets its own IP address as the DHCP default gateway, so there is no need to configure it. However, to manually configure the default gateway, or set it to a different networking device's IP address, use the following command:

```
CCNAS-ASA(config)# dhcpd option 3 ip 192.168.1.1
```

c. Enable the DHCP daemon within the ASA to listen for DHCP client requests on the enabled interface (inside).

```
CCNAS-ASA(config)# dhcpd enable inside
```

d. Verify the DHCP daemon configuration by using the **show run dhcpd** command.

```
CCNAS-ASA(config)# show run dhcpd
dhcpd dns 209.165.201.2
dhcpd option 3 ip 192.168.1.1
!
```

```
dhcpd address 192.168.1.5-192.168.1.100 inside
dhcpd enable inside
!
```

e. Access the Network Connection IP Properties for PC-B, and change it from a static IP address to a DHCP client so that it obtains an IP address automatically from the ASA DHCP server. The procedure to do this varies depending on the PC operating system. It may be necessary to issue the **ipconfig /renew** command on PC-B to force it to obtain a new IP address from the ASA.

Step 2: Configure AAA to use the local database for authentication.

a. Define a local user named admin by entering the **username** command. Specify a password of **admin01pass**.

```
CCNAS-ASA(config)# username admin password admin01pass
```

b. Configure AAA to use the local ASA database for SSH user authentication.

```
CCNAS-ASA(config)# aaa authentication ssh console LOCAL
```

Note: For added security, starting with ASA version 8.4(2), configure AAA authentication to support SSH connections. The Telnet/SSH default login is not supported. You can no longer connect to the ASA using SSH with the default username and the login password.

Step 3: Configure SSH remote access to the ASA.

You can configure the ASA to accept SSH connections from a single host or a range of hosts on the inside or outside network.

a. Generate an **RSA** key pair, which is required to support SSH connections. The modulus (in bits) can be 512, 768, 1024, or 2048. The larger the key modulus size you specify, the longer it takes to generate an RSA. Specify a modulus of **1024** using the **crypto key** command.

```
CCNAS-ASA(config)# crypto key generate rsa modulus 1024
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
```

Note: You may receive a message that a RSA key pair is already defined. To replace the RSA key pair enter **yes** at the prompt.

b. Save the RSA keys to persistent flash memory using either the **copy run start** or **write mem** command.

```
CCNA-ASA# write mem
Building configuration...
Cryptochecksum: 43b3e351 6b3fd965 fc8c4869 b46424c8


4844 bytes copied in 0.280 secs
[OK]
```

c. Configure the ASA to allow SSH connections from any host on the inside network (192.168.1.0/24) and from the remote management host at the branch office (172.16.3.3) on the outside network. Set the SSH timeout to **10** minutes (the default is 5 minutes).

```
CCNAS-ASA(config)# ssh 192.168.1.0 255.255.255.0 inside
CCNAS-ASA(config)# ssh 172.16.3.3 255.255.255.255 outside
CCNAS-ASA(config)# ssh timeout 10
```

d. On PC-C, use an SSH client (such as PuTTY) to connect to the ASA outside interface at the IP address **209.165.200.226**. The first time you connect you may be prompted by the SSH client to accept the RSA

host key of the ASA SSH server. Log in as user **admin** and provide the password **admin01pass**. You can also connect to the ASA inside interface from a PC-B SSH client using the IP address **192.168.1.1**.

Part 6: Configuring DMZ, Static NAT, and ACLs

Previously, you configured address translation using PAT for the inside network. In this part of the lab, you will create a DMZ on the ASA, configure static NAT to a DMZ server, and apply ACLs to control access to the server.

To accommodate the addition of a DMZ and a web server, you will use another address from the ISP range assigned 209.165.200.224/29 (.224-.231). Router R1 G0/0 and the ASA outside interface are already using 209.165.200.225 and .226. You will use the public address 209.165.200.227 and static NAT to provide address translation access to the server.

Step 1: Configure the DMZ interface Gi1/3 on the ASA.

a. Configure DMZ interface Gi1/3, which is where the public access web server will reside. Assign Gi1/3 the IP address **192.168.2.1/24**, name it **dmz**, and assign a security level of **70**.

```
CCNAS-ASA(config)# int gi1/3
CCNAS-ASA(config-if)# ip address 192.168.2.1 255.255.255.0
CCNAS-ASA(config-if)# nameif dmz
INFO: Security level for "dmz" set to 0 by default.INFO: Security level for
"dmz" set to 0 by default.

CCNAS-ASA(config-if)# security-level 70
CCNAS-ASA(config-if)# no shut
```

b. Display the status for all ASA interfaces using the **show interface ip brief** command.

```
CCNAS-ASA# show int ip brief
Interface                  IP-Address      OK? Method Status
Protocol
Virtual0                   127.1.0.1       YES unset  up
up
GigabitEthernet1/1         209.165.200.226 YES manual up
up
GigabitEthernet1/2         192.168.1.1     YES manual up
up
GigabitEthernet1/3         192.168.2.1     YES manual up
up
GigabitEthernet1/4         unassigned      YES unset administratively down
down
GigabitEthernet1/5         unassigned      YES unset administratively down
down
GigabitEthernet1/6         unassigned      YES unset administratively down
down
GigabitEthernet1/7         unassigned      YES unset administratively down
down
GigabitEthernet1/8         unassigned      YES unset administratively down
down
Management1/1              192.168.100.1   YES manual down                down
<output omitted>
```

c. Display the information for the interfaces using the **show ip address** command.

```
CCNAS-ASA# show ip address
System IP Addresses:
Interface                  Name                   IP address      Subnet mask
Method
GigabitEthernet1/1         outside                209.165.200.226
255.255.255.248 manual
GigabitEthernet1/2         inside                 192.168.1.1     255.255.255.0
manual
GigabitEthernet1/3         dmz                    192.168.2.1     255.255.255.0
manual
Management1/1              management             192.168.100.1   255.255.255.0
manual
Current IP Addresses:
Interface                  Name                   IP address      Subnet mask
Method
GigabitEthernet1/1         outside                209.165.200.226
255.255.255.248 manual
GigabitEthernet1/2         inside                 192.168.1.1     255.255.255.0
manual
GigabitEthernet1/3         dmz                    192.168.2.1     255.255.255.0
manual
Management1/1              management             192.168.100.1   255.255.255.0
manual
<output omitted>
```

Step 2: Configure static NAT to the DMZ server using a network object.

Configure a network object named **dmz-server** and assign it the static IP address of the DMZ server (**192.168.2.3**). While in object definition mode, use the **nat** command to specify that this object is used to translate a DMZ address to an outside address using static NAT, and specify a public translated address of **209.165.200.227**.

```
CCNAS-ASA(config)# object network dmz-server
CCNAS-ASA(config-network-object)# host 192.168.2.3
CCNAS-ASA(config-network-object)# nat (dmz,outside) static 209.165.200.227
```

Step 3: Configure an ACL to allow access to the DMZ server from the Internet.

Configure a named access list (**OUTSIDE-DMZ**) that permits any IP protocol from any external host to the internal IP address of the DMZ server. Apply the access list to the ASA outside interface in the **IN** direction.

```
CCNAS-ASA(config)# access-list OUTSIDE-DMZ permit ip any host 192.168.2.3
CCNAS-ASA(config)# access-group OUTSIDE-DMZ in interface outside
```

Note: Unlike IOS ACLs, the ASA ACL **permit** statement must permit access to the internal private DMZ address. External hosts access the server using its public static NAT address, the ASA translates it to the internal host IP address, and then applies the ACL.

You can modify this ACL to allow only services that you want to be exposed to external hosts, such as web (HTTP) or file transfer (FTP).

Step 4: Test access to the DMZ server.

a. Create a loopback 0 interface on Internet R2 representing an external host. Assign **Lo0** IP address **172.30.1.1** and a mask of **255.255.255.0**. Ping the DMZ server public address from R2 using the loopback interface as the source of the ping. The pings should be successful.

```
R2(config-if)# interface lo0
R2(config-if)# ip address 172.30.1.1 255.255.255.0
R2(config-if)# end
R2# ping 209.165.200.227 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.227, timeout is 2 seconds:
Packet sent with a source address of 172.30.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

b. Clear the NAT counters using the **clear nat counters** command.

```
CCNAS-ASA# clear nat counters
```

c. Ping from PC-C to the DMZ server at the public address **209.165.200.227**. The pings should be successful.

d. Issue the **show nat** and **show xlate** commands on the ASA to see the effect of the pings. Both the PAT (inside to outside) and static NAT (dmz to outside) policies are shown.

```
CCNA-ASA# show nat

Auto NAT Policies (Section 2)
1 (dmz) to (outside) source static dmz-server 209.165.200.227
    translate_hits = 0, untranslate_hits = 4
2 (inside) to (outside) source dynamic INSIDE-NET interface
    translate_hits = 0, untranslate_hits = 0
```

Note: Pings from inside to outside are translated hits. Pings from outside host PC-C to the DMZ are considered untranslated hits.

```
CCNA-ASA# show xlate
1 in use, 6 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from dmz:192.168.2.3 to outside:209.165.200.227
    flags s idle 0:00:02 timeout 0:00:00
```

Note: This time the flag is "**s**", which indicates a static translation.

e. You can also access the DMZ server from a host on the inside network because the ASA inside interface is set to a security level of 100 (the highest) and the DMZ interface is set to 70. The ASA acts like a router between the two networks.

Ping the DMZ server (PC-A) internal address (**192.168.2.3**) from inside network host PC-B (192.168.1.X). The pings should be successful because of the interface security level and the fact that ICMP is being inspected on the inside interface by the global inspection policy. The pings from PC-B to PC-A will not

affect the NAT translation counts because both PC-B and PC-A are behind the firewall, and no translation takes place.

f. The DMZ server cannot ping PC-B on the inside network because the DMZ interface has a lower security level.
Try to ping from the DMZ server PC-A to PC-B at IP address **192.168.1.3**. The pings should **Not** be successful.

g. Use the **show run** command to display the configuration for Gi1/3.

```
CCNAS-ASA# show run interface gi1/3
!
interface GigabitEthernet1/3
 nameif dmz
 security-level 70
 ip address 192.168.2.1 255.255.255.0
```

Note: An access list can be applied to the inside interface to control the type of access to be permitted or denied to the DMZ server from inside hosts.

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)