Practical 4

Configure IP ACLs to Mitigate Attacks

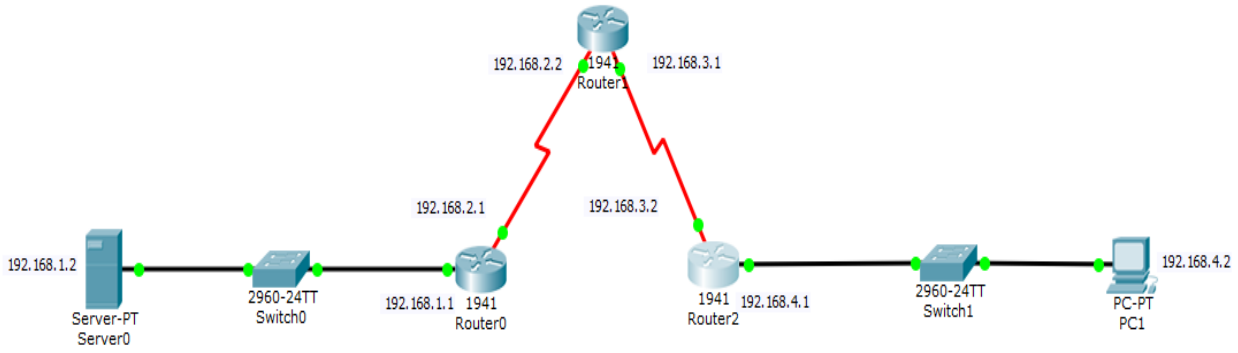
Access Control Lists (ACLs)
Network administrators must figure out how to deny unwanted access to the network while allowing internal users appropriate access to necessary services. Although security tools, such as passwords, callback equipment, and physical security devices are helpful, they often lack 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

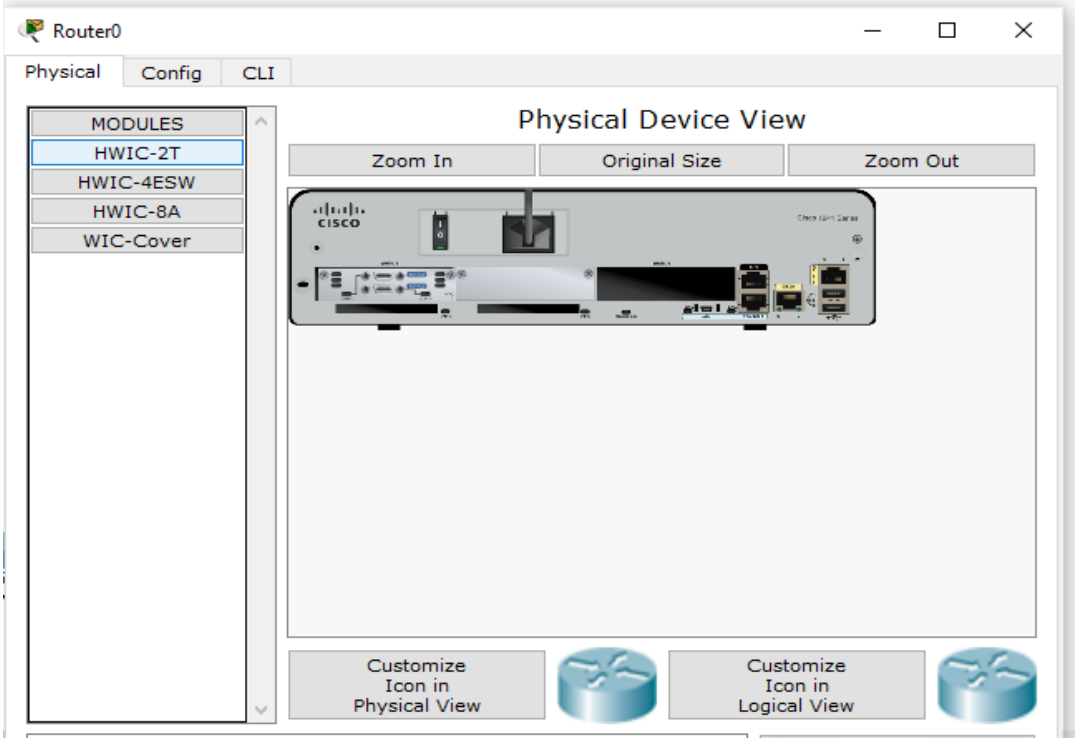
An access list is a sequential series of commands or filters. These lists tell the router what types of packets to: accept or deny Acceptance and denial can be based on specified conditions. ACLs applied on the router's interfaces.

Consider the following topology

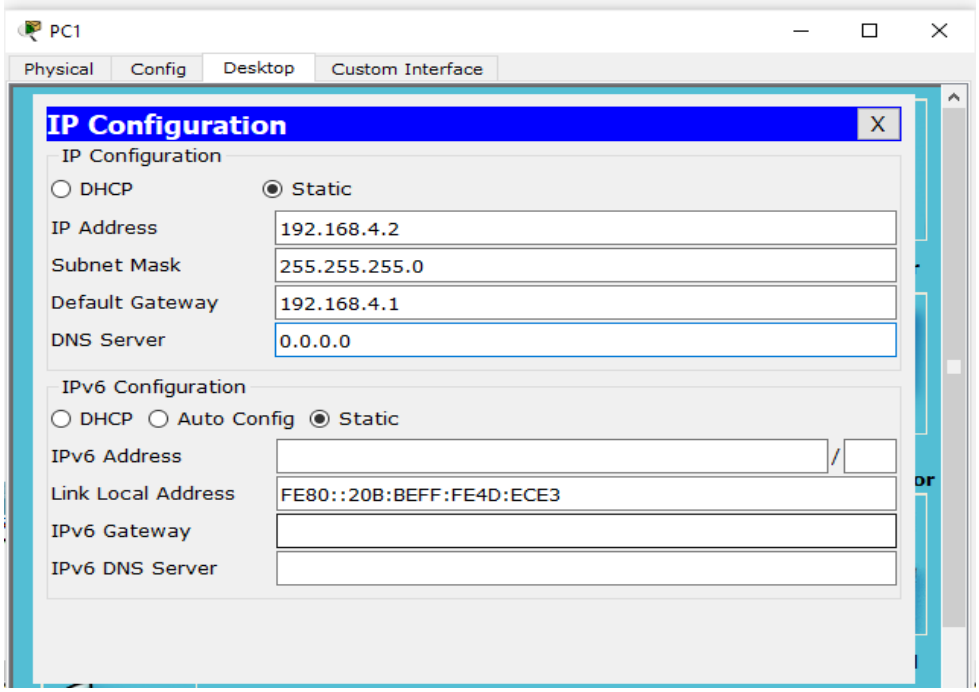


Topology Configuration

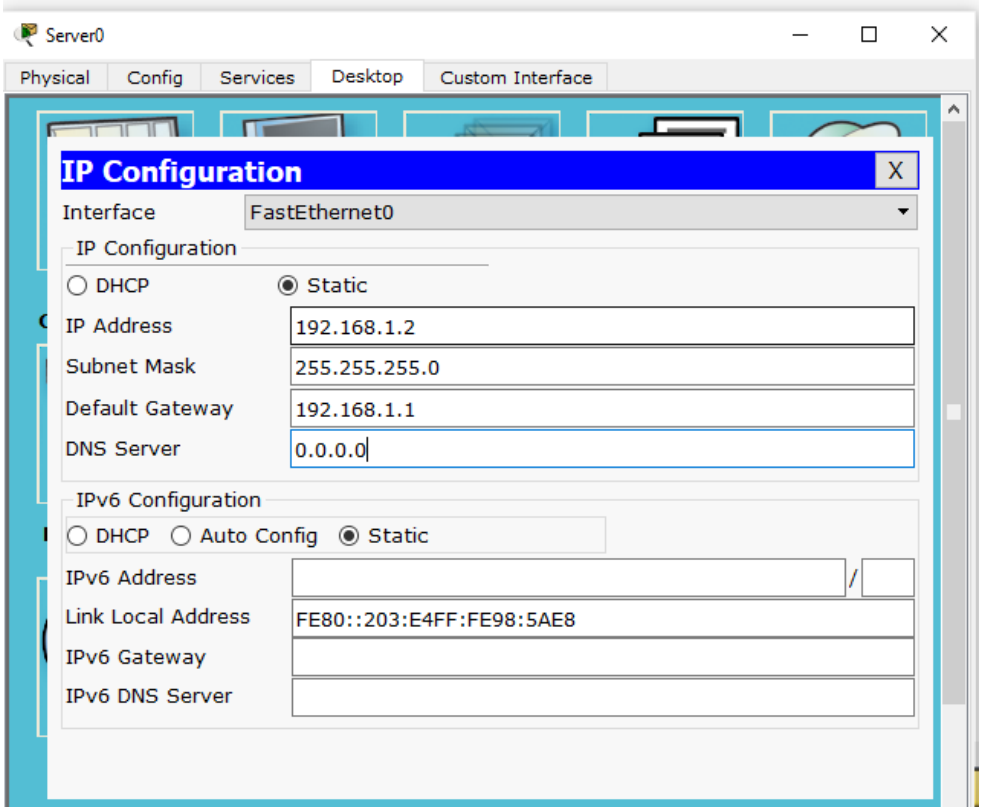
The serial interface in each Router is added as follows



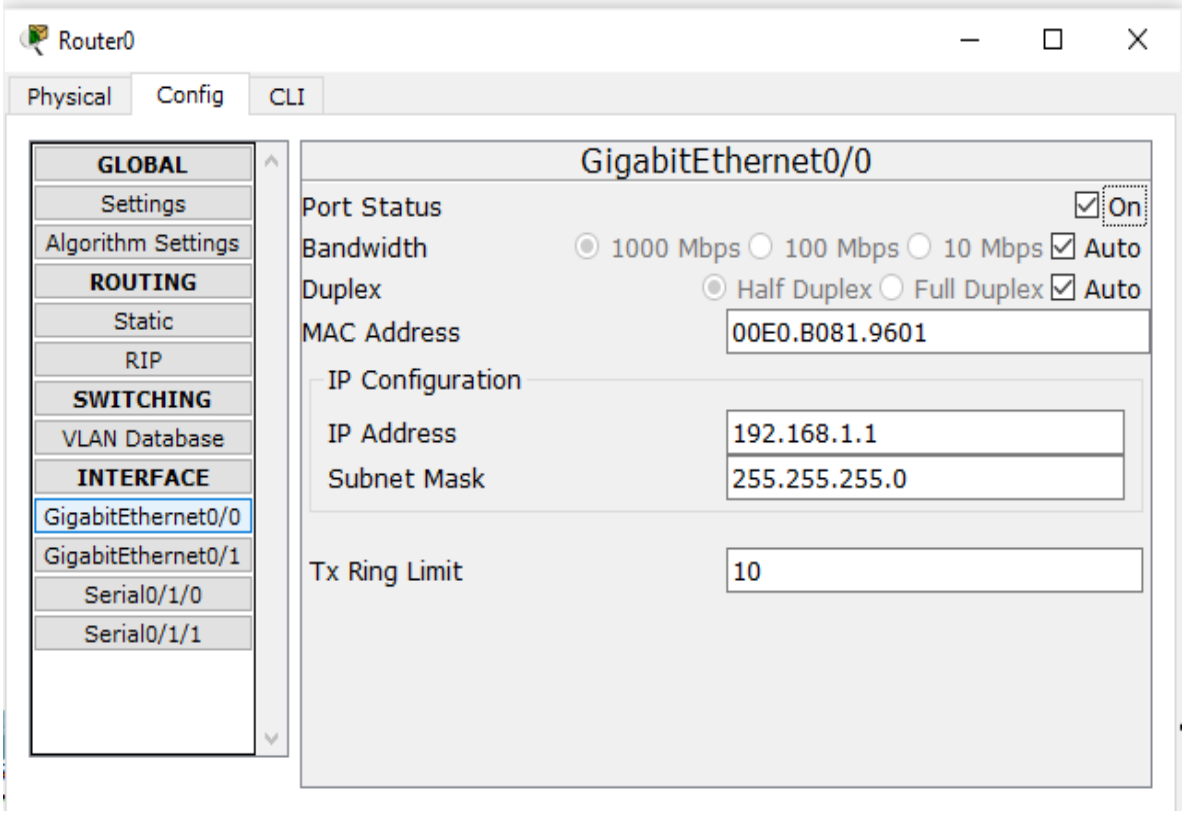
Configuring PC1

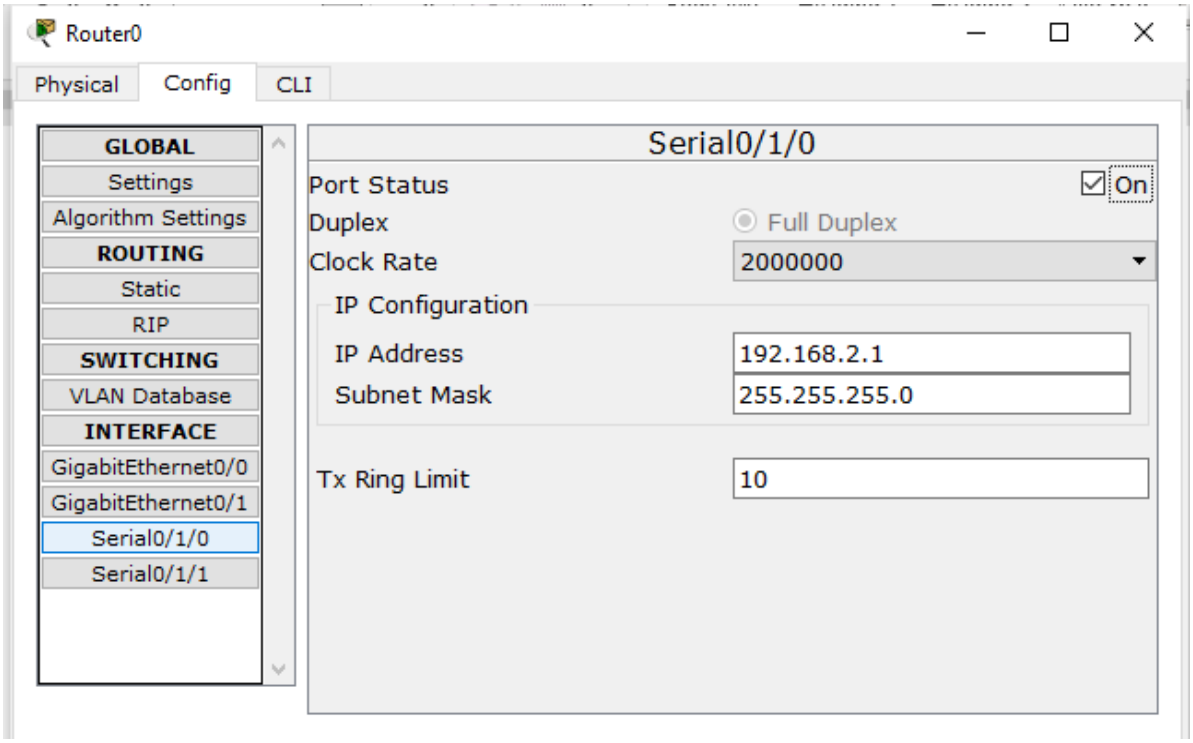


Configuring Server0

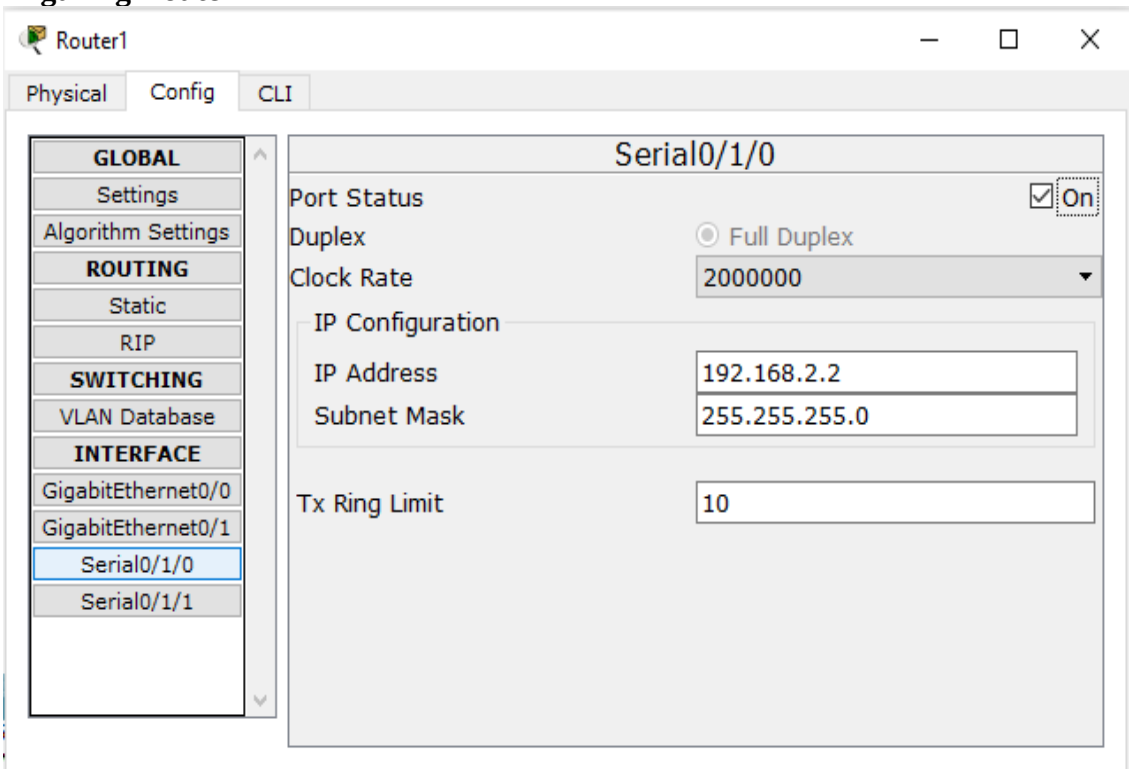


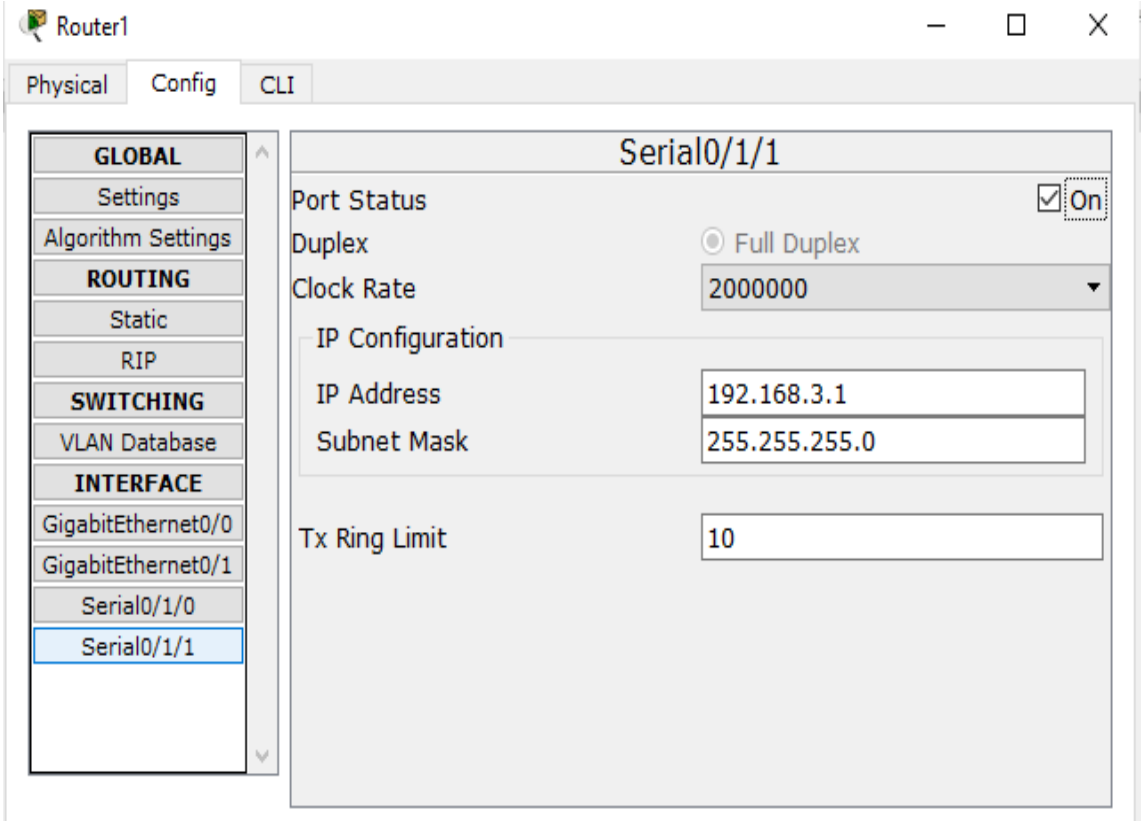
Configuring Router0



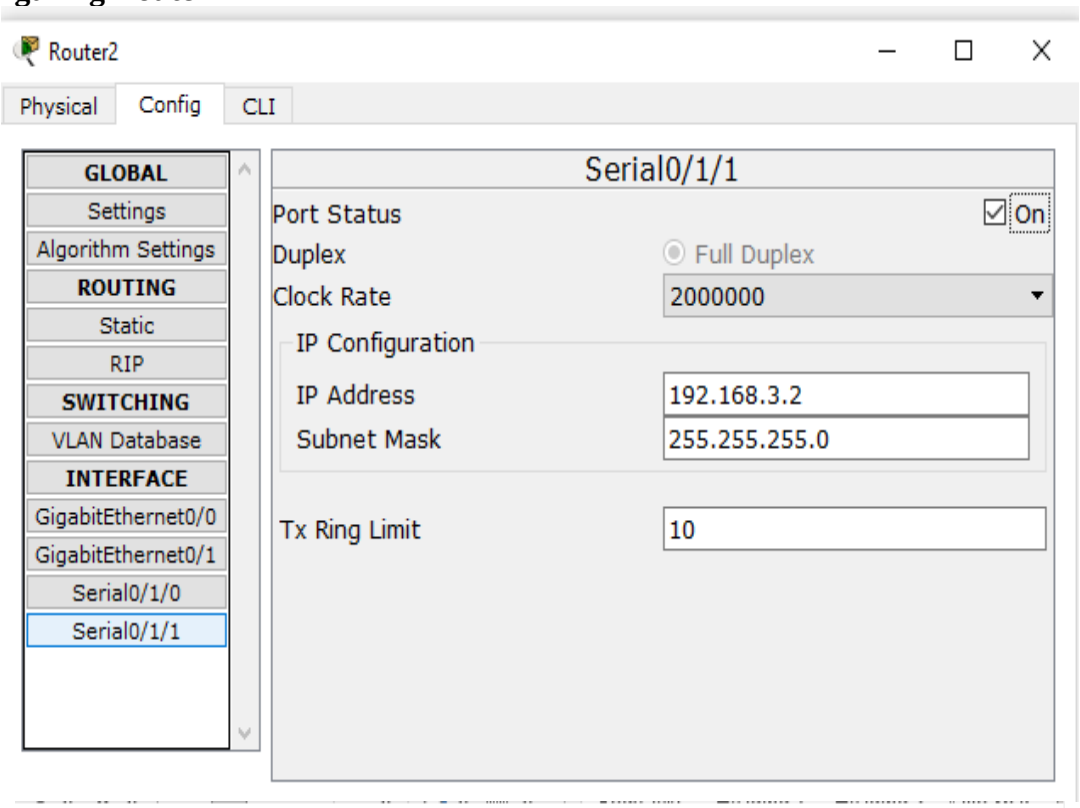


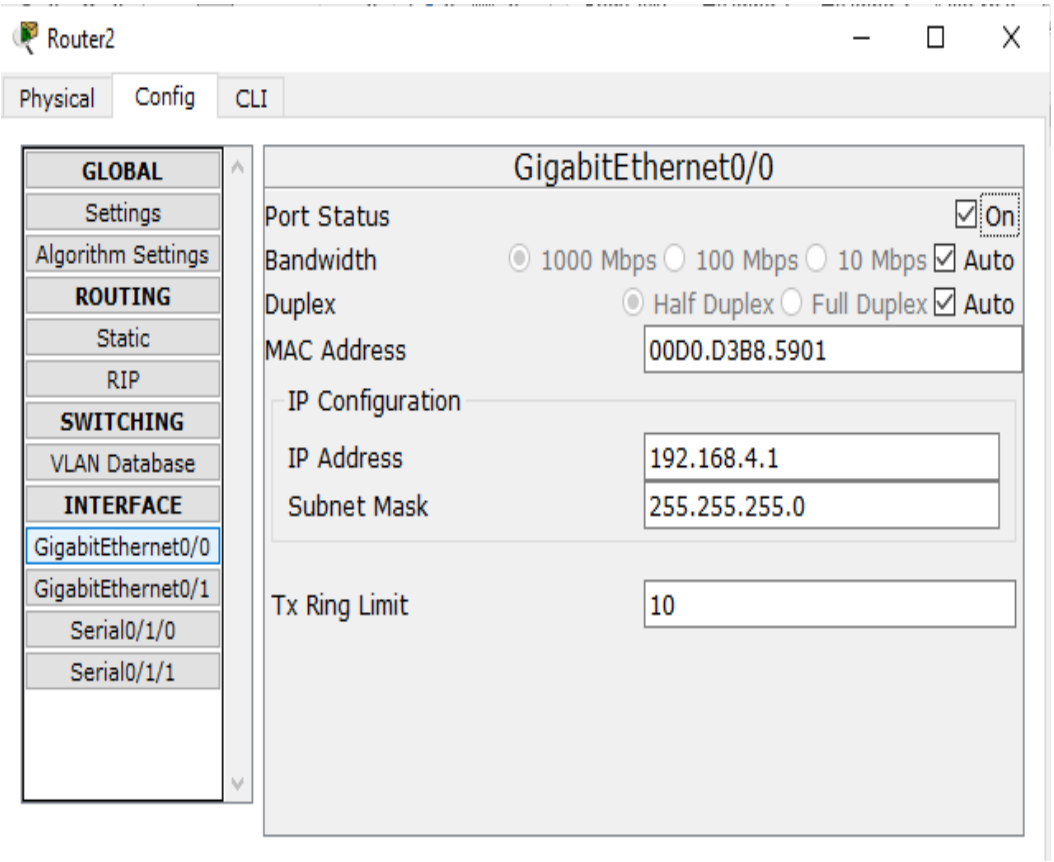
Configuring Router1



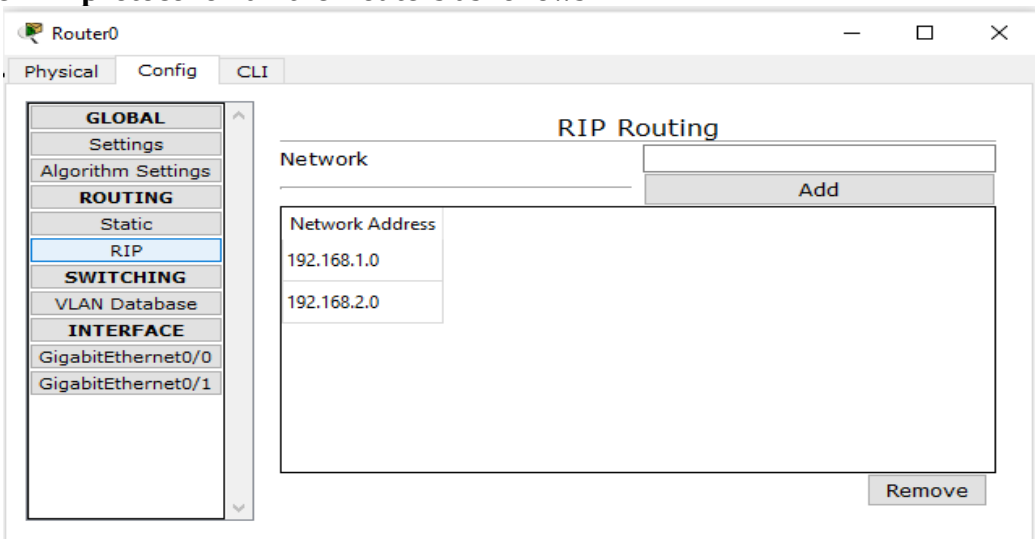


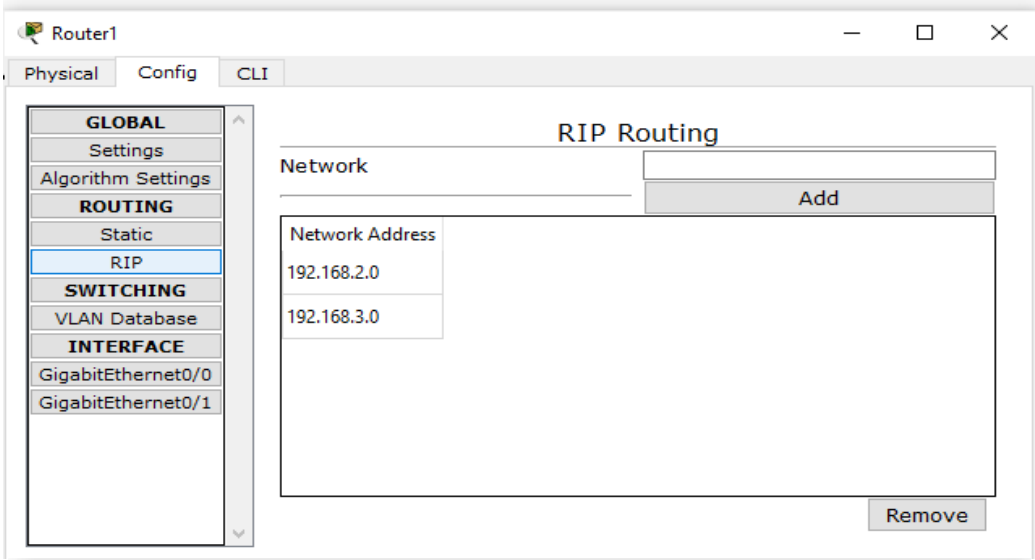
Configuring Router2

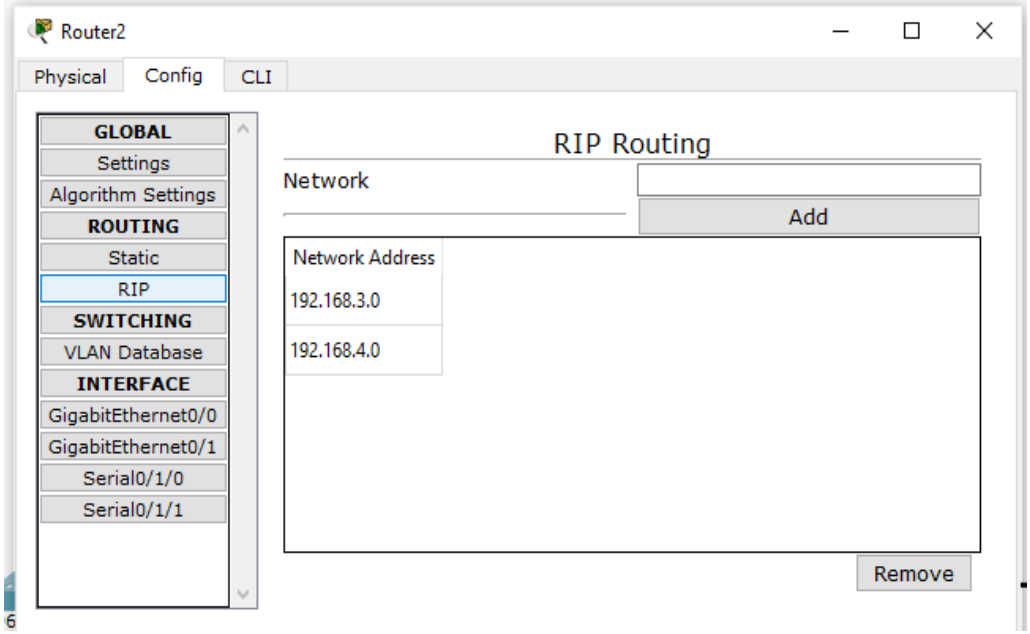




Set the RIP protocol on all the Routers as follows

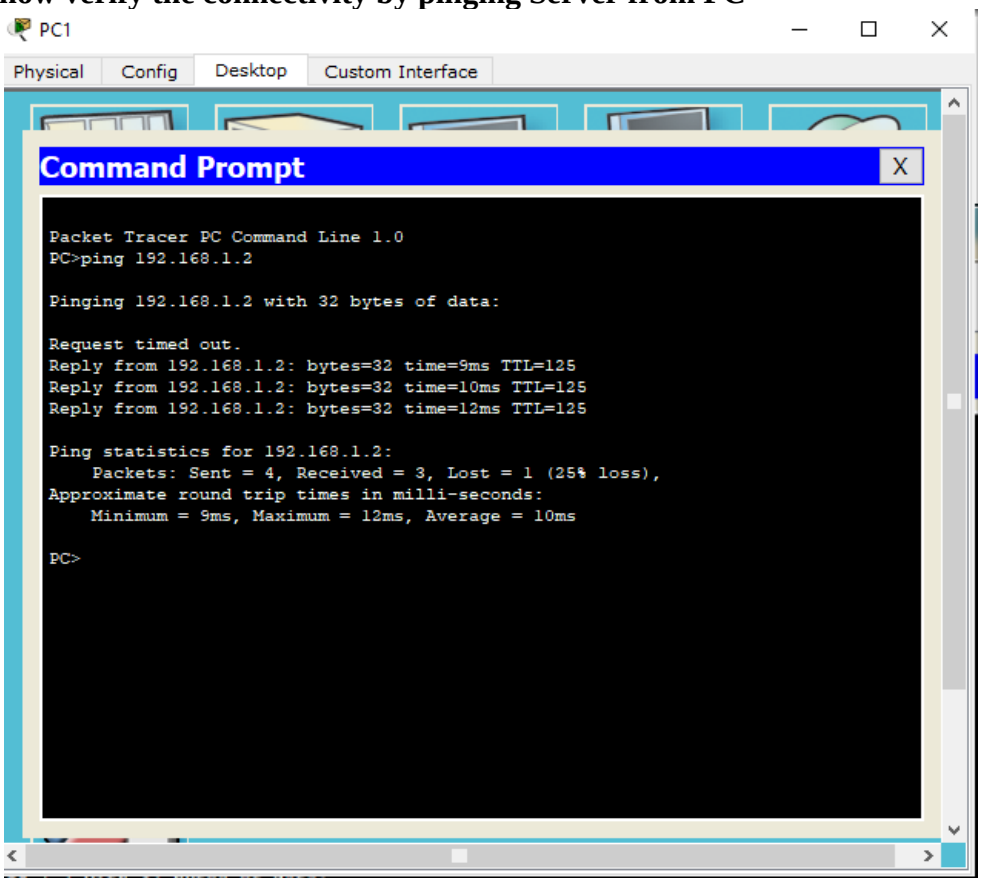




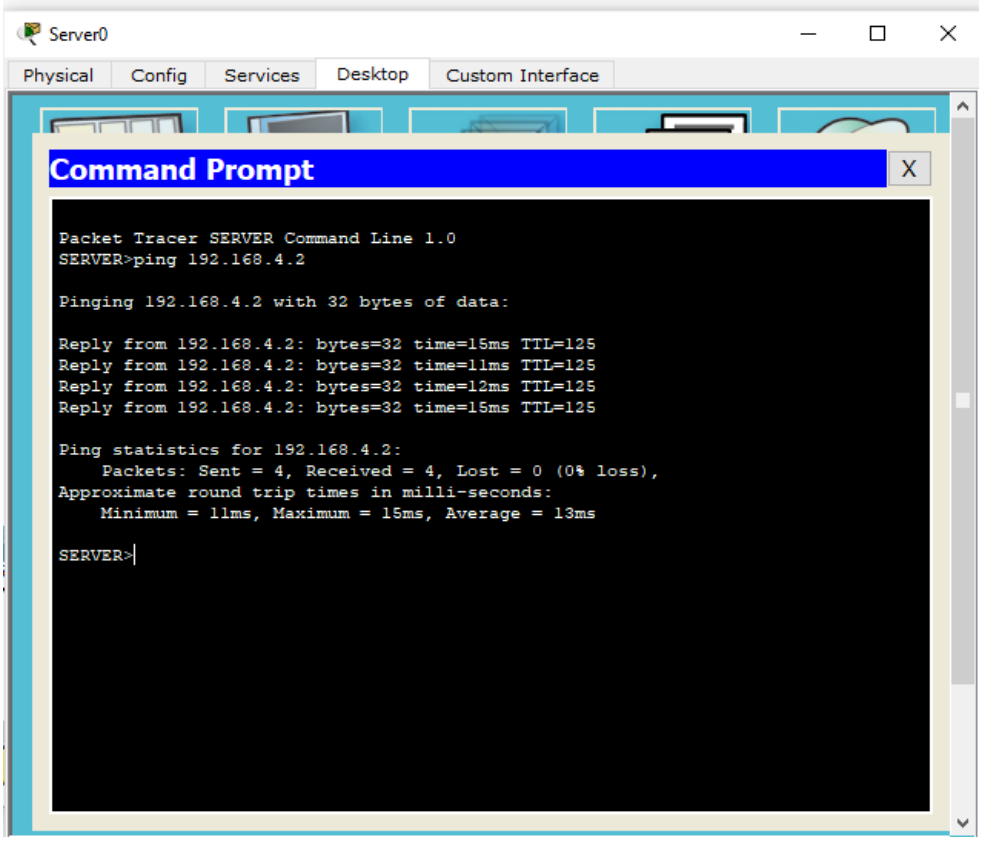


Part 1: Verify Basic Connectivity

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.

Part a) Set up the SSH protocol

Enter the following commands in CLI mode of all Routers.

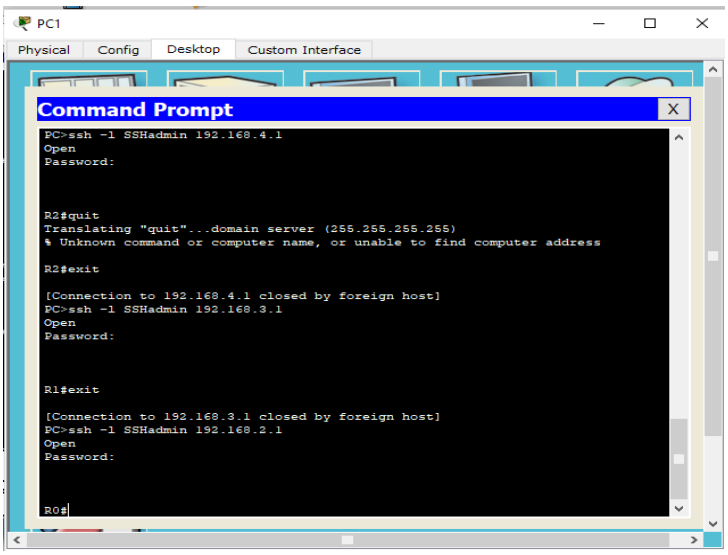
```
Router>en
Router#conf t
Router(config)# ip domain-name dalmia.com
Router(config)# hostname R0
R0(config)# crypto key generate rsa
R0(config)# line vty 0 4
R0(config-line)# transport input ssh
R0(config-line)# login local
R0(config-line)# exit
R0(config)# username SSHadmin privilege 15 password dalmia
R0(config)#exit
```

Part b) Create an ACL 10 to permit remote access to PC only

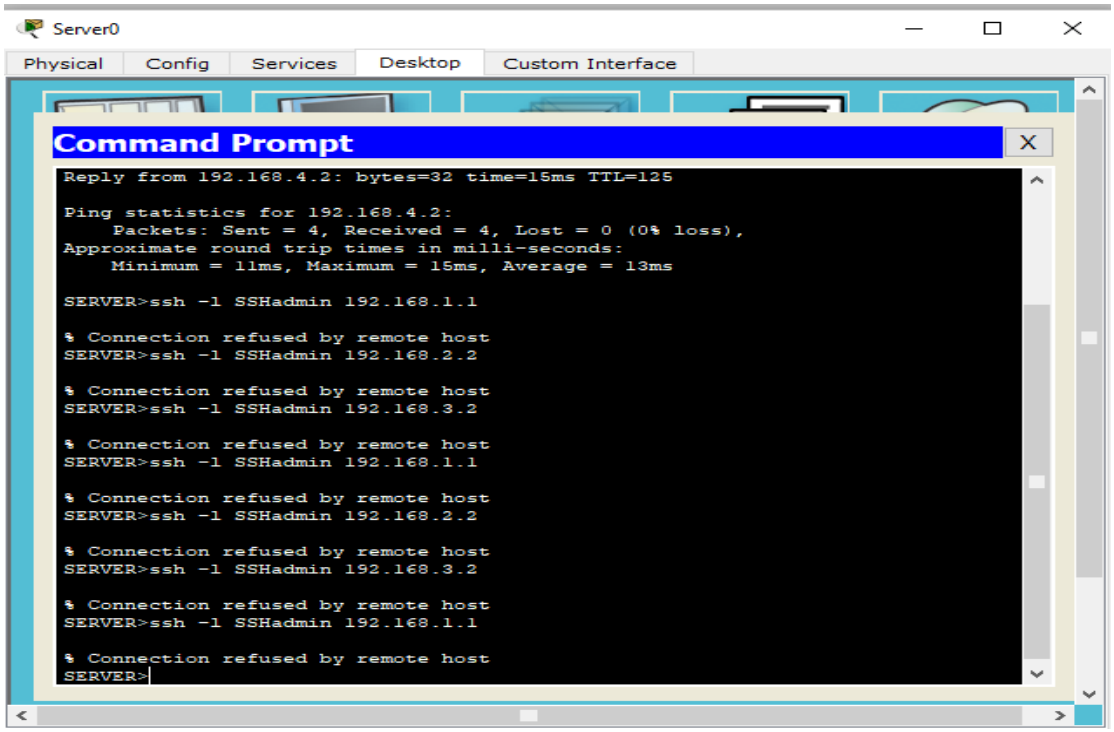
Enter the following commands in CLI mode of all Routers

```
Router>en
Router#conf t
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



Part 3: Create a Numbered IP ACL 120 on R1

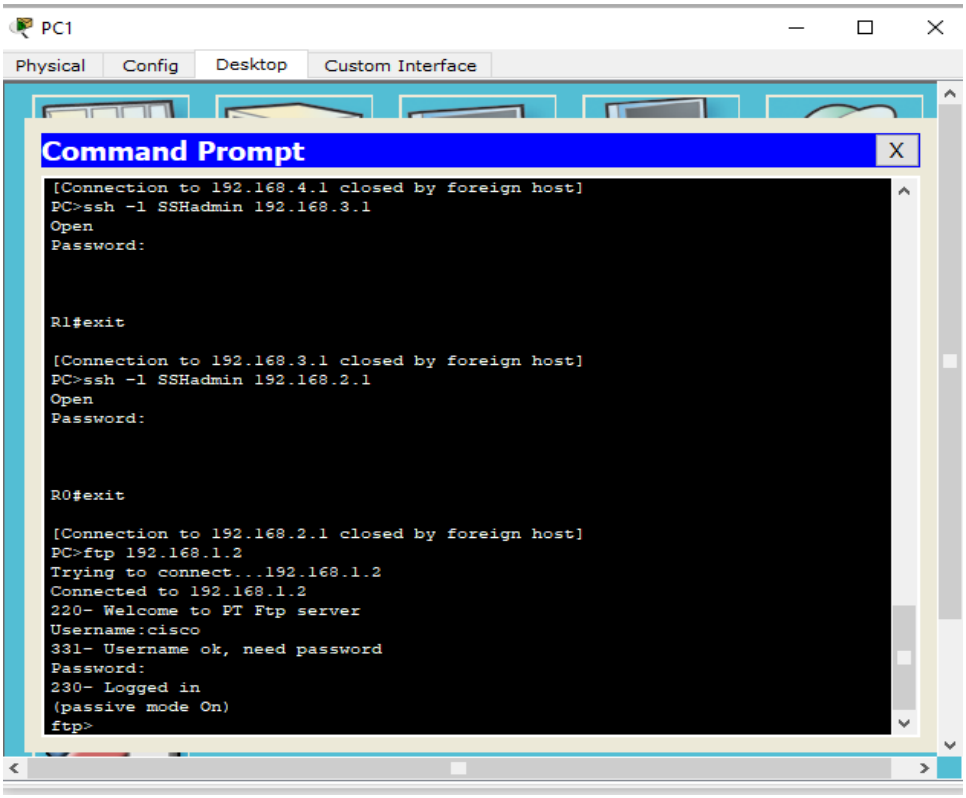
We need to perform the following in this part

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 **PC1 to** access **R1** via SSH. (done in previous part)

Enter the following commands in the CLI mode of Router1

```
R1>enable
R1#
R1#configure terminal
R1(config)#access-list 120 permit udp any host 192.168.1.2 eq domain
R1(config)#access-list 120 permit tcp any host 192.168.1.2 eq smtp
R1(config)#access-list 120 permit tcp any host 192.168.1.2 eq ftp
R1(config)#access-list 120 deny tcp any host 192.168.1.2 eq 443
R1(config)#exit
R1#configure terminal
R1(config)#interface Serial0/1/1
R1(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.

****