

# **PRACTICAL NO 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

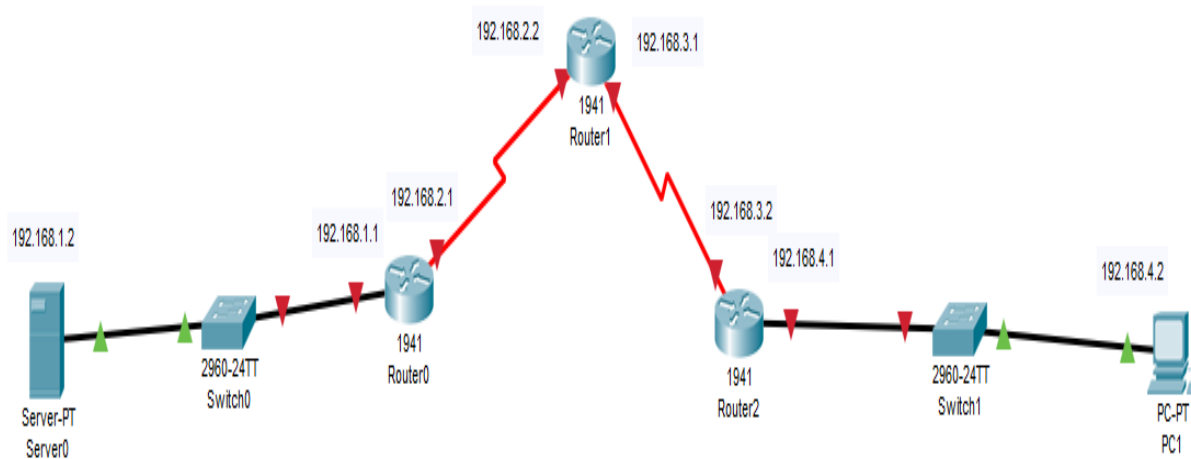
- Can only filter on source IP addresses

Extended IP ACLs Can filter on:

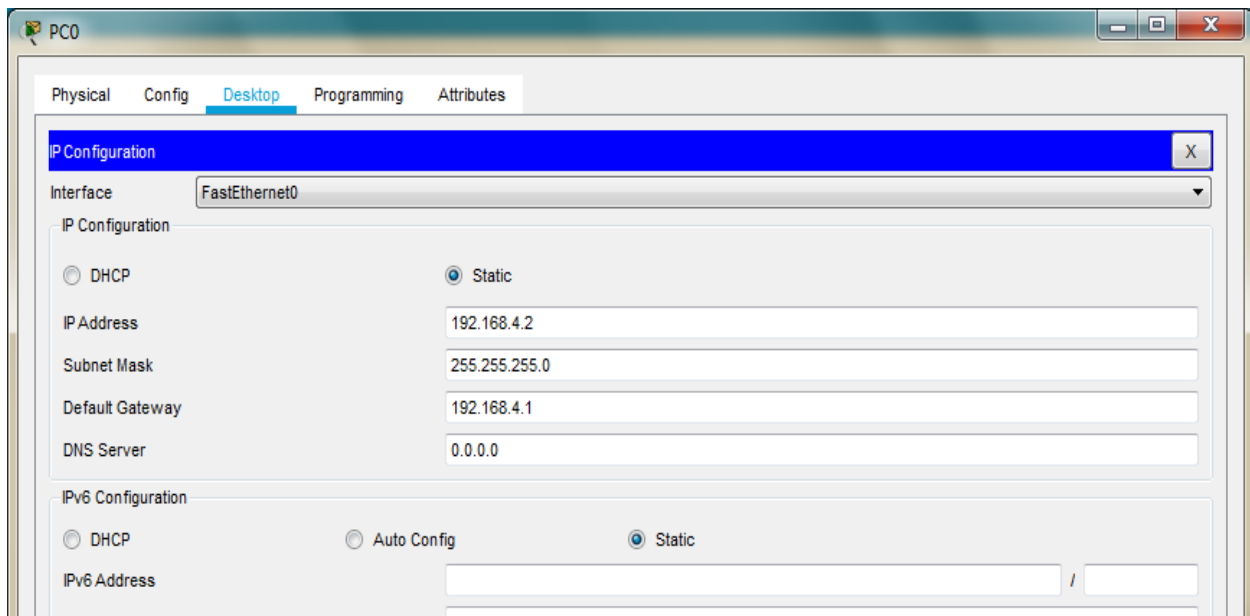
- 1) Source IP address
- 2) Destination IP address
- 3) Protocol (TCP, UDP)
- 4) Port Numbers (Telnet – 23, http – 80, etc.) and other parameters

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

**We use the following topology to study the present case**



## Configuring PC1

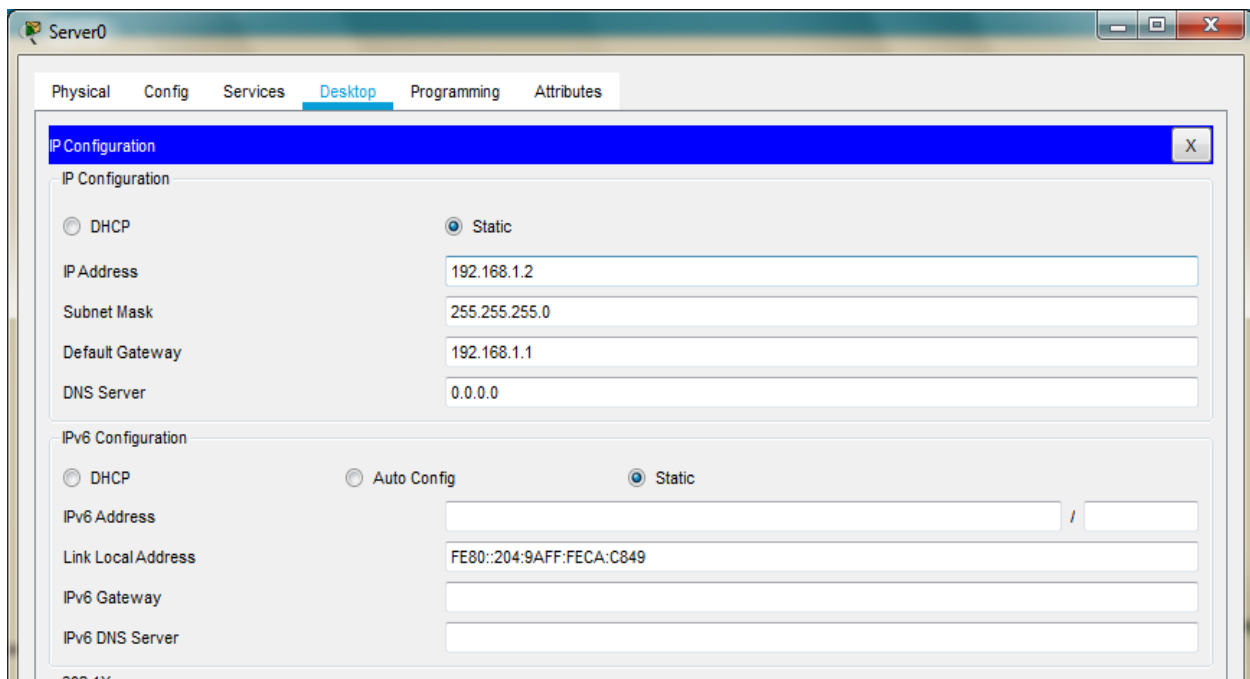


The screenshot shows the configuration window for PC0. The 'Desktop' tab is selected. The 'IP Configuration' section is expanded, showing the 'FastEthernet0' interface. The 'Static' radio button is selected under 'IP Configuration'. The fields are filled with the following values:

Field	Value
Interface	FastEthernet0
IP Configuration	Static
IP Address	192.168.4.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.4.1
DNS Server	0.0.0.0

The 'IPv6 Configuration' section is also visible, with 'Static' selected and the 'IPv6 Address' field empty.

## Configuring Server0



The screenshot shows the configuration window for Server0. The 'Desktop' tab is selected. The 'IP Configuration' section is expanded. The 'Static' radio button is selected under 'IP Configuration'. The fields are filled with the following values:

Field	Value
IP Configuration	Static
IP Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

The 'IPv6 Configuration' section is also visible, with 'Static' selected. The 'IPv6 Address' field is empty, and the 'Link Local Address' field is filled with 'FE80::204:9AFF:FECA:C849'.

## Configuring Router0

Router0

Physical **Config** CLI Attributes

**GLOBAL**

Settings

Algorithm Settings

**ROUTING**

Static

RIP

**SWITCHING**

VLAN Database

**INTERFACE**

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

**GigabitEthernet0/0**

Port Status ☒ On

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

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0060.3E2C.9501

IP Configuration

IP Address 192.168.1.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Router0

Physical **Config** CLI Attributes

**GLOBAL**

Settings

Algorithm Settings

**ROUTING**

Static

RIP

**SWITCHING**

VLAN Database

**INTERFACE**

GigabitEthernet0/0

GigabitEthernet0/1

**Serial0/1/0**

Serial0/1/1

**Serial0/1/0**

Port Status ☒ On

Duplex ☒ Full Duplex

Clock Rate 1200

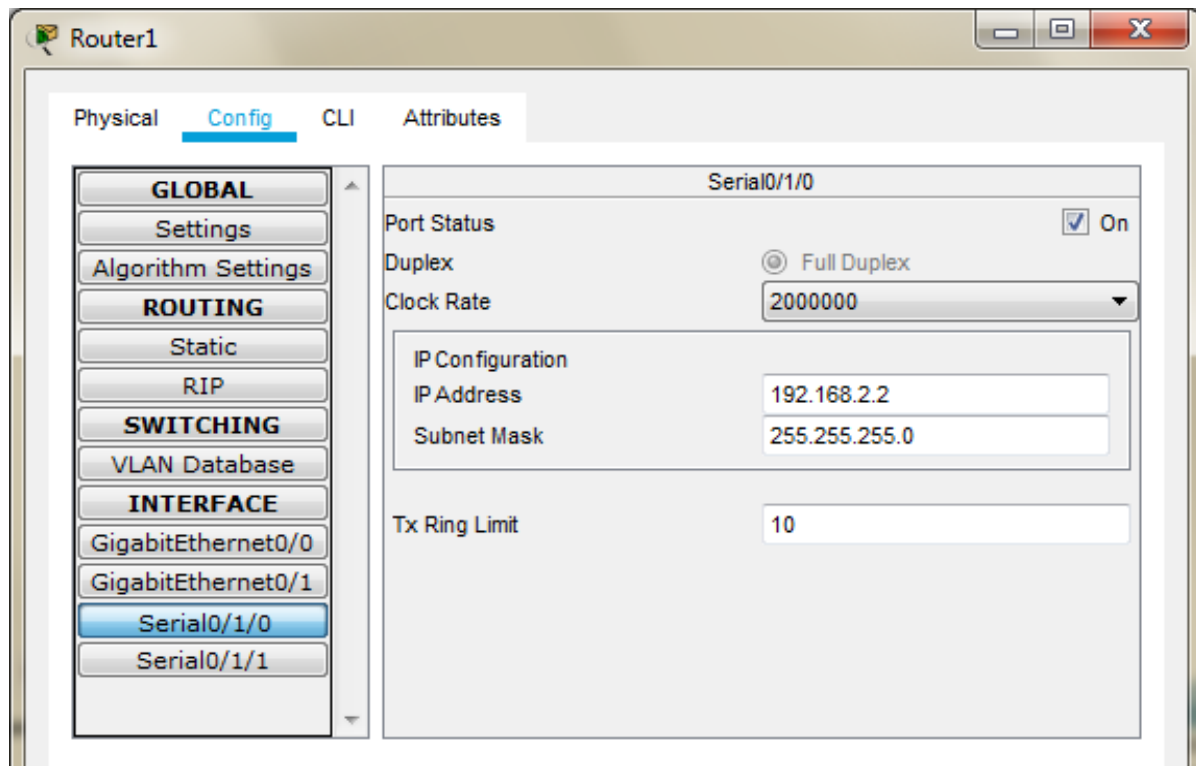
IP Configuration

IP Address 192.168.2.1

Subnet Mask 255.255.255.0

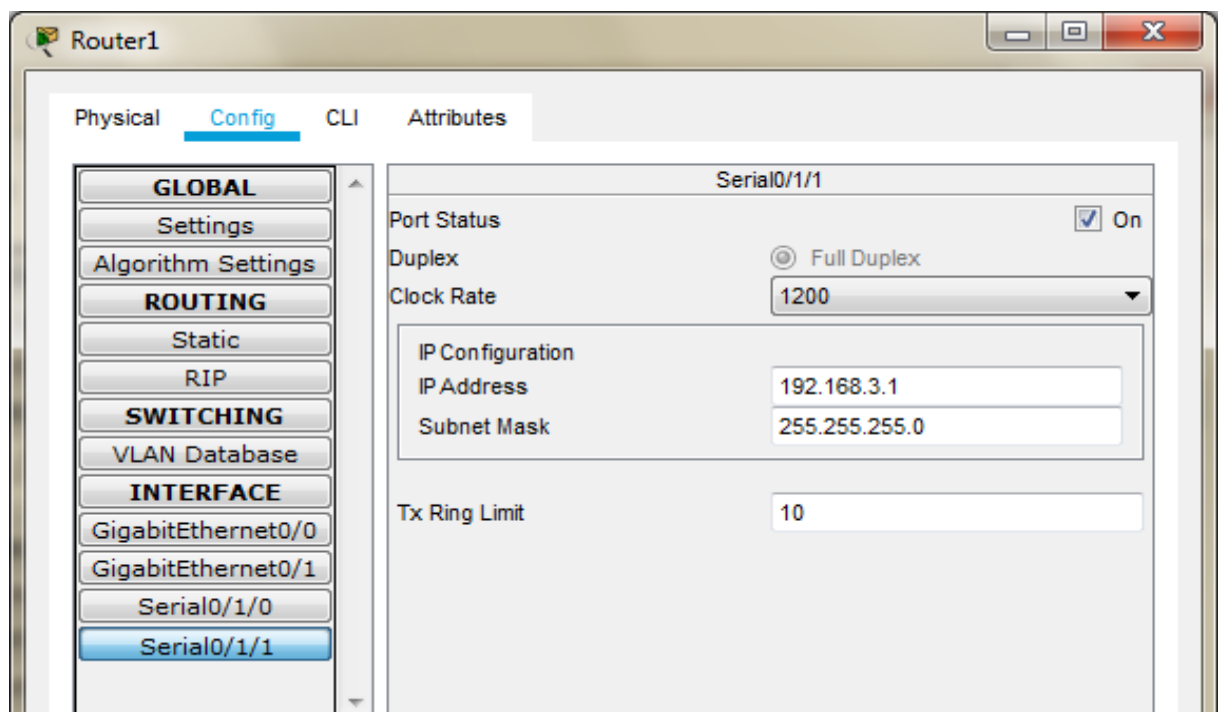
Tx Ring Limit 10

## Configuring Router1



The screenshot shows the 'Router1' configuration window with the 'Config' tab selected. The left sidebar contains a tree view with categories: GLOBAL, Settings, Algorithm Settings, ROUTING, Static, RIP, SWITCHING, VLAN Database, and INTERFACE. Under the INTERFACE category, 'Serial0/1/0' is selected. The main panel displays the configuration for 'Serial0/1/0'. The 'Port Status' is checked and set to 'On'. The 'Duplex' is set to 'Full Duplex'. The 'Clock Rate' is set to '2000000'. The 'IP Configuration' section shows 'IP Address' as '192.168.2.2' and 'Subnet Mask' as '255.255.255.0'. The 'Tx Ring Limit' is set to '10'.

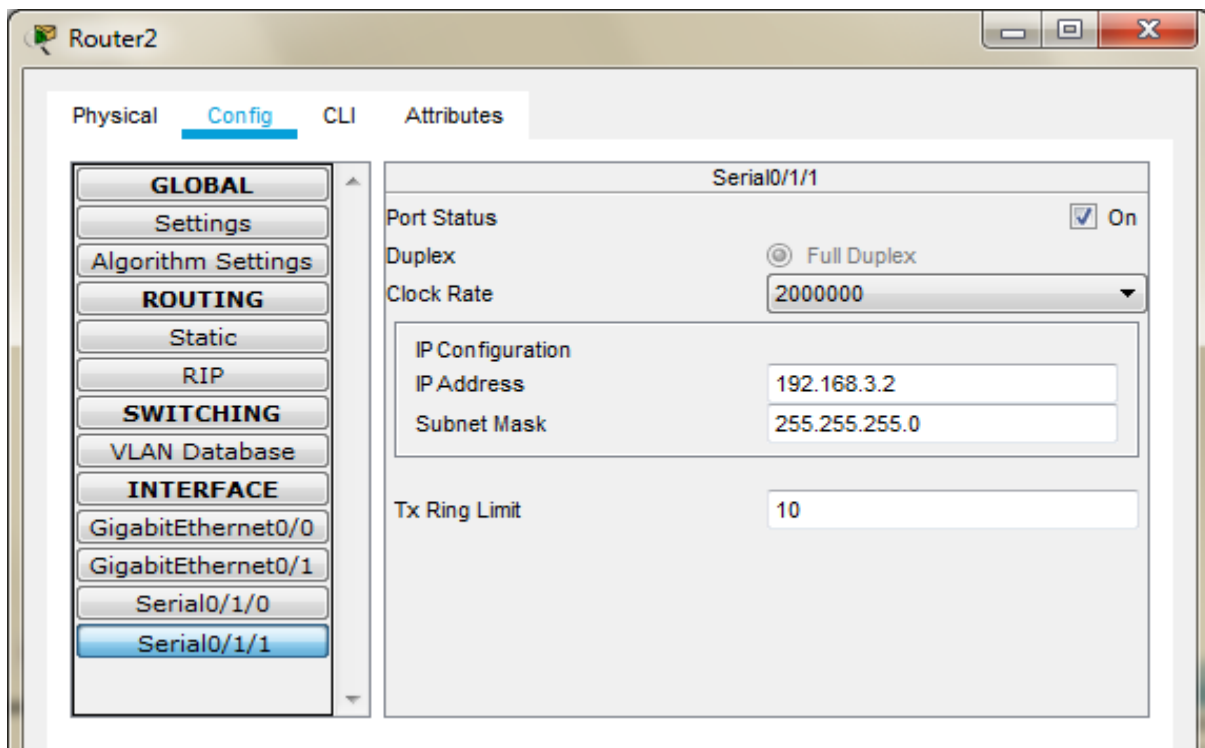
Serial0/1/0	
Port Status	<input checked="" type="checkbox"/> On
Duplex	Full Duplex
Clock Rate	2000000
IP Configuration	
IP Address	192.168.2.2
Subnet Mask	255.255.255.0
Tx Ring Limit	10



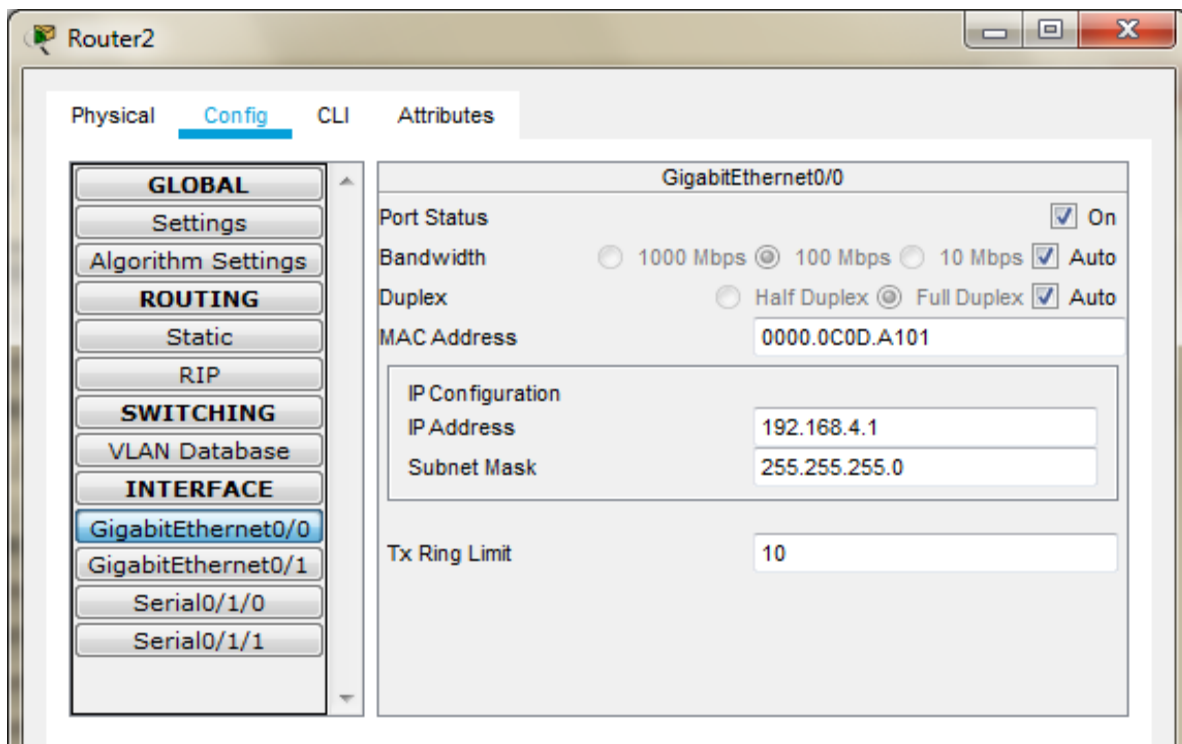
The screenshot shows the 'Router1' configuration window with the 'Config' tab selected. The left sidebar is the same as the previous window, but 'Serial0/1/1' is now selected under the INTERFACE category. The main panel displays the configuration for 'Serial0/1/1'. The 'Port Status' is checked and set to 'On'. The 'Duplex' is set to 'Full Duplex'. The 'Clock Rate' is set to '1200'. The 'IP Configuration' section shows 'IP Address' as '192.168.3.1' and 'Subnet Mask' as '255.255.255.0'. The 'Tx Ring Limit' is set to '10'.

Serial0/1/1	
Port Status	<input checked="" type="checkbox"/> On
Duplex	Full Duplex
Clock Rate	1200
IP Configuration	
IP Address	192.168.3.1
Subnet Mask	255.255.255.0
Tx Ring Limit	10

## Configuring Router2

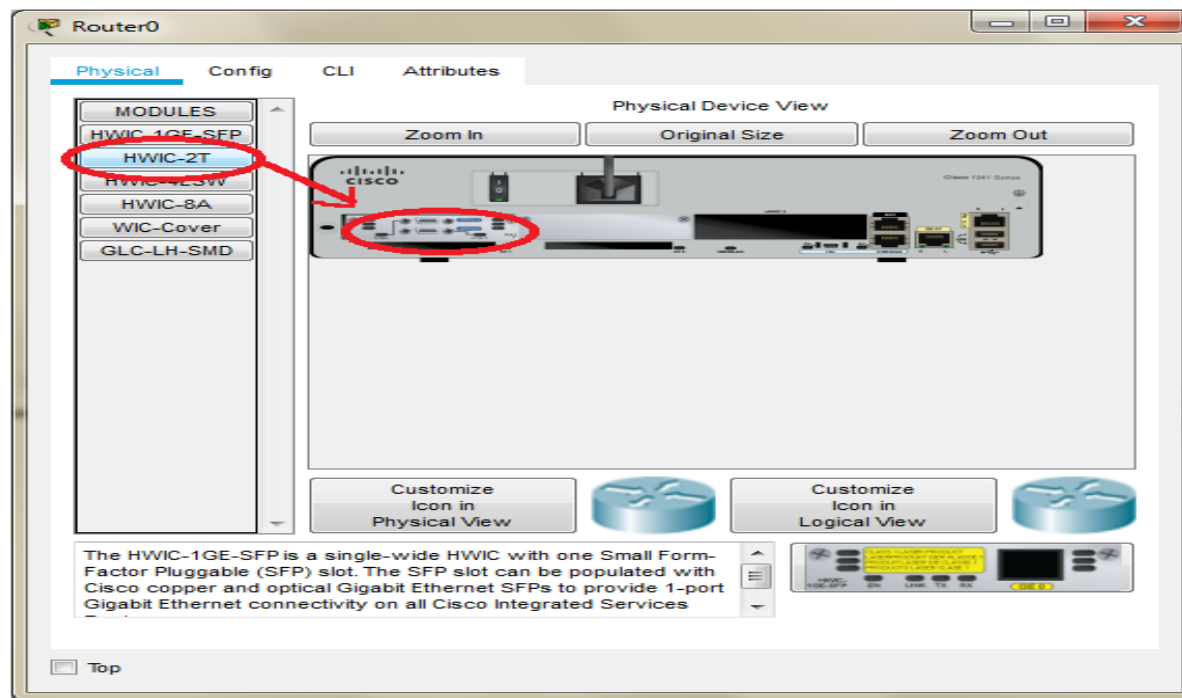


The screenshot shows the 'Router2' configuration window with the 'Config' tab selected. The left sidebar contains a tree view with categories: GLOBAL, Settings, Algorithm Settings, ROUTING, Static, RIP, SWITCHING, VLAN Database, and INTERFACE. Under the INTERFACE category, 'Serial0/1/1' is selected. The main configuration area for 'Serial0/1/1' includes: Port Status (checked 'On'), Duplex (radio button selected for 'Full Duplex'), Clock Rate (dropdown menu set to '2000000'), IP Configuration (IP Address: '192.168.3.2', Subnet Mask: '255.255.255.0'), and Tx Ring Limit (text box set to '10').

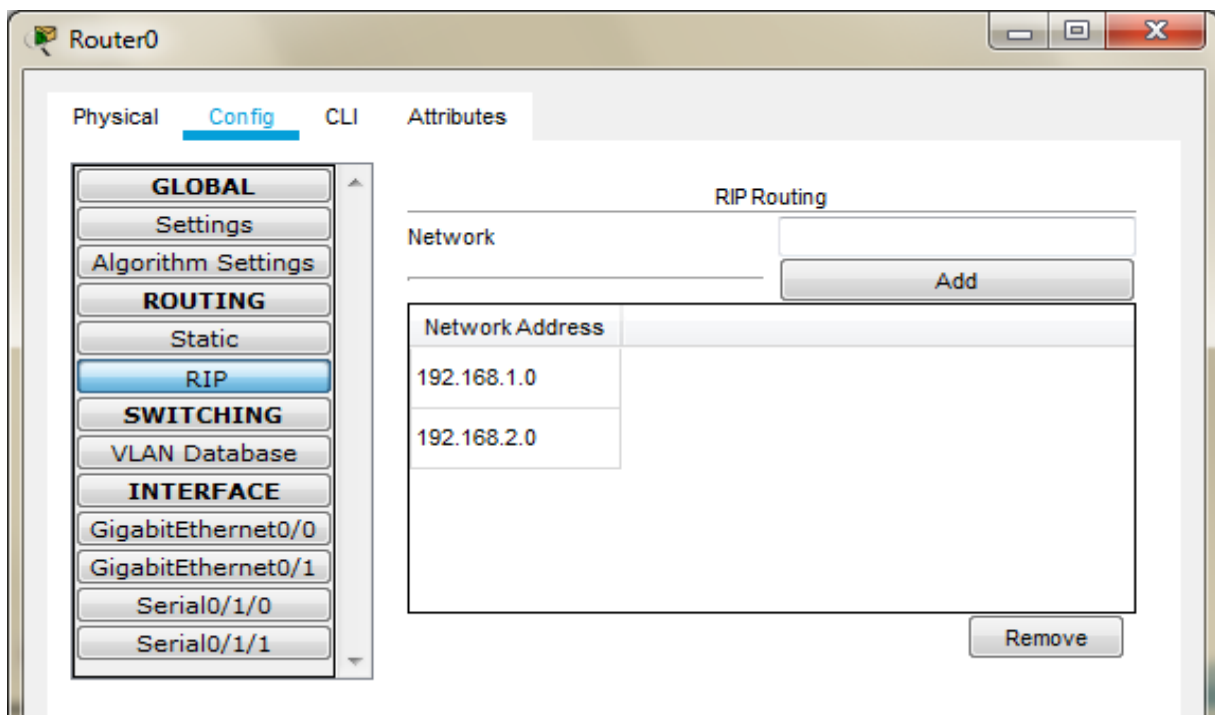


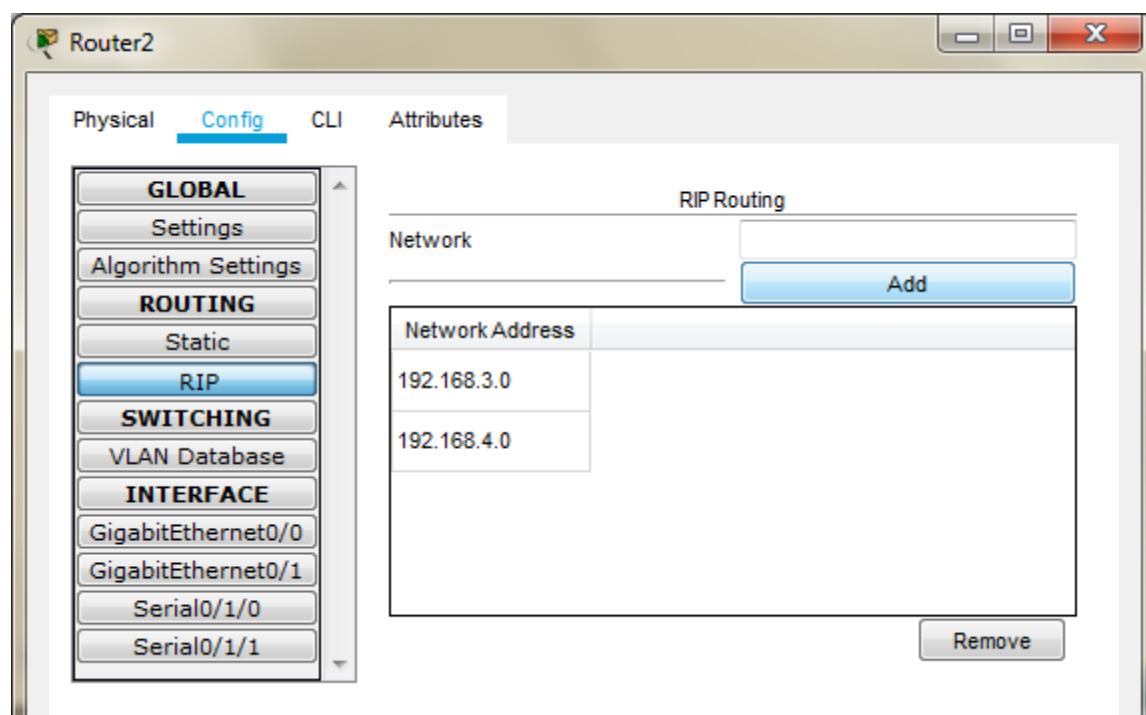
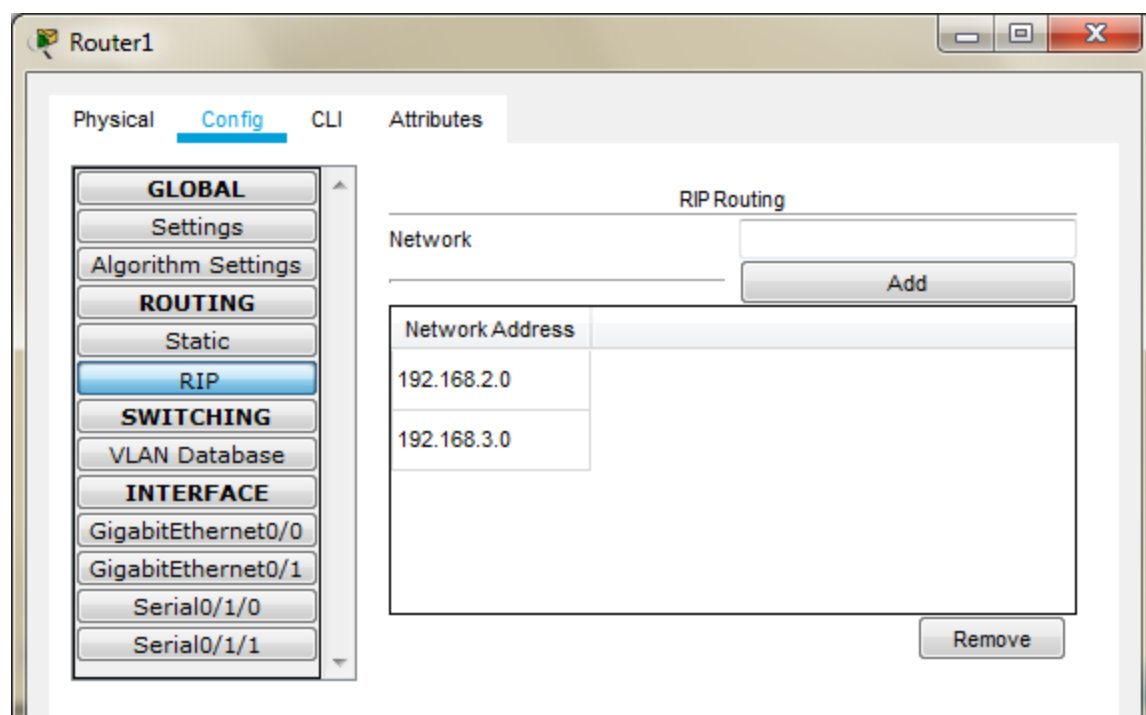
The screenshot shows the 'Router2' configuration window with the 'Config' tab selected. The left sidebar is the same as the previous window, but 'GigabitEthernet0/0' is selected under the INTERFACE category. The main configuration area for 'GigabitEthernet0/0' includes: Port Status (checked 'On'), Bandwidth (radio buttons for '1000 Mbps', '100 Mbps', and '10 Mbps', with '100 Mbps' selected), Duplex (radio buttons for 'Half Duplex' and 'Full Duplex', with 'Full Duplex' selected), MAC Address (text box set to '0000.0C0D.A101'), IP Configuration (IP Address: '192.168.4.1', Subnet Mask: '255.255.255.0'), and Tx Ring Limit (text box set to '10').

The serial interface in each Router are added as follows



Set the RIP on each Router

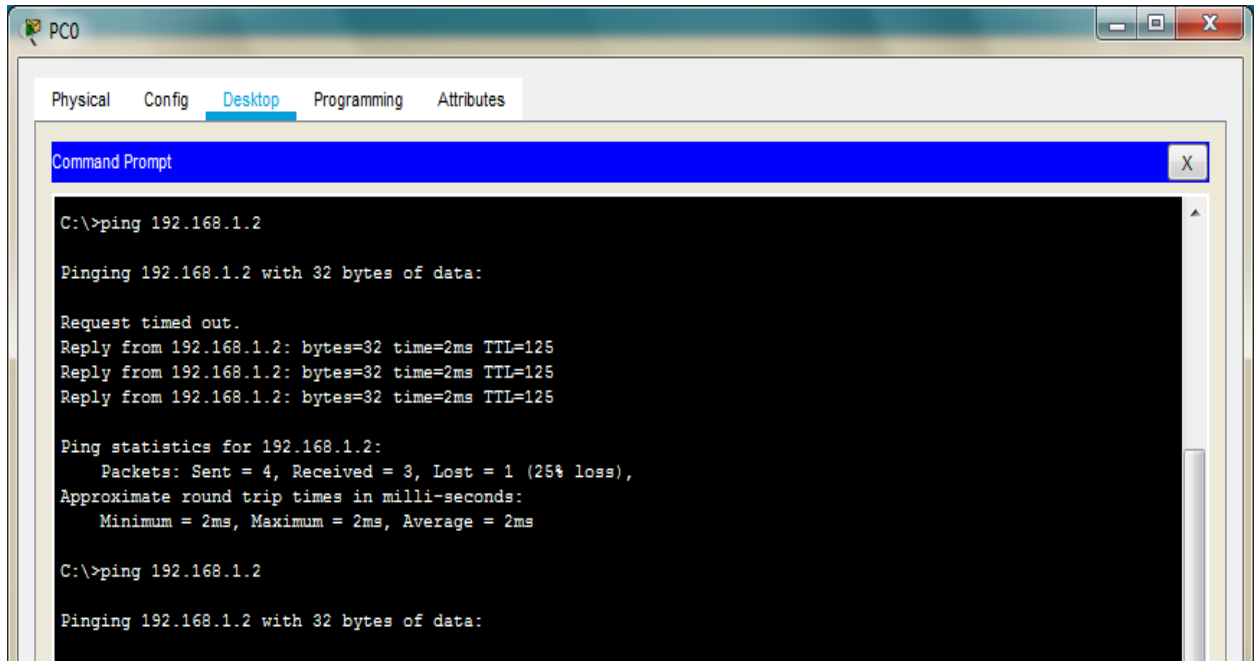




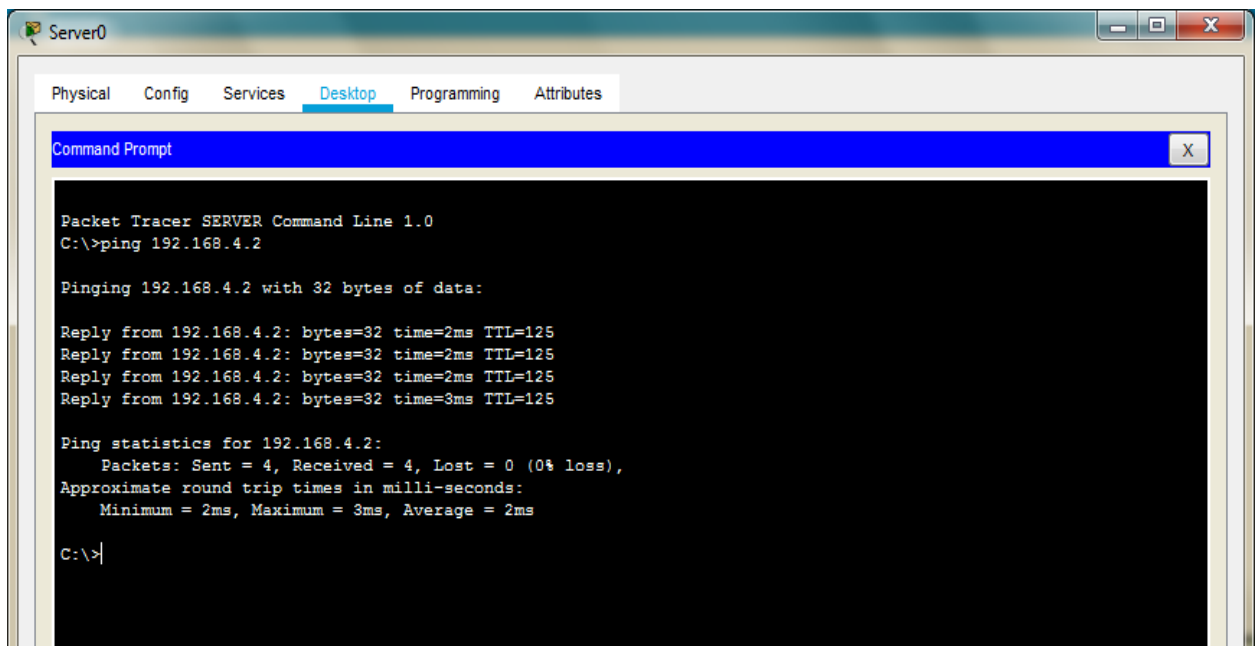


## Part 1: Verify Basic Connectivity

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

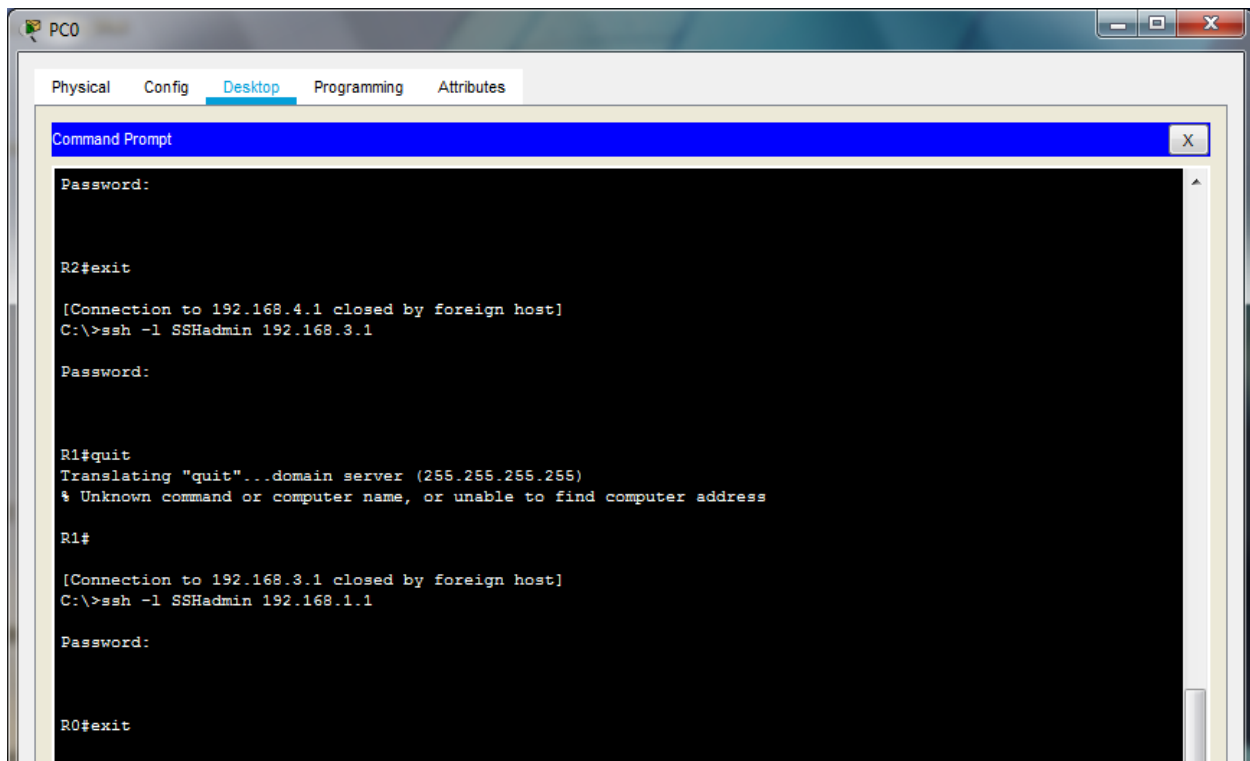
```
Router>enable
Router#configure t
Router(config)#ip domain-name ismail.com
Router(config)#hostname R0
R0(config)#
R0(config)#crypto key generate rsa
R0(config)#line vty 0 4
R0(config-line)#transport input ssh
R0(config-line)#login local
R0(config-line)#exit
R0(config)#username SSHadmin privilege 15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

### **Part b) 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**



The screenshot shows a Windows Command Prompt window titled "PC0". The window has tabs for "Physical", "Config", "Desktop" (selected), "Programming", and "Attributes". The command history is as follows:

```
Command Prompt
Password:

R2#exit
[Connection to 192.168.4.1 closed by foreign host]
C:\>ssh -l SSHAdmin 192.168.3.1

Password:

R1#quit
Translating "quit"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

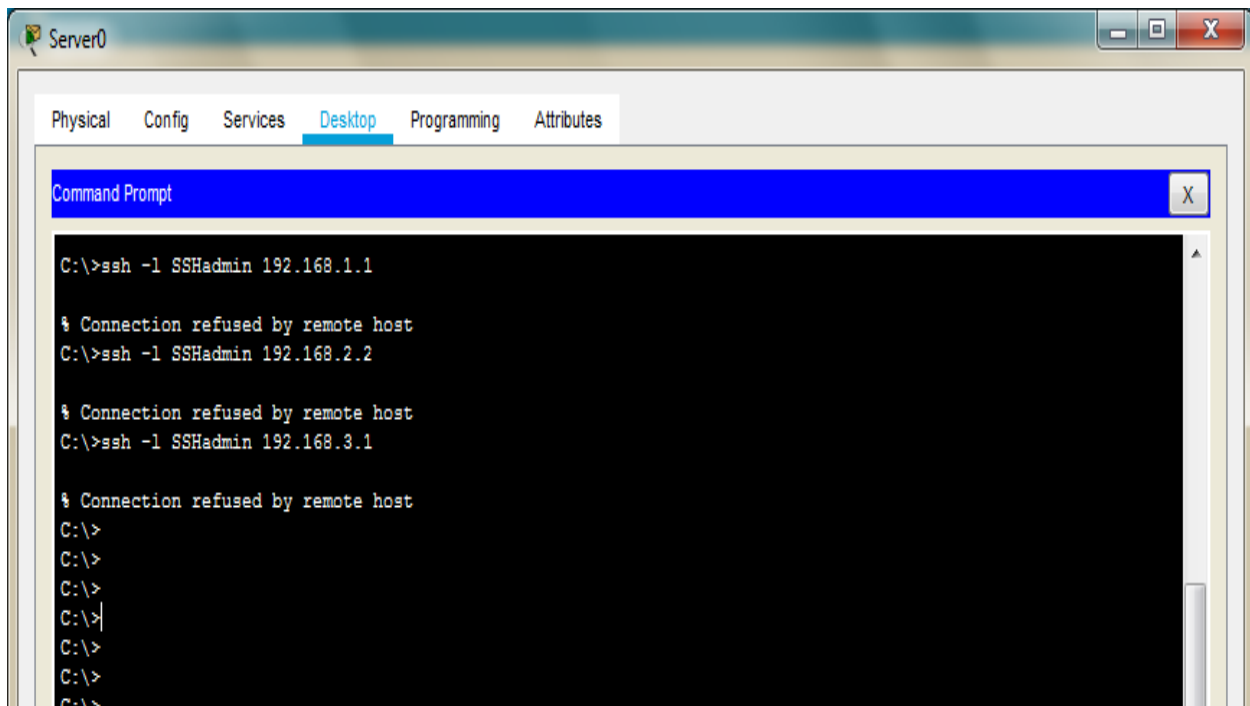
R1#

[Connection to 192.168.3.1 closed by foreign host]
C:\>ssh -l SSHAdmin 192.168.1.1

Password:

R0#exit
```

**Now we verify the remote access from Server using the following and find it to be a Failure**



The screenshot shows a Windows Command Prompt window titled "Server0". The window has tabs for "Physical", "Config", "Services", "Desktop" (selected), "Programming", and "Attributes". The command history is as follows:

```
Command Prompt

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:\>
C:\>
C:\>
C:\>
C:\>
C:\>
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 **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#
R1#configure terminal
R1(config)#interface Serial0/1/1
R1(config-if)#ip access-group 120 in
R1(config-if)#exit
```

Verify the above entering the following commands in the PC

