LAB ASSIGNMENT – 1

INFORMATION SECURITY MANAGEMENT

NAME: ADITYA KALRA

REG NO: 19BCE0390

Question – 1: Connecting two VLANs using switches.

***Aim*:**

Connecting two VLANs using switches.

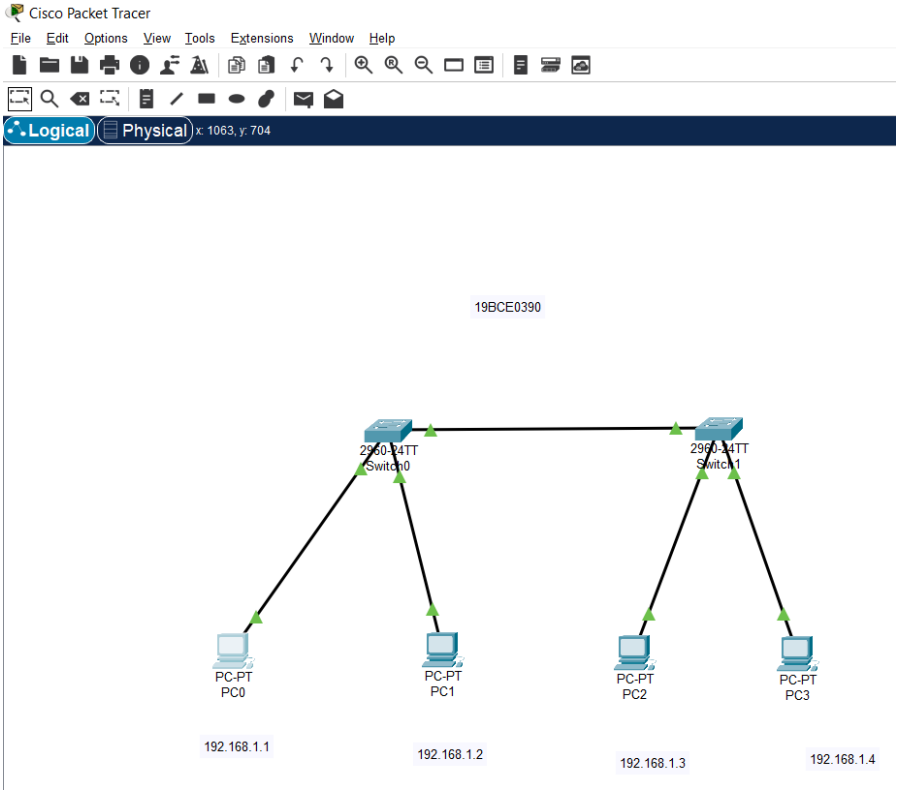
***Procedure*:**

Steps:

1) Place two 2690 switches and 4 PCs.
2) Connect the two switches using copper straight through wire.
3) Connect two PCs to switch-1 and other PCs to switch-2 using copper straight through wire.
4) Assign IP addresses to the PCs (192.168.1.1 to 192.168.1.4)
5) Configure the IP of both the switches using CLI command. Give IP 10.0.0.1 to switch-1 and 10.0.0.2 to switch-2.
6) Send packages between the PCs to confirm the connection.

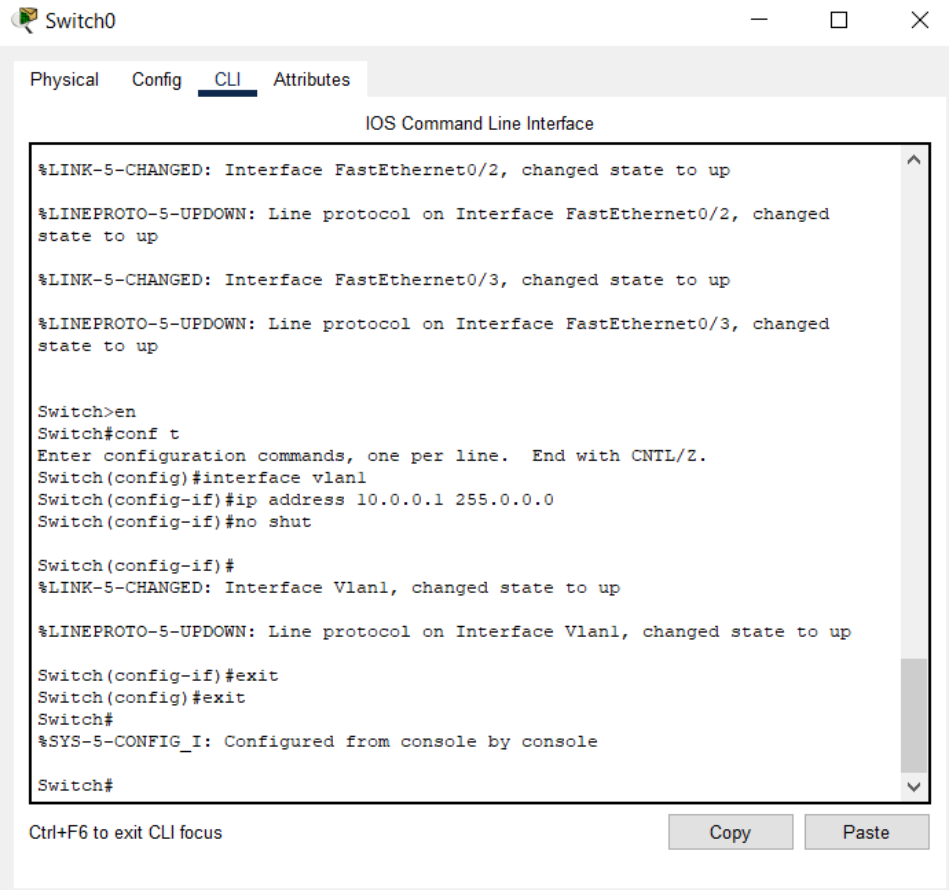
***Screenshots*:**

Network:

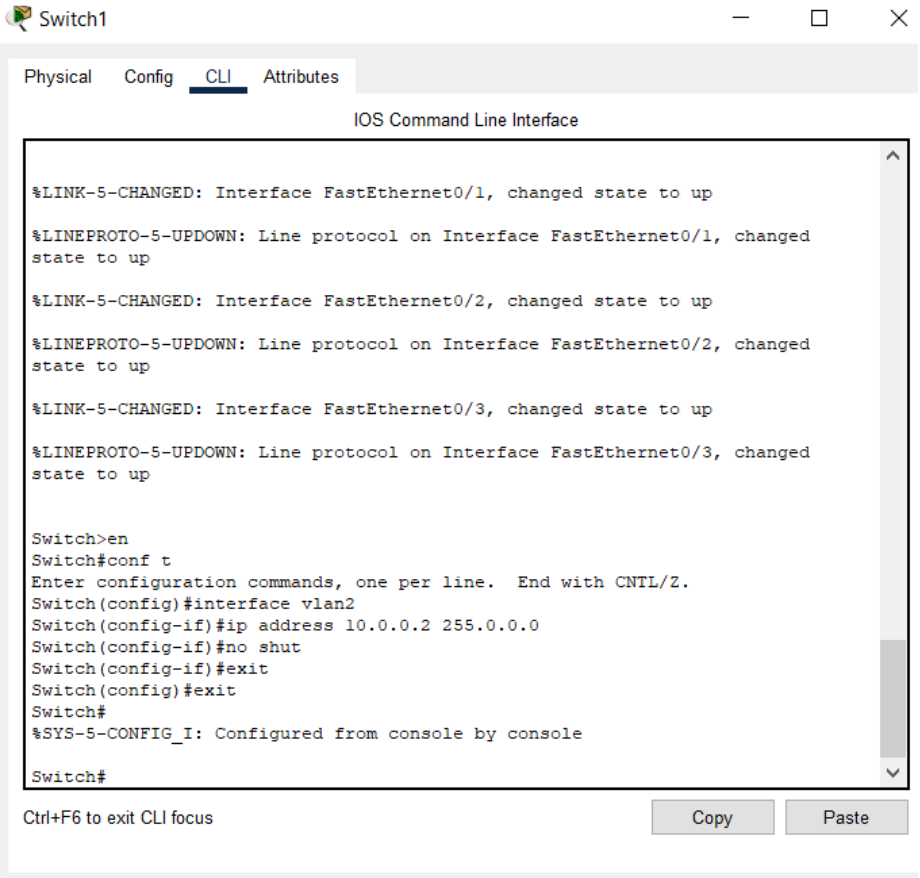

Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical Physical x: 1063, y: 704
19BCE0390
2960-24TT
Switch0
2960-24TT
Switch1
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
192.168.1.1
192.168.1.2
192.168.1.3
192.168.1.4

CLI:

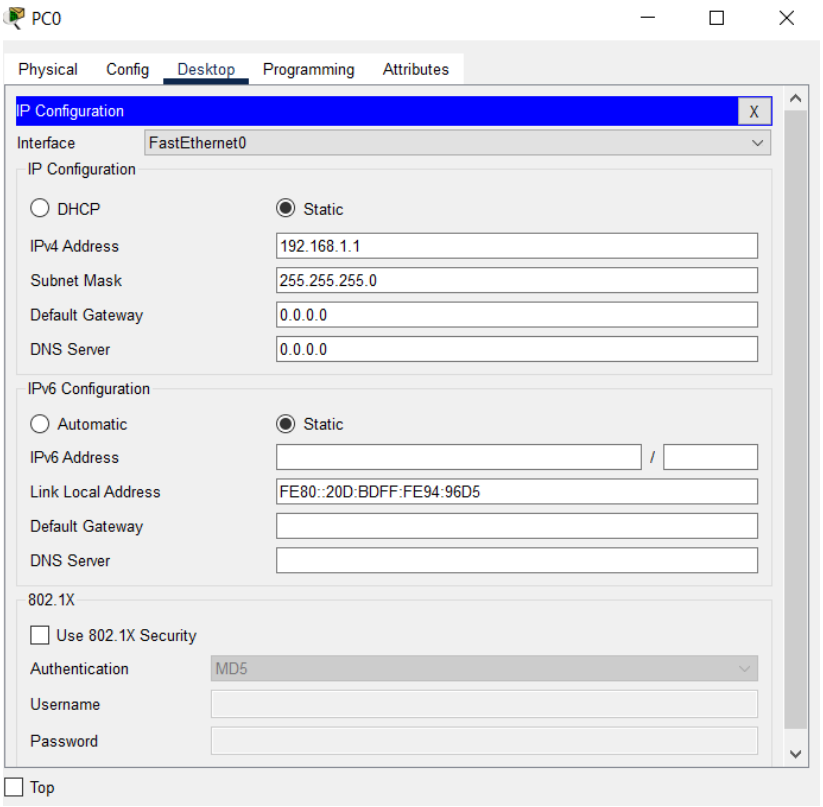
Switch0:

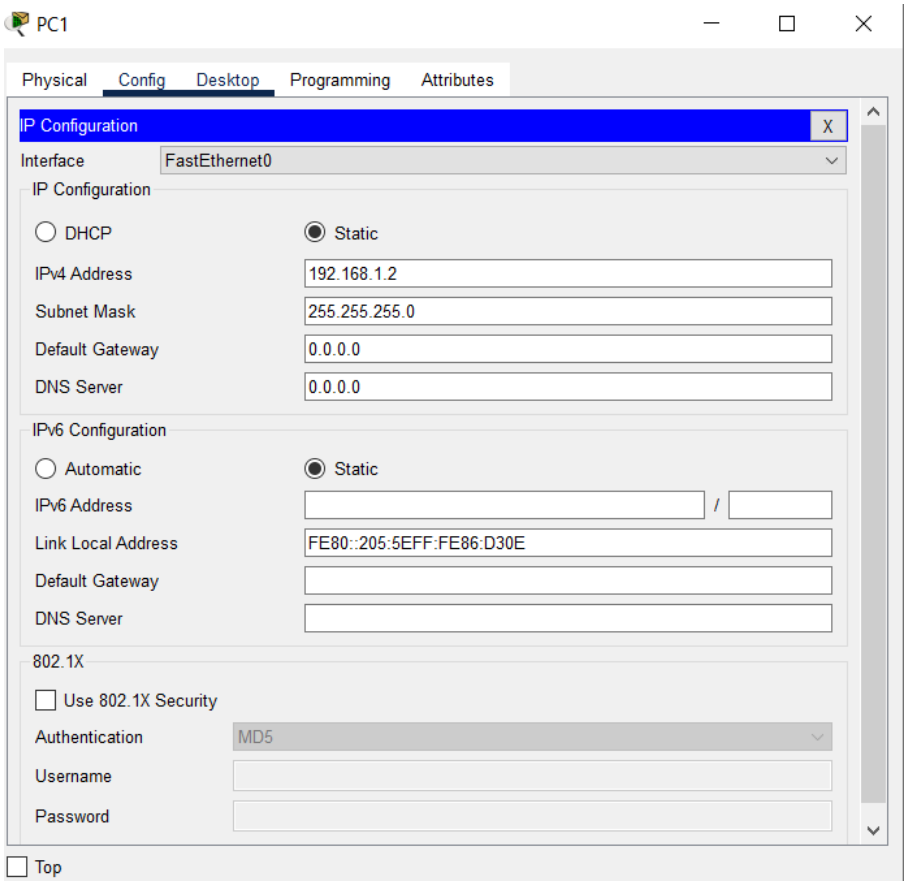

Switch0
Physical Config CLI Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan1
Switch(config-if)#ip address 10.0.0.1 255.0.0.0
Switch(config-if)#no shut
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#
Ctrl+F6 to exit CLI focus
Copy
Paste

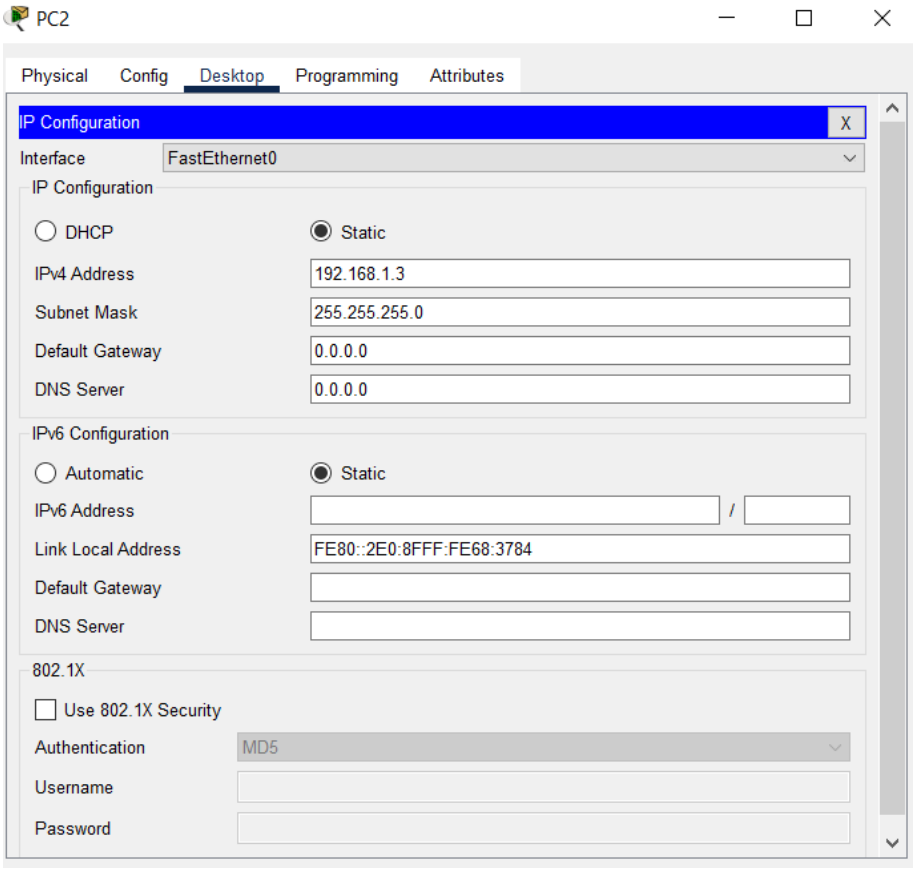
Switch1:

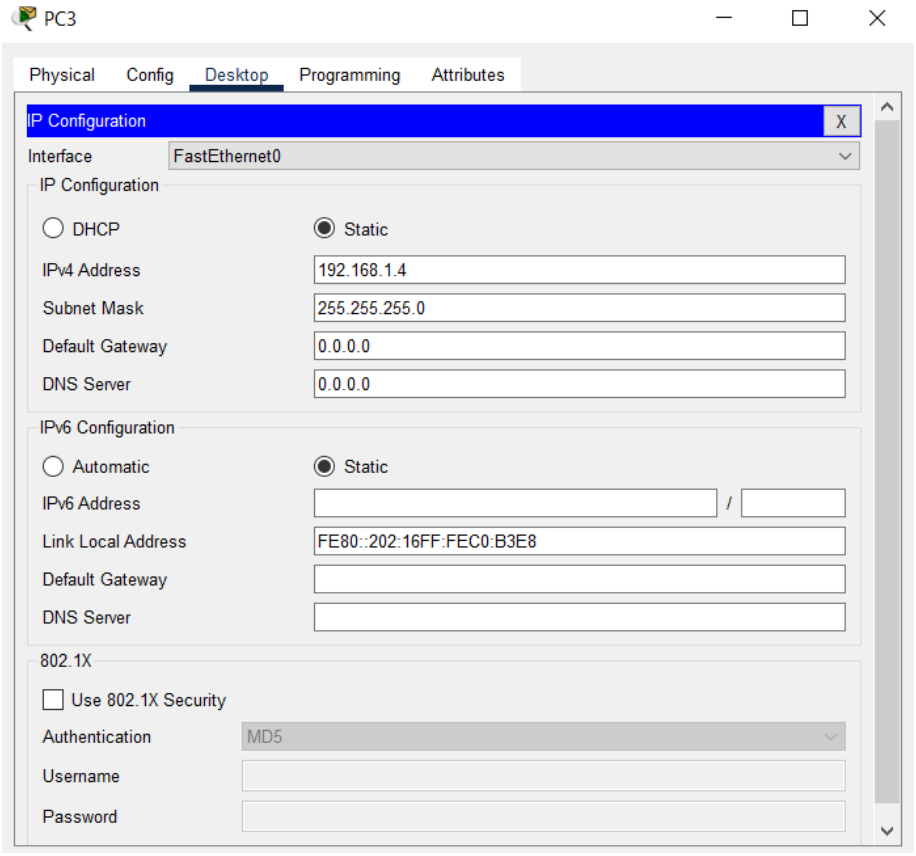


IP config of PCs:

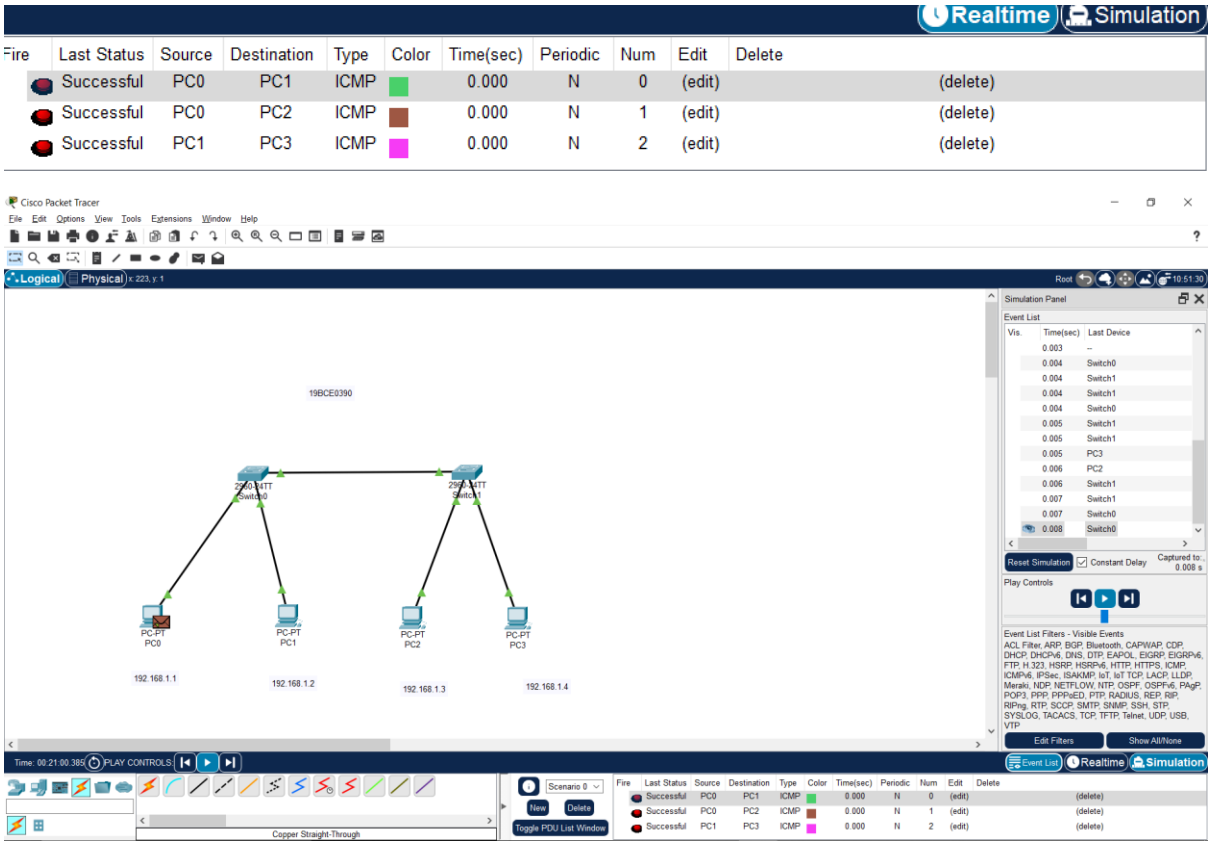



PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::205:5EFF:FE86:D30E
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::2E0:8FFF:FE68:3784
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password



Packets transfer:



***Conclusion*:**

I sent three packets from PC0 to PC1, PC0 to PC2 and PC1 to PC3. All the packets were reached successfully and I was able to connect VLANs using switches.

Question – 2: Connecting two networks by configuring a router.

***Aim*:**

Connecting two networks by configuring a Router.

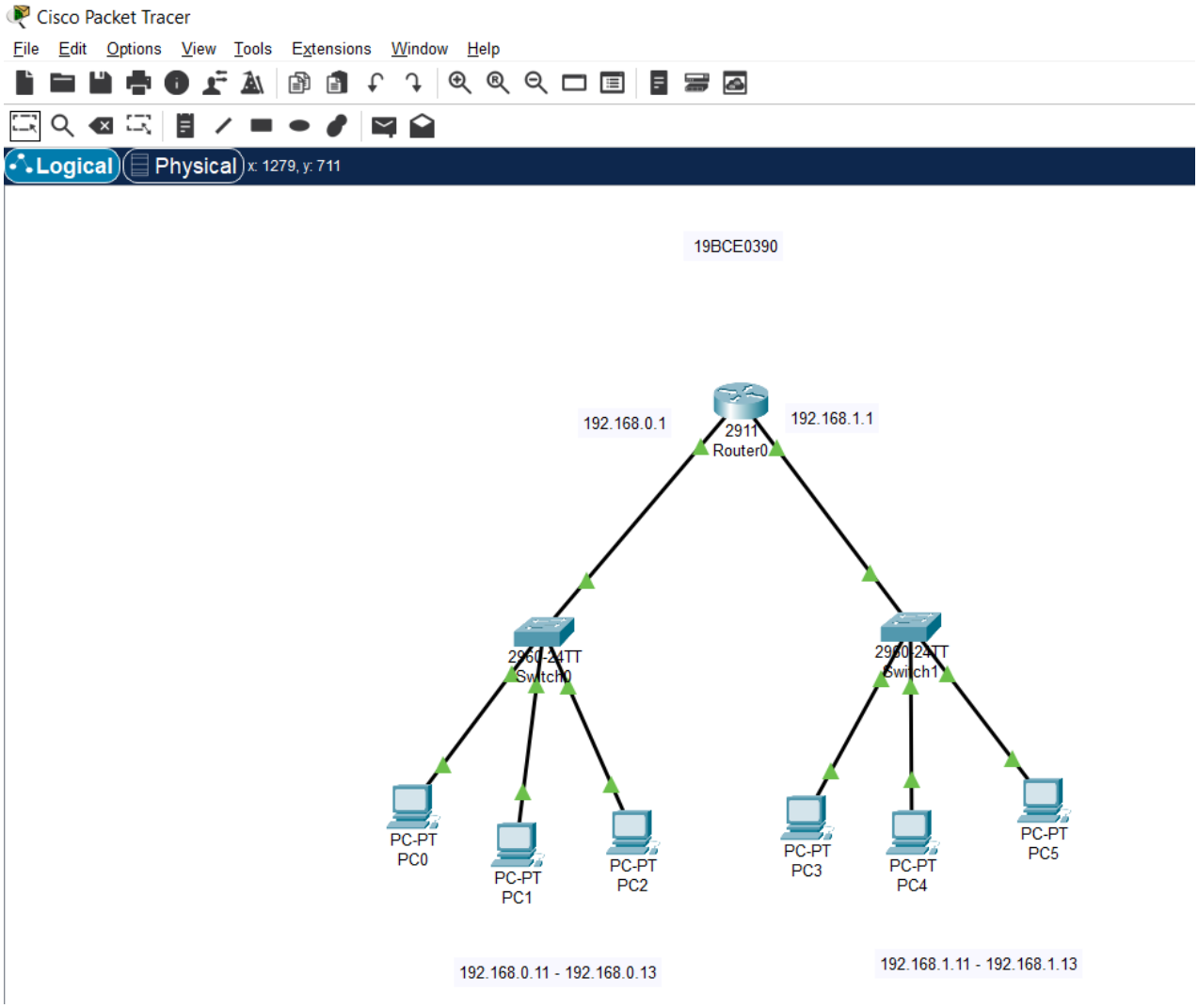
***Procedure*:**

Steps:

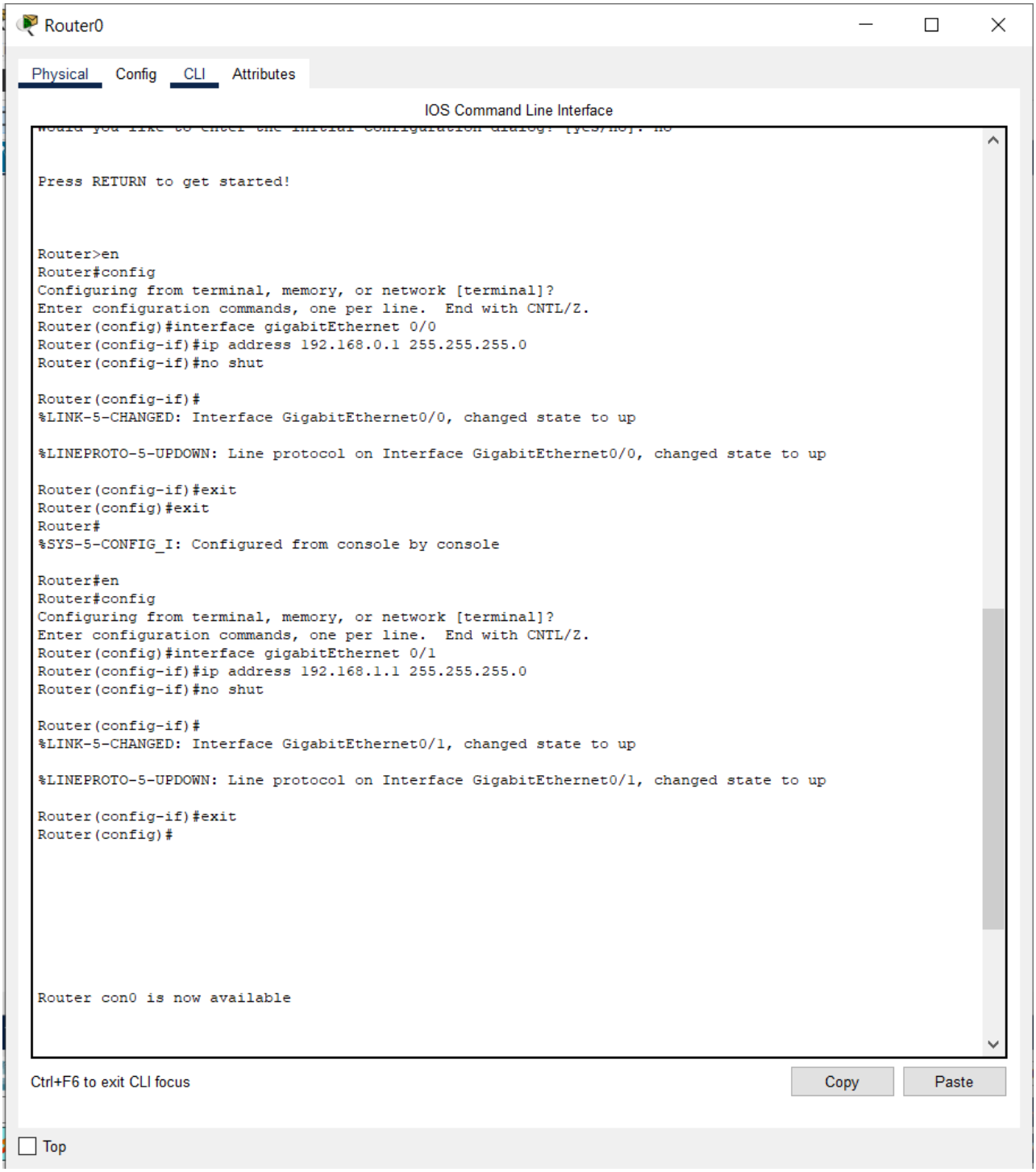
1) Place a 2911 router.
2) Place two 2690 switches and 6 PCs.
3) Connect the switches to the router using copper straight through wire through GigabitEthernet of the router.
4) Connect three PCs to switch-1 and other PCs to switch-2 using copper straight through wire.
5) Assign IP addresses to the PCs. (192.168.0.11 - 192.168.0.11 to PC0 to PC2 and 192.168.1.11 - 192.168.1.11 to PC3 to PC5).
6) Configure the IP of the router using CLI command. Give IP 192.168.0.1 to router at gigabitEthernet 0/0 and IP 192.168.1.1 to router at gigabitEthernet 0/1.
7) Send packages between the PCs to confirm the connection.

***Screenshots*:**

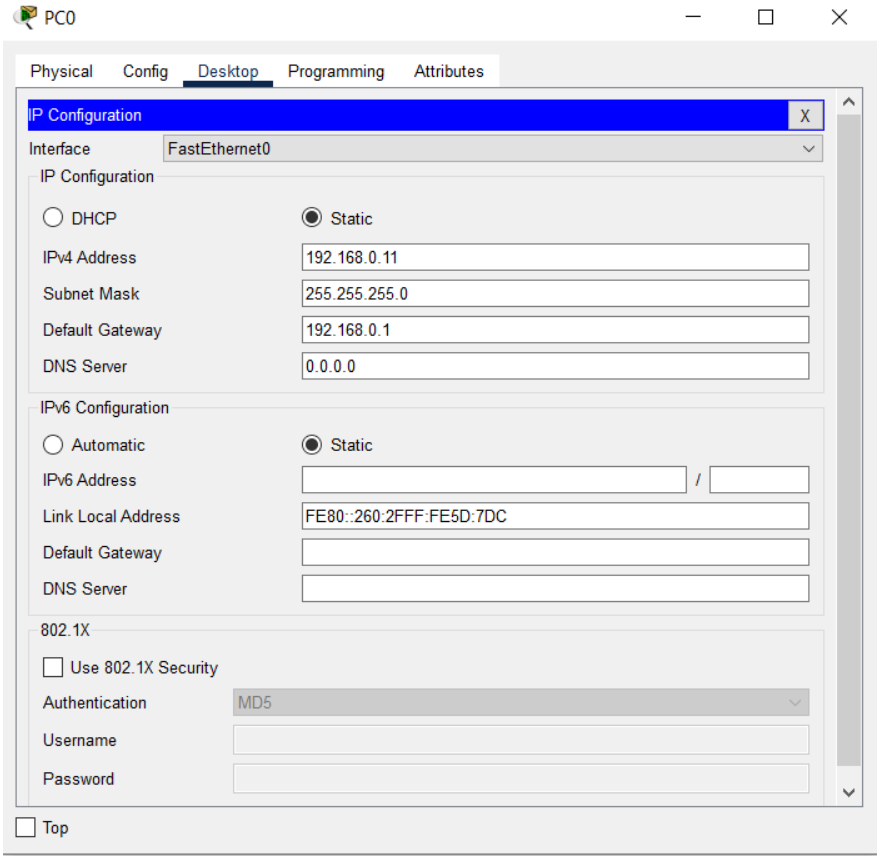
Network:

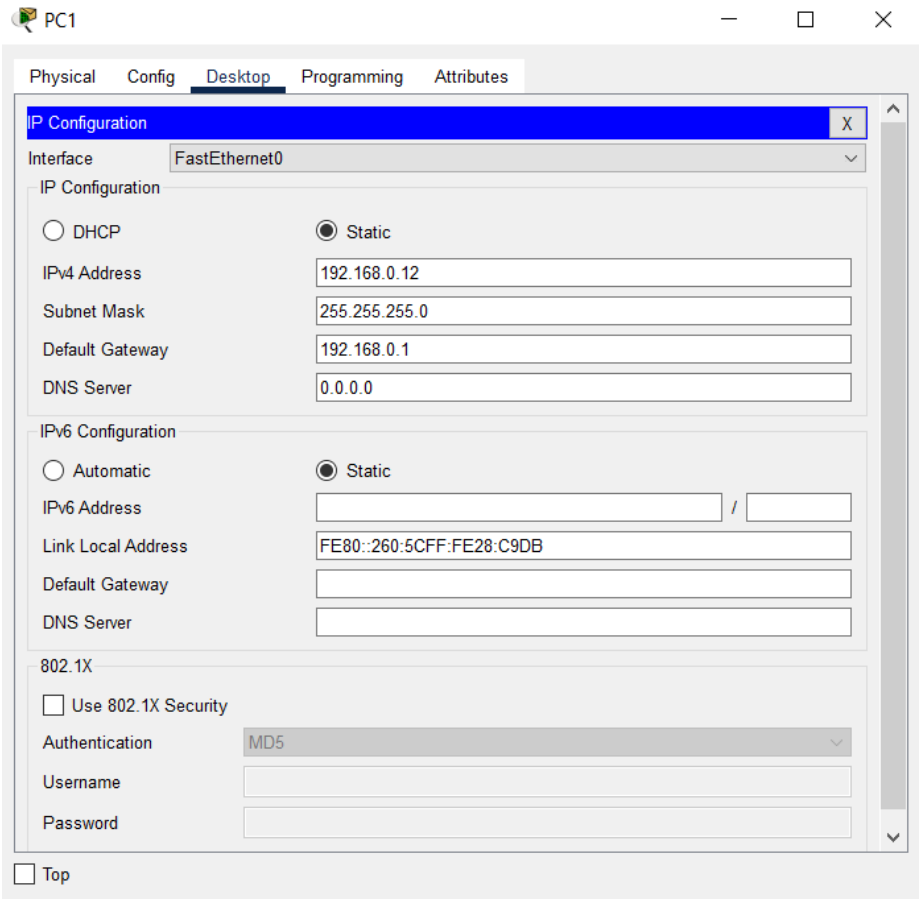

Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical Physical x: 1279, y: 711
19BCE0390
192.168.0.1
2911
Router0
192.168.1.1
2960-24TT
Switch0
2960-24TT
Switch1
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
PC-PT
PC4
PC-PT
PC5
192.168.0.11 - 192.168.0.13
192.168.1.11 - 192.168.1.13

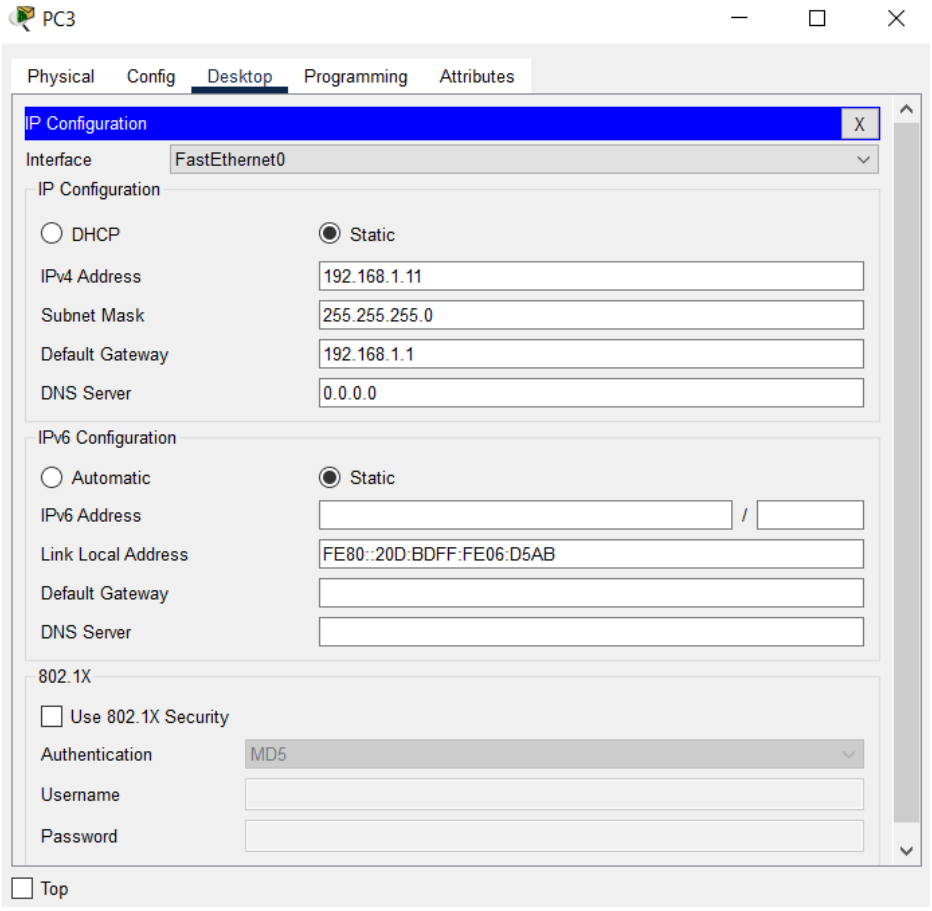
CLI:

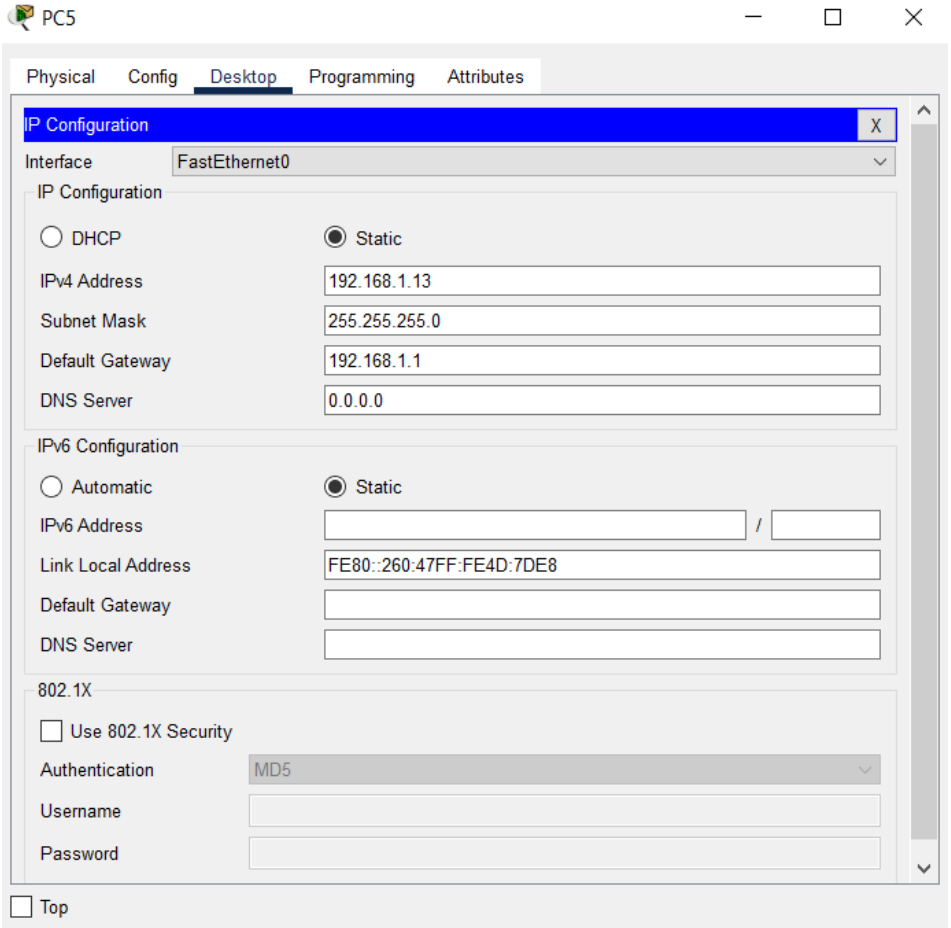


IP config of PCs:

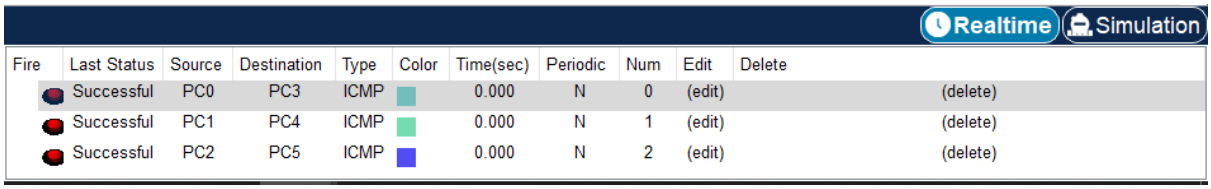

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.0.11
Subnet Mask
255.255.255.0
Default Gateway
192.168.0.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::260:2FFF:FE5D:7DC
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.0.12
Subnet Mask
255.255.255.0
Default Gateway
192.168.0.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::260:5CFF:FE28:C9DB
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

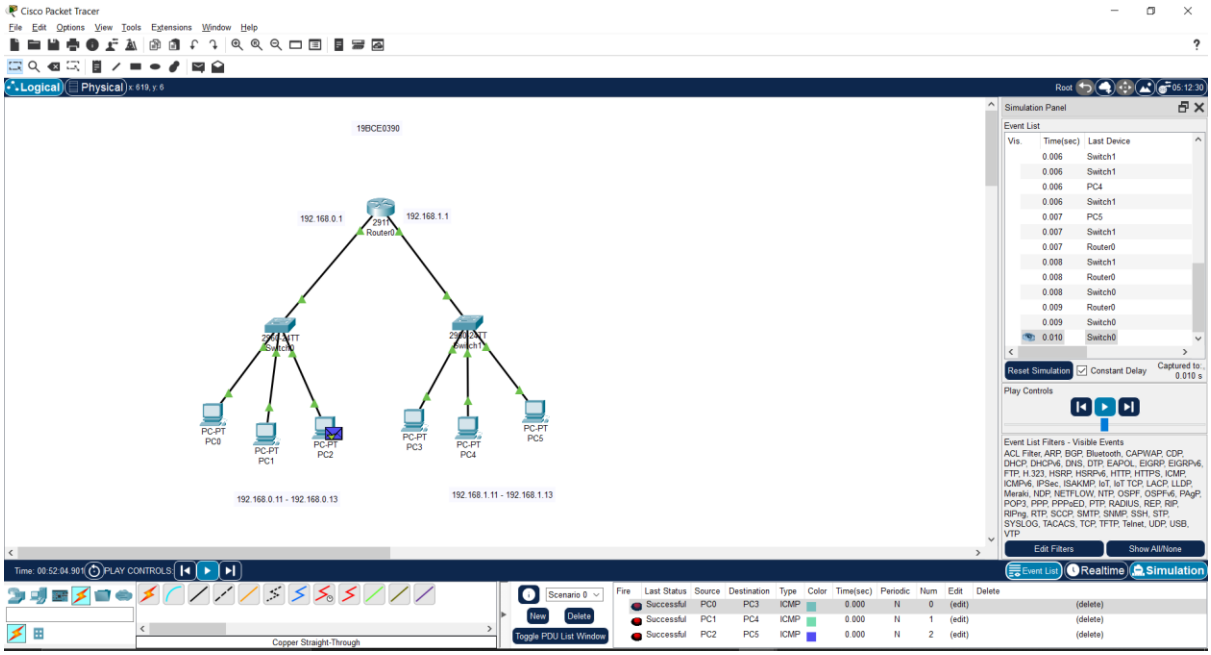

PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.11
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::20D:BDFF:FE06:D5AB
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC5
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.13
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::260:47FF:FE4D:7DE8
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

Packet transfer:



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC3	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC1	PC4	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC2	PC5	ICMP		0.000	N	2	(edit)	(delete)



Conclusion:

I sent three packets from PC0 to PC3, PC1 to PC4 and PC2 to PC5. All the packets were reached successfully and I was able to connect two networks by configuring a router.

LAB ASSIGNMENT – 2

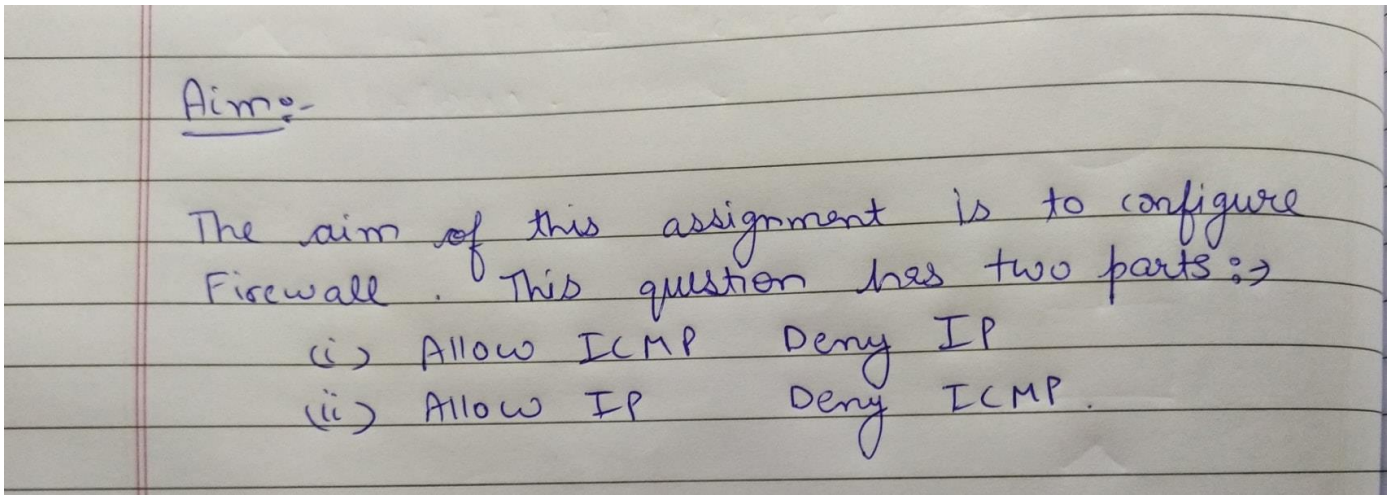
INFORMATION SECURITY MANAGEMENT

NAME: ADITYA KALRA

REG NO: 19BCE0390

Question – 1: Firewall Configuration.

***Aim*:**



***Procedure*:**

Procedure:-

1. Place a server, a Hub and 3 PCs.
2. Connect server to Hub and all the PCs to the Hub using copper straight Through Wire.
3. Provide IP address to the server 20.0.0.1
4. Switch on HTTP and DHCP services in servers.
5. In the IP configuration of each PC click on DHCP. It will dynamically allocate the IP address to the PCs.
6. Go to Desktop of the server and select IPV4 firewall.

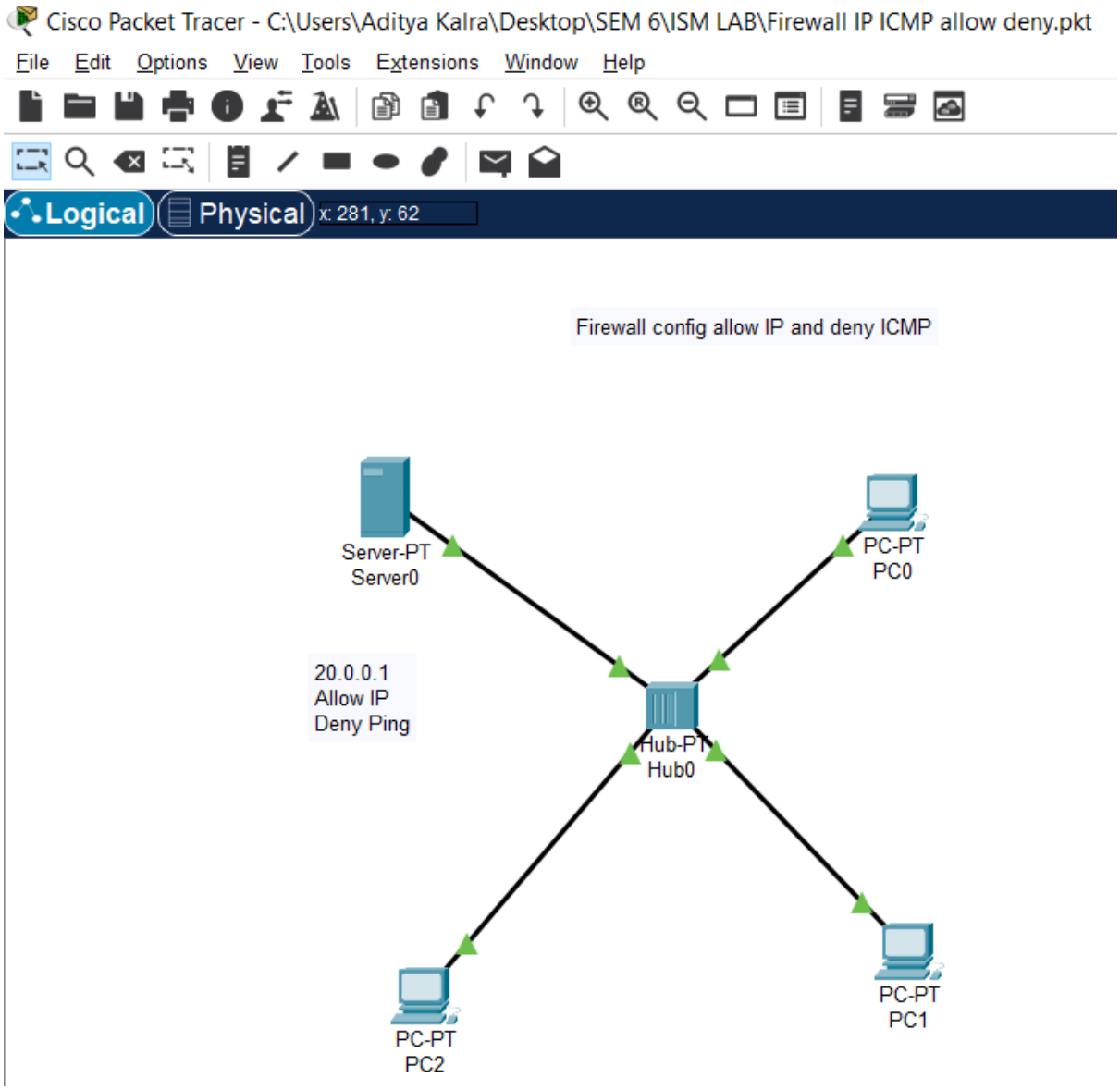
It has two parts:
- Allow IP Deny ICMP
- Allow ICMP Deny IP.

At each part try to access the server through ping command & web browsers.

To allow/deny, ICMP/IP choose from the drop down menu and give remote IP 0.0.0.0 & v Mask as 255.255.255.255
Remote Wildcard

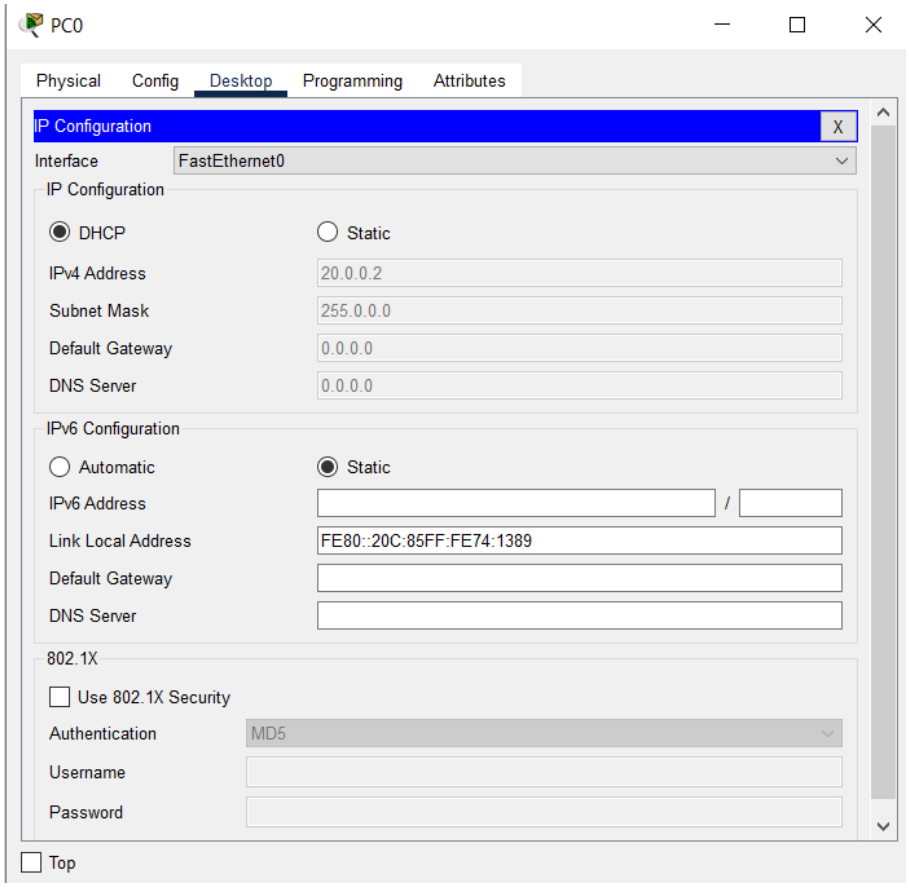
Screenshots:

Network:

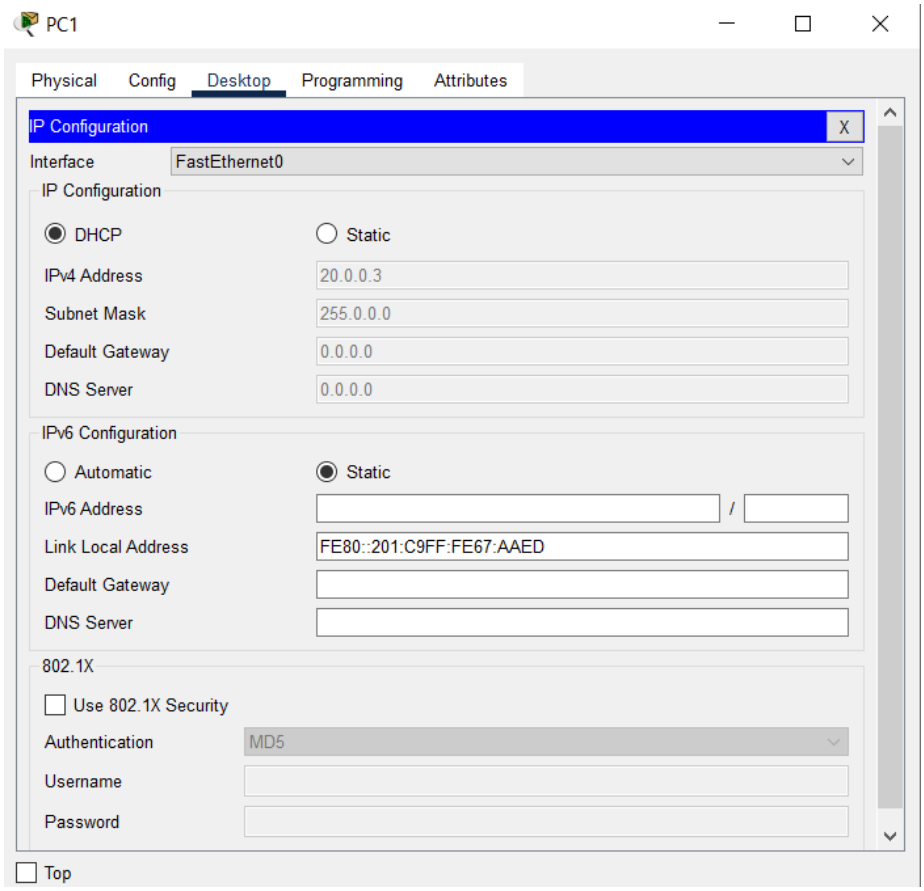


IP Config:

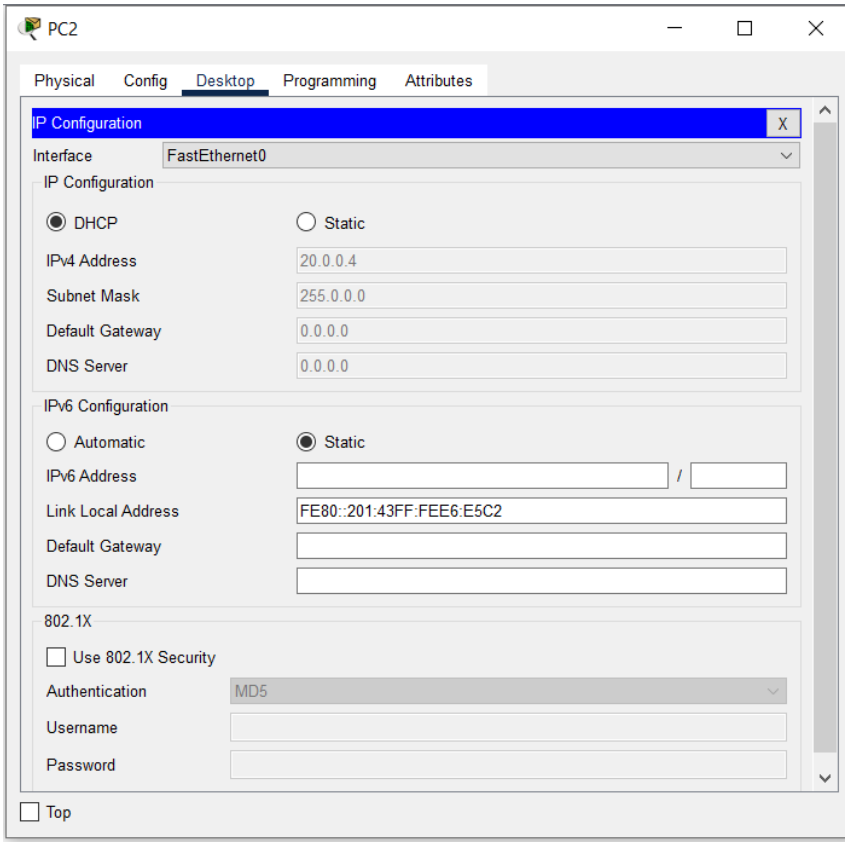
PC0:


PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
20.0.0.2
Subnet Mask
255.0.0.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::20C:85FF:FE74:1389
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

PC1:

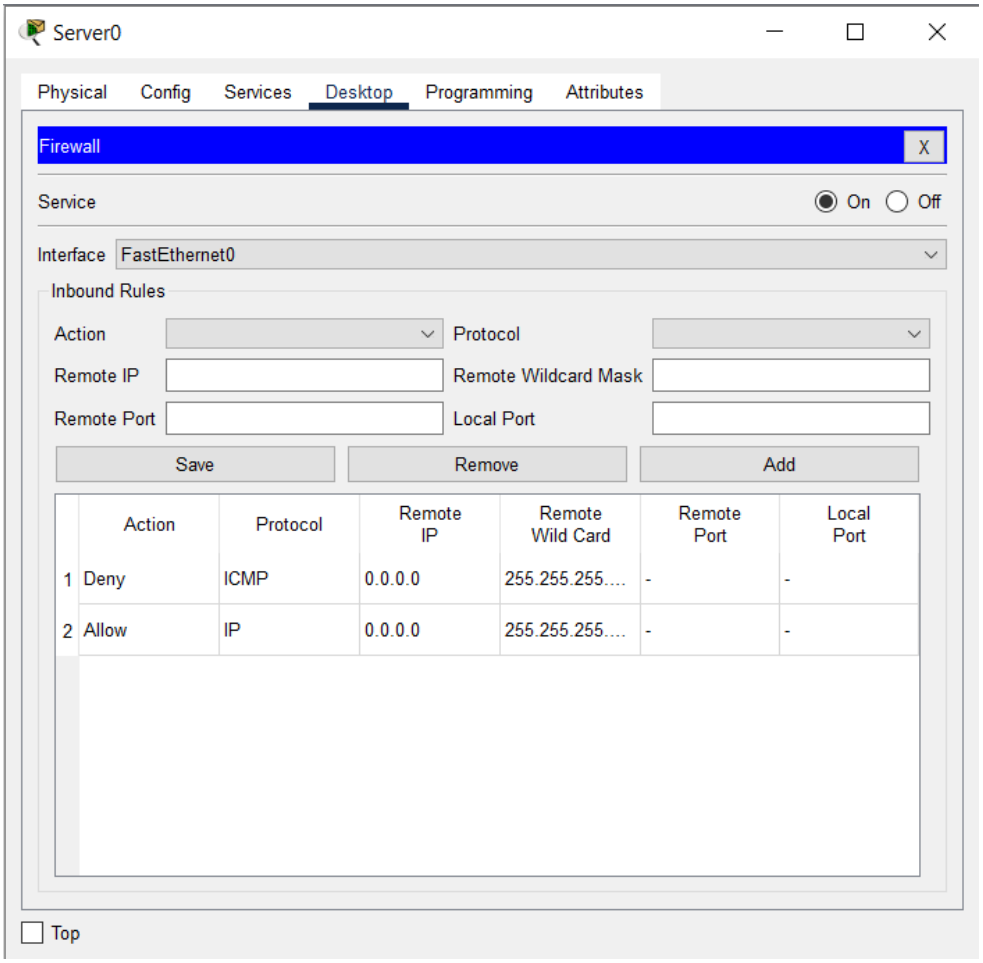

PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
20.0.0.3
Subnet Mask
255.0.0.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::201:C9FF:FE67:AAED
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

PC2:

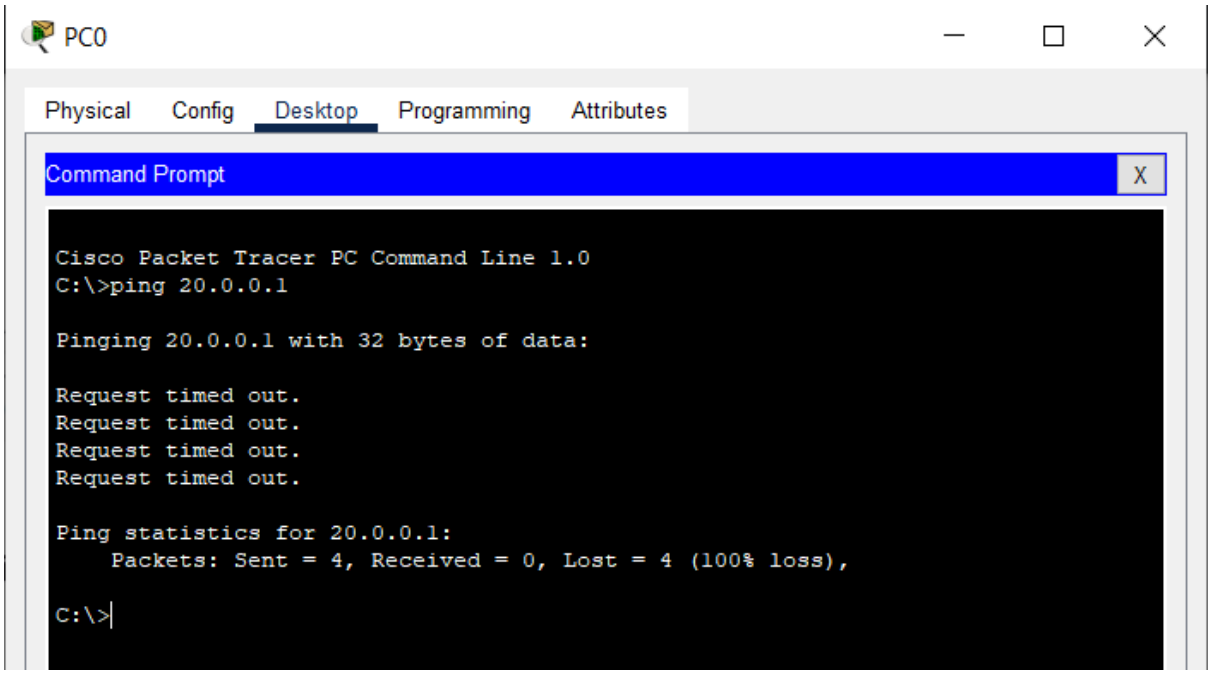


Part a) Deny ICMP Allow IP.

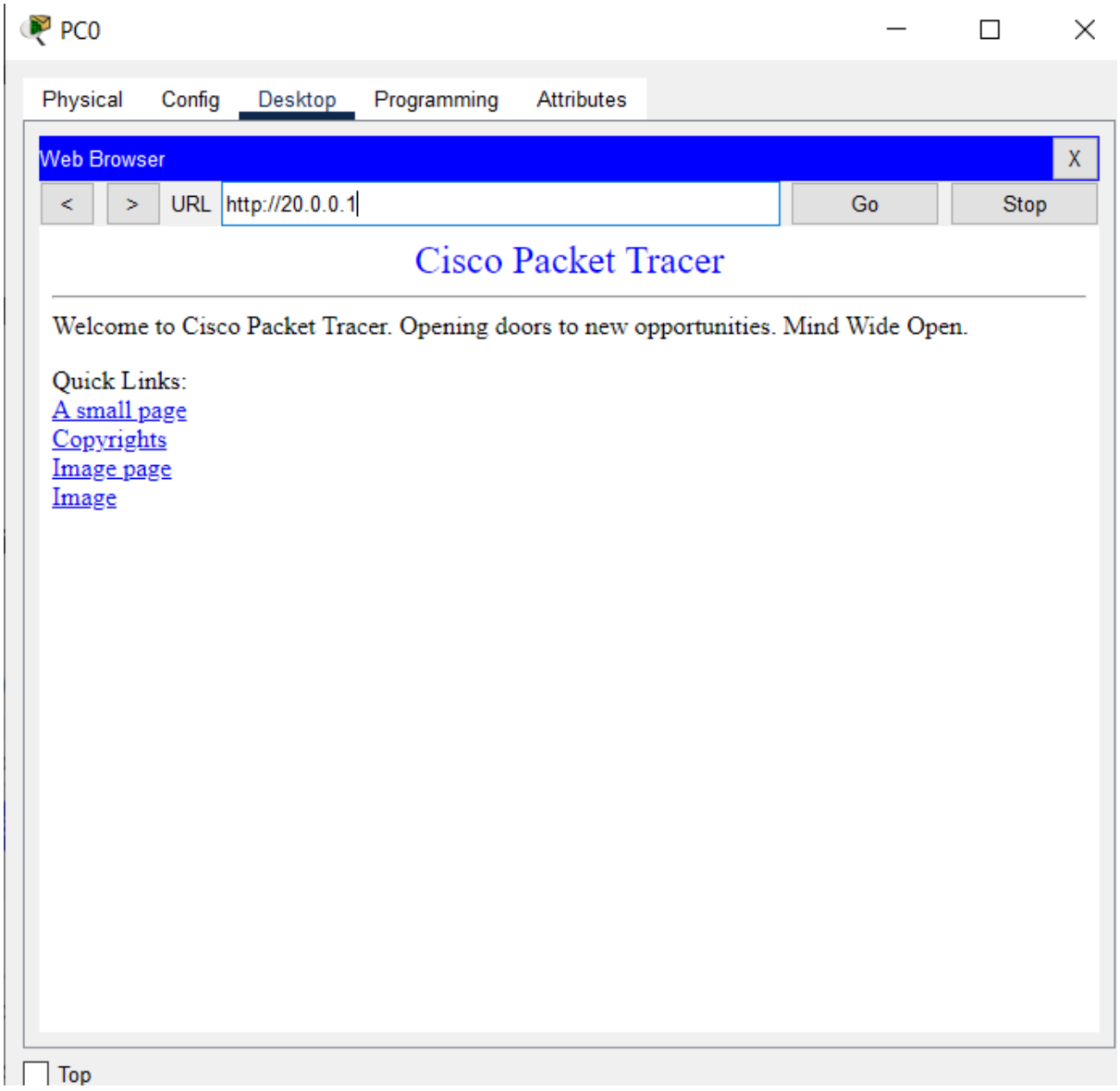
Firewall in Server:



Checking ping command:

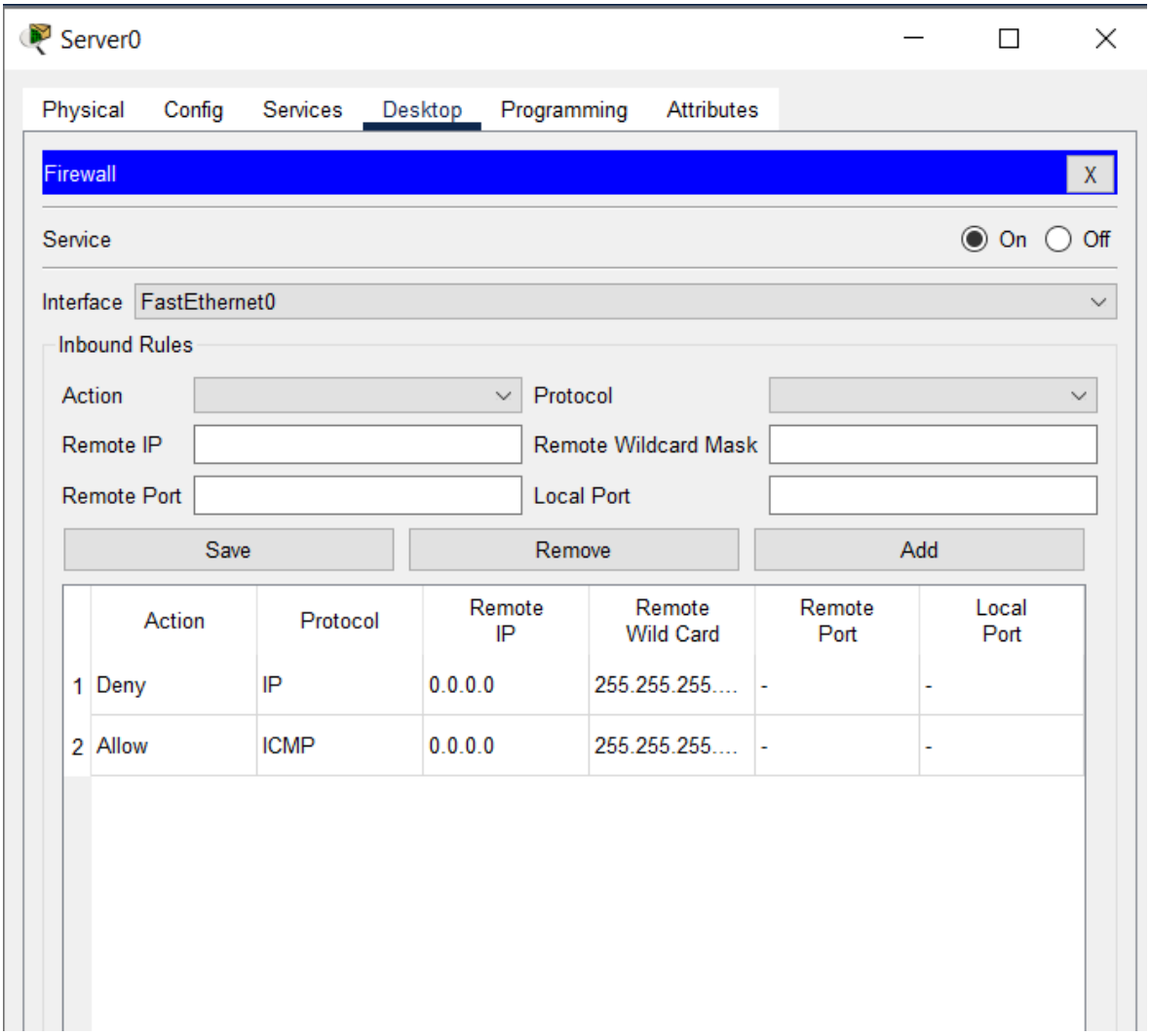


Accessing site:

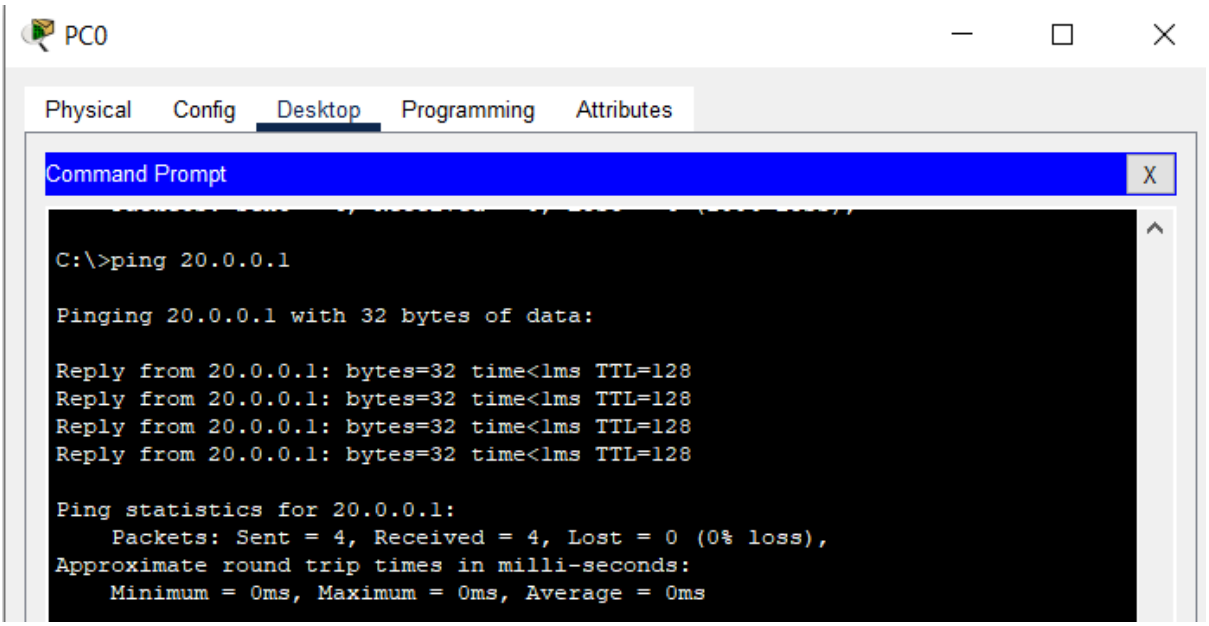


Part b) Deny IP Allow ICMP.

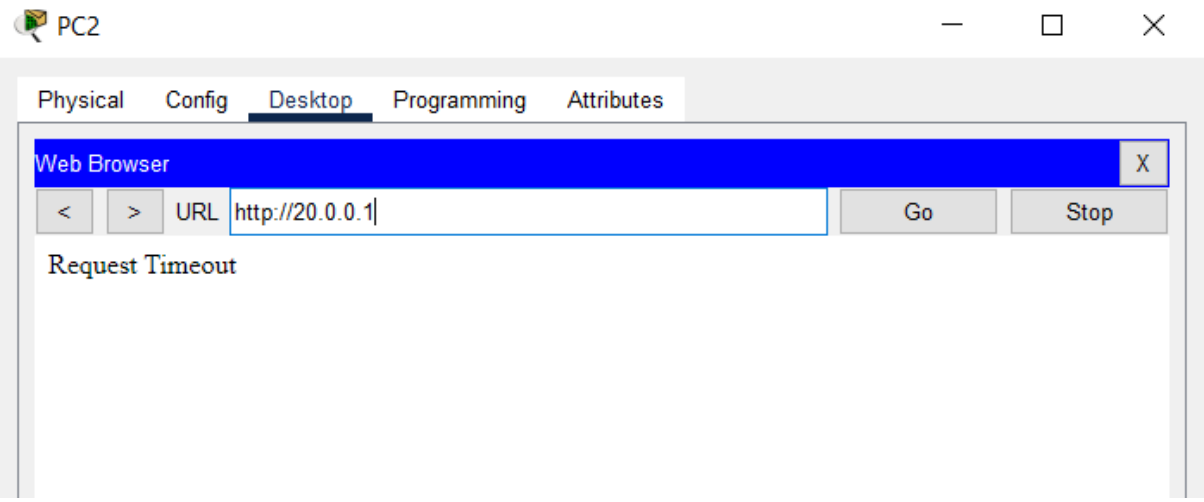
Firewall in Server:



Ping Command:



Accessing Site:



***Conclusion*:**

A we can see that when we allow ICMP and deny IP in the firewall of the server, we can access the server only through ping command and not through the web browser but when we allow IP and deny ICMP we can access the server through web browser but not through the ping command.

Question – 2: Implementing Access Control List.

Aim:

Aim:

The aim of this assignment is to implement the access control list in Cisco Packet Tracer.

***Procedure*:**

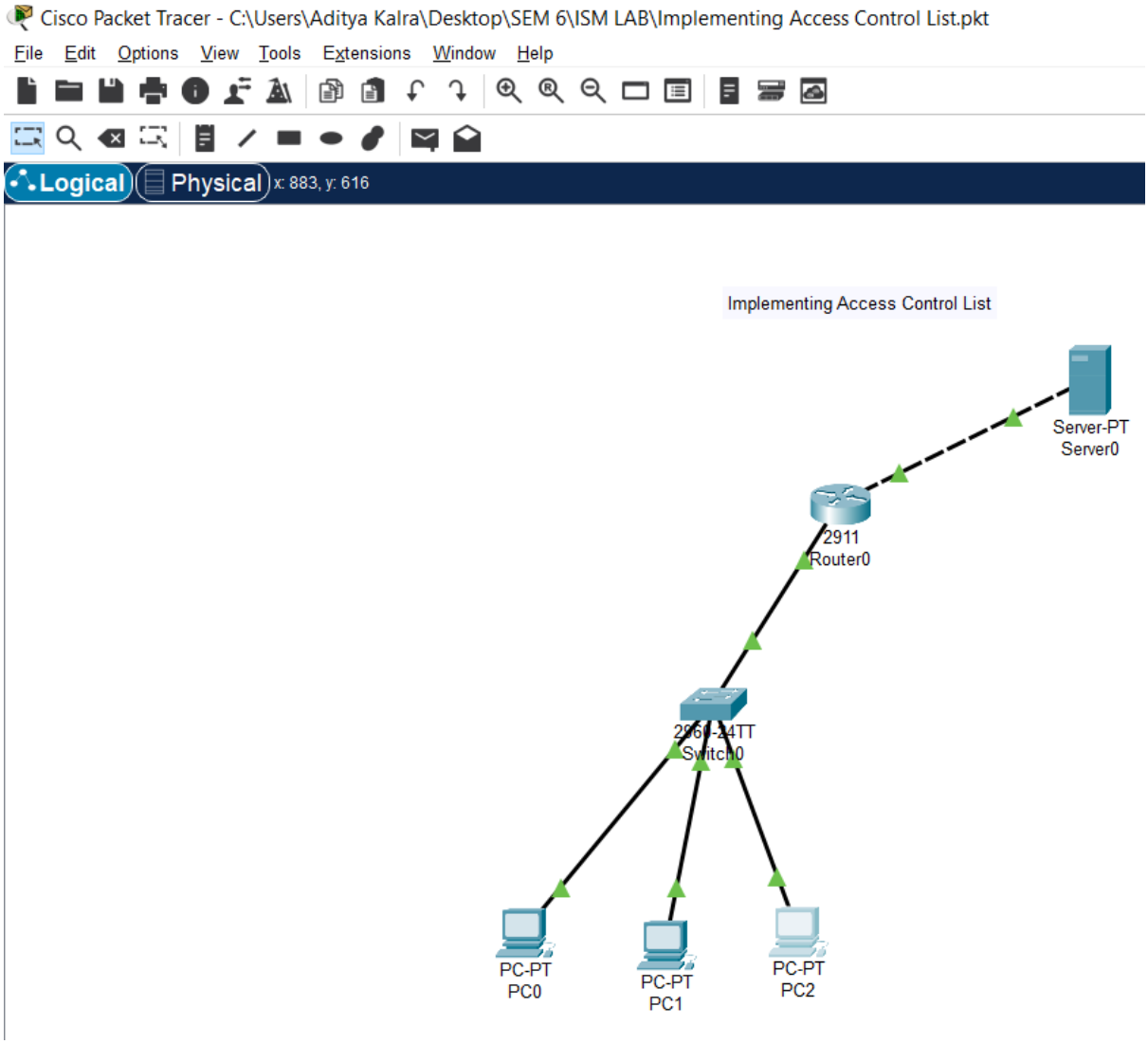
Aditya Kalra 19BCE0390

Procedure:

1. Place the following components:
   - 2911 Router
   - Server
   - 2960 Switch
   - 3 PCs
2. ~~Join~~ Connect all the PCs to switch and switch to router using copper straight through.
3. Connect Router to Server.
4. Configure the CLI and give IP 192.168.10.10 to gigabit ethernet 0/0. & 10.10.10.10 to gigabit ethernet 0/1.
5. Configure the IP addresses of all the PCs and give them IPs from 192.168.10.1 to 3 to PC0, PC1 & PC2 respectively.
6. Now the network is formed and all the PCs can communicate to the server.
7. TO block a PC from communication configure the access control list using CLI in the server and deny host 192.168.10.2.
8. Now we run the ping commands again and find out that PC1 can't run ping command.

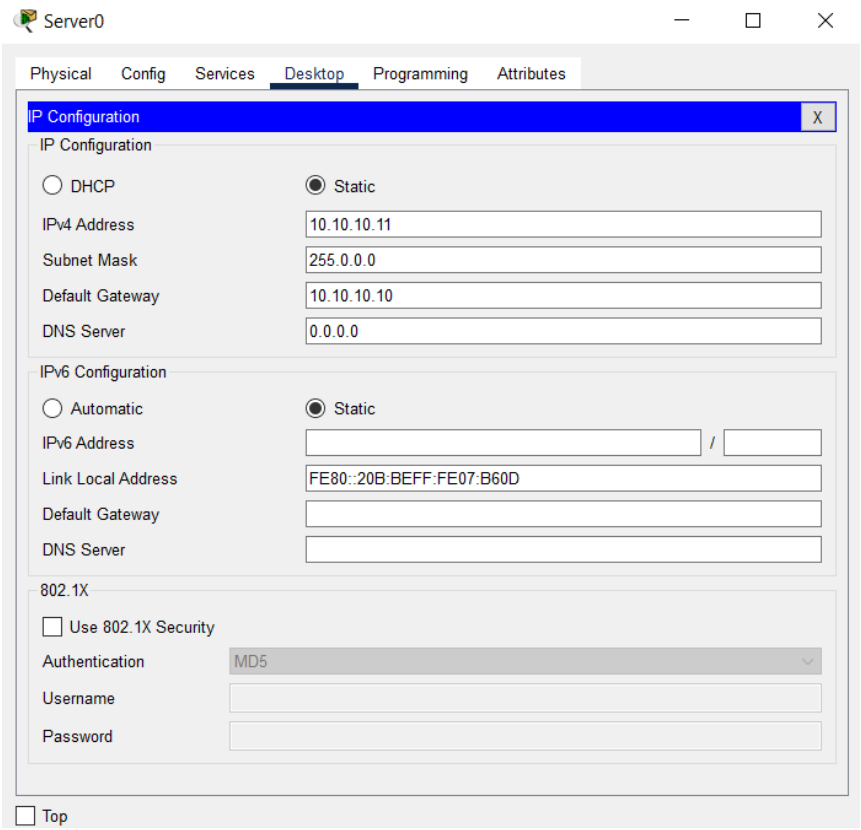
Screenshots:

Network:

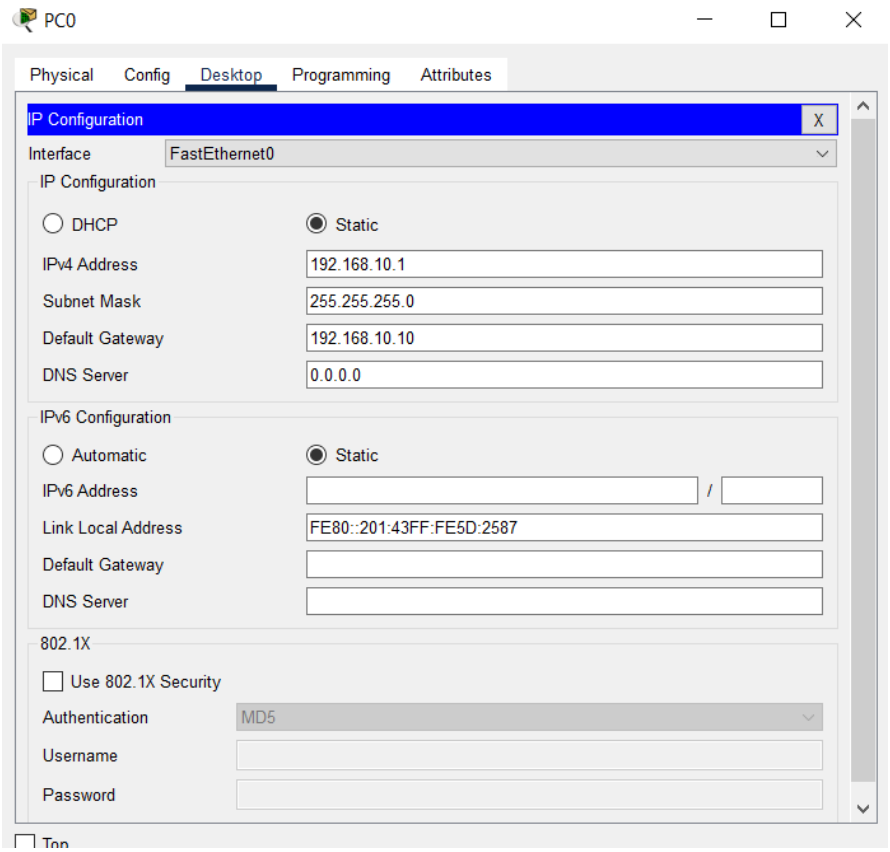


IP Configuration:

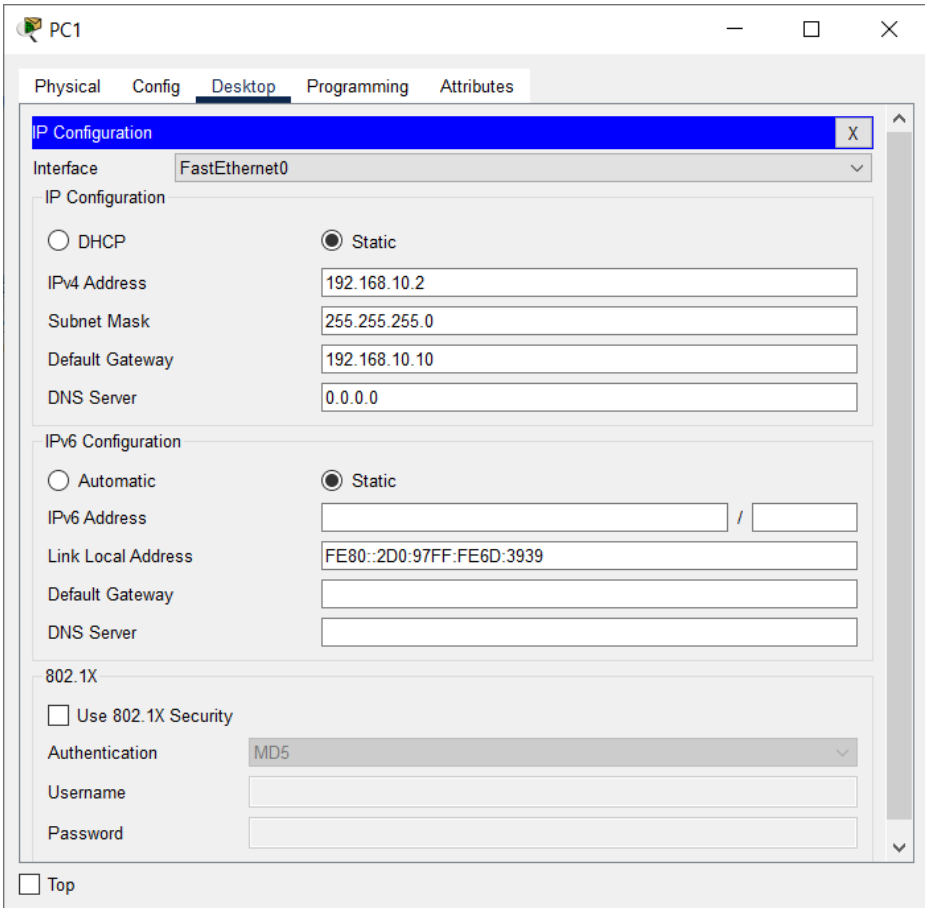
Server:


Server0
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
10.10.10.11
Subnet Mask
255.0.0.0
Default Gateway
10.10.10.10
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::20B:BEFF:FE07:B60D
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

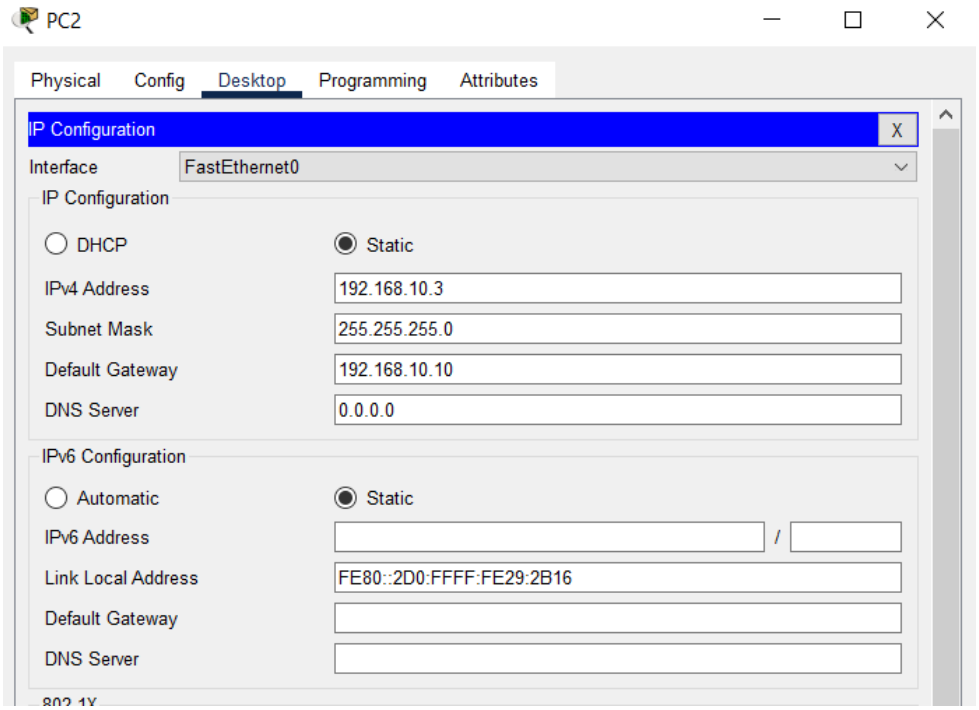
PC0:


PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.10.1
Subnet Mask
255.255.255.0
Default Gateway
192.168.10.10
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::201:43FF:FE5D:2587
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

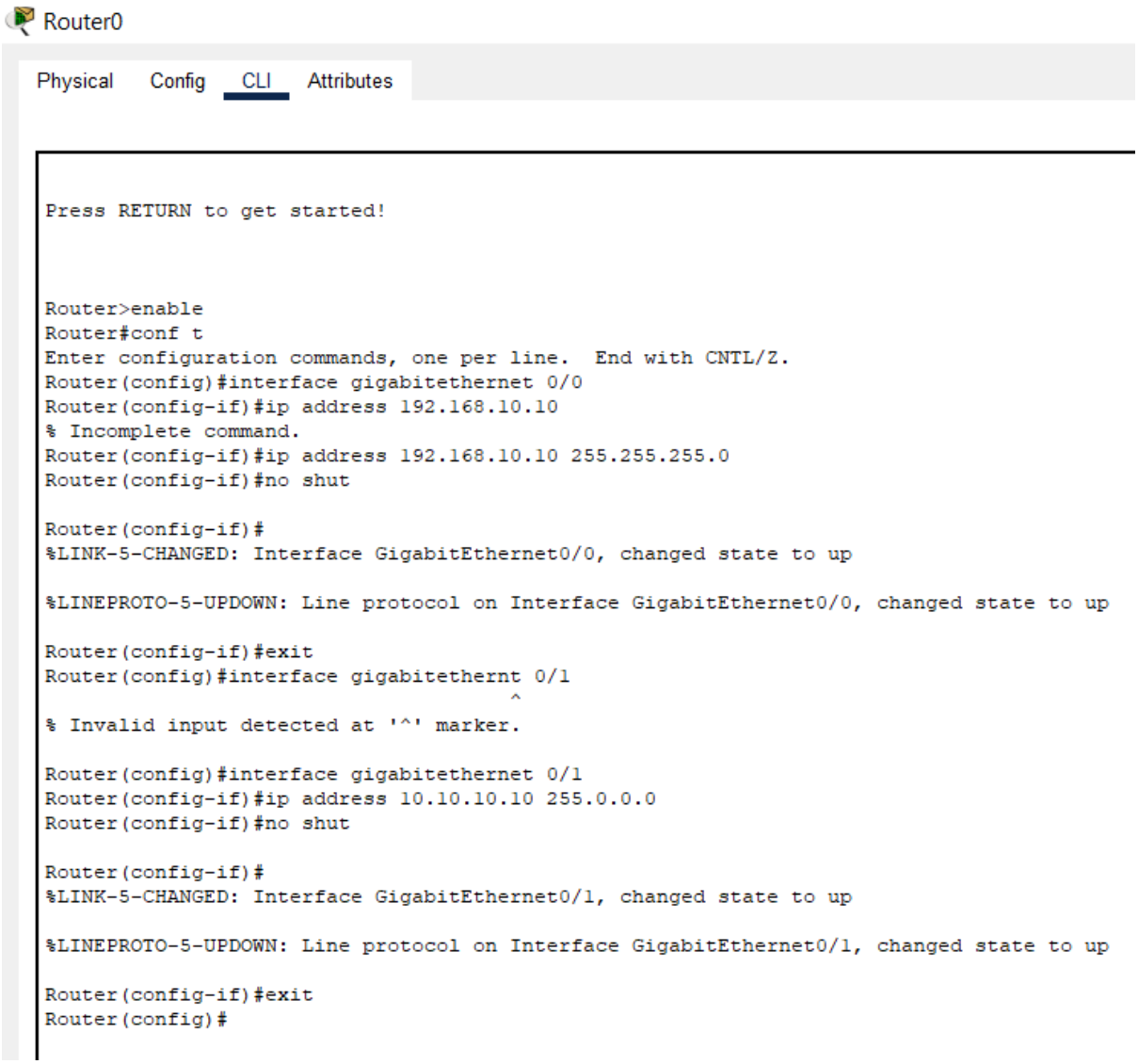
PC1:


PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.10.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.10.10
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::2D0:97FF:FE6D:3939
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

PC2:


PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.10.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.10.10
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::2D0:FFFF:FE29:2B16
Default Gateway
DNS Server

CLI commands:



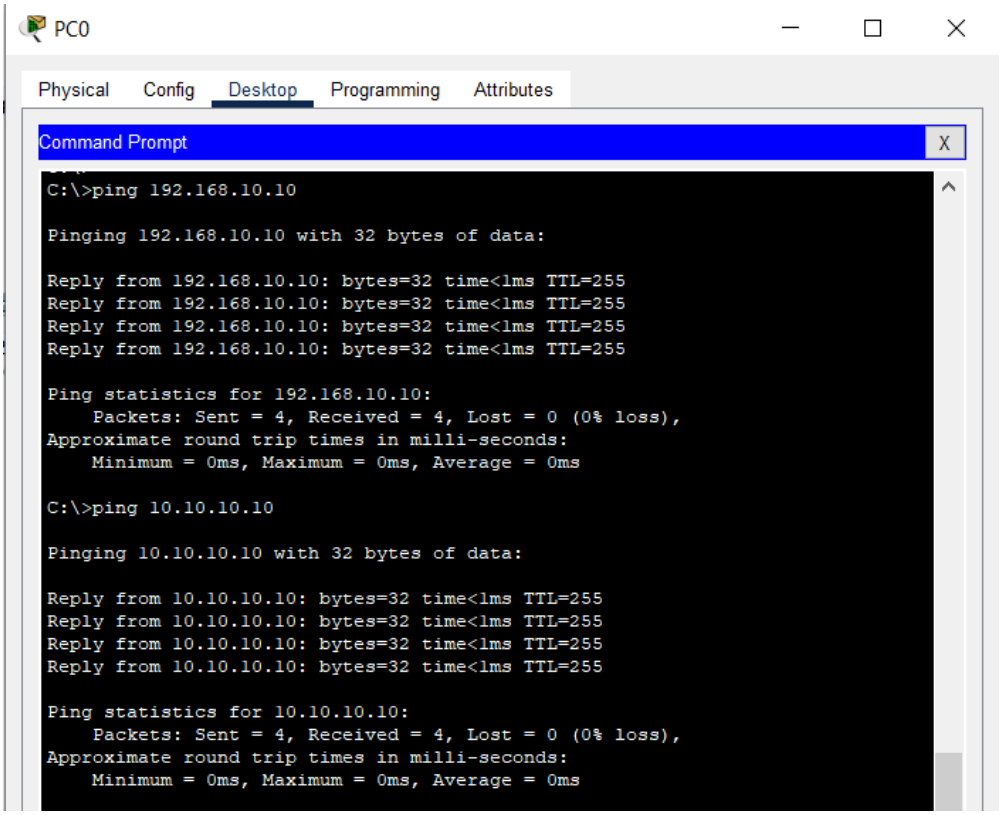
Router0

Physical Config CLI Attributes

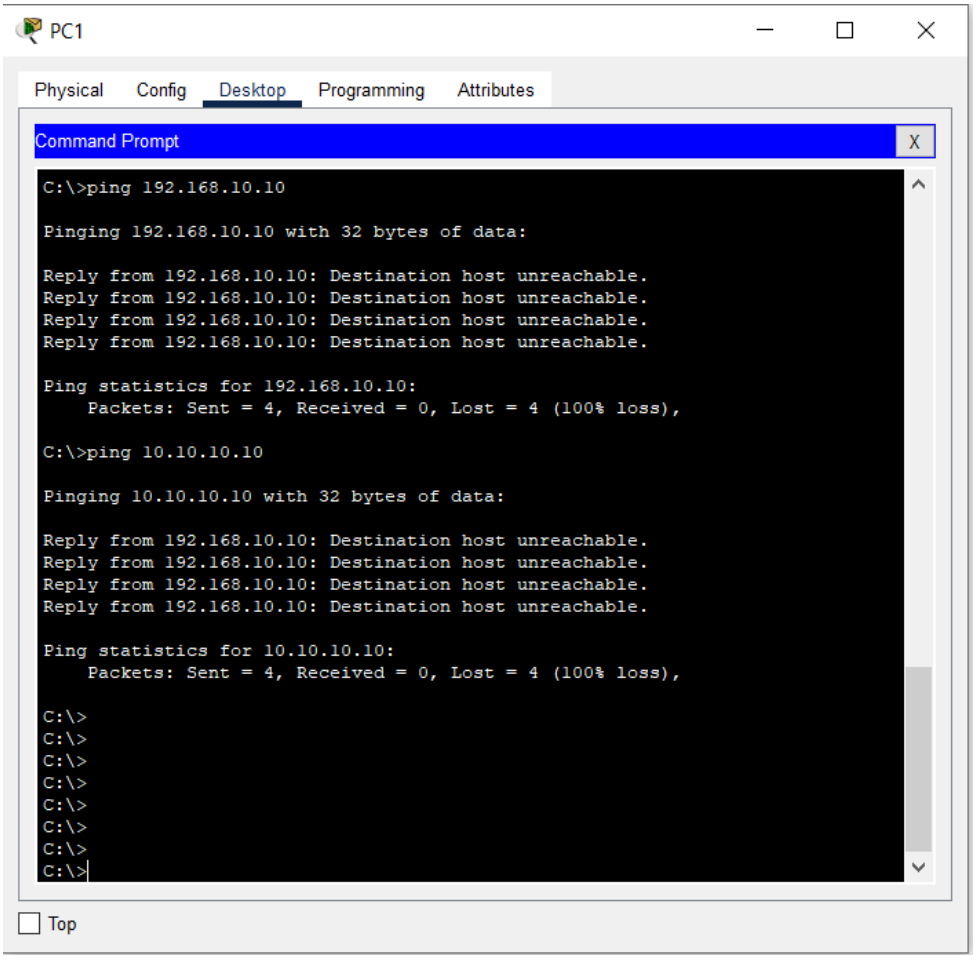
```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list standard 11
Router(config-std-nacl)#deny host 192.168.10.2
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show access-lists
Standard IP access list 11
    10 deny host 192.168.10.2
    20 permit any

Router#enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gigabitethernet 0/0
Router(config-if)#ip access-group 11 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show access-lists
Standard IP access list 11
    10 deny host 192.168.10.2
    20 permit any

Router#
```

Ping commands in all PCs:

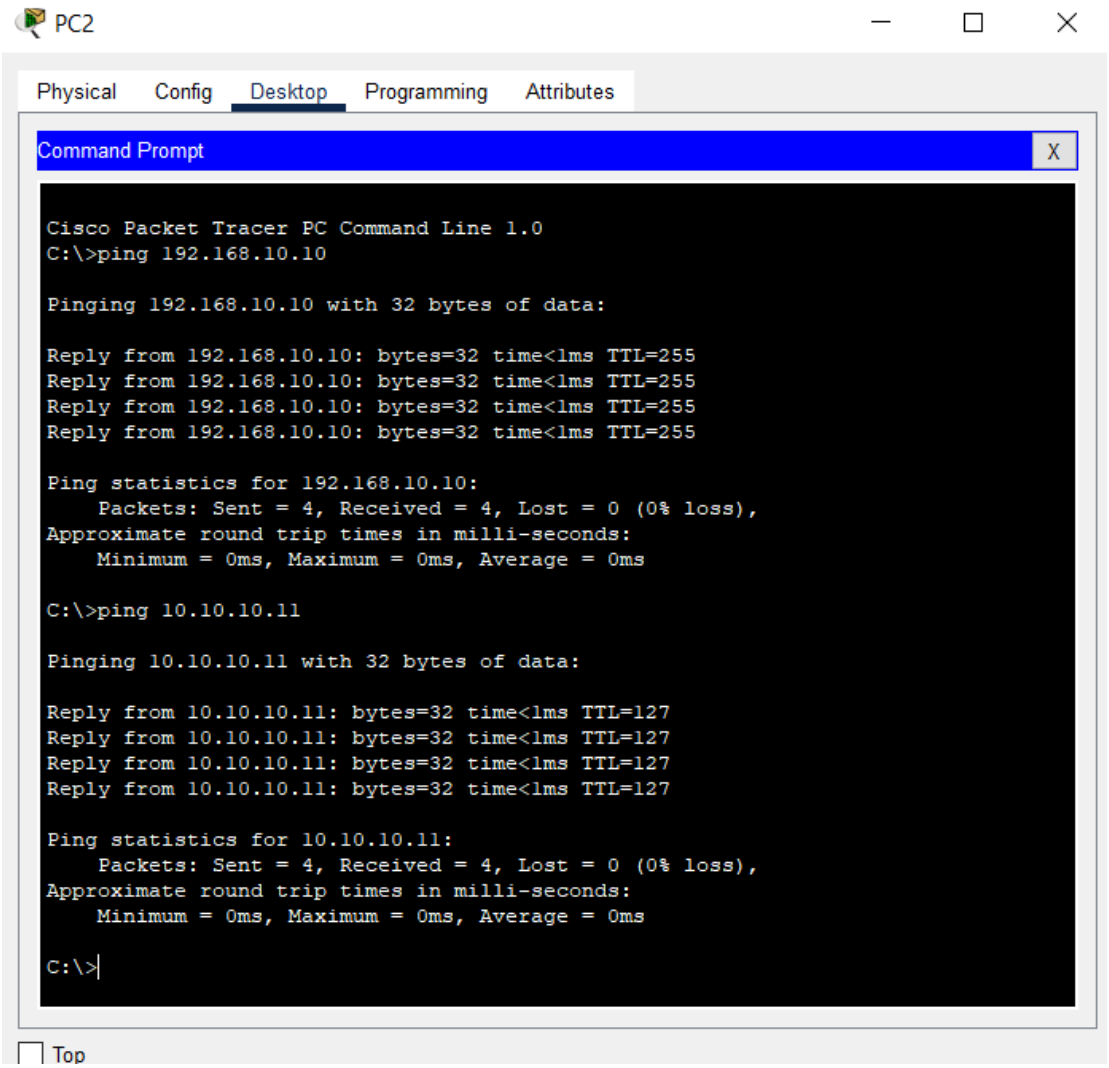
PC0:


PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
C:\>ping 192.168.10.10
Pinging 192.168.10.10 with 32 bytes of data:
Reply from 192.168.10.10: bytes=32 time<1ms TTL=255
Reply from 192.168.10.10: bytes=32 time<1ms TTL=255
Reply from 192.168.10.10: bytes=32 time<1ms TTL=255
Reply from 192.168.10.10: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.10.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 10.10.10.10
Pinging 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time<1ms TTL=255
Reply from 10.10.10.10: bytes=32 time<1ms TTL=255
Reply from 10.10.10.10: bytes=32 time<1ms TTL=255
Reply from 10.10.10.10: bytes=32 time<1ms TTL=255
Ping statistics for 10.10.10.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC1:


PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
C:\>ping 192.168.10.10
Pinging 192.168.10.10 with 32 bytes of data:
Reply from 192.168.10.10: Destination host unreachable.
Reply from 192.168.10.10: Destination host unreachable.
Reply from 192.168.10.10: Destination host unreachable.
Reply from 192.168.10.10: Destination host unreachable.
Ping statistics for 192.168.10.10:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 10.10.10.10
Pinging 10.10.10.10 with 32 bytes of data:
Reply from 192.168.10.10: Destination host unreachable.
Reply from 192.168.10.10: Destination host unreachable.
Reply from 192.168.10.10: Destination host unreachable.
Reply from 192.168.10.10: Destination host unreachable.
Ping statistics for 10.10.10.10:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
Top

PC2:



Conclusion:

As we can see that we can’t reach the server from PC1, which indicates that the access control list has been implemented successfully.

LAB ASSIGNMENT – 3

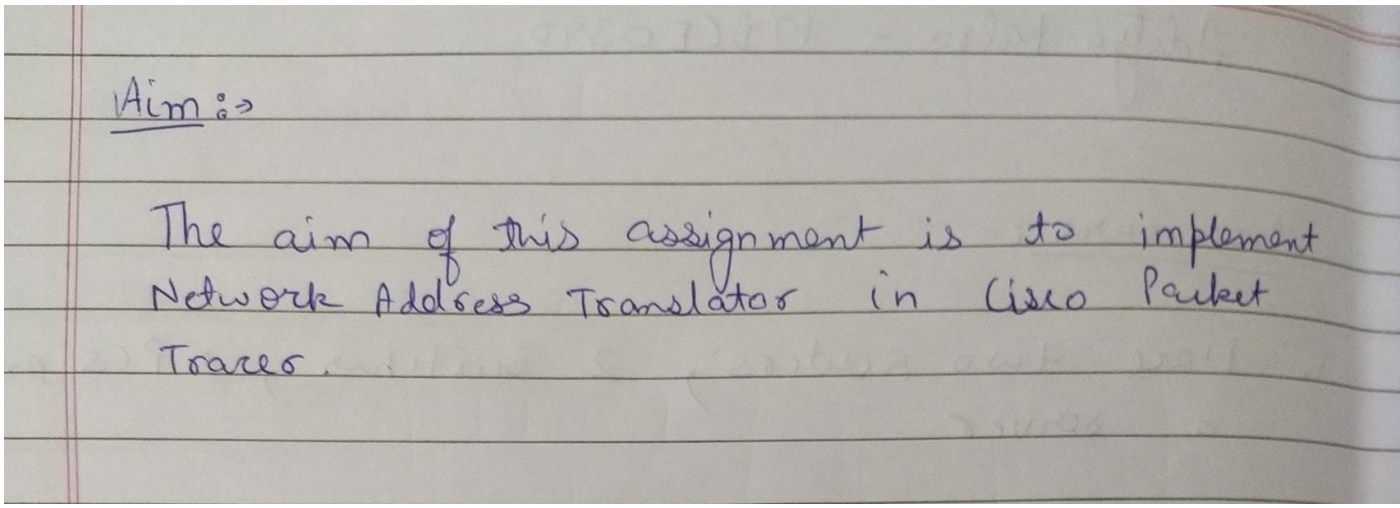
INFORMATION SECURITY MANAGEMENT

NAME: ADITYA KALRA

REG NO: 19BCE0390

Question – 1: Configuring Network Address Translation.

Aim:



Procedure:

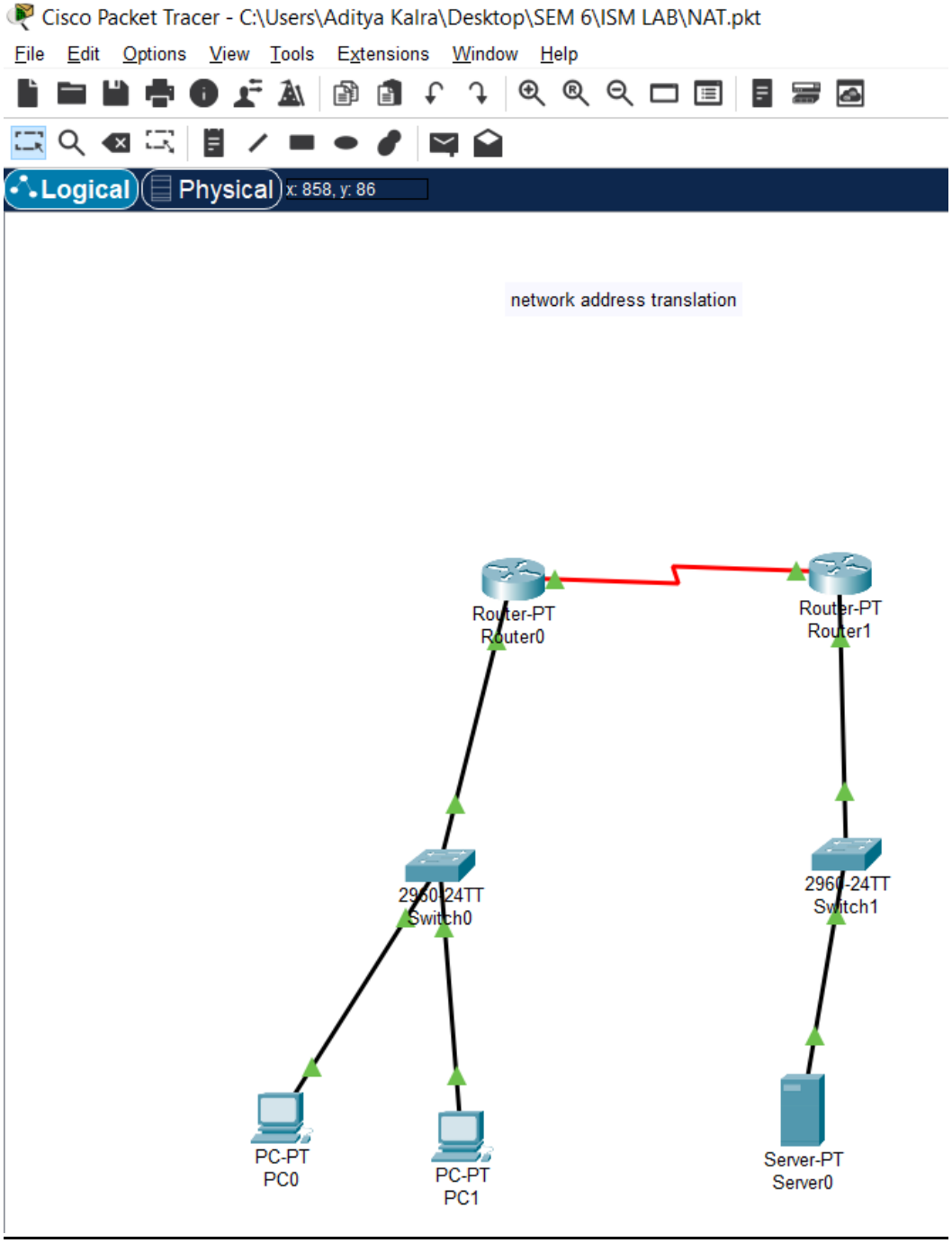
Aditya Kalra – 19BCE0390

Procedure :-

1. Place two Routers, 2 Switches, 2 PCs and a server.
2. Connect The two routers, Router 0 to switch 0, Router 1 to switch 1, Both PCs to switch 0 and the server to switch 1.
3. Give PC0 the IP 192.168.1.1 & PC1 192.168.1.2 & default gateway of 192.168.1.3 to both the PCs
4. Give server the IP address 172.16.10.1
5. Give CLI commands to Router 0 & Router 1. as instructed.
6. The NAT is implemented.
7. Send packets from PC1 & PC0 to server, to verify the connection.

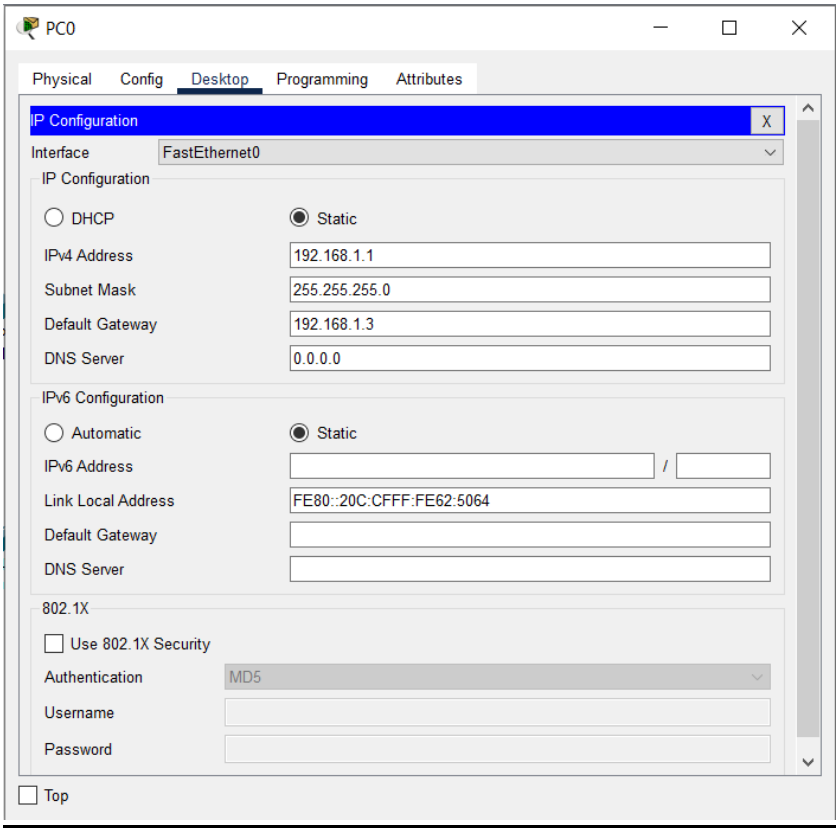
Screenshots:

Network:

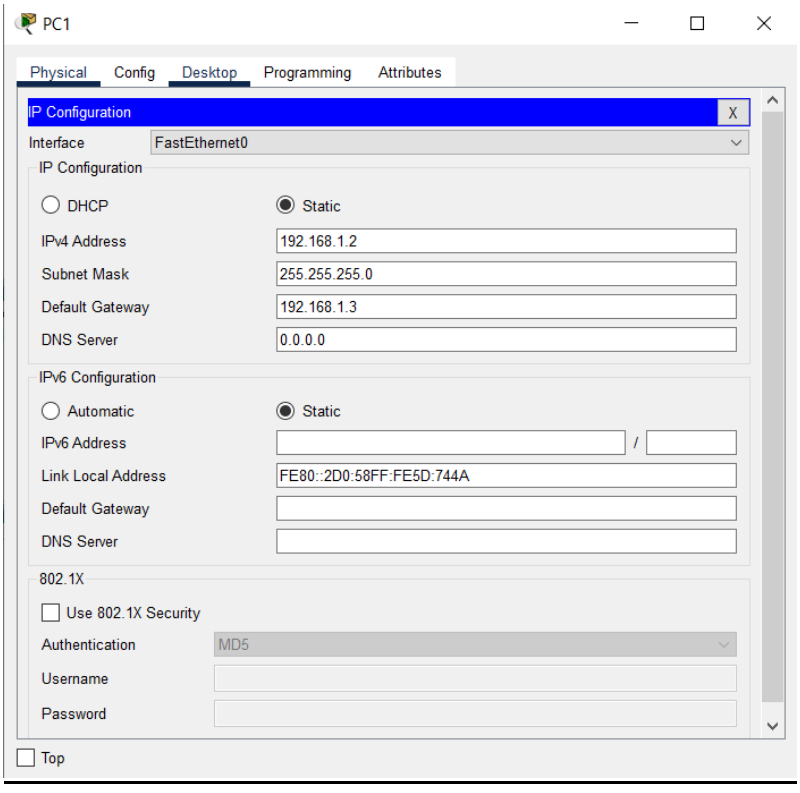


IP configuration:

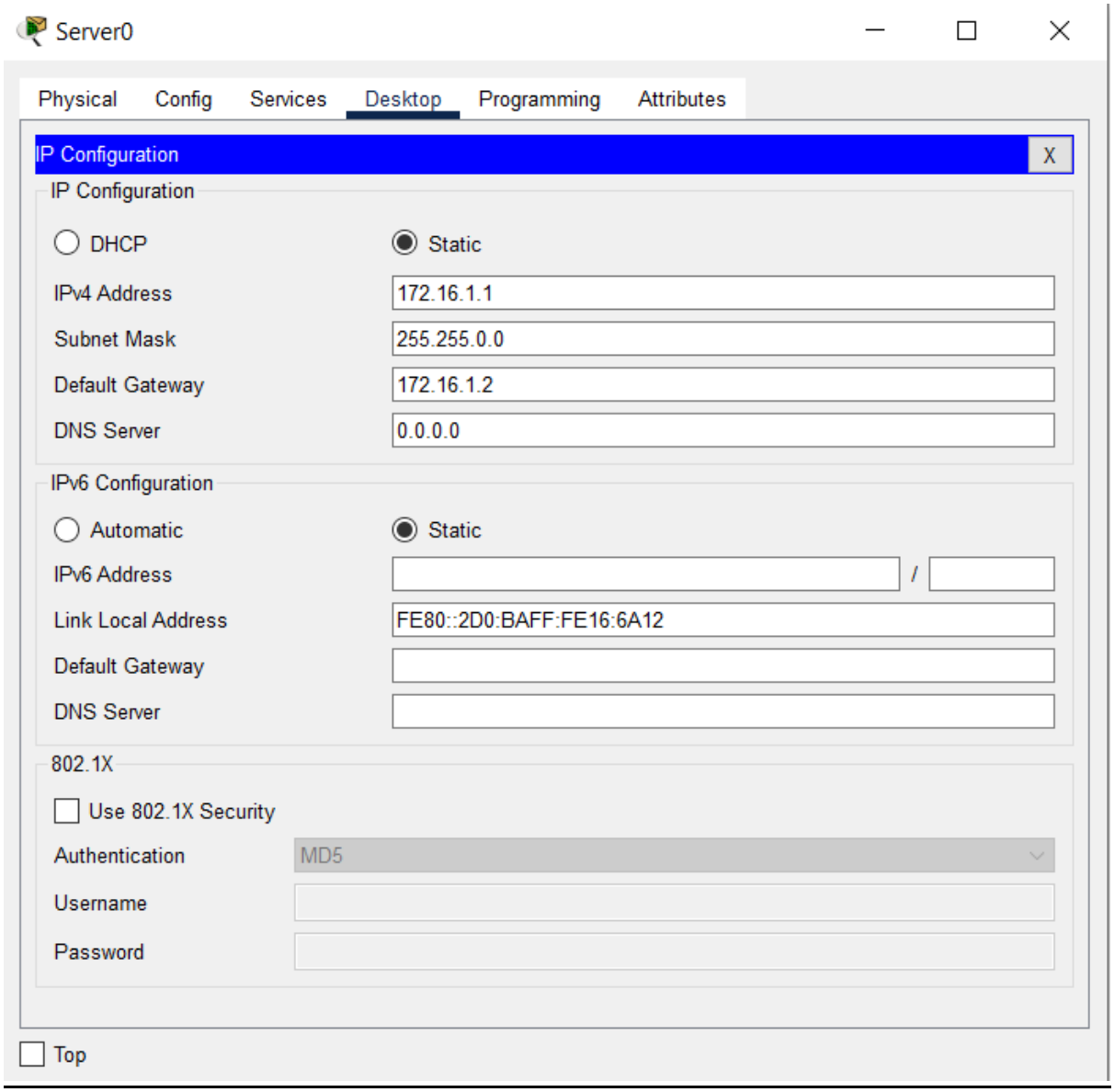
PC0:


PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.1
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.3
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::20C:CFFF:FE62:5064
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

PC1:


PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.3
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::2D0:58FF:FE5D:744A
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

Server 0:



CLI commands:

Router0:

Router0

Physical Config CLI Attributes

```
PI2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up


Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip address 192.168.1.3 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#int s0/0/0
                    ^
% Invalid input detected at '^' marker.

Router(config)#int se
Router(config)#int se2/0
Router(config-if)#ip address 1.0.0.1 255.0.0.0
Router(config-if)#clock rate 64000
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#int se2/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip nat inside source static 192.168.1.1 1.0.0.1
Router(config)#ip route 0.0.0.0 0.0.0.0 se2/0
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip nat tr
Pro  Inside global     Inside local       Outside local      Outside global
---  1.0.0.1           192.168.1.2        ---                ---

Router#
```

Router 1:

Router1

Physical Config CLI Attributes

```
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up


Router>int fa0/0
           ^
% Invalid input detected at '^' marker.

Router>ip address 172.16.1.2 255.255.0.0
          ^
% Invalid input detected at '^' marker.

Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip address 172.16.1.2 255.255.0.0
                    ^
% Invalid input detected at '^' marker.

Router(config)#int fa0/0
Router(config-if)#ip address 172.16.1.2 255.255.0.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#int se2.0
                      ^
% Invalid input detected at '^' marker.

Router(config)#int se2/0
Router(config-if)#ip address 1.0.0.2 255.0.0.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#
```

Sending packets:

Realtime | Simulation

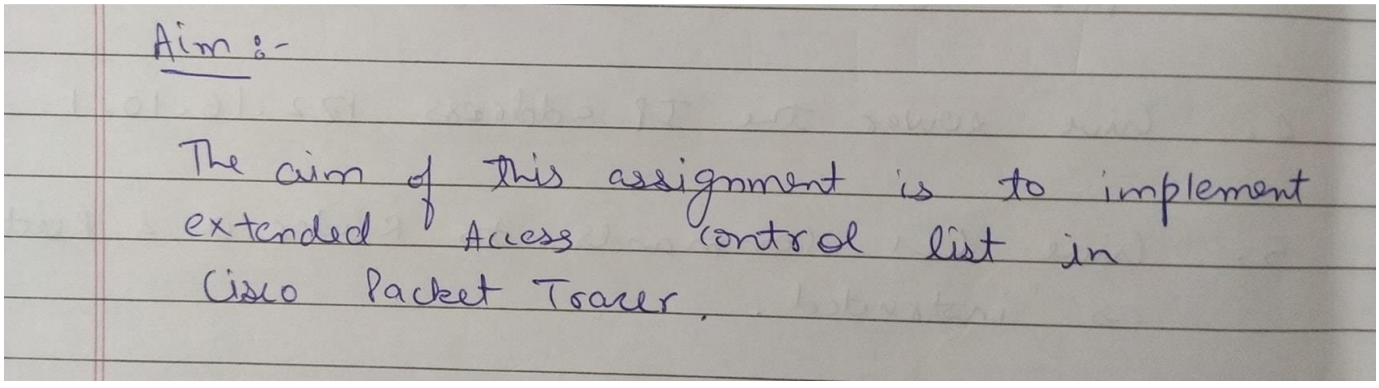
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	Server0	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC0	PC1	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC1	Server0	ICMP		0.000	N	2	(edit)	(delete)

Conclusion:

I was successfully able to implement NAT in Cisco Packet Tracer.

Question – 2: Extended Access Control List.

Aim:



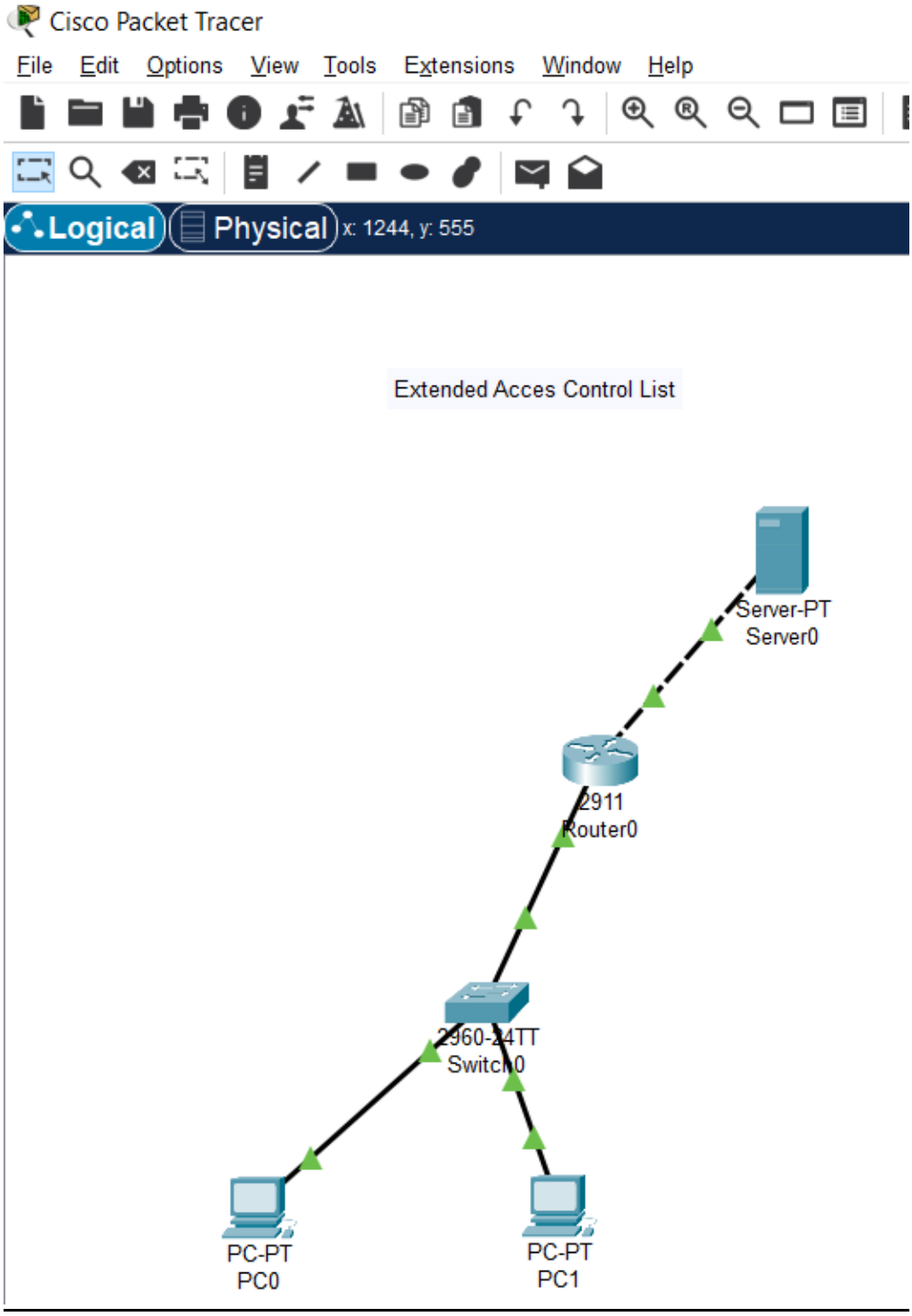
Procedure:

Aditya Kalra - 19BCE0390

1. Place the following components :
   - Server
   - 2911 Router
   - 2960 Switch
   - 2 PCs
2. Connect server to the router, Router to the switch and the two PCs to the switch.
3. Give PC0 the IP 192.168.10.1 & PC1 192.168.10.2 with default gateway 192.168.10.10 to both.
4. Assign the IP address 10.10.10.11 to the server.
5. Configure the CLI command of the router, give IP to ge 0/0 & ge 0/1 and configure the ACL.
6. Send packets from the PCs to the server and run ping command to verify the ACL.

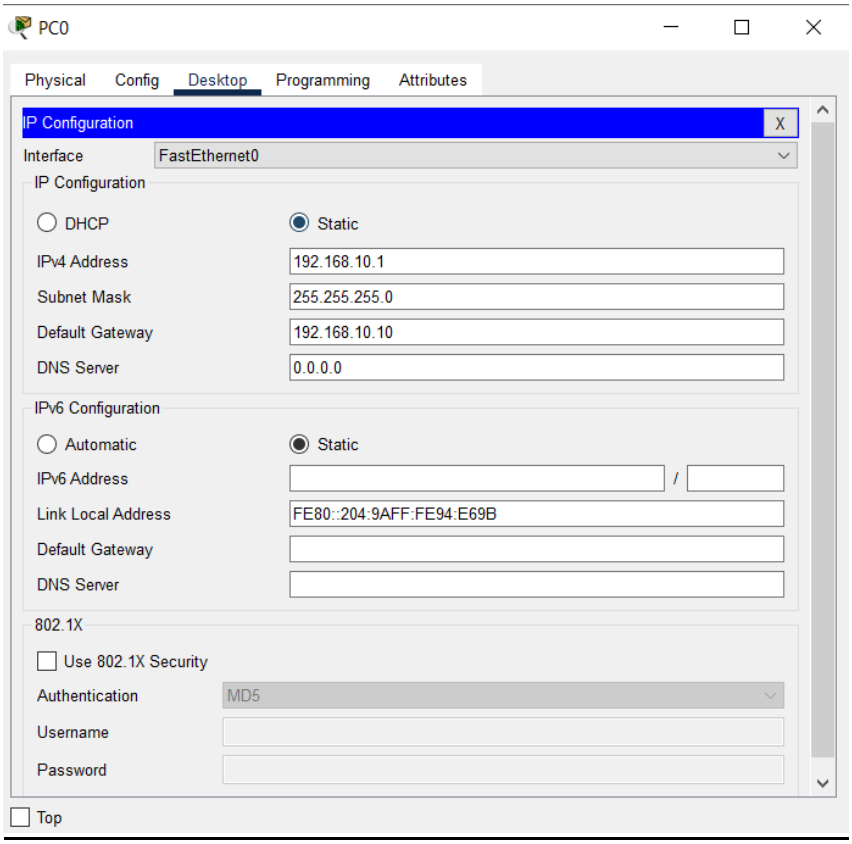
Screenshots:

Network:

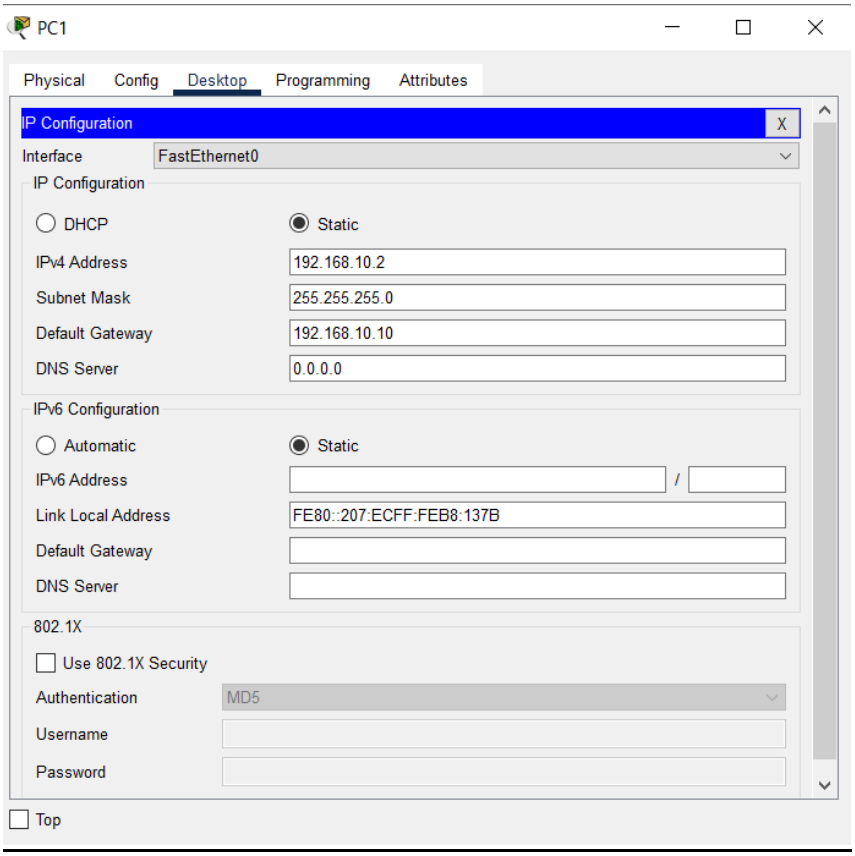


IP configuration:

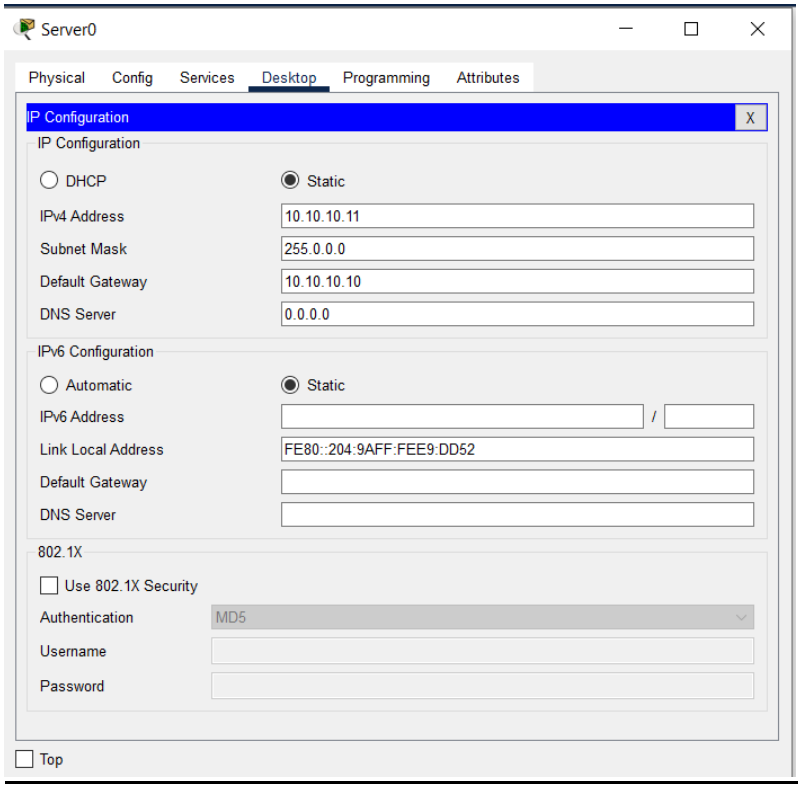
PC0:


PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.10.1
Subnet Mask
255.255.255.0
Default Gateway
192.168.10.10
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::204:9AFF:FE94:E69B
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

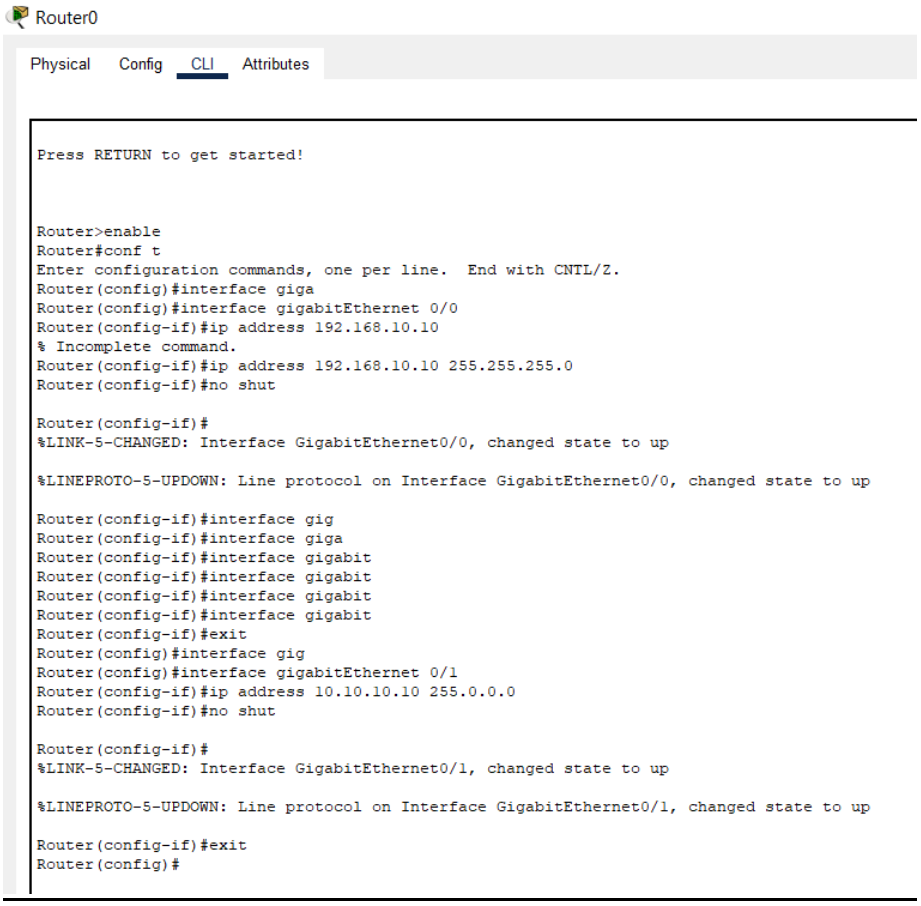
PC1:


PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.10.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.10.10
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::207:ECFF:FEB8:137B
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

Server:



CLI commands:



Router0

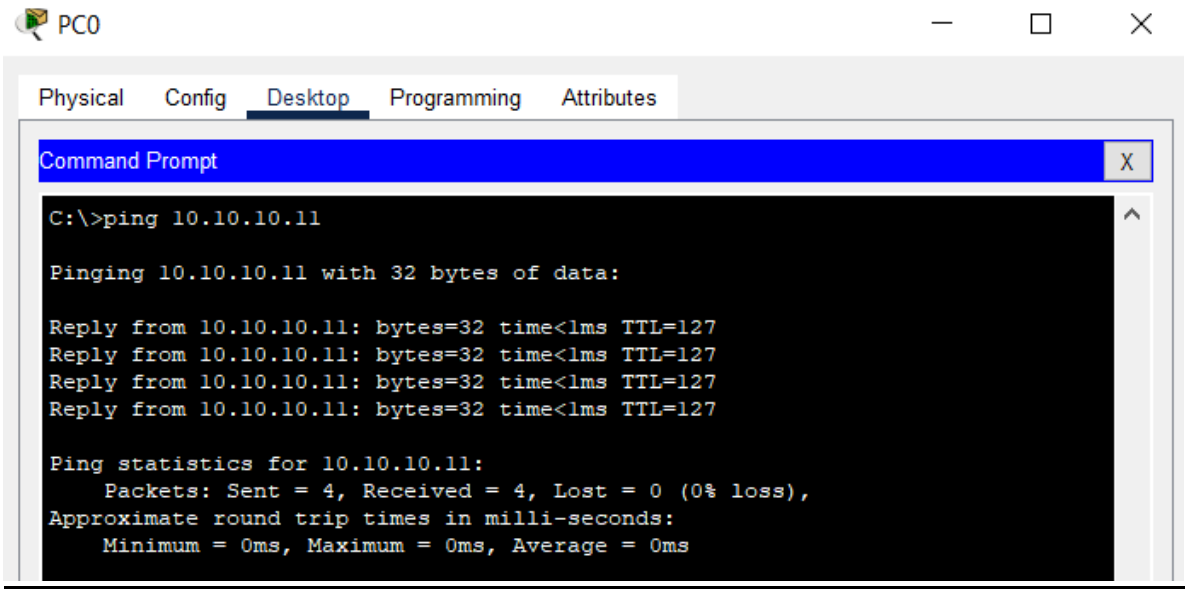
Physical Config CLI Attributes

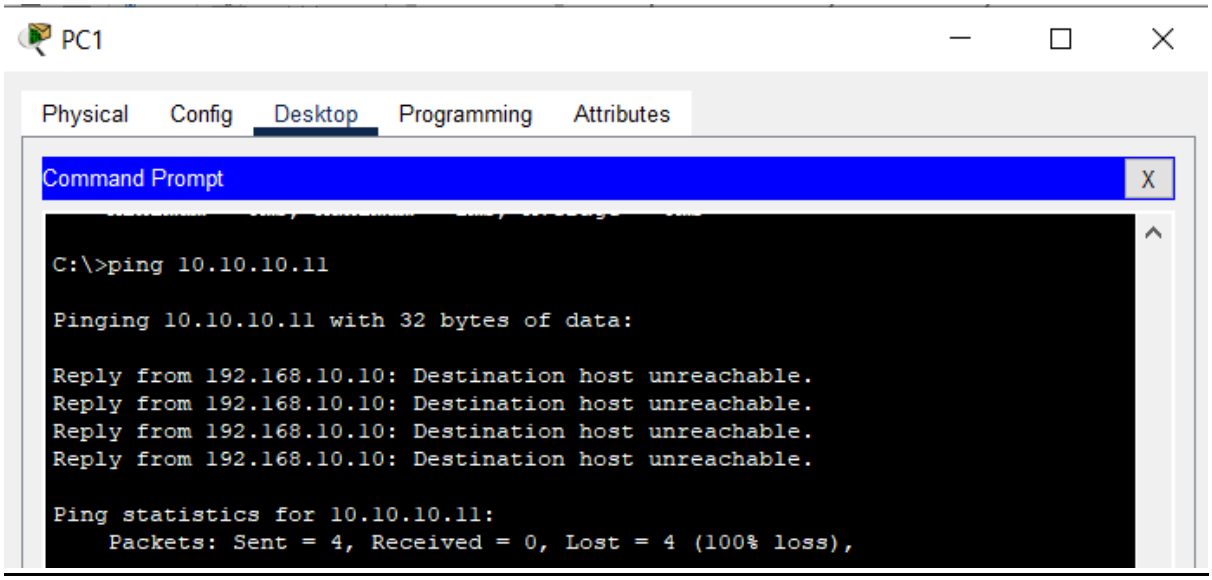
```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list extended 100
Router(config-ext-nacl)#permit icmp 192.168.10.10 host 10.10.10.10
                                                   ^
% Invalid input detected at '^' marker.

Router(config-ext-nacl)#permit icmp 192.168.10.10 255.255.255.0 host 10.10.10.10
Router(config-ext-nacl)#deny icmp host 192.168.10.2 host 10.10.10.10 host-unreachable
Router(config-ext-nacl)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router#show access-lists
Extended IP access list 100
    10 permit icmp 0.0.0.10 255.255.255.0 host 10.10.10.10
    20 deny icmp host 192.168.10.2 host 10.10.10.10 host-unreachable

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list extended 100
Router(config-ext-nacl)#permit icmp 192.168.10.10 255.255.255.0 host 10.10.10.11
Router(config-ext-nacl)#deny icmp host 192.168.10.2 host 10.10.10.11 host-unreachable
Router(config-ext-nacl)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router#show access-lists
Extended IP access list 100
    10 permit icmp 0.0.0.10 255.255.255.0 host 10.10.10.10
    20 deny icmp host 192.168.10.2 host 10.10.10.10 host-unreachable
    30 permit icmp 0.0.0.10 255.255.255.0 host 10.10.10.11
    40 deny icmp host 192.168.10.2 host 10.10.10.11 host-unreachable

Router#
```

Sending packets:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	Server0	ICMP		0.000	N	0	(edit)	(delete)
	Failed	Server0	PC1	ICMP		0.000	N	1	(edit)	(delete)
	Failed	PC1	Server0	ICMP		0.000	N	2	(edit)	(delete)

Ping command:





Conclusion:

As we can see in the above screenshots that the server is reachable from PC0 but not from PC1, so the ACL is successfully implemented.

LAB ASSIGNMENT – 4

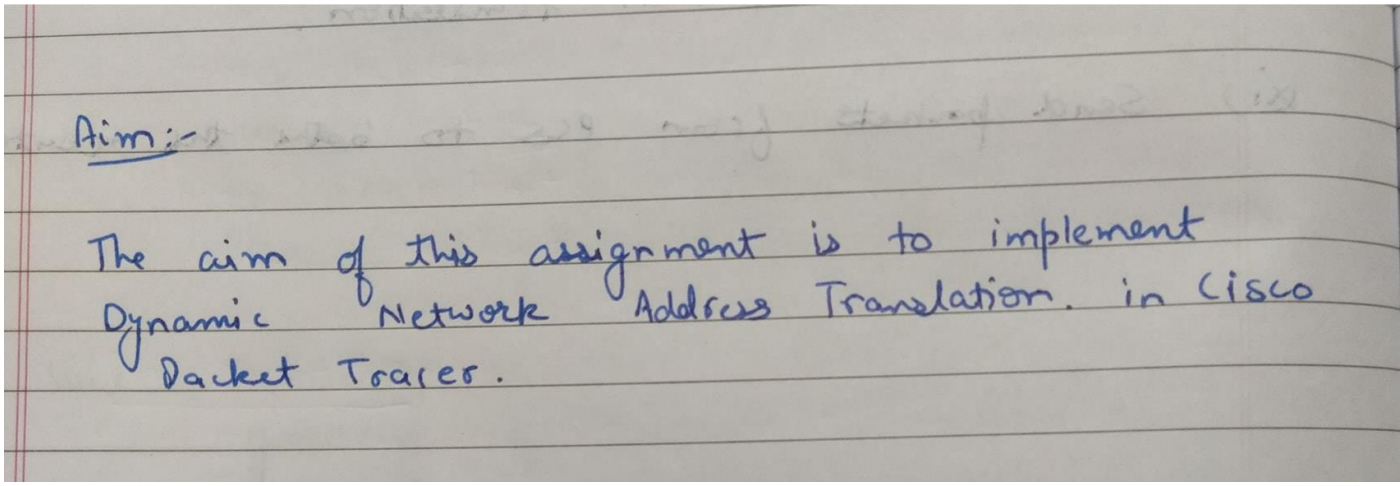
INFORMATION SECURITY MANAGEMENT

NAME: ADITYA KALRA

REG NO: 19BCE0390

Question – 1: Configuring Dynamic Network Address Translation.

Aim:



Procedure:

Aditya Kalra 19BCE0390

Procedure :-

(i) Place the following components :-
- 2 1941 Routers
- 1 2960 switches
- 2 PCs

(ii) Connect PCs to ~~Router~~ switch, switch to router 0 and router 0 to router 1 using appropriate wires.

(iii) Give IP of 192.168.10.10 with default-gateway of 192.168.10.1 to PC0.

(iv) Give IP of 192.168.10.20 with default gateway of 192.168.10.1 to PC1

(v) Configure Router 0 using CLI and add ip 192.168.10.1 to gigabit ethernet 0/0 and IP ~~192.168.~~ 10.10.10.1 to gigabit ethernet 0/1.

(vi) Configure Router 1 using CLI and add IP 10.0.0.2 to gigabit ethernet 0/0.

(vii) Ping to both the routers from PC0.

(viii) Configure Router 0 for Dynamic NAT using CLI command.

(ix) Ping both the routers from PCs.

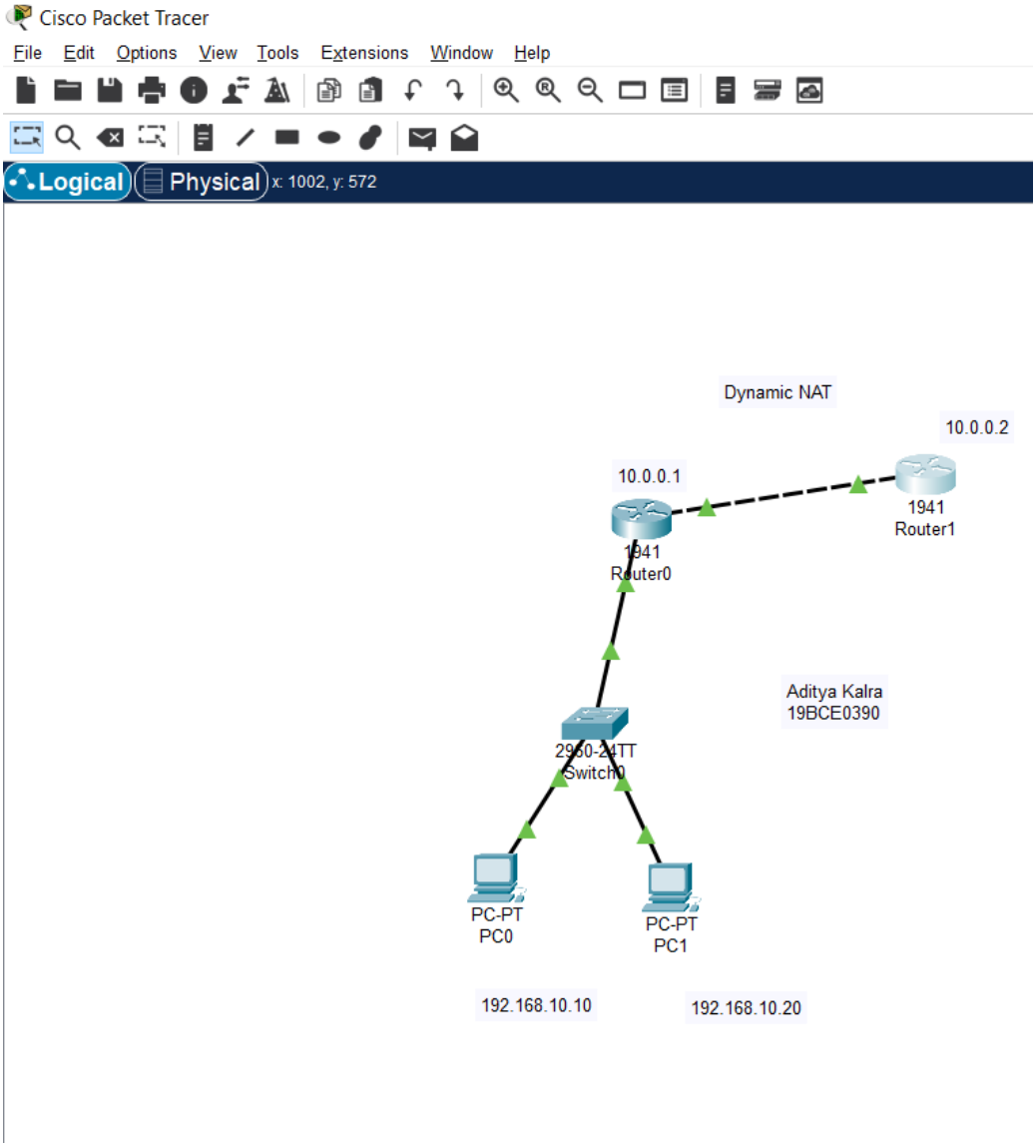
(x) Display the NAT table through the following command :-

show IP NAT translation.

(xi) Send packets from PCs to both the routers.

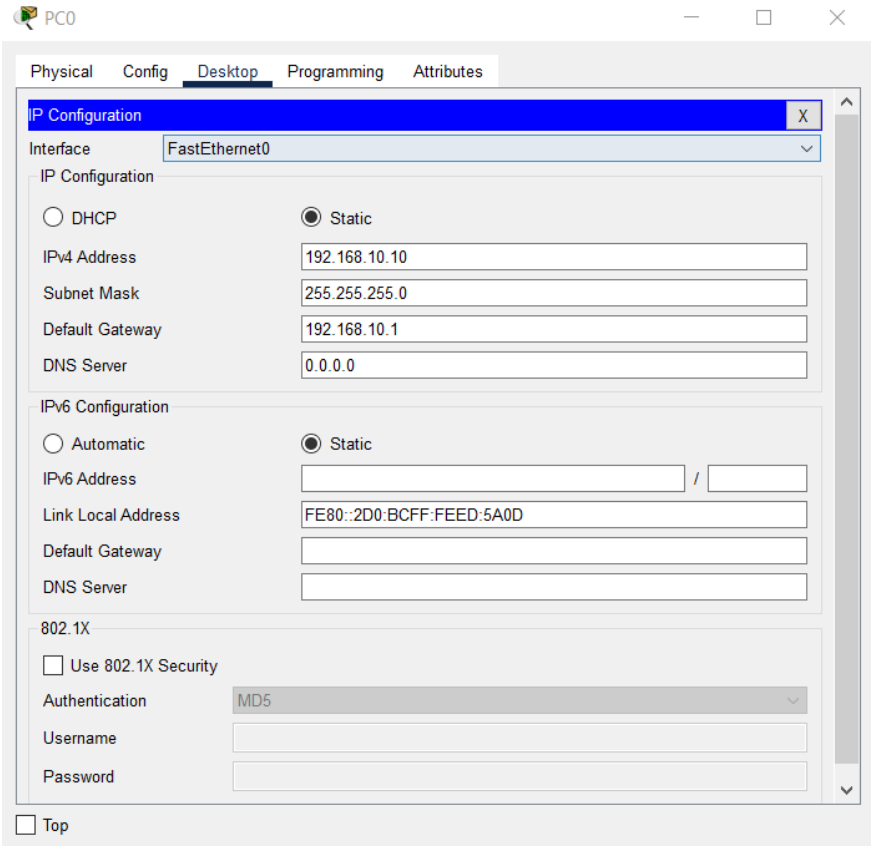
Screenshots:

Network:

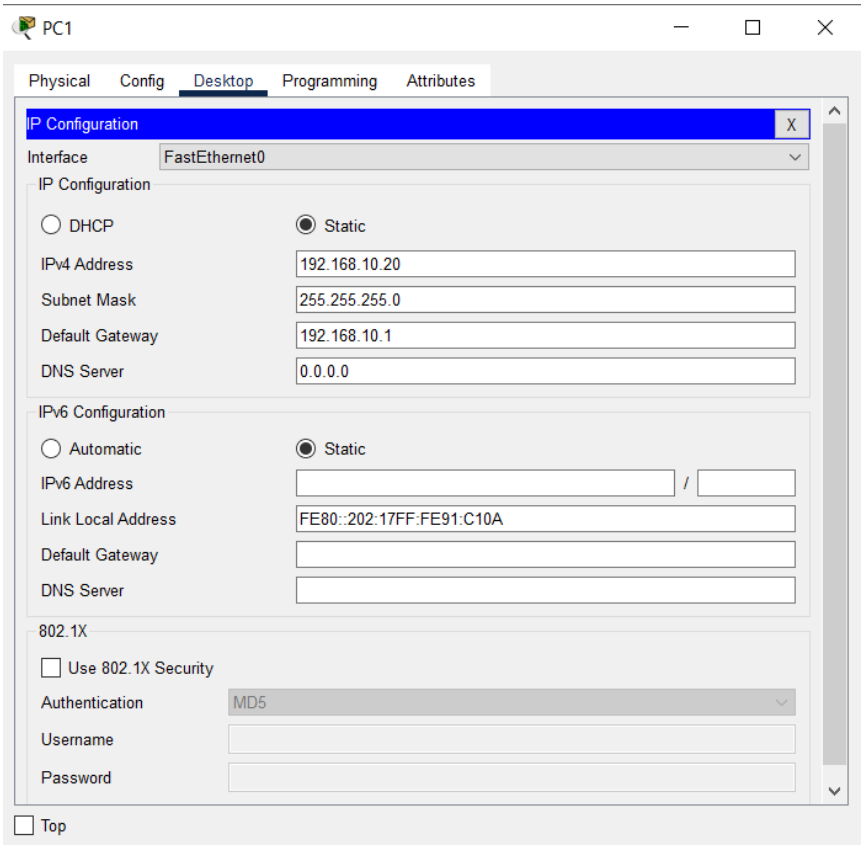


IP Configuration:

PC0:

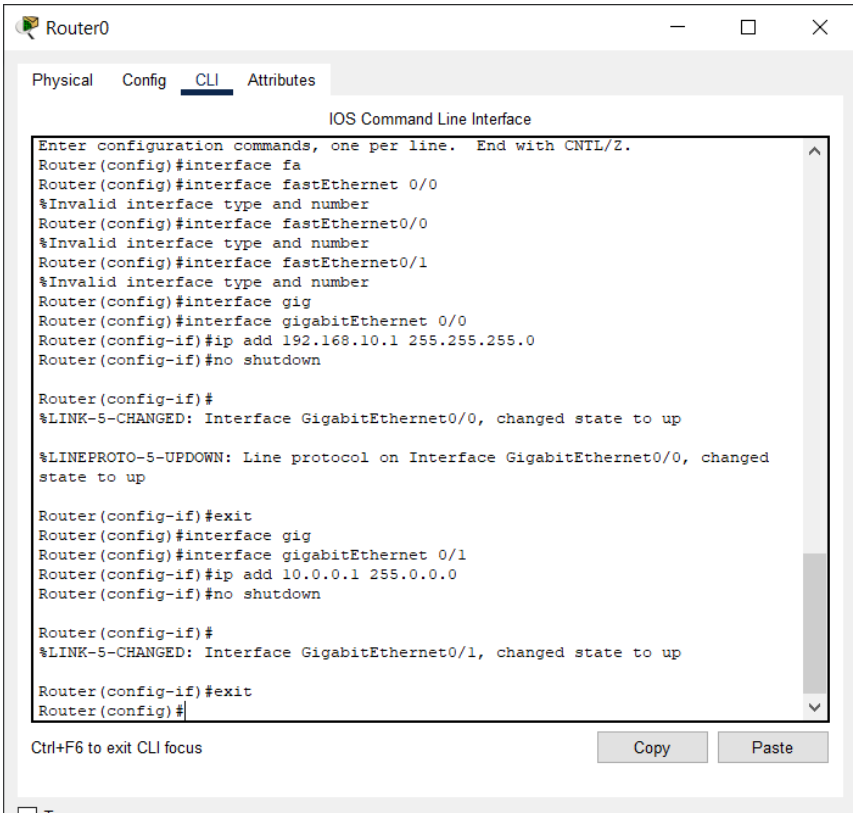

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.10.10
Subnet Mask
255.255.255.0
Default Gateway
192.168.10.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::2D0:BCFF:FEED:5A0D
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

PC1:

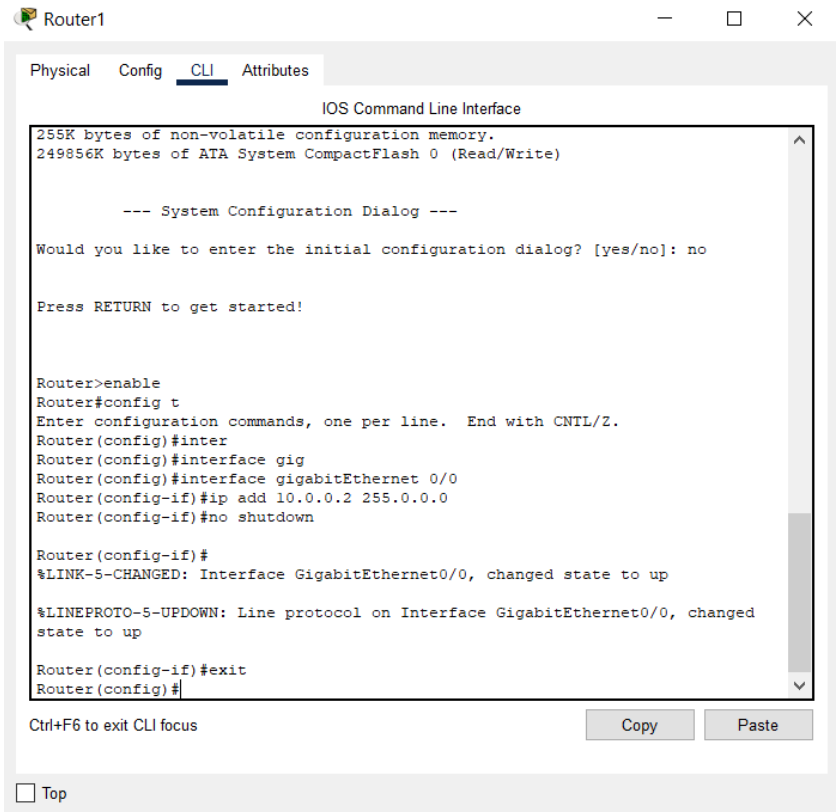

PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.10.20
Subnet Mask
255.255.255.0
Default Gateway
192.168.10.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::202:17FF:FE91:C10A
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

Configuring Router:

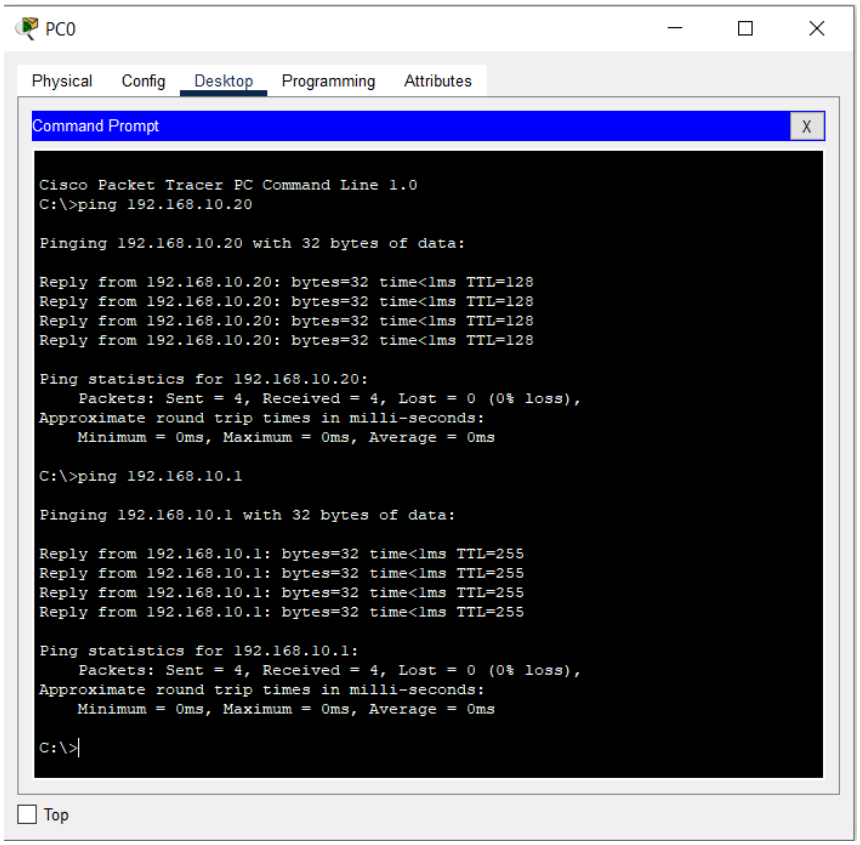
Router0:



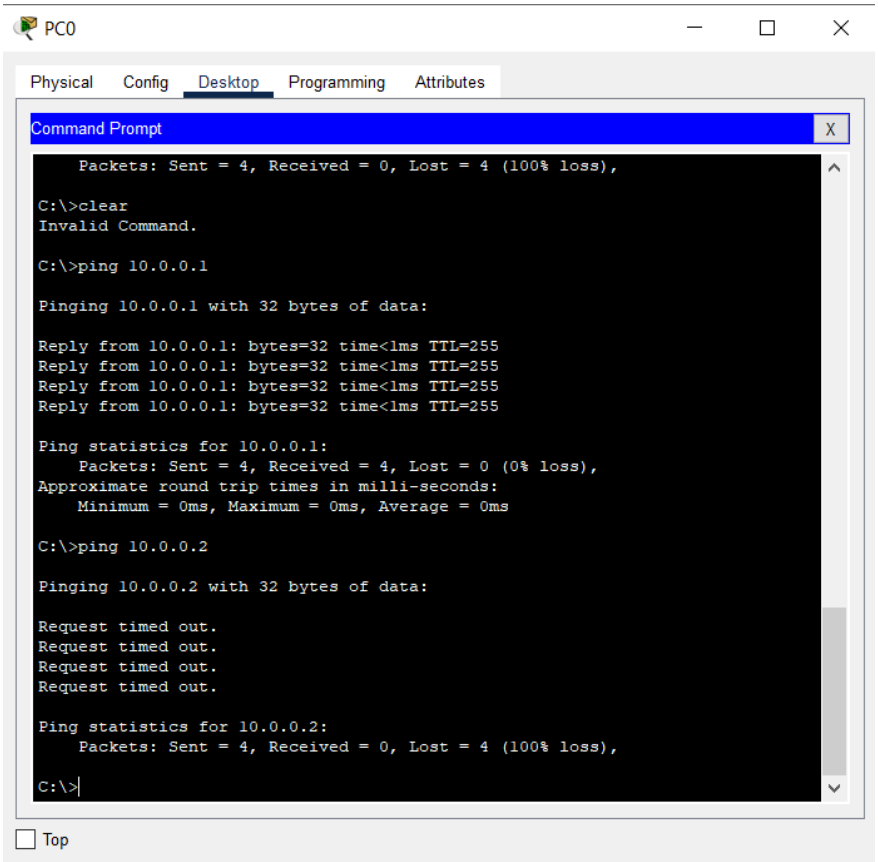
Router1:



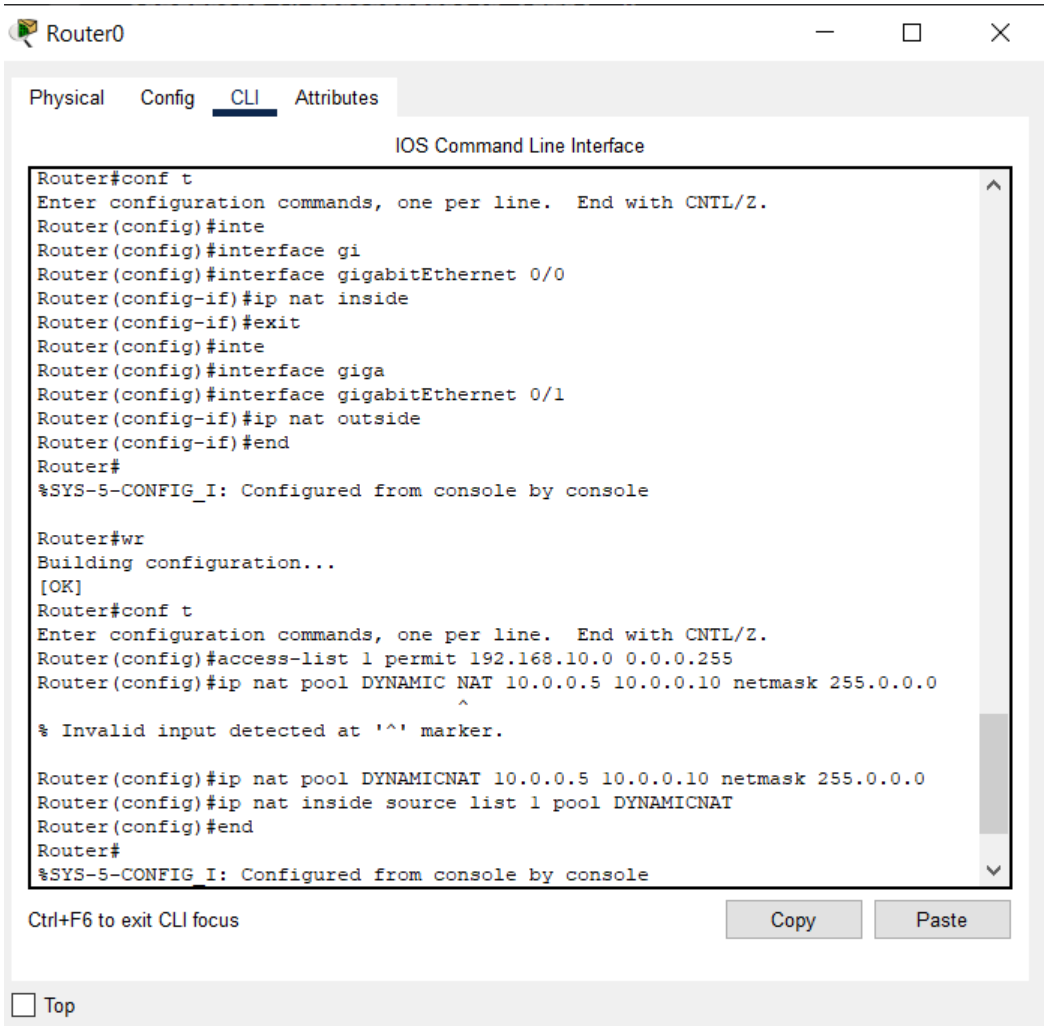
Pinging PC1 and server from PC0:



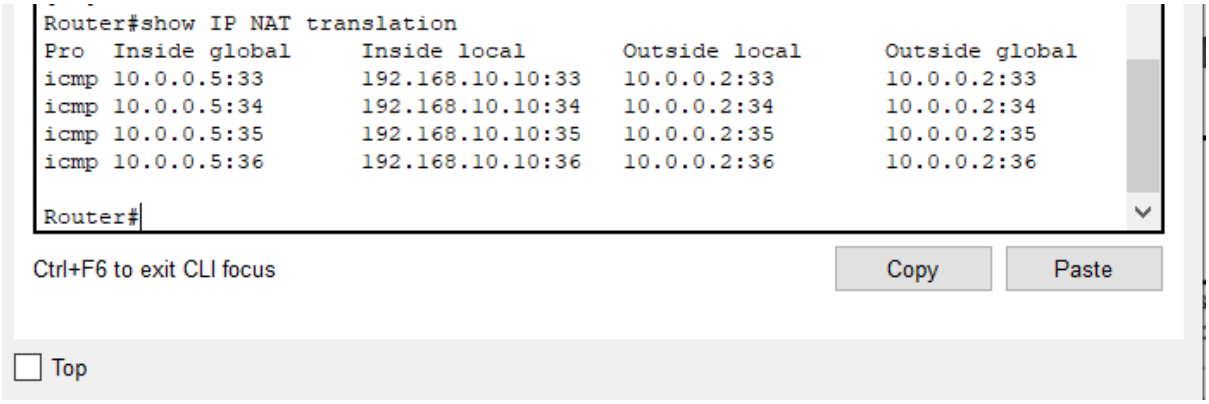
Pinging both the routers from PC0:



Configuring dynamic NAT:



NAT Table:



Sending packets:

Realtime Simulation

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	Router0	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC1	Router0	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC0	Router1	ICMP		0.000	N	2	(edit)	(delete)

Pinging router after NAT configuration:

```
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time<1ms TTL=254
Reply from 10.0.0.2: bytes=32 time<1ms TTL=254
Reply from 10.0.0.2: bytes=32 time<1ms TTL=254
Reply from 10.0.0.2: bytes=32 time<1ms TTL=254

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

C:\>
```

Top

Information Security Management

Digital assignment-5

Name: Aditya Kalra

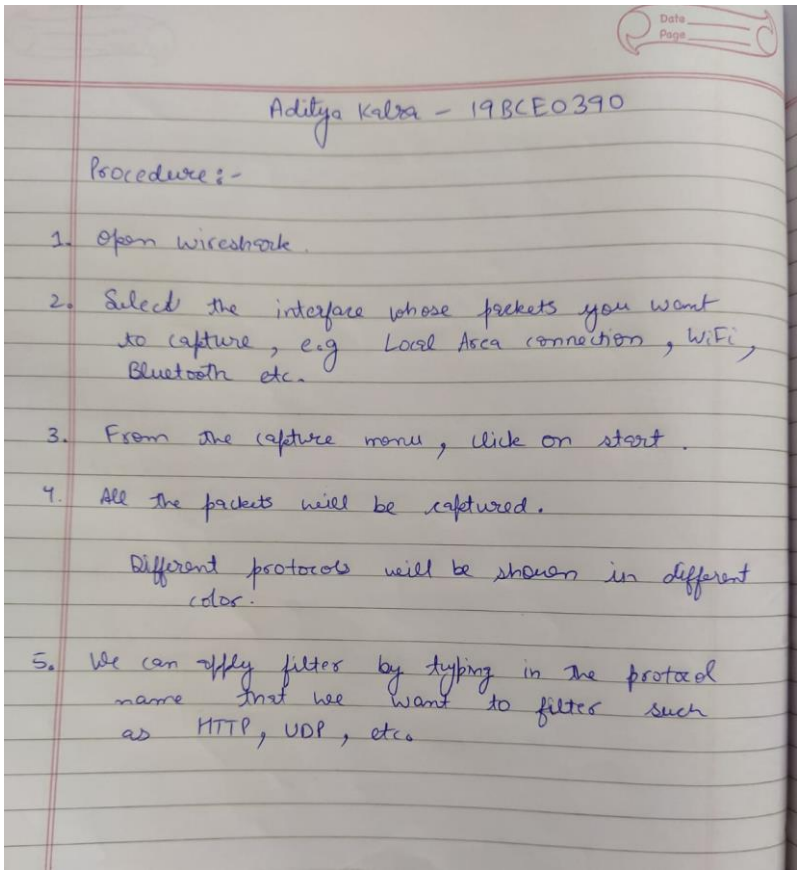
Reg No: 19BCE0390

Wireshark experiment:

Aim:

The aim of this assignment is to capture and analyse the packets using Wireshark. There can be many types of protocols that the packets use like HTTP, UDP etc. In this assignment we will filter the packets captured on the basis of the protocols used by them.

Procedure:



Aditya Kalra - 19BCE0390

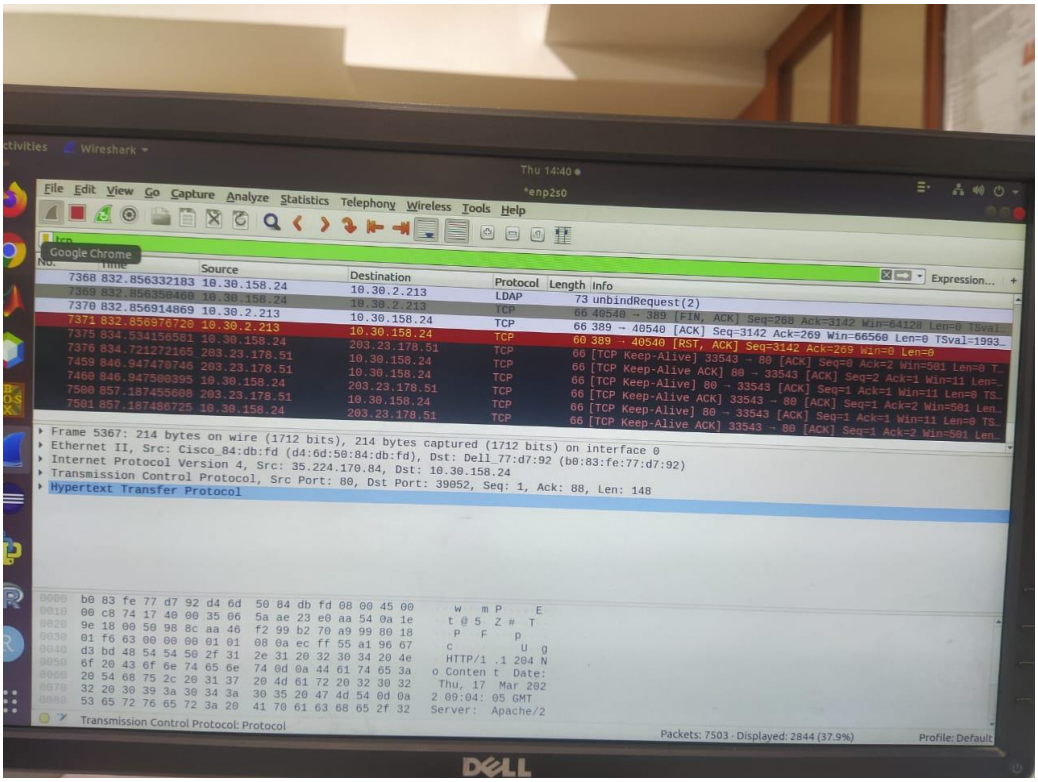
Procedure:-

1. Open wireshark.
2. Select the interface whose packets you want to capture, e.g Local Area connection, WiFi, Bluetooth etc.
3. From the capture menu, click on start.
4. All the packets will be captured.

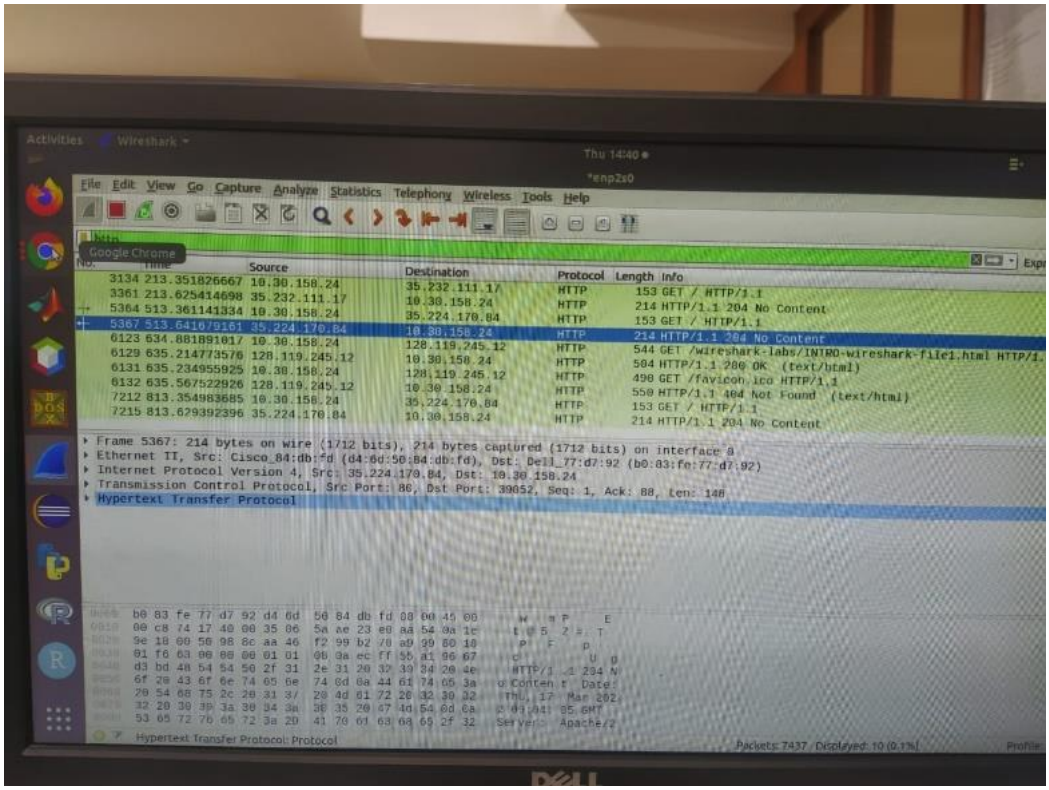
   Different protocols will be shown in different color.
5. We can apply filter by typing in the protocol name that we want to filter such as HTTP, UDP, etc.

Screenshots:

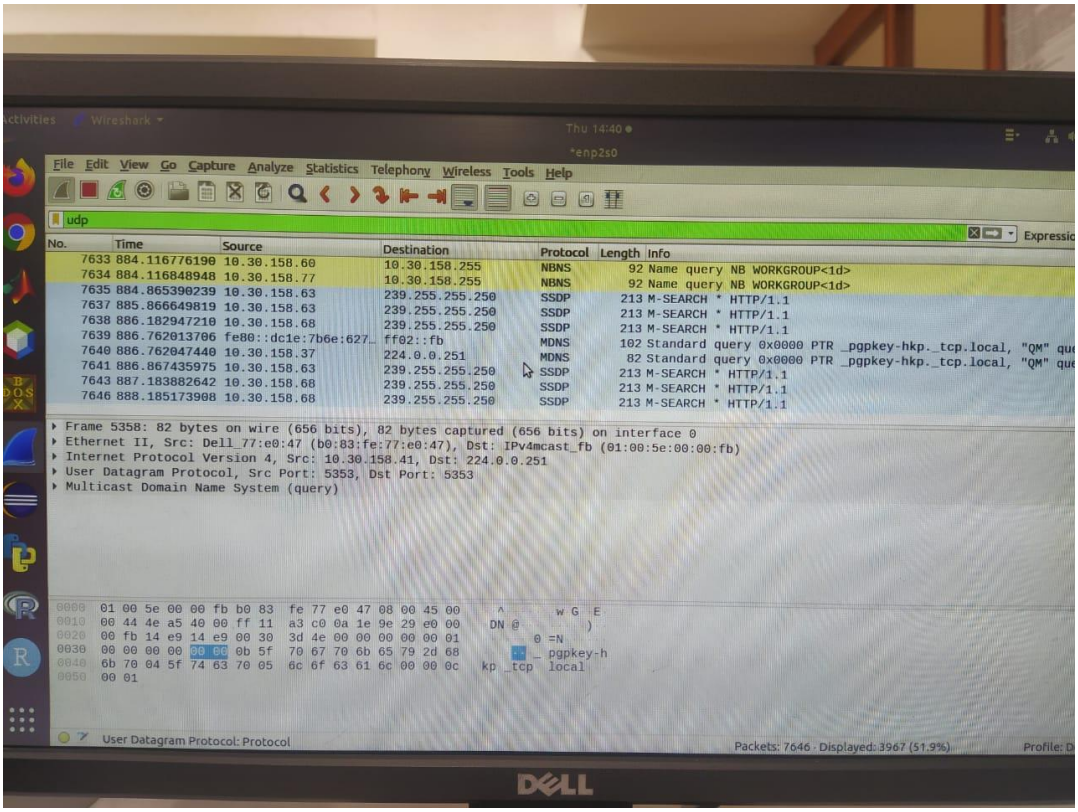
TCP:



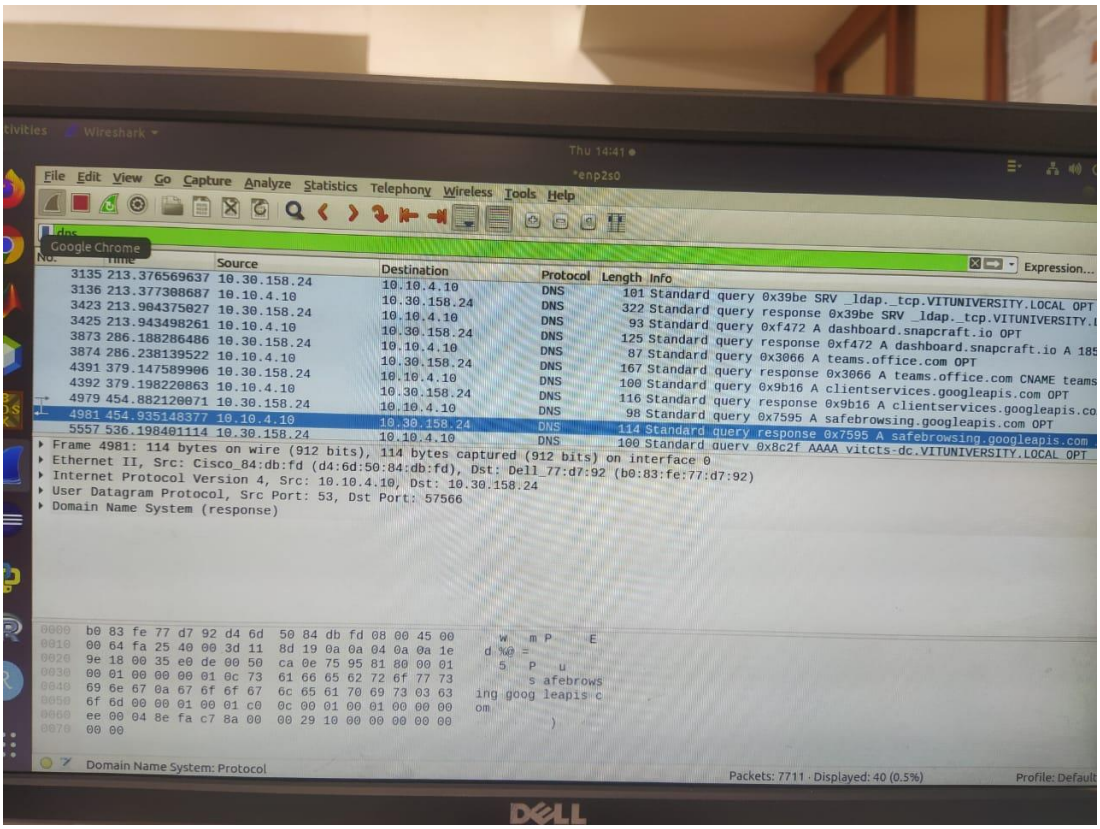
HTTP:



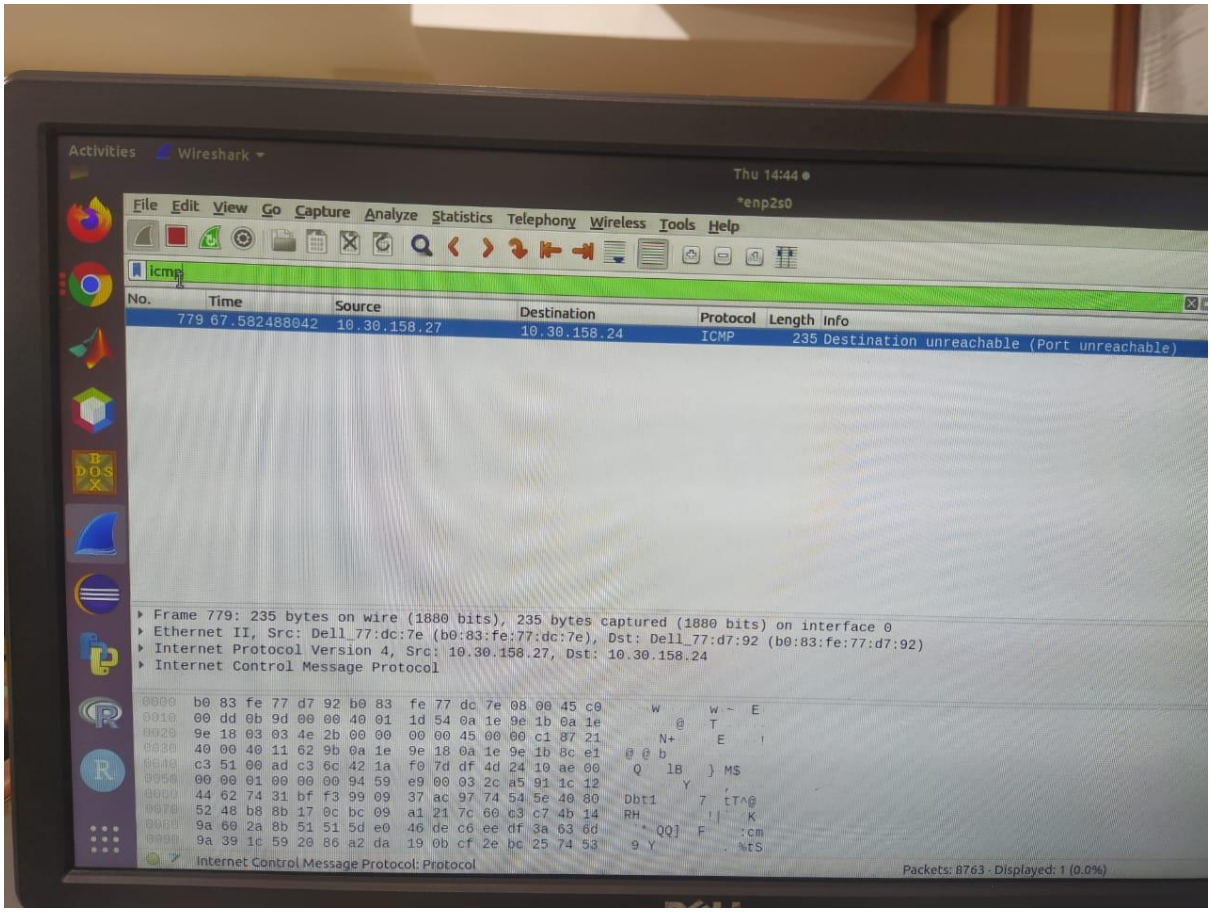
UDP:


Wireshark
Thu 14:40
*enp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
No. Time Source Destination Protocol Length Info
7633 884.116776190 10.30.158.60 10.30.158.255 NBNS 92 Name query NB WORKGROUP<1d>
7634 884.116848948 10.30.158.77 10.30.158.255 NBNS 92 Name query NB WORKGROUP<1d>
7635 884.865390239 10.30.158.63 239.255.255.250 SSDP 213 M-SEARCH * HTTP/1.1
7637 885.866649819 10.30.158.63 239.255.255.250 SSDP 213 M-SEARCH * HTTP/1.1
7638 886.182947210 10.30.158.68 239.255.255.250 SSDP 213 M-SEARCH * HTTP/1.1
7639 886.762013706 fe80::dc1e:7b6e:627… ff02::fb MDNS 102 Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "QM"
7640 886.762047440 10.30.158.37 224.0.0.251 MDNS 82 Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "QM"
7641 886.867435975 10.30.158.63 239.255.255.250 SSDP 213 M-SEARCH * HTTP/1.1
7643 887.183882642 10.30.158.68 239.255.255.250 SSDP 213 M-SEARCH * HTTP/1.1
7646 888.185173908 10.30.158.68 239.255.255.250 SSDP 213 M-SEARCH * HTTP/1.1
Frame 5358: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
Ethernet II, Src: Dell_77:e0:47 (b0:83:fe:77:e0:47), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
Internet Protocol Version 4, Src: 10.30.158.41, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)
User Datagram Protocol: Protocol
Packets: 7646 · Displayed: 3967 (51.9%)
DELL

DNS:


Wireshark
Thu 14:41
*enp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Google Chrome
No. Time Source Destination Protocol Length Info
3135 213.376569637 10.30.158.24 10.10.4.10 DNS 101 Standard query 0x39be SRV _ldap._tcp.VITUNIVERSITY.LOCAL
3136 213.377308687 10.10.4.10 10.30.158.24 DNS 322 Standard query response 0x39be SRV _ldap._tcp.VITUNIVERSITY.
3423 213.904375027 10.30.158.24 10.10.4.10 DNS 93 Standard query 0xf472 A dashboard.snapcraft.io OPT
3425 213.943498261 10.10.4.10 10.30.158.24 DNS 125 Standard query response 0xf472 A dashboard.snapcraft.io A 185
3873 286.188286486 10.30.158.24 10.10.4.10 DNS 87 Standard query 0x3066 A teams.office.com OPT
3874 286.238139522 10.10.4.10 10.30.158.24 DNS 167 Standard query response 0x3066 A teams.office.com CNAME teams
4391 379.147589906 10.30.158.24 10.10.4.10 DNS 100 Standard query 0x9b16 A clientservices.googleapis.com OPT
4392 379.198220863 10.10.4.10 10.30.158.24 DNS 116 Standard query response 0x9b16 A clientservices.googleapis.com
4979 454.882120071 10.30.158.24 10.10.4.10 DNS 98 Standard query 0x7595 A safebrowsing.googleapis.com OPT
4981 454.935148377 10.10.4.10 10.30.158.24 DNS 114 Standard query response 0x7595 A safebrowsing.googleapis.com
5557 536.198401114 10.30.158.24 10.10.4.10 DNS 100 Standard query 0x8c2f AAAA vitcts-dc.VITUNIVERSITY.LOCAL OPT
Frame 4981: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
Ethernet II, Src: Cisco_84:db:fd (d4:6d:50:84:db:fd), Dst: Dell_77:d7:92 (b0:83:fe:77:d7:92)
Internet Protocol Version 4, Src: 10.10.4.10, Dst: 10.30.158.24
User Datagram Protocol, Src Port: 53, Dst Port: 57566
Domain Name System (response)
Domain Name System: Protocol
Packets: 7711 · Displayed: 40 (0.5%)
DELL

ICMP:



Conclusion:

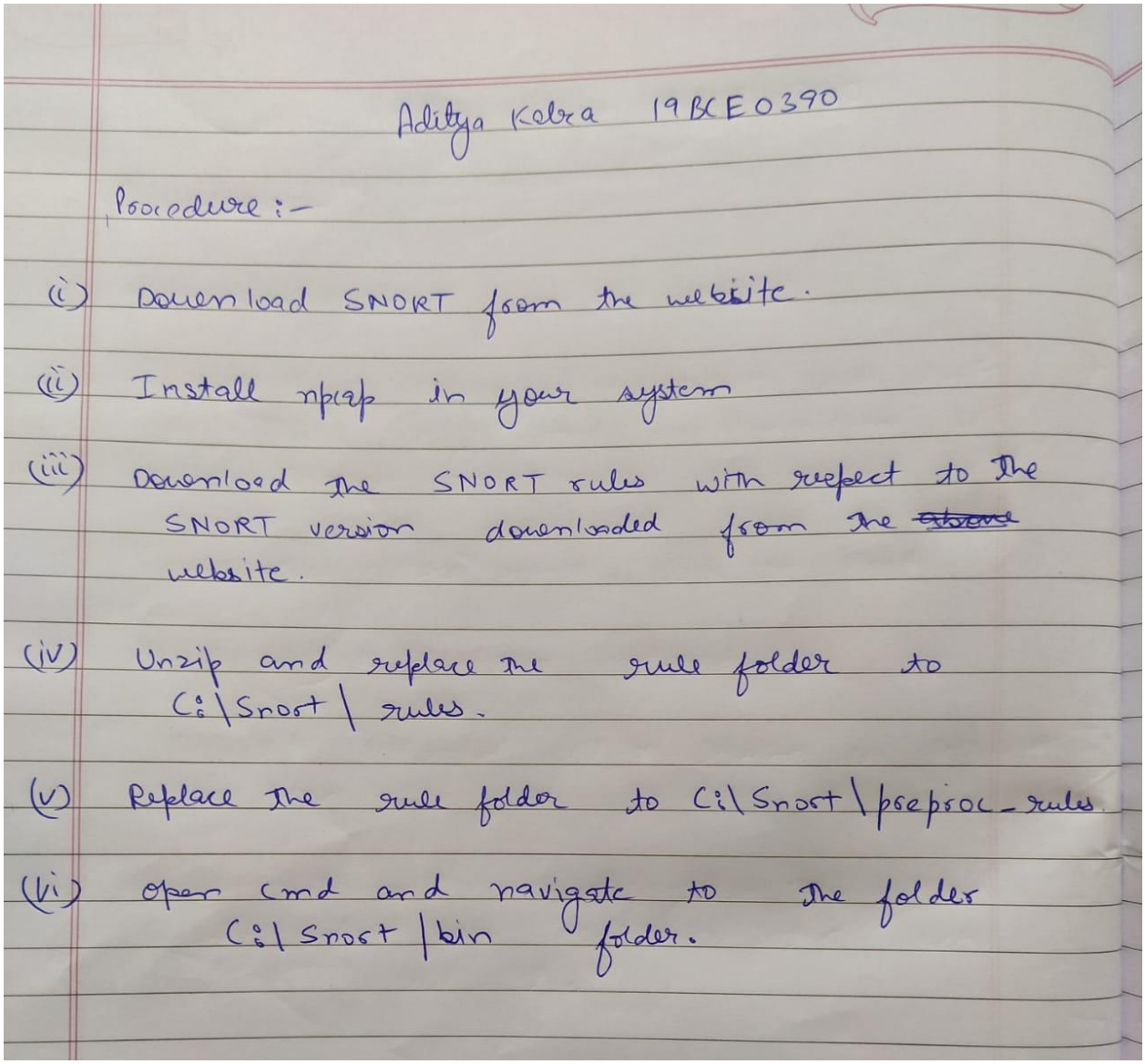
We were successfully able to capture the packets using Wireshark. Apart from that we could also filter the packets using the protocols used by them.

SNORT:

Aim:

The aim of this assignment is to show Intrusion Detection System using SNORT.

Procedure:



Aditya Kolra 19BCE0390

Procedure :-

(i) Download SNORT from the website.

(ii) Install npcap in your system

(iii) Download the SNORT rules with respect to the SNORT version downloaded from the website.

(iv) Unzip and replace the rule folder to C:\Snort\rules.

(v) Replace the rule folder to C:\Snort\preproc_rules

(vi) Open cmd and navigate to the folder C:\Snort\bin folder.

Screenshots:

snort -W

```
C:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.19-WIN64 GRE (Build 85)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       disabled        \Device\NPF_{3B71BE93-AECB-4F83-B497-1EB580CA25D1}      WAN Miniport (Network Monitor)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{F2BFE38A-1D68-474C-AD16-55007529A556}      WAN Miniport (IPv6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{4C8825F6-328D-4FE3-A9B1-8ED75FD75974}      WAN Miniport (IP)
    4   34:2E:B7:91:91:50       0000:0000:fe80:0000:0000:0000:616f:64d6 \Device\NPF_{FEB58C2A-26DA-4981-80BF-9AF5F9A69C19}      Intel(R) Wi-Fi 6 AX201 160MHz
    5   34:2E:B7:91:91:51       0000:0000:fe80:0000:0000:0000:a08b:9564 \Device\NPF_{6655BA17-EAD8-4876-BE3A-0675902DD6B3}      Microsoft Wi-Fi Direct Virtual Adapter
    6   36:2E:B7:91:91:50       0000:0000:fe80:0000:0000:0000:78ca:2de2 \Device\NPF_{76B0D9F6-A4C9-413D-9E95-07DE6D707C2B}      Microsoft Wi-Fi Direct Virtual Adapter #2
    7   00:00:00:00:00:00       disabled        \Device\NPF_Loopback    Adapter for loopback traffic capture
    8   00:2B:67:F1:6A:6C       0000:0000:fe80:0000:0000:0000:259b:d93c \Device\NPF_{4F87F54D-D2A2-4FB1-B404-17C9FEA101D2}      Realtek PCIe GbE Family Controller

C:\Snort\bin>
```

Snort -dev -I 4

```
C:\Snort\bin>snort -dev -i 4
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{68387752-A5E0-4AD3-8626-F13B40DC7796}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.19-WIN64 GRE (Build 85)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=3580)
*** Caught Int-Signal
===============================================================================
Run time for packet processing was 54.480000 seconds
Snort processed 0 packets.
Snort ran for 0 days 0 hours 0 minutes 54 seconds
   Pkts/sec:           0
===============================================================================
Packet I/O Totals:
   Received:           0
   Analyzed:           0 (  0.000%)
    Dropped:           0 (  0.000%)
   Filtered:           0 (  0.000%)
Outstanding:           0 (  0.000%)
   Injected:           0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:           0 (  0.000%)
       VLAN:           0 (  0.000%)
        IP4:           0 (  0.000%)
       Frag:           0 (  0.000%)
       ICMP:           0 (  0.000%)
        UDP:           0 (  0.000%)
```

Snort -v

```
C:\Snort\bin>snort -v
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{B2B4F1CD-2493-46E4-96D3-B0957EAB6699}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.19-WIN64 GRE (Build 85)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=12872)
*** Caught Int-Signal
===============================================================================
Run time for packet processing was 79.755000 seconds
Snort processed 0 packets.
Snort ran for 0 days 0 hours 1 minutes 19 seconds
   Pkts/min:           0
   Pkts/sec:           0
===============================================================================
Packet I/O Totals:
   Received:           0
   Analyzed:           0 (  0.000%)
    Dropped:           0 (  0.000%)
   Filtered:           0 (  0.000%)
Outstanding:           0 (  0.000%)
   Injected:           0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
       Eth:           0 (  0.000%)
      VLAN:           0 (  0.000%)
       IP4:           0 (  0.000%)
      Frag:           0 (  0.000%)
      ICMP:           0 (  0.000%)
```

```
   Eth Loop:           0 (  0.000%)
   Eth Disc:           0 (  0.000%)
   IP4 Disc:           0 (  0.000%)
   IP6 Disc:           0 (  0.000%)
   TCP Disc:           0 (  0.000%)
   UDP Disc:           0 (  0.000%)
  ICMP Disc:           0 (  0.000%)
All Discard:           0 (  0.000%)
      Other:           0 (  0.000%)
Bad Chk Sum:           0 (  0.000%)
    Bad TTL:           0 (  0.000%)
     S5 G 1:           0 (  0.000%)
     S5 G 2:           0 (  0.000%)
      Total:           0
===============================================================================

Memory Statistics for File at:Tue Apr  5 17:13:23 2022

Total buffers allocated:          0
Total buffers freed:              0
Total buffers released:           0
Total file mempool:               0
Total allocated file mempool:     0
Total freed file mempool:         0
Total released file mempool:      0

Heap Statistics of file:
          Total Statistics:
               Memory in use:             0 bytes
                No of allocs:             0
                 No of frees:             0
===============================================================================
Snort exiting
```

Snort -vd

```
C:\Snort\bin>snort -vd
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{B2B4F1CD-2493-46E4-96D3-B0957EAB6699}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.19-WIN64 GRE (Build 85)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=9068)
*** Caught Int-Signal
===============================================================================
Run time for packet processing was 14076.236000 seconds
Snort processed 0 packets.
Snort ran for 0 days 3 hours 54 minutes 36 seconds
    Pkts/hr:            0
   Pkts/min:            0
   Pkts/sec:            0
===============================================================================
Packet I/O Totals:
   Received:            0
   Analyzed:            0 (  0.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:            0 (  0.000%)
       VLAN:            0 (  0.000%)
        IP4:            0 (  0.000%)
```

```
   GRE IP6:          0 (  0.000%)
GRE IP6 Ext:         0 (  0.000%)
   GRE PPTP:         0 (  0.000%)
    GRE ARP:         0 (  0.000%)
    GRE IPX:         0 (  0.000%)
   GRE Loop:         0 (  0.000%)
       MPLS:         0 (  0.000%)
        ARP:         0 (  0.000%)
        IPX:         0 (  0.000%)
   Eth Loop:         0 (  0.000%)
   Eth Disc:         0 (  0.000%)
   IP4 Disc:         0 (  0.000%)
   IP6 Disc:         0 (  0.000%)
   TCP Disc:         0 (  0.000%)
   UDP Disc:         0 (  0.000%)
  ICMP Disc:         0 (  0.000%)
All Discard:         0 (  0.000%)
      Other:         0 (  0.000%)
Bad Chk Sum:         0 (  0.000%)
    Bad TTL:         0 (  0.000%)
     S5 G 1:         0 (  0.000%)
     S5 G 2:         0 (  0.000%)
      Total:         0
===============================================================================

Memory Statistics for File at:Tue Apr  5 21:09:40 2022

Total buffers allocated:          0
Total buffers freed:              0
Total buffers released:           0
Total file mempool:               0
Total allocated file mempool:     0
Total freed file mempool:         0
Total released file mempool:      0

Heap Statistics of file:
         Total Statistics:
              Memory in use:            0 bytes
               No of allocs:            0
                No of frees:            0
-------------------------------------------------------------------------------
Snort exiting
```