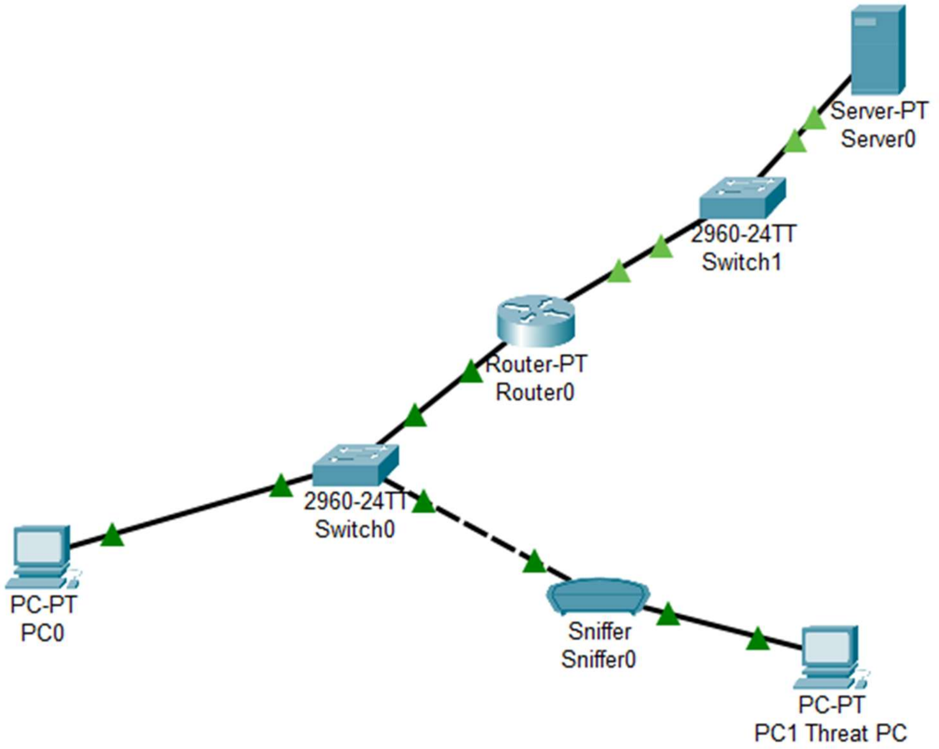
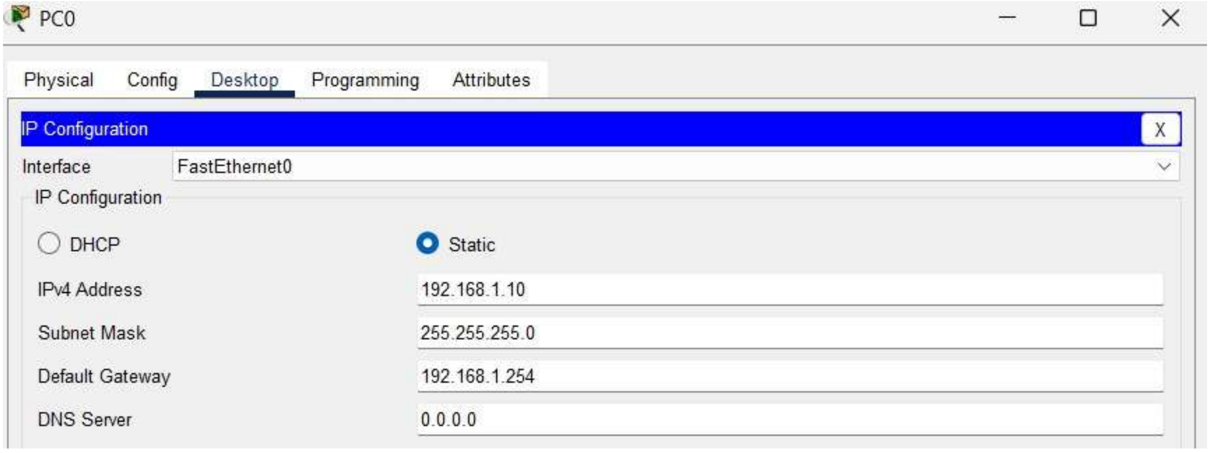
LINUX NETWORKING MODULE 5 ASSESSMENT SOLUTION

-BY SAKTHI KUMAR S

2) Using Packet Tracer, simulate an ARP spoofing attack. Analyze the behavior of devices on the network when they receive a malicious ARP response.



IP configurations:



PC0

IP Configuration

Interface: FastEthernet0

IP Configuration

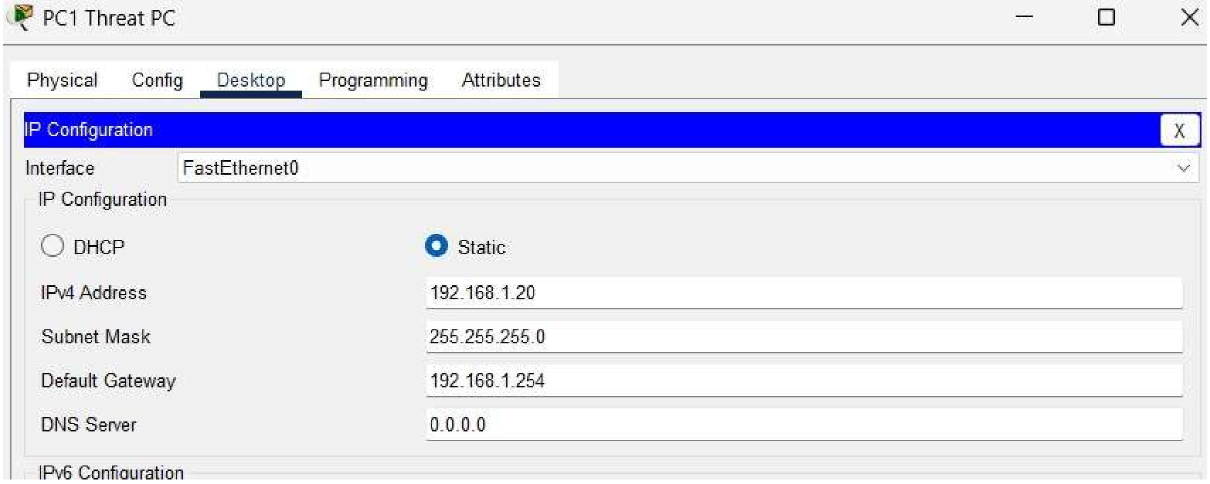
○ DHCP ● Static

IPv4 Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.254

DNS Server: 0.0.0.0



PC1 Threat PC

IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

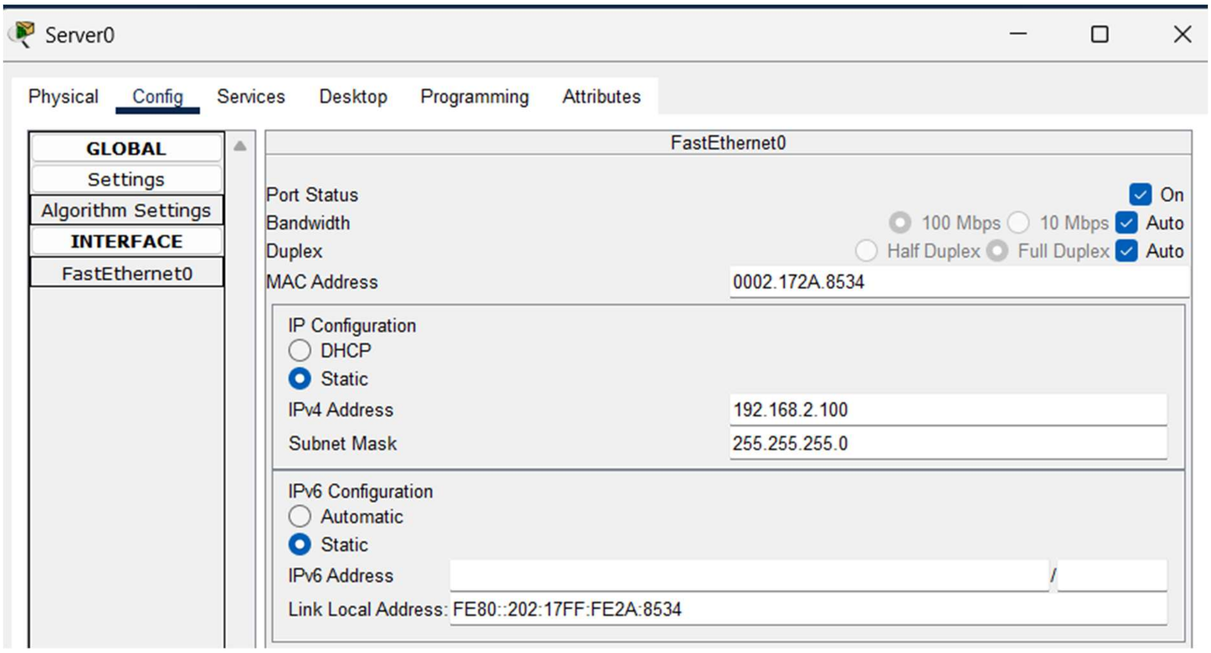
IPv4 Address: 192.168.1.20

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.254

DNS Server: 0.0.0.0

IPv6 Configuration



Server0

FastEthernet0

Port Status: ☑ On

Bandwidth: ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex: ○ Half Duplex ○ Full Duplex ☑ Auto

MAC Address: 0002.172A.8534

IP Configuration

○ DHCP

● Static

IPv4 Address: 192.168.2.100

Subnet Mask: 255.255.255.0

IPv6 Configuration

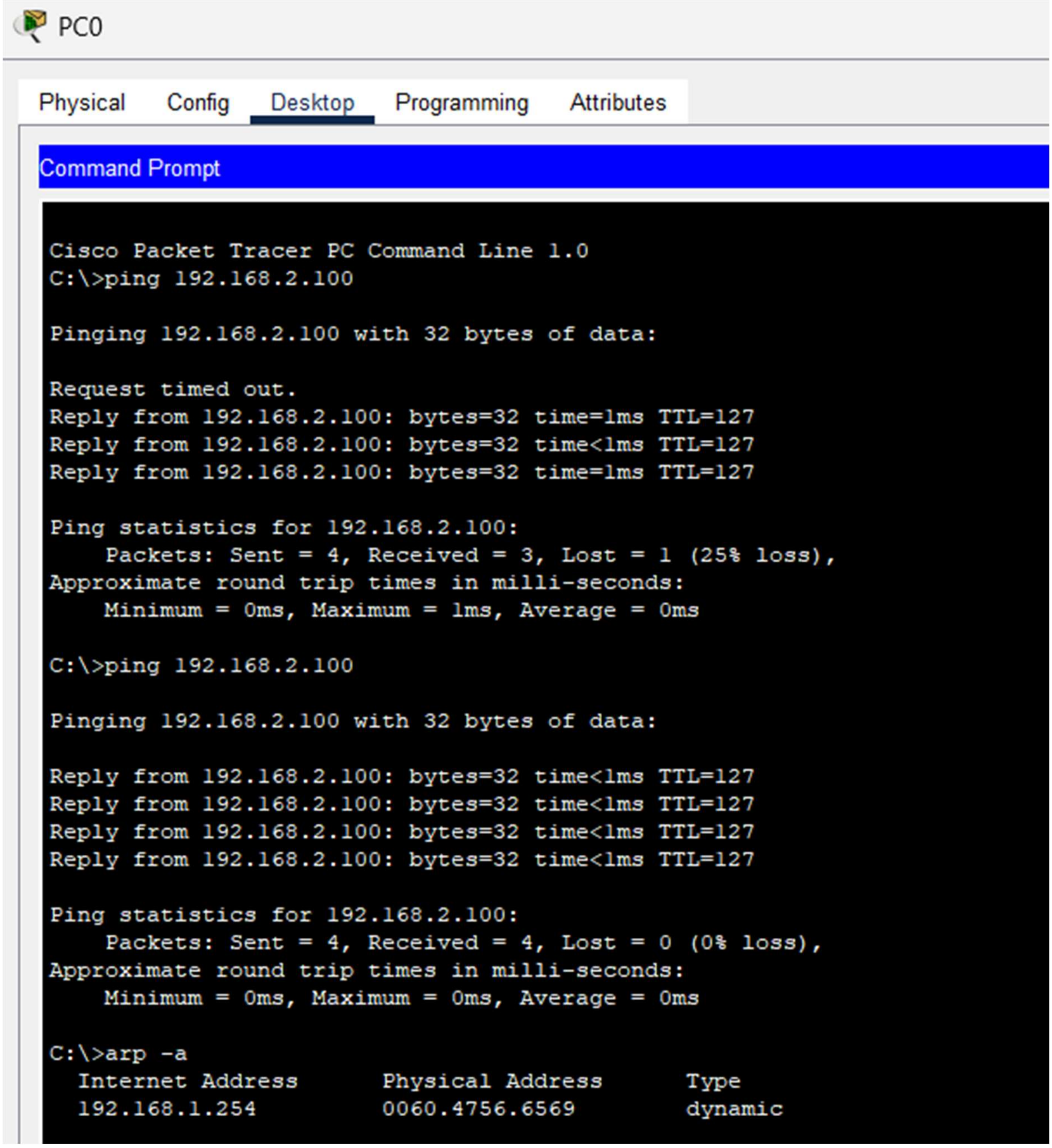
○ Automatic

● Static

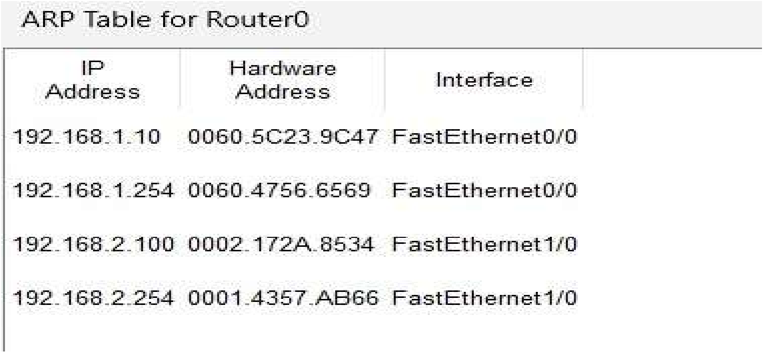
IPv6 Address: /

Link Local Address: FE80::202:17FF:FE2A:8534

Ping and ARP table before MAC change:



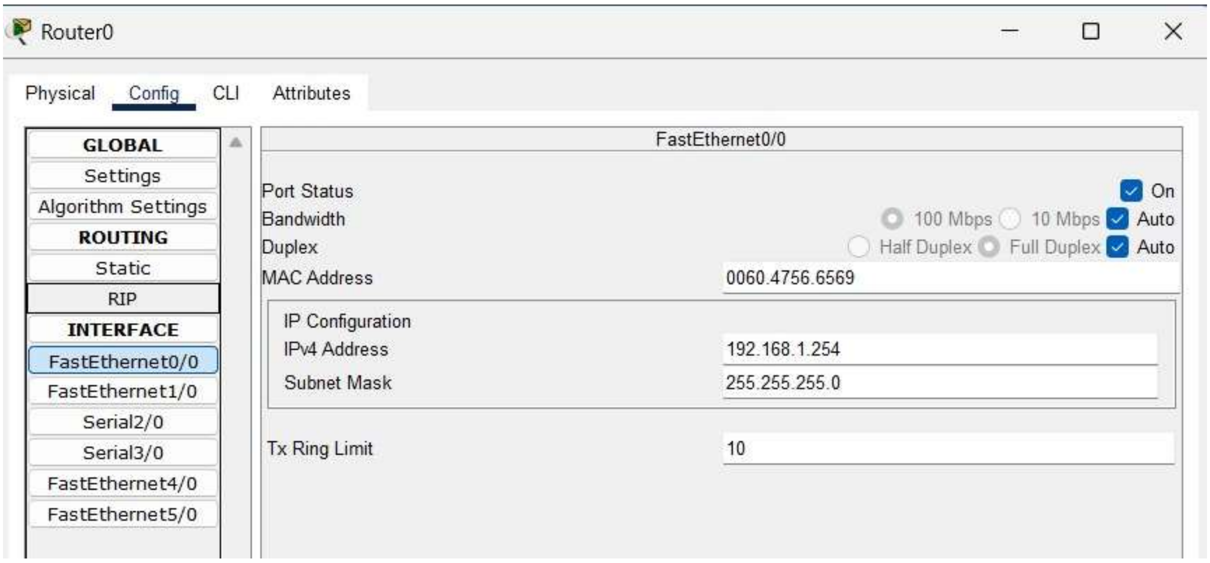
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.100

Pinging 192.168.2.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.100: bytes=32 time=1ms TTL=127
Reply from 192.168.2.100: bytes=32 time<1ms TTL=127
Reply from 192.168.2.100: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.2.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.2.100

Pinging 192.168.2.100 with 32 bytes of data:

Reply from 192.168.2.100: bytes=32 time<1ms TTL=127
Reply from 192.168.2.100: bytes=32 time<1ms TTL=127
Reply from 192.168.2.100: bytes=32 time<1ms TTL=127
Reply from 192.168.2.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.254         0060.4756.6569        dynamic
```



ARP Table for Router0

IP Address	Hardware Address	Interface
192.168.1.10	0060.5C23.9C47	FastEthernet0/0
192.168.1.254	0060.4756.6569	FastEthernet0/0
192.168.2.100	0002.172A.8534	FastEthernet1/0
192.168.2.254	0001.4357.AB66	FastEthernet1/0

Router Configurations and Threat PC MAC change:

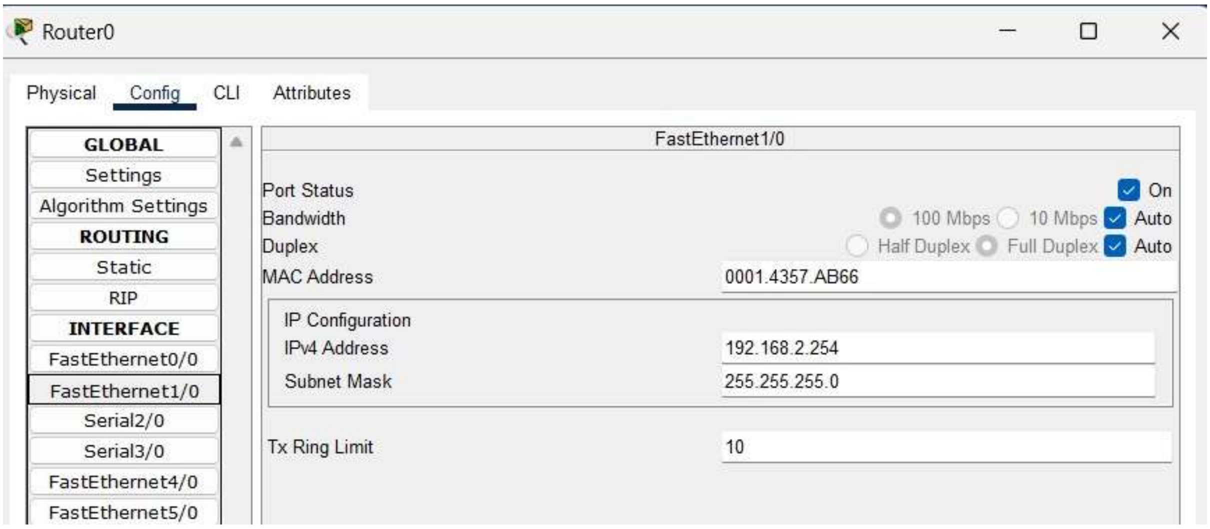


FastEthernet0/0

Port Status ☑ On
Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ● Full Duplex ☑ Auto
MAC Address 0060.4756.6569

IP Configuration
IPv4 Address 192.168.1.254
Subnet Mask 255.255.255.0

Tx Ring Limit 10

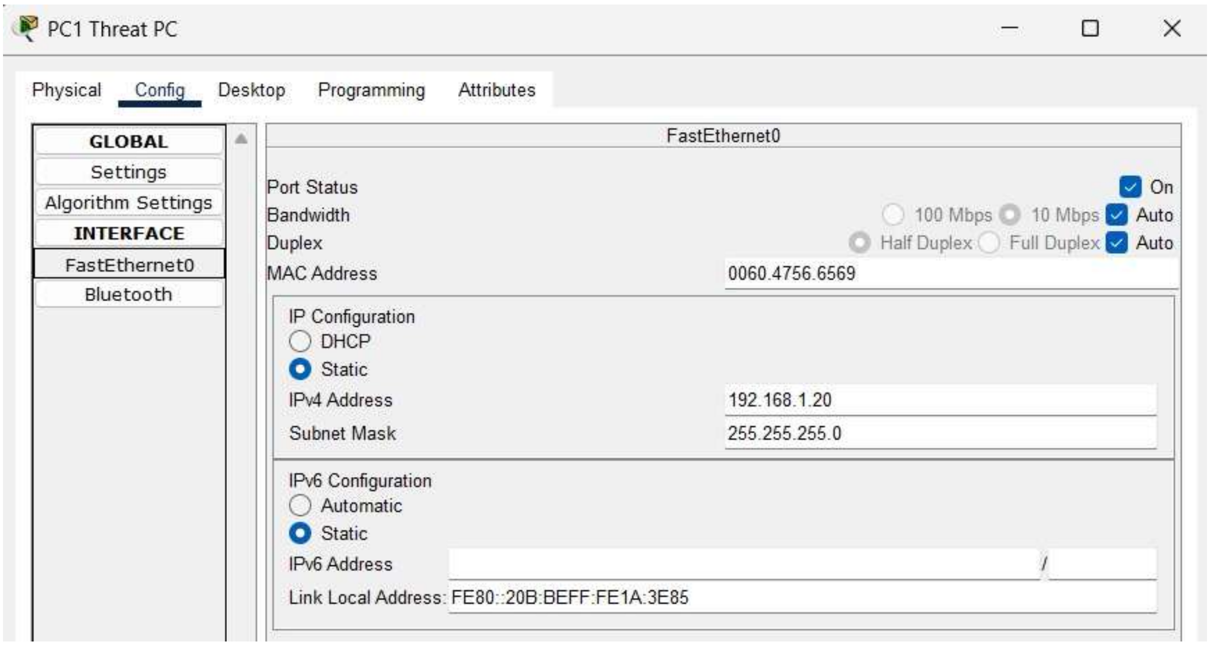


FastEthernet1/0

Port Status ☑ On
Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ● Full Duplex ☑ Auto
MAC Address 0001.4357.AB66

IP Configuration
IPv4 Address 192.168.2.254
Subnet Mask 255.255.255.0

Tx Ring Limit 10



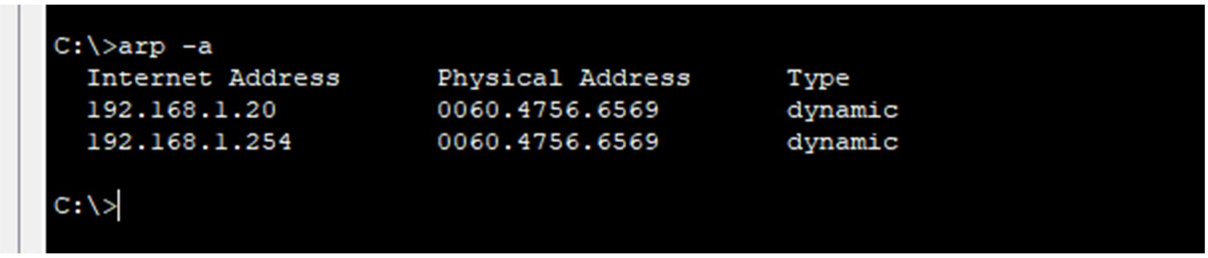
FastEthernet0

Port Status ☑ On
Bandwidth ○ 100 Mbps ● 10 Mbps ☑ Auto
Duplex ● Half Duplex ○ Full Duplex ☑ Auto
MAC Address 0060.4756.6569

IP Configuration
○ DHCP
● Static
IPv4 Address 192.168.1.20
Subnet Mask 255.255.255.0

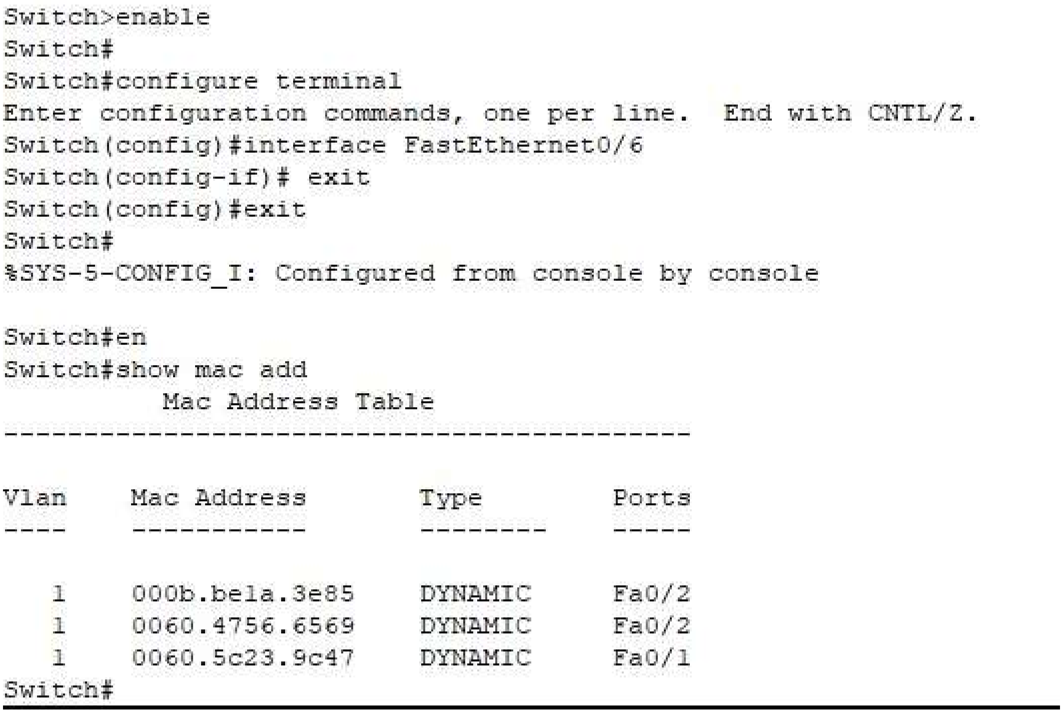
IPv6 Configuration
○ Automatic
● Static
IPv6 Address /
Link Local Address: FE80::20B:BEFF:FE1A:3E85

ARP Table after MAC change:



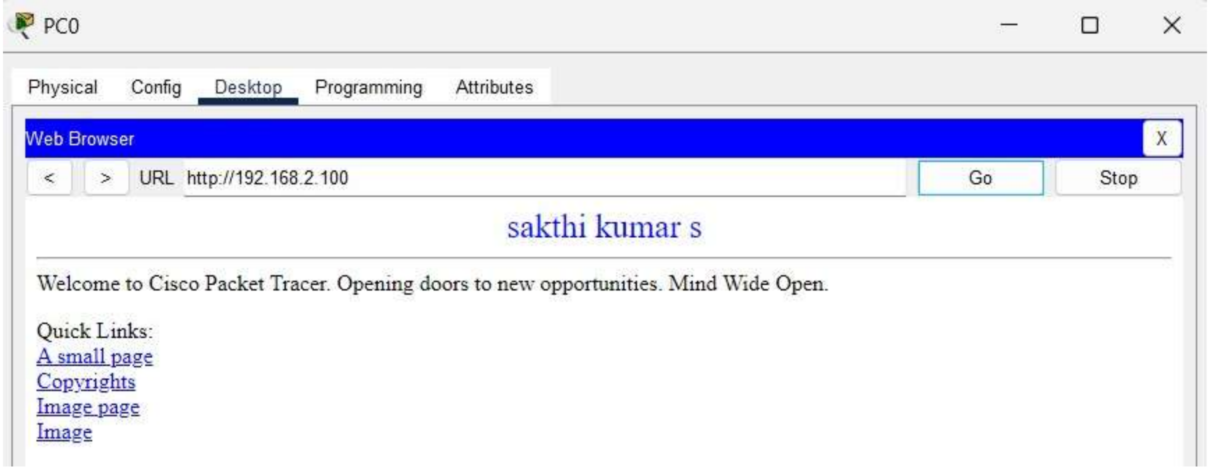
```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.20          0060.4756.6569        dynamic
  192.168.1.254         0060.4756.6569        dynamic

C:\>
```

MAC Address Table:



```
Switch>enable
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet0/6
Switch(config-if)# exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#en
Switch#show mac add
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    000b.bela.3e85    DYNAMIC     Fa0/2
   1    0060.4756.6569    DYNAMIC     Fa0/2
   1    0060.5c23.9c47    DYNAMIC     Fa0/1
Switch#
```

PC web browser to server connection before flooding with Threat PC Ping



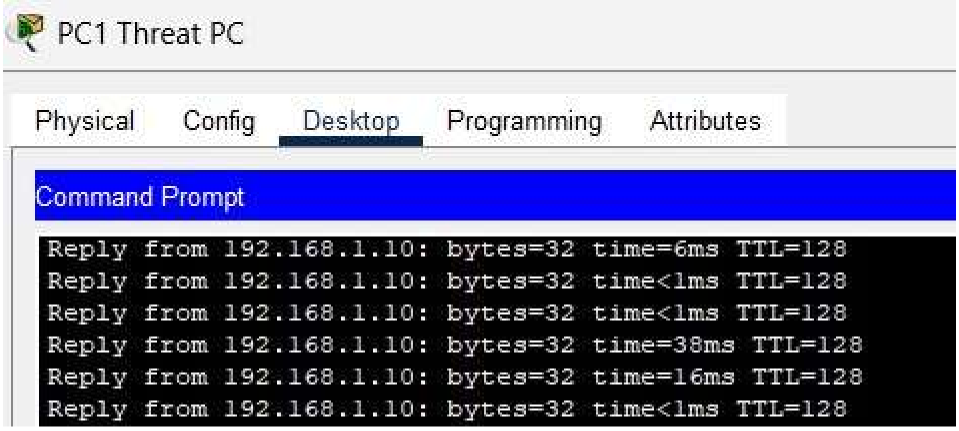
URL http://192.168.2.100

sakthi kumar s

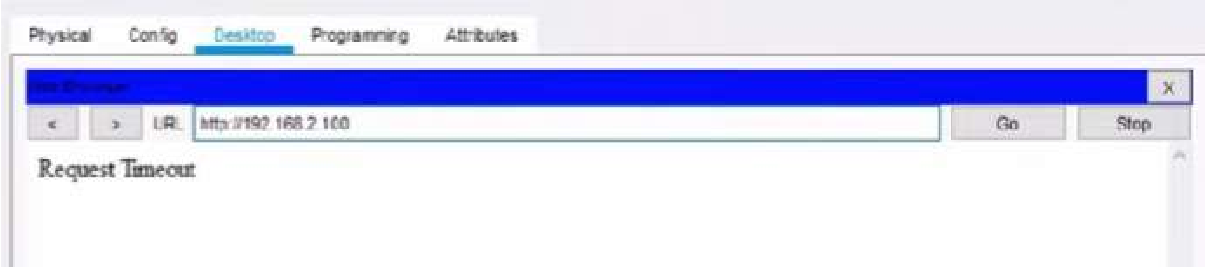
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

PC web browser to server connection After flooding with Threat PC Ping



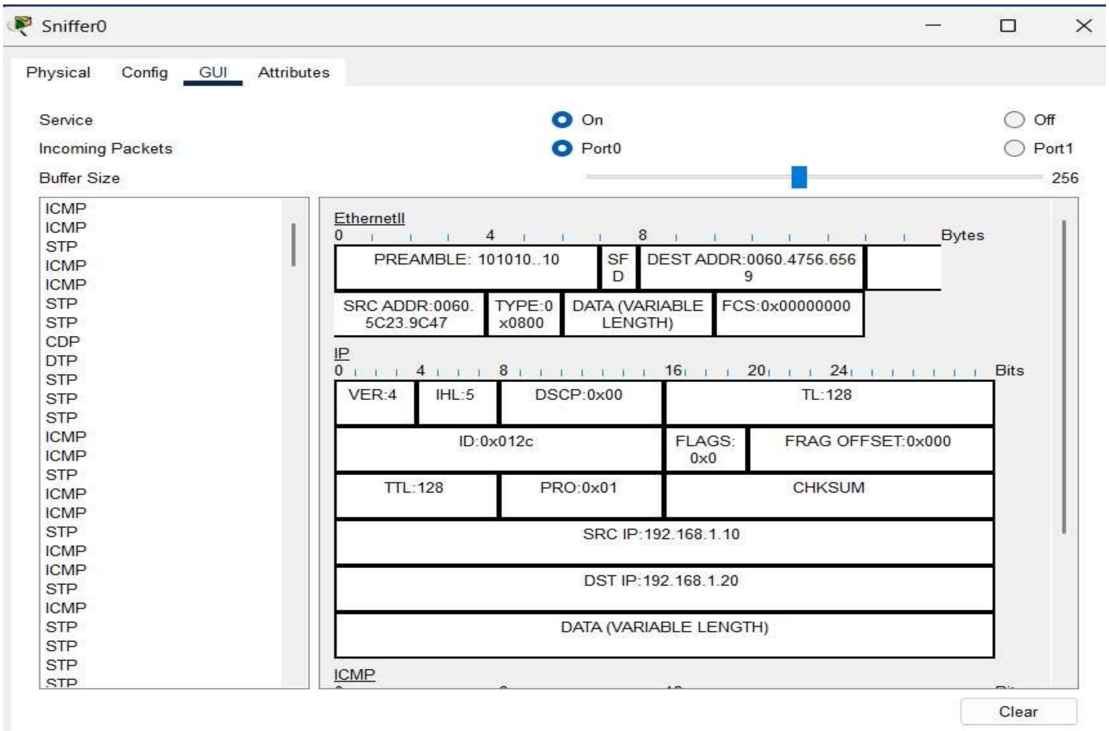
```
Reply from 192.168.1.10: bytes=32 time=6ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time=38ms TTL=128
Reply from 192.168.1.10: bytes=32 time=16ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
```



URL: http://192.168.2.100

Request Timeout

Packet sniffing near Threat PC to ensure spoofing is simulated by knowing the Packet flow between the Victim PC to server



Service ● On ○ Off

Incoming Packets ● Port0 ○ Port1

Buffer Size 256

ICMP
ICMP
STP
ICMP
ICMP
STP
STP
CDP
DTP
STP
STP
STP
ICMP
ICMP
STP
ICMP
ICMP
STP
ICMP
ICMP
STP
ICMP
STP
STP
STP
STP

EthernetII

PREAMBLE: 101010..10 | SFD | DEST ADDR:0060.4756.6569

SRC ADDR:0060.5C23.9C47 | TYPE:0x0800 | DATA (VARIABLE LENGTH) | FCS:0x00000000

IP

VER:4 | IHL:5 | DSCP:0x00 | TL:128

ID:0x012c | FLAGS: 0x0 | FRAG OFFSET:0x000

TTL:128 | PRO:0x01 | CHKSUM

SRC IP:192.168.1.10

DST IP:192.168.1.20

DATA (VARIABLE LENGTH)

ICMP