Name: Devansh Srivastava

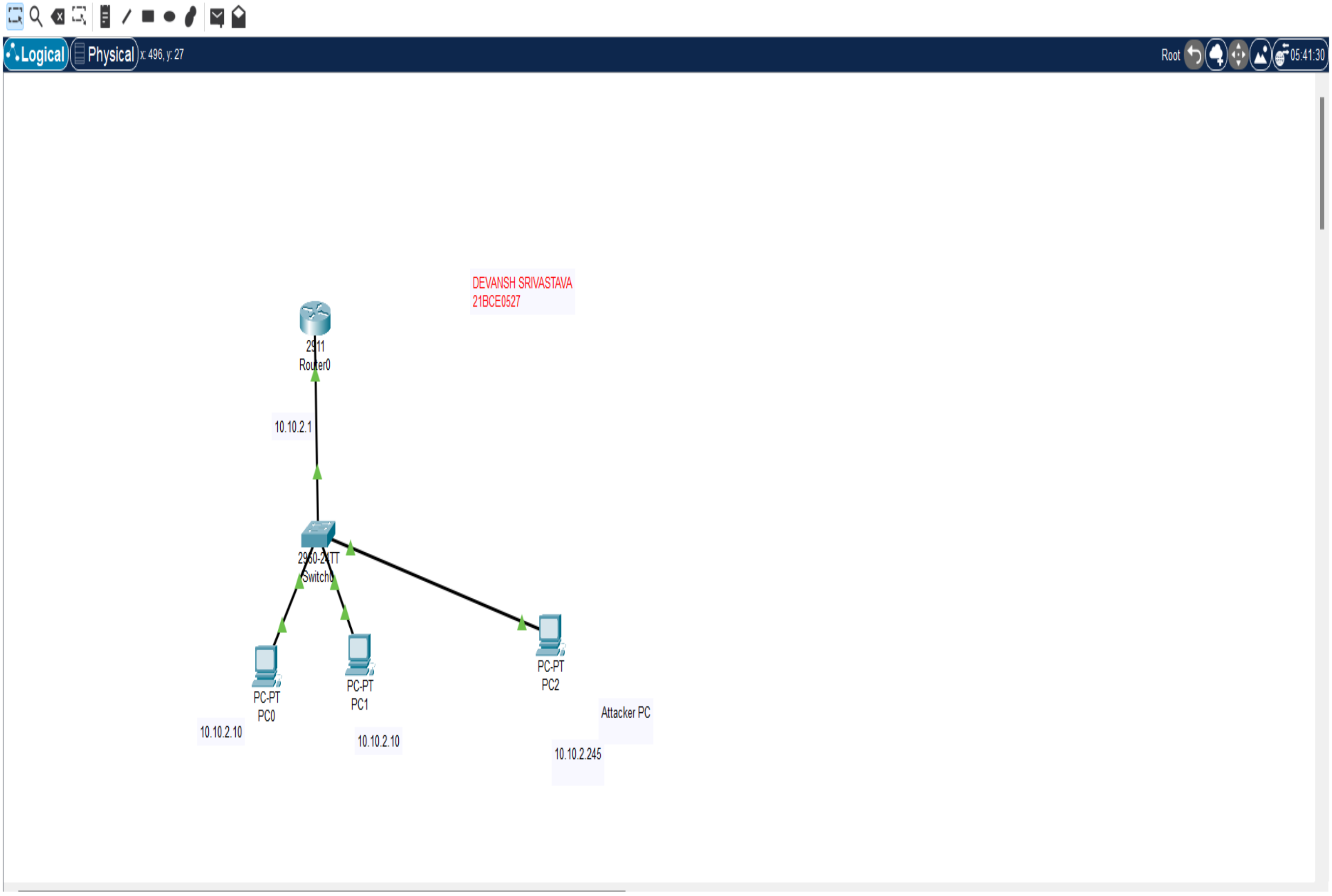
Registration No:21BCE0527

Network Training Programme

Module 5

Q2. Using Packet Tracer, simulate an ARP spoofing attack. Analyze the behavior of devices. on the network when they receive a malicious ARP response.

Network Diagram



1.Configure IP address to PC0,PC1 and PC2

2.Configure Default Gateway IP address to all three Pc
3.Configure IPV4 address to the router on correct GigaEthernet interface
4.Turn on the Router

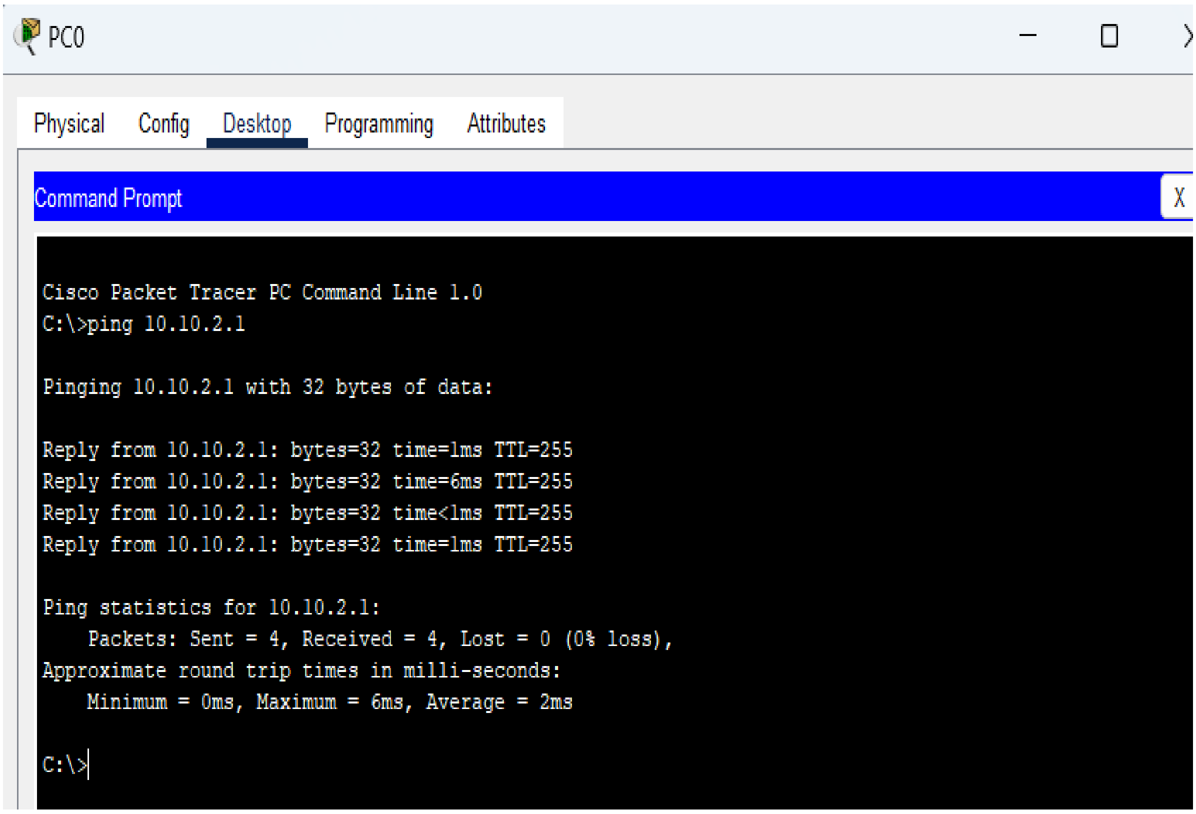
IP address of all devices:
PC0: 10.10.2.10(Victim PC)

PC1: 10.10.2.20(Victim PC)

PC2: 10.10.2.245(Attacker PC)

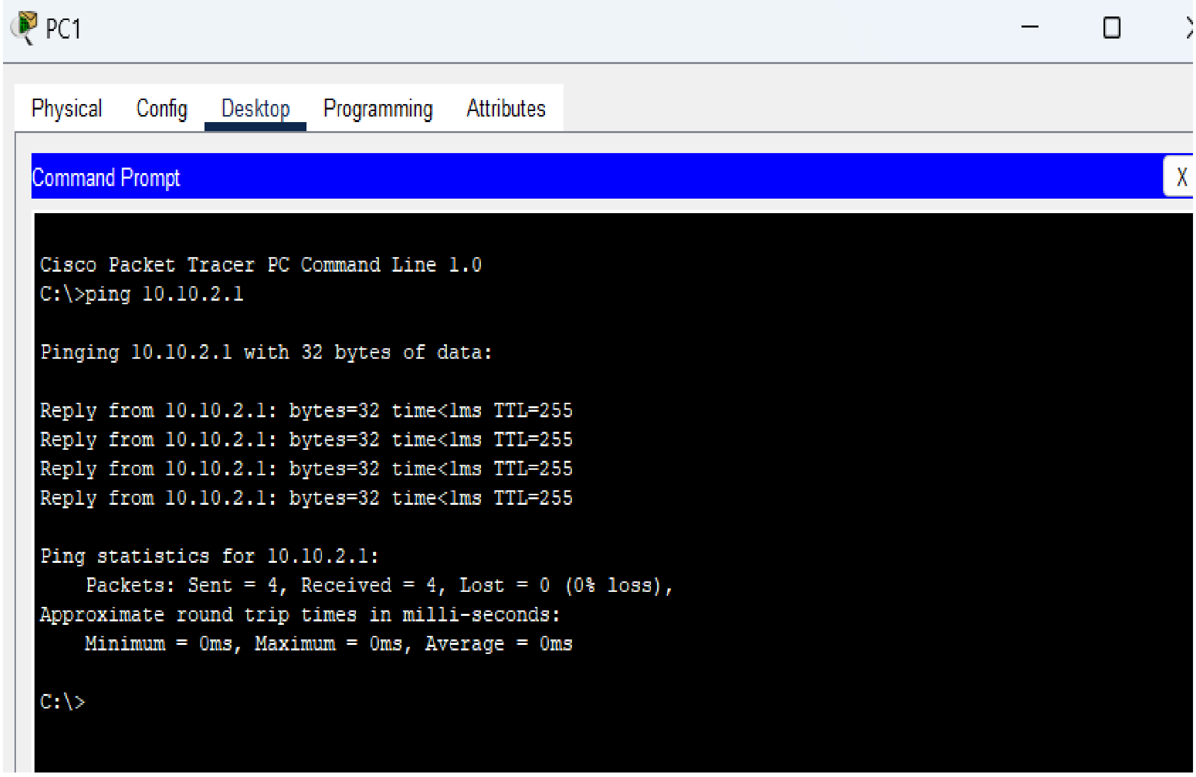
Using Ping command Ensure all PC able to communicate to Router

PC0:



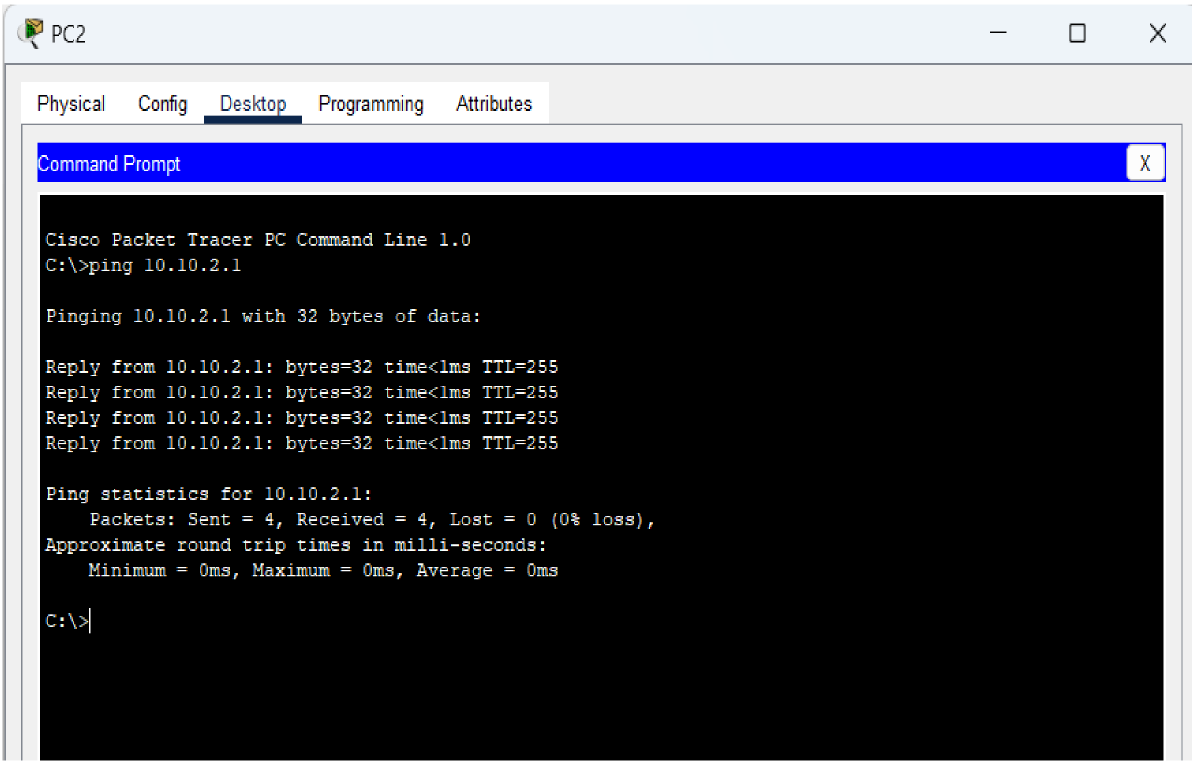
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.2.1

Pinging 10.10.2.1 with 32 bytes of data:

Reply from 10.10.2.1: bytes=32 time=1ms TTL=255
Reply from 10.10.2.1: bytes=32 time=6ms TTL=255
Reply from 10.10.2.1: bytes=32 time<1ms TTL=255
Reply from 10.10.2.1: bytes=32 time=1ms TTL=255

Ping statistics for 10.10.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 2ms

C:\>
```

PC1



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.2.1

Pinging 10.10.2.1 with 32 bytes of data:

Reply from 10.10.2.1: bytes=32 time<1ms TTL=255
Reply from 10.10.2.1: bytes=32 time<1ms TTL=255
Reply from 10.10.2.1: bytes=32 time<1ms TTL=255
Reply from 10.10.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

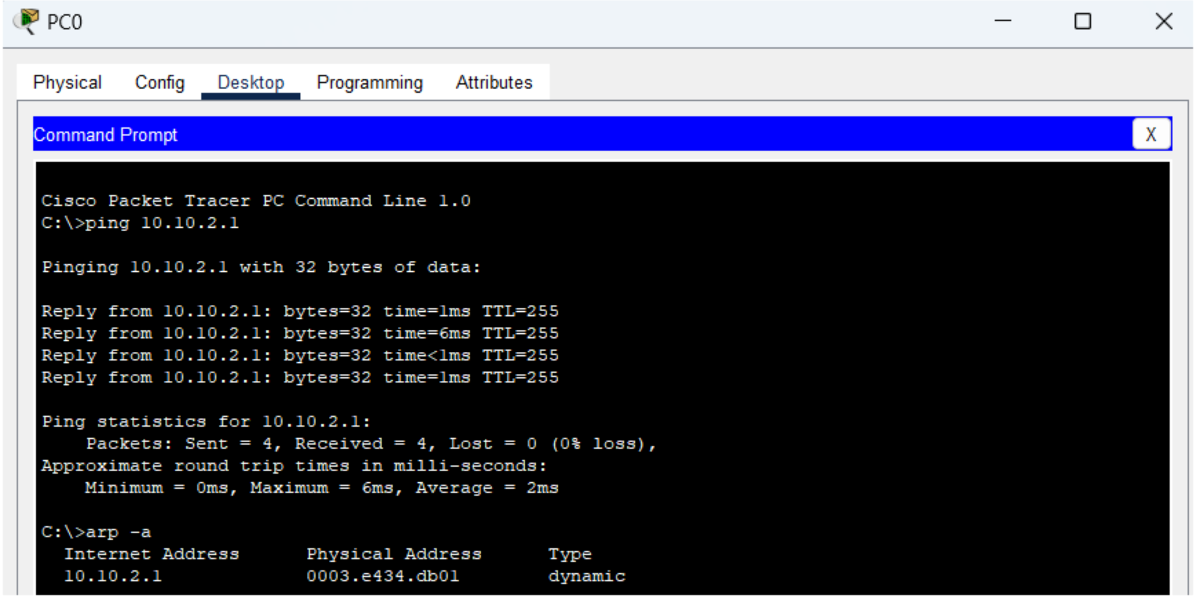
PC2(Attacker PC):



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.2.1

Pinging 10.10.2.1 with 32 bytes of data:

Reply from 10.10.2.1: bytes=32 time<1ms TTL=255
Reply from 10.10.2.1: bytes=32 time<1ms TTL=255
Reply from 10.10.2.1: bytes=32 time<1ms TTL=255
Reply from 10.10.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

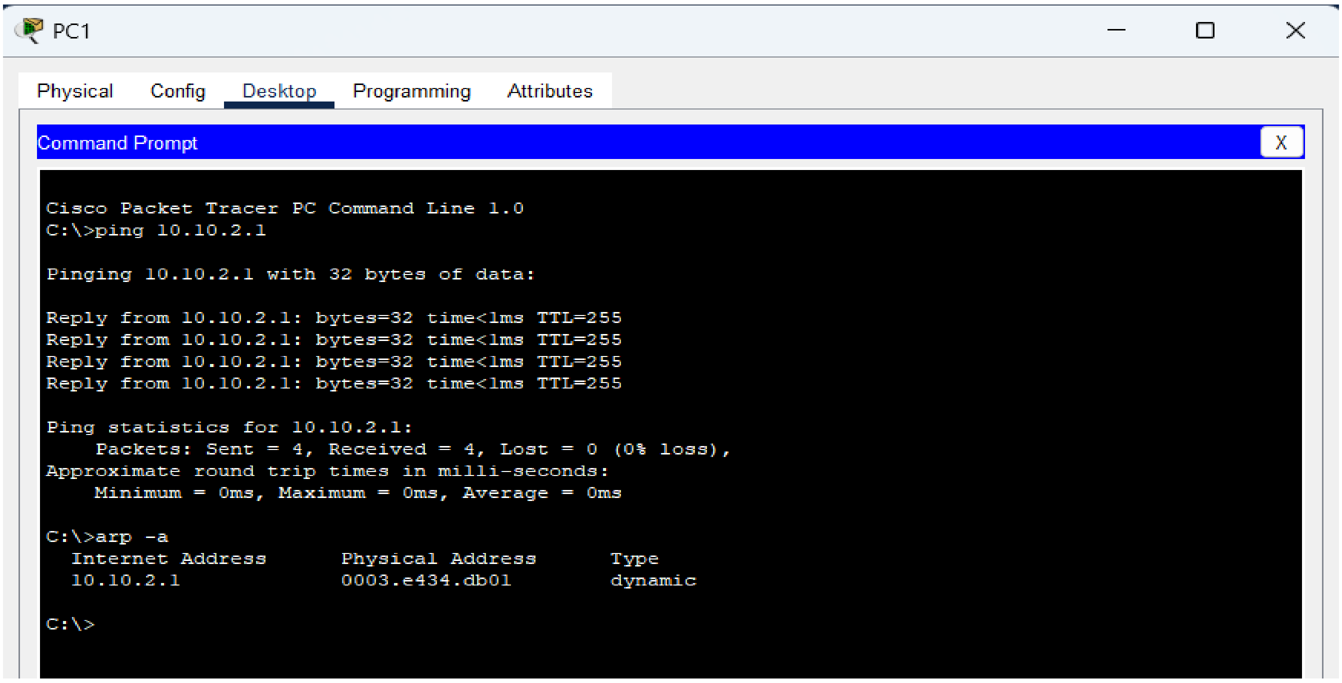
Before the attack :

ARP TABLE of PC0:



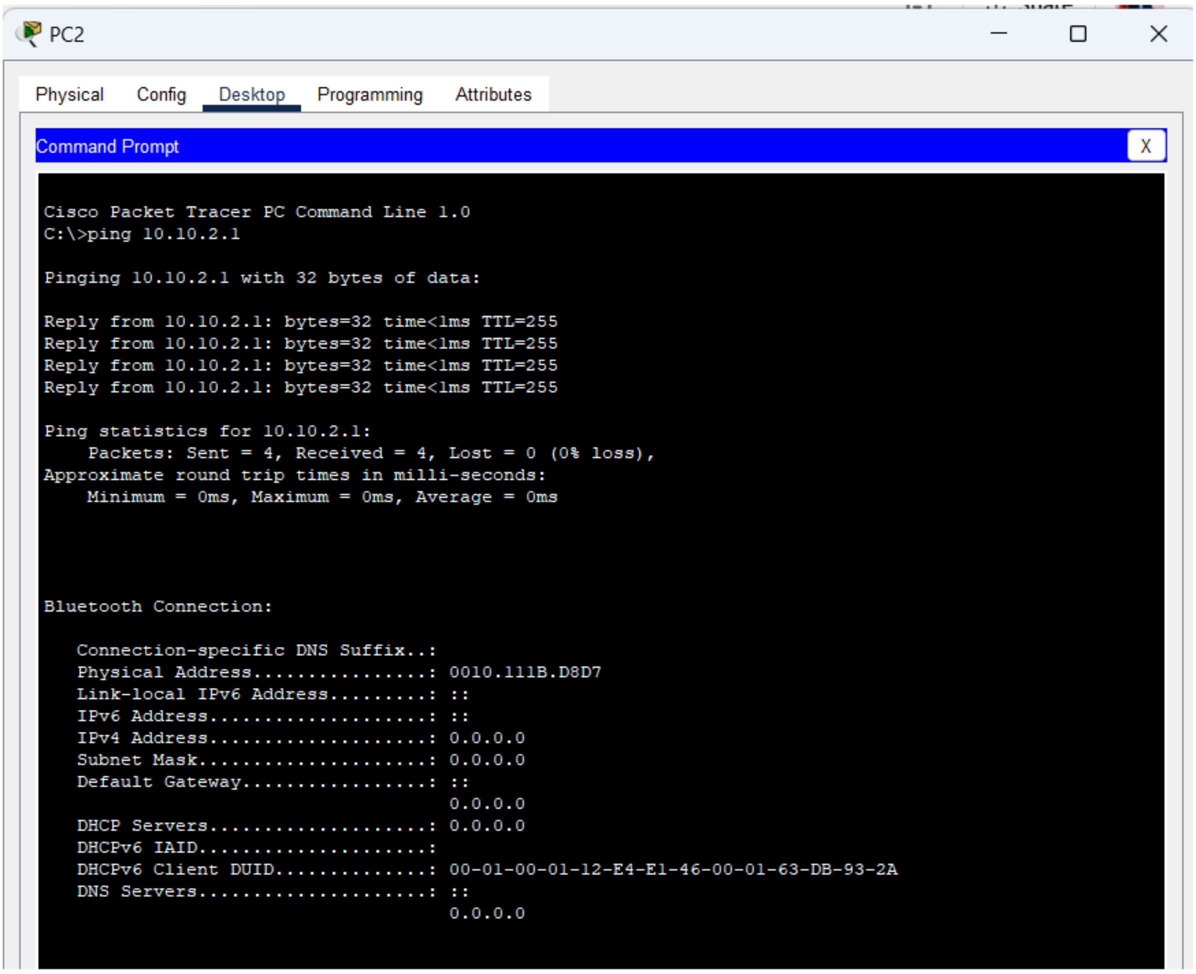
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.2.1

Pinging 10.10.2.1 with 32 bytes of data:

Reply from 10.10.2.1: bytes=32 time=1ms TTL=255
Reply from 10.10.2.1: bytes=32 time=6ms TTL=255
Reply from 10.10.2.1: bytes=32 time<1ms TTL=255
Reply from 10.10.2.1: bytes=32 time=1ms TTL=255

Ping statistics for 10.10.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 2ms

C:\>arp -a
  Internet Address      Physical Address      Type
  10.10.2.1             0003.e434.db01        dynamic
```

ARP TABLE of PC1:



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.2.1

Pinging 10.10.2.1 with 32 bytes of data:

Reply from 10.10.2.1: bytes=32 time<1ms TTL=255
Reply from 10.10.2.1: bytes=32 time<1ms TTL=255
Reply from 10.10.2.1: bytes=32 time<1ms TTL=255
Reply from 10.10.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.2.1:
    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
  10.10.2.1             0003.e434.db01        dynamic

C:\>
```

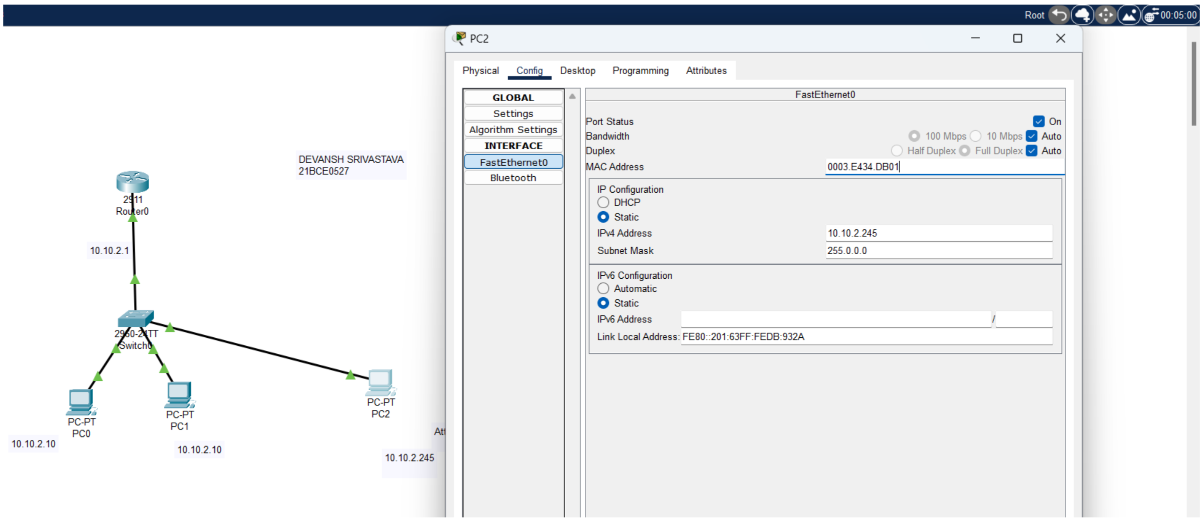
MAC Address of attacker



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.2.1

Pinging 10.10.2.1 with 32 bytes of data:

Reply from 10.10.2.1: bytes=32 time<1ms TTL=255
Reply from 10.10.2.1: bytes=32 time<1ms TTL=255
Reply from 10.10.2.1: bytes=32 time<1ms TTL=255
Reply from 10.10.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms




Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 0010.111B.D8D7
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-12-E4-E1-46-00-01-63-DB-93-2A
   DNS Servers.....................: ::
                                     0.0.0.0
```

Attacker Spoofing the ARP Request:

Now we will spoof the mac address of Router and use it as Attacker MAC address



FastEthernet0

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0003.E434.DB01

IP Configuration

○ DHCP

● Static

IPv4 Address 10.10.2.245

Subnet Mask 255.0.0.0

IPv6 Configuration

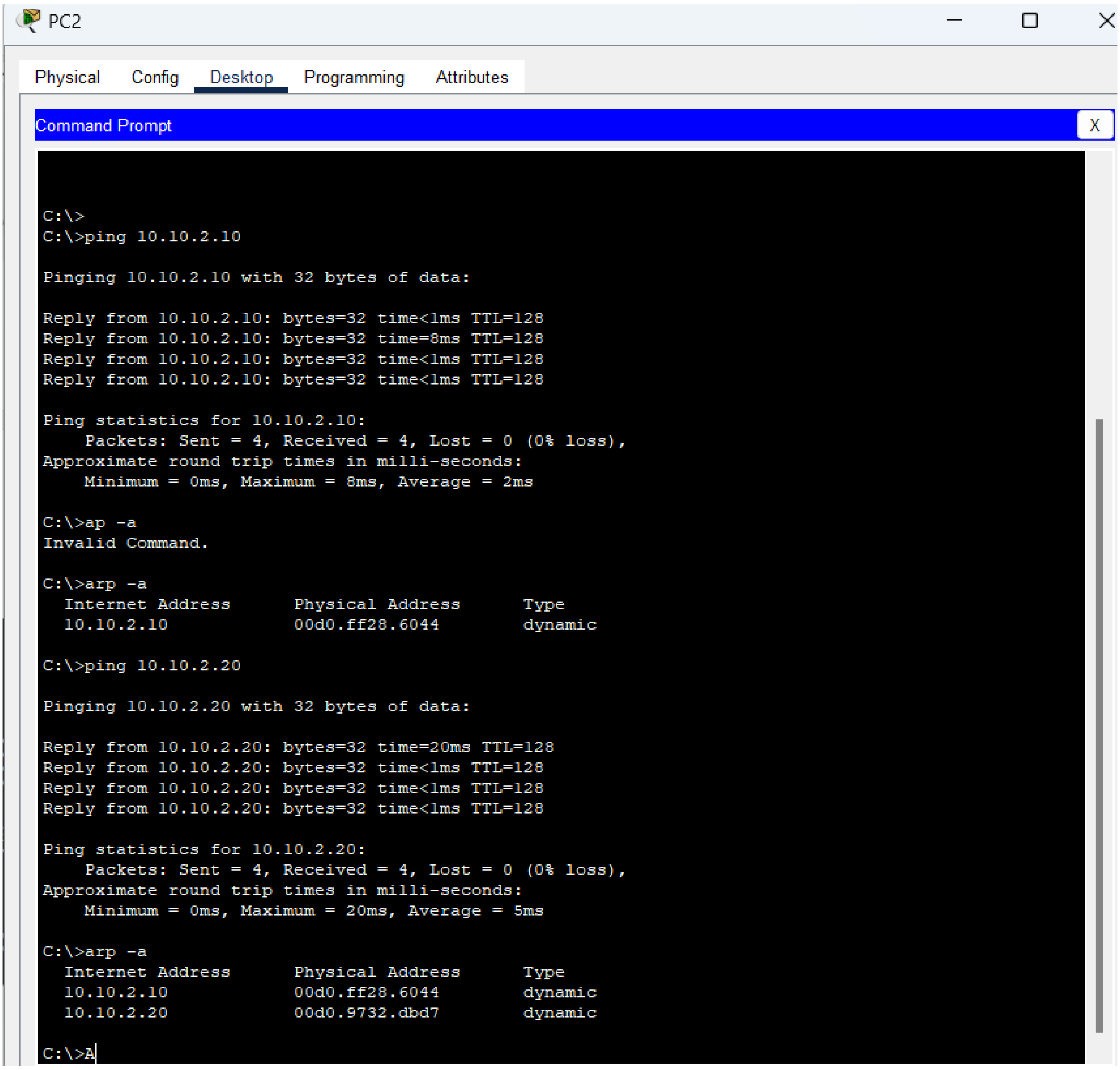
○ Automatic

● Static

IPv6 Address /

Link Local Address: FE80::201:63FF:FEDB:932A

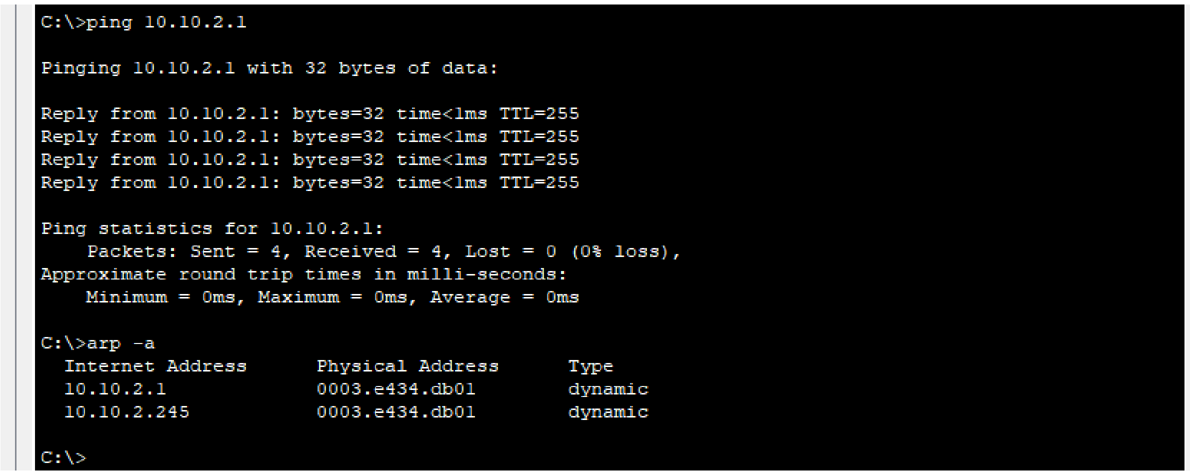
Now attacker send the packet to PC0 and PC1
 and get to know their physical Address(MAC Address)



```
C:\>
C:\>ping 10.10.2.10

Pinging 10.10.2.10 with 32 bytes of data:

Reply from 10.10.2.10: bytes=32 time<1ms TTL=128
Reply from 10.10.2.10: bytes=32 time=8ms TTL=128
Reply from 10.10.2.10: bytes=32 time<1ms TTL=128
Reply from 10.10.2.10: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 8ms, Average = 2ms

C:\>ap -a
Invalid Command.

C:\>arp -a
  Internet Address      Physical Address      Type
  10.10.2.10            00d0.ff28.6044        dynamic

C:\>ping 10.10.2.20

Pinging 10.10.2.20 with 32 bytes of data:

Reply from 10.10.2.20: bytes=32 time=20ms TTL=128
Reply from 10.10.2.20: bytes=32 time<1ms TTL=128
Reply from 10.10.2.20: bytes=32 time<1ms TTL=128
Reply from 10.10.2.20: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.2.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 20ms, Average = 5ms

C:\>arp -a
  Internet Address      Physical Address      Type
  10.10.2.10            00d0.ff28.6044        dynamic
  10.10.2.20            00d0.9732.dbd7        dynamic

C:\>A
```

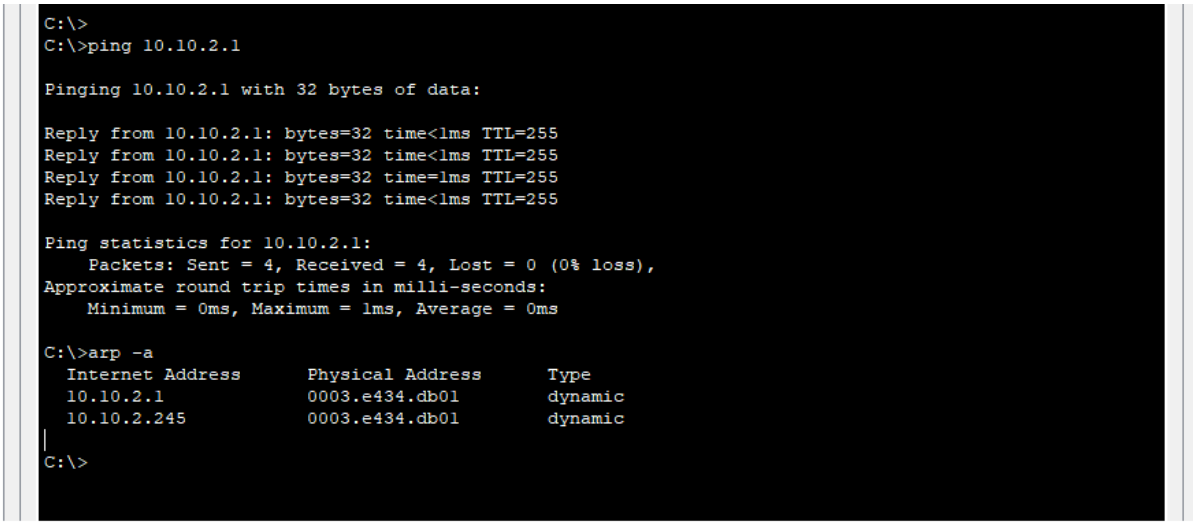
Now PC0 And PC1 ARP Table will show Attacker’s physical address when the ping to router in their ARP table

PC0:



```
C:\>ping 10.10.2.1

Pinging 10.10.2.1 with 32 bytes of data:

Reply from 10.10.2.1: bytes=32 time<1ms TTL=255
Reply from 10.10.2.1: bytes=32 time<1ms TTL=255
Reply from 10.10.2.1: bytes=32 time<1ms TTL=255
Reply from 10.10.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.2.1:
    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
  10.10.2.1             0003.e434.db01        dynamic
  10.10.2.245           0003.e434.db01        dynamic

C:\>
```

PC1:



```
C:\>
C:\>ping 10.10.2.1

Pinging 10.10.2.1 with 32 bytes of data:

Reply from 10.10.2.1: bytes=32 time<1ms TTL=255
Reply from 10.10.2.1: bytes=32 time<1ms TTL=255
Reply from 10.10.2.1: bytes=32 time=1ms TTL=255
Reply from 10.10.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>arp -a
  Internet Address      Physical Address      Type
  10.10.2.1             0003.e434.db01        dynamic
  10.10.2.245           0003.e434.db01        dynamic

C:\>
```

Key Learning:

1. Victim PCs update their ARP cache with fake MAC addresses.
2. Attacker can intercept, modify, or drop packets.
3. ARP spoofing is possible because ARP does not require authentication.