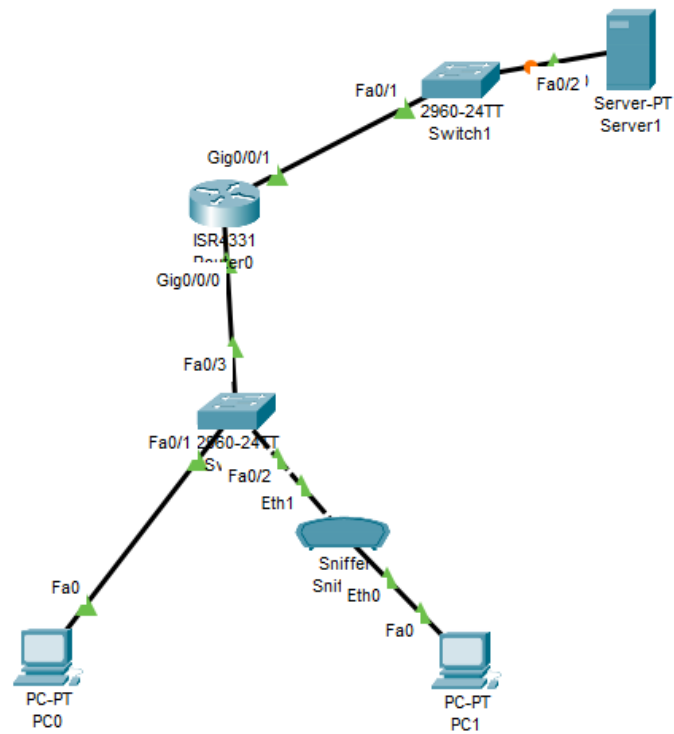


Name: J Kevin Immanuel

College: VIT Chennai

Q2) ARP Spoofing



We will be using the above network to simulate an ARP Spoofing attack.

First, let us see the ipconfig of regular user.

```
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Physical Address. . . . .: 0002.4A95.6E5B
    Link-local IPv6 Address . . . . .: FE80::202:4AFF:FE95:6E5B
    IPv6 Address. . . . .: ::
    IPv4 Address. . . . .: 192.168.1.10
    Subnet Mask. . . . .: 255.255.255.0
    Default Gateway. . . . .: ::
                                192.168.1.254
    DHCP Servers. . . . .: 0.0.0.0
    DHCPv6 IAID. . . . .:
    DHCPv6 Client DUID. . . . .: 00-01-00-01-C5-8C-76-3E-00-02-4A-95-6E-5B
    DNS Servers. . . . .: ::
                                0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Physical Address. . . . .: 0006.2AEA.743A
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address. . . . .: ::
    IPv4 Address. . . . .: 0.0.0.0
    Subnet Mask. . . . .: 0.0.0.0

C:\>
C:\>arp -a
No ARP Entries Found
C:\>
```

According to the output, the user computer knows the IP address of the default gateway, but the arp entry is empty. So, we will perform a ping to the server to fill up the entry.

```
No ARP Entries Found
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=8ms 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 = 8ms, Average = 2ms

C:\>
C:\>
C:\>
C:\>arp -a
    Internet Address      Physical Address        Type
    192.168.1.254         0010.1173.d001         dynamic

C:\>
```

Now, the user computer has knowledge about the default gateway MAC Address.

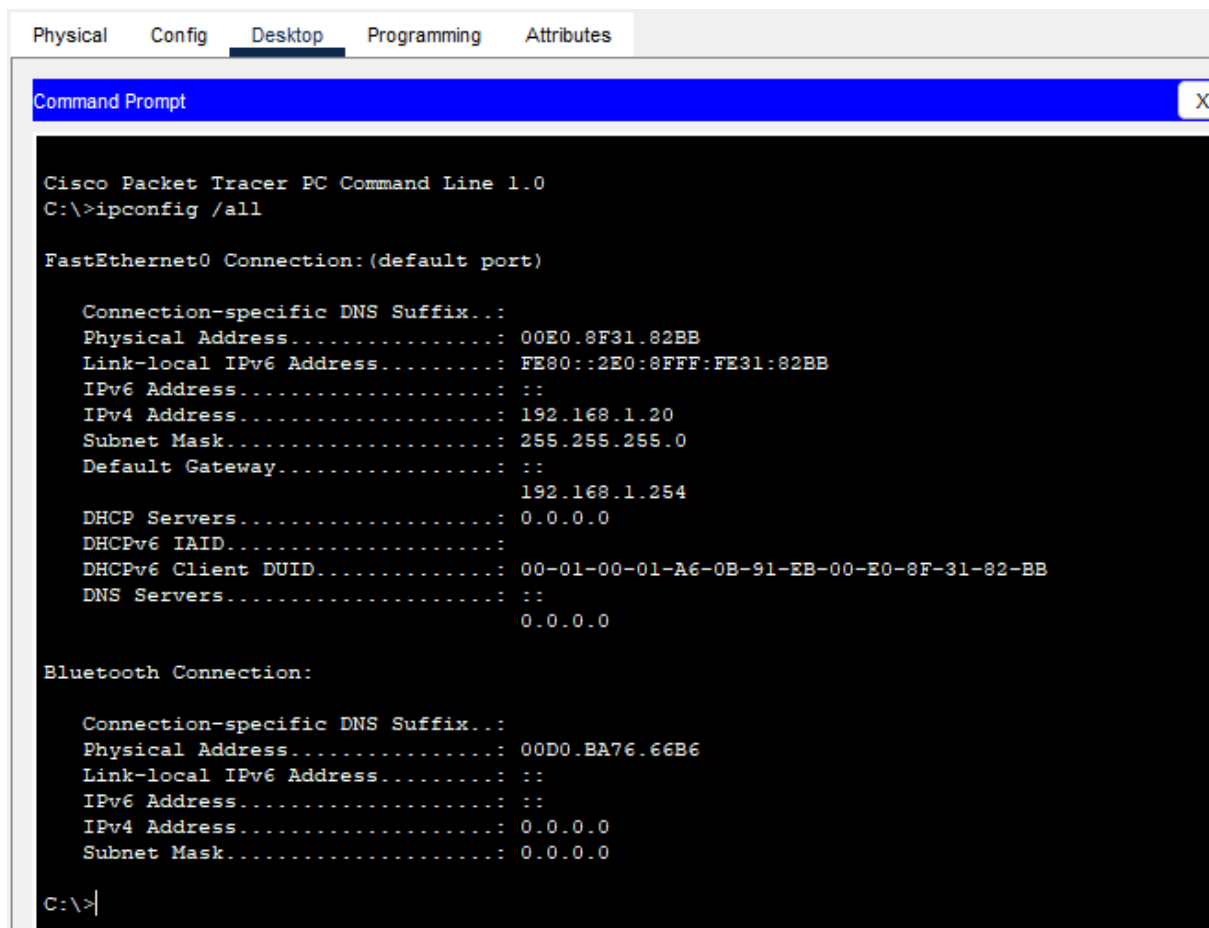
Let us also visit the http website of the webserver.



It works properly.

Now, let us create a MITM attack.

We will use the second computer as the attacker's PC



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Physical Address. . . . .: 00E0.8F31.82BB
    Link-local IPv6 Address . . . . .: FE80::2E0:8FFF:FE31:82BB
    IPv6 Address. . . . .: ::
    IPv4 Address. . . . .: 192.168.1.20
    Subnet Mask. . . . .: 255.255.255.0
    Default Gateway. . . . .: ::
                                192.168.1.254
    DHCP Servers. . . . .: 0.0.0.0
    DHCPv6 IAID. . . . .:
    DHCPv6 Client DUID. . . . .: 00-01-00-01-A6-0B-91-EB-00-E0-8F-31-82-BB
    DNS Servers. . . . .: ::
                                0.0.0.0

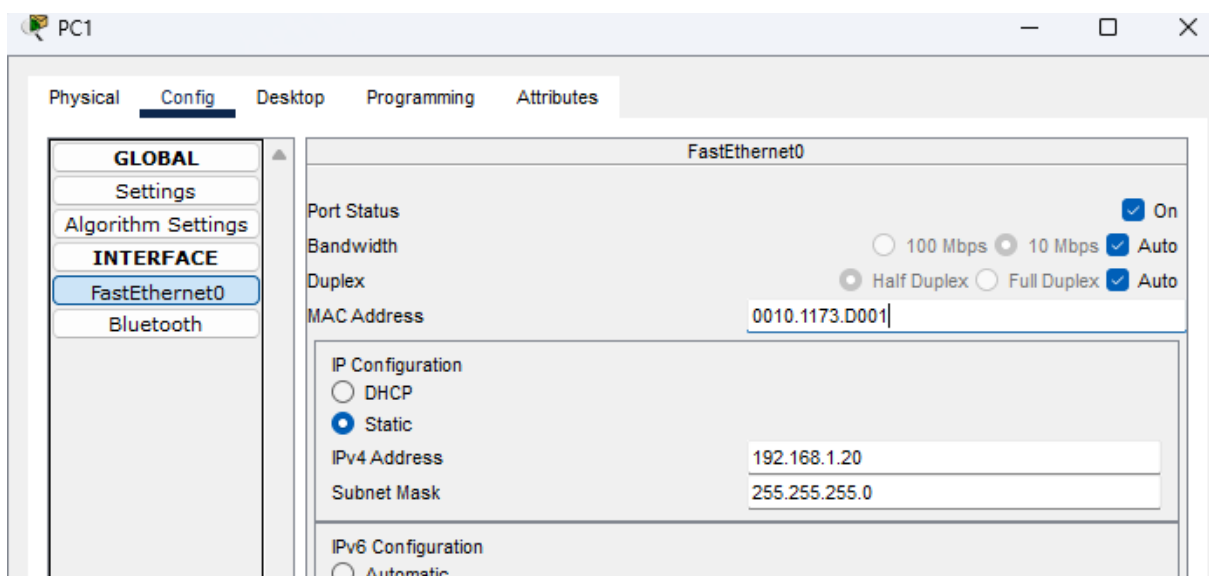
Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Physical Address. . . . .: 00D0.BA76.66B6
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address. . . . .: ::
    IPv4 Address. . . . .: 0.0.0.0
    Subnet Mask. . . . .: 0.0.0.0

C:\>
```

The second computer has an IP address, a MAC address of 00E0.8F31.82BB and knows the IP of the default gateway.

Now, we will change the MAC address of the attacker to be the MAC address of the default gateway.



We have changed the attacker's MAC address to be the same as the default gateway's MAC Address.

Now, we will ping the user PC, to update its arp cache

Pinging PC0:

```
C:\>
C:\>
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time=6ms TTL=128
Reply from 192.168.1.10: bytes=32 time=12ms TTL=128
Reply from 192.168.1.10: bytes=32 time=6ms TTL=128

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 6ms
```

Let us check the arp cache of the user pc:

```
C:\>
C:\>
C:\>arp -a

Internet Address      Physical Address      Type
192.168.1.20          0010.1173.d001        dynamic
192.168.1.254         0010.1173.d001        dynamic
```

Notice that now we have two devices, one being the default gateway and the other is the attacker. Notice that the MAC address is same, but IP is different.

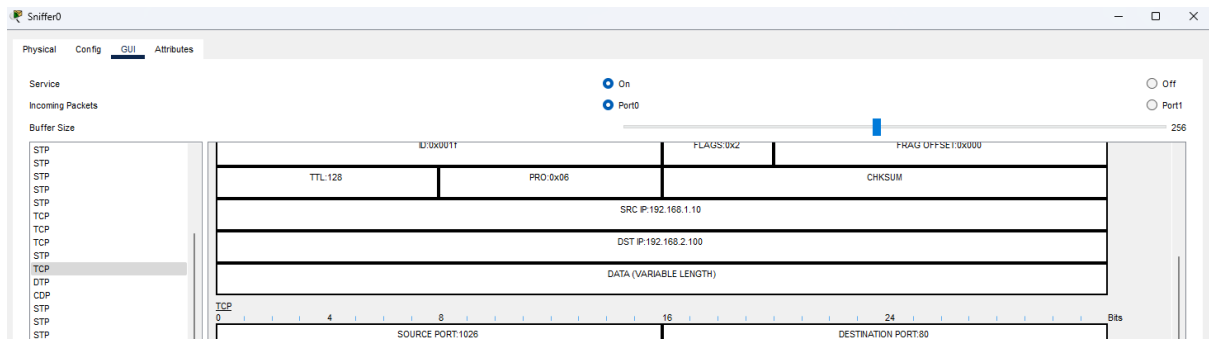
Let's verify the MAC address table of the switch.

```
Switch>
Switch>en
Switch#show mac-address-table dynamic

Mac Address Table
-----
Vlan    Mac Address      Type        Ports
----    -
1       0002.4a95.6e5b   DYNAMIC     Fa0/1
1       0010.1173.d001   DYNAMIC     Fa0/3
Switch#
```

The MAC address table has been updated with the gateway's MAC address in the attacker PC.

Now what happens when the user PC tries to access the web server?



The attacker gets the TCP requests from User PC and can view every data sent from the user.

