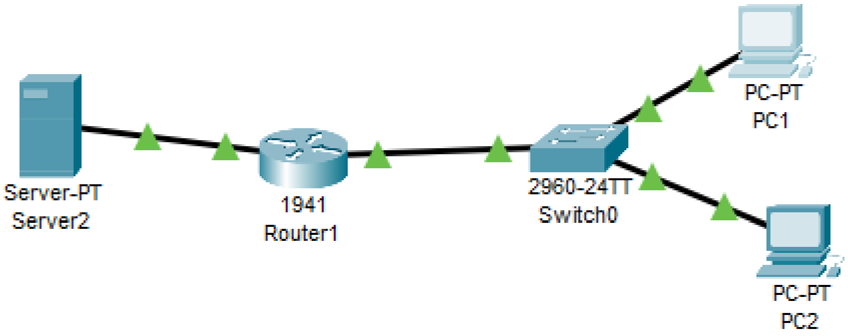
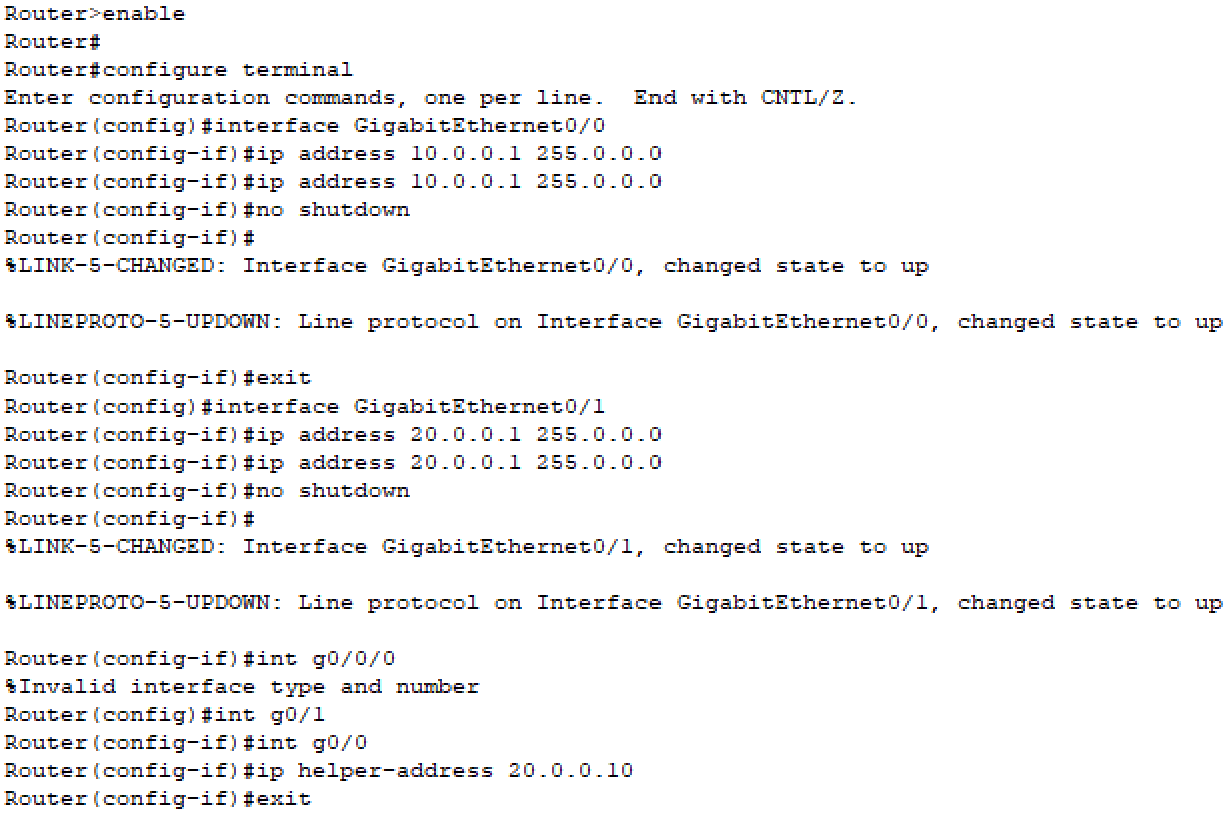
Rogue DHCP server attack:

1. Rogues DHCP server is a Man-in-the-Middle attacker server. If an attacker is able to bring up a DHCP server on a machine in the same subnet as that same client PC. When the client broadcasts its DHCP request and tries to go through the DORA process, the rogue server could make a carefully crafted DHCP reply where its own IP address is in the default gateway field. Making the client use the rogue DHCP server as the default gateway and router all it's layer 3 and above traffic through it. The attacker can forward the packets to the correct destination, and examine every packet that it intercepts.
2. Demo:

Company Network Topology:

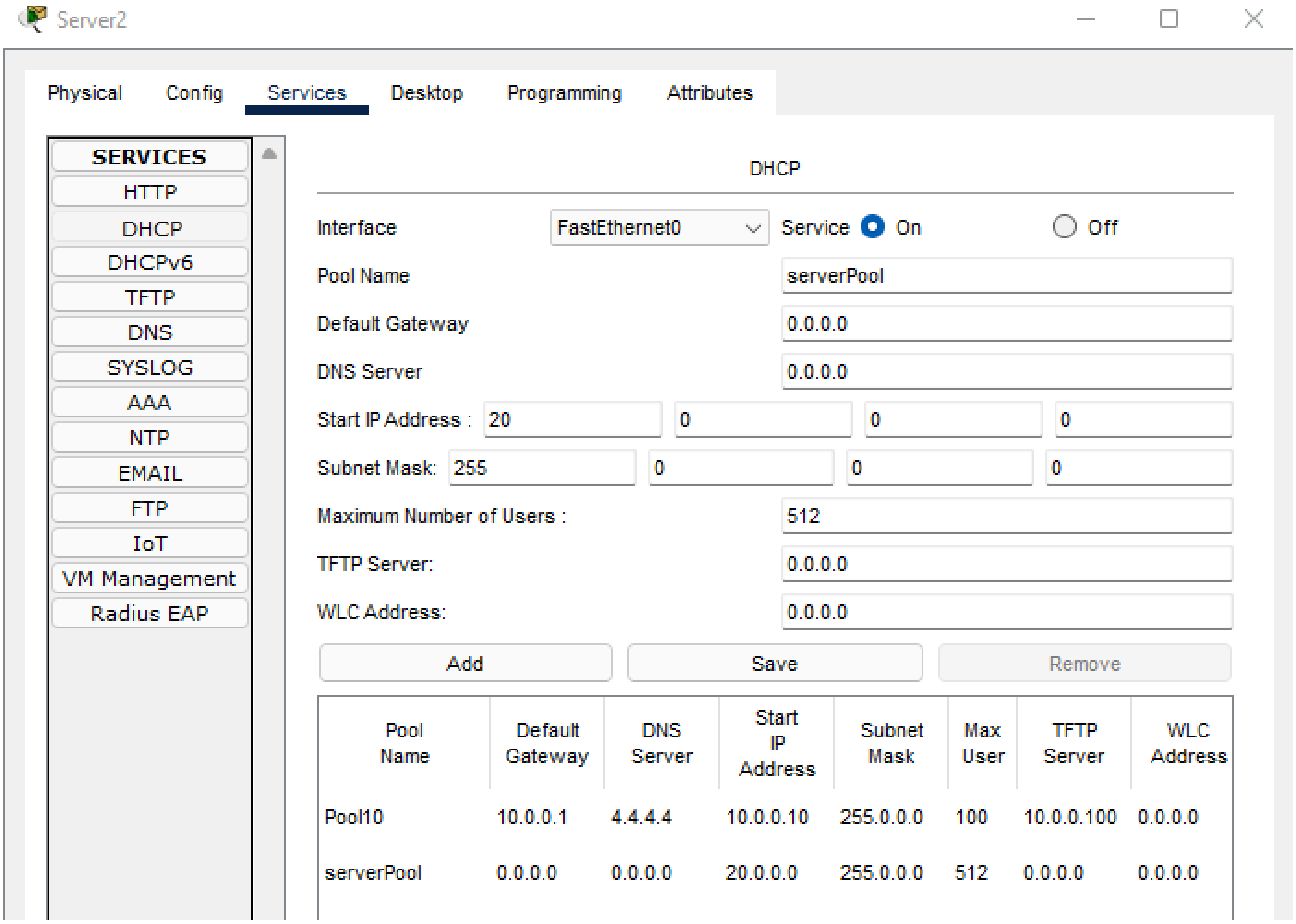


Router Configuration:



```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip address 20.0.0.1 255.0.0.0
Router(config-if)#ip address 20.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Router(config-if)#int g0/0/0
%Invalid interface type and number
Router(config)#int g0/1
Router(config-if)#int g0/0
Router(config-if)#ip helper-address 20.0.0.10
Router(config-if)#exit
```

Company DHCP Configuration:



DHCP

Interface: FastEthernet0 Service ● On ○ Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Start IP Address : 20 0 0 0

Subnet Mask: 255 0 0 0

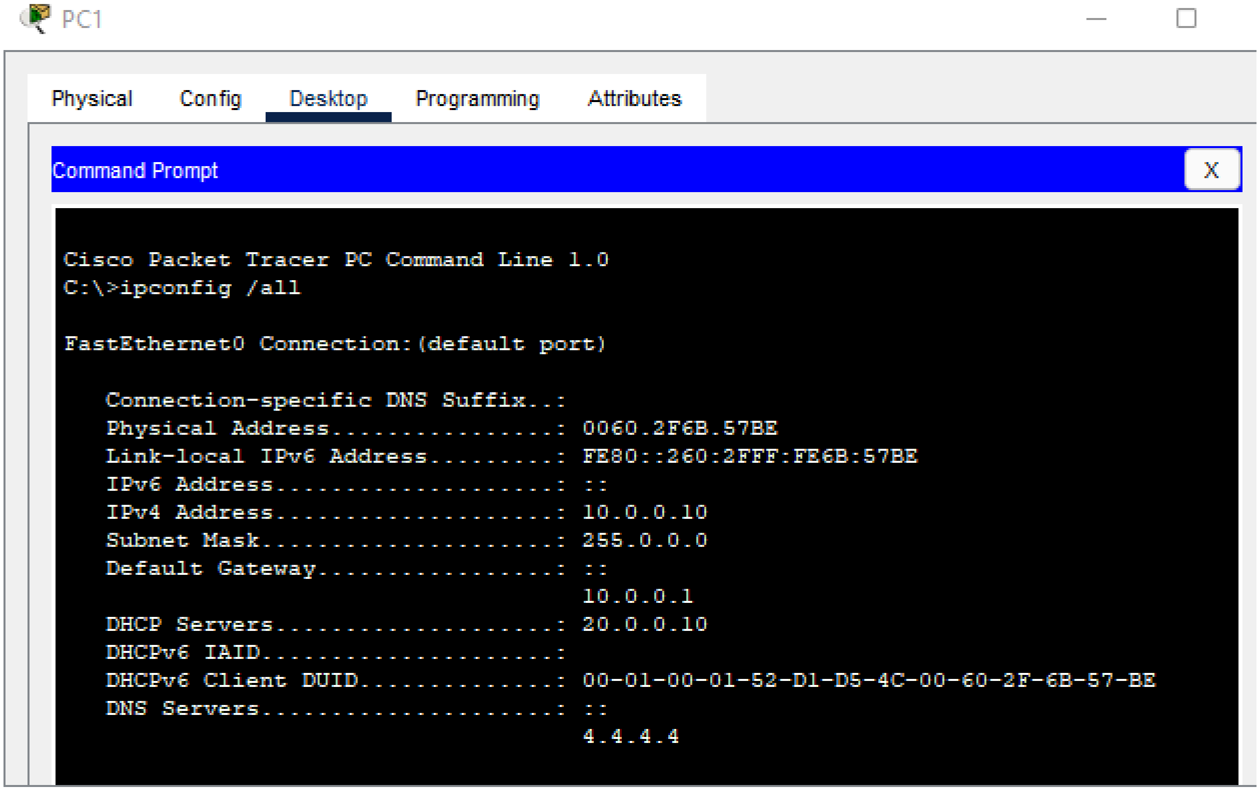
Maximum Number of Users : 512

TFTP Server: 0.0.0.0

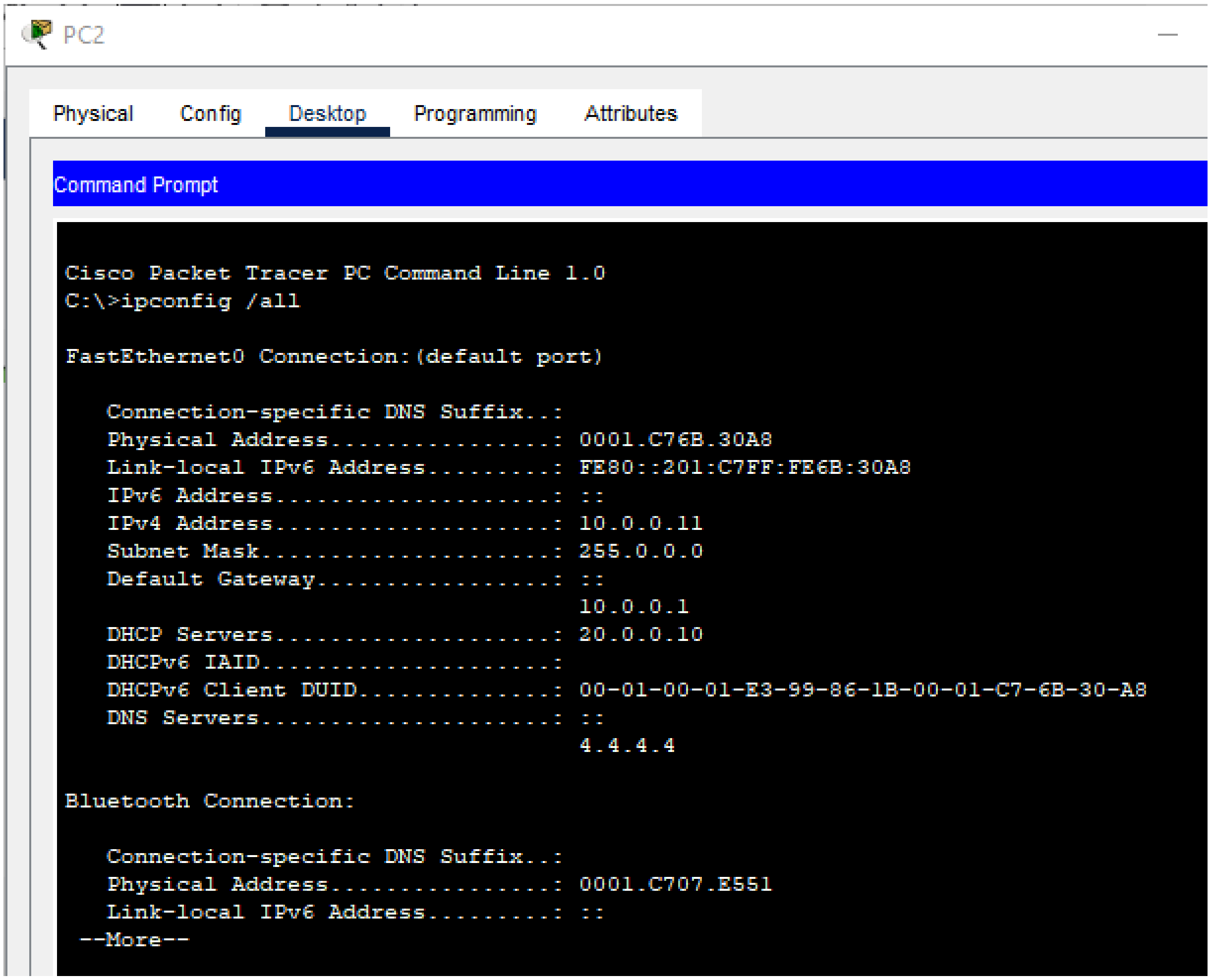
WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Pool10	10.0.0.1	4.4.4.4	10.0.0.10	255.0.0.0	100	10.0.0.100	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	20.0.0.0	255.0.0.0	512	0.0.0.0	0.0.0.0

PCs receiving IP through DHCP normally:

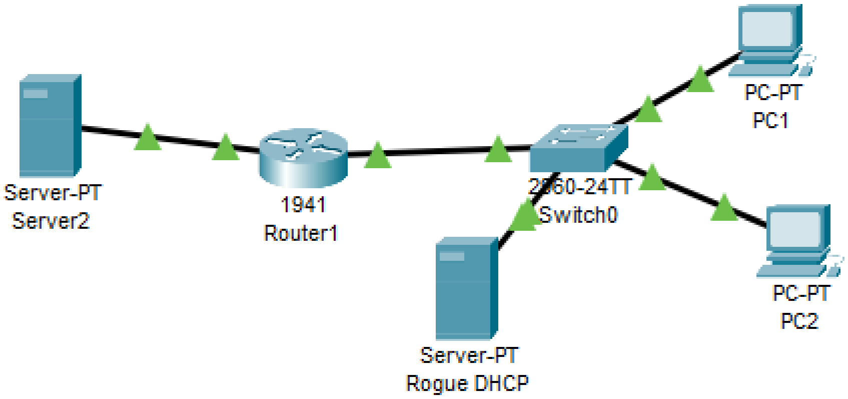


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0060.2F6B.57BE
   Link-local IPv6 Address.........: FE80::260:2FFF:FE6B:57BE
   IPv6 Address....................: ::
   IPv4 Address....................: 10.0.0.10
   Subnet Mask.....................: 255.0.0.0
   Default Gateway.................: ::
                                     10.0.0.1
   DHCP Servers....................: 20.0.0.10
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-52-D1-D5-4C-00-60-2F-6B-57-BE
   DNS Servers.....................: ::
                                     4.4.4.4
```

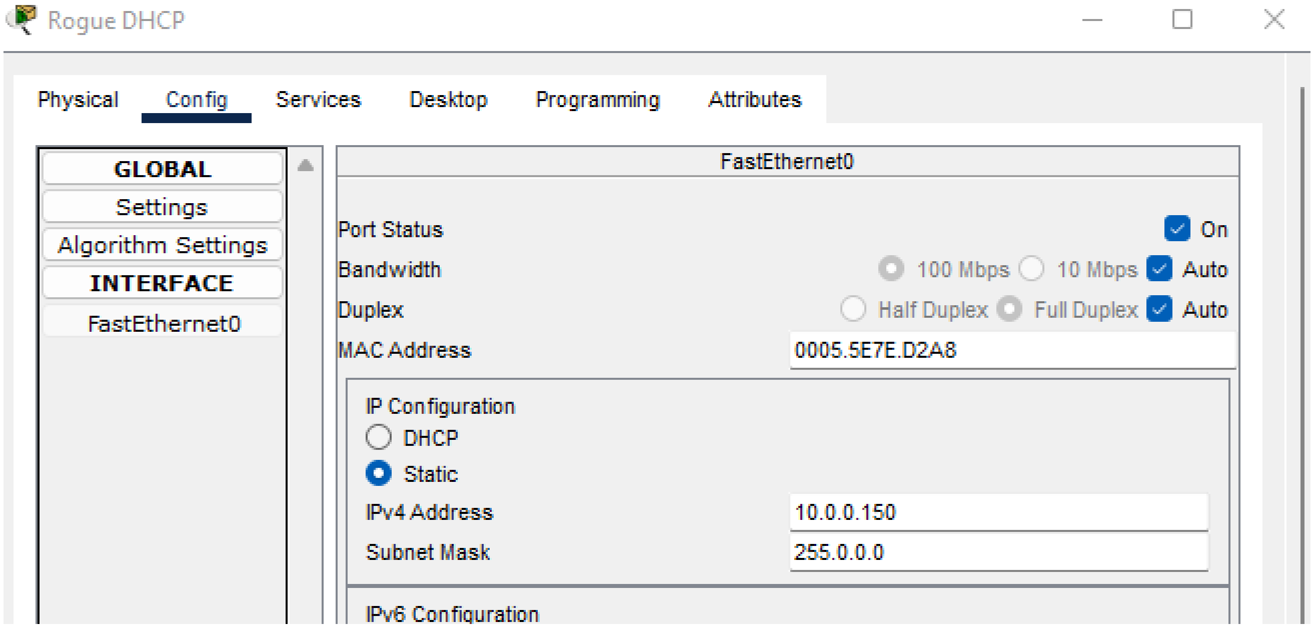


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0001.C76B.30A8
   Link-local IPv6 Address.........: FE80::201:C7FF:FE6B:30A8
   IPv6 Address....................: ::
   IPv4 Address....................: 10.0.0.11
   Subnet Mask.....................: 255.0.0.0
   Default Gateway.................: ::
                                     10.0.0.1
   DHCP Servers....................: 20.0.0.10
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-E3-99-86-1B-00-01-C7-6B-30-A8
   DNS Servers.....................: ::
                                     4.4.4.4

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 0001.C707.E551
   Link-local IPv6 Address.........: ::
 --More--
```

Now lets add the Rogue DHCP server to the topology:



Rogues DHCP configuration:



FastEthernet0

Port Status ☑ On

Bandwidth ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ○ Full Duplex ☑ Auto

MAC Address 0005.5E7E.D2A8

IP Configuration

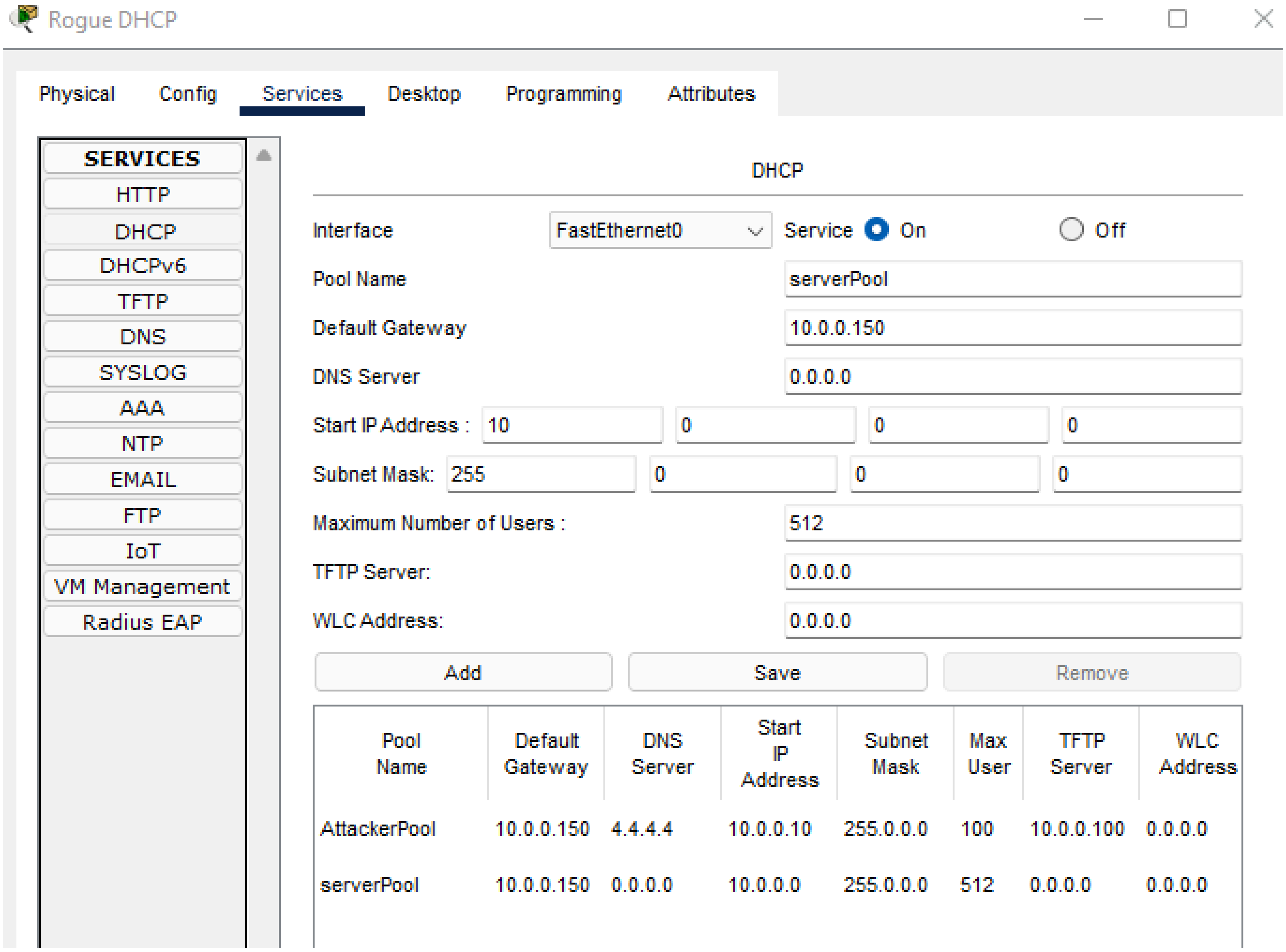
○ DHCP

● Static

IPv4 Address 10.0.0.150

Subnet Mask 255.0.0.0

IPv6 Configuration



DHCP

Interface FastEthernet0 Service ● On ○ Off

Pool Name serverPool

Default Gateway 10.0.0.150

DNS Server 0.0.0.0

Start IP Address : 10 0 0 0

Subnet Mask: 255 0 0 0

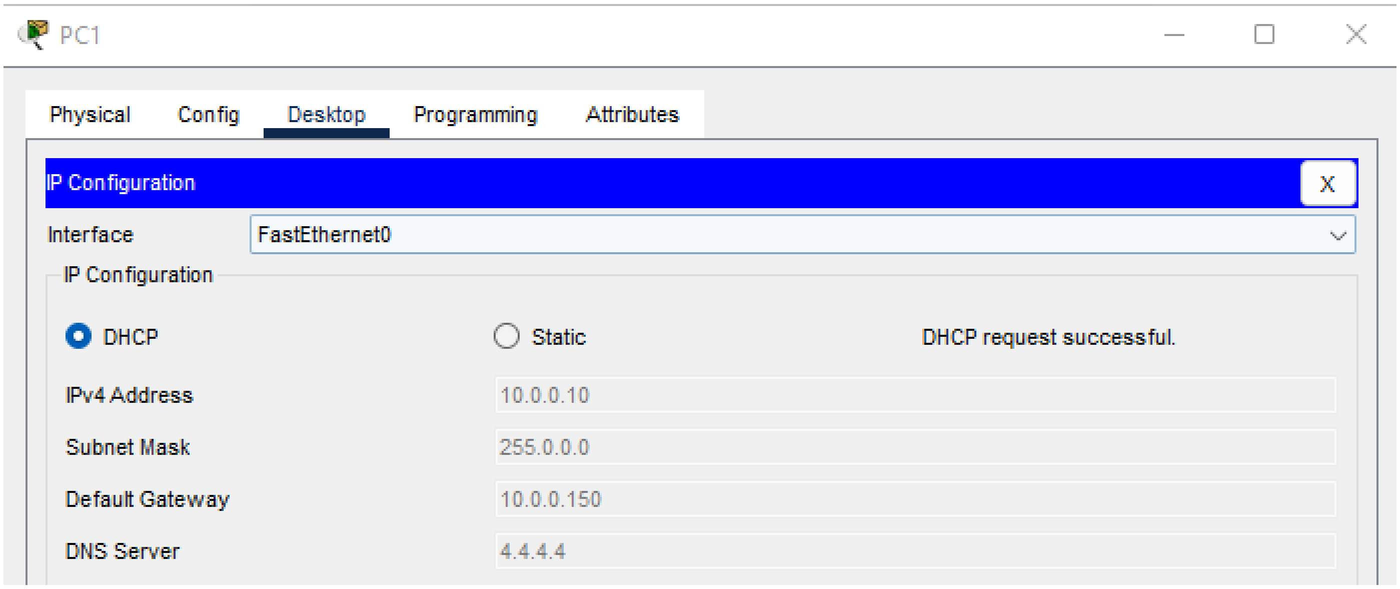
Maximum Number of Users : 512

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
AttackerPool	10.0.0.150	4.4.4.4	10.0.0.10	255.0.0.0	100	10.0.0.100	0.0.0.0
serverPool	10.0.0.150	0.0.0.0	10.0.0.0	255.0.0.0	512	0.0.0.0	0.0.0.0

After switching between static and DHCP in the Configuration of the PC. The PC is getting an IP from the Rogue DHCP server and setting it’s default gateway as the ip address of the Rogue DHCP server.



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address: 10.0.0.10

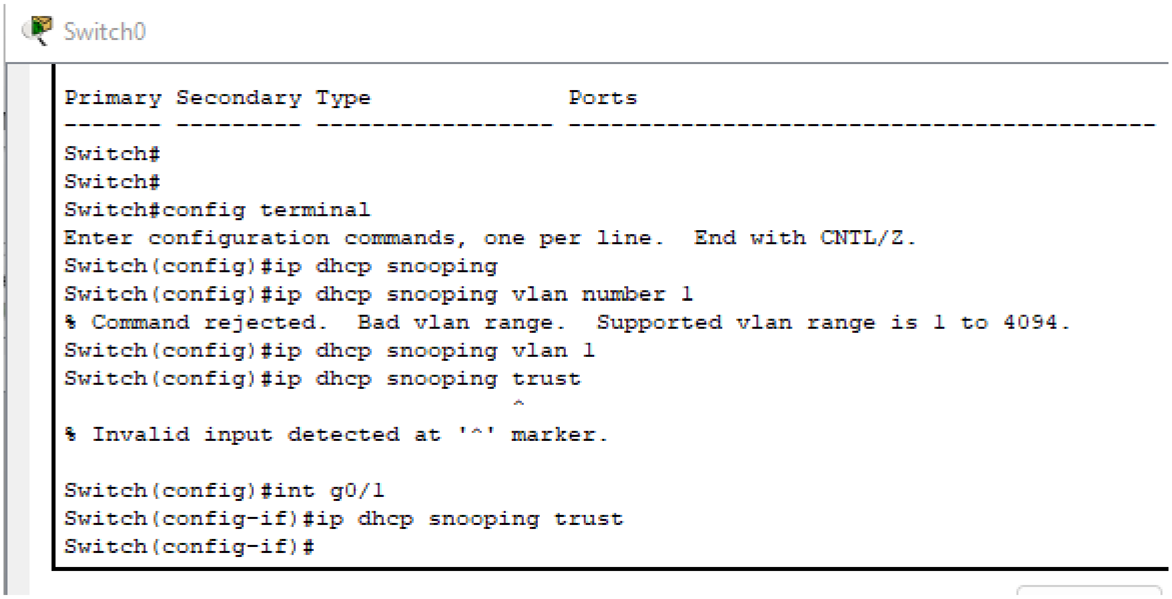
Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.150

DNS Server: 4.4.4.4

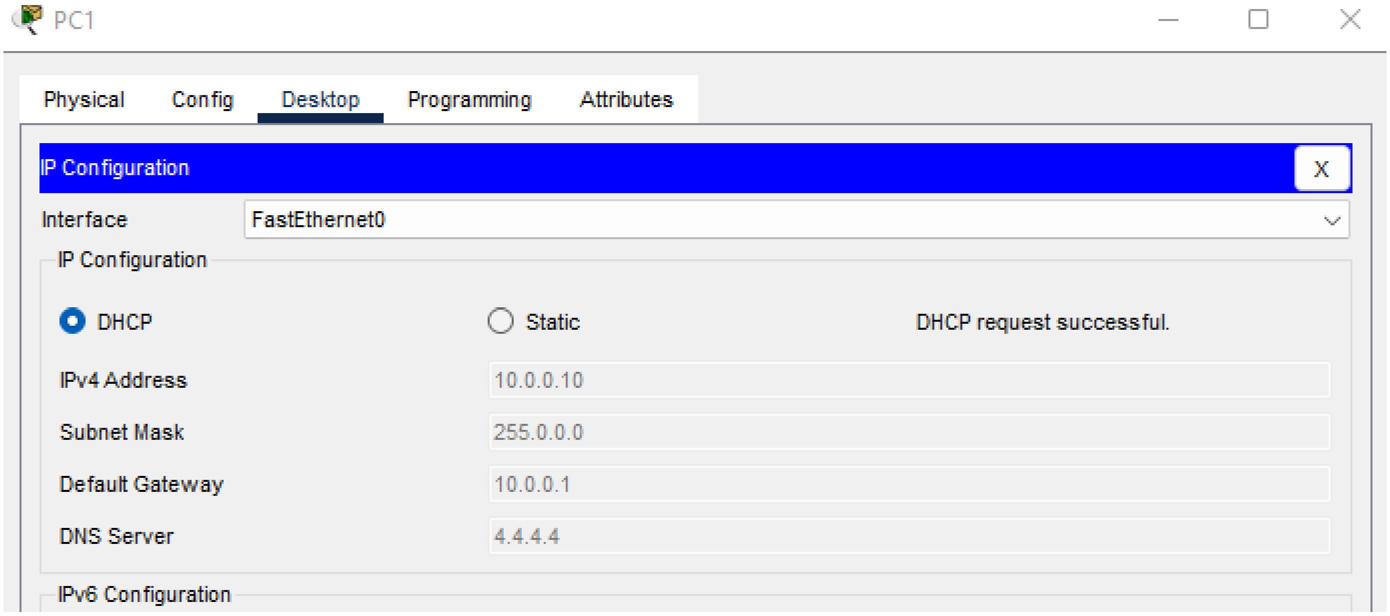
3. Mitigation through DHCP Snooping

Switch configuration:



```
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
Switch#
Switch#
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan number 1
% Command rejected.  Bad vlan range.  Supported vlan range is 1 to 4094.
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#ip dhcp snooping trust
                                ^
% Invalid input detected at '^' marker.

Switch(config)#int g0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#
```

After switching between static and DHCP configuration the pc finally gets the correct ip address of the default gateway showing that we are successfully able to block traffic from the DHCP server.



PC1

IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address: 10.0.0.10

Subnet Mask: 255.0.0.0

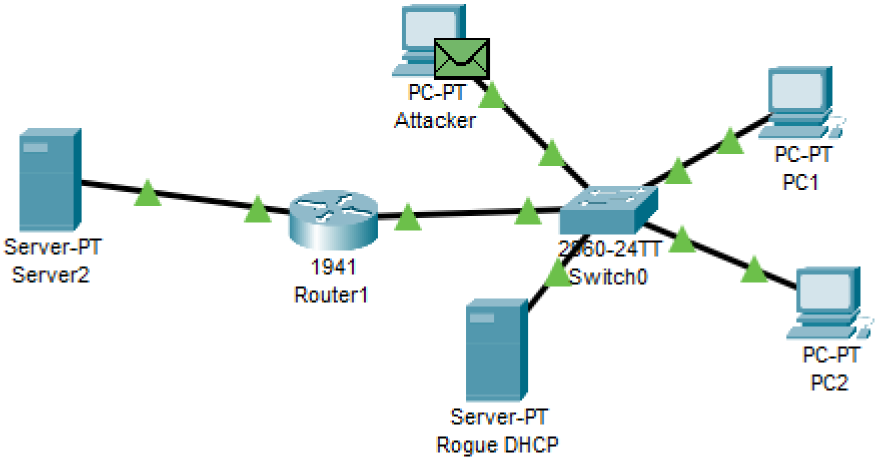
Default Gateway: 10.0.0.1

DNS Server: 4.4.4.4

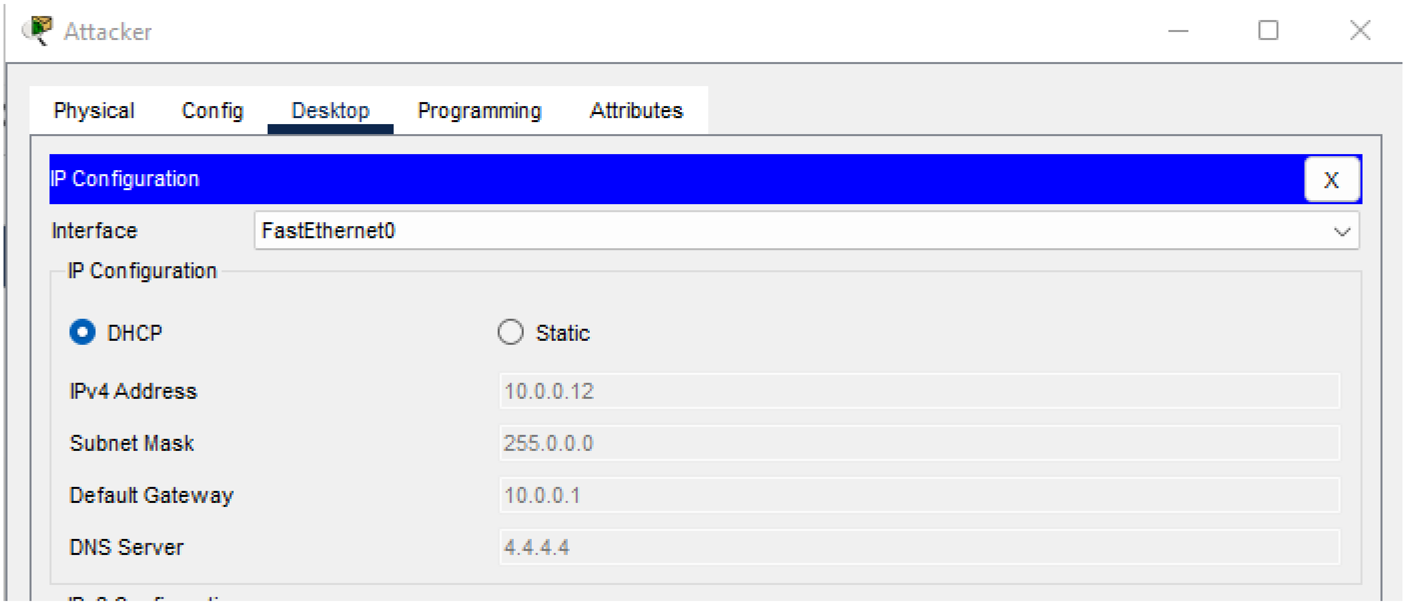
IPv6 Configuration

IP Spoofing:

1. IP Spoofing is when a compromised PC uses legitimate or allowed addresses, or spoofed addresses borrowed from other hosts to disguise themselves for when sending malicious traffic, for example, to DDOS a web server.
2. Demo
   This is the same topology as above except with the attacker machine now.



Lets just say the attacker was able to find the IP address of PC2, for example, by scanning the network. Using a traffic generator I changed the source IP to be from PC2 to destination IP of PC1.



IP Configuration

Interface: FastEthernet0

IP Configuration

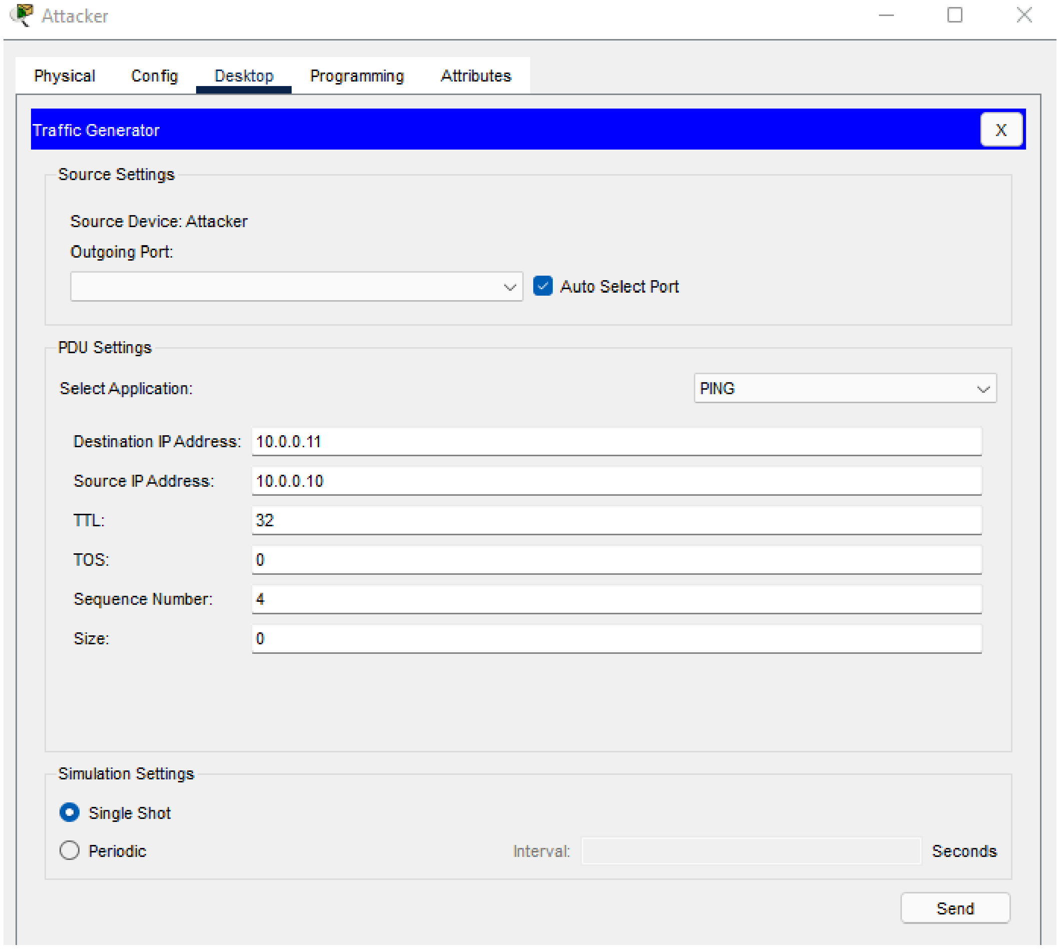
● DHCP ○ Static

IPv4 Address: 10.0.0.12

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server: 4.4.4.4



Traffic Generator

Source Settings

Source Device: Attacker

Outgoing Port:

☑ Auto Select Port

PDU Settings

Select Application: PING

Destination IP Address: 10.0.0.11

Source IP Address: 10.0.0.10

TTL: 32

TOS: 0

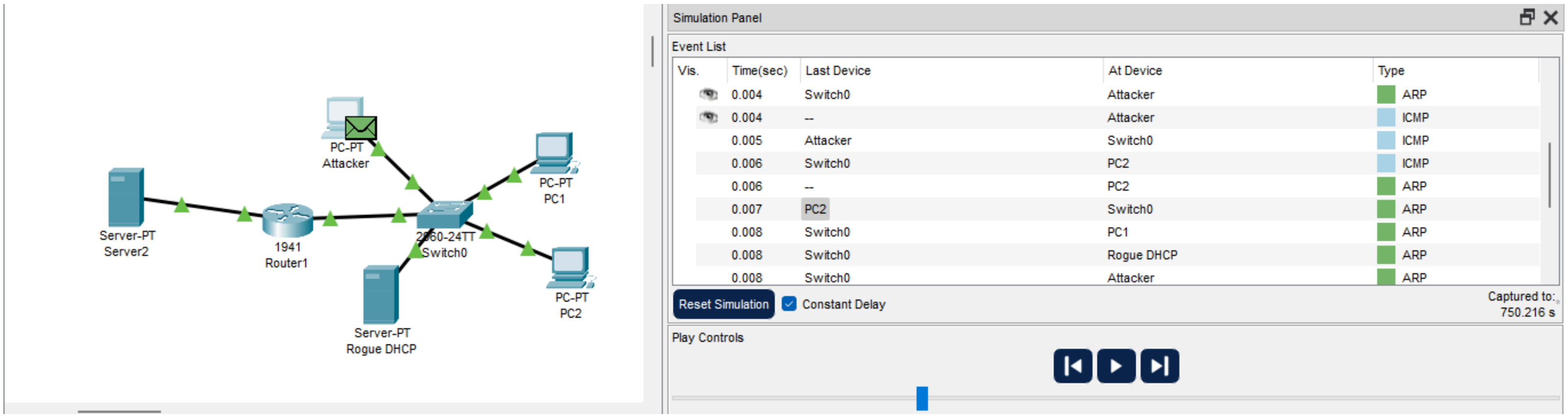
Sequence Number: 4

Size: 0

Simulation Settings

● Single Shot

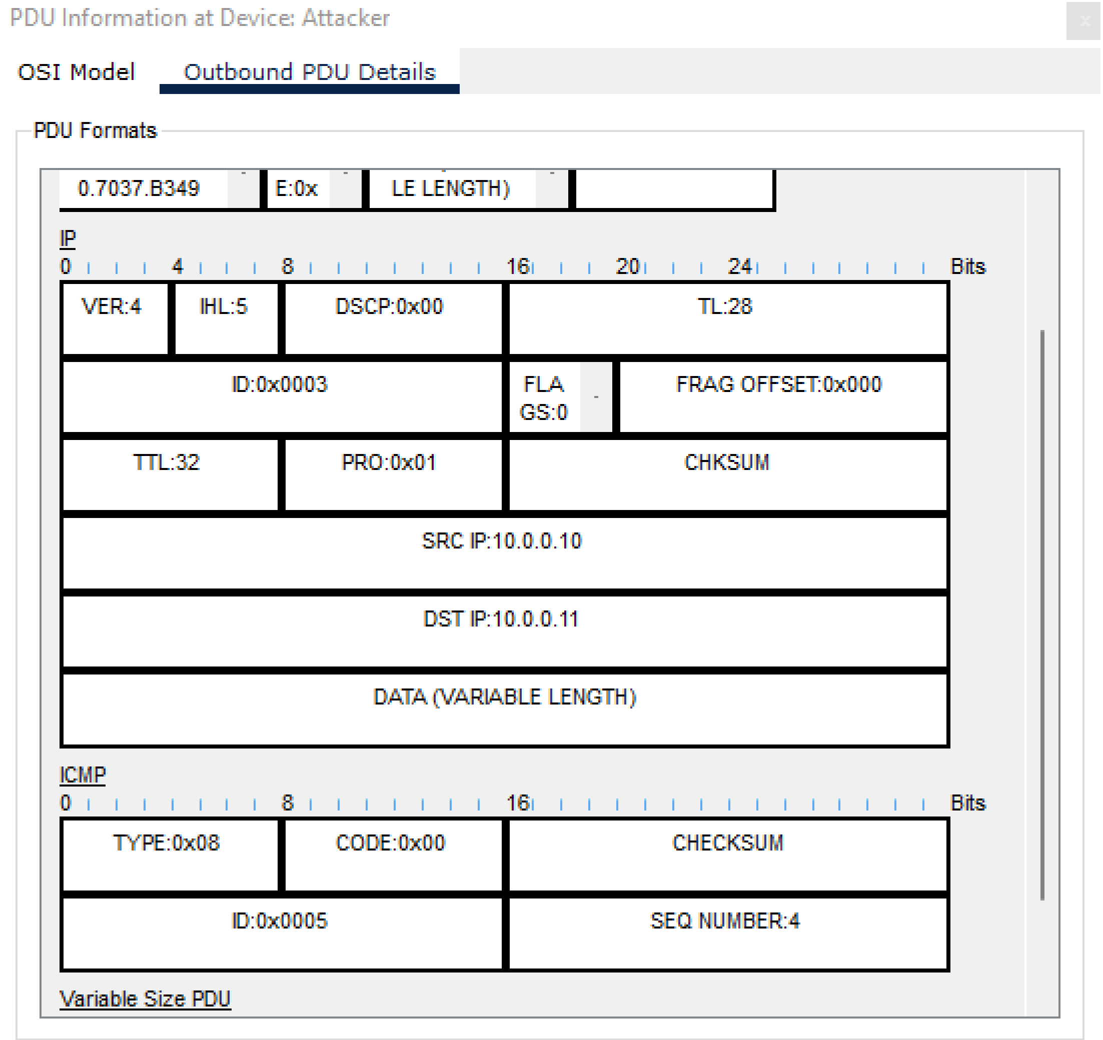
○ Periodic Interval: Seconds



Vis.	Time(sec)	Last Device	At Device	Type
👁	0.004	Switch0	Attacker	🟩 ARP
👁	0.004	--	Attacker	🟦 ICMP
	0.005	Attacker	Switch0	🟦 ICMP
	0.006	Switch0	PC2	🟦 ICMP
	0.006	--	PC2	🟩 ARP
	0.007	PC2	Switch0	🟩 ARP
	0.008	Switch0	PC1	🟩 ARP
	0.008	Switch0	Rogue DHCP	🟩 ARP
	0.008	Switch0	Attacker	🟩 ARP

☑ Constant Delay

Captured to:
750.216 s



PDU Information at Device: Attacker

0.7037.B349	E:0x	LE LENGTH)

IP

0 4 8 16 20 24 Bits

VER:4	IHL:5	DSCP:0x00	TL:28	
ID:0x0003			FLAGS:0	FRAG OFFSET:0x000
TTL:32		PRO:0x01	CHKSUM	
SRC IP:10.0.0.10				
DST IP:10.0.0.11				
DATA (VARIABLE LENGTH)				

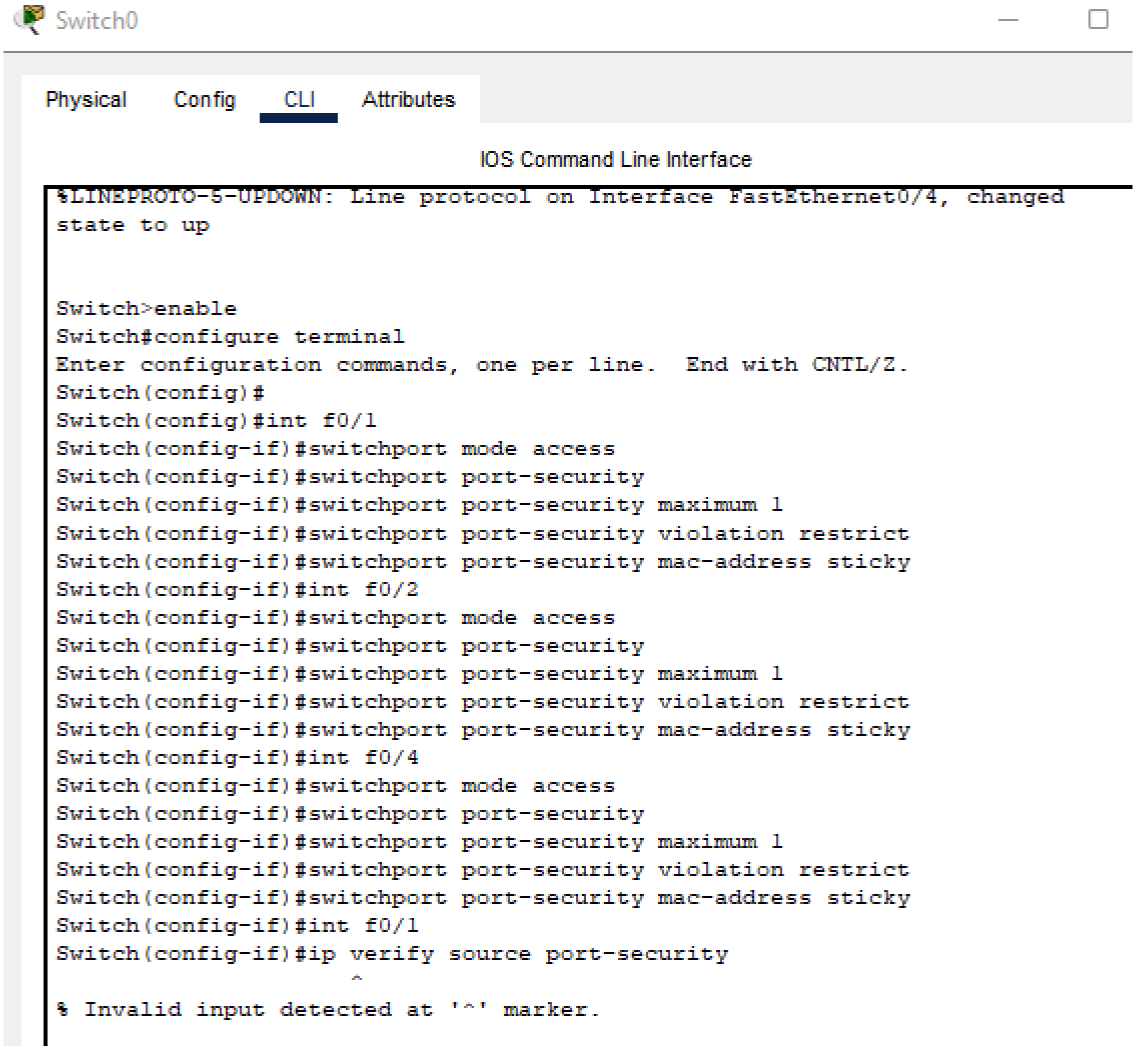
ICMP

0 8 16 Bits

TYPE:0x08	CODE:0x00	CHECKSUM
ID:0x0005		SEQ NUMBER:4

Variable Size PDU

3. Mitigation with IP source guard. However, none of the switches in the packet allow the command “ip verify source” or “ip source verify port-security”. I was just able to turn on port security for all the ports.

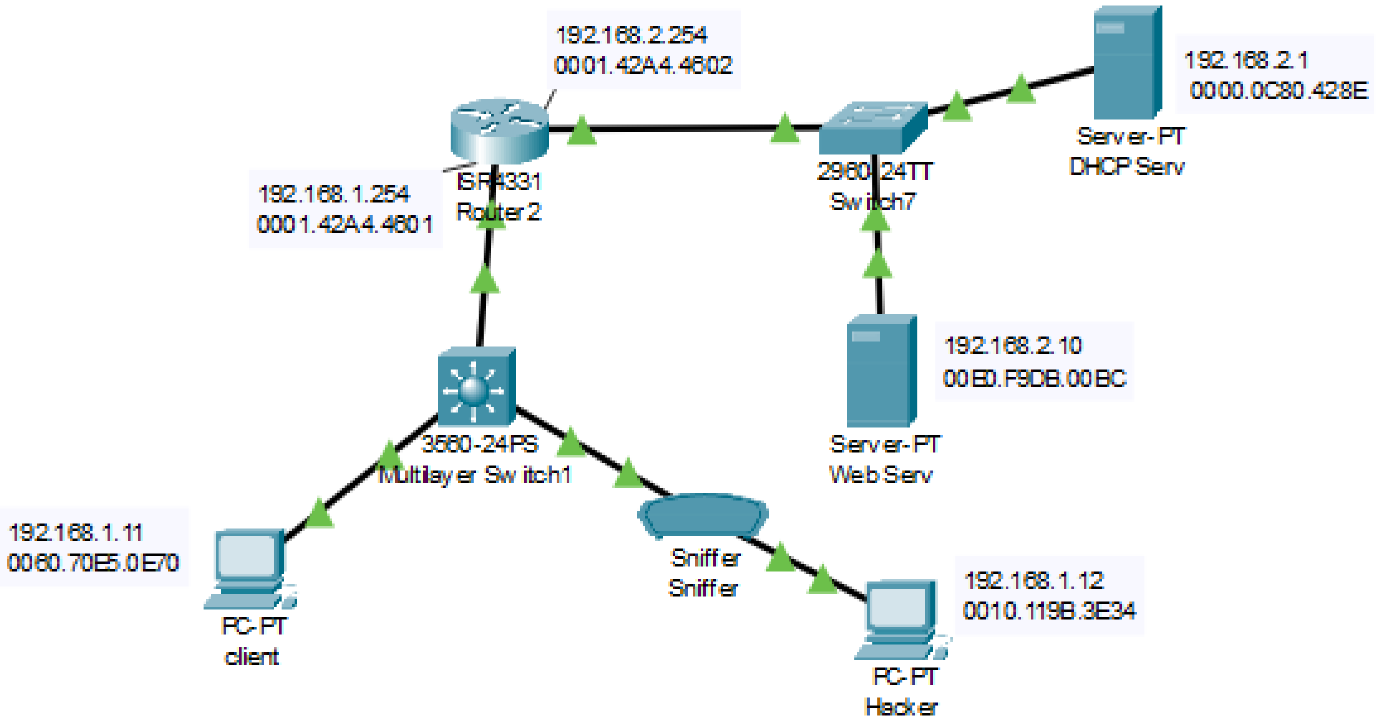


```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed
state to up


Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#int f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#int f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#int f0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#int f0/1
Switch(config-if)#ip verify source port-security
                      ^
% Invalid input detected at '^' marker.
```

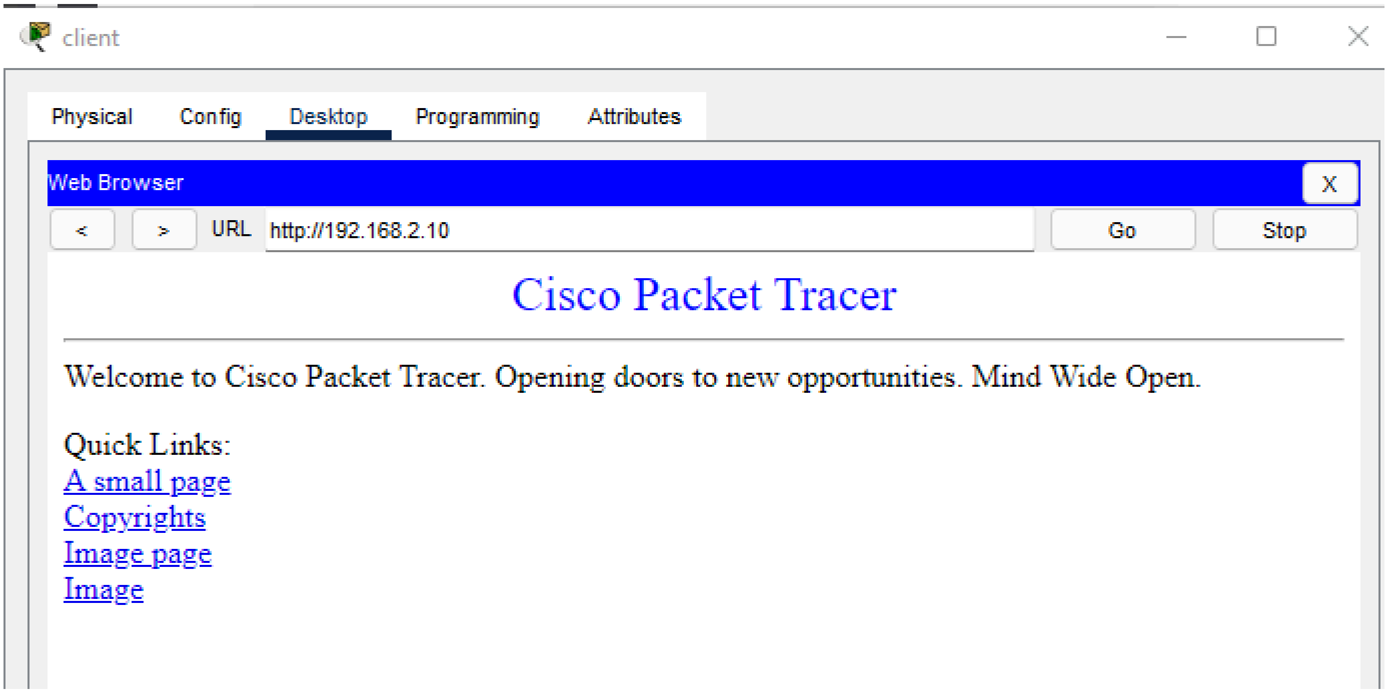
- Conceptually, ip source guard features detect and suppress address spoofing attacks, even if they occur within the same subnet. A layer 2 port and a layer 2 switch normally learns and stores MAC addresses. The switch lookup MAC addresses and finds out what IP addresses are associated with them by using the DHCP snooping database and static IP source binding entries. If the address is something other than the one learned or statically configured, the switch drops the packet.

ARP cache poisoning attack:

1. .
2. Demo:
   This is the topology:



I can initially reach the web server from client



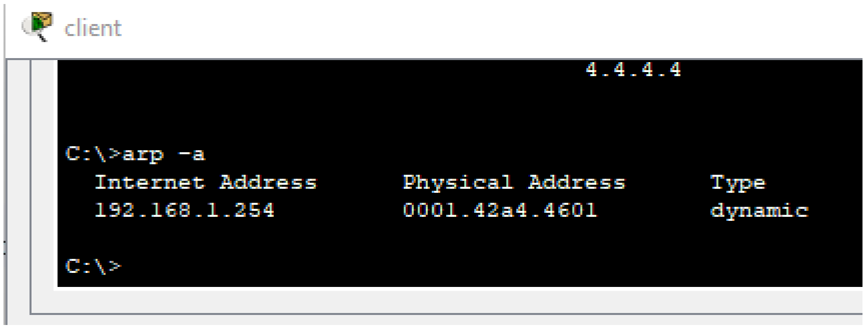
http://192.168.2.10

Cisco Packet Tracer

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

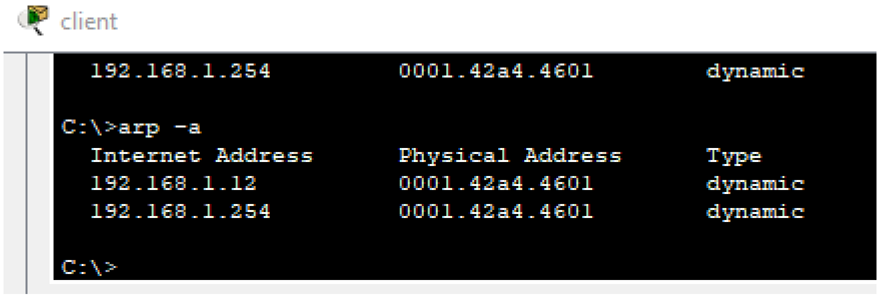
Quick Links:
A small page
Copyrights
Image page
Image

The host arp table:



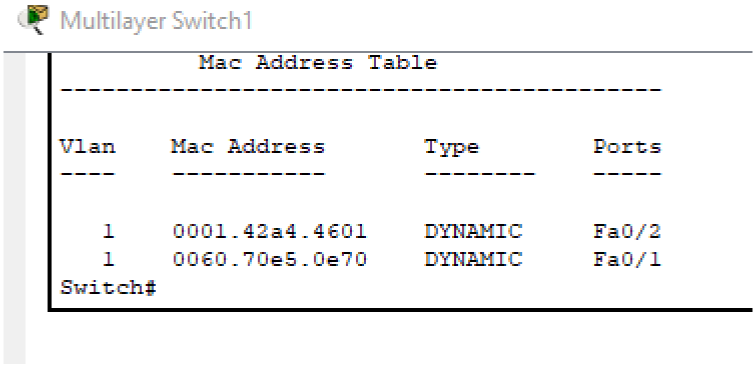
```
                                    4.4.4.4


C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.254         0001.42a4.4601        dynamic

C:\>
```

Lets take the MAC address of the interface of the router that has an ip of 192.168.1.254, and use it as the ip of pc5. Then I decided to send a constant ping to the client, which added pc5 IP with the mac address of the router.



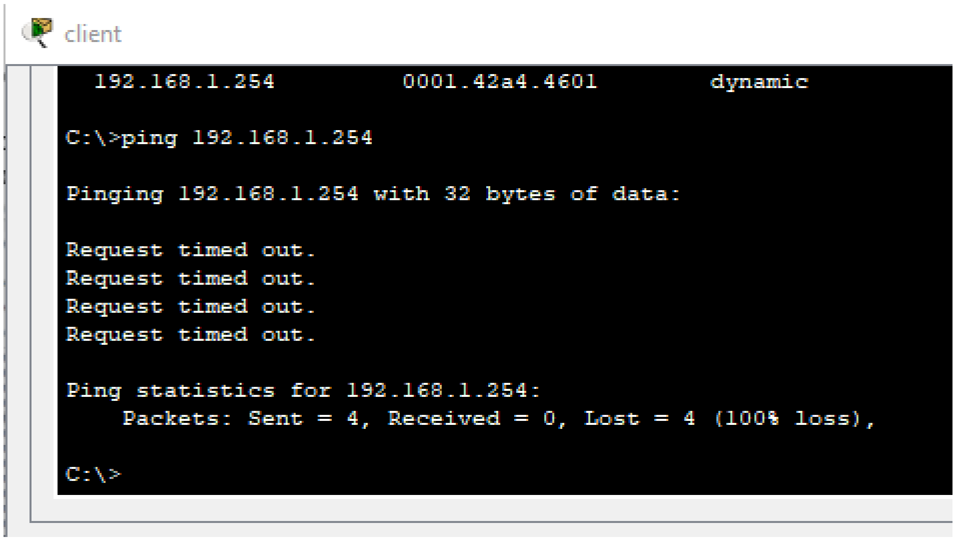
```
  192.168.1.254         0001.42a4.4601        dynamic

C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.12          0001.42a4.4601        dynamic
  192.168.1.254         0001.42a4.4601        dynamic

C:\>
```

The switch also changed the default gateway port to the the port that pc5 connected:



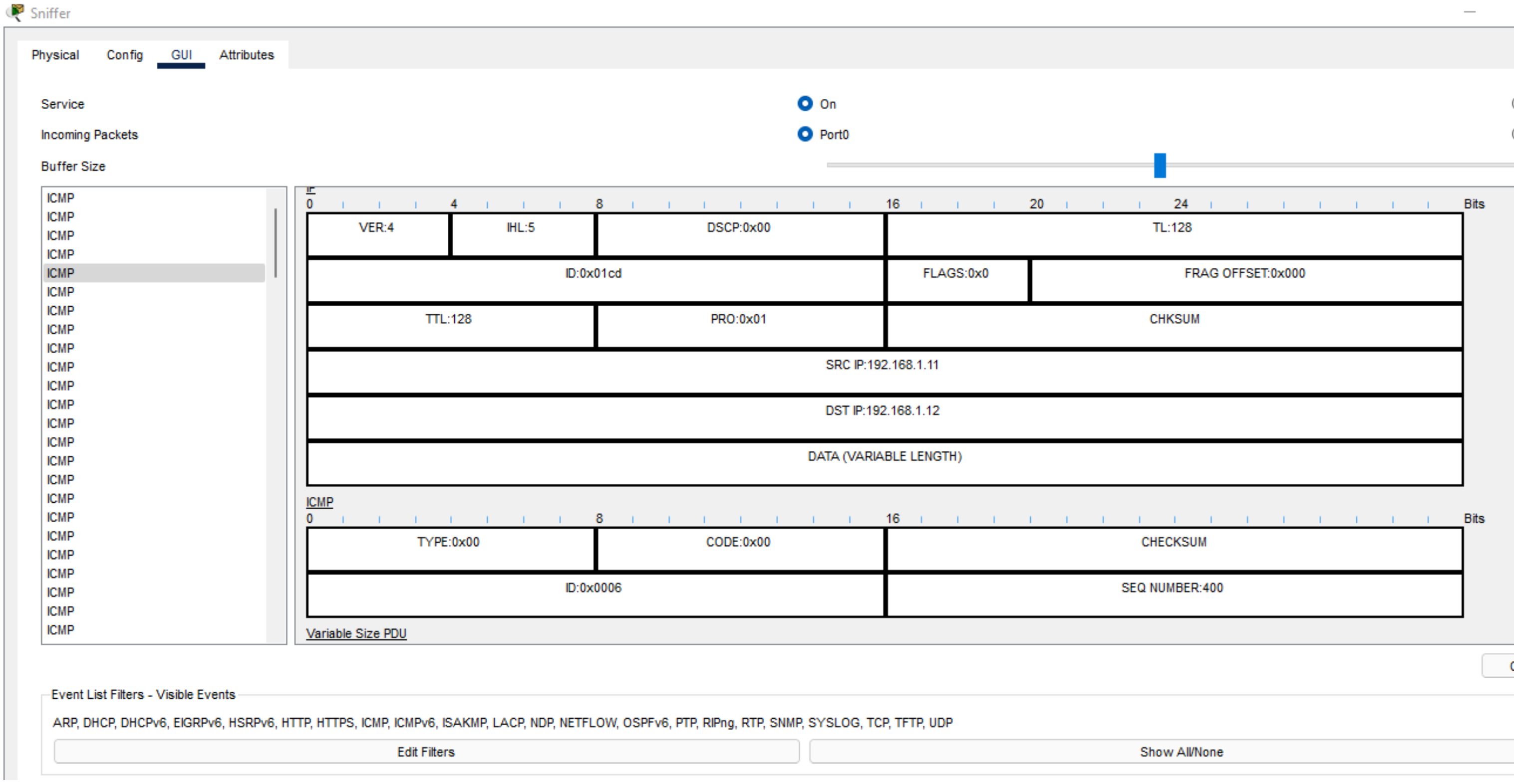
```
          Mac Address Table
-------------------------------------------

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

   1    0001.42a4.4601    DYNAMIC     Fa0/2
   1    0060.70e5.0e70    DYNAMIC     Fa0/1
Switch#
```

When I try to connect to the website again it doesn't work.



```
  192.168.1.254         0001.42a4.4601        dynamic

C:\>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Packet that was captured by the sniffer of icmp packet coming from the client. When if was supposed to be sending it to the router.



Service ● On

Incoming Packets ● Port0

Buffer Size

ICMP
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP
ICMP

IP

0 4 8 16 20 24 Bits

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

ID:0x01cd | FLAGS:0x0 | FRAG OFFSET:0x000

TTL:128 | PRO:0x01 | CHKSUM

SRC IP:192.168.1.11

DST IP:192.168.1.12

DATA (VARIABLE LENGTH)

ICMP

0 8 16 Bits

TYPE:0x00 | CODE:0x00 | CHECKSUM

ID:0x0006 | SEQ NUMBER:400

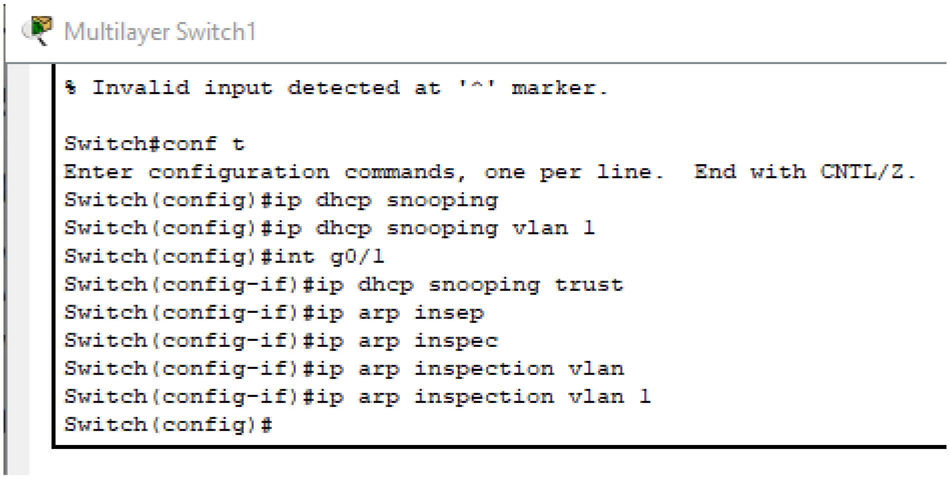
Variable Size PDU

Event List Filters - Visible Events

ARP, DHCP, DHCPv6, EIGRPv6, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, ISAKMP, LACP, NDP, NETFLOW, OSPFv6, PTP, RIPng, RTP, SNMP, SYSLOG, TCP, TFTP, UDP

3. Mitigation:
    a. Dynamic Arp Inspection

       Making switch configuration



```
% Invalid input detected at '^' marker.

Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#int g0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#ip arp insep
Switch(config-if)#ip arp inspec
Switch(config-if)#ip arp inspection vlan
Switch(config-if)#ip arp inspection vlan 1
Switch(config)#
```

    b. Private VLAN cannot be done as mentioned in the lab instructions
        - Mitigation with Private VLANs (PVLANs) in switches provides enhanced network isolation within the same physical VLAN by segmenting it into multiple smaller VLANs. This setup allows for strict control over which devices can communicate with each other, effectively mitigating the risk of internal threats and improving security. PVLANs typically include promiscuous ports that can communicate with all other port types, and isolated and community ports that have restricted communications, ensuring that devices within the same VLAN can be isolated from each other while still accessing shared resources. This feature is particularly useful in environments requiring high levels of security and isolation, such as data centers or shared hosting platforms.

DHCP starvation attack: (Cannot be performed in packet tracer as stated in the instruction)

1. This type of attack is when a hacker sends a large number of DHCP Discover messages with random, spoofed MAC addresses, which could exhaust the DHCP server's pool of IP addresses and prevent legitimate clients from obtaining an IP address. Tools like Dhcpstarv, Gobbler, Yersinia, and Metasploit can automate such attacks.
2. How it works: A DHCP starvation attack is a malicious activity where a hacker floods a DHCP server with numerous fake DHCP DISCOVER messages using spoofed MAC addresses, thereby depleting the server's pool of IP addresses. This prevents legitimate clients from obtaining an IP address, leading to network disruption. Tools like Dhcpstarv, Gobbler, Yersinia, and Metasploit can be used to automate such attacks. Mitigation strategies include enabling DHCP snooping to ensure that the source MAC address in the frame matches the MAC address in the DHCP payload, which helps to prevent the allocation of IP addresses to illegitimate requests. Also, port security can be used for further mitigation.
3. Network switches with port security disable access to switch ports by restricting the number of connected devices depending on their MAC addresses. This security mechanism limits communication over a single port to known devices exclusively, preventing unauthorized access and network breaches. In order to properly limit access at the physical layer of the network infrastructure, administrators can enable port security to either explicitly designate which addresses are permitted or to dynamically learn and retain MAC addresses.
4. DHCP Snooping: This is a security feature that monitors DHCP messages within a network to prevent malicious activities. It involves adding information to the DHCP requests from untrusted ports, like the switch's MAC address and port identifier, to ensure that requests come from valid ports.