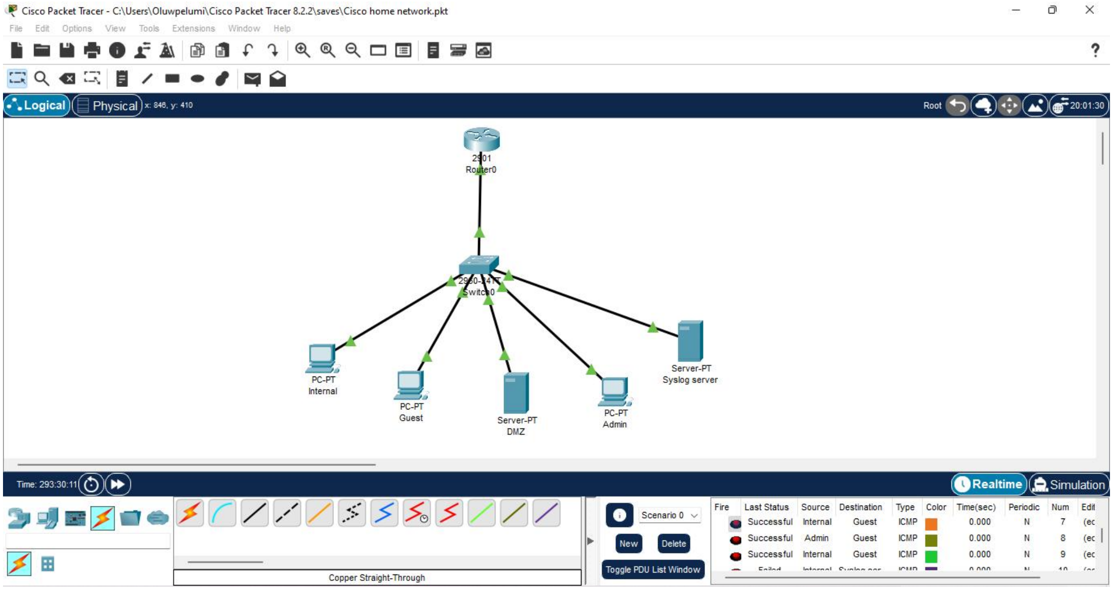
Home Network

Project Overview: I used Cisco Packet Tracer to build a segmented home network with Demilitarized Zone(DMZ), Access Control List(ACL) and Security Information Event Management(SIEM).It includes Router, Switch, a Server and Endpoint devices.

My Network Topology:



Cisco Packet Tracer - C:\Users\Oluwpelumi\Cisco Packet Tracer 8.2.2\saves\Cisco home network.pkt

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
●	Successful	Internal	Guest	ICMP	🟧	0.000	N	7	(ec
●	Successful	Admin	Guest	ICMP	🟩	0.000	N	8	(ec
●	Successful	Internal	Guest	ICMP	🟩	0.000	N	9	(ec
●	Failed	Internal	Syslog ser	ICMP	🟪	0.000	N	10	(ec

Step 1: Plan your Network:

Required Devices:

- 1 Router
- 1 Switch
- PCs for Internal, Guest & Admin
- 2 Servers (Syslog for SIEM & DMZ for HTTP service)

Subnets(VLAN)

VLAN	Name	Subnet	Purpose
10	Internal	192.168.1.1/24	Trusted device
20	Guest	192.168.2.1/24	Guest device
30	DMZ	192.168.3.1/24	Public services
40	Admin	192.168.4.1/24	Trusted device
50	Syslog	192.168.5.1/24	Monitoring/logging

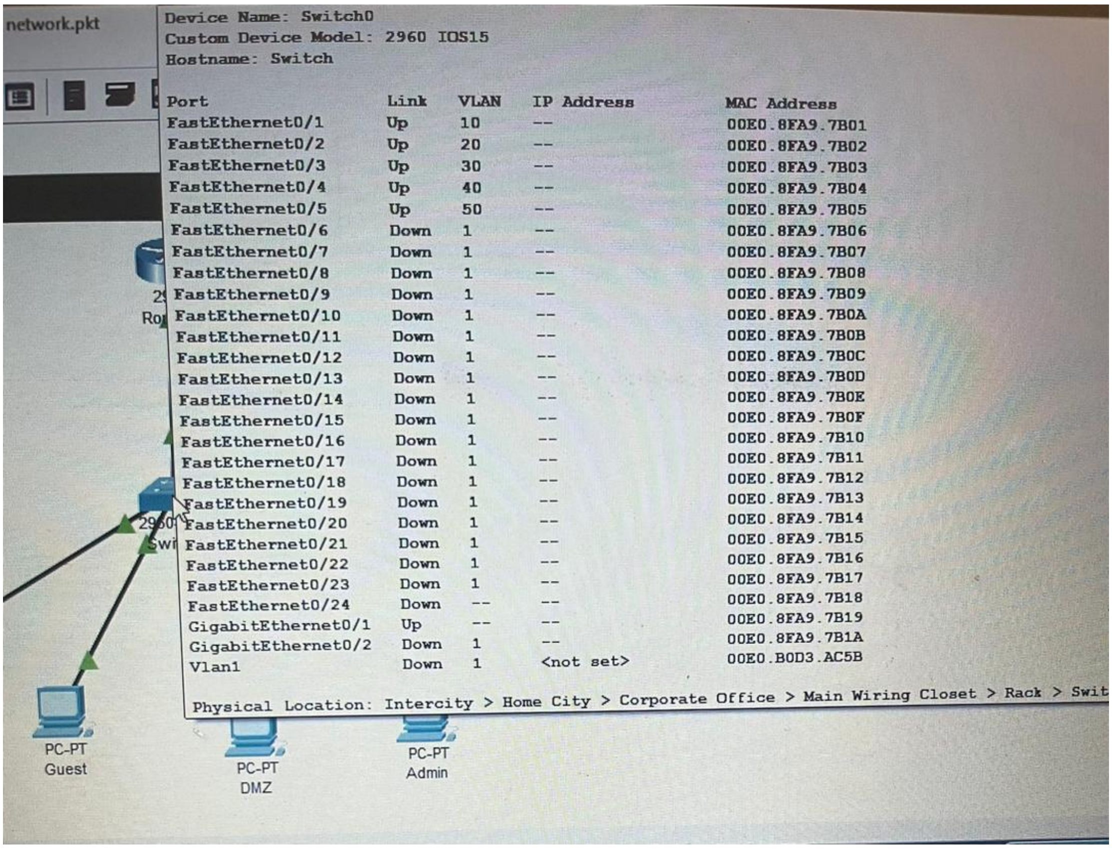
Step 2: Configure VLANs on Switch:

1. Click the switch > CLI:

```
enable
conf  t
vlan 10
  name Internal
vlan 20
  name Guest
vlan 30
  name DMZ
vlan 40
  name Admin
vlan 50
  name Syslog
```

2. Assign switch port to VLANs & switch trunk port: this is assigning the connection (copper straight through) connected from the devices to the switch, which is fastEthernet(fa) and the port the router is connected to on the switch is gigabitEthernet0/1(which is the port that will be set as trunk), click the switch and select CLI;

```
Interface fa0/1
switchport mode access
switchport access vlan 10
Interface fa0/2
switchport mode access
switchport access vlan 20
Interface fa0/3
switchport mode access
switchport access vlan 30
Interface fa0/4
switchport mode access
switchport access vlan 40
Interface fa0/5
switchport mode access
switchport access vlan 50
Interface g0/1
Switchport mode trunk
```



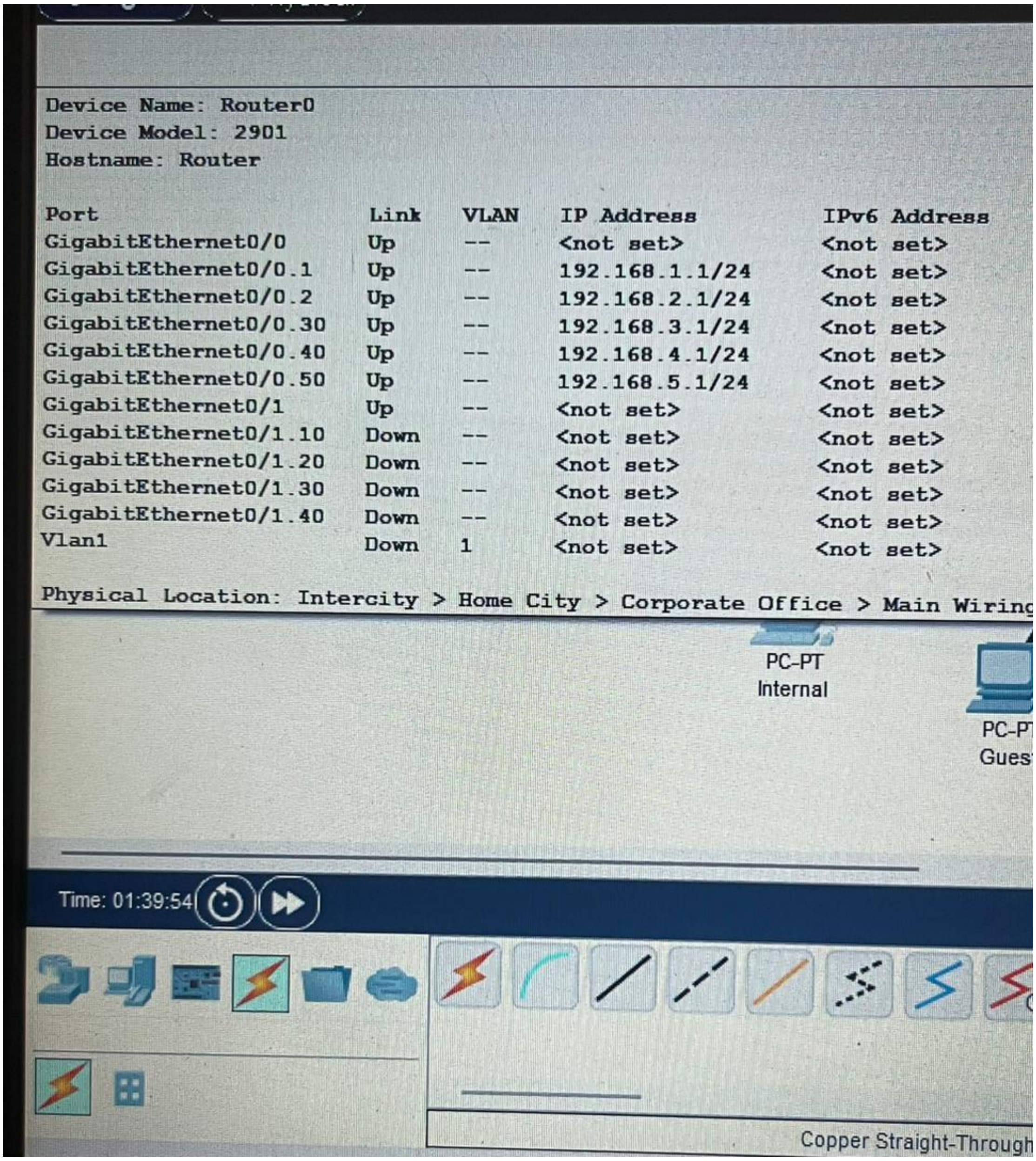
```
Device Name: Switch0
Custom Device Model: 2960 IOS15
Hostname: Switch

Port                 Link    VLAN   IP Address          MAC Address
FastEthernet0/1      Up      10     --                  00E0.8FA9.7B01
FastEthernet0/2      Up      20     --                  00E0.8FA9.7B02
FastEthernet0/3      Up      30     --                  00E0.8FA9.7B03
FastEthernet0/4      Up      40     --                  00E0.8FA9.7B04
FastEthernet0/5      Up      50     --                  00E0.8FA9.7B05
FastEthernet0/6      Down    1      --                  00E0.8FA9.7B06
FastEthernet0/7      Down    1      --                  00E0.8FA9.7B07
FastEthernet0/8      Down    1      --                  00E0.8FA9.7B08
FastEthernet0/9      Down    1      --                  00E0.8FA9.7B09
FastEthernet0/10     Down    1      --                  00E0.8FA9.7B0A
FastEthernet0/11     Down    1      --                  00E0.8FA9.7B0B
FastEthernet0/12     Down    1      --                  00E0.8FA9.7B0C
FastEthernet0/13     Down    1      --                  00E0.8FA9.7B0D
FastEthernet0/14     Down    1      --                  00E0.8FA9.7B0E
FastEthernet0/15     Down    1      --                  00E0.8FA9.7B0F
FastEthernet0/16     Down    1      --                  00E0.8FA9.7B10
FastEthernet0/17     Down    1      --                  00E0.8FA9.7B11
FastEthernet0/18     Down    1      --                  00E0.8FA9.7B12
FastEthernet0/19     Down    1      --                  00E0.8FA9.7B13
FastEthernet0/20     Down    1      --                  00E0.8FA9.7B14
FastEthernet0/21     Down    1      --                  00E0.8FA9.7B15
FastEthernet0/22     Down    1      --                  00E0.8FA9.7B16
FastEthernet0/23     Down    1      --                  00E0.8FA9.7B17
FastEthernet0/24     Down    --     --                  00E0.8FA9.7B18
GigabitEthernet0/1   Up      --     --                  00E0.8FA9.7B19
GigabitEthernet0/2   Down    1      --                  00E0.8FA9.7B1A
Vlan1                Down    1      <not set>           00E0.B0D3.AC5B

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Swit
```

This shows the ports have been assigned

Step 3: Configure Router-on-a-Stick (ROAS) subinterfaces:

This is where you assign the device subnets. I used gigabitEthernet0/0 because the switch is connected port;
Click the router, go to CLI:

```
enable
conf t
Interface g0/0.1
  encapsulation dot1Q 10
  ip address 192.168.1.1 255.255.255.0
Interface g0/0.2
  encapsulation dot1Q 20
  ip address 192.168.2.1 255.255.255.0
Interface g0/0.30
  encapsulation dot1Q 30
  ip address 192.168.3.1 255.255.255.0
Interface g0/0.40
  encapsulation dot1Q 40
  ip address 192.168.4.1 255.255.255.0
Interface g0/0.50
  encapsulation dot1Q 50
  ip address 192.168.5.1 255.255.255.0
Interface g0/0
 no shutdown
  exit
```



```
Device Name: Router0
Device Model: 2901
Hostname: Router

Port                     Link   VLAN   IP Address        IPv6 Address
GigabitEthernet0/0       Up     --     <not set>         <not set>
GigabitEthernet0/0.1     Up     --     192.168.1.1/24    <not set>
GigabitEthernet0/0.2     Up     --     192.168.2.1/24    <not set>
GigabitEthernet0/0.30    Up     --     192.168.3.1/24    <not set>
GigabitEthernet0/0.40    Up     --     192.168.4.1/24    <not set>
GigabitEthernet0/0.50    Up     --     192.168.5.1/24    <not set>
GigabitEthernet0/1       Up     --     <not set>         <not set>
GigabitEthernet0/1.10    Down   --     <not set>         <not set>
GigabitEthernet0/1.20    Down   --     <not set>         <not set>
GigabitEthernet0/1.30    Down   --     <not set>         <not set>
GigabitEthernet0/1.40    Down   --     <not set>         <not set>
Vlan1                    Down   1      <not set>         <not set>

Physical Location: Intercity > Home City > Corporate Office > Main Wiring
```

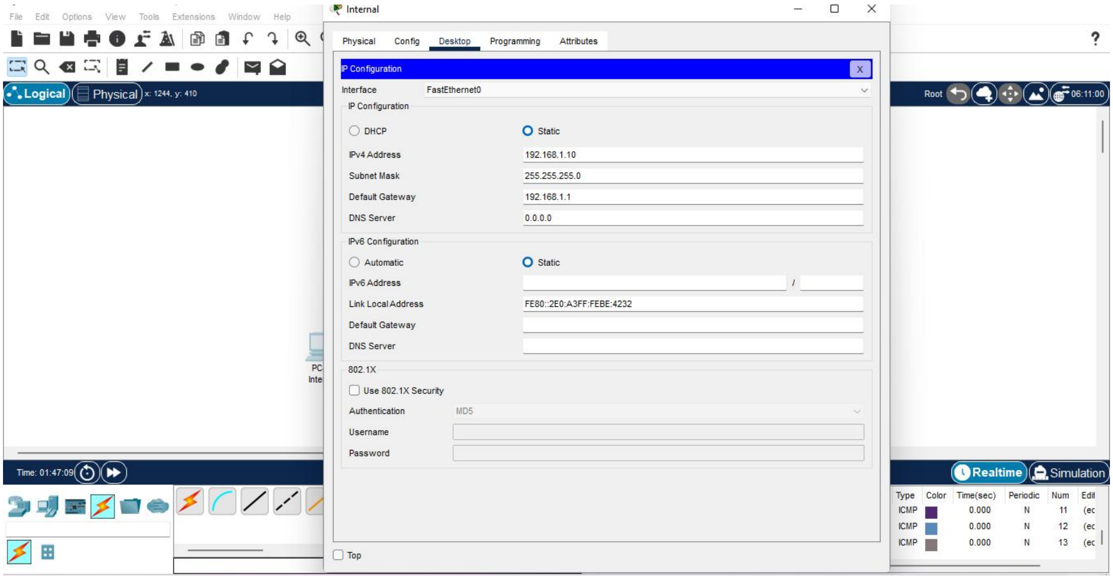
This shows all sub-interfaces have been assigned.

Step 4: Assign IP Addresses to Devices:

Manually configure the PCs & Servers.

Click each pc and select Desktop and click on IP configuration:

- Internal PC: 192.168.1.10, Gateway: 192.168.1.1
- Guest PC: 192.168.2.10, Gateway: 192.168.2.1
- DMZ PC: 192.168.3.10, Gateway: 192.168.3.1
- Admin PC: 192.168.4.10, Gateway: 192.168.4.1
- Syslog server: 192.168.5.10, Gateway: 192.168.5.1



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::2E0:A3FF:FEBE:4232

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

Username:

Password:

Type	Color	Time(sec)	Periodic	Num	Edit
ICMP	■	0.000	N	11	(ec
ICMP	■	0.000	N	12	(ec
ICMP	■	0.000	N	13	(ec

Step 5: Setting up Syslog Server for SIEM simulation.

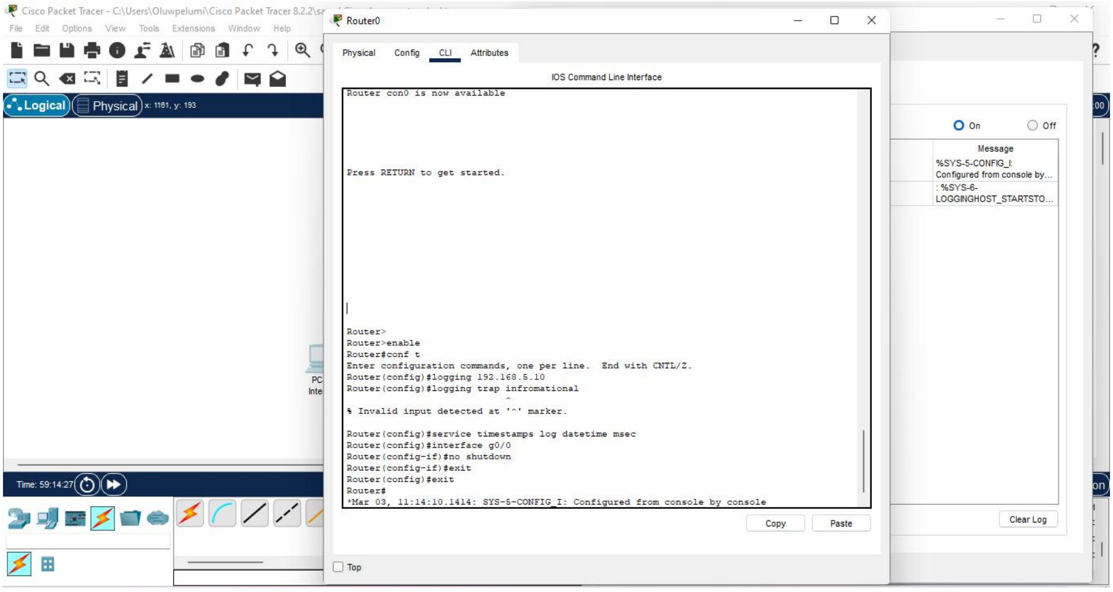
Since the server has been assigned to IP, click on the server and select services and select syslog and click on, this turns on the syslog and allows logging and monitoring event log, I configured the router so what ever changes is made is logged and monitored on the server.

Click router > CLI ;

```
logging 192.168.5.10
service timestamps log datetime msec
```

This command is to generate event log:

```
Interface g0/0
no shutdown
exit
```


Cisco Packet Tracer - C:\Users\Oluwpelumi\Cisco Packet Tracer 8.2.2\s
Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Logical
Physical
Copy
Paste
Clear Log
Top

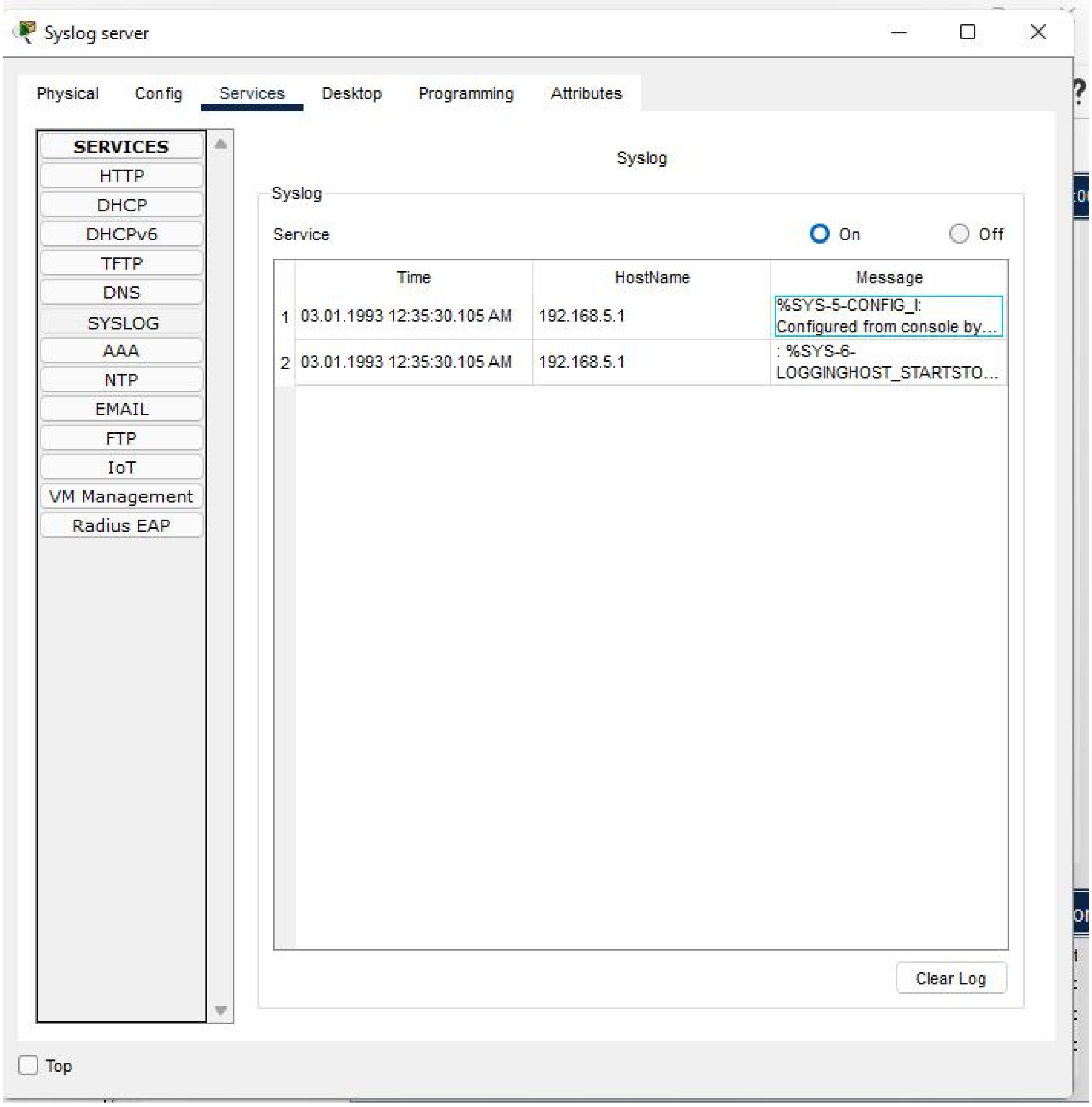
```
Router con0 is now available



Press RETURN to get started.








Router>
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#logging 192.168.5.10
Router(config)#logging trap infromational
                                    ^
% Invalid input detected at '^' marker.

Router(config)#service timestamps log datetime msec
Router(config)#interface g0/0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
Router#
*Mar 03, 11:14:10.1414: SYS-5-CONFIG_I: Configured from console by console
```

● On ○ Off

Message

```
%SYS-5-CONFIG_I: Configured from console by...
: %SYS-6-LOGGINGHOST_STARTSTO...
```

The result has been logged in the syslog server.



Syslog

Syslog

Service ● On ○ Off

	Time	HostName	Message
1	03.01.1993 12:35:30.105 AM	192.168.5.1	%SYS-5-CONFIG_I: Configured from console by...
2	03.01.1993 12:35:30.105 AM	192.168.5.1	: %SYS-6-LOGGINGHOST_STARTSTO...

Syslog Output

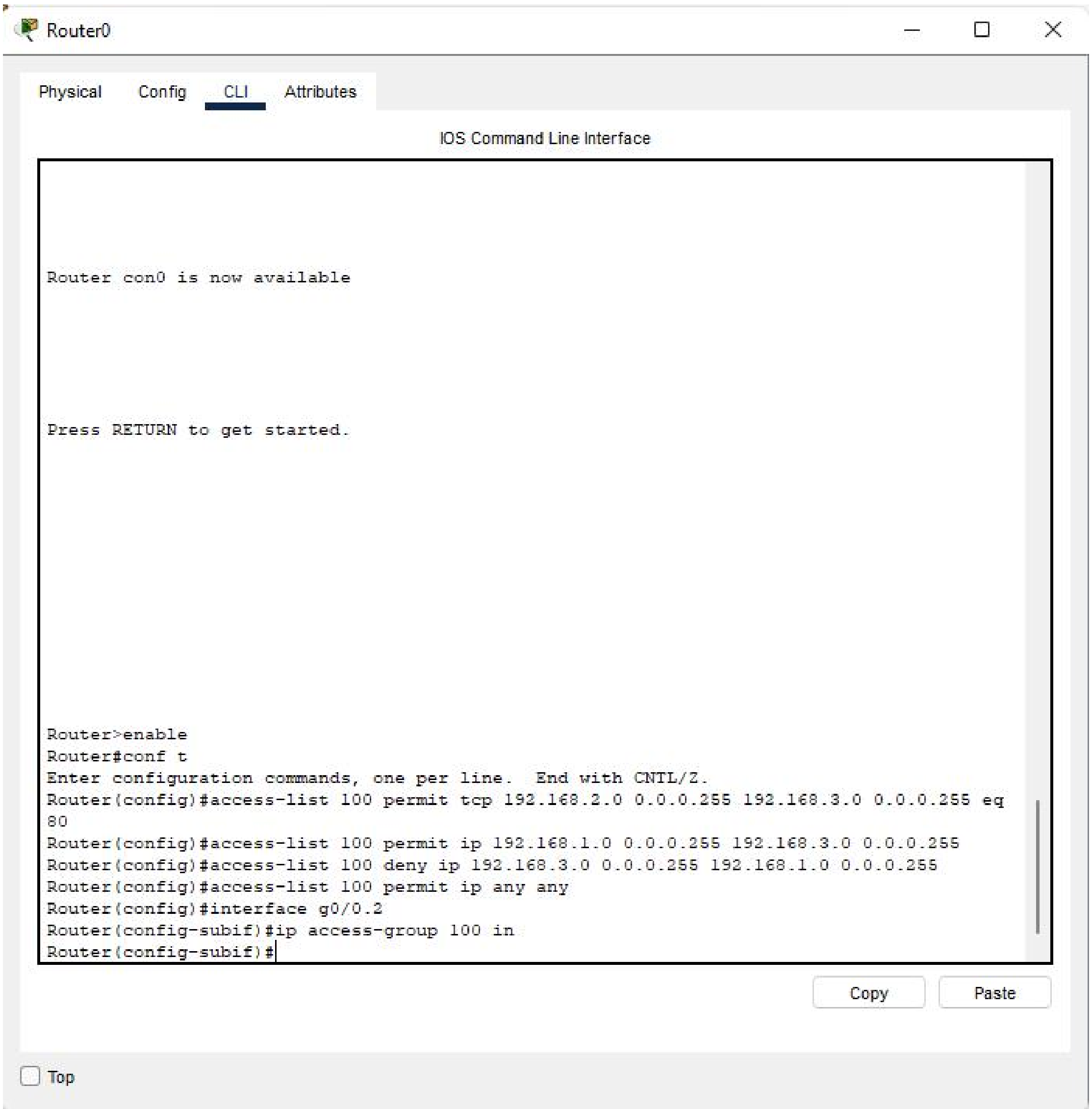
Step 6: Setting up ACL & DMZ:

DMZ(Demilitarized Zone) is a network segment where you place public-facing servers(web or FTP servers), so that the internet(Guest VLAN) can access them, but the devices can't access internal network.

Since the DMZ VLAN is already assigned and configured, setup the Access Control List(ACL) I used extended ACL; I allowed internal VLAN to access DMZ, Guest to access only HTTP(port 80) also, DMZ cannot initiate traffic to internal:

Click router > CLI:

```
access-list 100 permit tcp 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255 eq  80
access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
access-list 100 deny ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 100 permit ip any any
interface g0/0.2
ip access-group 100 in
```

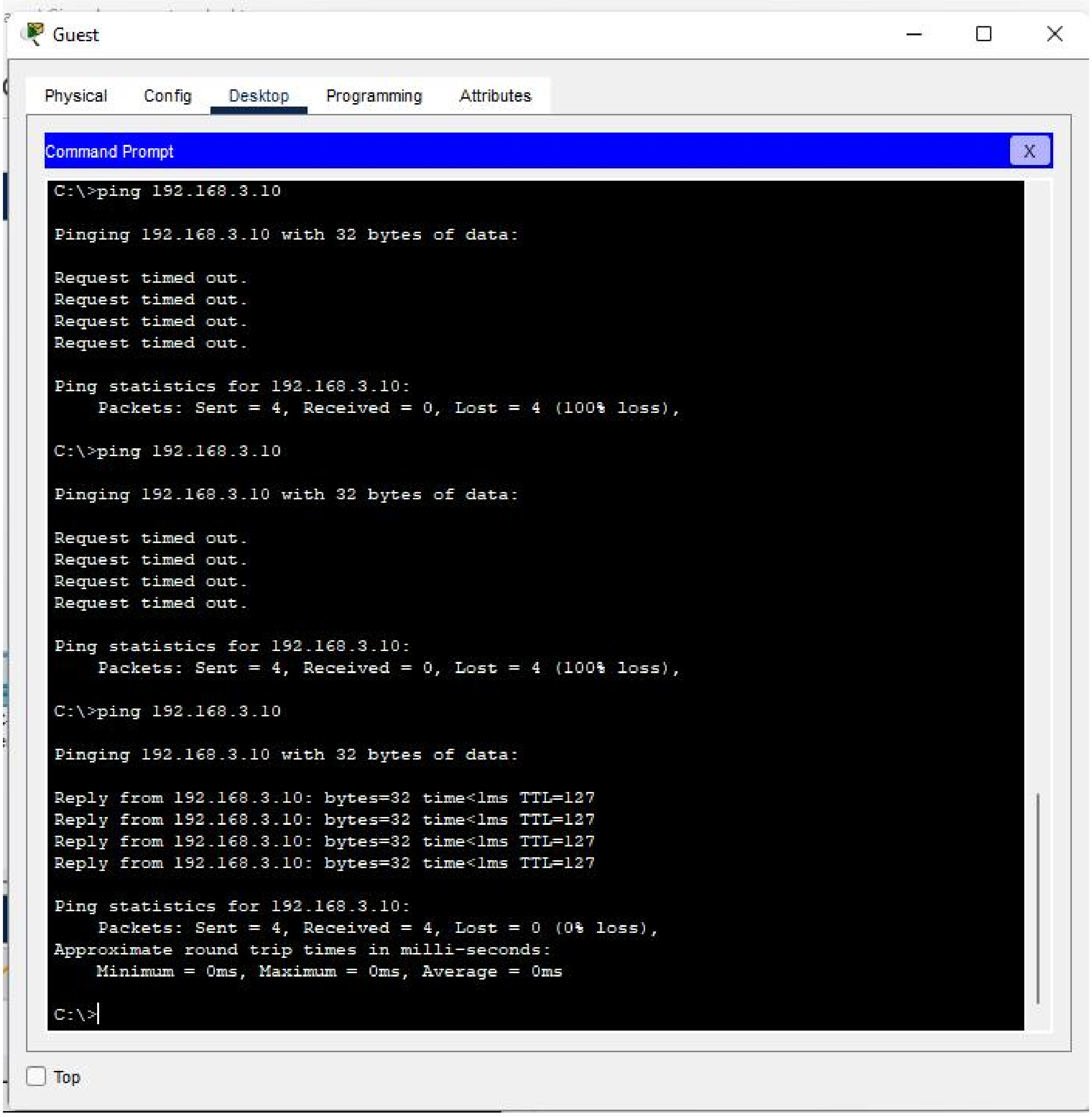


```
Router con0 is now available



Press RETURN to get started.








Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 permit tcp 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255 eq
80
Router(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
Router(config)#access-list 100 deny ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config)#access-list 100 permit ip any any
Router(config)#interface g0/0.2
Router(config-subif)#ip access-group 100 in
Router(config-subif)#
```

Verify ping on Guest PC first

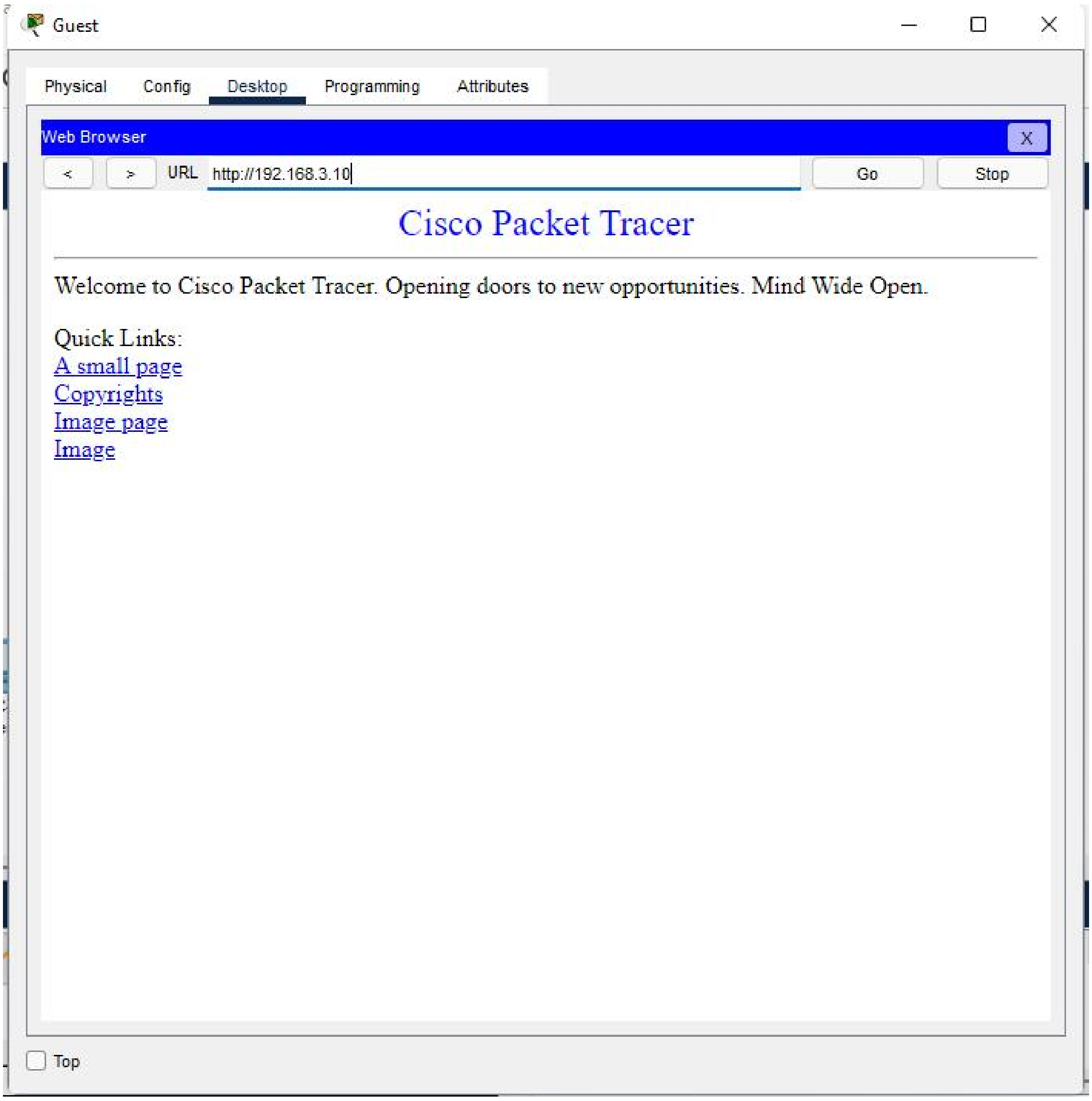
ping 192.168.3.10

If successful proceed to visit the guest pc web browser



```
C:\>ping 192.168.3.10

Pinging 192.168.3.10 with 32 bytes of data:

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

Ping statistics for 192.168.3.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.3.10

Pinging 192.168.3.10 with 32 bytes of data:

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

Ping statistics for 192.168.3.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.3.10

Pinging 192.168.3.10 with 32 bytes of data:

Reply from 192.168.3.10: bytes=32 time<1ms TTL=127
Reply from 192.168.3.10: bytes=32 time<1ms TTL=127
Reply from 192.168.3.10: bytes=32 time<1ms TTL=127
Reply from 192.168.3.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.3.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Go to Guest PC > Desktop > Web Browser
Enter http://192.168.3.10 (DMZ IP address) and expect to successful connection like the screenshot below:



http://192.168.3.10

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

Skills Learned:

- Network troubleshooting using ping and logs
- Understanding DMZ security and segmentation
- Application of extended ACL
- Configuration of subinterfaces, VLANs and ROAS.
- Deployment of Syslog server to monitor SIEM from router

Conclusion:

This virtual lab provides hands-on experience on how network is designed, configured and implemented in real-life using tools like Cisco Packet Tracer. The skills gained are foundation in network engineering and Security Operation Center.