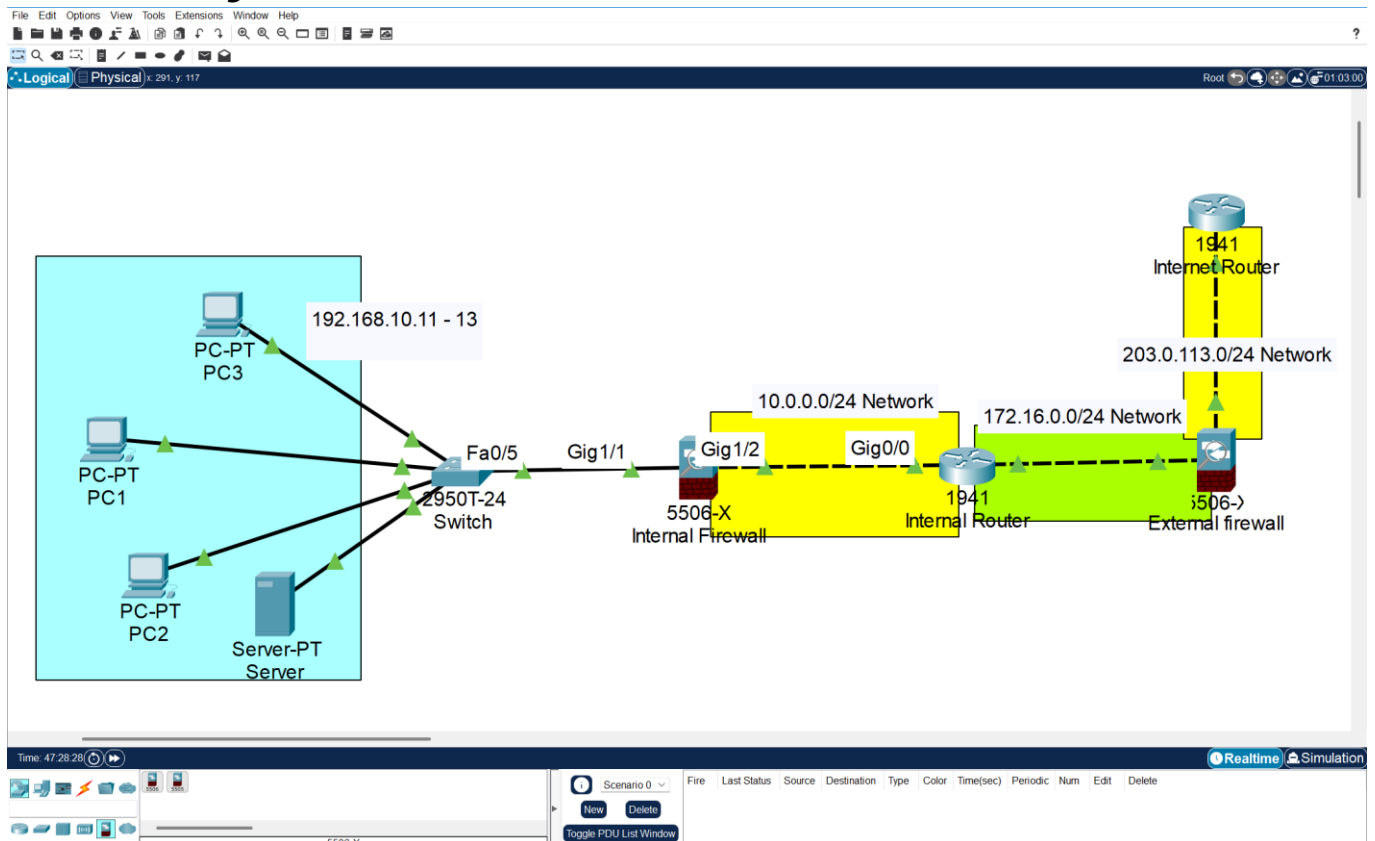


SIMULATION AND ANALYSIS IN CISCO PACKET TRACER

Here, I simulated a network topology using 3 PCs, switch, router, 2 firewalls (internal & external) and a Cloud/internet gateway. I have also included the commands and configurations used in this document.

This network is simple but at the same time, has some loose endings which I will be explaining at the end of this document.

Here is the design



Here is a [link](#) to the Cisco Packet tracer file

Here is the network configurations for each device used.

Device	Interface	IP Address
PC1–PC3	Fa0	192.168.10.11–13
DB Server	Fa0	192.168.10.100
Internal Firewall	Inside (Gig 1/1)	192.168.10.1
Internal Firewall	Outside (Gig 1/2)	10.0.0.1
Router0	Gig0/0	10.0.0.2
Router0	Gig0/1	172.16.0.1
External Firewall	Inside (Gig 1/1)	172.16.0.2
External Firewall	Outside (Gig 1/2)	203.0.113.2
Internet Router	Gig 0/0	203.0.113.1
Default gateway for PCs and sever		192.168.1.1

SUMMARY & EXPLANANTION OF COMMANDS USED

Command	Explanation
interface GigabitEthernet1/1	This selects the physical interface G1/1 on the device. It can either FastEthernet or GigabitEthernet interface.
nameif inside	Names the interface "inside". This is the trusted/internal side of the network. (inside of the firewall)
security-level 100	Sets the highest security level (100). ASA uses this to define trust levels — 100 = fully trusted, 0 = untrusted (like the internet).
ip address 10.0.0.1 255.255.255.0	Assigns IP address 10.0.0.1 and subnet mask 255.255.255.0 to a particular interface
no shutdown	Enables (brings up) the interface.
	NAT CONFIGURATIONS
object network obj_any	Enables (brings up) the interface.

subnet 192.168.10.0 255.255.255.0	Defines the subnet that the object represents (192.168.10.0/24 in this case).
nat (inside,outside) dynamic interface	This configures dynamic NAT on the firewall to translate internal IP addresses to the IP address of the outside interface of the firewall when accessing external networks. This essentially uses dynamic NAT (PAT) and substitutes the source IP with the outside interface's IP.
	ROUTING CONFIGURATIONS
route outside 0.0.0.0 0.0.0.0 203.0.113.1	This is a default route: all unknown traffic from the outside interface will go to the next-hop gateway at 203.0.113.1 (This was our Internet router)
route inside 10.0.0.0 255.255.255.0 172.16.0.1 route inside 192.168.10.0 255.255.255.0 172.16.0.1	This means that traffic destined for 10.0.0.0/24 and 192.168.10.0/24 should be sent to 172.16.0.1 via the inside interface
route outside 192.168.10.0 255.255.255.0 203.0.113.1	This means to route traffic from 192.168.10.0/24 via the outside interface to 203.0.113.1.
	ACCESS CONTROL LISTS (ACLs)
access-list OUTSIDE-IN extended permit icmp any any	Allow all ICMP (e.g., ping) traffic from any source to any destination inbound from the outside.
access-list INSIDE-OUT extended permit ip any any	Allow all protocols from inside to any destination (very permissive). Often used in basic setups, but not secure long-term.
access-list INSIDE-OUT extended permit icmp any any	Allow users inside to ping any device (even public internet). This is okay for diagnostic purposes.

The PC IP CONFIGURATIONS

For the PC configurations, I used a static IP configuration of 192.168.10.0/24 network using the IP address of the Gig 1/1 of the internal firewall as default gateway. For all the PCs. The subnet mask is 255.255.255.0

The network is 192.168.10.0 /24.

Image configuration for PC2

The screenshot shows the configuration window for PC2. The 'Config' tab is active, and the 'FastEthernet0' interface is selected. The 'IP Configuration' section is expanded, showing 'Static' as the selected option. The IP address is set to 192.168.10.12, the subnet mask is 255.255.255.0, and the default gateway is 192.168.10.1. The 'IPv6 Configuration' section is also expanded, showing 'Static' as the selected option. The IPv6 address is set to FE80::201:C9FF:FE76:CDE1. The '802.1X' section is expanded, showing 'Use 802.1X Security' as checked, and the authentication method is set to MD5. The 'Username' and 'Password' fields are empty.

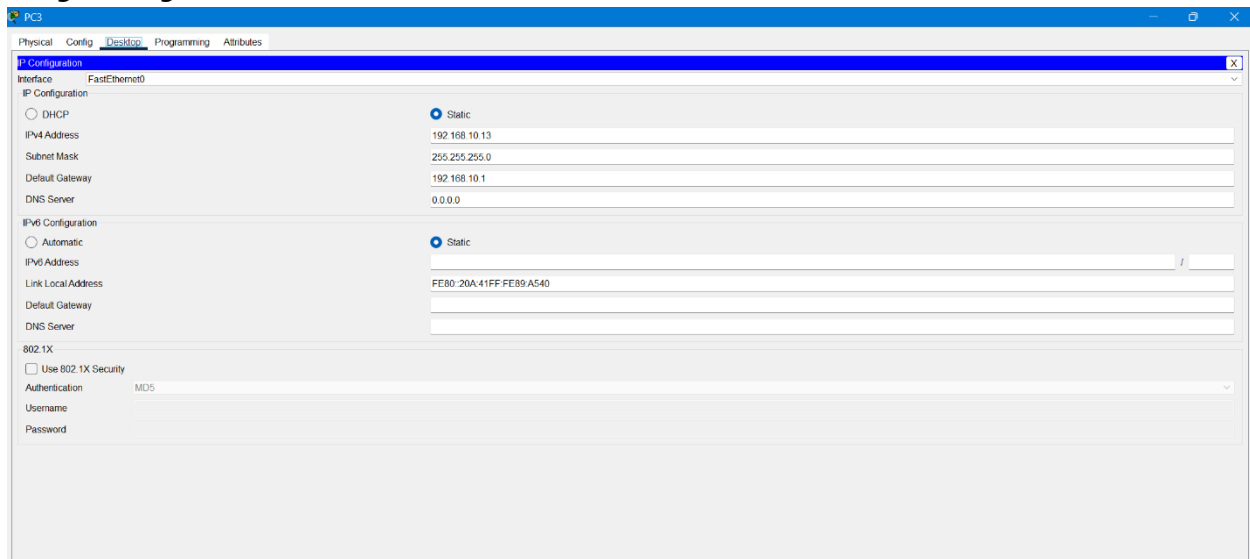
Interface	FastEthernet0
IP Configuration	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.12
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	0.0.0.0
IPv6 Configuration	<input checked="" type="radio"/> Static
IPv6 Address	FE80::201:C9FF:FE76:CDE1
Link Local Address	
Default Gateway	
DNS Server	
802.1X	<input checked="" type="checkbox"/> Use 802.1X Security
Authentication	MD5
Username	
Password	

Image configuration for PC1

The screenshot shows the configuration window for PC1. The 'Config' tab is active, and the 'FastEthernet0' interface is selected. The 'IP Configuration' section is expanded, showing 'Static' as the selected option. The IP address is set to 192.168.10.11, the subnet mask is 255.255.255.0, and the default gateway is 192.168.10.1. The 'IPv6 Configuration' section is also expanded, showing 'Static' as the selected option. The IPv6 address is set to FE80::201:96FF:FE43:37C5. The '802.1X' section is expanded, showing 'Use 802.1X Security' as checked, and the authentication method is set to MD5. The 'Username' and 'Password' fields are empty.

Interface	FastEthernet0
IP Configuration	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.11
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	0.0.0.0
IPv6 Configuration	<input checked="" type="radio"/> Static
IPv6 Address	FE80::201:96FF:FE43:37C5
Link Local Address	
Default Gateway	
DNS Server	
802.1X	<input checked="" type="checkbox"/> Use 802.1X Security
Authentication	MD5
Username	
Password	

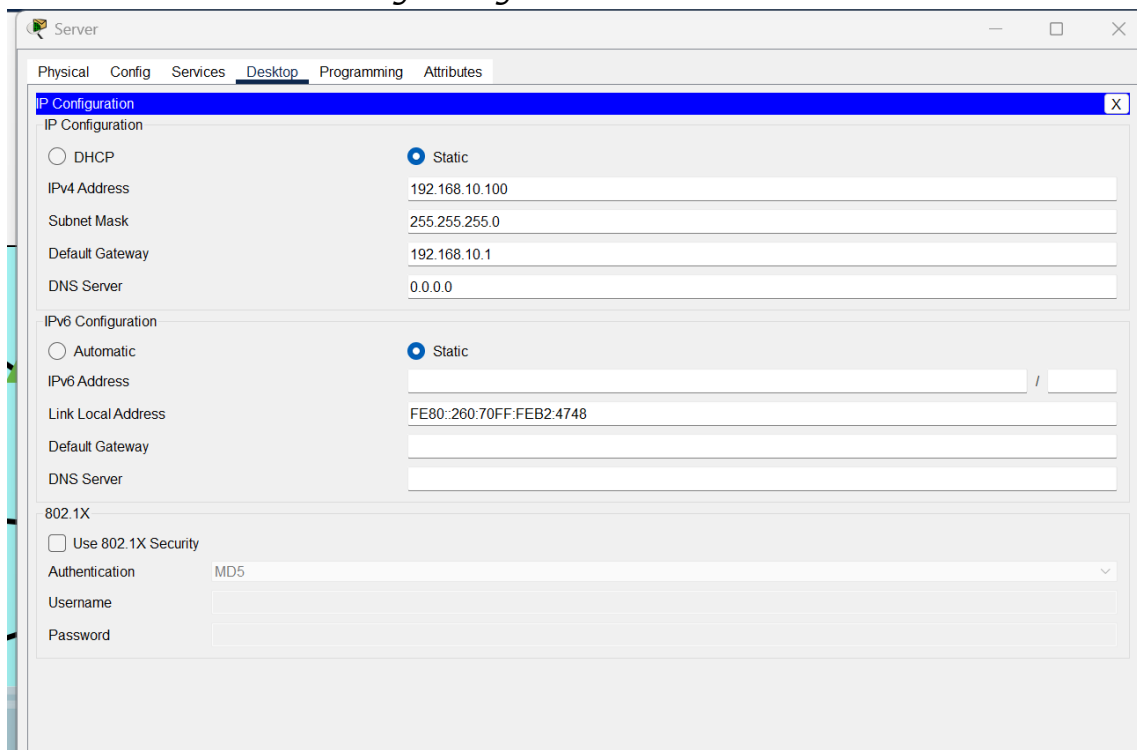
Image configuration for PC3



DB SERVER CONFIGURATION

The DB server is configured with an IP address 192.168.10.100 belonging to the same network as the three PCs using the GUI (Graphic User Interface) of the Server. The default gateway is 192.168.10.1 (IP address of the internal firewall - inside).

Image configuration for the Database Server



INTERNAL FIREWALL CONFIGURATION

The internal firewall was configured with IP address belonging to the same network of the 3 PCs to allow traffic to move outside from the PC to the firewall, then finally to reach the cloud. There are 2 interfaces; the inside security level was set to 100. While, for the external interface, the security level is set to 0.

The commands used:

```
interface GigabitEthernet1/1
nameif inside
security-level 100
ip address 10.0.0.1 255.255.255.0
no shutdown
```

```
interface GigabitEthernet1/2
nameif outside
security-level 0
ip address 192.168.10.1 255.255.255.0
no shutdown
object network obj_any
subnet 192.168.10.0 255.255.255.0
nat (inside,outside) dynamic interface
```

```
route outside 0.0.0.0 0.0.0.0 10.0.0.2
access-list OUTSIDE-IN extended permit icmp any any
access-list INSIDE-OUT extended permit ip any any
access-list INSIDE-OUT extended permit icmp any any
access-group OUTSIDE-IN in interface outside
access-group INSIDE-OUT in interface inside
```

Image showing the internal firewall configuration



ROUTER CONFIGURATION

The router is located between the two firewalls. The Gig 0/0 interface is configured with the IP address belonging to the same network of outside interface of the internal firewall. The Gig 0/1 interface is configured with the Ip address belonging to the same network portion of the external firewall (internal interface).

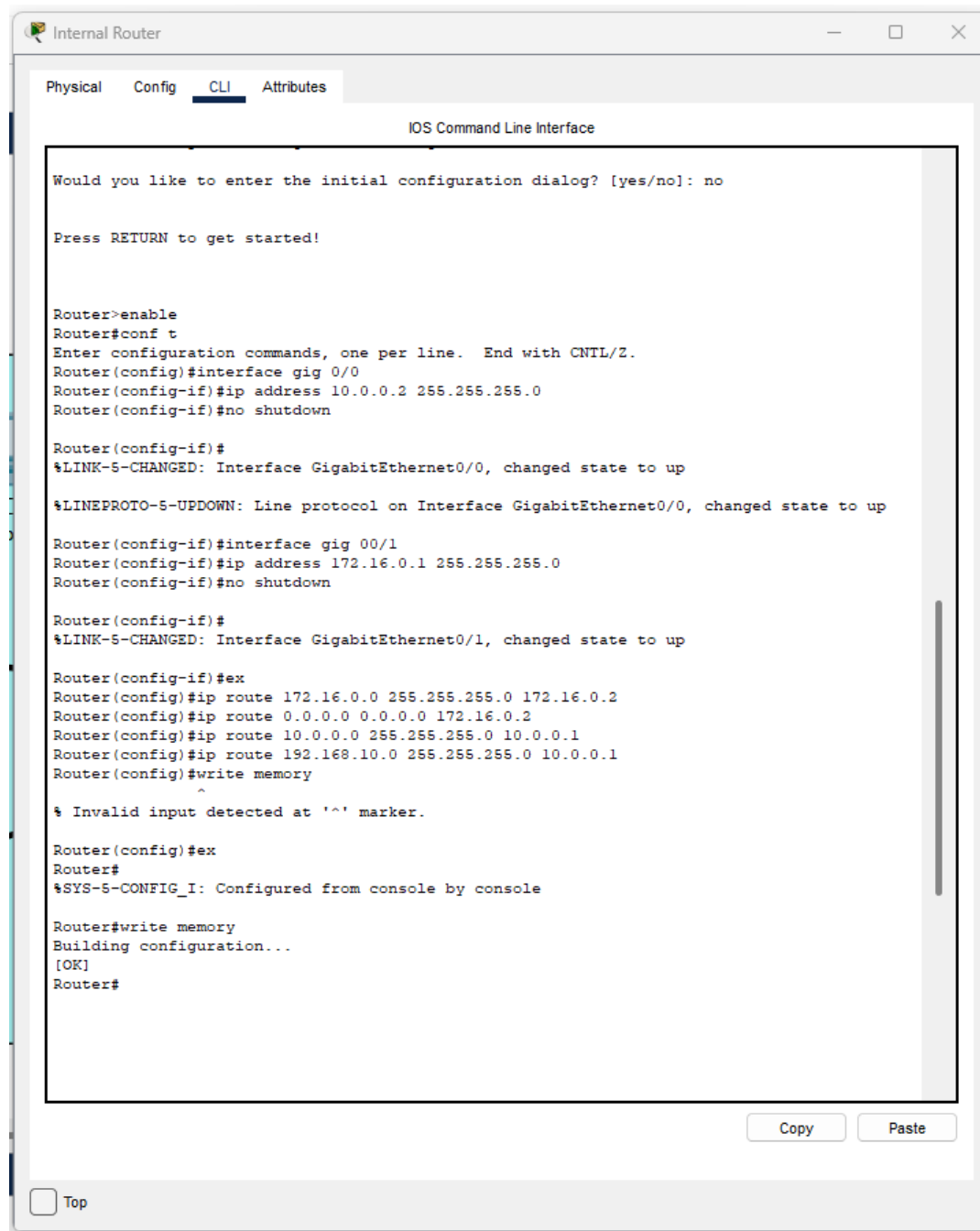
After each configuration, no shutdown command was used to power the router.
The configurations are shown in the screenshot below.

Commands used:

```
interface GigabitEthernet 0/0  
ip address 10.0.0.2 255.255.255.0  
no shutdown
```

```
interface GigabitEthernet0/0/1  
ip address 172.16.0.1 255.255.255.0  
no shutdown
```


Image showing the external router configuration



EXTERNAL FIREWALL CONFIGURATION

The external firewall was configured with IP address belonging to the same network as the router Gig 0/1 interface, because the firewall is located between the router and the

cloud. There are 2 interfaces; the inside security level was set to 100. While, for the external interface, the security level is set to 0.

Commands used:

```
interface GigabitEthernet1/1
nameif inside
security-level 100
ip address 203.0.113.2 255.255.255.0
no shutdown
```

```
interface GigabitEthernet1/2
nameif outside
security-level 0
ip address 172.16.0.2 255.255.255.0
no shutdown
```

```
object network LAN
subnet 192.168.10.0 255.255.255.0
nat (inside,outside) dynamic interface
object network external-net
subnet 203.0.113.0 255.255.255.0
nat (inside,outside) dynamic interface
```

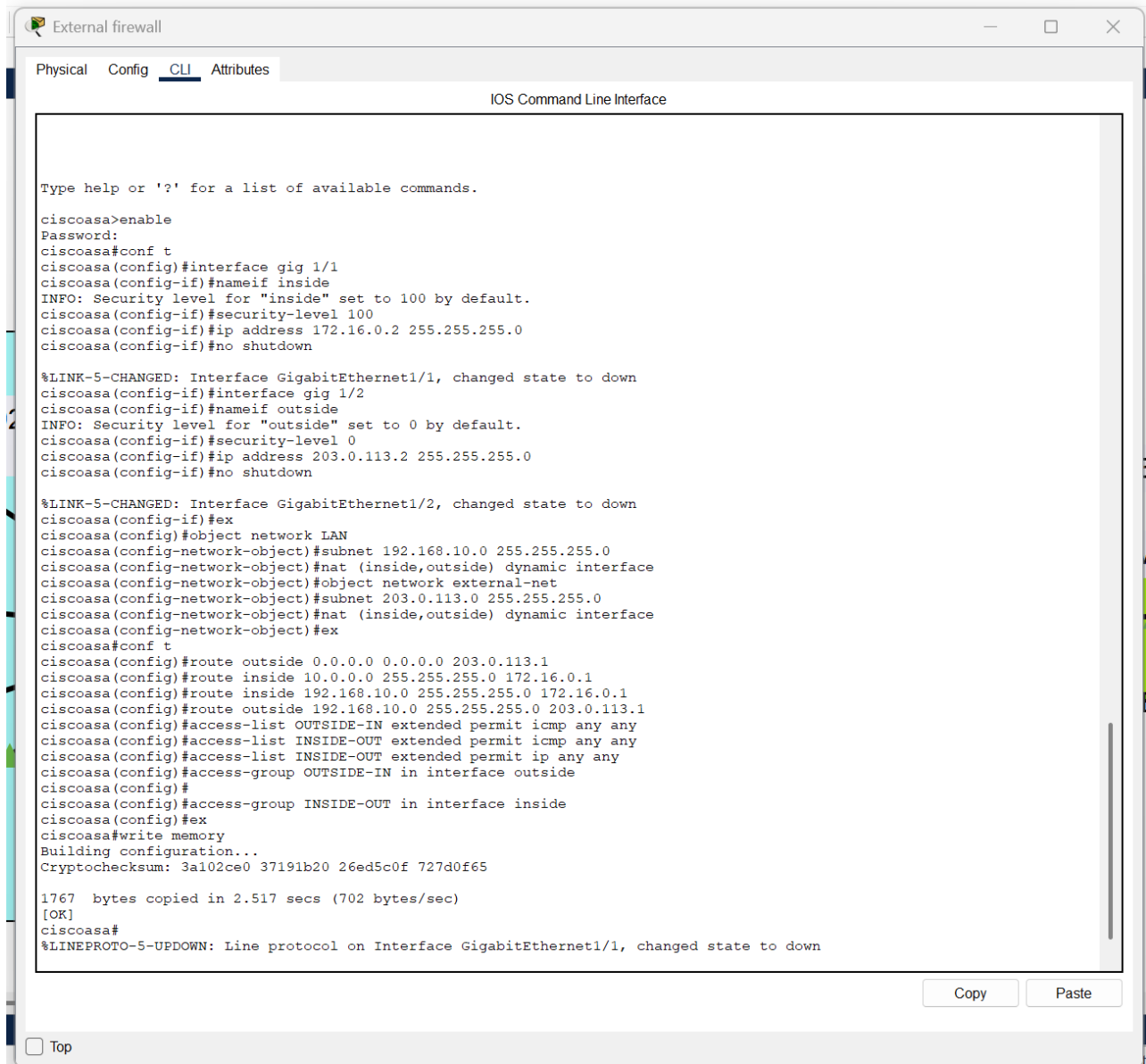
```
route outside 0.0.0.0 0.0.0.0 203.0.113.1
route inside 10.0.0.0 255.255.255.0 172.16.0.1
route inside 192.168.10.0 255.255.255.0 172.16.0.1
route outside 192.168.10.0 255.255.255.0 203.0.113.1
```

```
access-list OUTSIDE-IN extended permit icmp any any
access-list INSIDE-OUT extended permit icmp any any
access-list INSIDE-OUT extended permit ip any any
```

access-group OUTSIDE-IN in interface outside

access-group INSIDE-OUT in interface inside

Image showing the external firewall configuration



```
External firewall
Physical Config CLI Attributes
IOS Command Line Interface

Type help or '?' for a list of available commands.
ciscoasa>enable
Password:
ciscoasa#conf t
ciscoasa(config)#interface gig 1/1
ciscoasa(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#ip address 172.16.0.2 255.255.255.0
ciscoasa(config-if)#no shutdown

%LINK-5-CHANGED: Interface GigabitEthernet1/1, changed state to down
ciscoasa(config-if)#interface gig 1/2
ciscoasa(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#ip address 203.0.113.2 255.255.255.0
ciscoasa(config-if)#no shutdown

%LINK-5-CHANGED: Interface GigabitEthernet1/2, changed state to down
ciscoasa(config-if)#ex
ciscoasa(config)#object network LAN
ciscoasa(config-network-object)#subnet 192.168.10.0 255.255.255.0
ciscoasa(config-network-object)#nat (inside,outside) dynamic interface
ciscoasa(config-network-object)#object network external-net
ciscoasa(config-network-object)#subnet 203.0.113.0 255.255.255.0
ciscoasa(config-network-object)#nat (inside,outside) dynamic interface
ciscoasa(config-network-object)#ex
ciscoasa#conf t
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 203.0.113.1
ciscoasa(config)#route inside 10.0.0.0 255.255.255.0 172.16.0.1
ciscoasa(config)#route inside 192.168.10.0 255.255.255.0 172.16.0.1
ciscoasa(config)#route outside 192.168.10.0 255.255.255.0 203.0.113.1
ciscoasa(config)#access-list OUTSIDE-IN extended permit icmp any any
ciscoasa(config)#access-list INSIDE-OUT extended permit icmp any any
ciscoasa(config)#access-list INSIDE-OUT extended permit ip any any
ciscoasa(config)#access-group OUTSIDE-IN in interface outside
ciscoasa(config)#
ciscoasa(config)#access-group INSIDE-OUT in interface inside
ciscoasa(config)#ex
ciscoasa#write memory
Building configuration...
Cryptochecksum: 3a102ce0 37191b20 26ed5c0f 727d0f65

1767 bytes copied in 2.517 secs (702 bytes/sec)
[OK]
ciscoasa#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/1, changed state to down
```

Copy Paste

☐ Top

TESTING NETWORK CONNECTIVITY

- a) Testing the PC connectivity to other PCs
- b) Testing the connectivity of the device to the server located inside the internal network
- c) Testing the connectivity to the Internet router by pinging its IP address

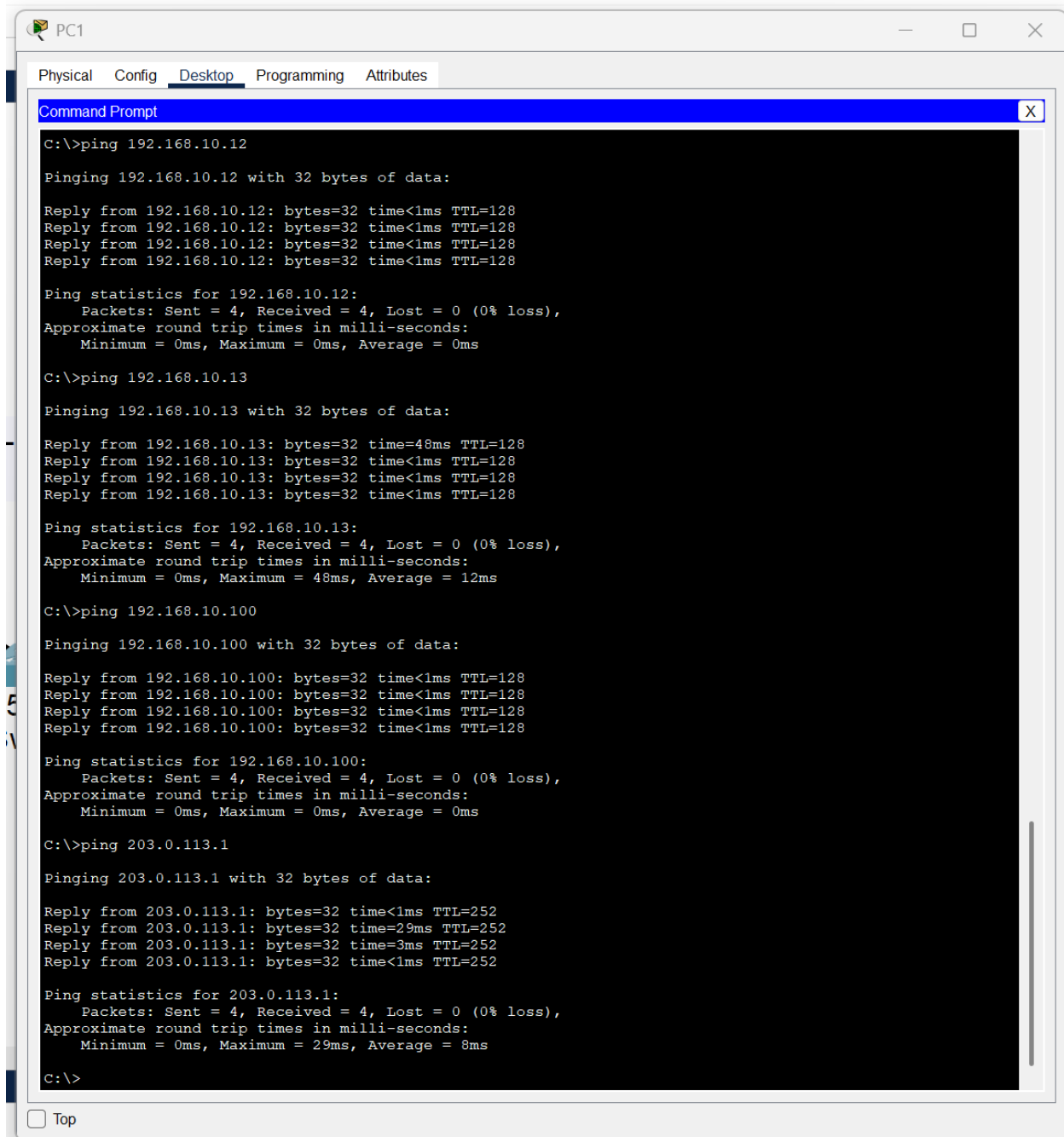
The commands used are:

Ping 192.168.10.10 -13 – for PC1 to PC3

Ping 192.168.10.100 – for the server

Ping 203.0.113.1 – for the internet router

Here is a successful ping from PC1 to PC2, PC3, Server and Internet router



The screenshot shows a PC1 desktop environment with a taskbar at the bottom. The 'Desktop' tab is selected in the top navigation bar. A 'Command Prompt' window is open, displaying the results of four ping commands. Each command shows four successful replies with 32 bytes of data, a time of less than 1ms, and a TTL of 128. Ping statistics for each target show 4 packets sent, 4 received, 0% loss, and approximate round trip times in milliseconds.

```
C:\>ping 192.168.10.12

Pinging 192.168.10.12 with 32 bytes of data:

Reply from 192.168.10.12: bytes=32 time<1ms TTL=128
Reply from 192.168.10.12: bytes=32 time<1ms TTL=128
Reply from 192.168.10.12: bytes=32 time<1ms TTL=128
Reply from 192.168.10.12: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.13

Pinging 192.168.10.13 with 32 bytes of data:

Reply from 192.168.10.13: bytes=32 time=48ms TTL=128
Reply from 192.168.10.13: bytes=32 time<1ms TTL=128
Reply from 192.168.10.13: bytes=32 time<1ms TTL=128
Reply from 192.168.10.13: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 48ms, Average = 12ms

C:\>ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:

Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 203.0.113.1

Pinging 203.0.113.1 with 32 bytes of data:

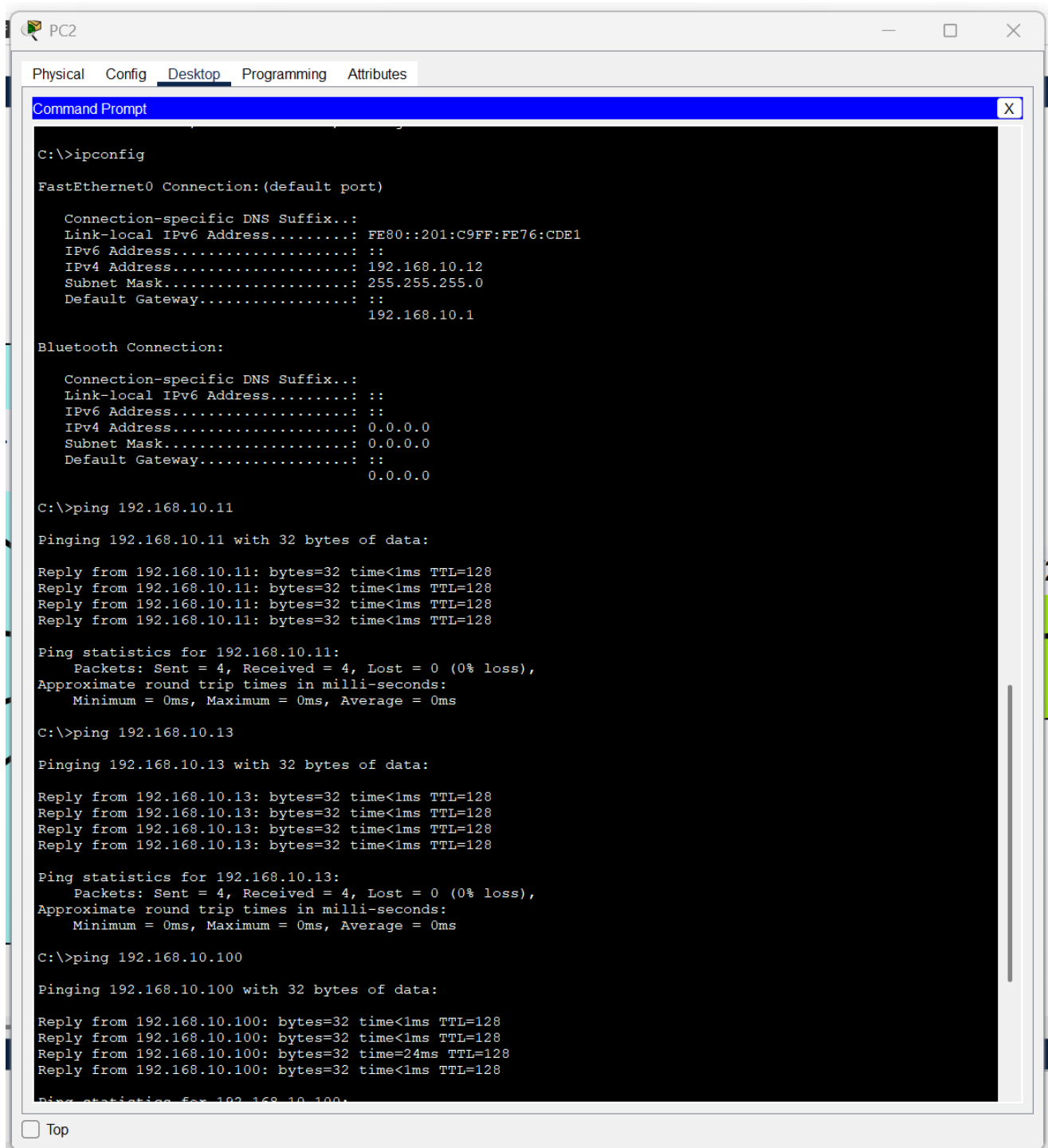
Reply from 203.0.113.1: bytes=32 time<1ms TTL=252
Reply from 203.0.113.1: bytes=32 time=29ms TTL=252
Reply from 203.0.113.1: bytes=32 time=3ms TTL=252
Reply from 203.0.113.1: bytes=32 time<1ms TTL=252

Ping statistics for 203.0.113.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 29ms, Average = 8ms

C:\>
```

☐ Top

Here is also a successful ping from PC2 to PC1, PC3, Server and Internet router



The screenshot shows a virtual PC2 desktop with a taskbar at the top. The 'Desktop' tab is selected in the top navigation bar. A 'Command Prompt' window is open, displaying the following text:

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::201:C9FF:FE76:CDE1
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.10.12
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                   192.168.10.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                   0.0.0.0

C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.13

Pinging 192.168.10.13 with 32 bytes of data:

Reply from 192.168.10.13: bytes=32 time<1ms TTL=128
Reply from 192.168.10.13: bytes=32 time<1ms TTL=128
Reply from 192.168.10.13: bytes=32 time<1ms TTL=128
Reply from 192.168.10.13: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:

Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time=24ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.100:
```

At the bottom left of the window, there is a 'Top' button.

PC2

Physical Config Desktop Programming Attributes

Command Prompt

```
Subnet Mask..... 0.0.0.0
Default Gateway..... ::
                  0.0.0.0

C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.13

Pinging 192.168.10.13 with 32 bytes of data:

Reply from 192.168.10.13: bytes=32 time<1ms TTL=128
Reply from 192.168.10.13: bytes=32 time<1ms TTL=128
Reply from 192.168.10.13: bytes=32 time<1ms TTL=128
Reply from 192.168.10.13: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:

Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time=24ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 24ms, Average = 6ms

C:\>ping 203.0.113.1

Pinging 203.0.113.1 with 32 bytes of data:

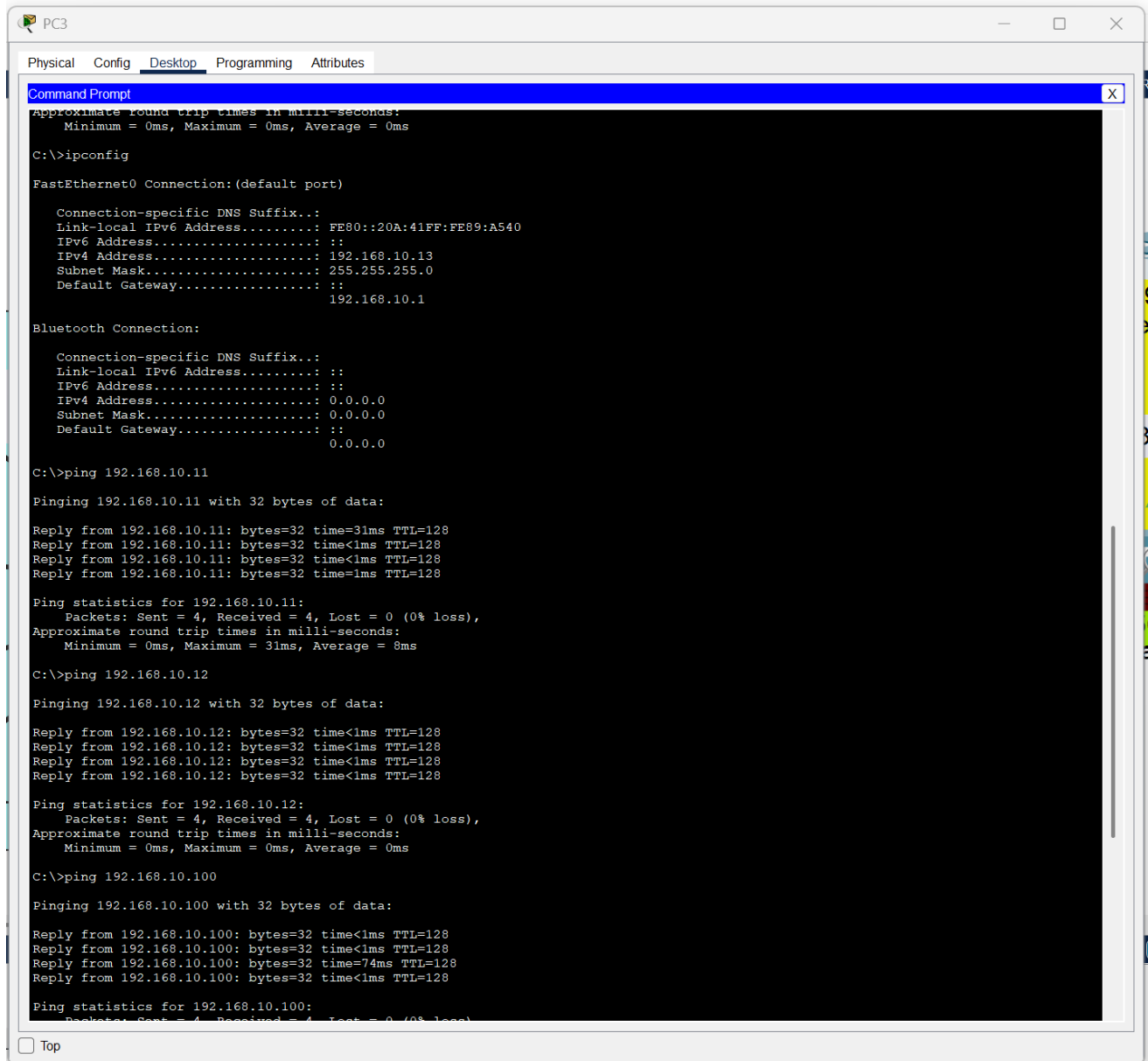
Reply from 203.0.113.1: bytes=32 time<1ms TTL=252
Reply from 203.0.113.1: bytes=32 time<1ms TTL=252
Reply from 203.0.113.1: bytes=32 time<1ms TTL=252
Reply from 203.0.113.1: bytes=32 time<1ms TTL=252

Ping statistics for 203.0.113.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

☐ Top

Here is also a successful ping from PC 3 to PC2, PC1, Server and Internet router



The screenshot shows a Windows Command Prompt window titled "PC3" with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, displaying the Command Prompt. The prompt shows the output of the 'ipconfig' command, displaying network settings for FastEthernet0 and Bluetooth. It then shows successful ping results to 192.168.10.11, 192.168.10.12, and 192.168.10.100.

```
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::20A:41FF:FE89:A540
    IPv6 Address . . . . .: ::
    IPv4 Address. . . . .: 192.168.10.13
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                192.168.10.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address. . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                0.0.0.0

C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.10.11: bytes=32 time=31ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 31ms, Average = 8ms

C:\>ping 192.168.10.12

Pinging 192.168.10.12 with 32 bytes of data:

Reply from 192.168.10.12: bytes=32 time<1ms TTL=128
Reply from 192.168.10.12: bytes=32 time<1ms TTL=128
Reply from 192.168.10.12: bytes=32 time<1ms TTL=128
Reply from 192.168.10.12: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:

Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time=74ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

☐ Top

PC3

Physical Config Desktop Programming Attributes

Command Prompt

```
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 31ms, Average = 8ms

C:\>ping 192.168.10.12

Pinging 192.168.10.12 with 32 bytes of data:

Reply from 192.168.10.12: bytes=32 time<1ms TTL=128
Reply from 192.168.10.12: bytes=32 time<1ms TTL=128
Reply from 192.168.10.12: bytes=32 time<1ms TTL=128
Reply from 192.168.10.12: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:

Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time=74ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 74ms, Average = 18ms

C:\>ping 203.0.113.1

Pinging 203.0.113.1 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 203.0.113.1: bytes=32 time=10ms TTL=252
Reply from 203.0.113.1: bytes=32 time=7ms TTL=252

Ping statistics for 203.0.113.1:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 10ms, Average = 8ms

C:\>ping 203.0.113.1

Pinging 203.0.113.1 with 32 bytes of data:

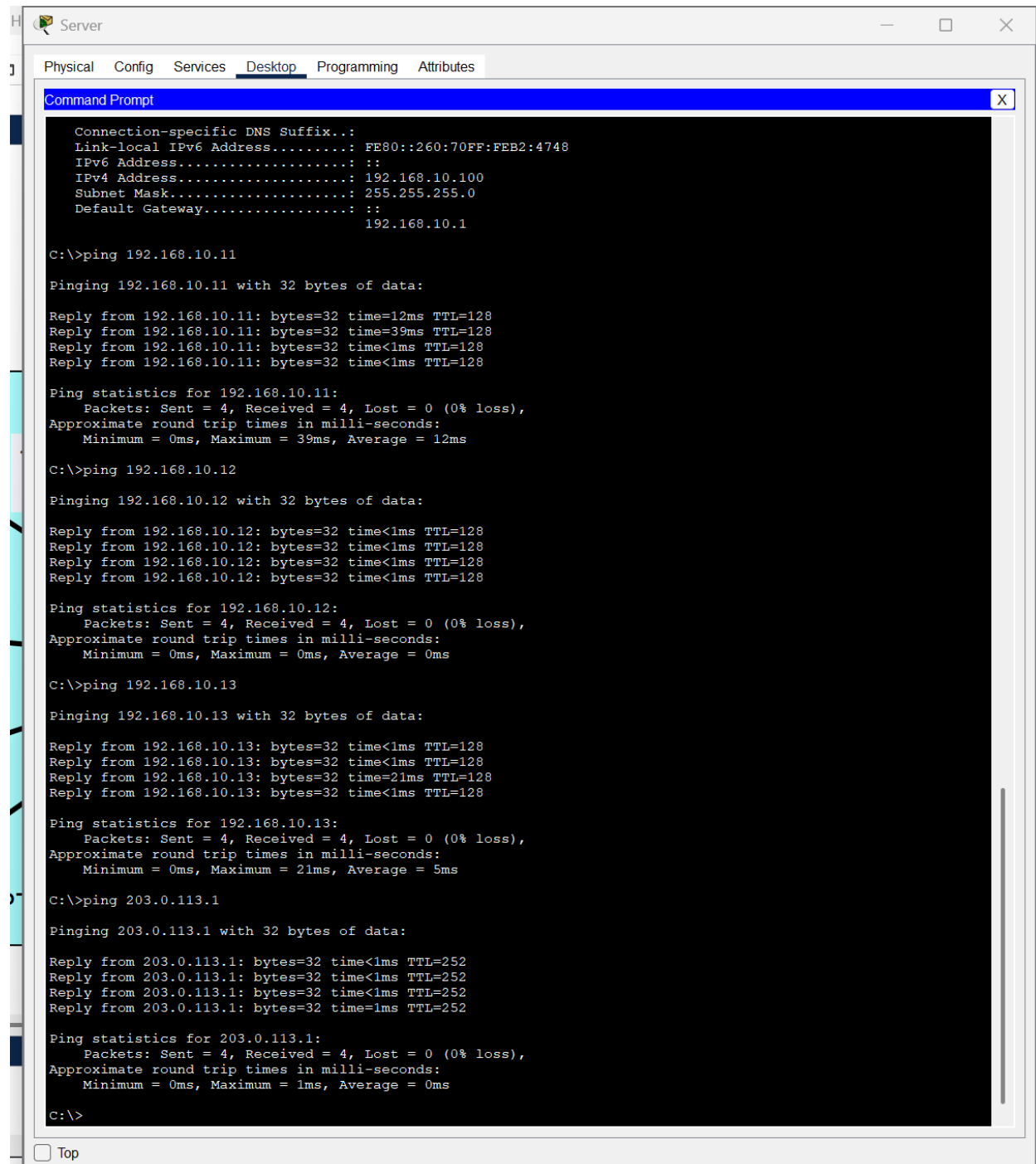
Reply from 203.0.113.1: bytes=32 time<1ms TTL=252
Reply from 203.0.113.1: bytes=32 time=44ms TTL=252
Reply from 203.0.113.1: bytes=32 time=10ms TTL=252
Reply from 203.0.113.1: bytes=32 time=11ms TTL=252

Ping statistics for 203.0.113.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 44ms, Average = 16ms

C:\>
```

☐ Top

Here is also a successful ping from the server to all the PCs and internet router.



The screenshot shows a Packet Tracer window titled "Server" with tabs for Physical, Config, Services, Desktop, Programming, and Attributes. The "Desktop" tab is active, displaying a "Command Prompt" window. The Command Prompt shows the following output:

```
Connection-specific DNS Suffix...:
Link-local IPv6 Address . . . . .: FE80::260:70FF:FEB2:4748
IPv6 Address . . . . .: ::
IPv4 Address . . . . .: 192.168.10.100
Subnet Mask . . . . .: 255.255.255.0
Default Gateway . . . . .: ::
                             192.168.10.1

C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.10.11: bytes=32 time=12ms TTL=128
Reply from 192.168.10.11: bytes=32 time=39ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 39ms, Average = 12ms

C:\>ping 192.168.10.12

Pinging 192.168.10.12 with 32 bytes of data:

Reply from 192.168.10.12: bytes=32 time<1ms TTL=128
Reply from 192.168.10.12: bytes=32 time<1ms TTL=128
Reply from 192.168.10.12: bytes=32 time<1ms TTL=128
Reply from 192.168.10.12: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.13

Pinging 192.168.10.13 with 32 bytes of data:

Reply from 192.168.10.13: bytes=32 time<1ms TTL=128
Reply from 192.168.10.13: bytes=32 time<1ms TTL=128
Reply from 192.168.10.13: bytes=32 time=21ms TTL=128
Reply from 192.168.10.13: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 21ms, Average = 5ms

C:\>ping 203.0.113.1

Pinging 203.0.113.1 with 32 bytes of data:

Reply from 203.0.113.1: bytes=32 time<1ms TTL=252
Reply from 203.0.113.1: bytes=32 time<1ms TTL=252
Reply from 203.0.113.1: bytes=32 time<1ms TTL=252
Reply from 203.0.113.1: bytes=32 time=1ms TTL=252

Ping statistics for 203.0.113.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

At the bottom left of the window, there is a checkbox labeled "Top" which is currently unchecked.

NETWORK SECURITY CONCERNS & RECOMMENDATIONS

Here are the potential weaknesses and actionable improvements to enhance security, segmentation, monitoring, and redundancy:

1. Lack of Proper Segmentation: If devices (e.g., servers, IoT, workstations) share the same subnet, lateral movement by attackers becomes easier.
2. Insufficient Monitoring & Logging
3. No HA (High Availability) for Core Devices: A single router/firewall failure could disrupt the entire network.
4. No Zero Trust Policies: Excessive trust between internal devices increases insider threat risks.
5. Allowing all ICMP (e.g., ping) traffic from any source to any destination inbound from the outside is risky in production. It opens your firewall to ping scans and diagnostics from the public internet.

Recommended actions to improve security

1. Enhance Segmentation
2. Implement VLANs: Separate traffic by department
3. Micro-Segmentation: Use firewalls or SDN to restrict east-west traffic (e.g., only allow DB servers to talk to app servers).
4. Improve Redundancy
5. Dual ISP Connections: Ensure up time if one ISP fails.
6. Adopt Zero Trust: Require MFA and least privilege access for all users/devices.
7. Replace access-list OUTSIDE-IN extended permit icmp any any with a more restrictive one. E.g. access-list OUTSIDE-IN extended permit icmp any host 192.168.10.1 echo