Building and Securing a Small Network

Project 1

Team Members:

Name	Email	Student ID
Ahmed Ahmed Abdelhaleem elattar	Elattar.ahmedahmed@gmail.com	21073293
Ahmed Mohamed Mohamed Mostafa	Okashaa819@gmail.com	21089749
Ibrahim Yasser Ibrahim	Ibrahim.yasser1882@gmail.com	21091393
Mohamed Fetouh Mohamed	mofetouh10@gmail.com	21081976

Network Development Summary

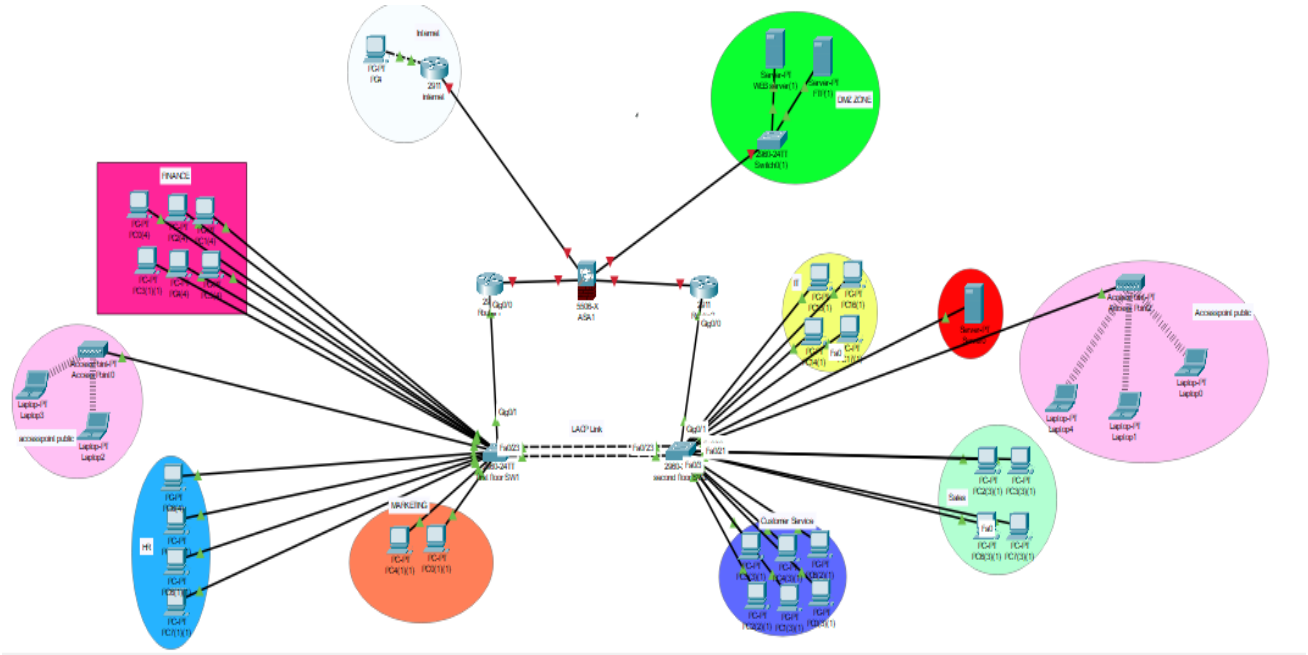
In this project, we designed and implemented a **secure and redundant network infrastructure** for a company with **two floors**, each housing different departments, including **HR, Finance, Marketing, Sales, Customer Service, and IT**. To ensure seamless wireless connectivity, **access points were deployed on each floor**.

The network includes **a web server and an FTP server**, accessible from the external network, and an **internal server**, which is restricted to internal access only. To achieve **high security and redundancy**, the following key components were implemented:

- **Inter-VLAN Routing:** Used to enable communication between different departments.
- **Redundancy:** Implemented using **two routers with HSRP**, ensuring load balancing by prioritizing certain VLANs on **Router 1** and others on **Router 2**. Additionally, **EtherChannel** was configured between the two switches for **high-speed connectivity and fault tolerance**.
- **Firewall Security:** A firewall was configured with **three security zones**:
    - **DMZ** (for public-facing services like web and FTP servers)
    - **Internal Network** (for company resources)
    - **Internet** (external access)
    - ACLs were used to **control access between zones** and **restrict unwanted services** in the DMZ.

- **Routing:** Implemented **OSPF** for efficient dynamic routing.
- **NAT:**
    - **Dynamic NAT** enabled internal devices to access the internet securely.
    - **Static NAT** ensured public accessibility for the **web and FTP servers**.
- **DHCP:** Used for **automatic IP assignment** to internal clients.
- **Layer 2 Security Enhancements:**
    - **Port Security** to prevent unauthorized device connections.
    - **DTP (switchport nonegotiate)** to disable unnecessary trunking.
    - **DHCP Snooping** to prevent rogue DHCP servers.
    - **Dynamic ARP Inspection (DAI)** to block ARP spoofing attacks.
    - **PortFast & BPDU Guard** to protect against spanning tree attacks.

This network design ensures high availability, performance, and security, meeting the company's operational requirements while protecting against potential threats.



Effectiveness of implementing Security measures

Security switch configuration effectively enhances network security, reliability, and efficiency by implementing multiple protective measures. **Port security** limits unauthorized access by restricting MAC addresses per port, using **sticky** MAC addresses to retain known devices, and enforcing violation **restrict** mode to drop unauthorized addresses without shutting down the port and sends a log.

DHCP snooping protects against rogue DHCP servers and DHCP starvation attacks by marking specific ports as trusted and limiting DHCP request rates to prevent getting many fake DHCP requests.

Dynamic ARP Inspection (DAI) further secures the network by validating ARP packets and preventing spoofing attacks, with only trusted ports allowed to send ARP replies.

Spanning Tree enhancements, including **PortFast** and **BPDU Guard**, optimize network performance by reducing delays for end devices and preventing unauthorized switches from affecting the topology and preventing any device connected to untrusted port to act as root switch.

Additionally, disabling **DTP negotiations** with "switchport nonegotiate" secures trunk ports from potential attacks. Overall, this configuration provides a strong security posture while maintaining operational efficiency and network stability.

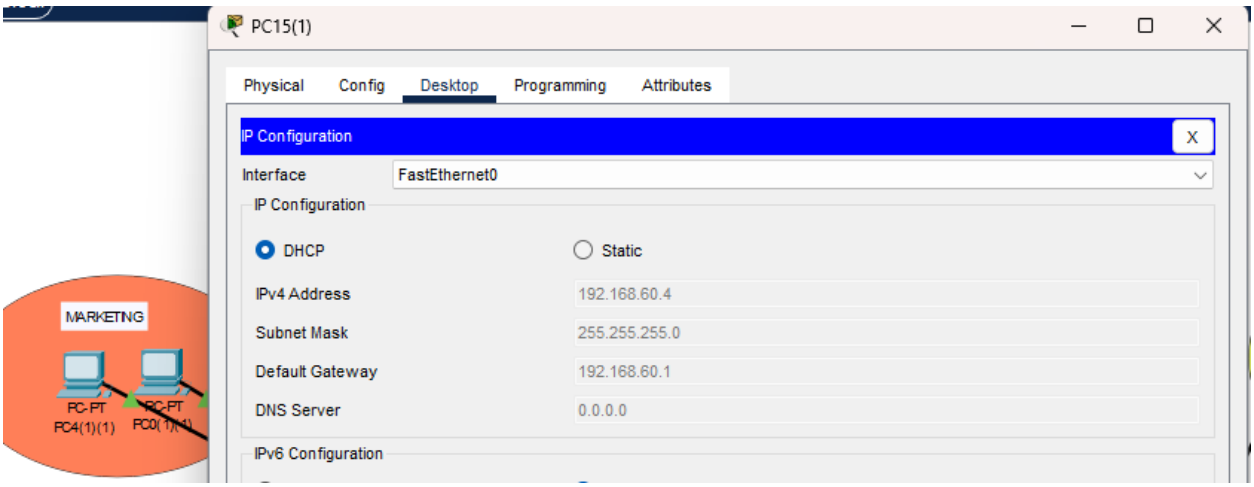
VLan	Name	Network	Interface
10	Hr	192.168.10.0/24	SW1: fa0/1-5
20	Finance	192.168.20.0/24	SW1: fa0/6-15
30	Marketing	192.168.30.0/24	SW1: fa0/16-20
40	Sales	192.168.40.0/24	SW2: fa0/1-5
50	Customer service	192.168.50.0/24	SW2: fa0/6-15
60	IT	192.168.60.0/24	SW2: fa0/16-19
70	Access point	192.168.70.0/24	SW1: fa0/21 & SW2: fa0/21
80	File server	192.168.80.0/24	SW2: fa0/20
90	Management vlan	192.168.90.0/24	N/A
99	Native vlan	192.168.99.0/24	N/A

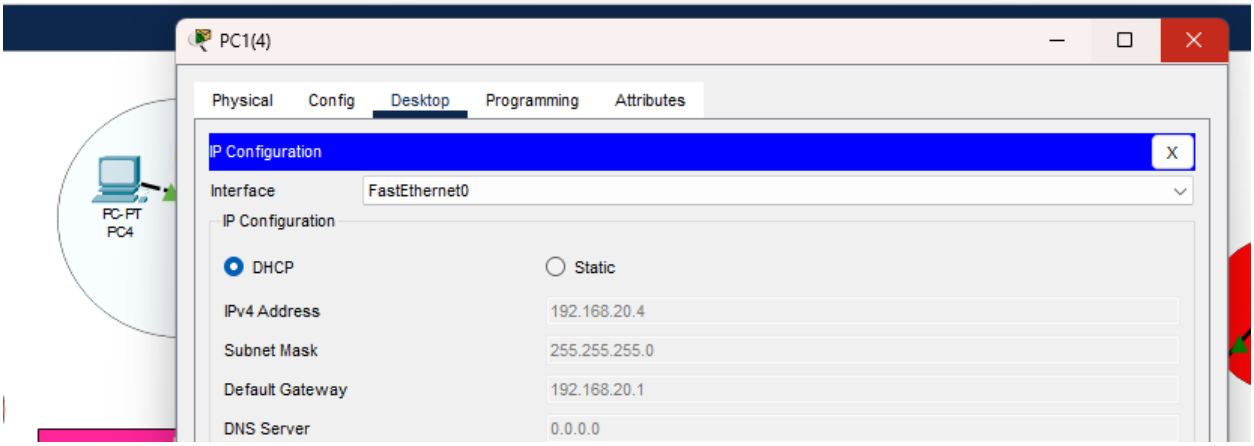
Device	Interface	IP Address	Global IP
R1	Gig0/0.10	192.168.10.2	209.165.200.226
	Gig0/0.20	192.168.20.2	
	Gig0/0.30	192.168.30.2	
	Gig0/0.40	192.168.40.2	
	Gig0/0.50	192.168.50.2	
	Gig0/0.60	192.168.60.2	
	Gig0/0.70	192.168.70.2	
	Gig0/0.80	192.168.80.2	
	Gig0/0.90	192.168.90.2	
	Gig0/0.99	192.168.99.1	
	Gig0/1	10.1.2.2/30	
R2	Gig0/0.10	192.168.10.3	
	Gig0/0.20	192.168.20.3	
	Gig0/0.30	192.168.30.3	
	Gig0/0.40	192.168.40.3	
	Gig0/0.50	192.168.50.3	
	Gig0/0.60	192.168.60.3	
	Gig0/0.70	192.168.70.3	
	Gig0/0.80	192.168.80.3	
	Gig0/0.90	192.168.90.3	
	Gig0/0.99	192.168.99.2	
	Gig0/1	10.1.1.2/30	
SW1	Vlan 90	192.168.90.2	
SW2	Vlan 90	192.168.90.3	
ASA Firewall	Gig1/1	10.1.2.1/30	
	Gig1/2	10.1.1.1 255…252	
	Gig1/3	192.168.100.1	
	Gig1/4	209.165.200.226 255.255.255.248	
File Server		192.168.80.4	N/A
FTP Server		192.168.100.2	209.165.200.228
Web Server		192.168.100.3	209.165.200.227

ASA Firewall Enable Password = group$1

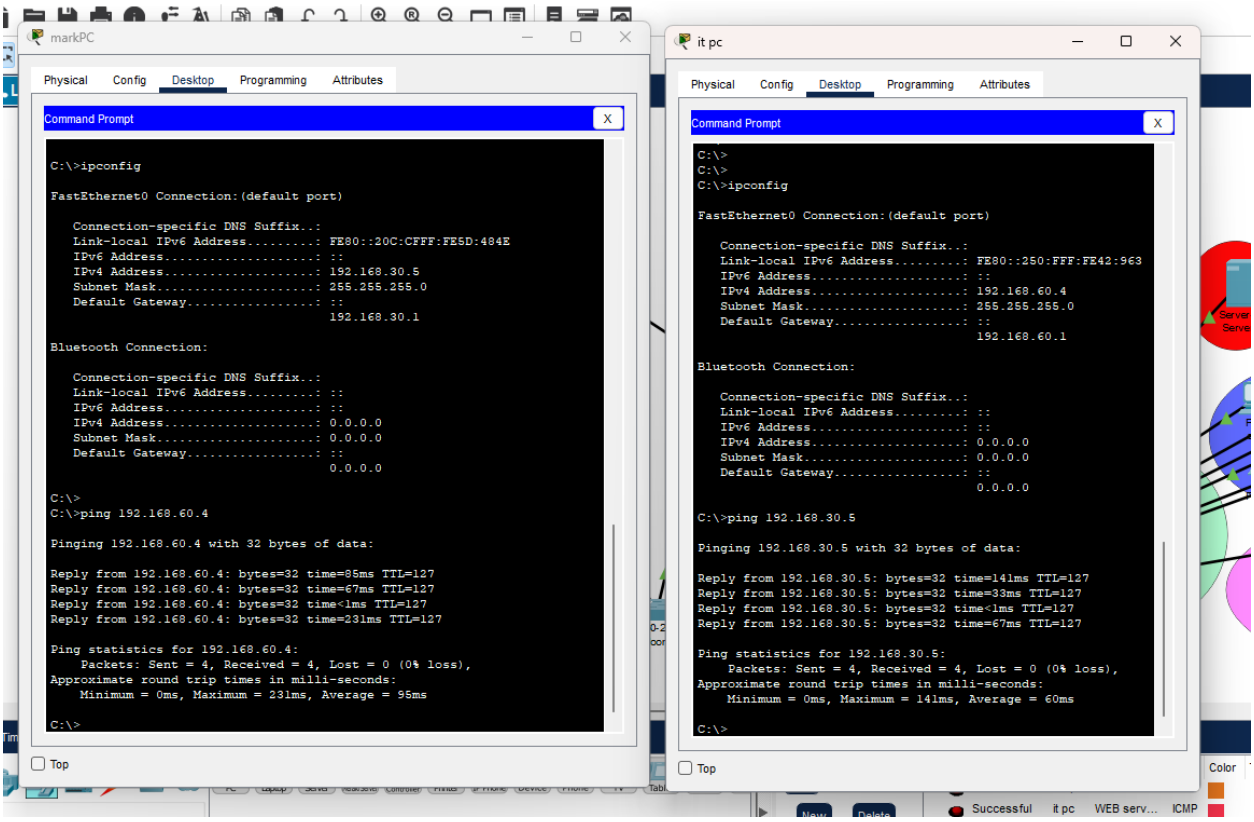
Testing:

1) Ensure that the DHCP server is functioning correctly, assigning unique IP addresses based on the VLAN membership of each PC.

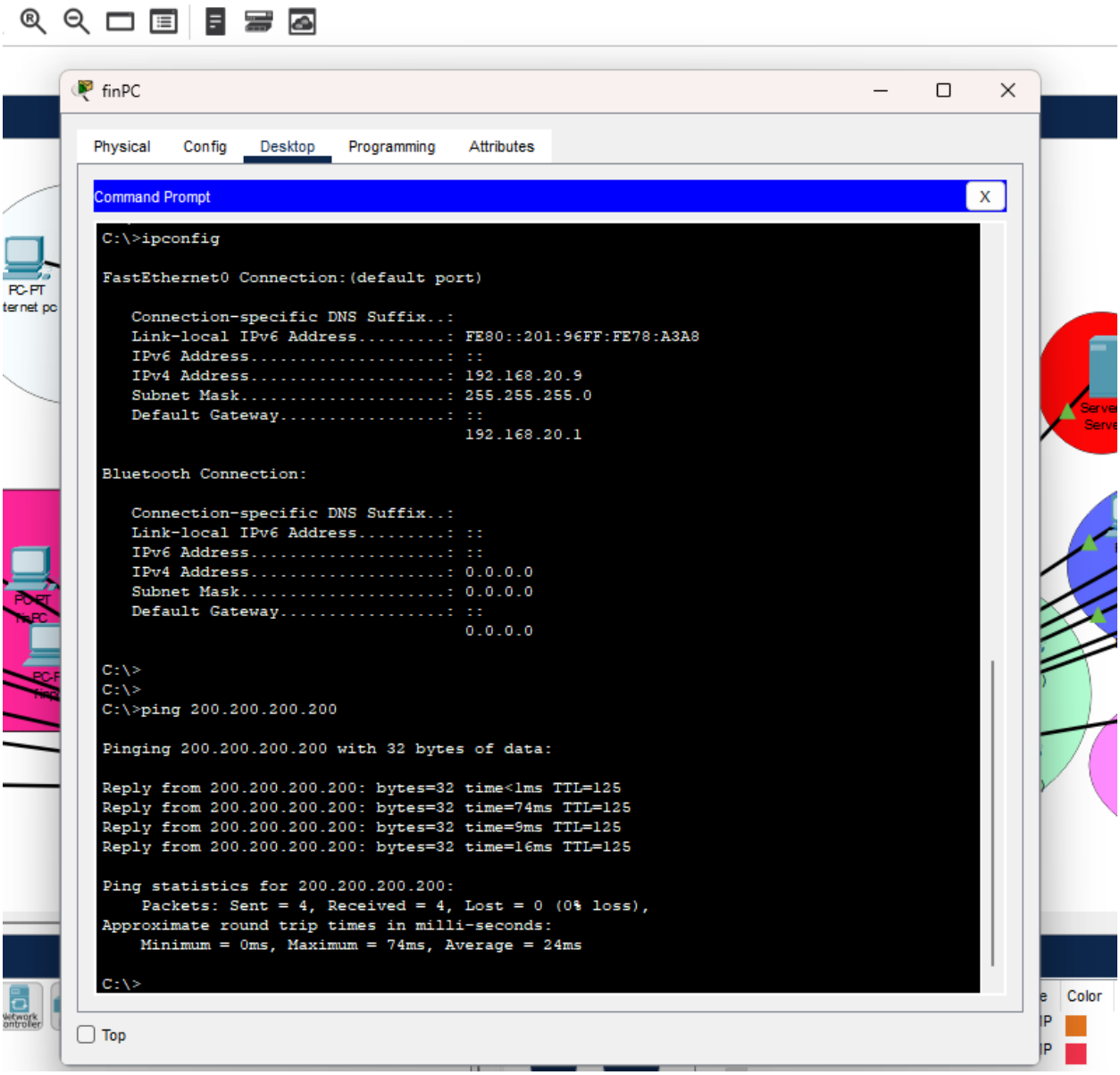

PC15(1)
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.60.4
Subnet Mask
255.255.255.0
Default Gateway
192.168.60.1
DNS Server
0.0.0.0
IPv6 Configuration
MARKETING
PC-PT
PC4(1)(1)
PC-PT


PC1(4)
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.20.4
Subnet Mask
255.255.255.0
Default Gateway
192.168.20.1
DNS Server
0.0.0.0
PC-PT
PC4

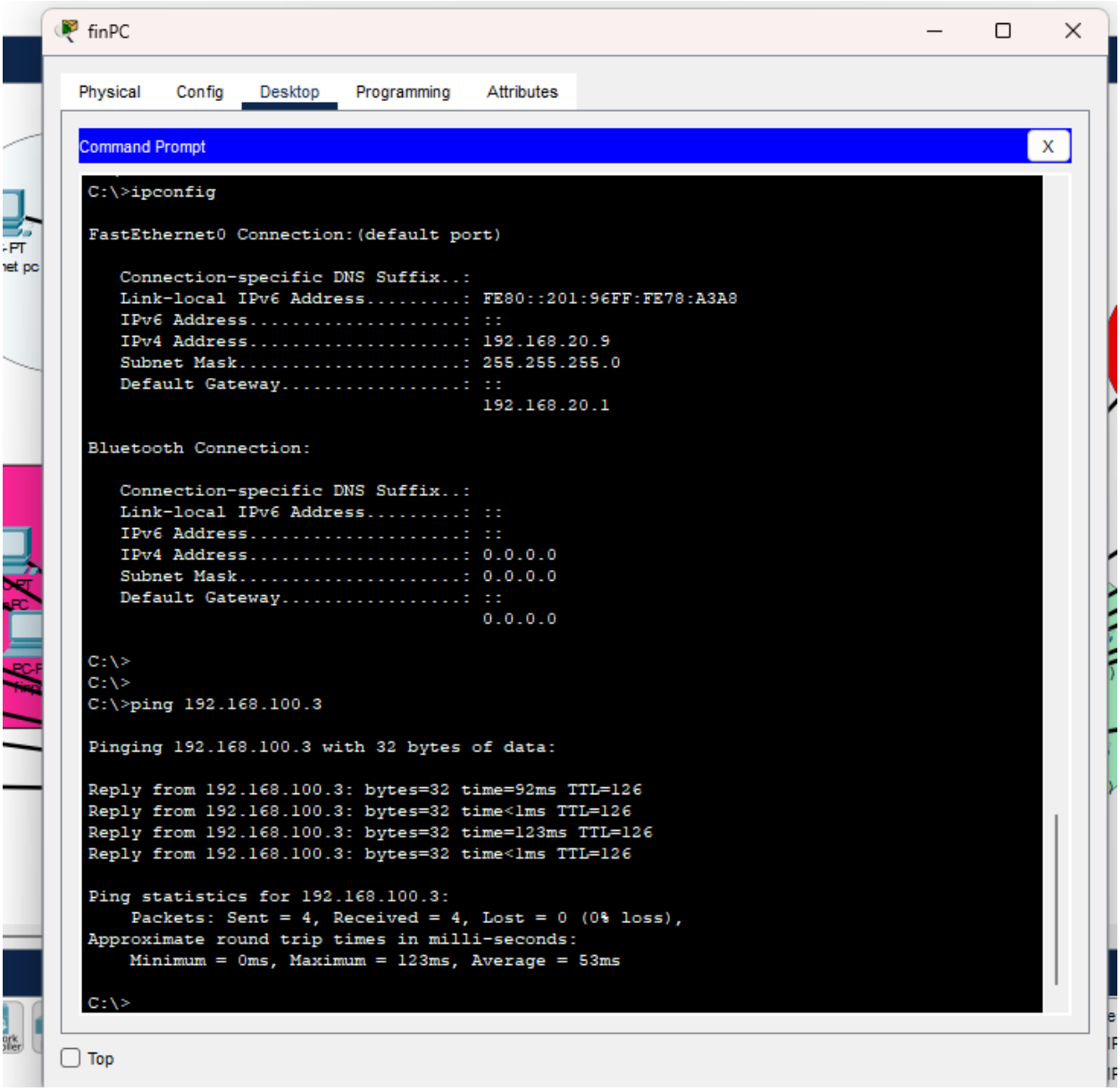
2) Ping between internal PCs is functioning as expected.



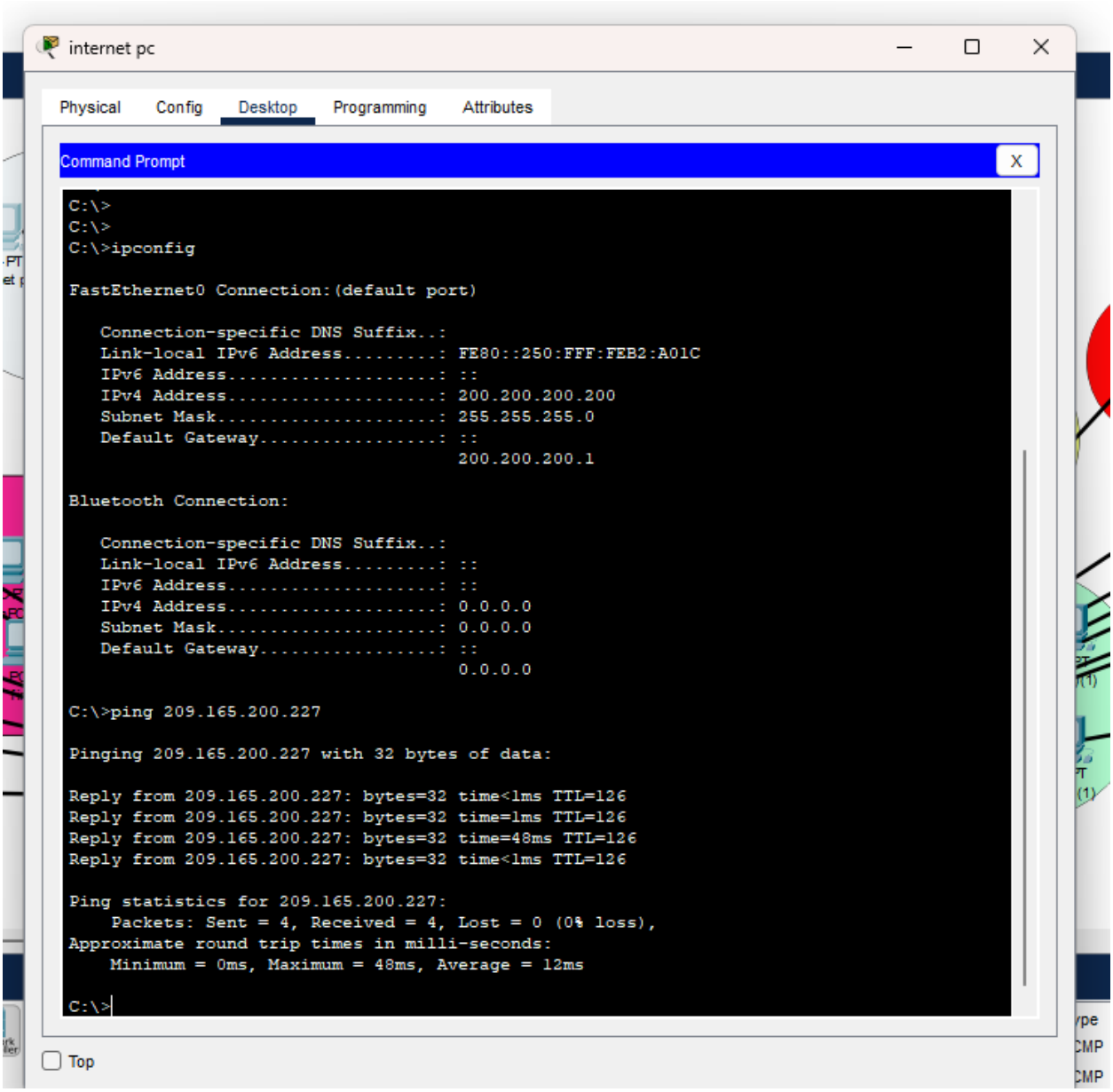
3) Ping from an internal PC to the internet is functioning as expected.



4) Ping from an internal PC to the DMZ is working as expected.



5) Ping from the internet to the DMZ is functioning as expected.



6) As designed, access from the internet to the internal network is blocked.

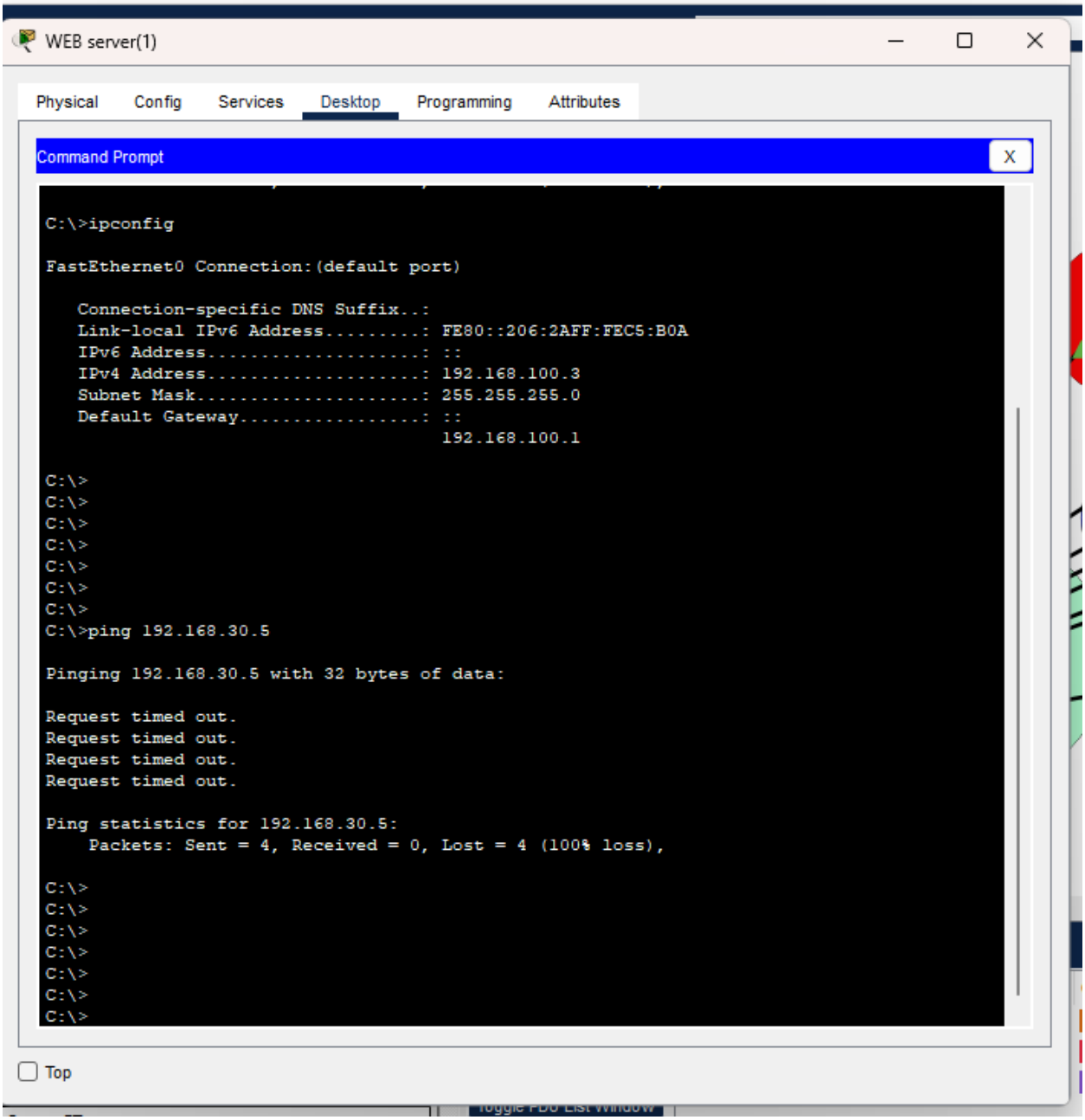
internet pc

Physical | Config | Desktop | Programming | Attributes

Command Prompt

```
C:\>
C:\>
C:\>
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::250:FFF:FEB2:A01C
   IPv6 Address....................: ::
   IPv4 Address....................: 200.200.200.200
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     200.200.200.1

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:\>
C:\>ping 209.165.200.226

Pinging 209.165.200.226 with 32 bytes of data:

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

Ping statistics for 209.165.200.226:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

7) As expected, access to the internal network from the DMZ is restricted, as demonstrated in the attached screenshot.



8) **Port Security was tested by connecting multiple PCs to the same switch port. As a result, the new PC was unable to obtain a DHCP address, remained disconnected from the network, and the violation counter increased by one, indicating that the security mechanism functioned as expected.**