VIETNAM NATIONAL UNIVERSITY, HO CHI MINH CITY
UNIVERSITY OF TECHNOLOGY
FACULTY OF COMPUTER SCIENCE AND ENGINEERING

COMPUTER NETWORKS (CO3093)

Assignment

NETWORK DESIGN AND SIMULATION FOR A CRITICAL LARGE HOSPITAL

Advisor(s): Nguyễn Lê Duy Lai, *CSE-HCMUT*

Students: Nguyễn Văn Đức Long - 2153535
Trần Nguyễn Gia Huy - 2153395
Lê Dương Khánh Huy - 2153380

HO CHI MINH CITY, APRIL 2024

Contents

General Information

Acknowledgement

First of all, we would like to acknowledge and give our warmest regards to our main instructor **Nguyễn Lê Duy Lai** , who has given us a lot of advice and provided us with many instructions on the subject Computer Networks.

Secondly, we would also like to thank our team members who have worked so hard on this project. Everyone has made enjoyable moment, brilliant comments and suggestions. Throughout the project, we have learned how to collaborate effectively between team members to solve many problems.

1 Members' Contribution

No.	Fullname	Student ID	Problems	Contribution
1	Nguyễn Văn Đức Long	2153535	- Logical design, Main site	33.33%
2	Trần Nguyễn Gia Huy	2153395	- Auxiliary site, Connection configuration	33.33%
3	Lê Dương Khánh Huy	2153380	- Report	33.33%

2 Introduction

In response to the construction of Specialized Hospital, CCC (Computer & Construction Consultant) has been entrusted with the pivotal task of designing a robust computer network infrastructure for the hospital Main site (at Ho Chi Minh City) and its two Auxiliary Sites (at DBP street and BHTQ street). This report outlines the comprehensive approach undertaken by CCC to address the unique IT requirements of the hospital and ensure seamless connectivity, enhanced security, and future scalability.

3 Network Structure Design

3.1 Network Topology and Hardware Requirements

The main site:

- Floors (in each building A and B): 5 floors with 10 rooms each
- Data center, IT and cabling central local are in separate room
- Servers: 10
- Networking Devices: 12
- Connectivity:
  - Wired and wireless connections
  - Fiber cabling (GPON)
  - GigaEthernet 1GbE/10GbE/40GbE
- VLAN Structure: Organize the network according to departments
- WAN Connection: Leased lines for interconnecting branches (SD-WAN, MPLS), 2 xDSL for Internet access with load balancing
- Security: Firewall, IPS/IDS, phishing detection
- Software: Mix of licensed and open-source software
- High Availability: Implement redundancy and failover mechanisms

Auxiliary Sites (DBP Street and BHTQ Street):

- Floors: 2 floors
- Floor: IT room and Cabling Central
- Servers: 2
- Networking Devices: 5
- Connectivity: Interconnect with the main sites using selected WAN technology
- Security: Implement firewall and basic security measures
- Software: Use standard office applications and required hospital software

3.2 VPN Configuration

Site-to-site VPN: Use IPSec for secure communication between Headquarters and Branches.
Teleworker VPN: Implement SSL VPN for remote employees connecting to the Company LAN securely.

3.3 WAN Connection Technology

Options:

- SD-WAN: Cost-effective, efficient use of multiple connections.
- MPLS: Reliable and secure, but may be more expensive.

Cost Analysis:

- Compare initial setup costs and recurring expenses.
- Consider long-term scalability and ease of management.

Advantages and Disadvantages:

- SD-WAN:
  - Advantages: Cost-effective, flexible, easy to manage.
  - Disadvantages: May have lower security compared to MPLS.
- MPLS:
  - Advantages: High security, reliable, suitable for critical applications.
  - Disadvantages: Higher cost, potential for longer implementation.

3.4 Network System Requirements and Scalability

- Growth Rate: Plan for a 20% growth in the future.
- Traffic Analysis: Peak hours, dataflow, and workload considerations.
- Network Load Balancing: Implement load balancers at critical points for optimal performance.
- Device Configuration: Choose devices based on high-load areas.

3.5 Network Structure and Aesthetics

- Building Architecture: Design network structure considering aesthetics.
- Wireless Environment: Ensure secure wireless access points (WAPs).
- Network Security Standards: Implement standard security protocols (firewalls, DMZ).
- Server Farm: Centralize servers in a secure server farm.
- Partitioning: Set up partitions for network servers and devices (e.g., DMZ for externalfacing services).

3.6 Checklist for Installation Locations

- Verify the availability of power outlets.
- Confirm physical security measures.
- Check for cable pathways and accessibility.
- Validate network coverage for wireless environments.

4 Technical Requirements

4.1 List of Minimum Requrements

The Main site:

- Switches:
  - Quantity: 13 x 48-port GigaEthernet switches for 600 workstations
  - Quantity: 1 x 24-port GigaEthernet switch for 10 servers
  - Quantity: 1 x 12-port GigaEthernet switch for 12 networking devices
- Routers:
  - Quantity: 10 x Router with SD-WAN capabilities or MPLS support for building A & B.
  - Quantity: 1 x Firewall/Security Appliance for DMZ
- Access Points:
  - Quantity: 10 x Sufficient wireless access points for complete coverage, 1 for each floor
- Servers:
  - Quantity: 3 x Servers with recommended specifications, including 1 for the internet
- Cabling:
  - Quantity: Sufficient Cat6 cables for workstations, servers, and networking devices
  - Quantity: Fiber optic cables for GPON connections
- Security Devices:
  - Quantity: 1 x Intrusion Prevention System (IPS)
  - Quantity: 1 x Phishing Detection Appliance
- Teleworker VPN:
  - Quantity: Licenses for SSL VPN connections

Auxiliary Sites:

- Switches:
  - Quantity: 3 x 24-port GigaEthernet switch for 60 workstations

  - Quantity: 1 x 12-port GigaEthernet switch for servers and networking devices

- Routers/Firewall:
  - Quantity: 1 x Firewall for basic security
  - Quantity: 4 x Router for 4 floors

- Access Points:
  - Quantity: 4 x Sufficient wireless access points for complete coverage, 1 for each floor

- Servers:
  - Quantity: 3 x Servers with recommended specifications, including 1 for the internet

- Cabling:
  - Quantity: Sufficient Cat6 cables for workstations, servers, and networking devices

4.2 Subnet Size

The subnet mask we have employed is 255.255.255.0, yielding a capacity for hosts represented by 2^8, which is equivalent to 256. This allocation proves sufficient to meet the numerical demands for workstation.

4.3 IP Plan

The main Site:

- VLAN1: Separate room: The data center, IT, and Cabling Central Local - 192.168.2.0/24
- VLAN2: First Floor - 192.168.3.0/24
- VLAN3: Second Floor - 192.168.4.0/24
- VLAN4: Third Floor - 192.168.5.0/24
- VLAN5: Fourth Floor - 192.168.6.0/24
- VLAN6: Fifth Floor - 192.168.7.0/24
- VLAN7: Camera - 192.168.8.0/24

Auxiliary Site (DBP Street)

- VLAN1: First Floor: IT room and Cabling Central Local - 192.168.9.0/24
- VLAN2: Second Floor - 192.168.10.0/24
- VLAN3: Camera - 192.168.11.0/24

Auxiliary Site (DBHTQ Street)

- VLAN1: First Floor: IT room and Cabling Central Local - 192.168.12.0/24
- VLAN2: Second Floor - 192.168.13.0/24
- VLAN3: Camera - 192.168.14.0/24

4.4 Recommended Equipment and Specifications

- Switches:
  - Model: Cisco Catalyst 2960X Series
  - Specifications: 48-port GigaEthernet, Layer 2/Layer 3 capabilities
- Router/Firewall:
  - Model: Cisco ISR 4000 Series
  - Specifications: SD-WAN capable, or MPLS support, integrated firewall
- Access Points:
  - Model: Cisco Aironet 2800 Series
  - Specifications: Dual-band, high-performance wireless access points
- Servers:
  - Model: Dell PowerEdge R640
  - Specifications: Dual processors, ample RAM and storage
- Cabling:
  - Type: Cat6 for Ethernet, Fiber optic for GPON
  - Specifications: Compliant with industry standards
- Security Devices:
  - IPS: Cisco Firepower Next-Generation IPS
  - Phishing Detection: Cisco Email Security Appliance
- VPN Solution:
  - Model: Cisco AnyConnect for SSL VPN

4.5 WAN Coneection Diagram

- SD-WAN Configuration:
  - Utilize multiple ISP connections for redundancy and load balancing.
  - Implement SD-WAN controllers for intelligent routing and traffic optimization.
- MPLS Configuration:
  - Establish MPLS connections between Headquarters and Branches for secure and reliable communication.
  - Implement OSPF routing protocol for dynamic route management within the MPLS network.
- Connection Redundancy:
  - Ensure fail-over mechanisms for both SD-WAN and MPLS connections.
- Firewall Configuration:
  - Implement firewall rules to control traffic between Main site and Auxiliary sites.

5 Technical Configuration

5.1 Main site network

- The total download estimate of each server is about 1000 MB/day and the upload estimate is 2000 MB/day. The dataflows and workload of the headquarter is about 80% at peak hours 9g-11g and 15g-16g. We have 10 servers:

$$\text{Throughput} = \frac{10 \times 3000 \times 8}{24 \times 3600} = 2.78\,\text{Mbps}$$

$$\text{Bandwidth} = \frac{10 \times 3000 \times 0.8 \times 8}{3 \times 3600} = 17.78\,\text{Mbps}$$

- The total download estimate of each workstation is about 500 MB/day and the upload estimate is 100 MB/day. The dataflows and workload of the headquarter is about 80% at peak hours 9g-11g and 15g-16g. We have 600 workstations:

$$\text{Throughput} = \frac{600 \times 600 \times 8}{24 \times 3600} = 33.33\,\text{Mbps}$$

$$\text{Bandwidth} = \frac{600 \times 600 \times 0.8 \times 8}{3 \times 3600} = 213.33\,\text{Mbps}$$

- WiFi-connected devices from customer's access is 500 MB/day

$$\text{Throughput} = \frac{500 \times 8}{24 \times 3600} = 0.046\,\text{Mbps}$$

$$\text{Bandwidth} = \frac{500 \times 0.8 \times 8}{3 \times 3600} = 0.296\,\text{Mbps}$$

- The total throughput and bandwidth of the Main site

$$\text{Throughput} = 2.78 + 33.33 + 0.046 = 36.156\ \text{Mbps}$$
$$\text{Bandwidth} = 17.78 + 213.33 + 0.296 = 231.406\ \text{Mbps}$$

5.2 Auxiliary site network

- The total download estimate of each server is about 1000 MB/day and the upload estimate is 2000 MB/day. The dataflows and workload of the headquarter is about 80% at peak hours 9g-11g and 15g-16g. We have 2 servers:

$$\text{Throughput} = \frac{2 \times 3000 \times 8}{24 \times 3600} = 0.556\,\text{Mbps}$$

$$\text{Bandwidth} = \frac{2 \times 3000 \times 0.8 \times 8}{3 \times 3600} = 3.556\,\text{Mbps}$$

- The total download estimate of each workstation is about 500 MB/day and the upload estimate is 100 MB/day. The dataflows and workload of the headquarter is about 80% at peak hours 9g-11g and 15g-16g. We have 600 workstations:

$$\text{Throughput} = \frac{60 \times 600 \times 8}{24 \times 3600} = 3.333\,\text{Mbps}$$

$$\text{Bandwidth} = \frac{60 \times 600 \times 0.8 \times 8}{3 \times 3600} = 21.333\,\text{Mbps}$$

- WiFi-connected devices from customer's access is 500 MB/day

$$\text{Throughput} = \frac{500 \times 8}{24 \times 3600} = 0.046\,\text{Mbps}$$

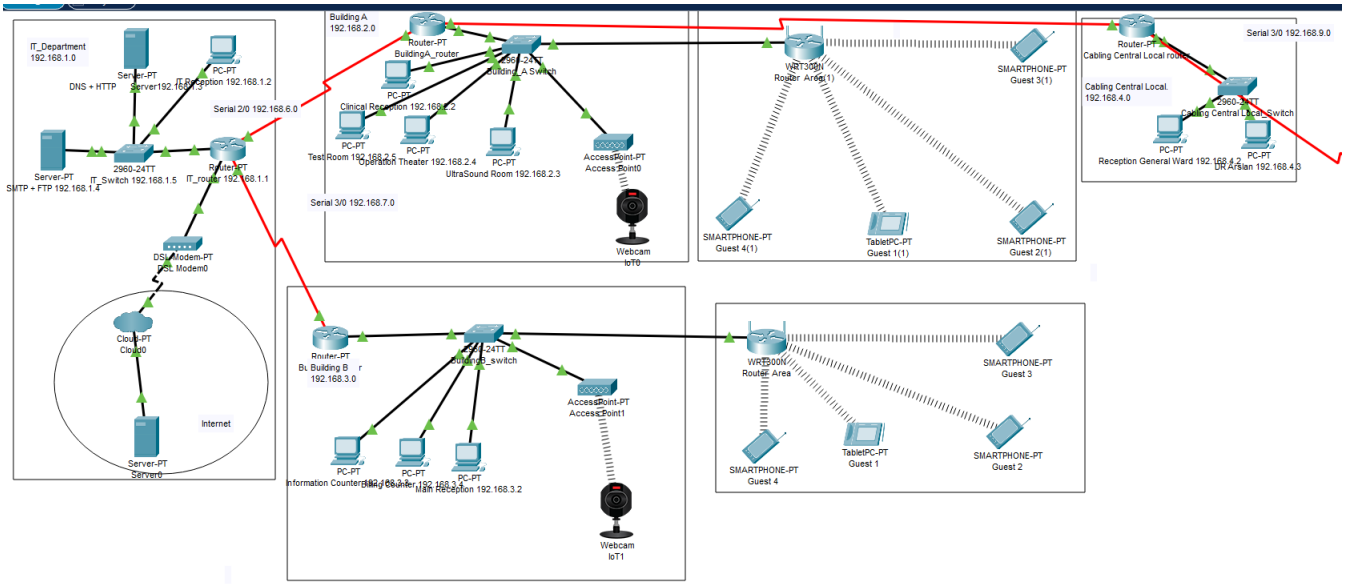
$$\text{Bandwidth} = \frac{500 \times 0.8 \times 8}{3 \times 3600} = 0.296\,\text{Mbps}$$

- The total throughput and bandwidth of the Main site

$$\text{Throughput} = 0.556 + 3.333 + 0.046 = 3.935\ \text{Mbps}$$
$$\text{Bandwidth} = 3.556 + 21.333 + 0.296 = 25.185\ \text{Mbps}$$

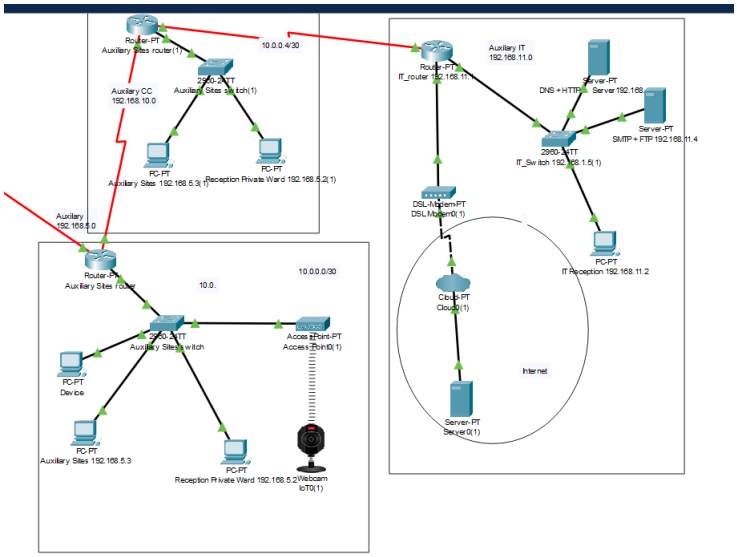
6 Network Map Design

6.1 Main site



Hình 1: Main Site

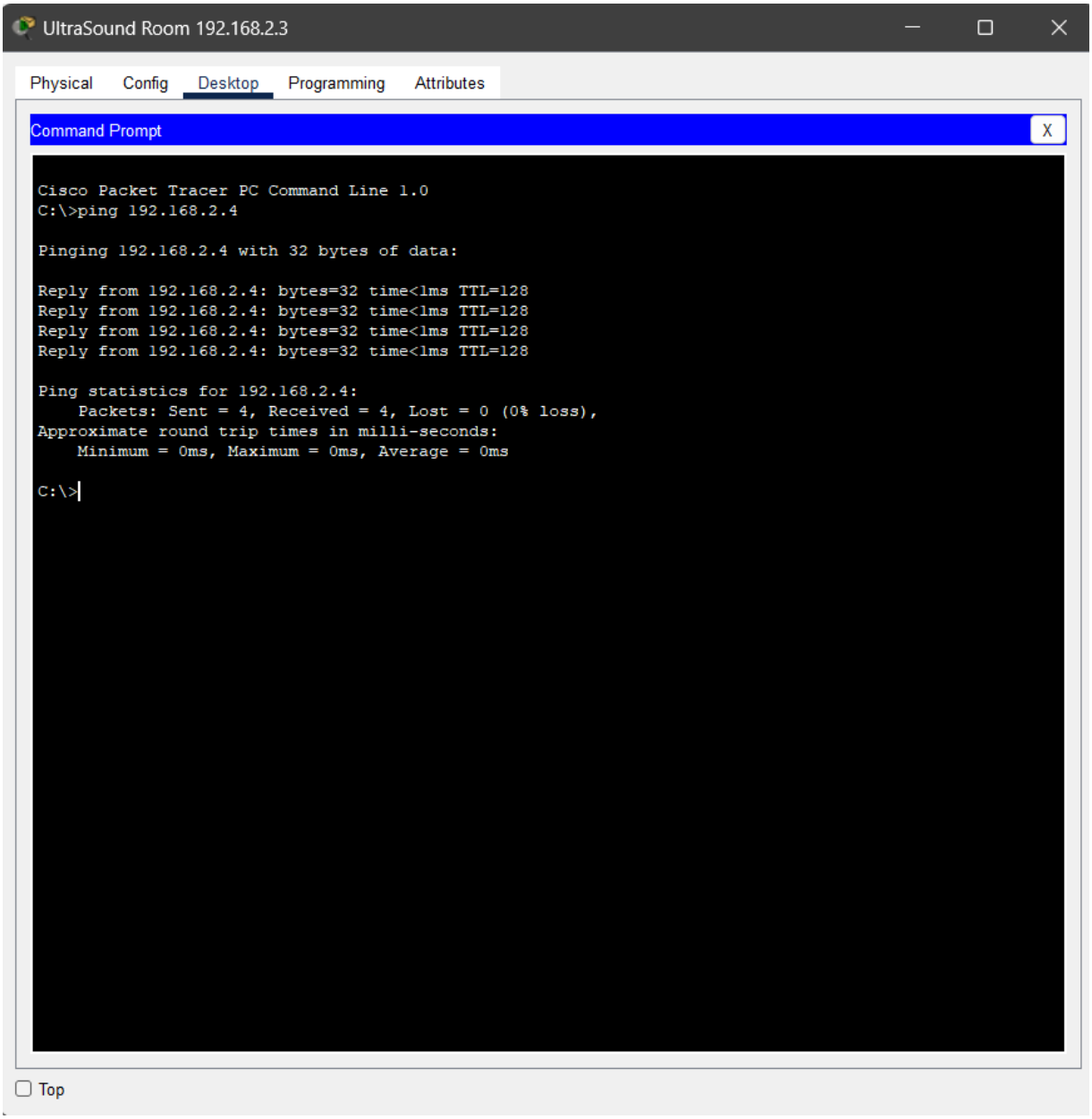
6.2 Auxiliary site



Hình 2: Auxiliary Site

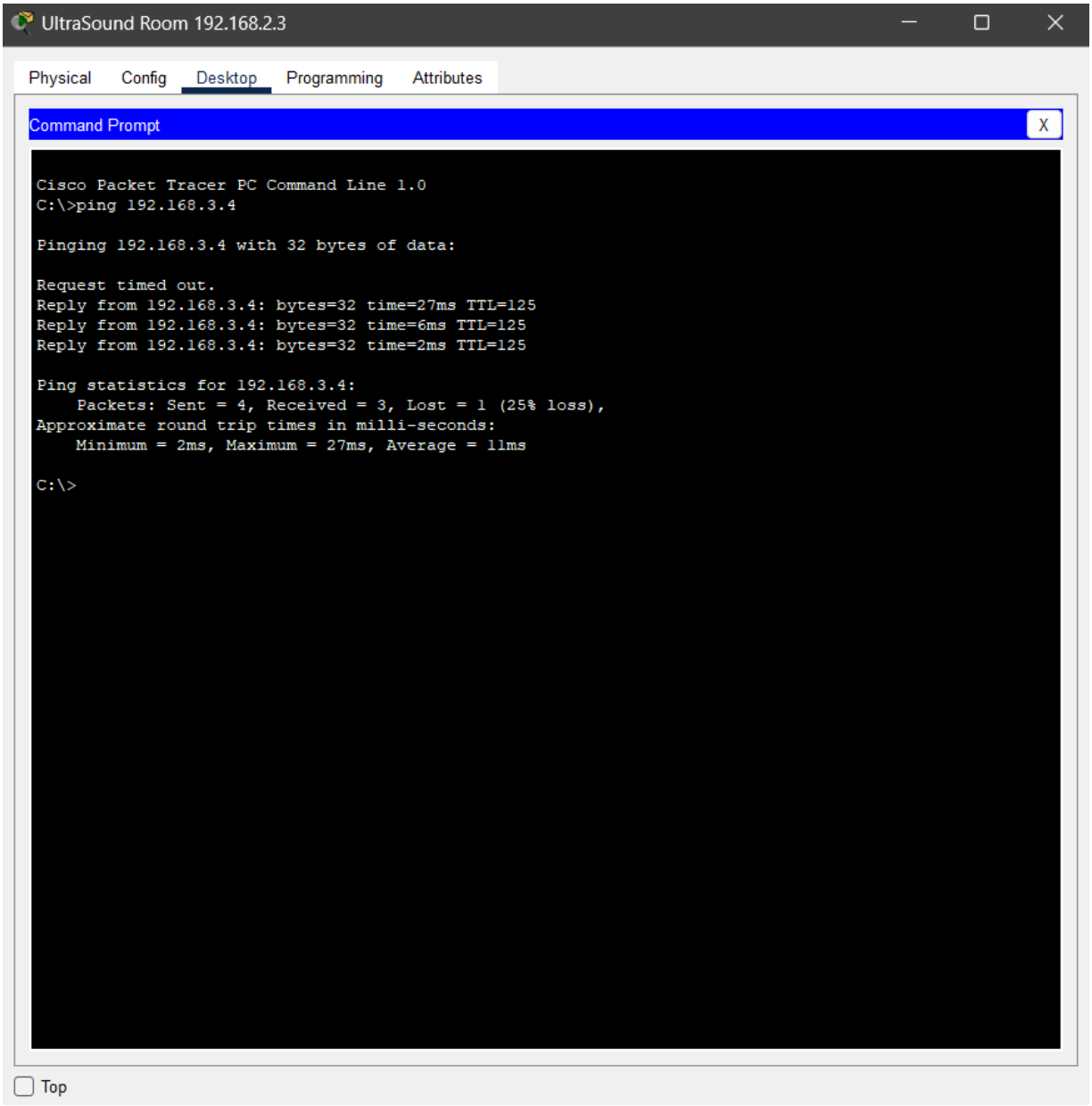
7 Testing

7.1 Connection between PCs in the same VLAN



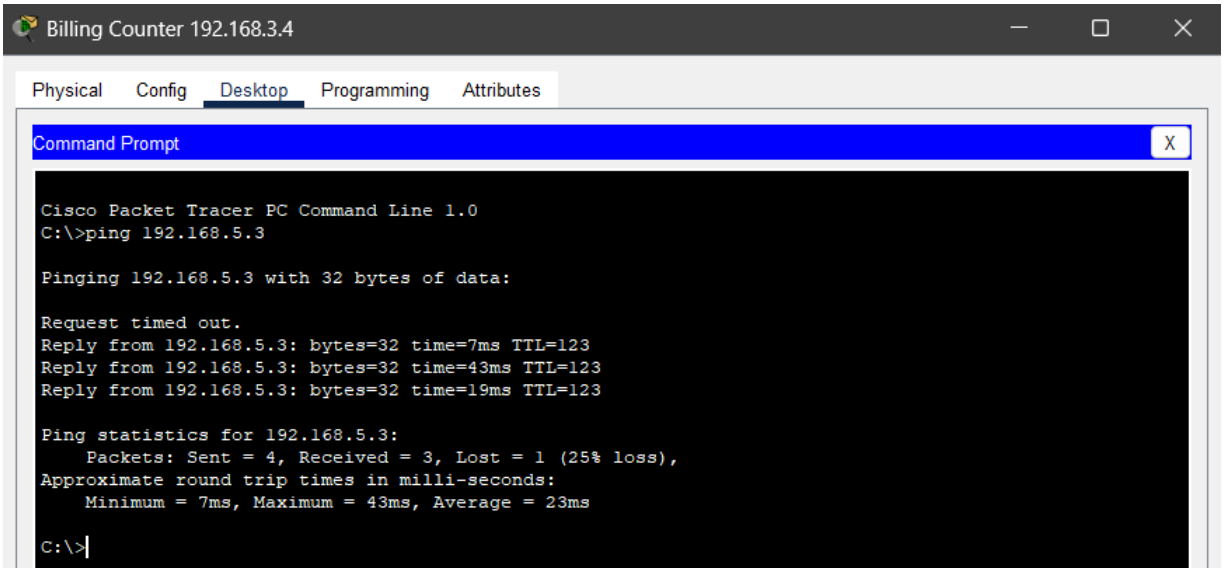
Hình 3: Connection between PCs in building A (same VLAN)

7.2 Connection PCs between VLANs

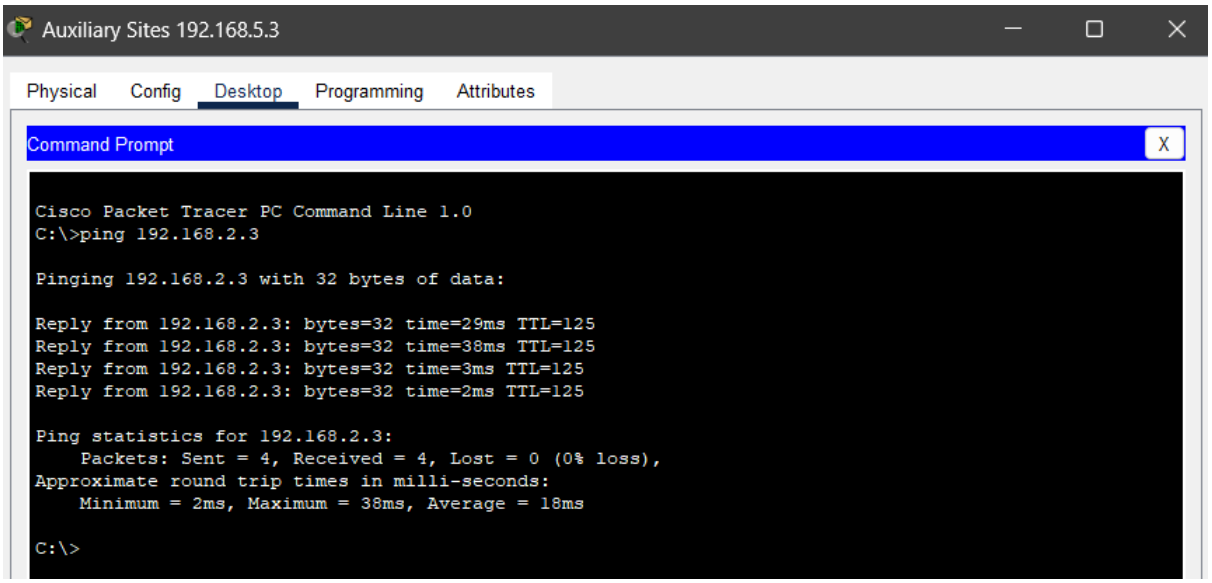


Hình 4: Connection from PC in building A to building B (different VLAN)

7.3 Connection PCs between the main Site and the two Auxiliary Sites

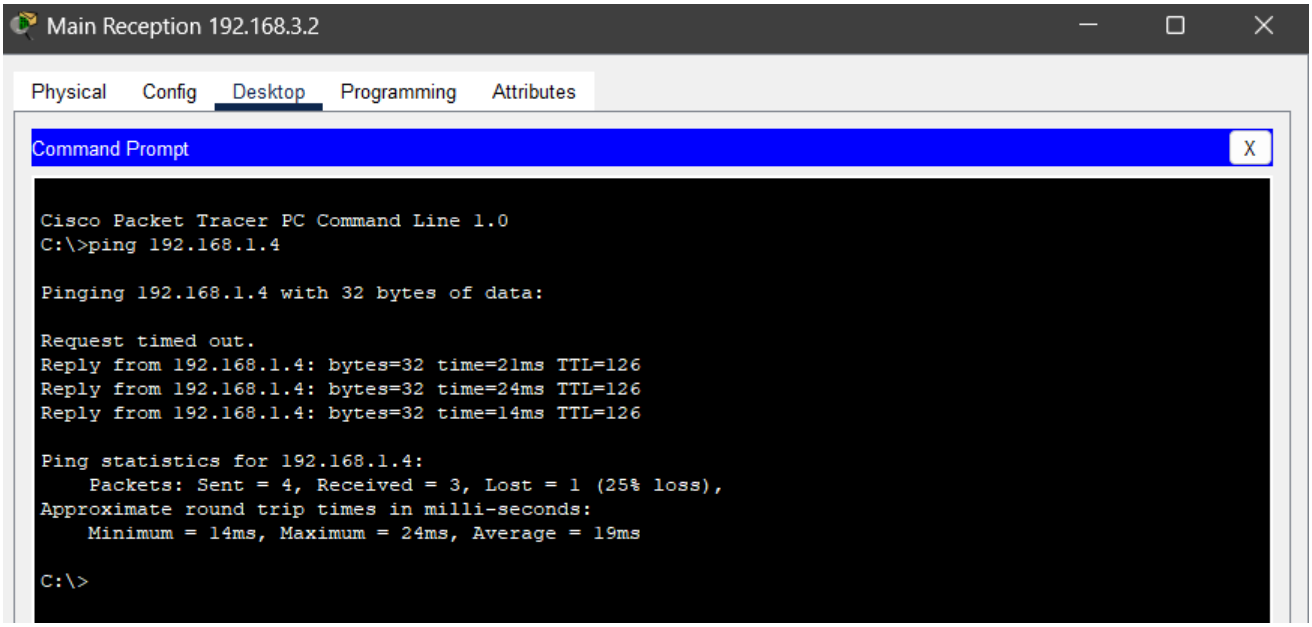


Hình 5: Connection from PC in building A to PC in Auxiliary site

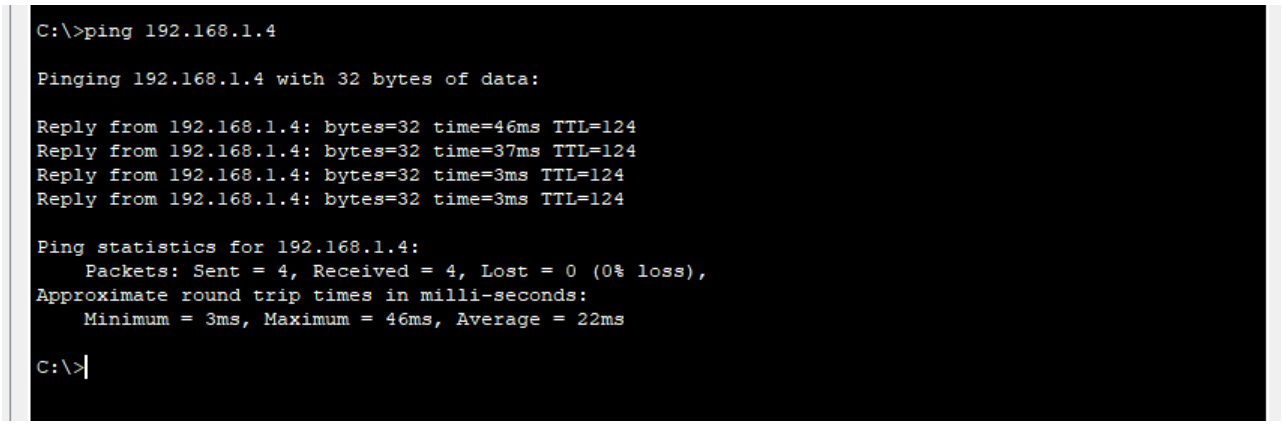


Hình 6: Connection from PC in Auxiliary site to PC in building A

7.4 Connection to server in the DMZ

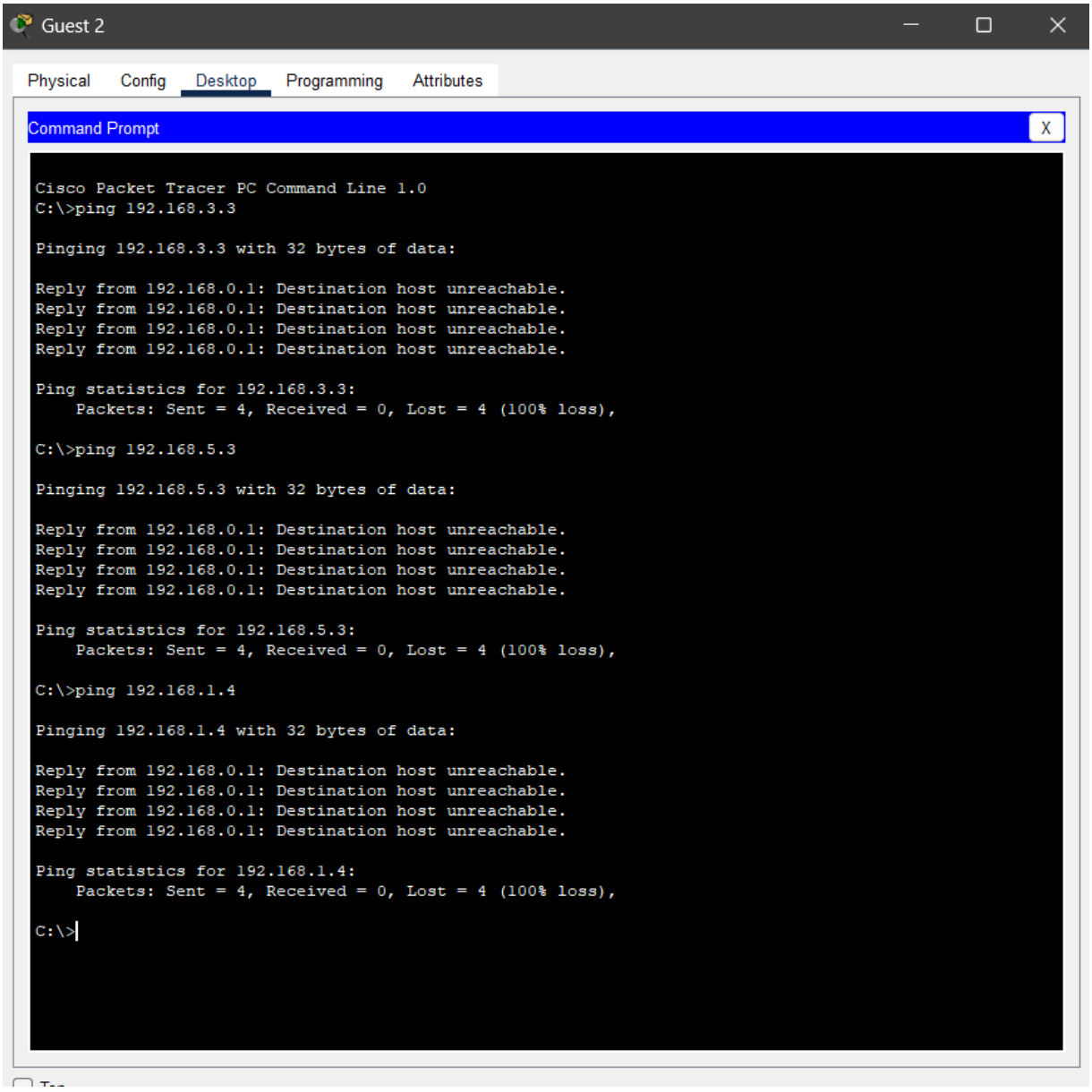


Hình 7: Connection from PC in main site to server in DMZ



Hình 8: Connection from PC in Auxiliary site to server in DMZ

7.5 No connections from Customers' devices to PCs on the LAN



Hình 9: Connection from guest's device to PC in main site, auxiliary site and server in DMZ

8 System Evaluation & Development Orientation

8.1 Reliability

The system ensures communication between devices following the requirements.

8.2 Security

- Prevent unauthorized access from the Internet to the internal network system.
- Guarantee that servers situated in the "Non-military" DMZ zone are unable to establish connections with the internal network.
- Prevent customers using WiFi connections from accessing the internal network system.
- Restrict access to the cameras to only computers within the Security department.

8.3 Remaining problems

- We have not configured any firewall and DMZ, so the security of the system is extremely weak and traffic from the Internet can access enterprise's network.
- We don't have specific knowledge about a particular enterprise network, so when designing, we encounter difficulties in deciding which models, technologies, and devices should be used.
- The system doesn't have load balancing devices to manage unexpected spikes in network traffic, particularly when branches are simultaneously connecting to the Internet.
- The system doesn't have VPN connections in place for employees to access the company LAN network while working remotely.
- The system lacks IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) capabilities to identify and stop intrusion attempts.
- Strategy for data growth and implement efficient backup and archiving solutions.

8.4 Future Development Orientation

- The network architecture should be re-designed to provide a more structured and organized topology that allows for better traffic management and control.
- Access control policies should be implemented to control who has access to the network and what they are authorized to do. This can help prevent unauthorized access and reduce the risk of data breaches.
- Utilize automation tools for tasks like provisioning, configuration, and patching for improved efficiency.
- Continuously evaluate new technologies and adapt the network design accordingly to remain competitive.

9 Conclusion

Throughout this network design assignment, we acquired invaluable experience in crafting topologies for enterprise or public networks.

Employing tools like Packet Tracer presented challenges, yet the process was ultimately rewarding. Conquering hurdles such as configuring firewalls and OSPF routing bolstered our problem-solving abilities.

This project not only enhanced our comprehension of network architecture, security protocols, and routing methodologies but also ignited a deeper passion for network design and simulation.

Overall, we are satisfied with the results. This assignment afforded us hands-on practice and furnished us with the expertise needed to address real-world network complexities.