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

COMPUTER NETWORK (CO3093)

Assignment 2

NETWORK DESIGN AND SIMULATION FOR A CRITICAL LARGE HOSPITAL

Instructor: Bùi Xuân Giang
Students: Đặng Quốc An - 2210002.
Nguyễn Phúc An - 2210022.
Ngô Trường Bách - 2210183.
Nguyễn Duy Bách - 2210185.

Contents

Member list & Work Load

STT	Họ và tên	MSSV	% hoàn thành
1	Đặng Quốc An	2210002	100%
2	Nguyễn Phúc An	2210022	100%
3	Ngô Trường Bách	2210183	100%
4	Nguyễn Duy Bách	2210185	100%

Bảng 1: Danh sách thành viên & Nhiệm vụ

1 Suitable Network Structures for Buildings

1.1 Network System Requirements of the Main Site and Two Auxiliary Sites

1.1.1 Main Site

- Includes two buildings (A and B), each with 5 floors and 10 rooms per floor, equipped with computers and medical devices.
- The Data Center, IT Room, and Cabling Central (using patch panels for cable management) are housed in a separate facility, located approximately 50 meters from buildings A and B.
- Medium-scale infrastructure with around 600 workstations, 10 servers, and 12 networking devices (potentially more when including security appliances).
- Wireless coverage must extend throughout the entire Main Site.
- Utilizes modern network technologies including both wired and wireless connections, fiber cabling (GPON), and GigaEthernet standards (1GbE/10GbE/40GbE). The network is structured using VLANs to separate departmental traffic.
- The Main Site subnetwork connects to the two Auxiliary Sites (DBP and BHTQ) through two leased lines for WAN connectivity, potentially applying SD-WAN, MPLS, and OSPF routing protocols.
- Dual xDSL lines provide Internet access with load-balancing for optimized traffic management. All outbound Internet traffic routes through the Main Site.
- Software environment includes a mix of licensed and open-source applications, hospital information systems (HIS, RIS-PACS, LIS, CRM), office tools, client-server applications, multimedia, and database systems.
- The network must support scalability, robust security (e.g., firewalls, IPS/IDS, phishing protection), high availability, and resilience in case of failures. The infrastructure should also allow for easy upgrades.
- A VPN configuration is required for both site-to-site connections and for remote teleworkers to securely access the hospital's LAN.
- A surveillance camera system must be proposed for the hospital premises.

1.1.2 Auxiliary Sites

- Each building consists of 2 floors, with an IT room and a Cabling Central on the ground floor.
- Small-scale setup with approximately 60 workstations, 2 servers, and at least 5 networking devices.

1.1.3 System Throughput and Bandwidth

- Propose cost-effective options and analyze the pros and cons of each solution.
- Peak data traffic occurs between 9:00–11:00 and 15:00–16:00, accounting for about 80% of total load across the Main and Auxiliary Sites.
- Servers handle tasks such as software updates, web services, and database access. Estimated total daily download is about 1000 MB, with 2000 MB of upload.
- Each workstation is used for web browsing, downloading documents, and handling customer interactions. Per workstation, daily download is estimated at 500 MB and upload at 100 MB.
- WiFi access for patients and visitors accounts for approximately 500 MB of daily download.
- The hospital network is expected to grow by 20% over the next 5 years in terms of users, traffic load, and physical expansion.

1.2 Pre-Installation Checklist at Deployment Sites

Before installing networking devices:

1. Verify that each floor has sufficient physical space for all planned workstations and networking equipment. Pay special attention to the ground floor due to critical equipment being installed there.
2. Ensure physical security for the IT room to prevent unauthorized access.
3. Confirm that adequate ventilation or cooling systems are in place to maintain optimal operating conditions for servers and network hardware.
4. Position edge switches and wireless access points securely to discourage tampering by staff or visitors.
5. Check the inventory to ensure all necessary devices are available for deployment.

After installation and configuration:

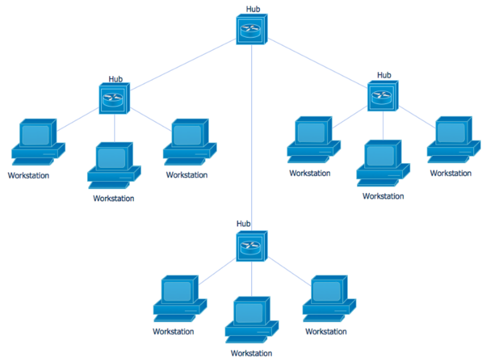
1. Each workstation should be able to communicate with others on the same floor, across the building, and throughout the hospital network.
2. Workstations must be capable of uploading/downloading data from local and remote servers according to hospital access policies.

1.3 High Load Areas

- Network Load Balancing is a critical feature, ensuring traffic is evenly distributed across servers performing similar functions. This prevents server overloads and facilitates system uptime by redirecting traffic if a server fails. It allows for easy scalability by adding or removing servers as needed.
- The hospital's web server infrastructure must support high-speed and stable access, particularly for public-facing services.
- Buildings A and B experience high foot traffic from patients and visitors and generate significant data. These should be prioritized for load balancing and performance optimization.

1.4 Network Structure

- The network is designed using a star topology with 100/1000 Mbps switches.



Hình 1: Star Topology

This topology is scalable and allows devices to be added or removed without affecting the rest of the network. Each device connects directly to a central hub, simplifying troubleshooting and maintenance, and improving overall performance and expandability.

- The server infrastructure located in the IT room includes:
  - File Server – Centralized storage for documents and data needed across departments.
  - Authentication Server – Handles user login and access permissions.
  - Print Server – Manages print jobs and coordinates printer access across the hospital.
  - VPN Server – Enables secure remote access to hospital resources for authorized users.
  - PACS Server – Stores and manages medical imaging data (e.g., X-rays, MRI).

1.5 Wireless Network Usage

- Wireless access points (WAPs) are installed on floors that provide patient services to enhance customer convenience.
- Each WAP is in the same subnet as the workstations and switches on its respective floor.
- Using WAPs reduces the need for high-port-count switches and extensive cabling, helping lower infrastructure costs.

1.6 VPN Configuration Proposal

1.6.1 Site-to-Site VPN

- Site-to-site IPSec VPN tunnels enable secure data, voice, and video transmission between remote locations (e.g., departments or branches) over the public Internet, using strong encryption for confidentiality.
- Configuration involves two main phases:

- ISAKMP (IKE) – Phase 1: Establishes the secure tunnel parameters.
- IPSec – Phase 2: Implements Access Control Lists (ACLs), Crypto Maps, and other settings to secure data within the tunnel.

1.7 Surveillance Camera System Proposal

The surveillance system design depends on the building's architecture. Below are general requirements applicable to various camera deployments:

- Star Topology: Cameras on each floor are connected to a central Ethernet switch.
- Power over Ethernet (PoE): Use PoE switches to deliver power and data through a single cable, simplifying installation.
- Bandwidth Requirements: Assess based on resolution and frame rate. Ensure infrastructure supports peak video data transmission.
- Network Switches: Use managed Gigabit switches with sufficient ports. PoE support is mandatory.
- Firewalls and Security: Protect camera network from unauthorized access using appropriate security appliances.
- Remote Monitoring: Implement secure VPN access for remote viewing by authorized personnel.
- Network Segmentation: Isolate the surveillance network from the main hospital network to improve security and performance.

2 List of Minimum Equipment, IP Plan, and Wiring Diagram (Cabling)

2.1 List of Recommended Equipment and Typical Specifications

2.1.1 Router: Cisco ISR4331-SEC/K9

Hình 2: Cisco ISR4331-SEC/K9

Attribute	Specification
Product Code	Cisco ISR4331-SEC/K9
Bundle	Security Bundle
Aggregate Throughput	100 Mbps to 300 Mbps
Total Onboard WAN/LAN 10/100/1000 Ports	3
RJ-45-Based Ports	2
SFP-Based Ports	2
Enhanced Service-Module (SM-X) Slot	1
Network Interface Module (NIM) Slots	2
Onboard ISC Slot	1
Memory	4 GB (default) / 16 GB (maximum)
Flash Memory	4 GB (default) / 16 GB (maximum)
Power Supply Options	Internal: AC and PoE
Rack Height	1 RU
Dimensions (H $\times$ W $\times$ D)	44.45 $\times$ 438.15 $\times$ 438.15 mm
Package Weight	12.96 kg

Bảng 2: Technical specifications of Cisco ISR4331-SEC/K9

2.1.2 Layer 2 Switch: Cisco WS-C2960+24TT-L

Hình 3: Cisco WS-C2960+24TT-L

Attribute	Specification
Product Code	WS-C2960-24TT-L
Enclosure Type	Rack-mountable - 1U
Feature Set	LAN Base
Uplink Interfaces	2 $\times$ 10/100/1000 TX
Ports	24 $\times$ Ethernet 10/100
Throughput	6.5 Mpps
Backplane Capacity	16 Gbps
DRAM	16 MB
Dimensions	1.73 $\times$ 17.5 $\times$ 9.3 in
Package Weight	8.15 kg

Bảng 3: Technical specifications of Cisco WS-C2960+24TT-L

2.1.3 Layer 3 Switch: Cisco WS-C3650-24PS-S

Hình 4: Cisco WS-C3650-24PS-S

Attribute	**Specification**
Product Code	WS-C3650-24PS-S
Enclosure Type	Rack-mountable - 1U
Feature Set	IP Base
Uplink Interfaces	$4 \times$ 1G SFP
Ports	$24 \times$ 10/100/1000 (PoE+)
Available PoE Power	390 W
Maximum Stacking Number	9
Stack Bandwidth	88 Gbps
Forwarding Performance	41.66 Mpps
Switching Capacity	88 Gbps
RAM	4 GB
Flash Memory	2 GB
Dimensions	$44.5 \times 44.5 \times 4.4$ cm
Package Weight	17.49 kg

Bảng 4: Technical specifications of Cisco WS-C3650-24PS-S

2.1.4 Access Point: Cisco CW9162I-MR (Wi-Fi 6E, 802.11ax)

Hình 5: Cisco CW9162I-MR 802.11ax Wi-Fi 6E Access Point

Attribute	**Specification**
Part Number	CW9162I-MR
Software Standard	802.11ax
MU-MIMO 5 GHz down)	2×2 (6 GHz up/down, 2.4
Key Features	OFDMA, TWT, BSS Coloring, MRC, Beamforming
Channel Widths	20/40/80/160 MHz (6 GHz), 20/40/80 MHz (5 GHz), 20 MHz (2.4 GHz)
PHY Data Rate	Up to 3.9 Gbps
Packet Aggregation	A-MPDU, A-MSDU
Security Support	DFS, CSD, WPA3
Integrated Antennas	2.4 GHz: 4 dBi, 5 GHz: 5 dBi, 6 GHz: 5 dBi (Omnidirectional)
Interfaces	1× 100M/1G/2.5G Ethernet, RJ-45; Console, USB 2.0
LED Indicators	Status: boot, association, errors, operation
Dimensions	200 × 200 × 44.45 mm (7.8 × 7.8 × 1.7 in)
Weight	0.93 kg (2.05 lb)
System Memory	2048 MB DRAM, 1024 MB Flash

Bảng 5: Technical specifications of Cisco CW9162I-MR

2.1.5 Camera: Hikvision DS-2GN5750-HH

Hình 6: Hikvision DS-2GN5750-HH

Feature	Description
Resolution	4 MP high-quality imaging
Low-Light Performance	Superior low-light visibility
Compression Technology	H.265+ compression
Durability	IP67 water and dust resistance
24/7 Imaging	Full-color imaging around the clock
Smart Detection	Human and vehicle detection support

Bảng 6: Technical specifications of DS-2GN5750-HH

2.2 Schematic Physical Setup of the Network

2.2.1 Main Site VLAN Configuration

VLAN	Name	Network Address	IP Range
VLAN110	FreeWifi_Guest	10.110.110.0/24	10.110.110.1–10.110.110.255
VLAN10	Floor_1	10.10.10.0/24	10.10.10.1–10.10.10.255
VLAN20	Floor_2	10.20.20.0/24	10.20.20.1–10.20.20.255
VLAN30	Floor_3	10.30.30.0/24	10.30.30.1–10.30.30.255
VLAN40	Floor_4	10.40.40.0/24	10.40.40.1–10.40.40.255
VLAN50	Floor_5	10.50.50.0/24	10.50.50.1–10.50.50.255
VLAN60	Floor_6	10.60.60.0/24	10.60.60.1–10.60.60.255
VLAN70	Floor_7	10.70.70.0/24	10.70.70.1–10.70.70.255
VLAN80	Floor_8	10.80.80.0/24	10.80.80.1–10.80.80.255
VLAN90	Floor_9	10.90.90.0/24	10.90.90.1–10.90.90.255
VLAN100	Floor_10	10.100.100.0/24	10.100.100.1–10.100.100.255

Bảng 7: VLAN Configuration of the Main Site

2.2.2 Auxiliary Sites VLAN Configuration

BHTQ Site

VLAN	Name	Network Address	IP Range
VLAN10	Floor_1	10.10.10.0/24	10.10.10.1–10.10.10.255
VLAN20	Floor_2	10.20.20.0/24	10.20.20.1–10.20.20.255
VLAN30	Guest	10.30.30.0/24	10.30.30.1–10.30.30.255

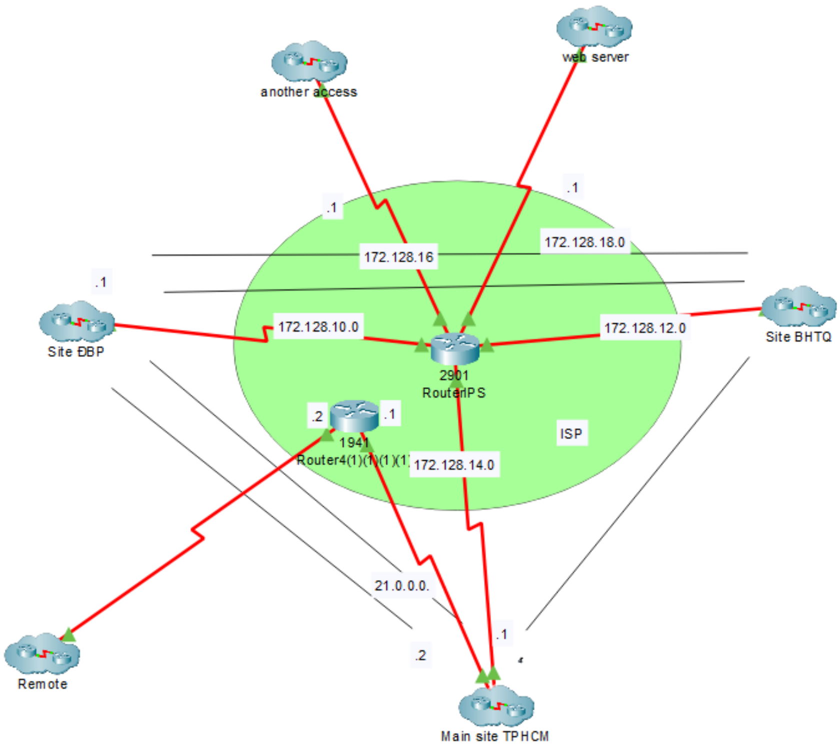
Bảng 8: VLAN Configuration of the BHTQ Site

ĐBP Site

VLAN	Name	Network Address	IP Range
VLAN10	Floor_1	10.10.10.0/24	10.10.10.1–10.10.10.255
VLAN20	Floor_2	10.20.20.0/24	10.20.20.1–10.20.20.255
VLAN30	Guest	10.30.30.0/24	10.30.30.1–10.30.30.255

Bảng 9: VLAN Configuration of the ĐBP Site

2.3 Wiring Diagram (Cabling)



Hình 7: Network Wiring Diagram

3 Calculate the necessary throughput and bandwidth for the system

As given in the requirements:

- Each server's download estimate is 1000 MB/day and the upload estimate is 2000 MB/day. Therefore, the total for each server is 3000 MB/day.
- Each workstation's download estimate is 500 MB/day and the upload estimate is 100 MB/day. Therefore, the total for each workstation is 600 MB/day.
- WiFi-connected devices from customer access make up about 500 MB/day of upload and download combined.

Given that 80% of the load occurs during peak hours (from 9 am to 11 am and 3 pm to 4 pm), we can calculate the throughput and bandwidth requirements for the main site and branch.

3.1 Main Site

The Main Site hosts 600 workstations and 10 servers. We can estimate the daily throughput of the Main Site's network as follows:

$$\text{Throughput}_{\text{Main Site}} = (600\times600)+(10\times3000)+500 = 360{,}000+30{,}000+500 = 390{,}500\,\text{MB/day}$$

The bandwidth required during peak hours (which accounts for 80% of the total daily load) is:

$$\text{Bandwidth}_{\text{Main Site}} = \frac{390{,}500 \times 0.8 \times 8}{10{,}800} \approx 231.3\,\text{Mbps}$$

Considering a 20% growth in the future, the required peak bandwidth would be:

$$231.3 \times 1.2 = 277.6\,\text{Mbps}$$

Therefore, 1 Gbps (1000 Mbps) interfaces on the routers will be sufficient for the Main Site to handle peak traffic and future growth.

3.2 Auxiliary Site

The Auxiliary Site hosts 60 workstations and 2 servers. We can estimate the daily throughput of the Auxiliary Site's network as follows:

$$\text{Throughput}_{\text{Auxiliary Site}} = (60\times600)+(2\times3000)+500 = 36{,}000+6{,}000+500 = 42{,}500\,\text{MB/day}$$

The bandwidth required during peak hours is:

$$\text{Bandwidth}_{\text{Auxiliary Site}} = \frac{42{,}500 \times 0.8 \times 8}{10{,}800} \approx 25.2\,\text{Mbps}$$

With a 20% future growth, the peak bandwidth required would be:

$$25.2 \times 1.2 = 30.2\,\text{Mbps}$$

Therefore, 100 Mbps interfaces on the routers should be sufficient for the Auxiliary Site.

3.3 Summary of Bandwidth Requirements

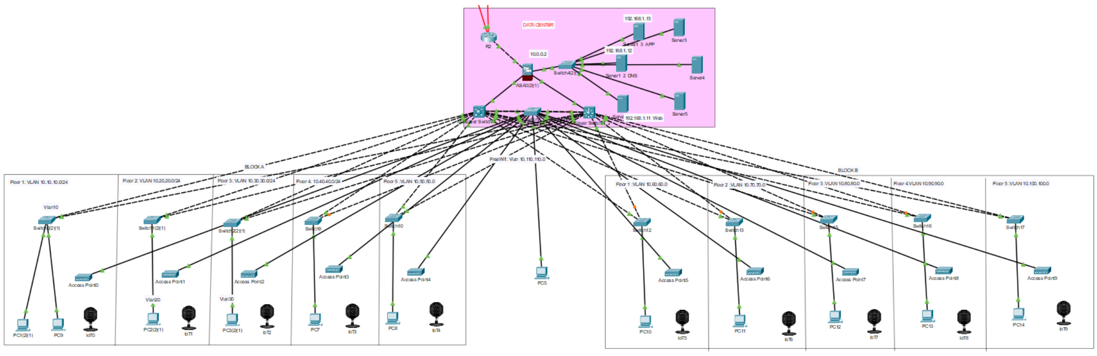
1. Main Site:
    - Peak bandwidth: 231.3 Mbps
    - With 20% growth: 277.6 Mbps
    - Router interface: 1 Gbps (1000 Mbps)
2. Auxiliary Site:
    - Peak bandwidth: 25.2 Mbps
    - With 20% growth: 30.2 Mbps
    - Router interface: 100 Mbps

Conclusion

The Main Site requires high-capacity 1 Gbps interfaces to handle peak bandwidth and future growth, while the Auxiliary Site requires 100 Mbps interfaces. This ensures the hospital's network can handle the expected load and scale over time.

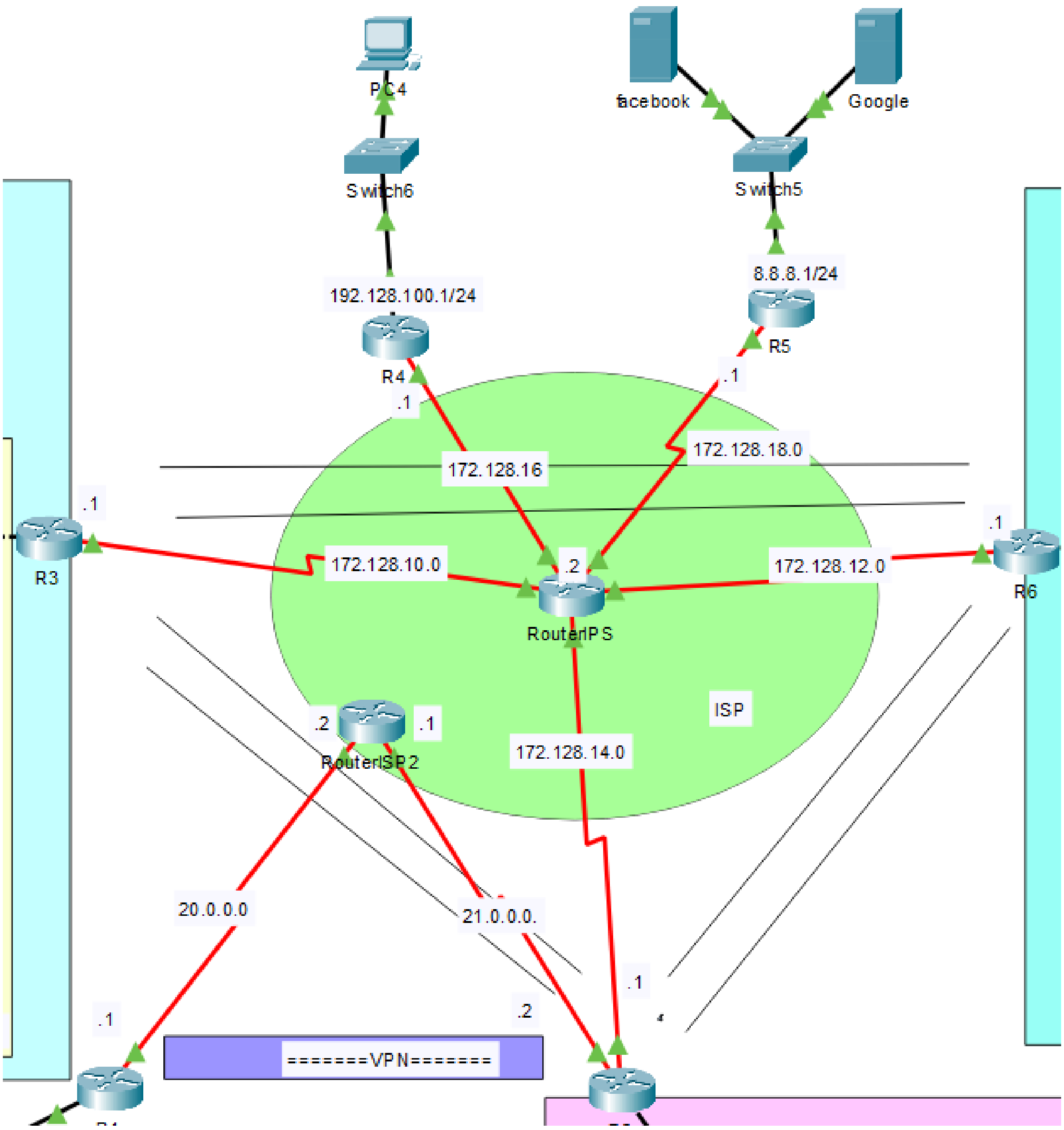
4 Design the network map using Packet Tracer

4.1 Main Site



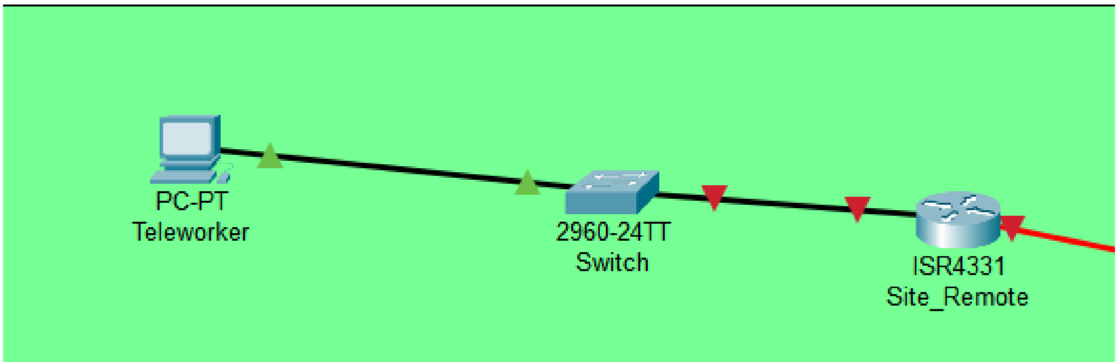
Hình 8: Main Site

4.2 Internet



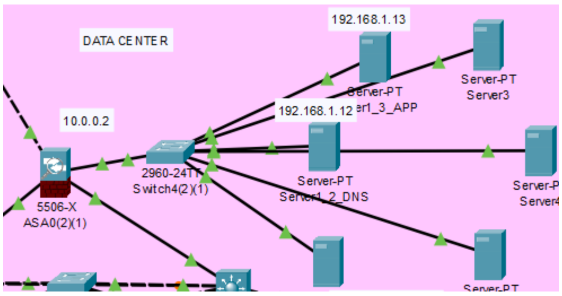
Hình 9: Internet

4.3 Teleworker

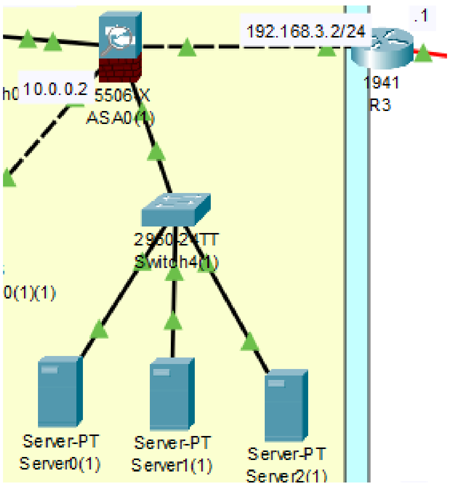


Hình 10: Teleworker

4.4 DMZ

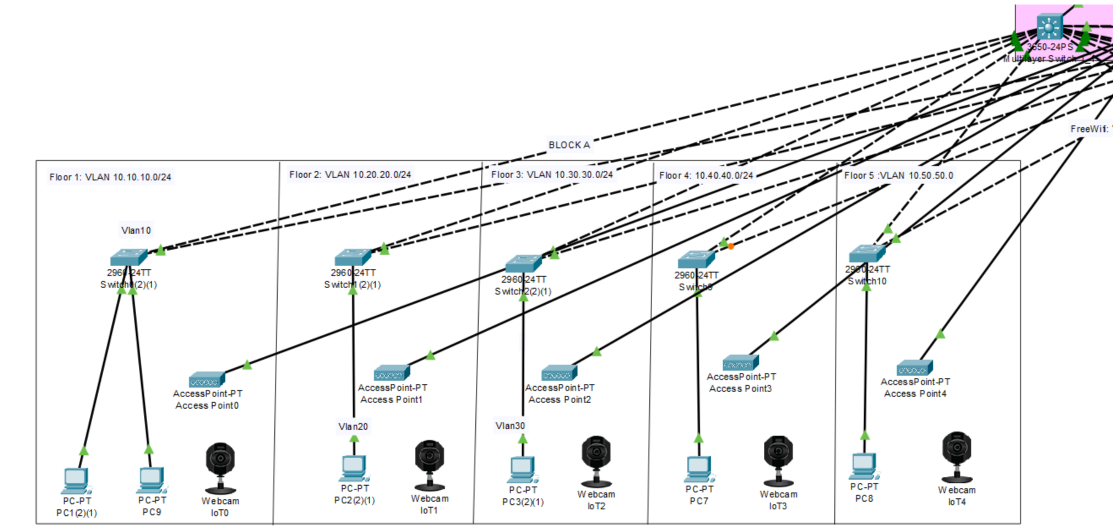


Hình 11: DMZ ở cơ sở chính



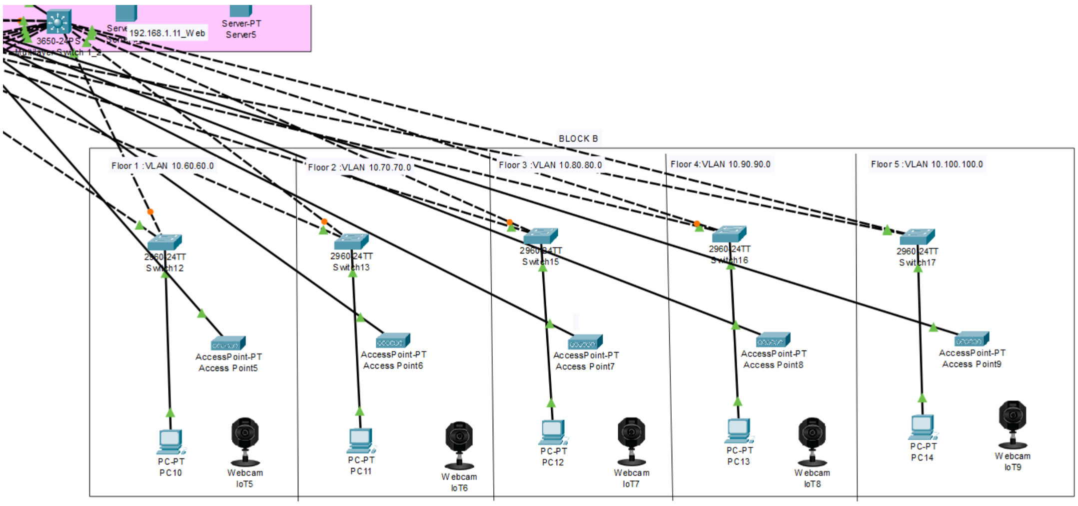
Hình 12: DMZ ở cơ sở phụ

4.5 Building A



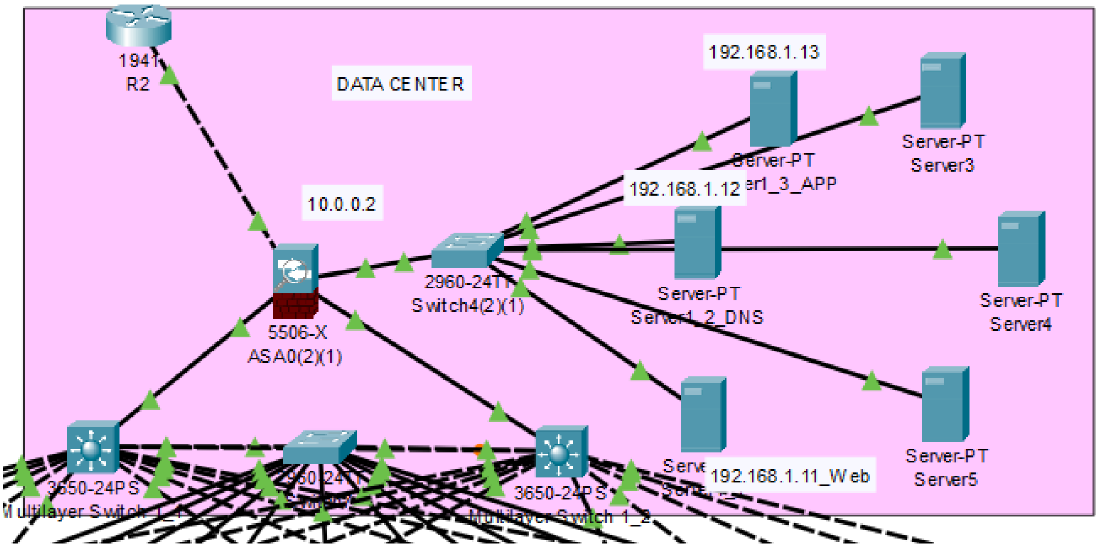
Hình 13: Building A

4.6 Building B



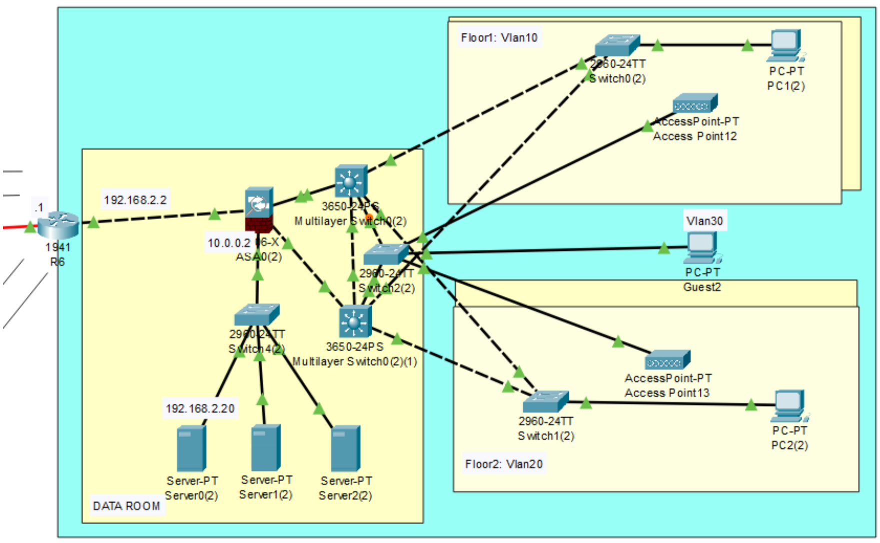
Hình 14: Building B

4.7 IT room and Data Center of Main Site



Hình 15: IT room and Data Center of Main Site

4.8 DBP Auxiliary



Hình 16: DBP_BHTQ Auxiliary

5 Re-evaluate the designed network system

5.1 The remaining problems for the project

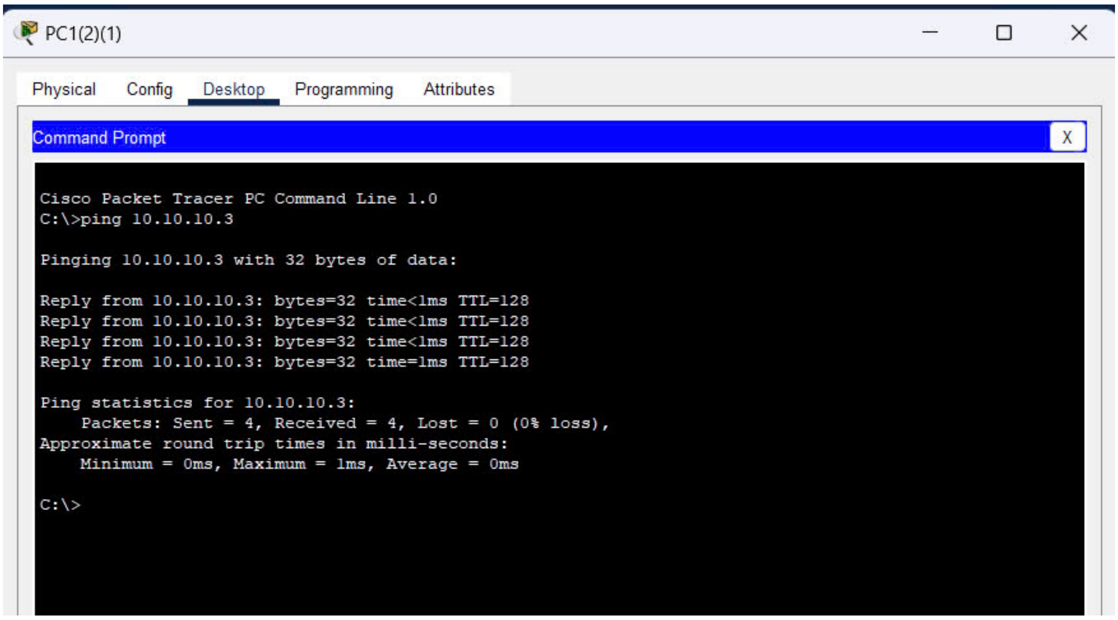
- We do not have specific knowledge about a particular hospital network, so when designing, we encounter difficulties in deciding which models, technologies, and devices should be used.
- Insufficient background knowledge about networking standards makes the system messy and difficult to debug.
- The system still has many centralized connection points (core switches, core routers), causing system-wide disruptions when these devices fail.
- The cost of Cisco network devices is high, though reductions are possible in some areas.

5.2 Development orientation in the future

- The network architecture should be redesigned to provide a more structured and organized topology that allows better traffic management and control.
- Find alternatives to Cisco devices to save money.
- 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.

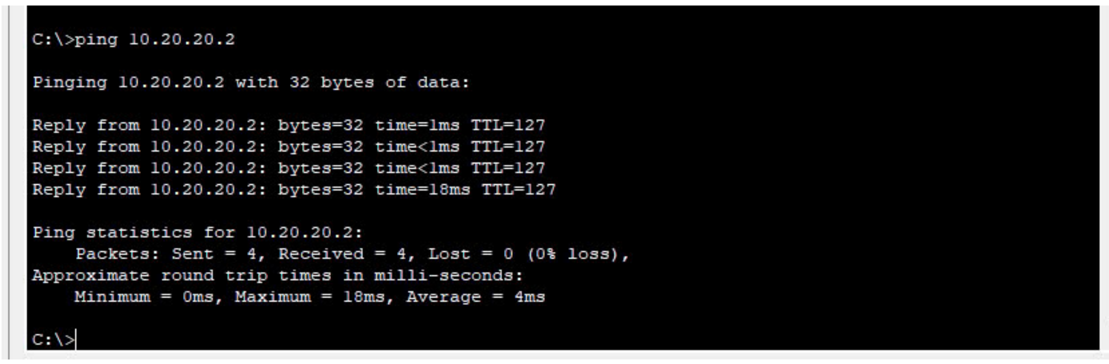
6 Test on simulated system

6.1 Connect between PCs in the same VLAN



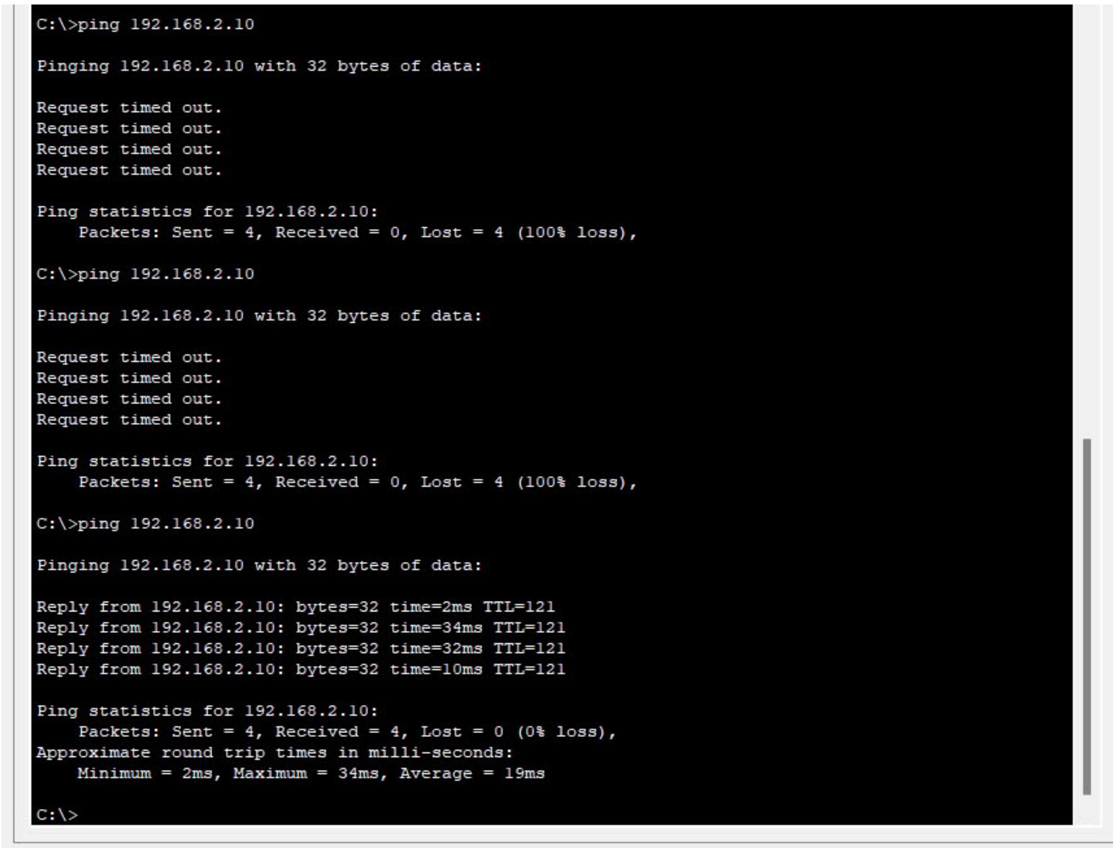
Hình 17: Connect between PCs in the same VLAN

6.2 Connect PCs between VLAN



Hình 18: Connect PCs between VLAN

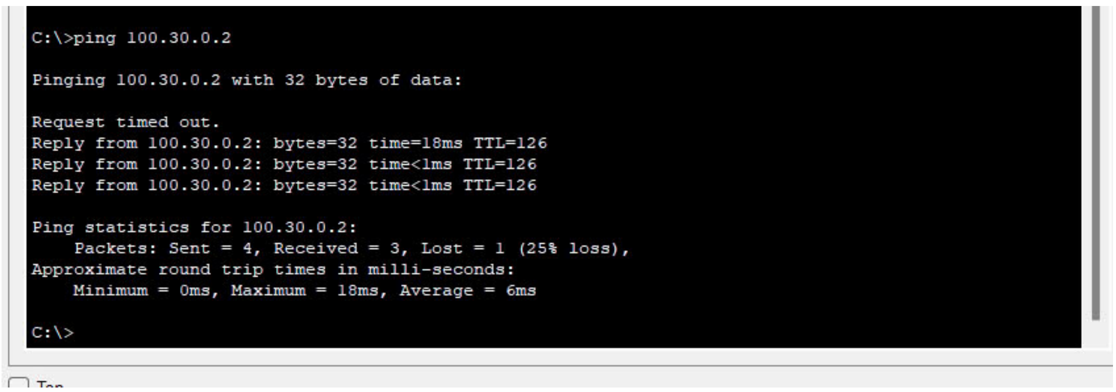
6.3 Connect PCs between the main Site and the two Auxiliary Sites



```
C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

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

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

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

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Reply from 192.168.2.10: bytes=32 time=2ms TTL=121
Reply from 192.168.2.10: bytes=32 time=34ms TTL=121
Reply from 192.168.2.10: bytes=32 time=32ms TTL=121
Reply from 192.168.2.10: bytes=32 time=10ms TTL=121

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 34ms, Average = 19ms

C:\>
```

Hình 19: Connect PCs between the main Site and the two Auxiliary Sites

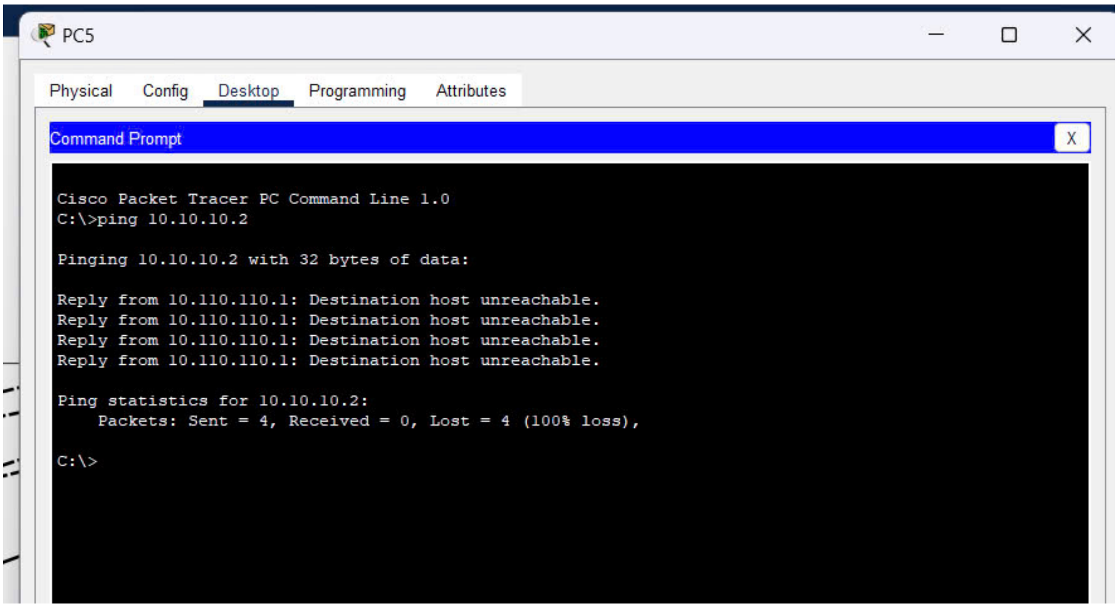
6.4 Connect to server in the DMZ



```
C:\>ping 100.30.0.2

Pinging 100.30.0.2 with 32 bytes of data:

Request timed out.
Reply from 100.30.0.2: bytes=32 time=18ms TTL=126
Reply from 100.30.0.2: bytes=32 time<1ms TTL=126
Reply from 100.30.0.2: bytes=32 time<1ms TTL=126

Ping statistics for 100.30.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 18ms, Average = 6ms

C:\>
```

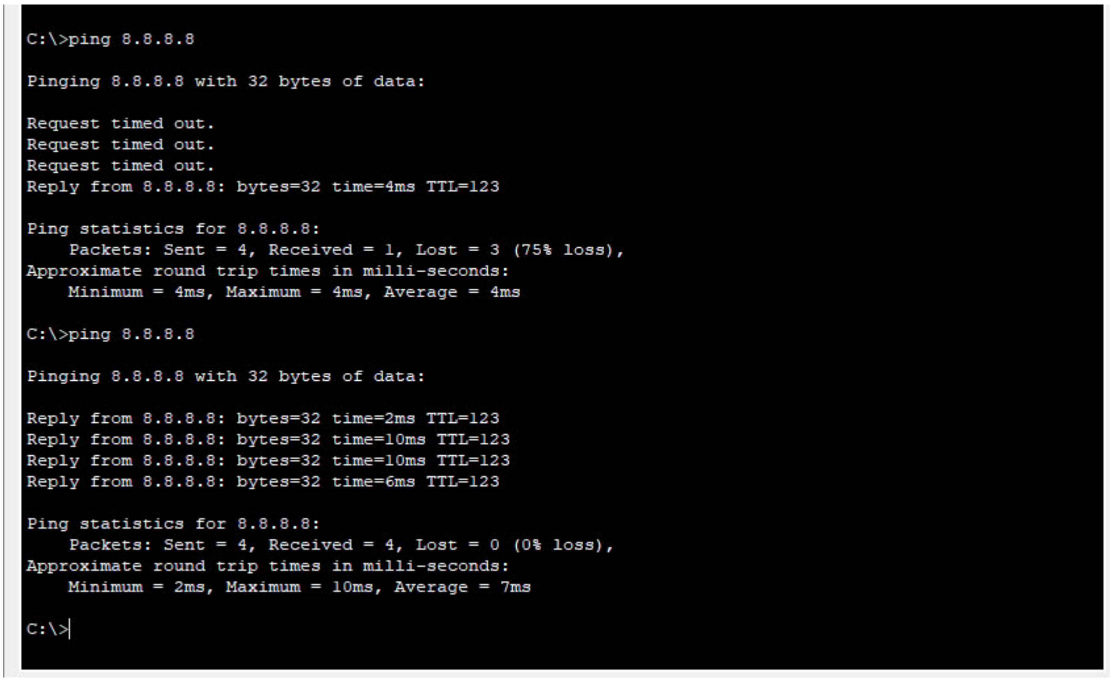
Hình 20: Connect to server in the DMZ

6.5 No connections from customer's device to PCs on the Lan



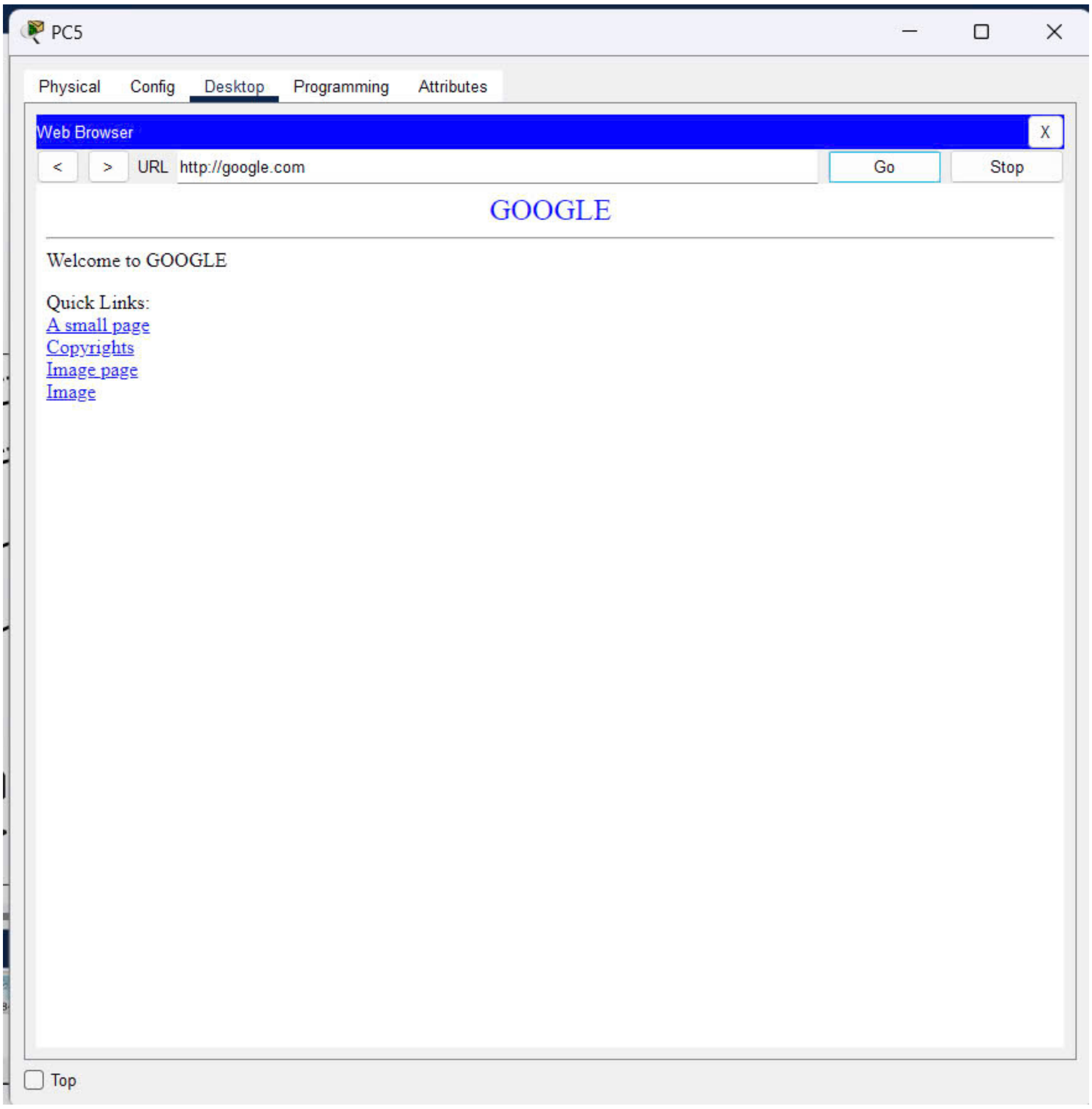
Hình 21: No connections from customer's device to PCs on the Lan

6.6 connect to the Internet to a Web server



Hình 22: connect to the Internet to a Web server

6.7 connect to the Internet to google



Hình 23: connect to Google

7 Evaluation

7.1 Achievements

- High reliability: The use of static routing configuration, which is suitable for an environment with minimal changes, ensures stable transmission and overcomes the limitations of hop count in routing.
- Easy scalability: The chosen devices are based on real calculations and projected growth of the hospital, making system expansion in the future convenient without significant disruptions.
- Support for diverse software: The installed hardware is compatible with various software types, enabling the deployment of applications that serve business operations.
- System safety assurance: The system integrates load balancing features, distributing data across transmission links and ensuring continuous connectivity even when one link fails.
- High security: The system is equipped with firewalls at both the main site and branch offices, creating a multi-layered security architecture that minimizes unauthorized access to the internal network.

7.2 Limitations

- Incomplete Internet transmission: The system is still heavily reliant on the central configuration and lacks full redundancy solutions.
- Potential congestion at the main site: All transmission paths go through the router at the main site, which could become a bottleneck if traffic increases, impacting overall system performance.

7.3 Scalability

- Bandwidth: Flexible upgrades can be made through Internet service packages from the provider without the need for physical structure changes.
- Security: The model can integrate additional local firewalls at branch and main sites, while enhancing security for individual network devices to prevent unauthorized external access.
- User access control: Additional solutions to segregate LAN access—especially controlling Wi-Fi user connections—can be deployed via firewalls or Layer 3 Switches, helping protect the internal system more effectively.

8 Conclusion

Through the survey, analysis, and network design for the specialized hospital in Ho Chi Minh City and its two branches (DBP and BHTQ), the team has developed a modern overall network model that effectively meets the performance, scalability, and security requirements.

The system uses a 3-tier hierarchical architecture (Access – Distribution – Core), combining high-speed wired LAN and Wi-Fi 6 wireless networks, with VLANs segmented according to medical functions. Advanced technologies such as SD-WAN, next-generation firewalls, IP surveillance cameras, remote VPN, Load Balancing, and PoE power systems have been integrated to ensure the system operates stably, securely, and is easy to manage.

Overall, the design approach meets the project's requirements, is highly practical, and can be applied to modern hospitals today. In addition, the team has identified a few limitations and proposed directions for future system development, aiming toward an intelligent, secure, and flexible healthcare technology infrastructure.