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

Computer Network (CO3093)

Assignment

NETWORK DESIGN AND SIMULATION FOR A CRITICAL LARGE HOSPITAL

Lecturer:	Nguyễn Lê Duy Lai
Students:	Đặng Hoàng Gia - 2153312
	Nguyễn Đức Bảo Huy - 2152089

HO CHI MINH CITY, December 2023

Contents

1 Member list & Workload

No.	Fullname	Student ID	Tasks	Percentage of work
1	Đặng Hoàng Gia	2153312	Logical Design, Routing, Report	100%
2	Nguyễn Đức Bảo Huy	2152089	Logical Design, VLAN DHCP, Report	100%

2 Introduction

This assignment involves creating a network structure for a sizable corporation where various departments operate across different buildings. The goal is to establish connectivity among these departments, enabling seamless data exchange and communication. The network design will be implemented and simulated using software like Cisco Packet Tracer, which allows for the creation and analysis of different network setups, including topology configurations and router path optimization

3 Case study and Requirements Analysis

3.1 Case study

The CCC (Computer and Construction Consultant) Agency has been tasked with designing a computer network for a Specialized Hospital under construction. The network will be deployed at the Main Site in Ho Chi Minh City and two Auxiliary Sites on DBP Street and BHTQ Street. The hospital has specific IT needs, including:

Main site (HCMC):

- 2 buildings A and B (5 floors with 10 rooms/floor) equipped with computers and medical devices.
- The data center, IT, and Cabling Central Local (using patch panels gathering wires) are located in a separate room, 50 meters from buildings A and B.
- Medium-scale: 600 workstations, 10 servers, 12 networking devices (or maybe more with security-specific devices).
- The wireless connection has to be covered for the whole Site.
- Using new technologies for network infrastructure including wired and wireless connections, fiber cabling (GPON), and GigaEthernet 1GbE/10GbE/40GbE. The network is organized according to the VLAN structure for different departments
- The main Site subnetwork connects two other Sites (Site DBP and Site BHTQ) subnetworks by 2 leased lines for WAN connection (possibly applying SD-WAN, MPLS).
- 2 xDSL for Internet access with a load-balancing mechanism. All traffic to the Internet passes through the main site subnet.
- For software acquisition, the Hospital uses a mix of licensed and open-source software, hospital software (HIS, RIS - PACS, LIS, CRM, etc.), office applications, client-server applications, multimedia, and databases.
- Requirements for capability of extension, high security (e.g., firewall, IPS/IDS, phishing detection), high availability (HA), robustness when problems occur, ease of upgrading the system
- Propose a VPN configuration for site-to-site and for a teleworker to connect to Company LAN
- Propose a surveillance camera system for the Company

Other Sites:

- The building has 2 floors, the first floor is equipped with 1 IT room and 1 Cabling Central Local.
- Small-scale: 60 workstations, 2 servers, 5 or more networking devices

3.2 Functional Requirements

- Design three local network systems: Main site, two Auxiliary sites.
- Implement connections between the Main site and two other sites using 2 Leased lines to ensure stable and high-speed data transmission.
- Customers and employees must have separate network connections. Customers will use a wireless network and cannot access the internal network.
- At the three sites, utilize modern technologies such as optical fiber, GigaEthernet 1GbE/10GbE transmission lines, and wireless connections.
- Main site: 600 computers, 10 servers, and 12 network devices.
- Two auxiliary sites: 60 workstations, 2 servers, 5 networking devices.

3.3 Non-functional Requirements

1. Reliability and Availability:
    - The network must be highly reliable to ensure continuous access to medical records, communication systems and critical applications.
    - High availability is essential to support healthcare operations 24/7.
2. Security:
    - The network should incorporate robust security measures to protect sensitive patient data.
    - Security features may include firewalls, intrusion prevention systems, intrusion detection systems, phishing detection mechanisms.
    - Customers and hospital staffs should have separate connections. For convenience, customers may use the wireless network system and should not be able to access the hospital's internal network.
    - In the Main site and two Auxiliary sites, Each floor (or each two floors) may belong to a different VLAN to increase security and flexibility.
    - Implementing a DMZ zone for servers and firewalls might ensure the safety of the system before receiving connections from outside.
3. Scalability:
    - The network must be scalable to accommodate the growth of the hospital over time, including an estimated 20% increase in users, network load, and site extensions over five years.

- Scalability ensures that the network can expand seamlessly without compromising performance or reliability.

4. Performance:
    - The network should deliver high performance to support real-time applications such as telemedicine, medical imaging, and video conferencing.
    - Low latency and high bandwidth are necessary for smooth operation, particularly during peak hours when workload is high.

4 System Design

4.1 Equipment and specification

4.1.1 Router Cisco 1941/K9

The Cisco 1941 Integrated Services Router is a versatile networking device de-signed for small to medium-sized businesses. Offering a throughput of up to 2 Mbps, it supports various WAN interfaces, including T1/E1, xDSL, and Gigabit Ethernet, providing flexible con- nectivity options. With integrated security features, modular design for scalability, and support for advanced routing and switching protocols, the Cisco 1941 ensures robust performance and adaptability.

- Number of units used: 5
- Technical specifications:
    - Forwarding rate: 180 Mbps
    - Number of WAN interfaces: 2
    - Number of LAN interfaces: 2
- Memory:
    - RAM: 512MB
    - Flash: 256MB
- Routing protocols: OSPF, IS-IS, BGP, EIGRP, static IPv4, static IPv6.
- Connections and interfaces used:
    - 2 Gigabit Ethernet ports
    - 4 Serial expansion ports
- Price: 19,000,000VND

4.1.2 Switch Layer 2: CISCO WS-C2960+24TT-L

The Cisco Catalyst WS-C2960+24TT-L is a Layer 2 managed switch designed for efficient and secure network connectivity. With 24 Ethernet 10/100 ports, it provides reliable and high-performance connectivity for various devices within a network. The switch supports advanced features such as VLANs like our project to optimize network traffic and enhance overall performance. Additionally, the switch can be easily integrated into a larger network infrastructure, making it a versatile choice for building scalable and reliable networks.

- Number of units used: 15
- Manufacturer: Cisco Systems, Inc.
- Manufacturer Part Number: Cisco WS-C2960-24TT-L.
- Product Type: Switch - 24 ports - Managed.
- Enclosure Type: Rack-mountable 1U.
- Uplink interface: 2 (SFP or 1000BASE-T).
- Ports: 24 x 10/100Mbps Ethernet.
- Bandwidth forwarding: 16 Gbps.
- DRAM: 128 MB.
- Flash Memory: 64 MB.
- Protocols: SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SSH.
- Compliant Standards: IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah, IEEE 802.1ab (LLDP).
- High Availability / High Responsiveness: PVST, Block Broadcast, Interrupt Unicast, Block Mulitcast, Spanning Tree, Portfast, Fast Uplink, Fast Backbone, 802.1s, 802.1w.
- Management features: SPAN, CiscoView, Cisco Discovery Protocol (CDP), Virtual Trunking Protocol (VTP), Telnet customers, BOOTP, TFTP, CiscoWorks, CWSI, RMON, SNMP, Clustering, Web Management.
- Throughput: 6.5 Mbps.
- Power: AC 120/230 V (50/60 Hz).
- Dimensions (WxDxH) 44.5 cm x 23.6 cm x 4.4 cm
- Weight 3.63 kg
- Price: 14,213,000 VNĐ

4.1.3 Switch Layer 3: Switch Cisco Catalyst WS-C3650-24PS-S

The Cisco Catalyst WS-C3650-24PS-S is a Layer 3 managed switch designed to deliver high-performance, feature-rich networking for organizations of varying sizes. With 24 Gigabit Ethernet ports, PoE+ support, and modular uplink options, this switch provides advanced connectivity for a range of devices. As a Layer 3 switch, it offers IP routing capabilities, enabling efficient inter-VLAN routing and enhancing network segmentation. The WS-C3650- 24PS-S also features Power over Ethernet (PoE) support, providing power to connected devices such as IP phones and cameras, and includes advanced security features to safeguard the network.

- Number of unit used: 2
- Manufacturer: Cisco Systems, Inc.
- Manufacturer Part Number: Cisco WS-C3560V-24PS-S.

- Enclosure Type: Rack-mountable 1U.
- Gate: 24 gates 10/100/1000 Ethernet.
- Bandwidth forwarding: 41,66Mpps.
- Power conversion: 88 Gb / s. RAM: 4 GB.
- Flash memory: 2 GB.
- Routing Protocol: RIP-1, RIP-2, Static IP.
- Features: Layer 3 switching, automatic recognition per device, DHCP support, auto-negotiation, load balancing, VLAN support, auto-linking (MDI/MDI-X), MAC address filtering, IPv6 Support Trunking Protocol (STP), DHCP snooping, DTP support, Port Aggregation Pro- tocol Support (PAgP), TFTP support, Access Control List (ACL), Quality of Service (QoS) support, Jumbo Frames support, Dynamic ARP Inspection (DAI), Time Domain Reflec- tometry (TDR).
- Compliant Standards: IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s.
- Power: AC 120/230 V (50/60 Hz).
- Dimensions (WxDxH): 44,3 x 29,5 x 4,4 cm.
- Weight: 4.6 kg.
- Price: 37,000,000 VNĐ

4.1.4 Access-point: Cisco-Linksys WRT300N Wireless-N Broadband Router

The Cisco-Linksys WRT300N Wireless-N Broadband Router is an access point designed to deliver reliable and high-speed wireless networking. Equipped with four Ethernet ports for wired connections and advanced security features such as WPA and WPA2 encryption, it ensures secure and seamless connectivity for a variety of devices. With an intuitive web-based interface for configuration and management, the WRT300N allows users to easily set up and customize their wireless network settings, making it a user-friendly solution for those seeking a reliable and feature-rich wireless access point.

- Quantity used: 12-14.
- Throughput: 540 Mbps.
- Data process with Layer 7 application fingerprinting and QoS Integrate with firewall.
- Air Marshal: Real-time WIPS (Wireless intrusion prevention system) with alarm.
- Each device is designed for high-density access to more than 100 users per device without bottlenecks, or processor crashes like conventional products. In addition, the device has traffic shapping technology to ensure that bandwidth is shared fairly between users.
- With Plug and Play technology, administrators only need to plug a new device into a power source, which will automatically tune in to devices of the same network and transmit waves to create an extended broadcast area without having to go through complicated configuration steps.

- Avoid common configuration errors of most wireless networks today. Devices without controllers when set to the same frequency band located close to each other will interfere with each other, which affect the performance and stability of the wireless network.
- Price 1.600.000 VND

4.1.5 Cisco Firewall ASA 5506-X

To enhance security for the hospital system, installing a Firewall is indispensable. In addition, the Firewall needs to support DMZ, VLAN, and mitigate network attacks. Therefore, the system will utilize the Cisco ASA 5506-X with the following prominent specifications:

- Quantity in use: 3
- Performance:
  - Firewall throughput: approximately 750 Mbps
  - Concurrent users: around 100 users
- Connection ports:
  - One Gigabit Ethernet port for management connection.
  - Seven Gigabit Ethernet ports for network connection.
- Security features:
  - Support for Stateful Firewall, Proxy Firewall, and Deep Packet Inspection. VPN support: IPsec VPN, SSL VPN, VPN client,...
  - Prevention of network attacks through IPS (Intrusion Prevention System). Support for features such as URL Filtering, Application Visibility and Control.
- Price: 23,000,000 VND.

4.2 IP plan

4.2.1 The Main site:

VLAN No	Name	Network address	IP Range	Description
VLAN4	Camera	192.168.4.0/24	192.168.4.2 - 192.168.4.254	VLAN used for surveillance cameras
VLAN5	AT1	192.168.5.0/24	192.168.5.2 - 192.168.5.254	VLAN used for floor 1 and 2
VLAN6	AT3	192.168.6.0/24	192.168.6.2 - 192.168.6.254	VLAN used for floor 3 and 4
VLAN7	AT5	192.168.7.0/24	192.168.7.2 - 192.168.7.254	VLAN used for floor 5

Table 1: IP Plan for Building A - Main site

VLAN	Name	Network address	IP Range	Description
VLAN8	BT1	192.168.8.0/24	192.168.8.2 - 192.168.8.254	VLAN used for floor 1 and 2
VLAN9	BT3	192.168.9.0/24	192.168.9.2 - 192.168.9.254	VLAN used for floor 3 and 4
VLAN10	BT5	192.168.10.0/24	192.168.10.2 - 192.168.10.254	VLAN used for floor 5
VLAN12	Camera	192.168.12.0/24	192.168.12.2 - 192.168.12.254	VLAN used for camera

Table 2: IP Plan for building B - Main site

Server and Security (DMZ) and Customer:

VLAN	Name	Network address	IP Range	Description
VLAN100	DMZ	192.168.100.0/28	192.168.10.2 - 192.168.10.14	VLAN used for servers
ASA-Router	ASA-Router	192.168.1.0/24	192.168.1.2 - 192.168.1.254	Firewall router
ASA-SW1	ASA-SW1	192.168.2.0/24	192.168.2.2 - 192.168.2.254	Firewall to Coreswitch Building A
ASA-SW2	ASA-SW2	192.168.3.0/24	192.168.3.2 - 192.168.3.254	Firewall to Coreswitch Building B
VLAN11	Security	192.168.11.0	192.168.11.2 - 192.168.11.254	VLAN for IT, Security room

Table 3: IP Plan for DMZ and Firewall

4.2.2 The Two Auxiliary sites:

Site DBP Street

VLAN	Network address	IP Range	Description
DMZ	192.168.15.0/29	192.168.15.4 - 192.168.15.5	IP for DMZ
DPB1	192.168.16.0/24	192.168.16.2 - 192.168.16.254	IP for DBP workstation

Table 4: IP Plan for DBP Site

Site BHTQ street

VLAN	Network address	IP Range	Description
DMZ	192.168.18.0/29	192.168.18.4 - 192.168.18.5	IP for DMZ
BHTQ1	192.168.19.0/24	192.168.19.2 - 192.168.19.254	IP for BHTQ workstation

Table 5: IP Plan for DBP Site

4.3 Connection Diagram

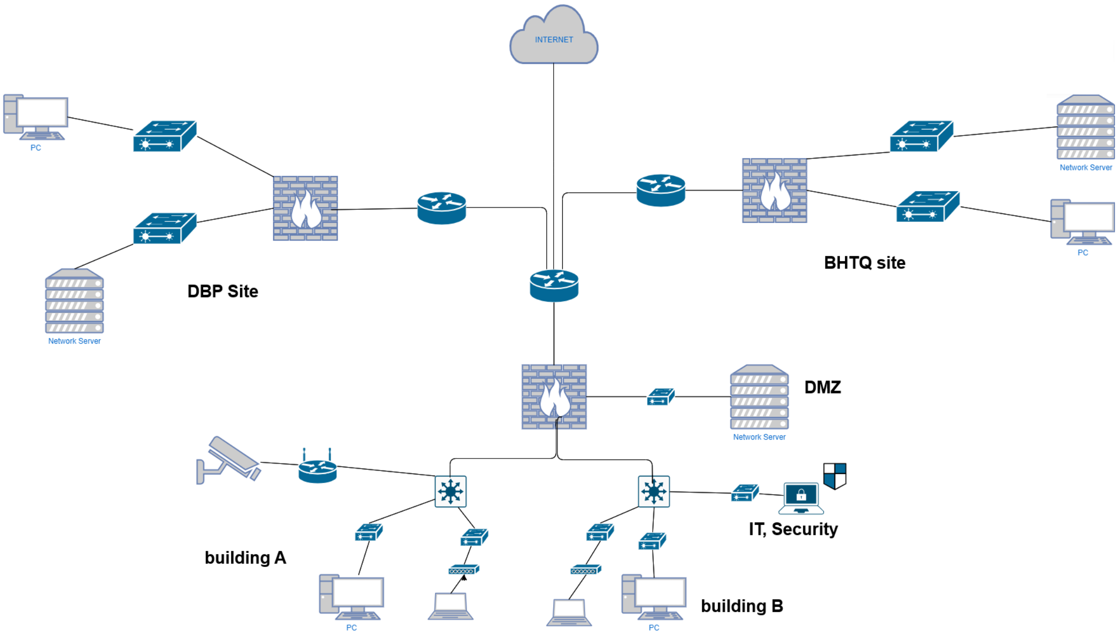


Figure 1: Wiring Diagram

5 Calculation Bandwidth and Throughput

5.1 Basic Concept

1. Bandwidth: Bandwidth refers to the maximum data transfer rate of a network connection, typically measured in bits per second (bps), kilobits per second (kbps), megabits per second (Mbps), or gigabits per second (Gbps). It represents the capacity of the network connection and indicates how much data can be transmitted over the network in a given amount of time.
2. Throughput: Throughput, on the other hand, refers to the actual amount of data that is successfully transmitted over a network connection in a given amount of time. It represents the effective data transfer rate and is usually measured in the same units as bandwidth (bps, kbps, Mbps, Gbps). Throughput can be affected by various factors such as network congestion, packet loss, latency, and network errors.

To calculate the required throughput and expected bandwidth for a hospital network, we consider factors such as the number of users/devices accessing the network, the types of applications and services being used (e.g., electronic medical records, imaging systems, video conferencing), the volume of data being transmitted, and the expected peak usage times.

As given in the requirements:

- Each server's download estimate is 1000 MB/day and the upload estimate is 2000 MB/day. Therefore total is 3000 MB/day.
- Each workstation's download estimate is 500 MB/day and the upload estimate is 100 MB/day. Therefore total is 600 MB/day.
- WiFi-connected devices from customers' access make up about 500 MB/day of upload and download.
- About 80 percent of the load is at the peak hours from 9am to 11am and from 3pm to
- Hospital Network is estimated to have a growth rate of 20% in 5 years (in terms of the number of users, network load, site extensions, etc.). 4pm.

5.2 Main site

There are 600 workstations and 10 servers. Hence we estimate the daily throughput of the Main site's network to be:

$$Throughput = 10 \times 3000 + 600 \times 600 + 500 = 390500\,\text{MB}$$

The bandwidth required at peak hours should then be:

$$Bandwidth = \frac{390500 \times 2^3 \times 0.8}{3 \times 3600} = 231.407\,\text{Mbps}$$

With the 20% growth in the future in mind, using 100Mbps interfaces on the routers should suffice as the peak bandwidth required will be $231.407 \times 1.2 = 277.69$Mbps

5.3 Two Auxiliary sites

There are 60 workstations and 2 servers. Hence we estimate the daily throughput of one Auxiliary site's network to be:

$$Throughput = 2 \times 3000 + 60 \times 600 + 500 = 42500\,\text{MB}$$

The bandwidth required at peak hours should then be:

$$Bandwidth = \frac{42500 \times 2^3 \times 0.8}{3 \times 3600} = 25.186\,\text{Mbps}$$

With the 20% growth in the future in mind, using 100Mbps interfaces on the routers should suffice as the peak bandwidth required will be $25.186 \times 1.2 = 30.223$Mbps

6 Network Design

6.1 Main site:

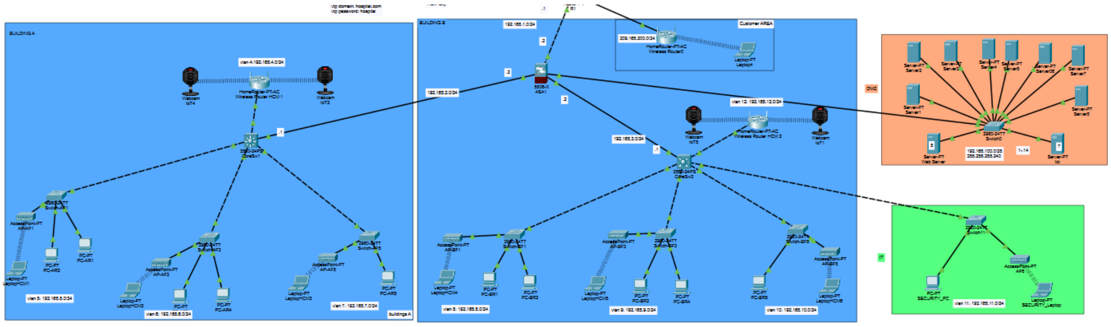


Figure 2: Main site Logical Design Network

6.2 Two Auxiliary sites:

6.2.1 DBP Street

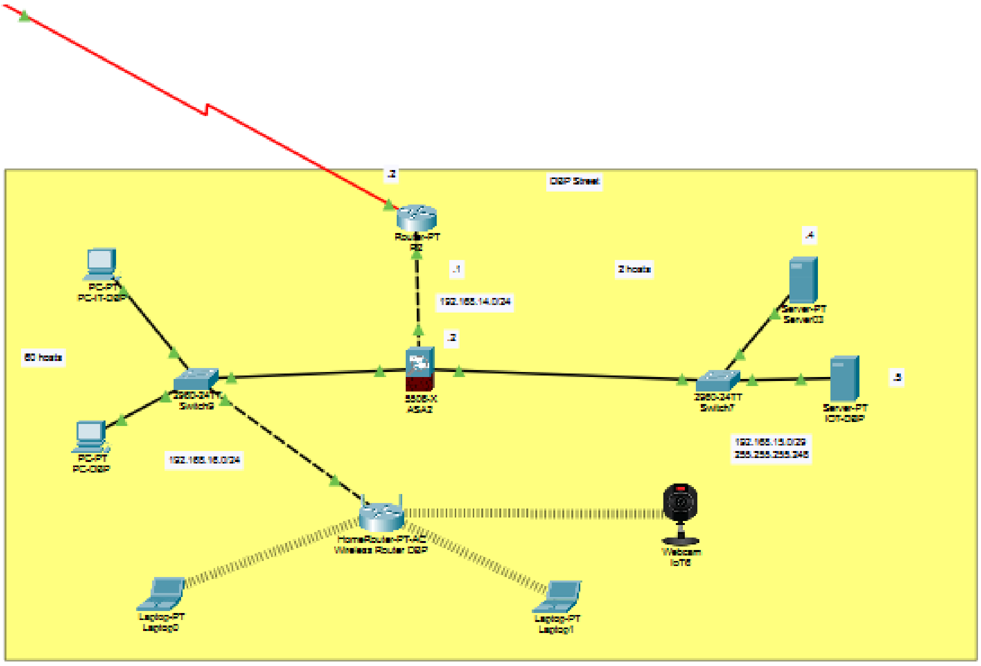


Figure 3: DBP ste Logical Design Network

6.2.2 BHTQ Street

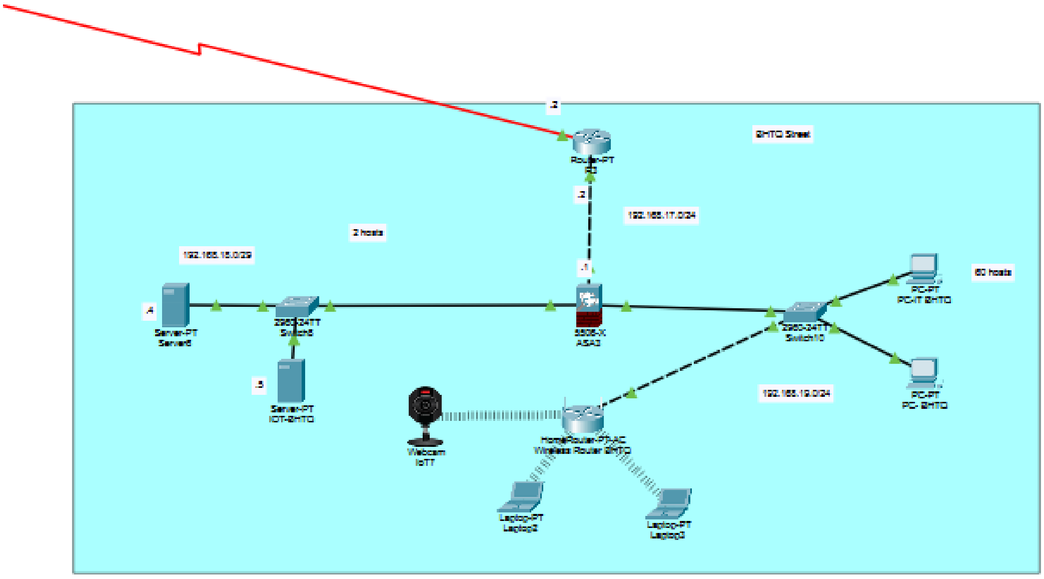
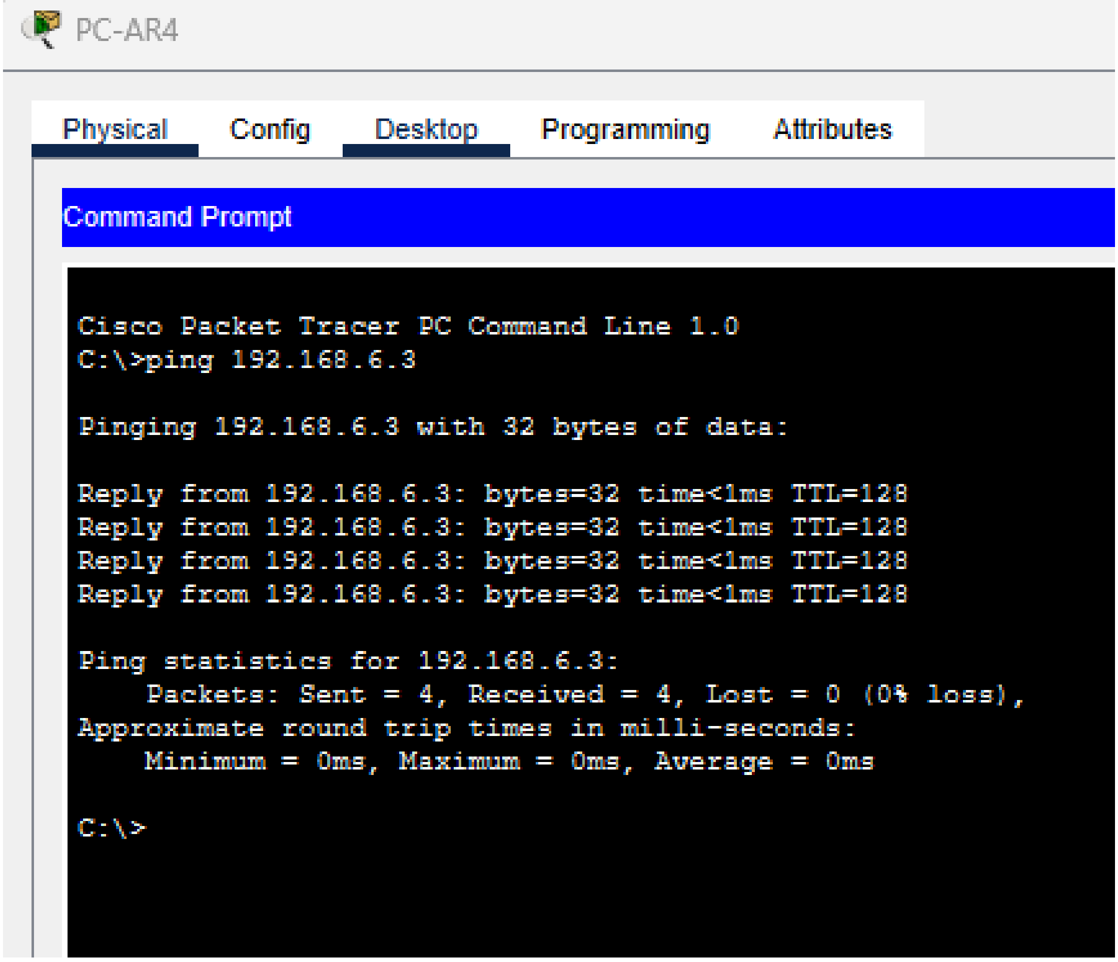


Figure 4: BHTQ site Logical Design Network

7 Testing

We have placed the link to the network design simulation below for further testing if desired.We have placed the link to the network design simulation below for further testing if desired: LINK

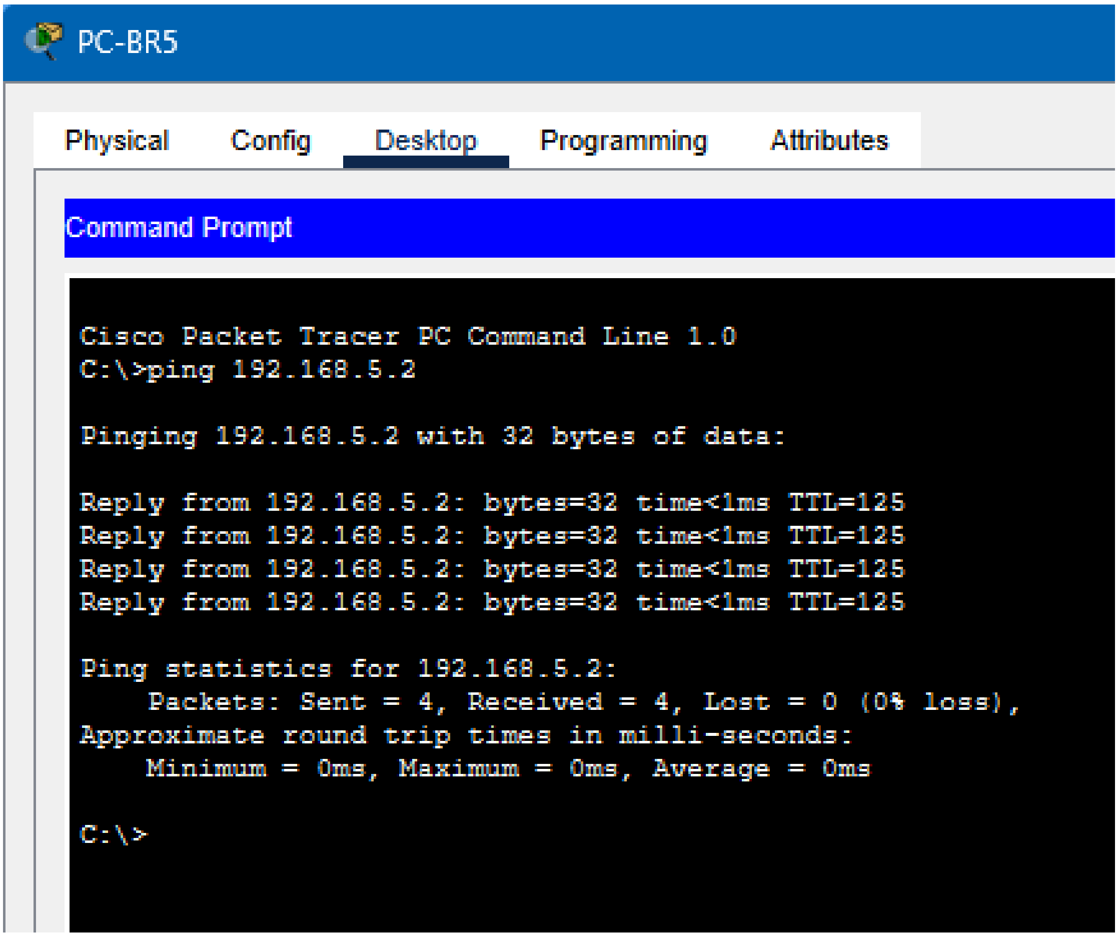
7.1 Connection between PCs in the same VLAN



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.6.3

Pinging 192.168.6.3 with 32 bytes of data:

Reply from 192.168.6.3: bytes=32 time<1ms TTL=128
Reply from 192.168.6.3: bytes=32 time<1ms TTL=128
Reply from 192.168.6.3: bytes=32 time<1ms TTL=128
Reply from 192.168.6.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.6.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figure 5: Test ping from AR4 to AR3 in the same VLAN 6

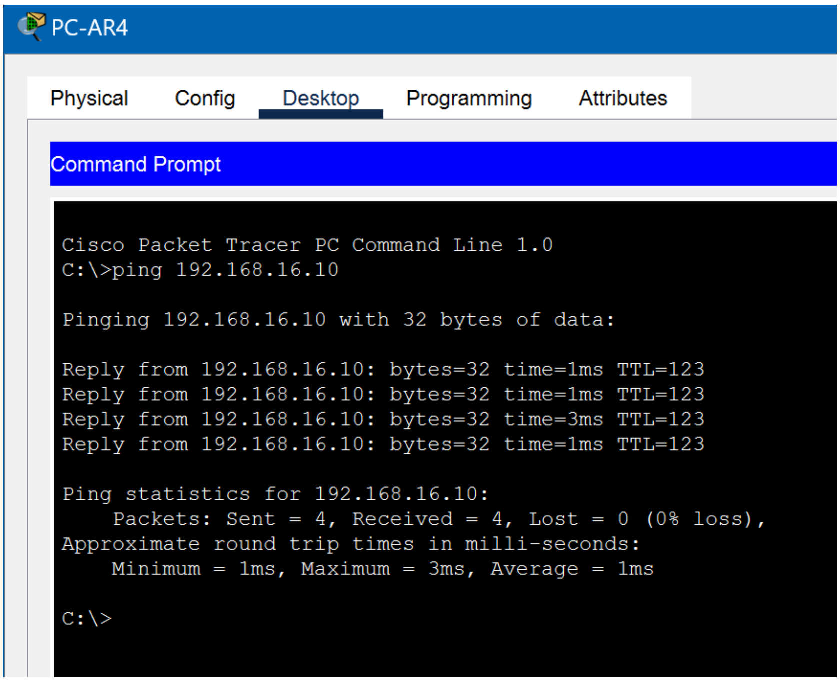
7.2 Connection PCs between VLANs



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.5.2

Pinging 192.168.5.2 with 32 bytes of data:

Reply from 192.168.5.2: bytes=32 time<1ms TTL=125
Reply from 192.168.5.2: bytes=32 time<1ms TTL=125
Reply from 192.168.5.2: bytes=32 time<1ms TTL=125
Reply from 192.168.5.2: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.5.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

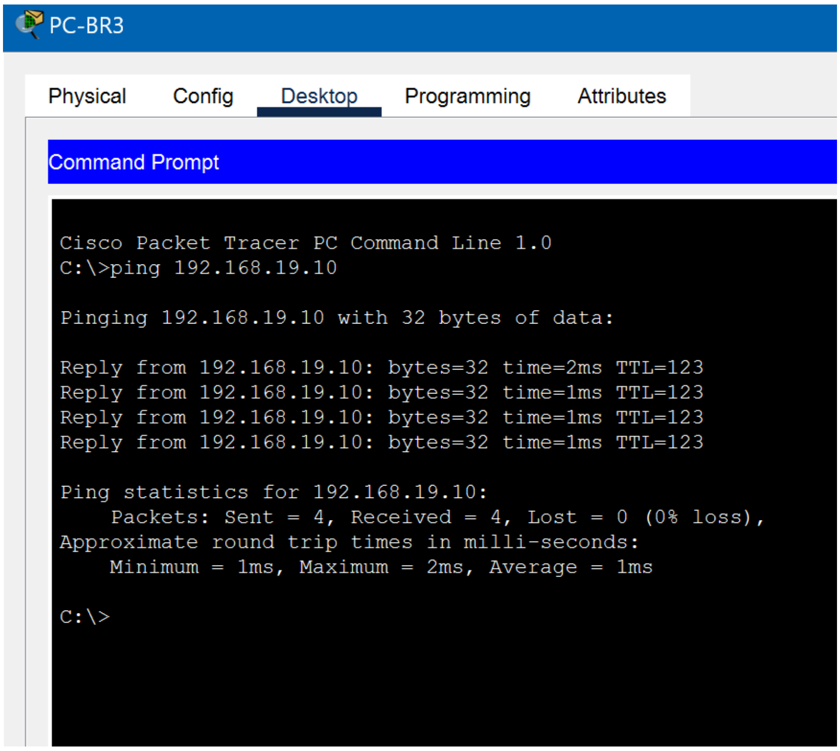
Figure 6: Test ping from BR5 to AR2

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



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.16.10

Pinging 192.168.16.10 with 32 bytes of data:

Reply from 192.168.16.10: bytes=32 time=1ms TTL=123
Reply from 192.168.16.10: bytes=32 time=1ms TTL=123
Reply from 192.168.16.10: bytes=32 time=3ms TTL=123
Reply from 192.168.16.10: bytes=32 time=1ms TTL=123

Ping statistics for 192.168.16.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms

C:\>
```

Figure 7: Test ping from AR3 to PC-DBP

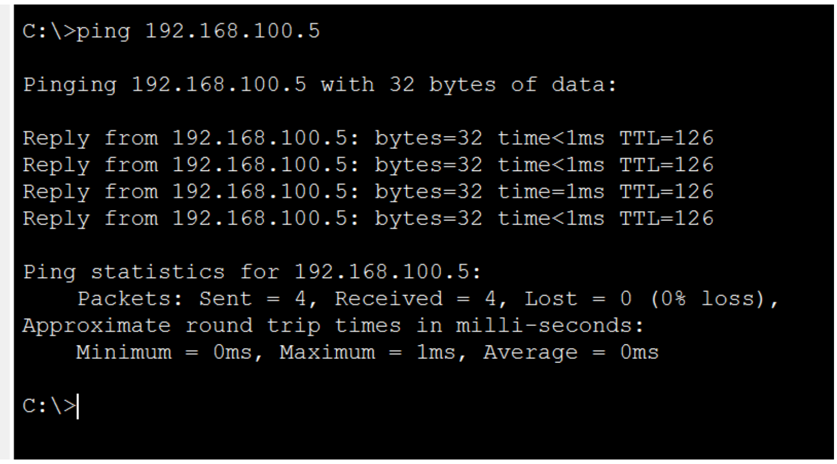


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.19.10

Pinging 192.168.19.10 with 32 bytes of data:

Reply from 192.168.19.10: bytes=32 time=2ms TTL=123
Reply from 192.168.19.10: bytes=32 time=1ms TTL=123
Reply from 192.168.19.10: bytes=32 time=1ms TTL=123
Reply from 192.168.19.10: bytes=32 time=1ms TTL=123

Ping statistics for 192.168.19.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

Figure 8: Test ping from BR3 to PC-BHTQ

7.4 Connection to server in the DMZ

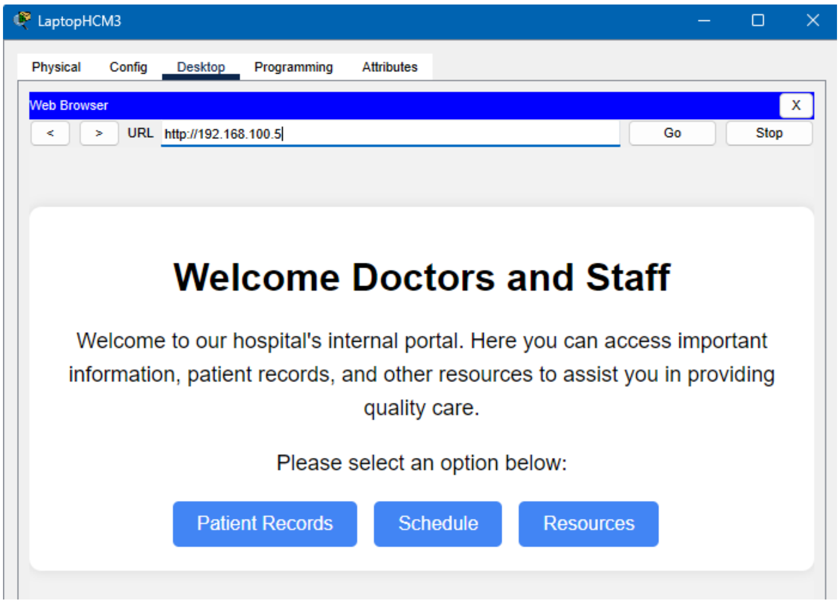
The main site and the auxiliary sites can access the DMZ, while the DMZ cannot access the sites (the INSIDE zone).



```
C:\>ping 192.168.100.5

Pinging 192.168.100.5 with 32 bytes of data:

Reply from 192.168.100.5: bytes=32 time<1ms TTL=126
Reply from 192.168.100.5: bytes=32 time<1ms TTL=126
Reply from 192.168.100.5: bytes=32 time=1ms TTL=126
Reply from 192.168.100.5: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.100.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Figure 9: Test ping from BR5 to DMZ

Moreover, DMZ provides Web services for Doctor and Staff to access Hospital Data.



URL: http://192.168.100.5

Welcome Doctors and Staff

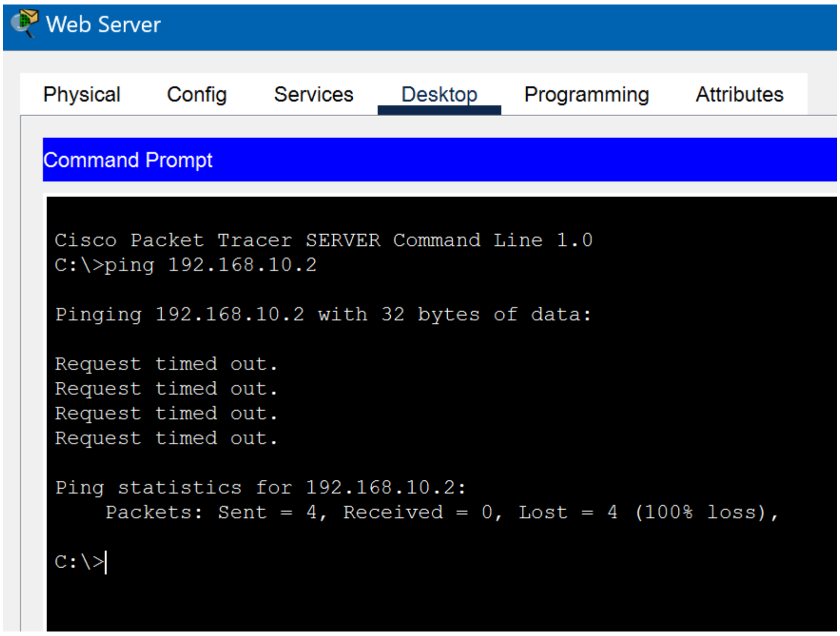
Welcome to our hospital's internal portal. Here you can access important information, patient records, and other resources to assist you in providing quality care.

Please select an option below:

Figure 10: HTML file for a Web Server simulation

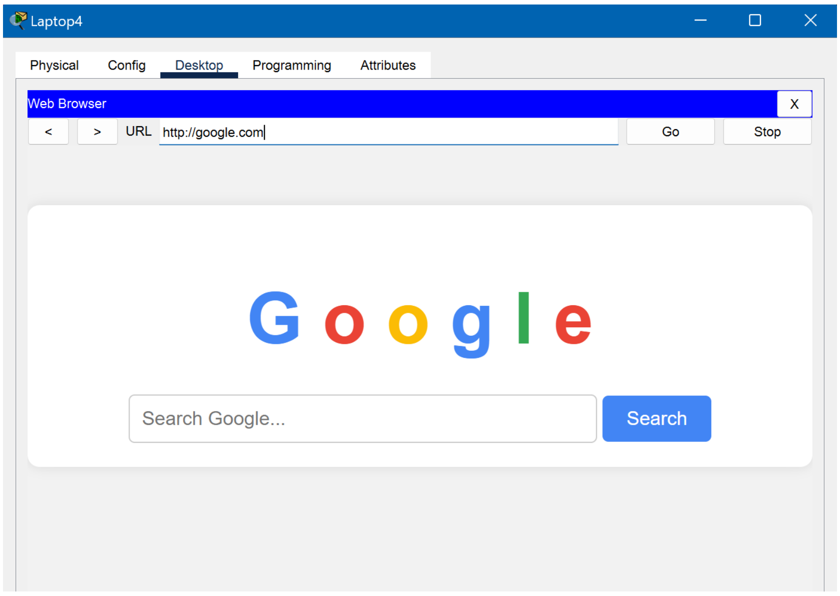
7.5 No connections from Customers' devices to PCs on the LAN

Customers at the Main site can get access to the Internet. However, they cannot get access to the PCs on the LAN.



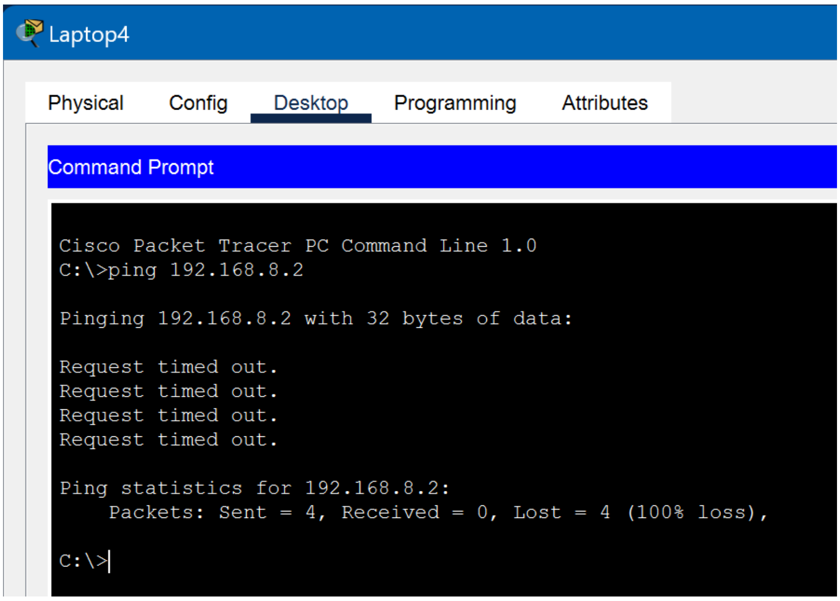
```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

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

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figure 11: No connection from DMZ to Main site



URL http://google.com

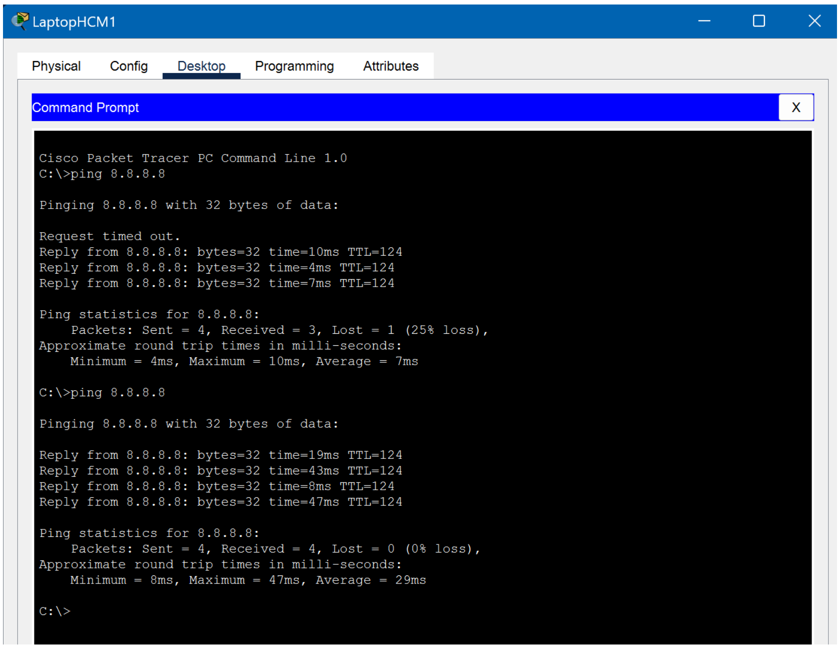
Figure 12: Customer laptop connects to the internet



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.8.2

Pinging 192.168.8.2 with 32 bytes of data:

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

Ping statistics for 192.168.8.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figure 13: No connection from Customer Laptop to VLAN 8

7.6 Internet Connection



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Request timed out.
Reply from 8.8.8.8: bytes=32 time=10ms TTL=124
Reply from 8.8.8.8: bytes=32 time=4ms TTL=124
Reply from 8.8.8.8: bytes=32 time=7ms TTL=124

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 10ms, Average = 7ms

C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time=19ms TTL=124
Reply from 8.8.8.8: bytes=32 time=43ms TTL=124
Reply from 8.8.8.8: bytes=32 time=8ms TTL=124
Reply from 8.8.8.8: bytes=32 time=47ms TTL=124

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 47ms, Average = 29ms

C:\>
```

Figure 14: Test ping from laptop Mainsite

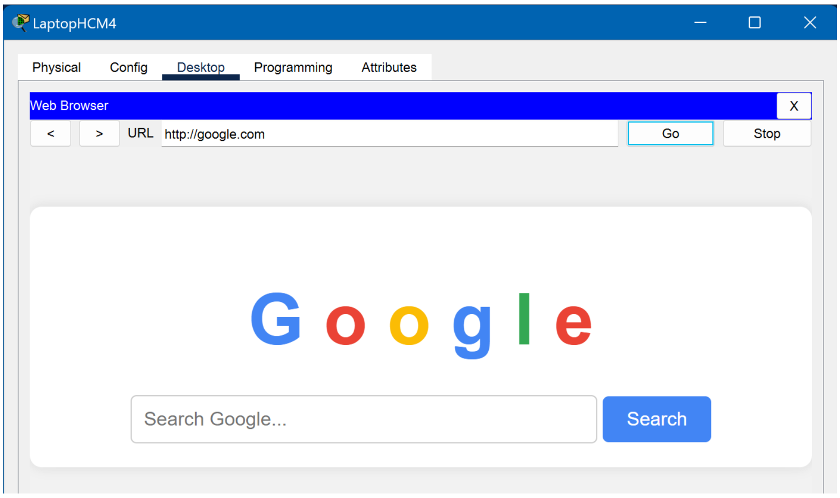


Figure 15: HCM Main site access Internet

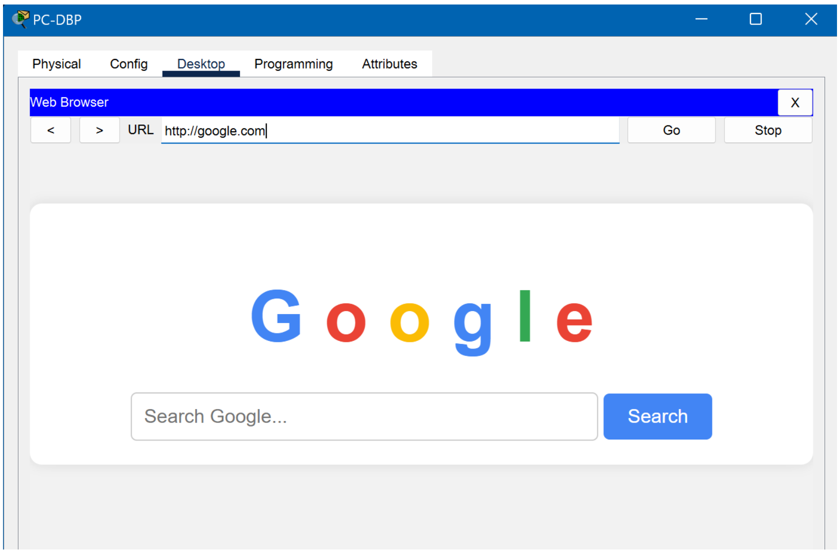


Figure 16: DBP access Internet

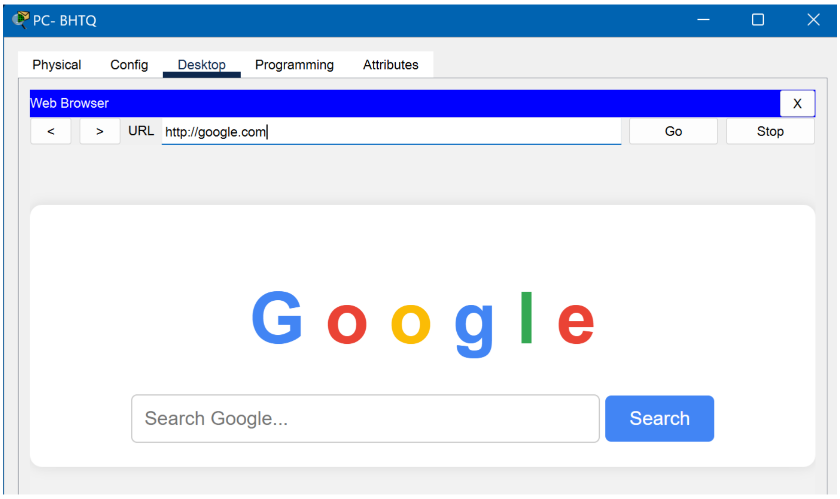


Figure 17: BHTQ access the Internet

8 System Evaluation

8.1 Reliability

8.1.1 Communication

- The system ensures communication between computers within the same department (same floor) of the main headquarters, as well as within the same branch.
- The system ensures communication between departments and floors of the main headquarters.
- The system ensures communication and connection between computers at the main headquarters and computers of the 2 branches, and vice versa.
- The system ensures connection between computers of the 2 branches.
- The system ensures that customers can access the Web server in the DMZ zone.
- The system ensures connectivity of computers within the system to the Internet.

8.2 Security

8.2.1 Features

- Prevent unauthorized access from the Internet to the internal network system.
- Ensure that servers in the ”Non-military” DMZ zone cannot connect to the internal network.
- Block access from customers using WIFI connection to the internal network system.
- Only allow Security department computers to access the Cameras.

8.3 Scalability

8.3.1 Capacity

- For each department, each floor of the main headquarters, and the main branch, corresponding to each VLAN, there are still plenty of IP addresses available to serve the system's expansion capability.

8.4 Limitations

8.4.1 General

- Overall, the network system lacks some network connection devices found in actual companies such as air conditioners, TVs, projectors, vacuum cleaning robots, etc.
- The system lacks load balancing devices to regulate sudden and abnormal increases in network traffic, especially when branches connect to the Internet simultaneously.
- The system lacks VPN connections to allow employees to connect to the company LAN network for remote work.
- The system does not have IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) to detect and prevent intrusion.

9 Conclusion

Throughout this network design assignment, we gained valuable insights into designing a topology for an enterprise or public network. Using tools like Packet Tracer was challenging yet rewarding. Overcoming obstacles like configuring firewalls and OSPF routing strengthened our problem-solving skills.

This project deepened our understanding of network architecture, security protocols, and routing strategies. It also sparked a greater interest in network design and simulation.

Overall, we're pleased with the outcome. This assignment provided us with hands-on experience and equipped us with skills to tackle real-world network challenges.

References

[1] Kurose, J. F., Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson.

[2] Cisco Networking Academy. "Creating a Simple Network Using Packet Tracer." Accessed 01/04/2024.