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

COMPUTER NETWORK - SEMESTER 241

ASSIGNMENT 2 REPORT

Lecturer: NGUYỄN MẠNH THÌN

Group: 3

Class: CC05

Students: Trần Trung Vĩnh - 2252914
Nguyễn Trần Huy Việt - 2252906
Phùng Gia Minh Khôi - 2252381
Trần Phú Đức - 2210814

HO CHI MINH CITY, NOVEMBER 2024

Contents

1 Contribution

Student	Student ID	Contribution	Percantage of work
Trần Trung Vĩnh	2252914	Test the system, Re-evaluate the network system	100%
Nguyễn Trần Huy Việt	2252906	IP diagram, wiring diagram (cabling), Packet tracer	100%
Phùng Gia Minh Khôi	2252381	Throughput, bandwidth, and safety parameters. Packet tracer	100%
Trần Phú Đức	2210814	Suitable network structures Recommended equipment	100%

2 Suitable network structures

2.1 Requirements analysis

- 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).
- 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
- 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.)
- Connect between PCs in the same VLAN
- Connect PCs between VLANs
- Connect PCs between the main Site and the two Auxiliary Sites
- Connect to servers in the DMZ
- No connections from Customers' devices to company local network on the LAN
- Connect to the Internet and a Web server.

2.2 Checklist

We will employ a hierarchical network model for each site, dividing the network into three distinct layers: core, distribution, and access.

2.2.1 Access Layer

- Devices: 24-port switches, access points
- Function: Connects workstations and customer's hosts to the network.

2.2.2 Distribution Layer

- Devices: Multilayer switches
- Function: Aggregates and filters traffic from the access layer, implementing network policies such as VLANs and routing protocols.

2.2.3 Core Layer

- Devices: Firewalls and routers
- Function:
  - Firewalls: Enforce security policies, filter traffic, and protect the network from threats.
  - Routers: Optimize network performance through load balancing, static routing for internet connectivity, and network address translation (NAT) between internal and external networks.

Routing Protocol: To enhance network efficiency and reliability, we will implement the Open Shortest Path First (OSPF) routing protocol on all multilayer switches, firewalls, and routers. OSPF facilitates dynamic routing, allowing for automatic route updates and optimal traffic flow.

2.2.4 Main site

We have 600 workstations which will be divided into half, each building will have 300 workstations. Each building has 5 floors, hence each floor has 60 workstations, which is split into 10 rooms. Hence, each room has 6 workstations. Therefore, we can expand the number of machines when needed since we reserve 96 - 72 + 2 = 26 ports each floor for more machines to come.

Since the number of workstations at each floor is very large, we will use 4 24-port switches to make access switches for each floor, and the remaining ports can be used for future expansion.

Each floor in building A and B has 2 cameras. There is another 2 camera in technical building. Every camera will connect to 1 switches that in turn connect to the firewall for ease of controlling traffic.

Each floor in building A and B will contain 1 access point. All access point will connect 1 switches that in turn connect to the firewall for ease of controlling traffic of customer hosts.

We use 1 central switch for each floor. This switch is a Layer 3 switch and is connected to **1 central firewall**. So that we can configure this switch and the firewall to allow or not allow VLANs to access each other. Each layer 3 switch will connect to every access layer switches in the site.

Regarding the hospital's servers, our team found that there are usually the following servers:

- Web server: customers can access information about their accounts in the hospital, as well as other services.
- File server: to share information.
- Mail server: store, send, and receive mail.
- DHCP Server: provides and assigns IP addresses for network devices.
- DNS server: translate domain names to IP addresses as requested.
- Database server: store the database.
- Backup server: stores the backup information.

We will use 10 servers as the followings:

- 2 Database Server
- 1 FTP Server
- 2 DHCP Server
- 1 DNS Server

- 1 Web server
- 1 Mail server
- 1 App server
- 2 Backup server

To ensure network stability and security, our data center houses ten servers connected to a dedicated switch. This switch, in turn, is linked to a firewall, allowing granular control over inbound and outbound traffic. The firewall is then connected to the main router at headquarters. From the headquarters router, two leased lines are connect 2 to two auxiliary sites. The headquarter router is where inbound and outbound traffic flow through the most with the traffic from 3 sites out and from the customers in to connect to the web server. For that reasons this router will have load balencing mechanism, with 2 xDSL connect to the outside and static routing. If one interface is down or throttled, the traffic can go through the other line. We also configure NAT at these 2 interfaces to ensure secure internet connections.

To enhance security and network segmentation, we employ a VLAN-based network structure. A Layer 3 switch serves as the core device, enabling fine-grained control over VLAN access to the external network and inter-VLAN communication. This approach effectively isolates different departments and minimizes potential security risks.

The network will be configured with VPN IPsec site-to-site encryption and decryption to ensure that any information contained in the packets remains secure and inaccessible to hackers, even if intercepted.

2.2.5 Other sites

The network system is classified into 3 levels:
- **Level 1**: Central branch router and firewall
- **Level 2**: The central layer 3 switch of the building.
- **Level 3**: Switch to connect to hosts.

On the first floor, the IT department, consisting of five workstations, and the Cabling Central Local, with three workstations, are connected alongside two servers. All devices on this floor connect to a single 24-port VLAN-capable switch, facilitating efficient network management and device interconnectivity.

Moving to the second floor, the infrastructure includes three VLAN-capable 24-port switches, each supporting up to 20 workstations. This arrangement ensures sufficient capacity and scalability for departmental needs. The entire building's network is anchored by a main Layer 3 switch, which seamlessly connects the four VLAN-capable switches on both floors. This main switch also interfaces with the firewall and the central router, maintaining a robust and secure connection similar to that of the main site.

To enhance security and network management, the company has implemented a VLAN structure. The Layer 3 switch acts as the core switch, allowing for customized access between departmental VLANs and the external network. This configuration ensures that network traffic is segmented, enhancing overall security while allowing controlled communication between departments. Using this VLAN setup, the company can effectively manage network access and maintain a high level of security across its infrastructure.

Switches in the first floor and layer 3 switch in the second floor will connect to a firewall. The firewall then connected to the branch router. The router will have one leased line connect to the headquarters router, so any connection to the Internet will go through the main routers. For each branch, we will use 2 servers as follows:

- 1 File Server

- 1 DHCP Server

3 Recommended equipment, IP diagram, and wiring diagram (cabling)

3.1 Recommended equipment and typical specifications

3.1.1 Switch CISCO Catalyst 2960

Figure 1: Switch CISCO Catalyst 2960 WS-C2960-24TT-L

WS-C2960-24TT-L is one of the Cisco Catalyst 2960 Series switches. Cisco Catalyst 2960 Series switches support voice, video, data, and highly secure access. They also deliver scalable management as your business needs change. The Common Features are included: Enhanced security including Cisco TrustSec for providing authentication, access control, and security policy administration, Multiple Fast or Gigabit Ethernet performance options, Cisco EnergyWise for power management, Scalable network management.

Ports	24 Ethernet 10/100 ports
Switching Bandwidth	32 Gbps
Uplinks	2 Ethernet 10/100/1000 ports
DC input voltages (RPS input)	12 V at 11.25 A (-48 V at 7.8 A)
Unicast MAC Addresses	8000
Power Rating	0.470 kVA
Max. Power Consumption	75W
Max. Watt Power	30W
IPv4 IGMP Groups	255
Voltage	100 to 240 VAC (Autoranging); 50 to 60 Hz
Packets per second	6.6 Mpps
Max VLANs	255
Switching Bandwidth	32 Gbps
Memory DRAM	64 MB
Flash Memory	32 MB
Forwarding Bandwidth	16 Gbps
VLAN IDs	4000
Jumbo Frames	9018 bytes

3.1.2 Multilayer Switch Layer 3 3650-24PS

Figure 2: Multilayer Switch Layer 3 WS-C3650-24PS-L

This Cisco 3650 Catalyst Switch supports both PoE (IEEE 802.3af) and PoE+ (IEEE 802.3at standard), which provide up to 30W of power per port. PoE removes the need for wall power to each PoE-enabled device and eliminates the cost for additional electrical cabling and circuits that would otherwise be necessary in IP phone and WLAN deployments. This Cisco 3650 Catalyst Switches can provide a lower TCO for deployments that incorporate Cisco IP phones, Cisco Aironet wireless LAN (WLAN) access points, or any IEEE 802.3at-compliant end device. The total PoE budget for this switch is 390W.

Model info:	WS-C3650-24PS-L
Enclosure type	Rack-mountable – 1U
Ports	24 x 10/100/1000 (POE+) + 4 x 1G SFP
Network management Interface	Ethernet management port: RJ-45 connectors 4-pair Cat-5 UTP cabling Management console port: RJ-45-to-DB9 cable for PC connections
Available PoE Power	390W
Switching Capacity	88Gbps
Maximum stacking number	9
Stack Bandwidth	160Gbps
Forwarding Performance	41.66Mpps
FNF entries	24000
Maximum VLANs IDs	4,094
Maximum VLANs IDs	32K
CPU	Multicore CPU
RAM	4 G
Flash Memory	2 G
Wireless	
Number of AP per switch/stack	50
Number of wireless clients per switch/stack	1000
Total number of WLANs per switch	64
Wireless bandwidth per switch	up to 20Gbps
Supported Aironet AP series	3700, 3600, 3500, 2600, 1600, 1260, 1140, 1040
Expansion / Connectivity	
Console ports	USB (Type-B), Ethernet (RJ-45)
Expansion Slot(s)	power redundant slot

3.1.3 Router cisco 2911/K9

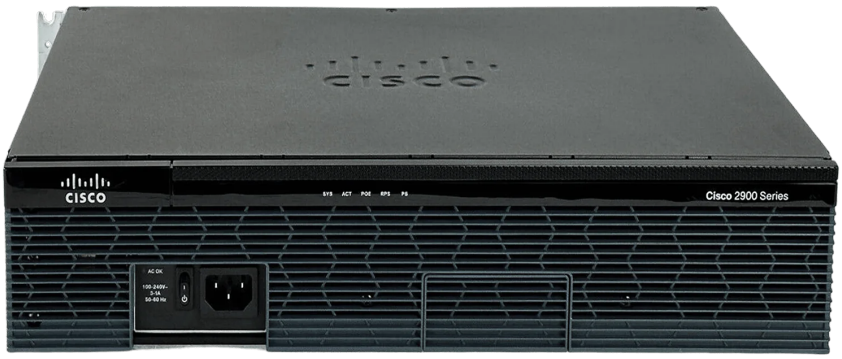

Figure 3: Router cisco 2911/K9

Cisco® 2900 Series Integrated Services Routers build on 25 years of Cisco innovation and product leadership. The new platforms are architected to enable the next phase of branch-office evolution, providing rich media collaboration and virtualization to the branch while maximizing operational cost savings The Integrated Services Routers Generation 2 platforms are future-enabled with multi-core CPUs, support for high capacity DSPs (Digital Signal Processors) for future enhanced video capabilities, high powered service modules with improved availability, Gigabit Ethernet switching with enhanced POE, and new energy monitoring and control capabilities while enhancing overall system performance. Additionally, a new Cisco IOS® Software Universal image and Services Ready Engine module enable you to decouple the deployment of hardware and software, providing a flexible technology foundation which can quickly adapt to evolving network requirements. Overall, the Cisco 2900 Series offer unparalleled total cost of ownership savings and network agility through the intelligent integration of market leading security, unified communications, wireless, and application services.

Rack Units	2RU
Interface	3 integrated 10/100/1000 Ethernet ports (RJ-45 only)
Expansion Slot(s)	1 service module slot1 Internal Service Module slot 2 onboard digital signal processor (DSP) slots 4 enhanced high-speed WAN interface card slots
RAM	512 MB (installed) / 2 GB (max)
Flash memory	256 MB (installed) / 8 GB (max)

3.1.4 Firewall Cisco ASA 5506-X

Figure 4: Firewall Cisco ASA 5506-X

Product Description	Cisco ASA5506-K9 ASA 5506-X with services 8GE Data, 1GE Mgmt, AC, 3DES/AES
Form Factor	DesktopRack/ Mountable
Interfaces	8 x 1 Gigabit Ethernet1 x Management port1 x USB type A 2.01 x RJ45 Serial port1 x Mini Console
Expansion Slot	N/A
Throughput: FW + AVC (1024B)	250 Mbps
Throughput: FW + AVC + IPS (1024B)	125 Mbps
Maximum concurrent sessions, with AVC	50,000
IPSec VPN Through (1024B TCP w/Fastpath)	100 Mbps
Application Visibility and Control (AVC)	Standard, supporting more than 4000 applications, as well as geolocations, users, and websites
Third-party and open-source ecosystem	Open API for integrations with third-party products; Snort® and OpenAppID community resources for new and specific threats
High availability and clustering	Requires Security Plus License; Active/standby
Solid-state drive	50 GB mSata
Memory	4GB
Flash	8GB
Stateful inspection firewall throughput	750 Mbps
Stateful inspection firewall throughput (multiprotocol)	300 Mbps
IPsec VPN throughput (450B UDP L2L test)	100 Mbps

3.1.5 Cat6 Cable

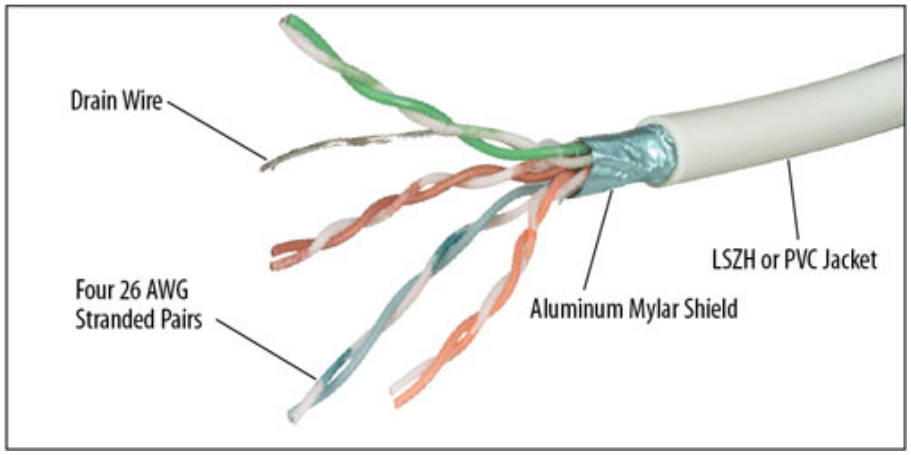

Figure 5: Cat6 Cable

- Affordable, but slightly more expensive than Cat5e
- Maximum frequency of 500MHz
- Maximum cable length is 100metres for slower network speeds (up to 1000Mbps), or 55 metres maximum for higher network speeds
- Less interference than Cat5e
- Top speed of 10Gbps over 55 metres of cable
- RJ45 Connectors

3.1.6 Optical fiber

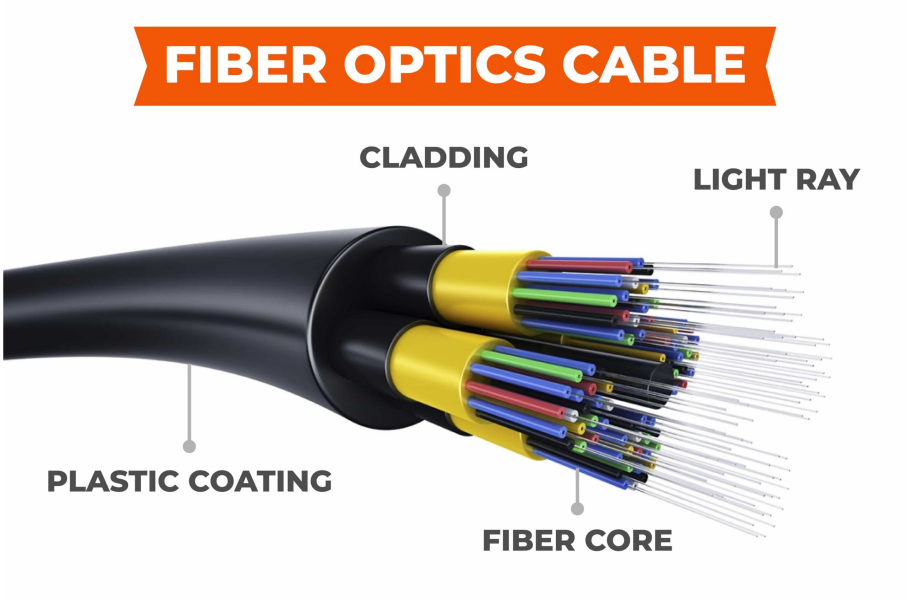

Figure 6: Optical fiber

- Shell: made of PE plastic.
- Coated steel core protects loose pipes.
- Machined steel core.
- Fiber type: Multi mode 50/125 um.
- Number of yarns: 4 strands.
- Maximum transmission speed: 1 Gigabit/s.

3.2 IP Diagram

3.2.1 Main Site:

Subnet	1	2	4	8	16
Host	4096	2048	1024	512	256
Subnet mask	/20	/21	/22	/23	/24

- **Required Hosts:** 600
- **Minimum Subnet Mask:** 255.255.240.0 (/20)
- **Usable Hosts per Subnet:** 4094

=> 2 floors per subnet

Subnet	16
Host	256
Subnet mask	/24

Floor	Network ID	Subnet Mask	Host ID Range	Usable Hosts	Broadcast ID	Vlan
Server	192.168.0.0	/24	192.168.0.1 - 192.168.0.254	254	192.168.0.255	
IT/Security	192.168.1.0	/24	192.168.1.1 - 192.168.1.254	254	192.168.1.255	7
Building A Floor 4 and 5	192.168.2.0	/24	192.168.2.1 - 192.168.2.254	254	192.168.2.255	2
Building A Floor 2 and 3	192.168.3.0	/24	192.168.3.1 - 192.168.3.254	254	192.168.3.255	3
Floor 1 of Building A and B	192.168.4.0	/24	192.168.4.1 - 192.168.4.254	254	192.168.4.255	4
Building B Floor 2 and 3	192.168.5.0	/24	192.168.5.1 - 192.168.5.254	254	192.168.5.255	5
Build B Floor 4 and 5	192.168.6.0	/24	192.168.6.1 - 192.168.6.254	254	192.168.6.255	6
Camera	192.168.7.0	/24	192.168.7.1 - 192.168.7.254	254	192.168.7.255	
Customer	192.168.8.0	/24	192.168.8.1 - 192.168.8.254	254	192.168.8.255	

3.2.2 Branch Sites:

- **Required Hosts per Site:** 60
- **Minimum Subnet Mask:** 255.255.255.0 (/24)
- **Usable Hosts per Subnet:** 255

Subnet	1	2	4	8	16
Host	256	128	64	32	16
Subnet mask	/24	/25	/26	/27	/28

Branch Site 1:

Network ID	Subnet Mask	Host ID Range	Usable Hosts	Broadcast ID	Vlan
192.168.20.0	/26	192.168.20.1 - 192.168.20.62	62	192.168.20.63	20
192.168.21.0	/26	192.168.21.1 - 192.168.21.62	62	192.168.21.63	21
192.168.22.0	/26	192.168.22.1 - 192.168.22.62	62	192.168.22.63	

Branch Site 2:

Network ID	Subnet Mask	Host ID Range	Usable Hosts	Broadcast ID	Vlan
192.168.30.0	/26	192.168.30.1 - 192.168.30.62	62	192.168.30.63	30
192.168.31.0	/26	192.168.31.1 - 192.168.31.62	62	192.168.31.63	31
192.168.32.0	/26	192.168.32.1 - 192.168.30.62	62	192.168.30.63	

3.3 Schematic physical setup of the network

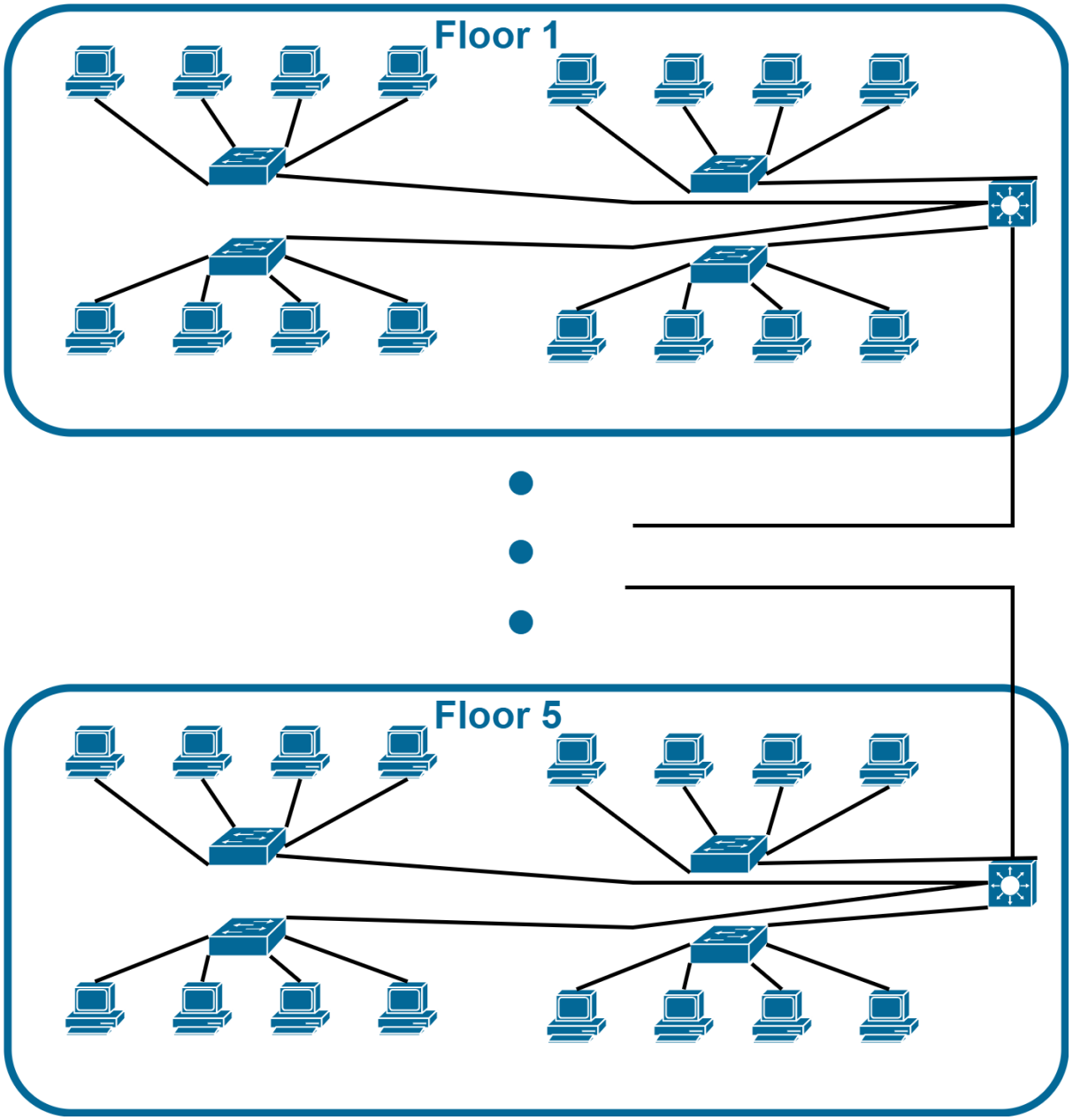

Figure 7: Each floor schematic physical setup in main site

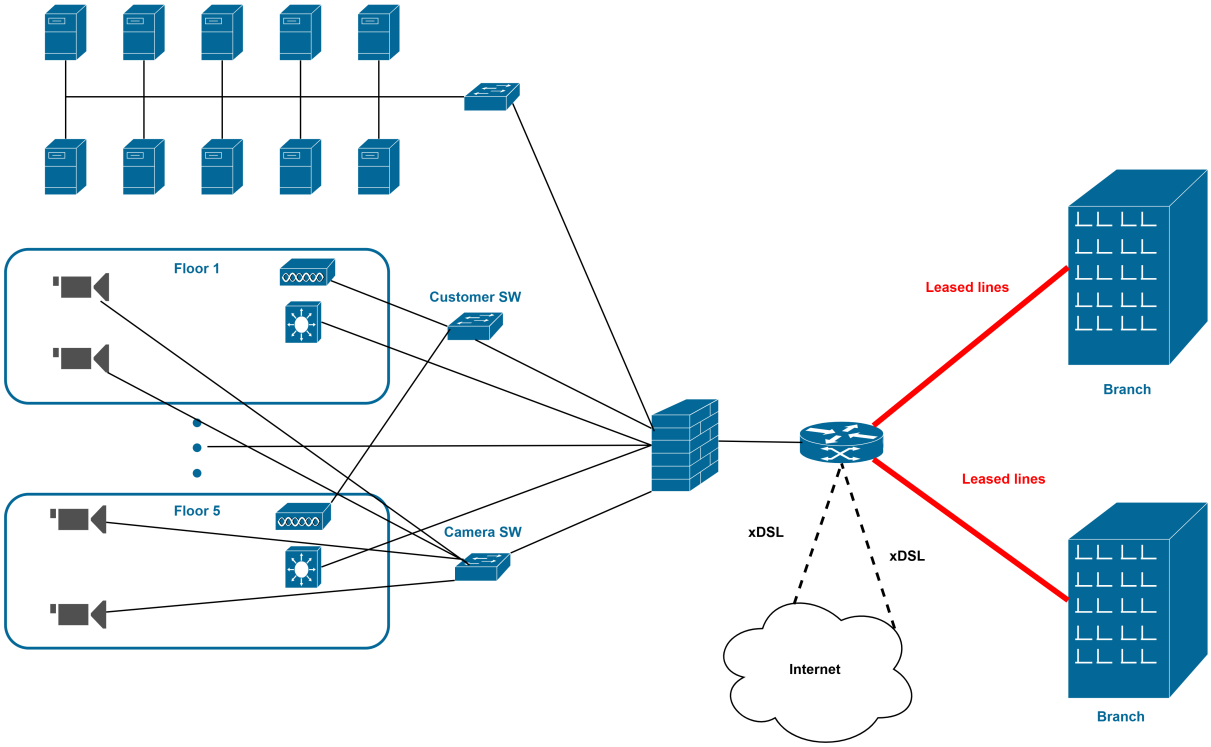

Figure 8: Wan connection diagram and main site schematic physical setup

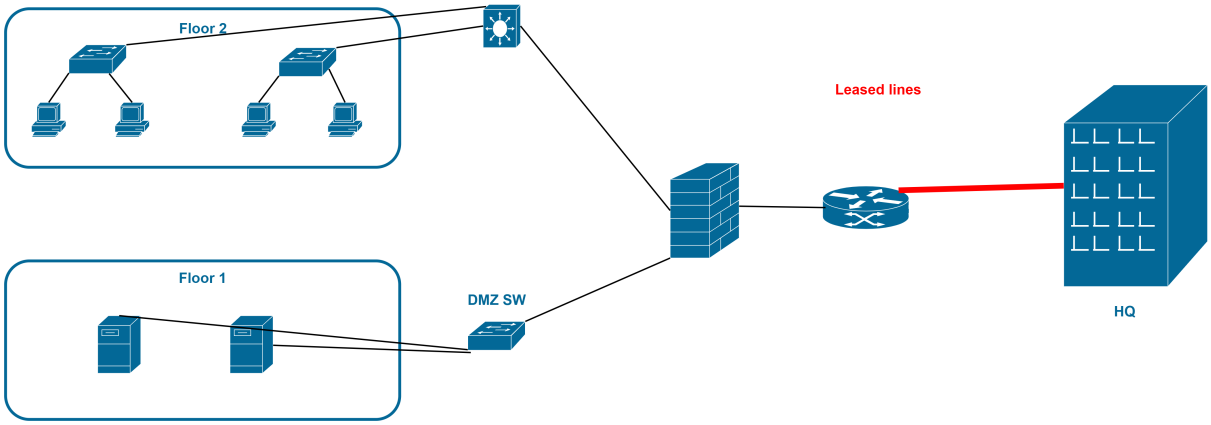

Figure 9: Auxiliary site schematic physical setup

4 Throughput, bandwidth, and configuration for the hospital network

4.1 Throughput and bandwidth

The dataflows and workload of the system can be shared for the main Site and the two Auxiliary Sites as follows:

- Servers for software updates, web access, and database access, ... The total download estimate is about 1000 MB/day and the upload estimate is 2000 MB/day.
- Each workstation is used for Web browsing, document downloads, and customer transactions, ... The total download estimate is about 500 MB/day and the upload estimate is 100 MB/day.

- WiFi-connected devices from customers' access for downloading are about 500 MB/day.
- The hospital is supposed to use Internet all the day.
- Thus, we need to calculate throughput and bandwidth (about 80%) at peak hours 9AM-11AM and 3PM-4PM. They accumulate 3 hours, or 1/8 of the day.

4.1.1 Main site

- There are 10 servers. The total upload capacity is about 2000 MB/day, and total download capacity is about 1000 MB/day. We calculate Throughput at the time of using the highest transmission line (Concentrated 80%) in 3 hours:

$$T_{up} = 10 \times \frac{2000}{86400} = 0.231 MBps$$

$$B_{up} = 10 \times \frac{2000 \times 0.8}{3 \times 3600} = 1.481 MBps$$

$$T_{down} = 10 \times \frac{1000}{86400} = 0.116 MBps$$

$$B_{down} = 10 \times \frac{1000 \times 0.8}{3 \times 3600} = 0.741 MBps$$

- There are total 600 workstations. The total upload capacity is about 100 MB/day, and total download capacity is about 500 MB/day. We calculate the Throughput at the time of using the highest transmission line:

$$T_{up} = 600 \times \frac{100}{86400} = 0.694 MBps$$

$$B_{up} = 600 \times \frac{100 \times 0.8}{3 \times 3600} = 4.444 MBps$$

$$T_{down} = 600 \times \frac{500}{86400} = 3.472 MBps$$

$$B_{down} = 600 \times \frac{500 \times 0.8}{3 \times 3600} = 22.222 MBps$$

- There are estimated 300 WiFi-connected devices from customers' access for downloading are about 500 MB/day. We can calculate Throughput when using the highest transmission line:

$$T = 300 \times \frac{500}{86400} = 1.736 MBps$$

$$B = 300 \times \frac{500 \times 0.8}{3 \times 3600} = 11.111 MBps$$

- The total throughput and bandwidth when all network systems work concurrently is:

$$T_{up} = 0.231 + 0.694 = 0.925 Mbps$$

$$B_{up} = 1.481 + 4.444 = 5.925MBps$$

$$T_{down} = 0.116 + 3.472 + 1.736 = 5.324Mbps$$

$$B_{down} = 1.481 + 4.444 + 11.111 = 17.036MBps$$

- To ensure the system works stably when there are more developments in the next 5 years, we extend 20%:

$$T_{up}^{'} = 0.925 \times 120\% = 1.11Mbps$$

$$B_{up}^{'} = 5.925 \times 120\% = 7.11MBps$$

$$T_{down}^{'} = 5.324 \times 120\% = 6.389Mbps$$

$$B_{down}^{'} = 17.036 \times 120\% = 20.443MBps$$

4.1.2 Branch

Two auxiliary sites have the same amount of servers, workstations, and WiFi-connected devices. Therefore, the result is same for both sites.

There are 2 servers. The total upload capacity is about 2000 MB/day, and total download capacity is about 1000 MB/day. We calculate Throughput at the time of using the highest transmission line (Concentrated 80%) in 3 hours:

$$T_{up} = 2 \times \frac{2000}{86400} = 0.046MBps$$

$$B_{up} = 2 \times \frac{2000 \times 0.8}{3 \times 3600} = 0.296MBps$$

$$T_{down} = 2 \times \frac{1000}{86400} = 0.023MBps$$

$$B_{down} = 2 \times \frac{1000 \times 0.8}{3 \times 3600} = 0.148MBps$$

- There are total 60 workstations. The total upload capacity is about 100 MB/day, and total download capacity is about 500 MB/day. We calculate the Throughput at the time of using the highest transmission line:

$$T_{up} = 60 \times \frac{100}{86400} = 0.069MBps$$

$$B_{up} = 60 \times \frac{100 \times 0.8}{3 \times 3600} = 0.444MBps$$

$$T_{down} = 60 \times \frac{500}{86400} = 0.347MBps$$

$$B_{down} = 60 \times \frac{500 \times 0.8}{3 \times 3600} = 2.222MBps$$

- There are estimated 300 WiFi-connected devices from customers' access for downloading are about 500 MB/day. We can calculate Throughput when using the highest transmission line:

$$T = 300 \times \frac{500}{86400} = 1.736 MBps$$

$$B = 300 \times \frac{500 \times 0.8}{3 \times 3600} = 11.111 MBps$$

- The total throughput and bandwidth when all network systems work concurrently is:

$$T_{up} = 0.046 + 0.069 = 0.115 Mbps$$

$$B_{up} = 0.296 + 0.444 = 0.74 MBps$$

$$T_{down} = 0.023 + 0.347 + 1.736 = 2.106 Mbps$$

$$B_{down} = 0.148 + 2.222 + 11.111 = 13.481 MBps$$

- To ensure the system works stably when there are more developments in the next 5 years, we extend 20%:

$$T_{up}^{'} = 0.115 \times 120\% = 0.138 Mbps$$

$$B_{up}^{'} = 0.74 \times 120\% = 0.888 MBps$$

$$T_{down}^{'} = 2.106 \times 120\% = 2.527 Mbps$$

$$B_{down}^{'} = 13.481 \times 120\% = 16.177 MBps$$

4.2 Configuration for the hospital network

4.2.1 Vlans and Switchs

Based on the information provided above, there are five VLANs distributed across ten floors. Each switch on these floors will reserve one port, specifically interface FastEthernet0/1, to operate in trunk mode for communication between different vlans. The remaining interfaces will be assigned to their respective VLANs. For example:

```
Switch#show run
Building configuration...
Current configuration : 2253 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
```

```
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
!
.
.
.
interface FastEthernet0/24
 switchport access vlan 2
 switchport mode access
!
```

4.2.2 Layer 3 switchs

For the Layer 3 switches, we create five VLANs, mirroring the VLANs designated for the floors. The interfaces that connect to the switches are configured as trunks, similar to the switches, to facilitate VLAN traffic. Each VLAN is assigned an IP address and a helper address, which serves as the DHCP server to enable hosts to request IP addresses. For example:

```
interface Vlan2
 mac-address 0009.7cdc.6501
 ip address 192.168.2.1 255.255.255.0
 ip helper-address 192.168.0.2
!
interface Vlan3
 mac-address 0009.7cdc.6502
 ip address 192.168.3.1 255.255.255.0
 ip helper-address 192.168.0.2
!
interface Vlan4
 mac-address 0009.7cdc.6503
 ip address 192.168.4.1 255.255.255.0
 ip helper-address 192.168.0.2
!
interface Vlan5
 mac-address 0009.7cdc.6504
 ip address 192.168.5.1 255.255.255.0
 ip helper-address 192.168.0.2
!
interface Vlan6
 mac-address 0009.7cdc.6505
 ip address 192.168.6.1 255.255.255.0
 ip helper-address 192.168.0.2
!
interface Vlan7
 mac-address 0009.7cdc.6506
```

```
 ip address 192.168.1.1 255.255.255.0
 ip helper-address 192.168.0.2
!
```

Next, configure the Layer 3 switch for IP routing to route traffic between VLANs and to other destinations using static routes. Additionally, we implement the OSPF protocol to enhance the efficiency of network traffic propagation. Finally, add a static route for any traffic not destined for an address within the hospital network or the internet, directing it straight to the firewall as the next destination. For example:

```
ip routing
!
router ospf 10
 router-id 0.0.0.2
 log-adjacency-changes
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.3.0 0.0.0.255 area 0
 network 192.168.4.0 0.0.0.255 area 0
 network 192.168.5.0 0.0.0.255 area 0
 network 192.168.6.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.100.4 0.0.0.3 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.100.5
!
```

4.2.3 Firewall

For the firewall, we start by configuring each interface. Designate one interface as INSIDE for the hospital's network, another as OUTSIDE for external traffic, a third as CAMERA for the camera system, and a fourth as CUSTOMER for the customer's internet connection.

```
interface GigabitEthernet1/1
 nameif OUTSIDE
 security-level 0
 ip address 192.168.100.1 255.255.255.252
!
interface GigabitEthernet1/2
 nameif INSIDE
 security-level 100
 ip address 192.168.100.5 255.255.255.252
!
interface GigabitEthernet1/3
 nameif CAMERA
 security-level 100
 ip address 192.168.7.1 255.255.255.0
!
interface GigabitEthernet1/4
 nameif GUEST
```

```
 security-level 0
 ip address 192.168.8.1 255.255.255.0
!
interface GigabitEthernet1/5
 nameif DMZ
 security-level 60
 ip address 192.168.0.1 255.255.255.0
!
```

Access-lists are a crucial component of the firewall configuration. To manage the hospital's network, we allow all traffic from the OUTSIDE interfaces to the firewall if it is destined for the web server or DNS server. However, for the ICMP protocol used for ping and trace route, we only permit signals originating from within the network to reach the firewall, while blocking all incoming ICMP traffic from the outside network:

```
access-list INTERNET-ACCESS extended permit tcp any any eq domain
access-list INTERNET-ACCESS extended permit udp any any eq domain
access-list INTERNET-ACCESS extended permit tcp any any eq www
access-list INTERNET-ACCESS extended permit tcp any any eq 443
access-list INTERNET-ACCESS extended permit tcp host 10.0.4.2 any
access-list INTERNET-ACCESS extended permit icmp 192.168.20.0 255.255.255.0 any
access-list INTERNET-ACCESS extended permit icmp 192.168.21.0 255.255.255.0 any
access-list INTERNET-ACCESS extended permit icmp 192.168.22.0 255.255.255.0 any
access-list INTERNET-ACCESS extended permit icmp 192.168.30.0 255.255.255.0 any
access-list INTERNET-ACCESS extended permit icmp 192.168.31.0 255.255.255.0 any
access-list INTERNET-ACCESS extended permit icmp 192.168.32.0 255.255.255.0 any
!
access-group INTERNET-ACCESS in interface OUTSIDE
```

For the DMZ interface, we will allow any signals that respond to web services or DNS. We will also permit connections for TCP and UDP protocols, provided they respond back to addresses within the network. Regarding the ICMP protocol, we will allow all signals to pass through the firewall from DMZ interfaces, enabling employees to ping and trace route the DMZ.

```
access-list DMZ-ACCESS extended permit icmp any any
access-list DMZ-ACCESS extended permit tcp any any eq domain
access-list DMZ-ACCESS extended permit udp any any eq domain
access-list DMZ-ACCESS extended permit udp any any eq bootps
access-list DMZ-ACCESS extended permit udp any any eq bootpc
access-list DMZ-ACCESS extended permit tcp any 192.168.2.0 255.255.255.0
access-list DMZ-ACCESS extended permit tcp any 192.168.1.0 255.255.255.0
access-list DMZ-ACCESS extended permit tcp any 192.168.3.0 255.255.255.0
access-list DMZ-ACCESS extended permit tcp any 192.168.4.0 255.255.255.0
access-list DMZ-ACCESS extended permit tcp any 192.168.5.0 255.255.255.0
access-list DMZ-ACCESS extended permit tcp any 192.168.6.0 255.255.255.0
access-list DMZ-ACCESS extended permit tcp any 192.168.20.0 255.255.255.0
access-list DMZ-ACCESS extended permit tcp any 192.168.21.0 255.255.255.0
access-list DMZ-ACCESS extended permit tcp any 192.168.30.0 255.255.255.0
access-list DMZ-ACCESS extended permit tcp any 192.168.31.0 255.255.255.0
```

```
access-list DMZ-ACCESS extended permit udp any 192.168.1.0 255.255.255.0
access-list DMZ-ACCESS extended permit udp any 192.168.2.0 255.255.255.0
access-list DMZ-ACCESS extended permit udp any 192.168.3.0 255.255.255.0
access-list DMZ-ACCESS extended permit udp any 192.168.4.0 255.255.255.0
access-list DMZ-ACCESS extended permit udp any 192.168.5.0 255.255.255.0
access-list DMZ-ACCESS extended permit udp any 192.168.6.0 255.255.255.0
access-list DMZ-ACCESS extended permit udp any 192.168.20.0 255.255.255.0
access-list DMZ-ACCESS extended permit udp any 192.168.21.0 255.255.255.0
access-list DMZ-ACCESS extended permit udp any 192.168.30.0 255.255.255.0
access-list DMZ-ACCESS extended permit udp any 192.168.31.0 255.255.255.0
access-list DMZ-ACCESS extended permit udp any 192.168.8.0 255.255.255.0
access-list DMZ-ACCESS extended permit tcp any 192.168.8.0 255.255.255.0
!
access-group DMZ-ACCESS in interface DMZ
```

Lastly, for customer internet access and the camera system, we will permit customer access only for web or DNS services. Additionally, we will only allow the IT department, with the IP address range 192.168.1.0/24, to ping or traceroute the camera system. For the remaining configuration, we will implement static routing to the router for internet access and utilize the OSPF protocol:

```
access-list CUSTOMER-ACCESS extended permit tcp 192.168.8.0 255.255.255.0 host 192.168.0.4 eq www
access-list CUSTOMER-ACCESS extended permit tcp 192.168.8.0 255.255.255.0 host 192.168.0.4 eq 443
access-list CUSTOMER-ACCESS extended permit tcp 192.168.8.0 255.255.255.0 host 192.168.0.3 eq domain
access-list CUSTOMER-ACCESS extended permit udp 192.168.8.0 255.255.255.0 host 192.168.0.3 eq domain
access-list CUSTOMER-ACCESS extended permit udp any any eq bootps
access-list CUSTOMER-ACCESS extended permit udp any any eq bootpc
access-list IT-CAMERA extended permit icmp any 192.168.1.0 255.255.255.0
!
access-group CUSTOMER-ACCESS in interface GUEST
access-group IT-CAMERA in interface CAMERA
!
router ospf 10
 log-adjacency-changes
 network 192.168.0.0 255.255.255.0 area 0
 network 192.168.7.0 255.255.255.0 area 0
 network 192.168.8.0 255.255.255.0 area 0
 network 192.168.100.4 255.255.255.252 area 0
 network 192.168.100.0 255.255.255.252 area 0
!
route OUTSIDE 0.0.0.0 0.0.0.0 192.168.100.2 1
```

4.2.4 Router

For the routers, each one will be configured with the OSPF protocol and connected to the main router at the headquarters to implement OSPF multi-area. The two routers will also have static routes to the main router at the headquarters. Additionally, each router will be configured with VPN IPsec site-to-site to encrypt the packets between sites, preventing them from being sniffed. Finally, the main headquarters router will have a NAT configuration to translate the IP addresses from the internal network to the external network. An example in main router:

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp key cisco address 10.0.0.2
crypto isakmp key cisco address 10.0.1.2
!
!
!
crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac
crypto ipsec transform-set VPN-SET1 esp-aes 256 esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
 set peer 10.0.0.2
 set transform-set VPN-SET
 match address 100
!
!
crypto map VPN-MAP1 10 ipsec-isakmp
 set peer 10.0.1.2
 set transform-set VPN-SET1
 match address 100
!

spanning-tree mode pvst
!
interface GigabitEthernet0/0
 ip address 192.168.100.2 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 10.0.2.1 255.255.255.252
 ip nat outside
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 10.0.3.1 255.255.255.252
 ip nat outside
 duplex auto
 speed auto
!
interface Serial0/3/0
 ip address 10.0.0.1 255.255.255.252
```

```
 ip nat inside
 clock rate 2000000
 crypto map VPN-MAP
!
interface Serial0/3/1
 ip address 10.0.1.1 255.255.255.252
 ip nat inside
 clock rate 2000000
 crypto map VPN-MAP1
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 10
 router-id 0.0.0.1
 log-adjacency-changes
 network 192.168.100.0 0.0.0.3 area 0
 network 10.0.0.0 0.0.0.3 area 1
 network 10.0.1.0 0.0.0.3 area 2
!
router rip
!
ip nat inside source list 10 interface GigabitEthernet0/2 overload
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.2.2
ip route 0.0.0.0 0.0.0.0 10.0.3.2
!
ip flow-export version 9
!
!
access-list 10 permit 192.168.0.0 0.0.255.255
access-list 100 permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
```

NOTE: Almost all the configurations mentioned above pertain to the network devices at the headquarters. All network devices at the branch sites will be configured similarly with different ip addresses, but without the camera system and customer internet access.

5 Design the network map

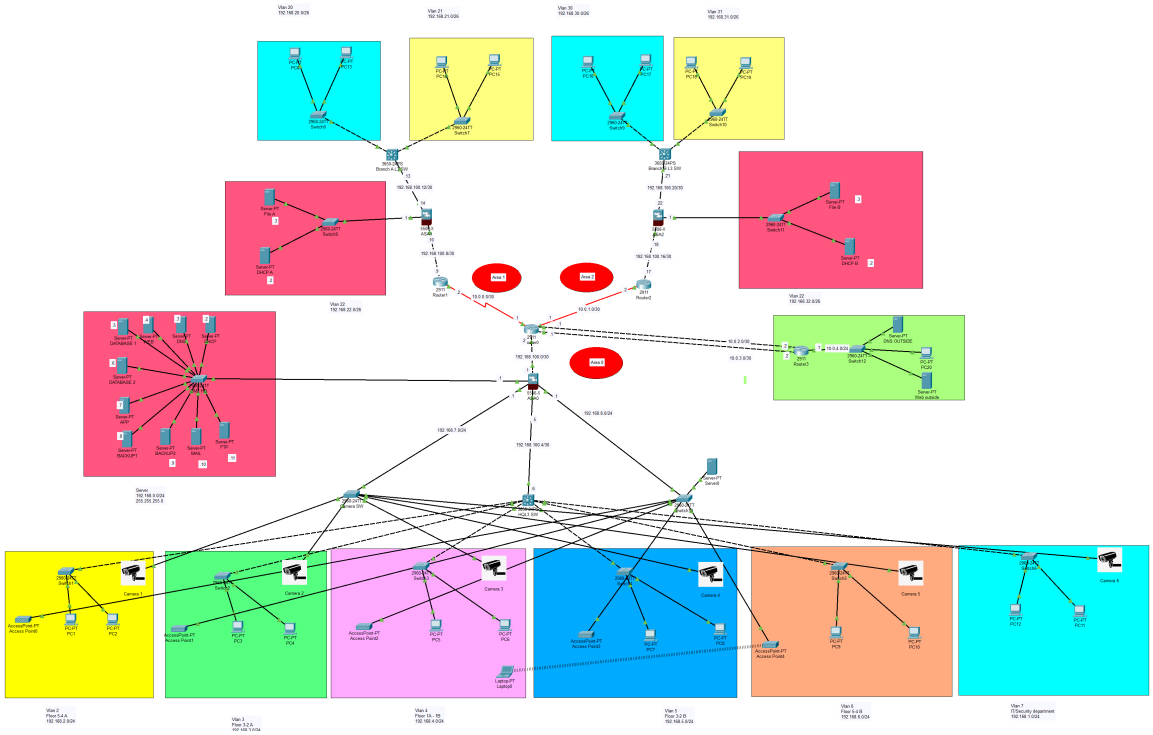

Figure 10: Network topoplogy in packet tracer

NOTE: Cisco Packet Tracer may appear glitchy during use, ensure to press the forward button a few times next to the timestamp for the network device to complete booting. If the connections do not appear as shown in the test, close without saving and reopen the file, then press forward multiple times again as before.

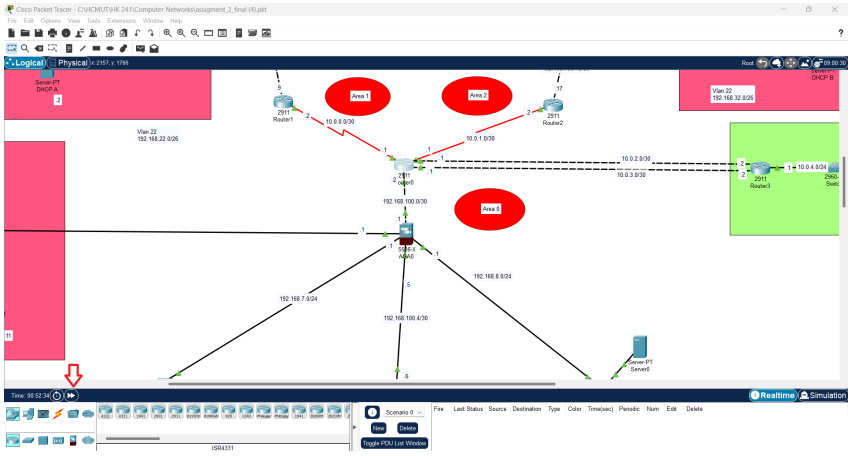

Figure 11: Forward button to the left of the screen

6 Test the system

6.1 Connect between PCs in the same VLAN

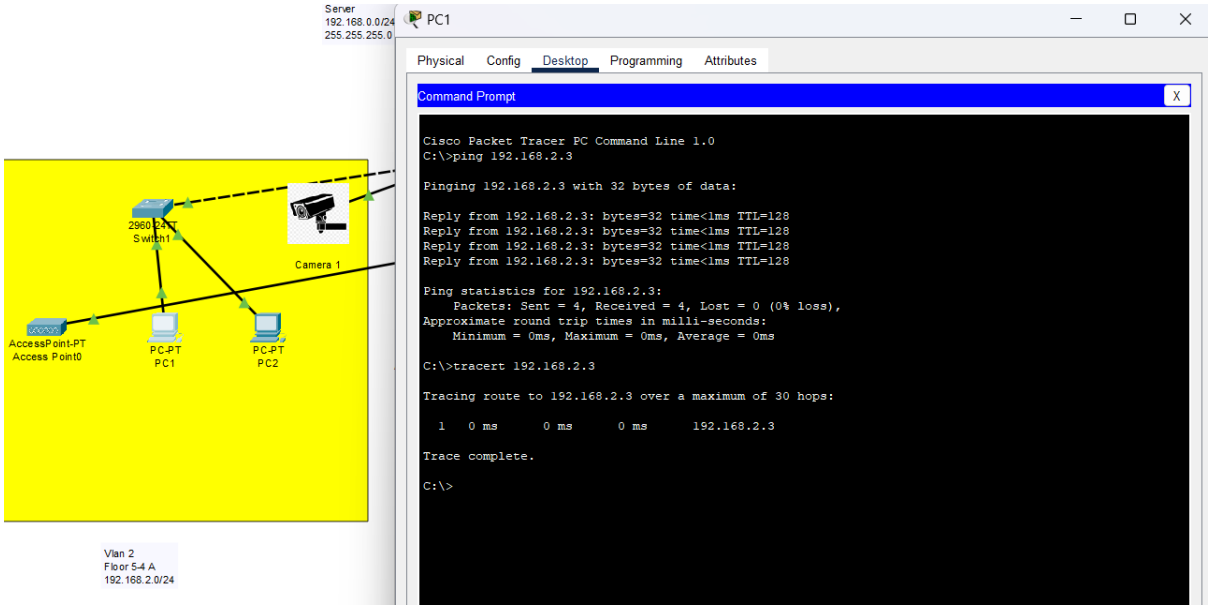

Figure 12: Connection between PC1 (192.168.2.2) and PC2 (192.168.2.3) in the same vlan

6.2 Connect PCs between VLANs

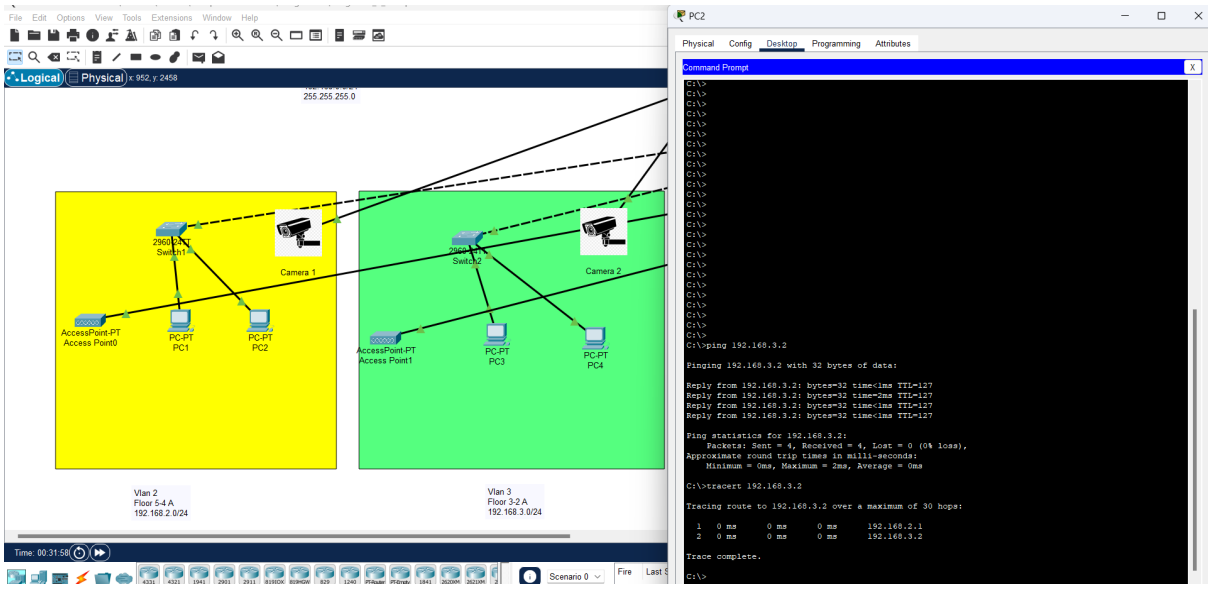

Figure 13: Connection between PC2 (192.168.2.3) and PC3 (192.168.3.2) between vlan 2 and 3

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

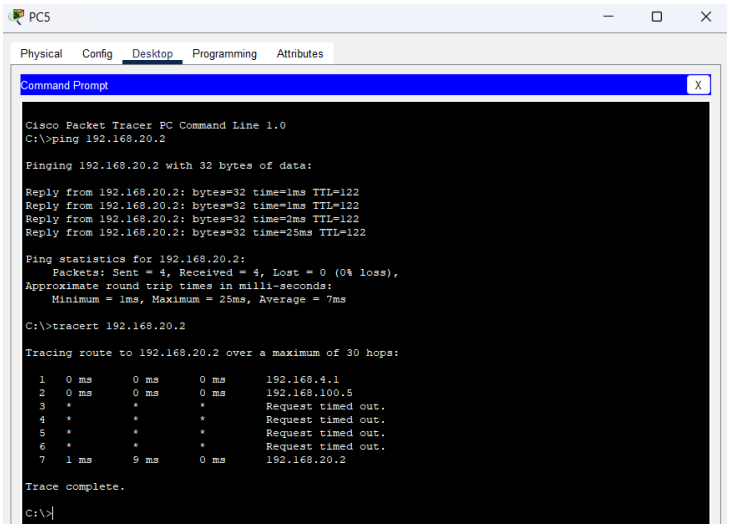

Figure 14: Connection between PC5 (192.168.4.3) and PC0 (192.168.20.2) between vlan 4 and 20, going from main branch to Auxiliary branch A

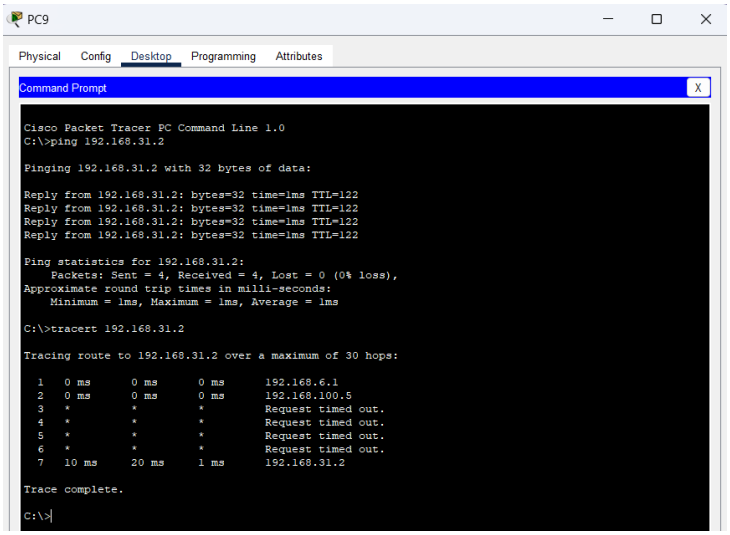

Figure 15: Connection between PC9 (192.168.6.3) and PC19 (192.168.31.2) between vlan 6 and 31, going from main branch to Auxiliary branch B

6.4 Connect to servers in the DMZ

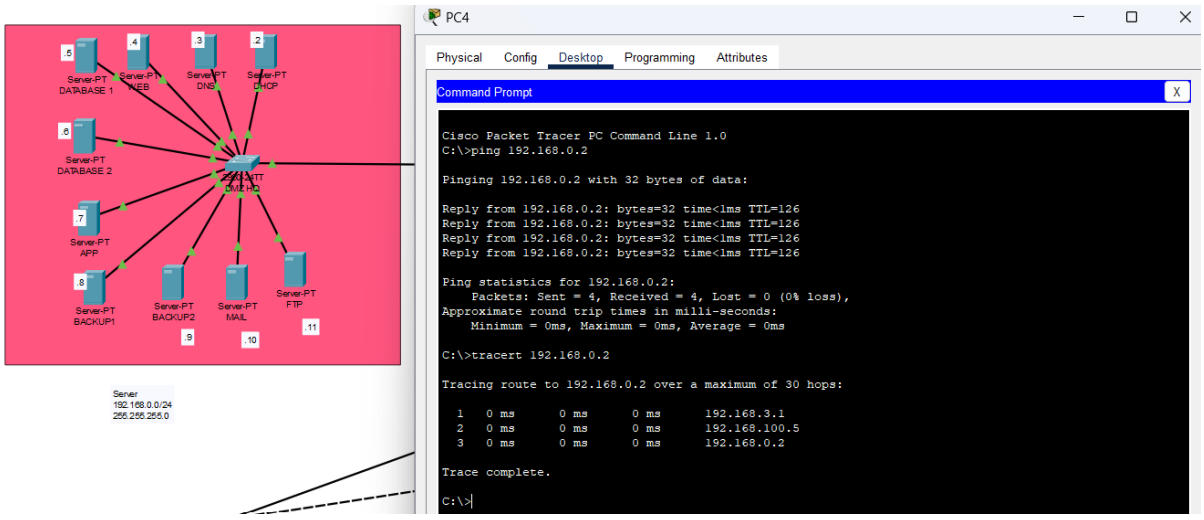

Figure 16: Connection between PC4 (192.168.6.3) and DHCP server (192.168.0.2)

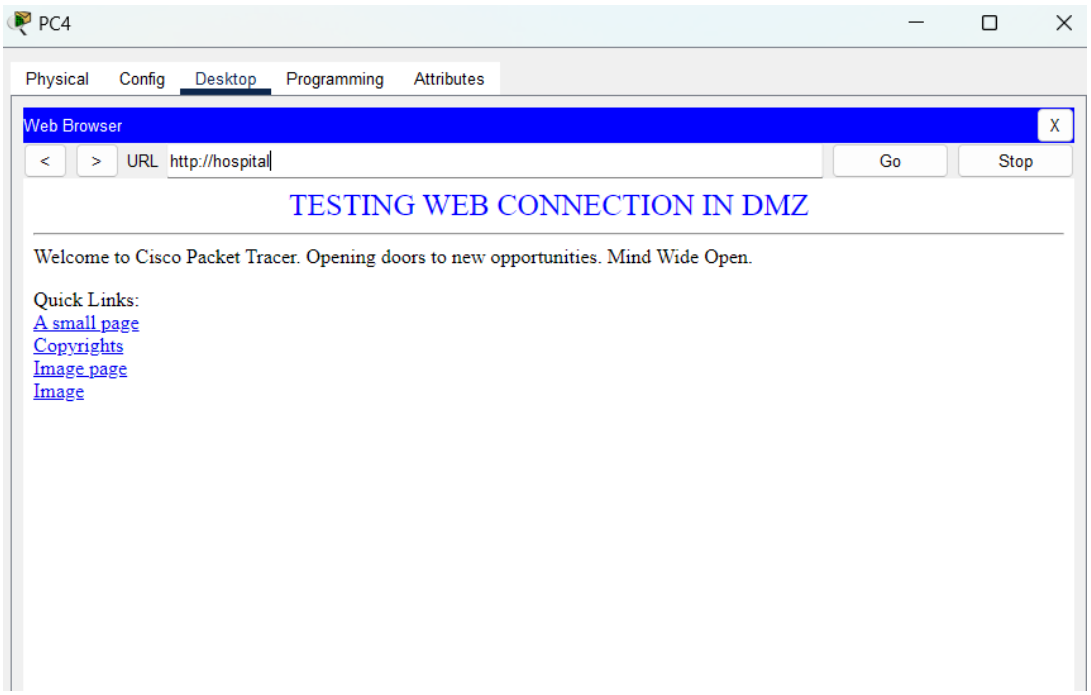

Figure 17: Combination of connections between PC4 (192.168.6.3), DHCP server (192.168.0.2), DNS server (192.168.0.3) and Web server (192.168.0.4) to retrive web page

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

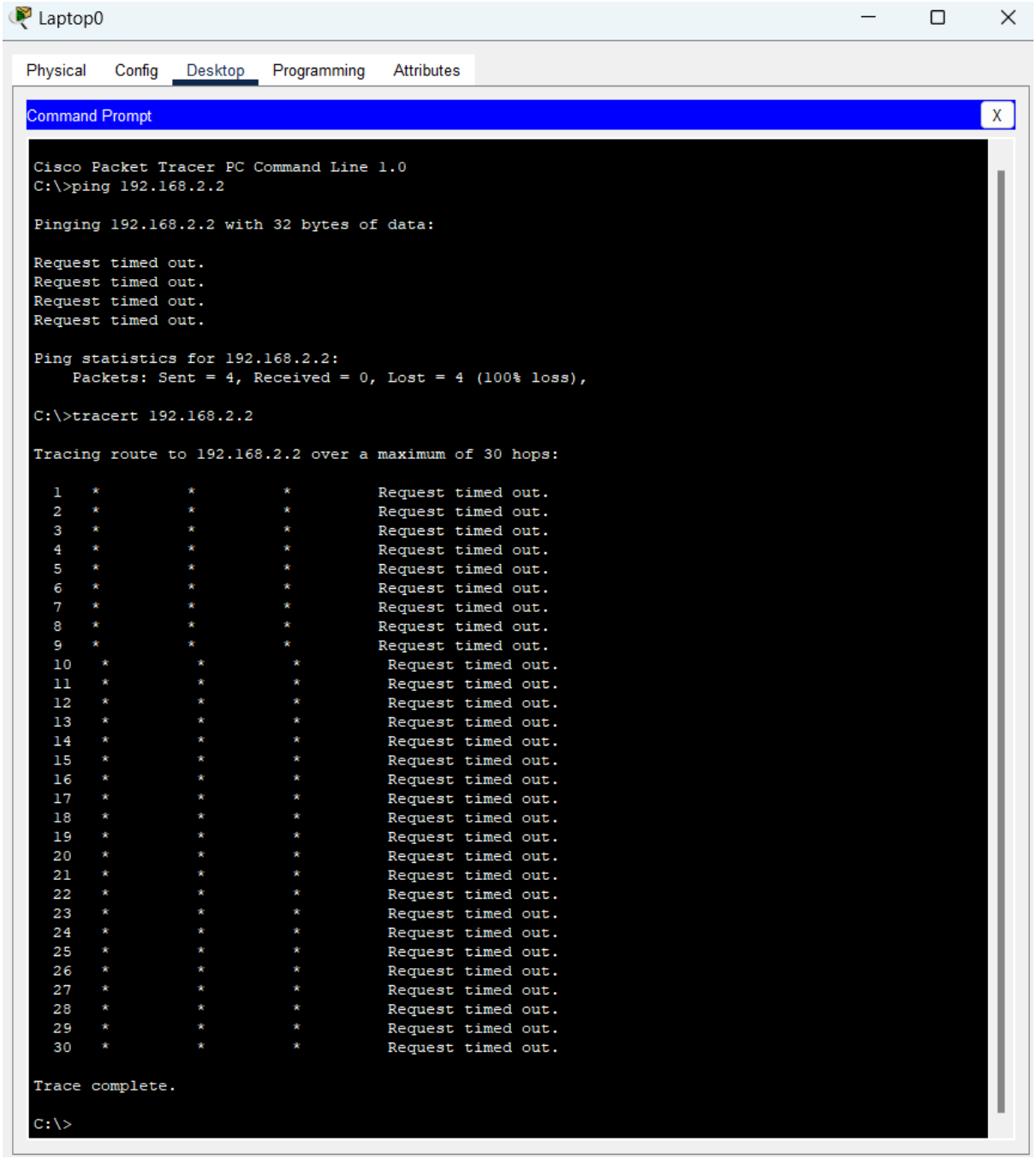

Figure 18: Connection between Customer laptop0 (192.168.8.3) and PC1(192.168.2.2)

6.6 Connect to the Internet to a Web server

Figure 19: Connection between PC12 (192.168.1.2) and Web server in the internet

6.7 Connect between 2 sites with VPN

```
Router#show crypto ipsec sa

interface: Serial0/3/0
    Crypto map tag: VPN-MAP, local addr 10.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
   current_peer 10.0.0.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 10.0.0.1, remote crypto endpt.:10.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/3/0
     current outbound spi: 0x62C5913A(1657114938)

     inbound esp sas:
      spi: 0x4EE5F5D8(1323693528)
        transform: esp-aes 256 esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3526)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE
```

Figure 20: Connect between 2 sites with VPN

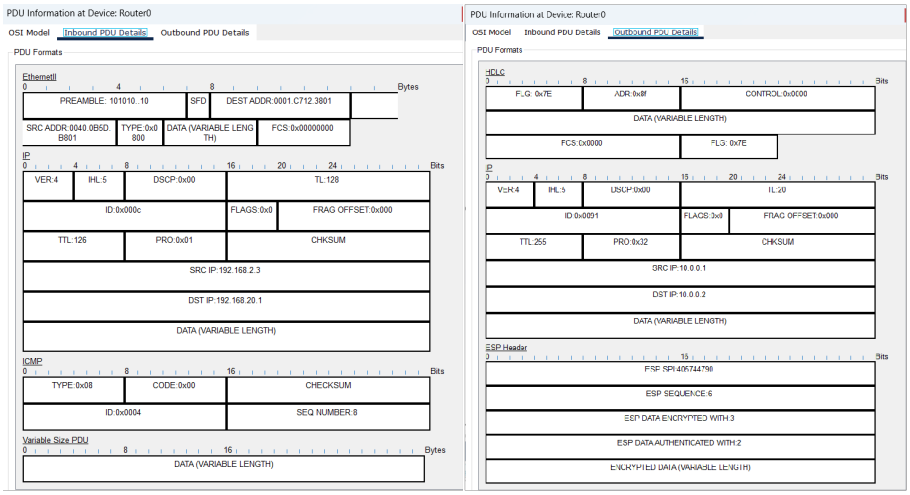

Figure 21: Comparison between inbound and outbound of encrypted packet

After using ping from PC1 (192.168.2.2) to PC (192.168.20.2) on the branch sites, we observe that there are some packet encrypted and decrypted.

7 Re-evaluate the network system

In this project, we have successfully learn and implement many computer network knowledge include:

- Vlan
- Trunking
- Static routing
- Subnetting and IP addressing
- Static ip address and Dynamic ip address (DHCP)
- DNS and Web server (HTTP, HTTPS)
- Inter vlan routing on layer switches
- Access control lists
- OSPF protocol
- NAT
- Firewall polacies configuration
- VPN IPSEC site-to-site

Besides that, the network still have many issues

7.1 The remaining problems for the project

- No implementation of FTP, Mail, Backup, File server
- No fiber cabling (GPON)
- WAN connection between sites is only one line. If the line is down the Auxiliary site can not contact other sites and using the internet.
- Only one router to connect the sites and the internet, if the router is down the hold hospital can not communicate with each other.
- No connection from teleworker to connect to Company LAN.

7.2 Development orientation in the future

- Implement FTP, Mail, Backup, File server
- Implement fiber cabling (GPON)
- Proposed better WAN connection
- Proposed better design of the topology to prevent Single Point of Failure (SPoF) of the main site and the two auxiliary sites

8 References

1. Kurose, J. F., & Ross, K. W. (2021). Computer networking : a top-down approach (8th ed.). Pearson.

2. Gurutech Networking Training - YouTube. www.youtube.com. https://www.youtube.com/@gurutechnetworks.

3. PM Networking - YouTube. Retrieved November 28, 2024, from. https://www.youtube.com/channel/UCSkbHbq0ZP0AsvakSLXGS4w.

4. SASiteNet. (n.d.). YouTube. Retrieved November 28, 2024, from https://www.youtube.com/channel/UC_NGil9Gw4STni97cTVaWNA.

5. Benard. (2024). Gurutech Networking Training. Otombenard.com. https://gurutechnetworks.otombenard.com/youtubeproject.