

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



Computer Network - CO3093

Assignment 2

Hospital Network Topology Design

Students: Vuong Khang- 2250008
Vo Hoang Long - 2053192
Tran Dang Khoa- 2252363

Instructor: Mr. Nguyen Le Duy Lai

HO CHI MINH CITY, November 2024

Contents

| | | |
|----------|--|-----------|
| 1 | Suitable Network Structure | 2 |
| 1.1 | Network System Requirements | 2 |
| 1.1.1 | Main Site | 2 |
| 1.1.2 | Auxiliary Site - Dien Bien Phu Street & Ba Huyen Thanh Quan Street | 2 |
| 1.1.3 | Data Flow and Work Load | 2 |
| 1.1.4 | Growing in the future | 2 |
| 1.2 | Surveyed Checklist at installation locations | 2 |
| 1.2.1 | Main Site | 2 |
| 1.2.2 | 2 auxiliary sites: Dien Bien Phu and Ba Huyen Thanh Quan Streets | 3 |
| 1.3 | High load area | 3 |
| 1.4 | Network Structure | 3 |
| 2 | List of minimum equipment, IP plan, and wiring diagram | 5 |
| 2.1 | Recommended equipment and typical specifications | 5 |
| 2.1.1 | Router CISCO PT-Empty | 5 |
| 2.1.2 | Layer 2 Switch CISCO Catalyst 2960 WS-C2960-24TT-L | 5 |
| 2.1.3 | WS-C3650-24PS-L Catalyst 3650 Switch | 7 |
| 2.1.4 | Lightweight Access Point Cisco 3702I-C-K9 | 8 |
| 2.1.5 | FIREWALL CISCO ASA 5506-X | 9 |
| 2.1.6 | Cisco 3504 Wireless Controller | 10 |
| 2.2 | IP Planning | 10 |
| 2.2.1 | Main Site | 10 |
| 2.2.2 | Auxiliary Site - Dien Bien Phu Street | 11 |
| 2.2.3 | Auxiliary Site - Ba Huyen Thanh Quan Street | 11 |
| 2.3 | Schematic Physical Setup | 12 |
| 2.3.1 | Wiring Diagram Main Site | 12 |
| 2.3.2 | Wiring Diagram Auxiliary Sites | 12 |
| 2.3.3 | SD-WAN | 12 |
| 3 | Calculate Throughput and Bandwidth and hospital network configuration suggestion | 13 |
| 3.0.1 | Main Site | 13 |
| 3.0.2 | 2 Auxiliary Sites | 13 |
| 4 | Design the network map using Packet Tracer | 15 |
| 4.0.1 | The whole system | 15 |
| 4.0.2 | BUILDING A | 16 |
| 4.0.3 | BUILDING B | 17 |
| 4.0.4 | IT | 18 |
| 4.0.5 | Dien Bien Phu Site | 19 |
| 4.0.6 | Ba Huyen Thanh Quan Site | 20 |
| 4.0.7 | DMZ | 21 |
| 4.0.8 | Internet | 22 |
| 5 | Test the system with popular tools such as ping, traceroute, etc. on the simulated system | 23 |
| 5.0.1 | Dynamic IP address on devices with DHCP server | 23 |
| 5.0.2 | Ping devices in the same VLAN | 24 |
| 5.0.3 | Ping devices in different VLANs | 25 |
| 5.0.4 | Ping from Customers'device to PCs on the LAN | 26 |



| | | |
|----------|---|-----------|
| 5.0.5 | Ping from PC on Main Site to PC on DBP Site | 27 |
| 5.0.6 | Ping from PC on DBP Site to PC on Main Site | 28 |
| 5.0.7 | Access to Web Server of Hospital located inside DMZ | 29 |
| 5.0.8 | Access to Web Server on the INTERNET (Google) | 31 |
| 5.0.9 | Network Address Translation (NAT) | 32 |
| 5.0.10 | Surveillance Camera System - IoT Server | 33 |
| 6 | Re-evaluate the designed network system through the following features: reliability, ease of upgrade, diverse support software, safety, network security, etc. | 35 |
| 6.1 | Security | 35 |
| 6.2 | Network Address Translation (NAT) | 35 |
| 6.3 | Redundancy and Load-balancing mechanism | 35 |
| 6.4 | Development orientation in future | 35 |
| 7 | Reference | 35 |
| 8 | Conclusion | 36 |



Members List

| No. | Full name | Student ID | Percentage of work |
|-----|----------------|------------|--------------------|
| 1 | Vương Khang | 2250008 | 100% |
| 2 | Võ Hoàng Long | 2053192 | 100% |
| 3 | Trần Đăng Khoa | 2252363 | 100% |

1 Suitable Network Structure

1.1 Network System Requirements

1.1.1 Main Site

At the Main Site of the Hospital, we have some requirements below:

- There are 2 buildings with 5 floors/building and 10 rooms/floor. Besides, there is a block including Data Center, IT, Central Cabling Local room located 50 meters from 2 buildings A and B.
- Medium-Scale: 600 workstations, 10 servers, 12 networking devices (maybe more with security-specific devices).
- Wireless network covers the whole site.
- Using new technologies for network infrastructure including wired and wireless connections, GPON, GigabitEthernet 1GbE/10GbE/40GbE. The network is organized according to the VLAN structure for different departments.
- Connect to 2 auxiliary sites through 2 leased-line for WAN connection.
- 2xDSL for Internet access with load balancing mechanism. All traffic to the Internet passes through the main site subnet.
- 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.

1.1.2 Auxiliary Site - Dien Bien Phu Street & Ba Huyen Thanh Quan Street

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

1.1.3 Data Flow and Work Load

The dataflow and workload reach the peak about 80% in the periods of time from 9AM to 11AM and from 3PM to 4 PM can be shared for 3 Sites as below:

- For software updates, web access, and database access,... The total download is about 1000 MB/day and the upload is estimated to be about 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.

1.1.4 Growing in the future

- 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).

1.2 Surveyed Checklist at installation locations

1.2.1 Main Site

At the main site of this hospital, we have a medium-scale 600 workstations so

- Each floor in 2 buildings A and B is installed with a layer 2 switch. Besides, there will be in average 60 workstations in each floor.
- There are 2 layer 3 switches for each building A, B and block IT for **Redundancy**. 5 layer 2 switches are connected to 2 layer 3 switches in each building and IT block.
- 1 Lightweight Access Point (LWAP) for each floor.

- 1 Wireless LAN Controller is connected to 1 of 2 layer 3 switches mentioned above for each building to control LWAPs in that building.
- 10 servers are placed inside the IT block.
- 6 layer 3 switches above are connected to 1 router. From this router, there are 2 leased-line to connect to 2 other sites and 1 line to connect to Firewall for security.
- 1 Firewall is used and connected to 1 more router. This router is then connected to 2 DSL modems and from that will be connected to Internet outside.
- **Note:** We use the term "IT" block representing for the area including IT, data center and Central Cabling Local.

1.2.2 2 auxiliary sites: Dien Bien Phu and Ba Huyen Thanh Quan Streets

At the auxiliary site of this hospital, we have a small-scale 60 workstations so

- First floor is used for IT area, we place all servers here.
- Second floor is equipped with 60 workstations.
- There are 2 layer 3 switches for **Redundancy**. 2 layer 2 switches on 2 floors are connected to these 2 layer 3 switches for **Redundancy**.
- 1 Lightweight Access Point (LWAP) for each floor.
- 1 Wireless LAN Controller is connected to 1 of 2 layer 3 switches mentioned above to control LWAPs.
- 2 layer 3 switches above are connected to 1 router. From this router, there are a leased-line connected to the main site.

1.3 High load area

In Computer Network, load balancing is a very important mechanism, which helps minimize the probability of overloaded or down network system. Connections between 2 auxiliary sites to the main site are the area with high load and this means we must consider load-balancing here. Also, DMZ with Web server and mail server will observe a high amount of connection. The reason is that the website of hospital is published to everyone, not only staff can access to this website but normal user inside LAN or in the Internet can access to it.

1.4 Network Structure

In this assignment, we design the hospital network based on a hierarchical network topology (extended star topology). An extended star network topology includes an additional networking device that is directly connected to the central networking device. It seems like a mesh of switches which are interconnected to the network and once central networking device which controls the network. There are 3 layers in a hierarchical network topology: Core Layer (Core Routers), Distribution Layer (Layer 3 Switches) and Access Layer (Layer 2 Switches and end devices). Hierarchical networks offer a wide range of benefits, such as enhanced performance, reliability, and scalability, better security, easier management and design, and improved cost-efficiency.

Also at distribution layer, we implement **Redundancy** as mentioned above. Redundancy is used to improve high availability and system robustness because in case 1 of 2 layer 3 switches has a problem, the system is not crashed and still works with the other layer 3 switch.

This assignment requires us to use 2 leased-line to connect from the main site to 2 auxiliary sites but we use in total 4 leased-line (2 for each connection to each auxiliary site) for load balancing. Dataflow at the router of main site will be high at peak hours so we have to ensure there will not be data congestion happening here between Sites. With these connections, we use Serial-DCE cables.

Access Control List (ACL) is applied on Layer 3 switches to prevent customer's devices (devices using Wireless connection) from communicating to host devices of hospital. Therefore, customer's devices like Laptops or phones using WiFi can communicate to every other devices in case they use WiFi also. They can not connect to Hospital's PCs.



Firewall ASA is installed at the main site to ensure the security for the system and ACL is also configured here to decide whether to accept or drop packets from Internet. This Firewall separates the system into 3 partitions: DMZ Zone, Outside and Inside. Actually, there is one more partition, which is ServerFarm (place important server here) but we place this zone inside the IT block and we consider it as INSIDE ZONE.

Connection from Hospital to Internet is transmitted over ADSL line provided by the ISP through 2 DSL modems.

2 List of minimum equipment, IP plan, and wiring diagram

2.1 Recommended equipment and typical specifications

2.1.1 Router CISCO PT-Empty



Figure 1: Router CISCO PT-Empty

- 10 Empty Slots to set-up modules based on what we want. In this assignment, we use ***PT-ROUTER-NM-1CGE*** and ***PT-ROUTER-NM-1SS***.
- **PT-ROUTER-NM-1CGE:** The single-port Cisco Gigabit Ethernet Network Module (part number PT-ROUTER-NM-1CGE) provides Gigabit Ethernet copper connectivity for access routers. The module is supported by the Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745 series routers. This network module has one gigabit interface converter (GBIC) slot to carry any standard copper or optical Cisco GBIC.
- **PT-ROUTER-NM-1SS:** The dual-serial port WAN interface cards (WICs) feature Cisco's new, compact, high-density Smart Serial connector to support a wide variety of electrical interfaces when used with the appropriate transition cable. Two cables are required to support the two ports on the WIC. Each port on a WIC is a different physical interface and can support different protocols such as Point-to-Point protocol (PPP) or Frame Relay and Data Terminal Equipment/Data Communications Equipment (DTE/DCE). This module is used for connection with Serial DCE cable between main site and 2 auxiliary sites.

2.1.2 Layer 2 Switch CISCO Catalyst 2960 WS-C2960-24TT-L



Figure 2: Layer 2 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.

Specifications

Specifications

| | |
|-------------------------------|---|
| 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 |
| Dimensions (H x W x D) | 4.4 x 44.5 x 23.6 cm |
| Weight | 3.6 kg |
| Rack Height | 1 RU |

Figure 3: CISCO Switch 2960

2.1.3 WS-C3650-24PS-L Catalyst 3650 Switch



Figure 4: WS-C3650-24PS-L Catalyst 3650 Switch

The Cisco® Catalyst® 3650 Series is the next generation of enterprise-class standalone and stackable access-layer switches that provide the foundation for full convergence between wired and wireless on a single platform. The 3650 Series is built on the advanced Cisco StackWise®-160, and takes advantage of the new Cisco Unified Access™ Data Plane (UADP) application-specific integrated circuit (ASIC). This switch can enable uniform wired-wireless policy enforcement, application visibility, flexibility, application optimization, and superior resiliency. The 3650 Series switches support full IEEE 802.3at Power over Ethernet Plus (PoE+), Cisco Universal Power over Ethernet (Cisco UPOE®) on the Cisco Catalyst 3650 Series multigigabit switches, and offer modular and field-replaceable redundant fans and power supplies. The 3650 Series switches also come in a 12-inch lower depth form factor so that you can deploy them in tight wiring closets in remote branches and offices where depth of the switch is a concern. In addition, the 3650 multigigabit switches support current and next-generation wireless speeds and standards (including 802.11ac Wave 2) on existing cabling infrastructure. The 3650 Series switches help increase wireless productivity and reduce TCO.

| | |
|---|--------------------------------------|
| Product Code | WS-C3650-24PS-L |
| Enclosure Type | Rack-mountable - 1U |
| Feature Set | LAN base |
| Uplink Interfaces | 4 x 1G SFP |
| Ports | 24 x 10/100/1000 PoE+ Ethernet ports |
| Available PoE Power | 390 W |
| Maximum stacking number | 9 |
| Stack bandwidth | 160 Gbps |
| Forwarding Bandwidth | 41.66Mpps |
| Switching Capacity | 88 Gbps |
| RAM | 4 G |
| Flash Memory | 2G |
| Number of AP per switch/stack | 50 |
| Number of wireless clients per switch/stack | 1000 |
| Dimensions | 4.4 cm x 44.5 cm x 44.8 cm |
| Package Weight | 17.49 Kg |

Figure 5: Layer 3 Switch 3650 Specification

2.1.4 Lightweight Access Point Cisco 3702I-C-K9



Figure 6: Lightweight Access Point

This Cisco Aironet 3702i Access Point is for indoor environments using internal antennas 802.11ac with 4x4 multiple-input multiple-output (MIMO) technology with three spatial streams, offering sustained 1.3-Gbps rates over a greater range for more capacity and reliability than competing access points.

- Software**
- Cisco Unified Wireless Network Software Release 7.6 or later
- Supported wireless LAN controllers**
- Cisco 2500 Series Wireless Controllers, Cisco Wireless Controller Module for ISR G2, Cisco Wireless services Module 2 (WISM2) for Catalyst 6500 Series Switches, Cisco 5500 Series Wireless controllers, Cisco Flex 7500 Series Wireless Controllers, Cisco 8500 Series Wireless Controllers, Cisco Virtual Wireless Controller
 - Cisco 5760 Wireless LAN Controller, Cisco Catalyst 3850 Series Switches
- 802.11n version 2.0 (and related) capabilities**
- 4x4 MIMO with three spatial streams
 - Maximal ratio combining (MRC)
 - 802.11n and 802.11a/g beamforming
 - 20- and 40-MHz channels
 - PHY data rates up to 450 Mbps (40 MHz with 5 GHz)
 - Packet aggregation: A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)
 - 802.11 dynamic frequency selection (DFS)
 - Cyclic shift diversity (CSD) support
- 802.11ac Wave 1 capabilities**
- 4x4 MIMO with three spatial streams
 - MRC
 - 802.11ac beamforming
 - 20-, 40-, and 80-MHz channels
 - PHY data rates up to 1.3 Gbps (80 MHz with 5 GHz)
 - Packet aggregation: A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)
 - 802.11 DFS
 - CSD support

Figure 7: Lightweight Access Point Specification

Cisco ASA 5500-X Next Generation, ASA 5506-X, 8*GE ports, 1GE Mgmt, AC, 3DES/AES, AVC, FirePower, FireSIGHT, unlimited user nodes.

| | |
|--|---|
| Product Code | ASA5506-K9 |
| Interface | 8 x 1 Gigabit Ethernet interface, 1 management port |
| Stateful inspection throughput (multiprotocol) | 300 Mbps |
| Maximum 3DES/AES VPN throughput | 100 Mbps |
| IPsec site-to-site VPN peers | 10; 50 with Security Plus license |
| VLAN Interfaces | 5; 30 with Security Plus license |
| Memory | 4GB |
| Flash | 8GB |
| Power (AC or DC) | AC only |
| Height (rack units) | Desk Top |
| Size (D x H x W) | 9.23 in x 1.72 in x 7.871 in |
| Weight | 3.78 Kg |

Figure 9: Firewall ASA 5506-X Specification

2.1.5 FIREWALL CISCO ASA 5506-X



Figure 8: Firewall ASA 5506-X

2.1.6 Cisco 3504 Wireless Controller



Figure 10: Wireless LAN Controller

The Cisco 3504 Wireless Controller provides centralized control, management, and troubleshooting for small to medium-sized enterprises and branch offices. It offers flexibility to support multiple deployment modes in the same controller—a centralized mode for campus environments, Cisco FlexConnect® mode for lean branches managed over the WAN, and a mesh (bridge) mode for deployments in which full Ethernet cabling is unavailable. As a component of the Cisco Unified Wireless Network, the 3504 controller provides real-time communications between Cisco Aironet® access points and Cisco Catalyst® access points, Cisco Prime® Infrastructure, and the Cisco Mobility Services Engine, and is interoperable with the Cisco 5520 and 8540 Wireless Controllers.

The Cisco Digital Network Architecture (Cisco DNA) is an open and extensible, software-driven architecture that accelerates and simplifies your enterprise network operations. The programmable architecture frees your IT staff from time-consuming, repetitive network configuration tasks so they can focus instead on innovation that positively transforms your business. SD-Access, as part of Cisco DNA, enables policy-based automation from edge to cloud with foundational capabilities. Cisco DNA Assurance, also part of Cisco DNA, provides a single source to monitor, modify, and manage your network and application data.

2.2 IP Planning

If you notice, you will see that we use /24 for the IP addresses. This means, the IP address of each VLAN will run from x.x.x.0 to x.x.x.255 (256 IP addresses). However, the first IP address (x.x.x.0) is used as the network address, the second one (x.x.x.1) is used as the default gateway and the last one (x.x.x.254) is used as the broadcast address. Therefore, we will have valid IP addresses for devices from x.x.x.2 to x.x.x.253. Actually, each floor will have below 100 devices so it seems to be redundant here in IP addresses for each floor (each VLAN) but if we consider the growth of the whole system in the future, this will help and it also makes IP addressing easier.

Moreover, in fact the valid IP addresses of devices run from x.x.x.2 to x.x.x.253 but we configured on the DHCP server that it will assign dynamically IP addresses for PCs from x.x.x.10 while for Wireless Connection from x.x.x.20. This is to have empty slots for future use. Until now, we have not known which one will be used at these empty slots but maybe in the future it will help and we have redundant IP addresses so why don't we let some empty slots at the beginning?

2.2.1 Main Site

1. Building A

| BUILDING A IP PLAN | | | | | | |
|--------------------|----------------|-----------------------|----------------------------------|-----------------|-------------------|----------------|
| VLAN Number | Name | Network & Subnet Mask | Valid IP Address Range | Default Gateway | Broadcast Address | WLC Address |
| 10 | Floor1A | 192.168.1.0/24 | 192.168.1.2 to 192.168.1.253 | 192.168.1.1 | 192.168.1.254 | None |
| 20 | Floor2A | 192.168.2.0/24 | 192.168.2.2 to 192.168.2.253 | 192.168.2.1 | 192.168.2.254 | None |
| 30 | Floor3A | 192.168.3.0/24 | 192.168.3.2 to 192.168.3.253 | 192.168.3.1 | 192.168.3.254 | None |
| 40 | Floor4A | 192.168.4.0/24 | 192.168.4.2 to 192.168.4.253 | 192.168.4.1 | 192.168.4.254 | None |
| 50 | Floor5A | 192.168.5.0/24 | 192.168.5.2 to 192.168.5.253 | 192.168.5.1 | 192.168.5.254 | None |
| 100 | WLANA | 192.168.100.0/24 | 192.168.100.2 to 192.168.100.253 | 192.168.100.1 | 192.168.100.254 | 192.168.100.15 |
| 200 | SecurityCamera | 192.168.200.0/24 | 192.168.200.2 to 192.168.200.253 | 192.168.200.1 | 192.168.200.254 | None |

Figure 11: Building A IP Addressing

2. Building B

| BUILDING B IP PLAN | | | | | | |
|--------------------|----------------|-----------------------|----------------------------------|-----------------|-------------------|----------------|
| VLAN Number | Name | Network & Subnet Mask | Valid IP Address Range | Default Gateway | Broadcast Address | WLC Address |
| 10 | Floor1B | 192.168.6.0/24 | 192.168.6.2 to 192.168.6.253 | 192.168.6.1 | 192.168.6.254 | None |
| 20 | Floor2B | 192.168.7.0/24 | 192.168.7.2 to 192.168.7.253 | 192.168.7.1 | 192.168.7.254 | None |
| 30 | Floor3B | 192.168.8.0/24 | 192.168.8.2 to 192.168.8.253 | 192.168.8.1 | 192.168.8.254 | None |
| 40 | Floor4B | 192.168.9.0/24 | 192.168.9.2 to 192.168.9.253 | 192.168.9.1 | 192.168.9.254 | None |
| 50 | Floor5B | 192.168.10.0/24 | 192.168.10.2 to 192.168.10.253 | 192.168.10.1 | 192.168.10.254 | None |
| 100 | WLANB | 192.168.101.0/24 | 192.168.101.2 to 192.168.101.253 | 192.168.101.1 | 192.168.101.254 | 192.168.101.15 |
| 200 | SecurityCamera | 192.168.201.0/24 | 192.168.201.2 to 192.168.201.253 | 192.168.201.1 | 192.168.201.254 | None |

Figure 12: Building B IP Addressing

3. IT Block

| IT IP PLAN | | | | | | |
|-------------|----------------|-----------------------|----------------------------------|-----------------|-------------------|----------------|
| VLAN Number | Name | Network & Subnet Mask | Valid IP Address Range | Default Gateway | Broadcast Address | WLC Address |
| 10 | Server | 192.168.12.0/24 | 192.168.12.2 to 192.168.12.253 | 192.168.12.1 | 192.168.12.254 | None |
| 20 | IT | 192.168.11.0/24 | 192.168.11.2 to 192.168.11.253 | 192.168.11.1 | 192.168.11.254 | None |
| 100 | WLAN | 192.168.102.0/24 | 192.168.102.2 to 192.168.102.253 | 192.168.102.1 | 192.168.102.254 | 192.168.102.15 |
| 200 | SecurityCamera | 192.168.202.0/24 | 192.168.202.2 to 192.168.202.253 | 192.168.202.1 | 192.168.202.254 | None |

Figure 13: IT Block IP Addressing

2.2.2 Auxiliary Site - Dien Bien Phu Street

| DBP IP PLAN | | | | | | |
|-------------|----------------|-----------------------|----------------------------------|-----------------|-------------------|----------------|
| VLAN Number | Name | Network & Subnet Mask | Valid IP Address Range | Default Gateway | Broadcast Address | WLC Address |
| 10 | Server | 192.168.15.0/24 | 192.168.15.2 to 192.168.15.253 | 192.168.15.1 | 192.168.15.254 | None |
| 20 | Room | 192.168.14.0/24 | 192.168.14.2 to 192.168.14.253 | 192.168.14.1 | 192.168.14.254 | None |
| 100 | WLAN | 192.168.102.0/24 | 192.168.102.2 to 192.168.102.253 | 192.168.102.1 | 192.168.102.254 | 192.168.102.15 |
| 200 | SecurityCamera | 192.168.203.0/24 | 192.168.203.2 to 192.168.203.253 | 192.168.203.1 | 192.168.203.254 | None |

Figure 14: Dien Bien Phu Site IP Addressing

2.2.3 Auxiliary Site - Ba Huyen Thanh Quan Street

| BHTQ IP PLAN | | | | | | |
|--------------|----------------|-----------------------|----------------------------------|-----------------|-------------------|----------------|
| VLAN Number | Name | Network & Subnet Mask | Valid IP Address Range | Default Gateway | Broadcast Address | WLC Address |
| 10 | Server | 192.168.17.0/24 | 192.168.17.2 to 192.168.17.253 | 192.168.17.1 | 192.168.17.254 | None |
| 20 | Room | 192.168.16.0/24 | 192.168.16.2 to 192.168.16.253 | 192.168.16.1 | 192.168.16.254 | None |
| 100 | WLAN | 192.168.103.0/24 | 192.168.103.2 to 192.168.103.253 | 192.168.103.1 | 192.168.103.254 | 192.168.103.15 |
| 200 | SecurityCamera | 192.168.204.0/24 | 192.168.204.2 to 192.168.204.253 | 192.168.204.1 | 192.168.204.254 | None |

Figure 15: Ba Huyen Thanh Quan Site IP Addressing

2.3 Schematic Physical Setup

2.3.1 Wiring Diagram Main Site

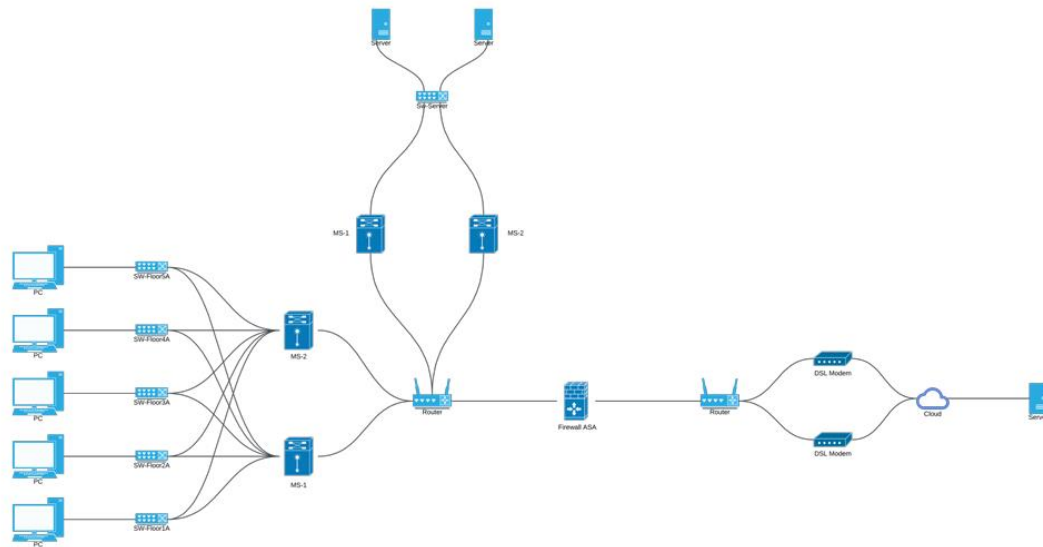


Figure 16: Wiring Diagram for Main Site

About wiring with building B, it's similar to building A so we did not draw it on this diagram to make it easy to observe and understand. Also, we do not draw Lightweight Access Point and Wireless LAN Controller here to make the diagram simple.

2.3.2 Wiring Diagram Auxiliary Sites

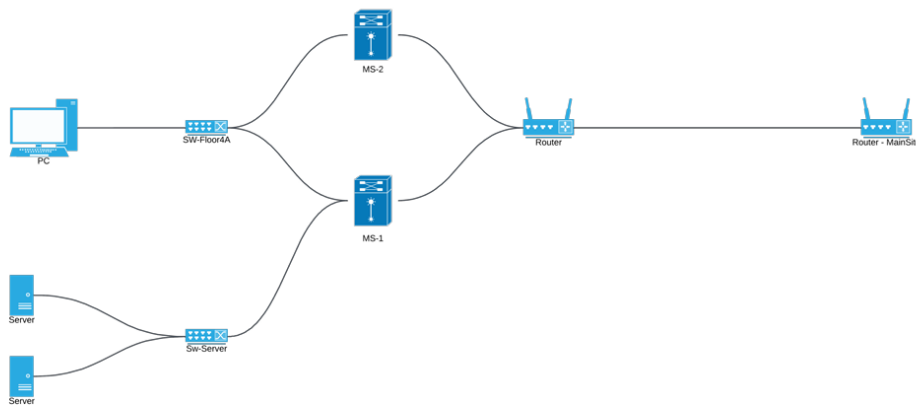


Figure 17: Wiring Diagram Auxiliary Sites

Because 2 auxiliary sites are similar to each other so here we only draw one time.

2.3.3 SD-WAN



Figure 18: SD-WAN diagram

3 Calculate Throughput and Bandwidth and hospital network configuration suggestion

The dataflow and workload reach the peak at 80% at 2 periods of time 9AM-11AM and 3PM-4PM. The total amount of peak time is 3 hours.

- 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. Therefore, the total upload and download is $2000 + 1000 = 3000$ 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. Therefore, the total upload and download is $500 + 100 = 600$ MB/day.
- WiFi-connected devices from customers' access for downloading are about 500 MB/day.

3.0.1 Main Site

- Throughput for server can be calculated: $Throughput_{servers} = \frac{3000 \times 10}{24 \times 3600} = \frac{25}{72}$ (MB/s) = $\frac{25}{9}$ (Mb/s) ≈ 2.78 (Mb/s).
- Throughput for workstations can be calculated: $Throughput_{workstations} = \frac{600 \times 600}{24 \times 3600} = \frac{25}{6}$ (MB/s) = $\frac{100}{3}$ (Mb/s) ≈ 33.33 (Mb/s).
- Throughput for server can be calculated: $Throughput_{WiFi} = \frac{500}{24 \times 3600} = \frac{5}{864}$ (MB/s) = $\frac{5}{108}$ (Mb/s) ≈ 0.05 (Mb/s).
- Based on 3 hours of peak time, we have throughput reaching 80% so the bandwidth here can be calculated: $Bandwidth_{servers} = \frac{10 \times 3000 \times 0.8}{3 \times 3600} = \frac{20}{9}$ (MB/s) = $\frac{160}{9}$ (Mb/s) ≈ 17.78 (Mb/s).
- Based on 3 hours of peak time, we have throughput reaching 80% so the bandwidth here can be calculated: $Bandwidth_{workstations} = \frac{600 \times 600 \times 0.8}{3 \times 3600} = \frac{80}{3}$ (MB/s) = $\frac{640}{3}$ (Mb/s) ≈ 213.33 (Mb/s).
- Based on 3 hours of peak time, we have throughput reaching 80% so the bandwidth here can be calculated: $Bandwidth_{WiFi} = \frac{500 \times 0.8}{3 \times 3600} = \frac{1}{27}$ (MB/s) = $\frac{8}{27}$ (Mb/s) ≈ 0.3 (Mb/s).
- Total Throughput: $Throughput_{total} = 2.78 + 33.33 + 0.05 = 36.16$ (Mb/s).
- Total Bandwidth: $Bandwidth_{total} = 17.78 + 213.33 + 0.3 = 231.41$ (Mb/s).

3.0.2 Two Auxiliary Sites

- Throughput for server can be calculated: $Throughput_{servers} = \frac{3000 \times 2}{24 \times 3600} = \frac{5}{72}$ (MB/s) = $\frac{5}{9}$ (Mb/s) ≈ 0.56 (Mb/s).
- Throughput for workstations can be calculated: $Throughput_{workstations} = \frac{60 \times 600}{24 \times 3600} = \frac{5}{12}$ (MB/s) = $\frac{10}{3}$ (Mb/s) ≈ 3.33 (Mb/s).
- Throughput for server can be calculated: $Throughput_{WiFi} = \frac{500}{24 \times 3600} = \frac{5}{864}$ (MB/s) = $\frac{5}{108}$ (Mb/s) ≈ 0.05 (Mb/s).

- Based on 3 hours of peak time, we have throughput reaching 80% so the bandwidth here can be calculated:
 $Bandwidth_{servers} = \frac{2 \times 3000 \times 0.8}{3 \times 3600} = \frac{4}{9} \text{ (MB/s)} = \frac{32}{9} \text{ (Mb/s)} \approx 3.56 \text{ (Mb/s)}.$
- Based on 3 hours of peak time, we have throughput reaching 80% so the bandwidth here can be calculated:
 $Bandwidth_{workstations} = \frac{60 \times 600 \times 0.8}{3 \times 3600} = \frac{8}{3} \text{ (MB/s)} = \frac{64}{3} \text{ (Mb/s)} \approx 21.33 \text{ (Mb/s)}.$
- Based on 3 hours of peak time, we have throughput reaching 80% so the bandwidth here can be calculated:
 $Bandwidth_{WiFi} = \frac{500 \times 0.8}{3 \times 3600} = \frac{1}{27} \text{ (MB/s)} = \frac{8}{27} \text{ (Mb/s)} \approx 0.3 \text{ (Mb/s)}.$
- Total Throughput: $Throughput_{total} = 0.56 + 3.33 + 0.05 = 3.94 \text{ (Mb/s)}.$
- Total Bandwidth: $Bandwidth_{total} = 3.56 + 21.33 + 0.3 = 25.19 \text{ (Mb/s)}.$

4 Design the network map using Packet Tracer

4.0.1 The whole system

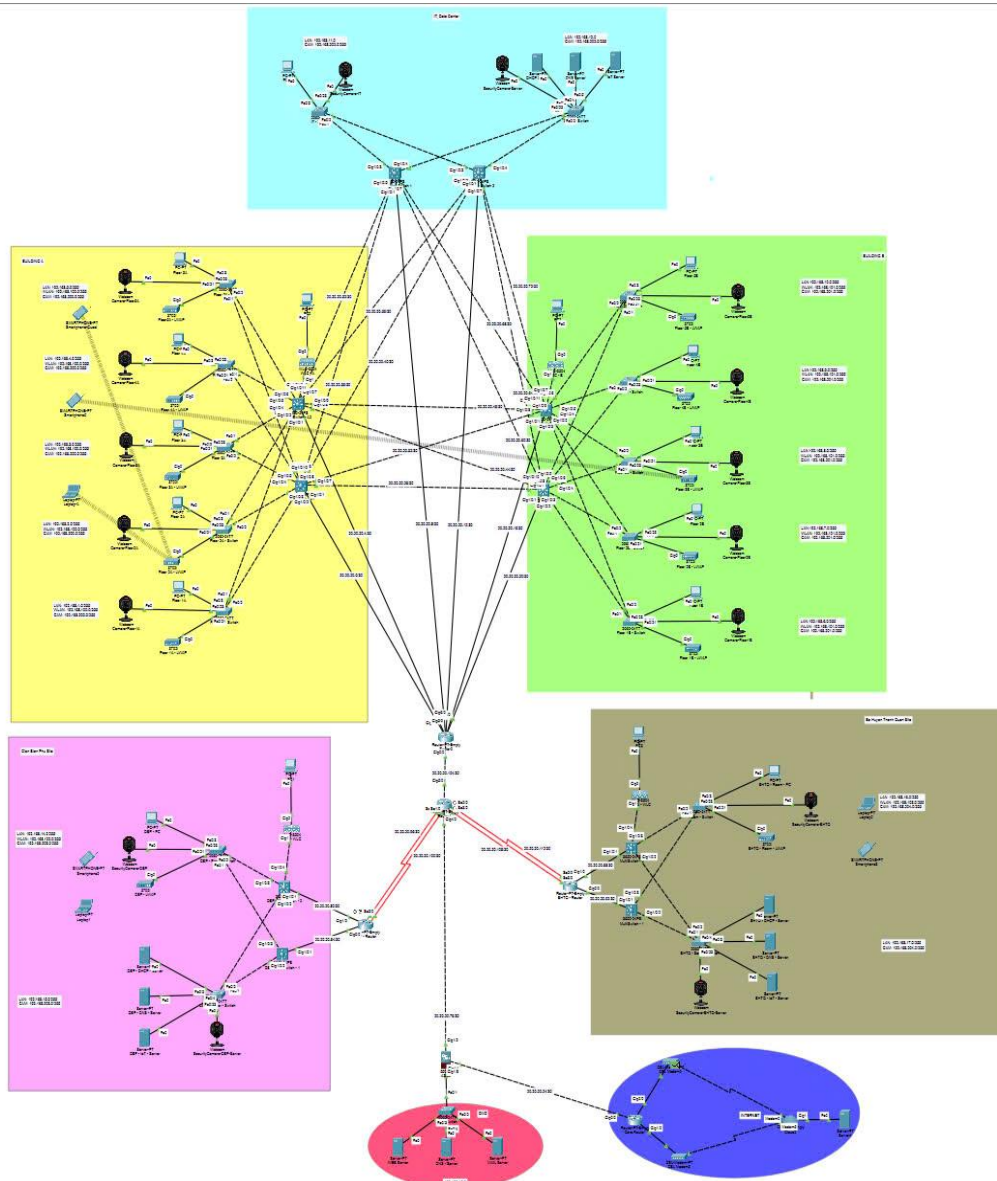


Figure 19: The whole system design in Cisco Packet Tracer

- 3 areas, which lie on top of the topology (yellow, light blue and light green), belong to Main Site with yellow is BUILDING A, light blue is BUILDING B and light green is IT.
- The light pink area is Dien Bien Phu Site while the brown one is Ba Huyen Thanh Quan Site.
- The red area is the DMZ area and the dark blue area is INTERNET area.
- EIGRP is utilized as the routing protocol for the whole system. We do not implement OSPF here.
- Connection among Sites is based on SD-WAN with leased-line using Serial DCE cable.

4.0.2 BUILDING A

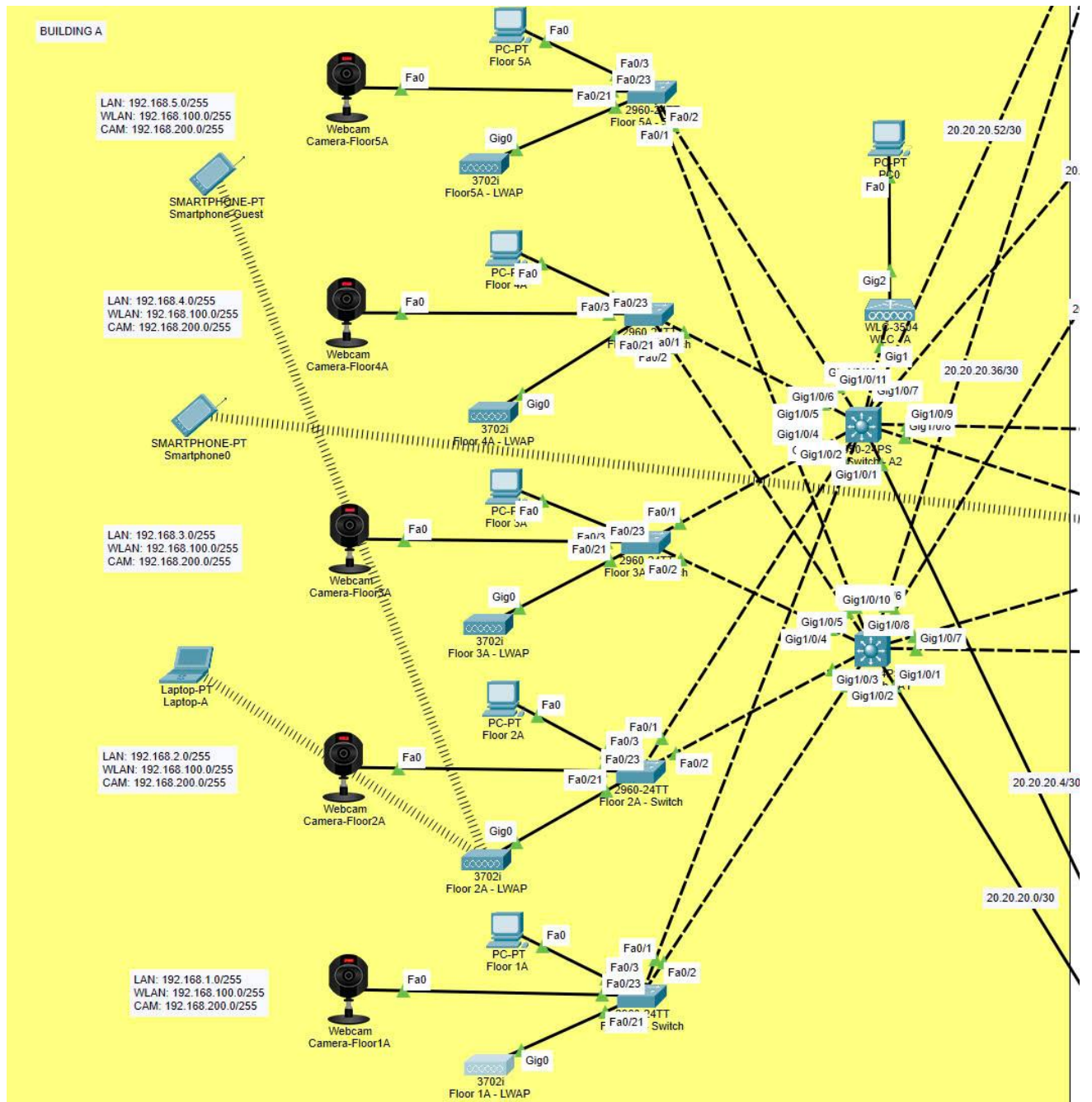


Figure 20: Building A

4.0.3 BUILDING B

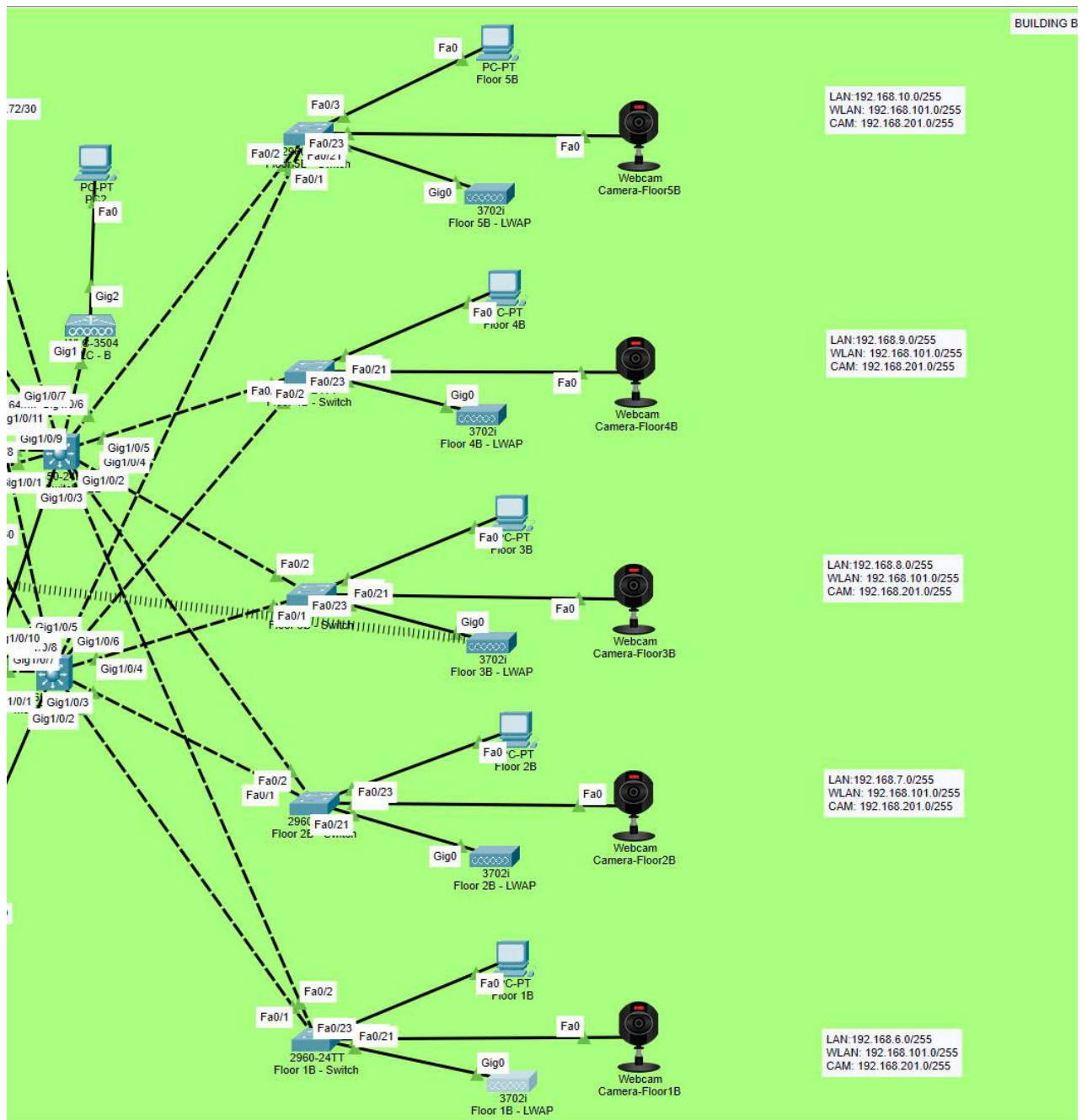


Figure 21: Building B

4.0.4 IT

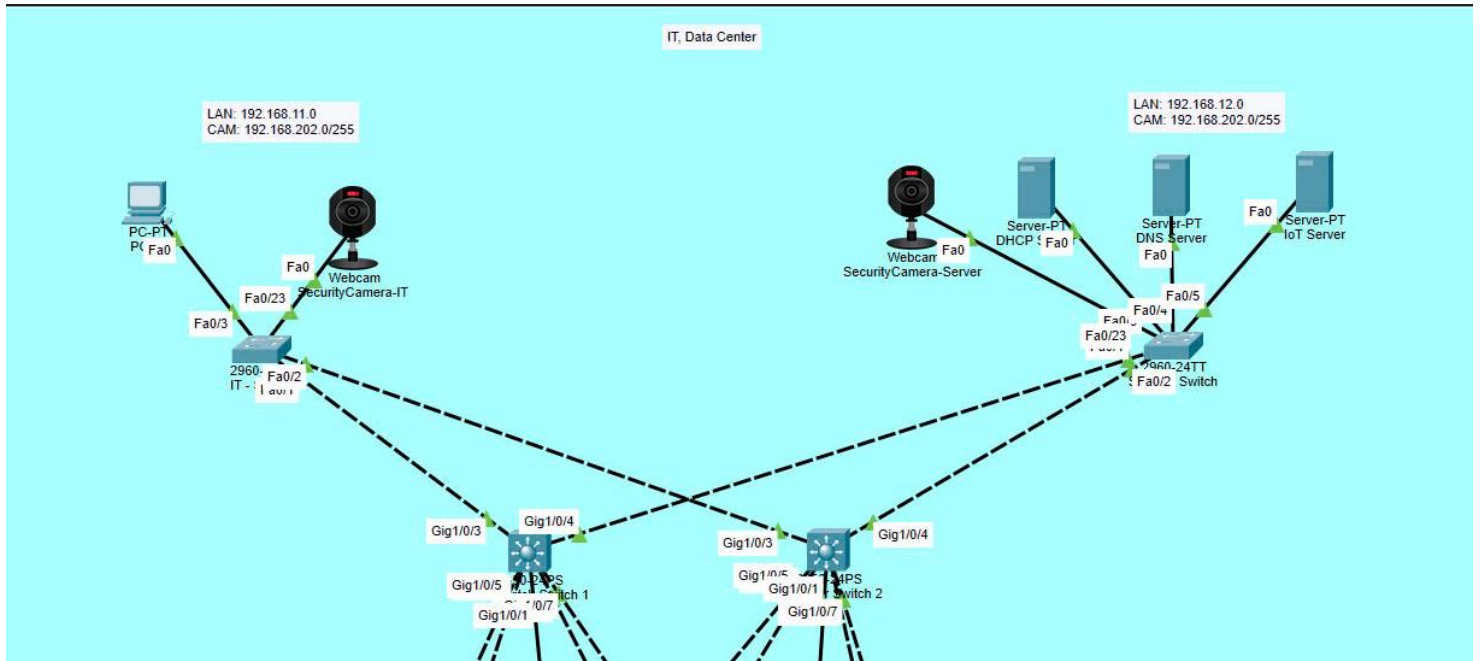


Figure 22: IT

4.0.5 Dien Bien Phu Site

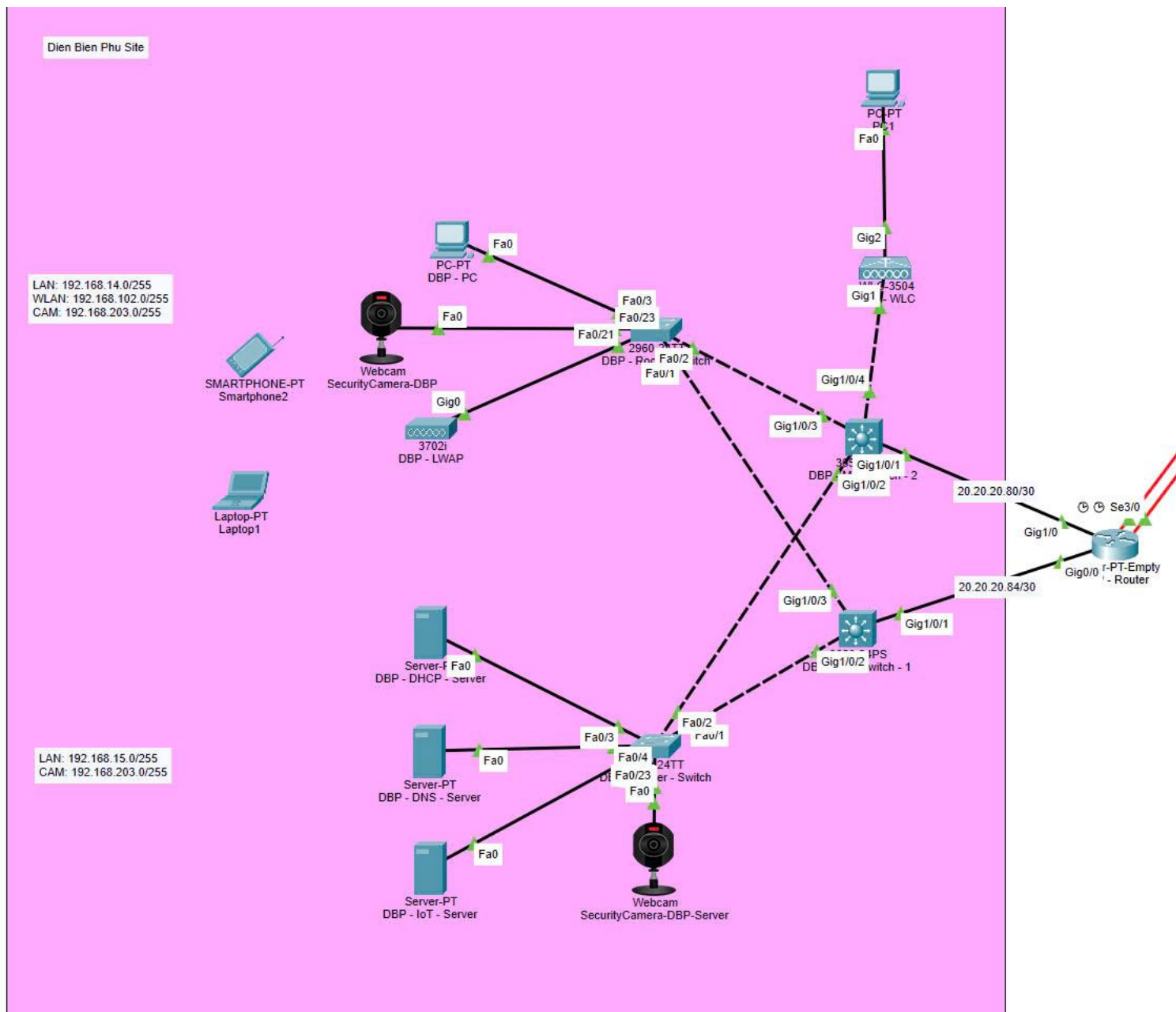


Figure 23: Dien Bien Phu Site

4.0.7 DMZ

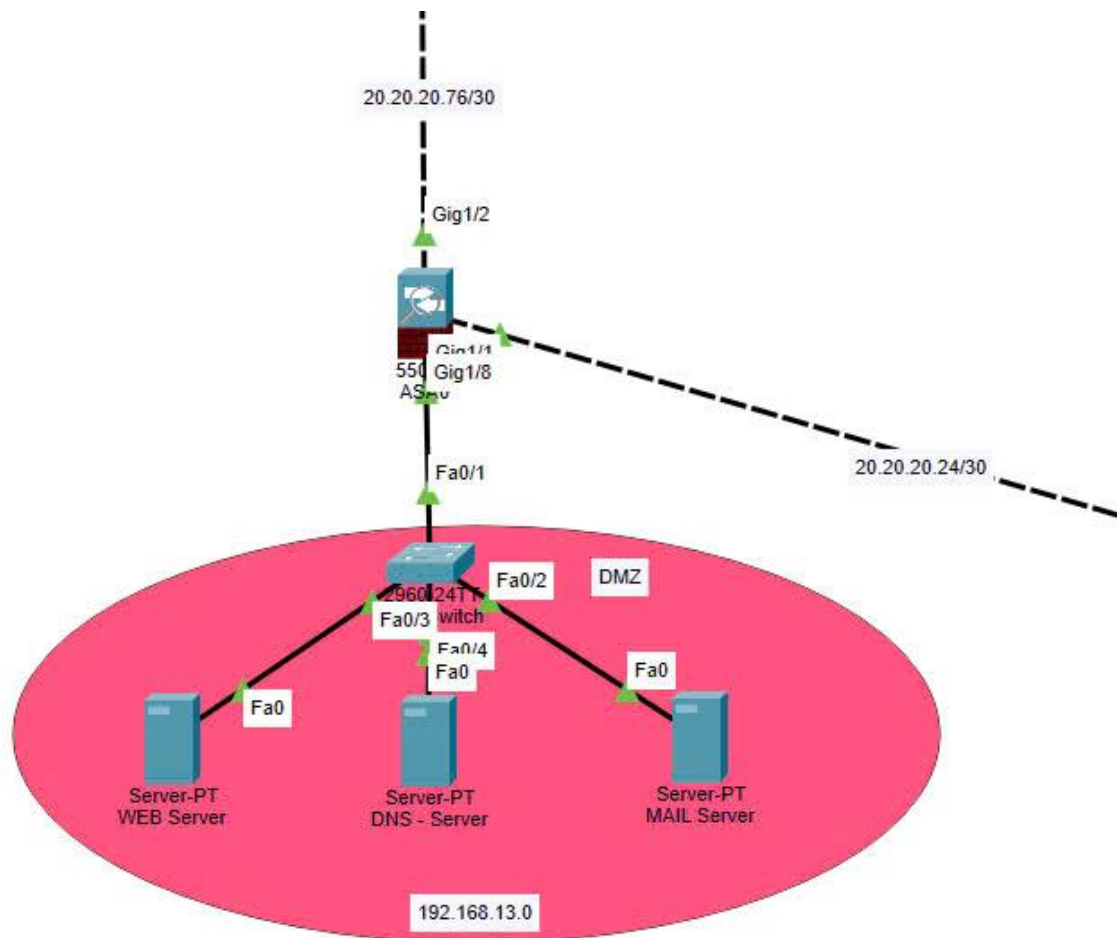


Figure 25: DMZ

4.0.8 Internet

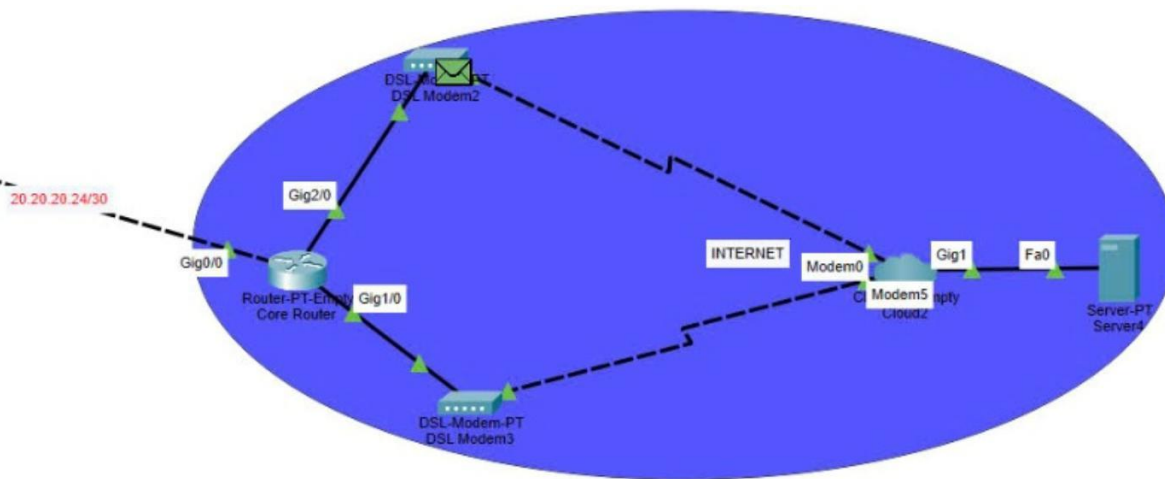


Figure 26: Internet

5 Test the system with popular tools such as ping, traceroute, etc. on the simulated system

5.0.1 Dynamic IP address on devices with DHCP server

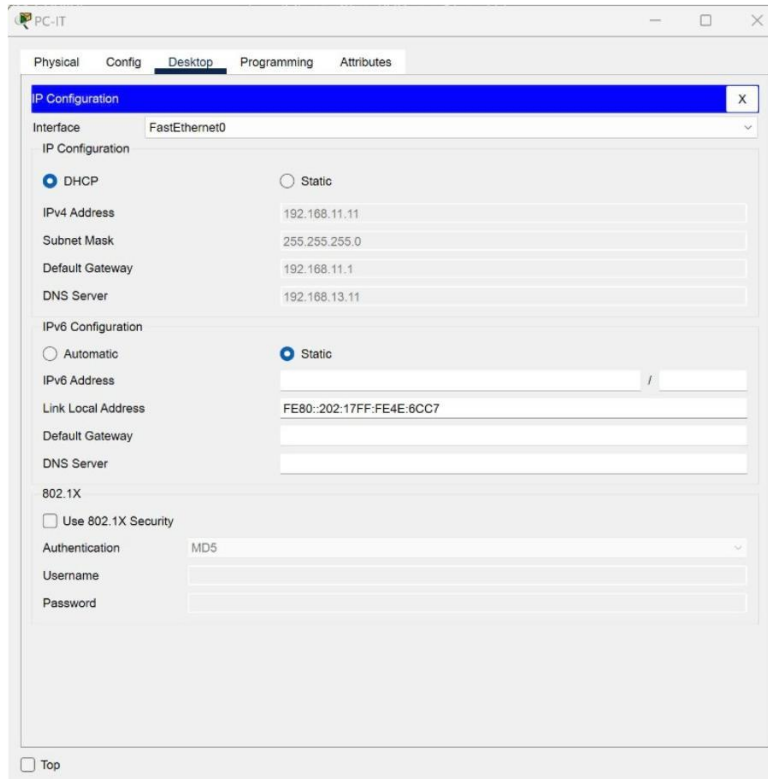


Figure 27: Dynamic IP Address from DHCP Server

As you can see, the IP address is dynamically assigned to devices with the help of DHCP server.

5.0.2 Ping PC in the same VLAN

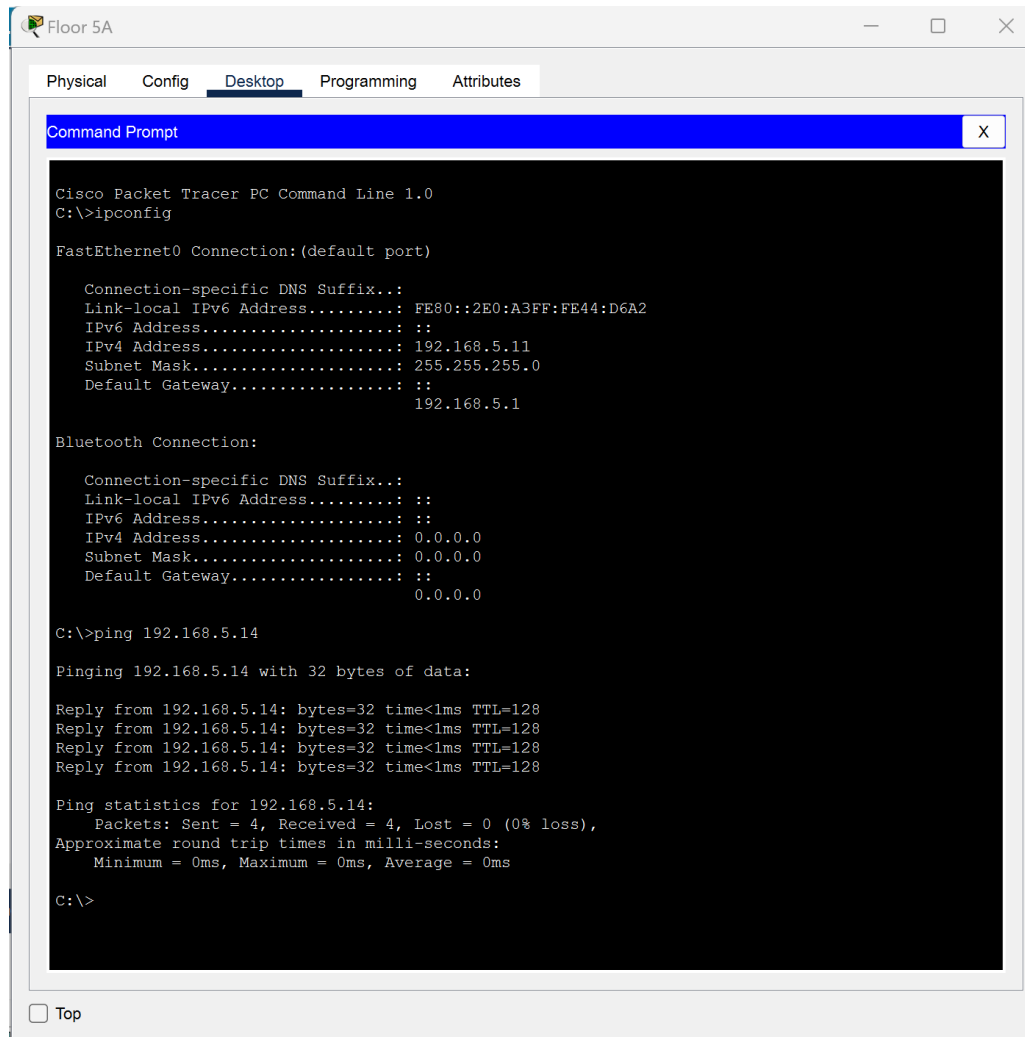
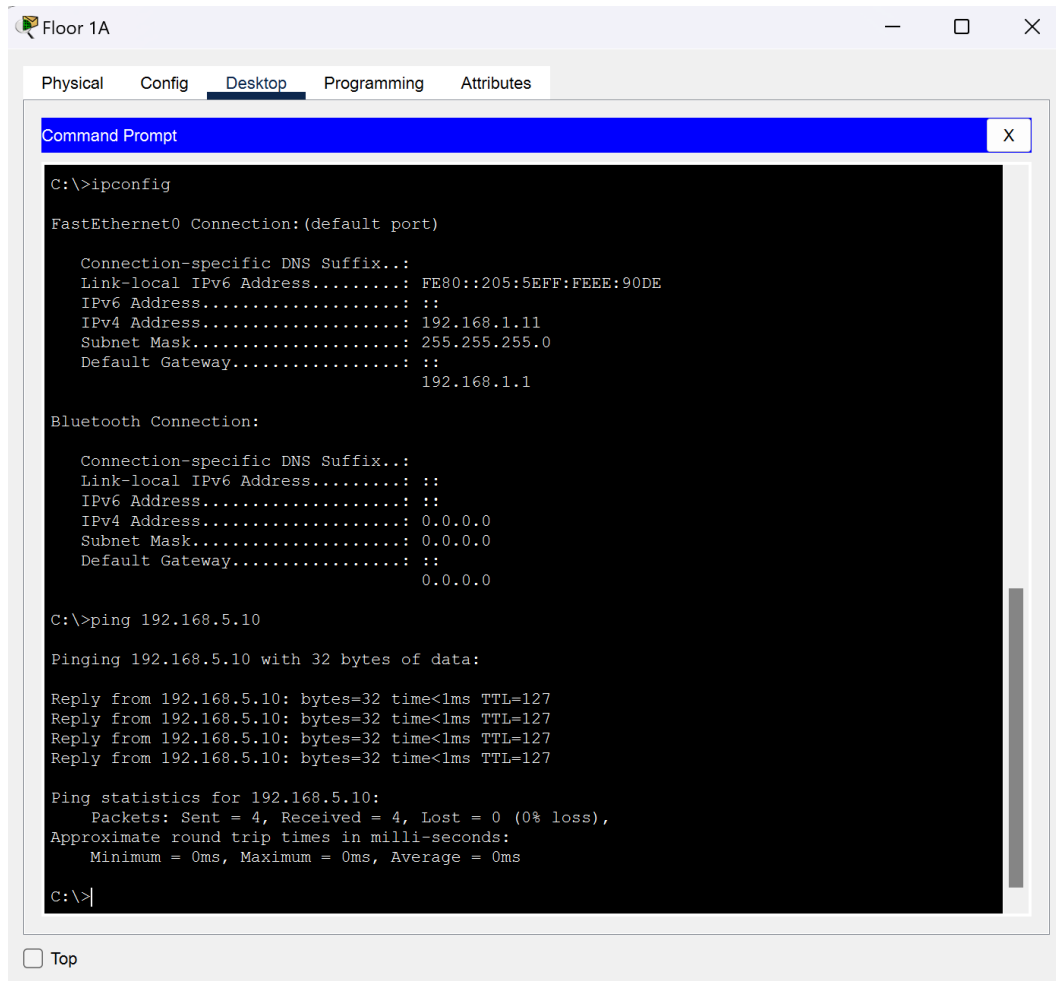


Figure 28: Ping PC in the same VLAN

We use "ping <IP address>" command line to ping devices in the same VLAN. Here, we consider the VLAN of Wireless connected devices (WiFi) in building A. All these devices belong to VLAN 100 with network address 192.168.100.0/24. As you can see, we ping from a PC having IP address 192.168.5.11 to a PC having IP address 192.168.5.14.

5.0.3 Ping devices in different VLANs



```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::205:5EFF:FEEE:90DE
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.11
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                   192.168.1.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                   0.0.0.0

C:\>ping 192.168.5.10

Pinging 192.168.5.10 with 32 bytes of data:

Reply from 192.168.5.10: bytes=32 time<1ms TTL=127
Reply from 192.168.5.10: bytes=32 time<1ms TTL=127
Reply from 192.168.5.10: bytes=32 time<1ms TTL=127
Reply from 192.168.5.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.5.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figure 29: Ping devices in different VLANs

- In this test, we ping 2 PCs on floor 5 and 1 of BUILDING A, which belong to different VLANs (VLAN 50 and VLAN 10). Corresponding IP addresses are 192.168.5.10 and 192.168.1.11.
- **Note:** We did not use ping from the Laptop mentioned on the first test above to PCs although they are in different VLAN too. The test below will show you the reason.

5.0.4 Ping from Customers' device to PCs on the LAN

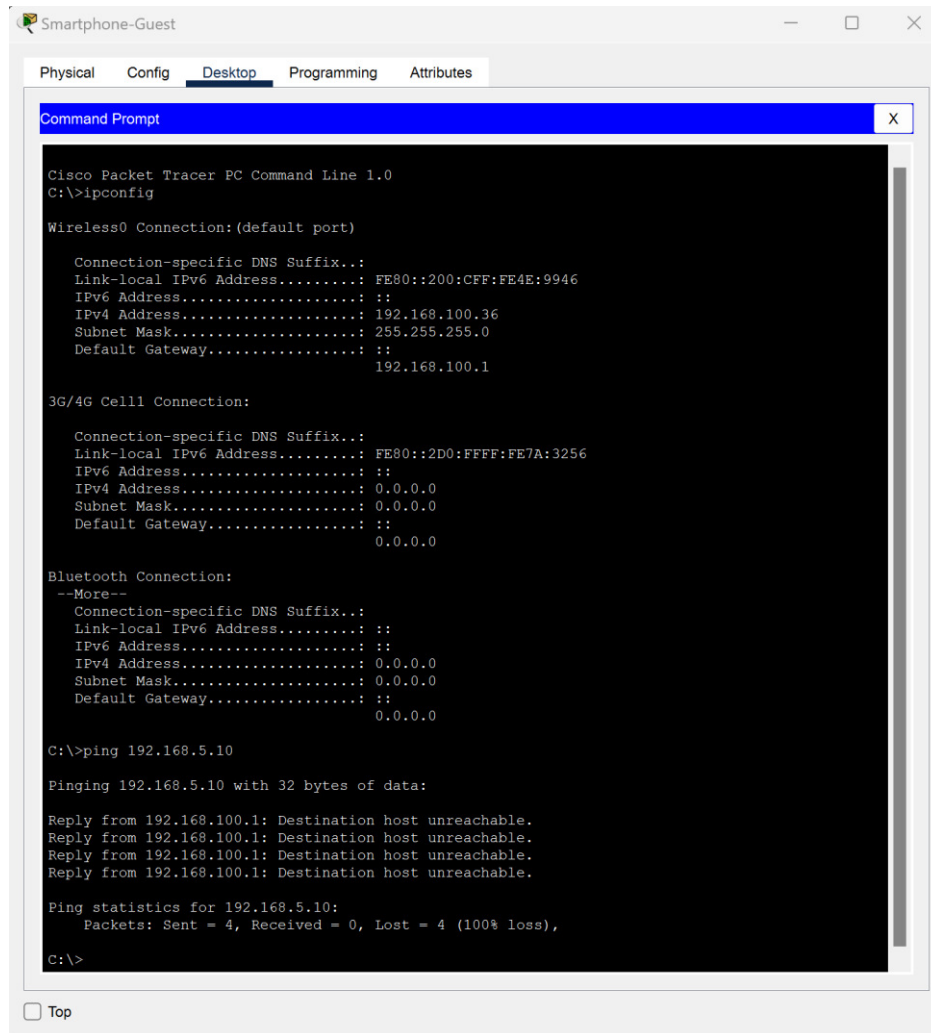
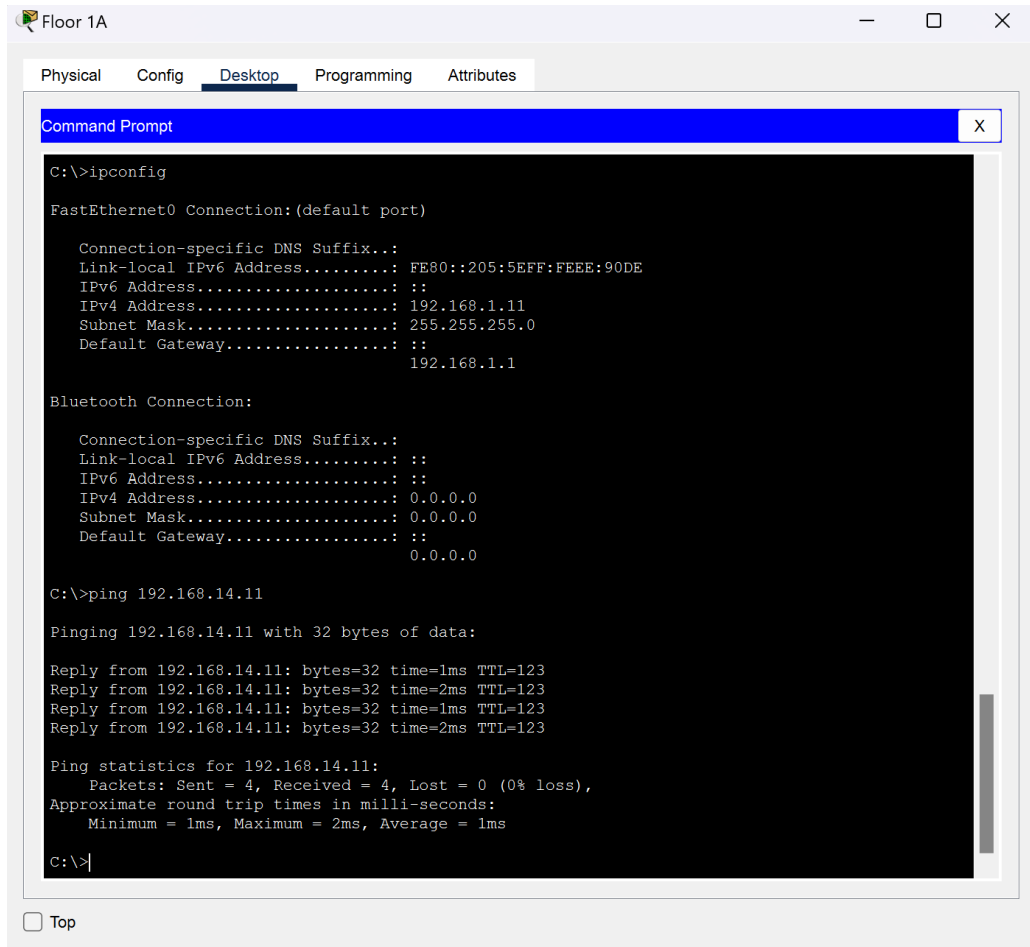


Figure 30: No access from Customers' device to PCs on the LAN

As you can see, when we ping from the laptop with Wireless connection (WiFi) to the PCs in the LAN of the system (IP addresses: 192.168.100.36 and 192.168.5.10 respectively), we have the result "**Destination host unreachable**". This is because we created an Access Control List (ACL) on the layer 3 switch 3650 to deny any messages sent from Wireless network to the PCs on the LAN.

5.0.5 Ping from PC on Main Site to PC on DBP Site



```
Floor 1A
Physical  Config  Desktop  Programming  Attributes

Command Prompt

C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address.....: FE80::205:5EFF:FEEE:90DE
    IPv6 Address.....: ::
    IPv4 Address.....: 192.168.1.11
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: ::
                        192.168.1.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address.....: ::
    IPv6 Address.....: ::
    IPv4 Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: ::
                        0.0.0.0

C:\>ping 192.168.14.11

Pinging 192.168.14.11 with 32 bytes of data:

Reply from 192.168.14.11: bytes=32 time=1ms TTL=123
Reply from 192.168.14.11: bytes=32 time=2ms TTL=123
Reply from 192.168.14.11: bytes=32 time=1ms TTL=123
Reply from 192.168.14.11: bytes=32 time=2ms TTL=123

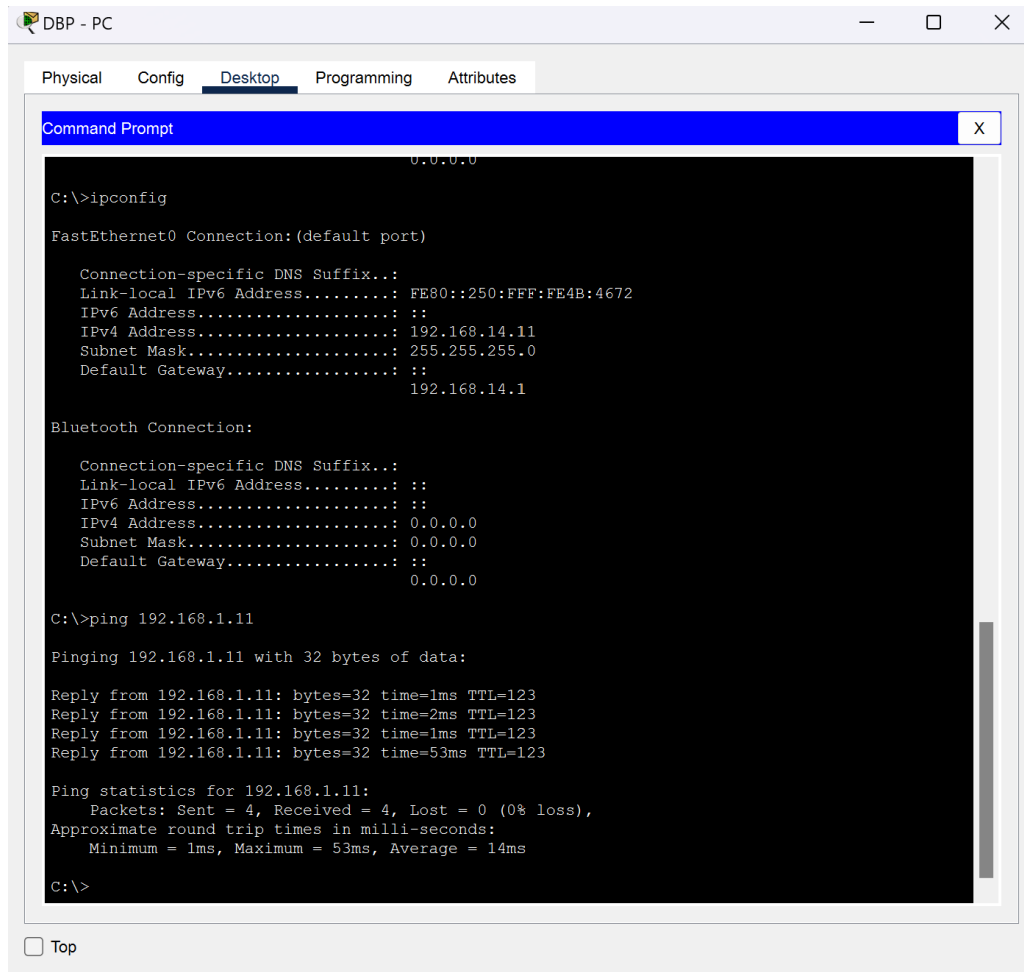
Ping statistics for 192.168.14.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

Figure 31: Ping from Main Site to Dien Bien Phu Site

Ping from Main Site to Ba Huyen Thanh Quan Site is similar to ping from Main Site to Dien Bien Phu Site so we only show one of them here. The PC on Dien Bien Phu Site is assigned dynamically IP Address by DHCP server also (192.168.14.11) and we can ping from PC at floor 1 of Building A to this IP address as you can see.

5.0.6 Ping from PC on DBP Site to PC on Main Site



The screenshot shows a window titled "DBP - PC" with tabs for Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is active, displaying a Command Prompt window. The Command Prompt shows the output of the `ipconfig` command, displaying details for the FastEthernet0 and Bluetooth connections. It then shows the output of the `ping 192.168.1.11` command, indicating successful connectivity with 0% loss and an average round trip time of 14ms.

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...: 
    Link-local IPv6 Address . . . . .: FE80::250:FFF:FE4B:4672
    IPv6 Address . . . . .: ::
    IPv4 Address. . . . .: 192.168.14.11
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                   192.168.14.1

Bluetooth Connection:

    Connection-specific DNS Suffix...: 
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address. . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                   0.0.0.0

C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time=1ms TTL=123
Reply from 192.168.1.11: bytes=32 time=2ms TTL=123
Reply from 192.168.1.11: bytes=32 time=1ms TTL=123
Reply from 192.168.1.11: bytes=32 time=53ms TTL=123

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 53ms, Average = 14ms

C:\>
```

Figure 32: Ping from Dien Bien Phu Site to Main Site

Ping from Ba Huyen Thanh Quan Site to Main Site is similar to ping from Dien Bien Phu Site to Main Site so we only show 1 of them here.

5.0.7 Access to Web Server of Hospital located inside DMZ

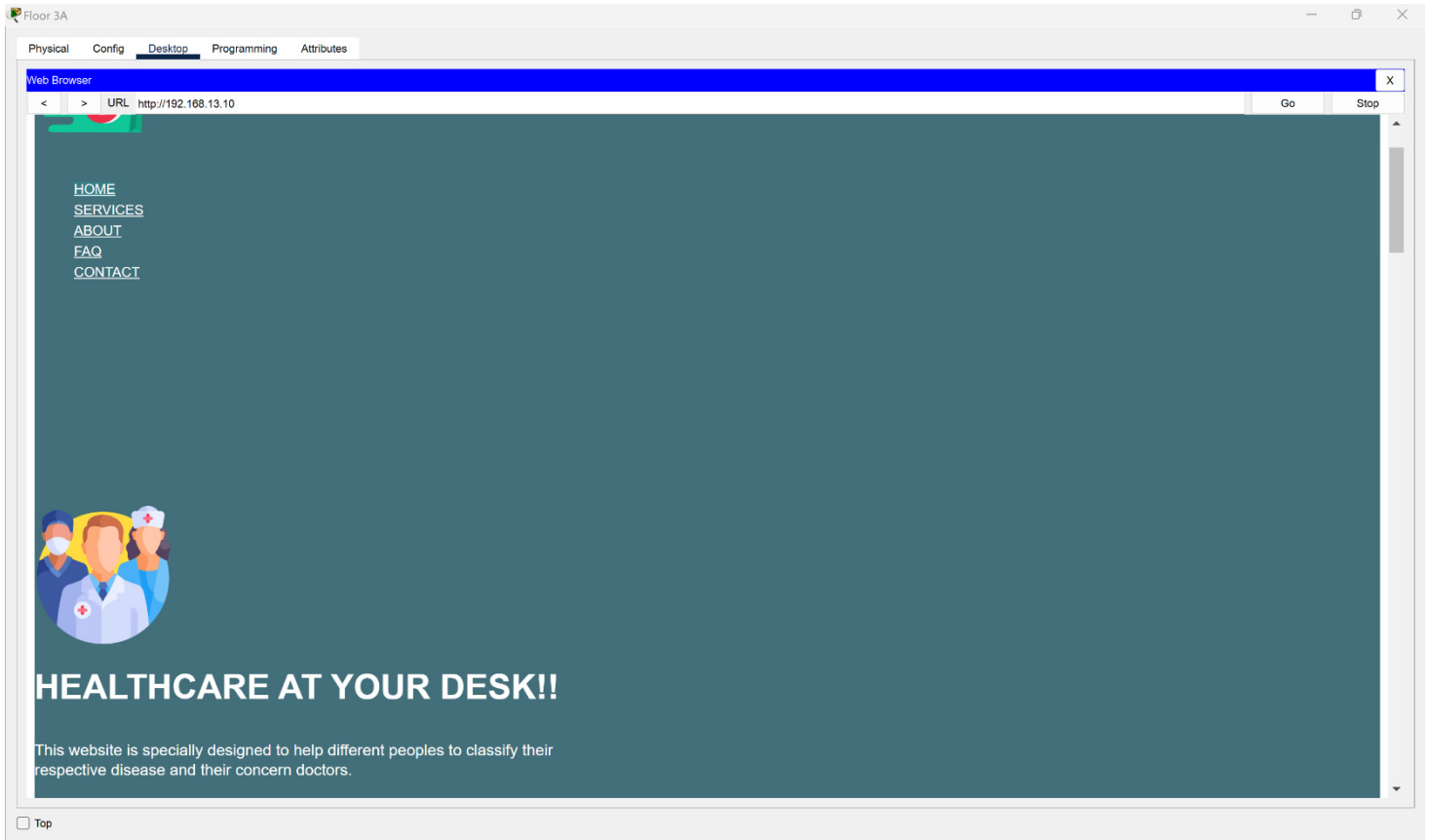


Figure 33: Access to Hospital Web Server

We have a Web Server located inside DMZ and we also configure basically a webpage on this server although it's not good. We do not have enough time to design the webpage's frontend look nice with CSS and also this is just for better simulation, not the main objective we aim to in this Assignment. Besides, we also configure DNS server with the domain-name for the hospital's web-server is *hcmuthospital.com*. You can see below, we can access to the web with the domain name above.

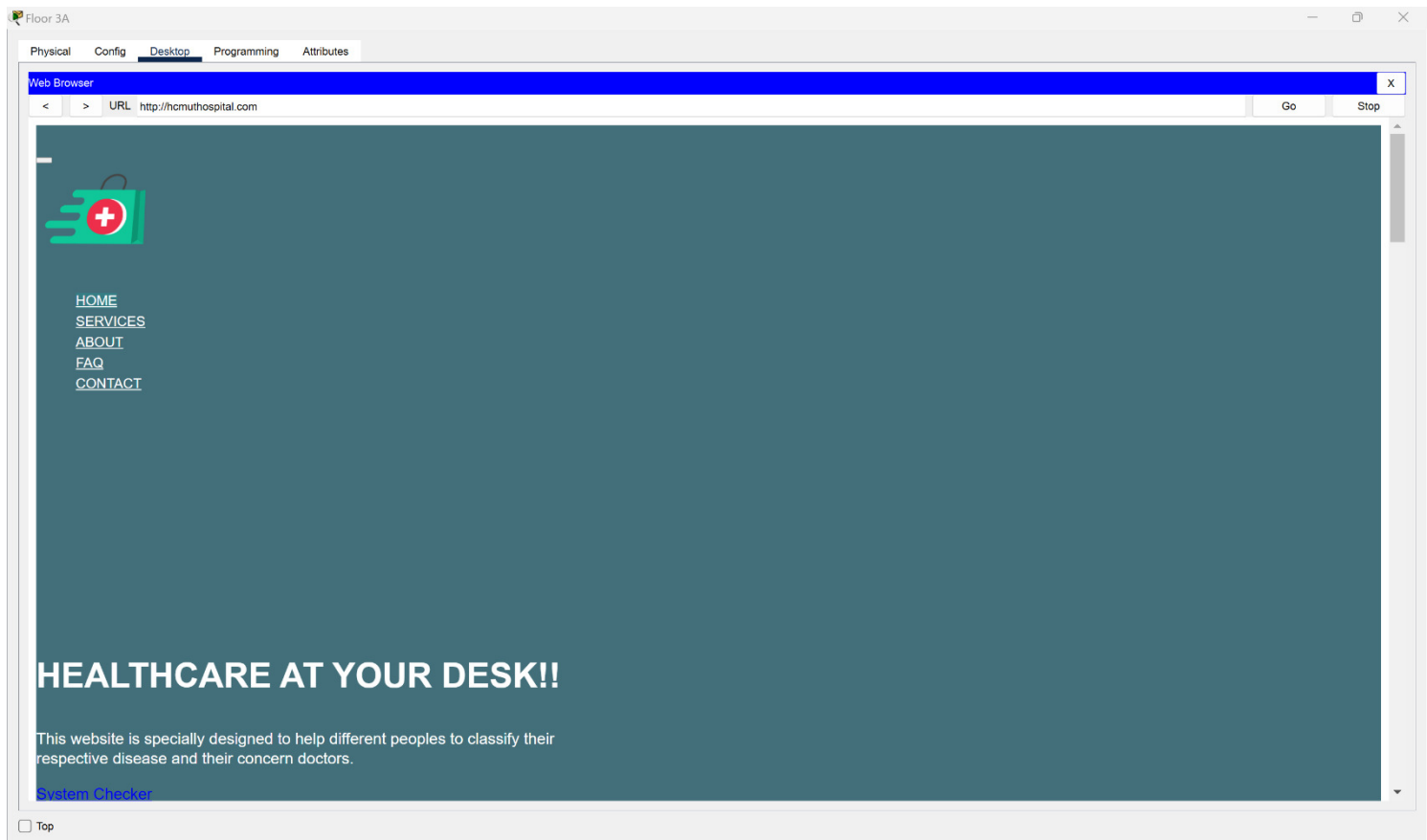


Figure 34: Access to Web inside DMZ but with Domain-name instead of IP Address



5.0.8 Access to Web Server on the INTERNET (Google)

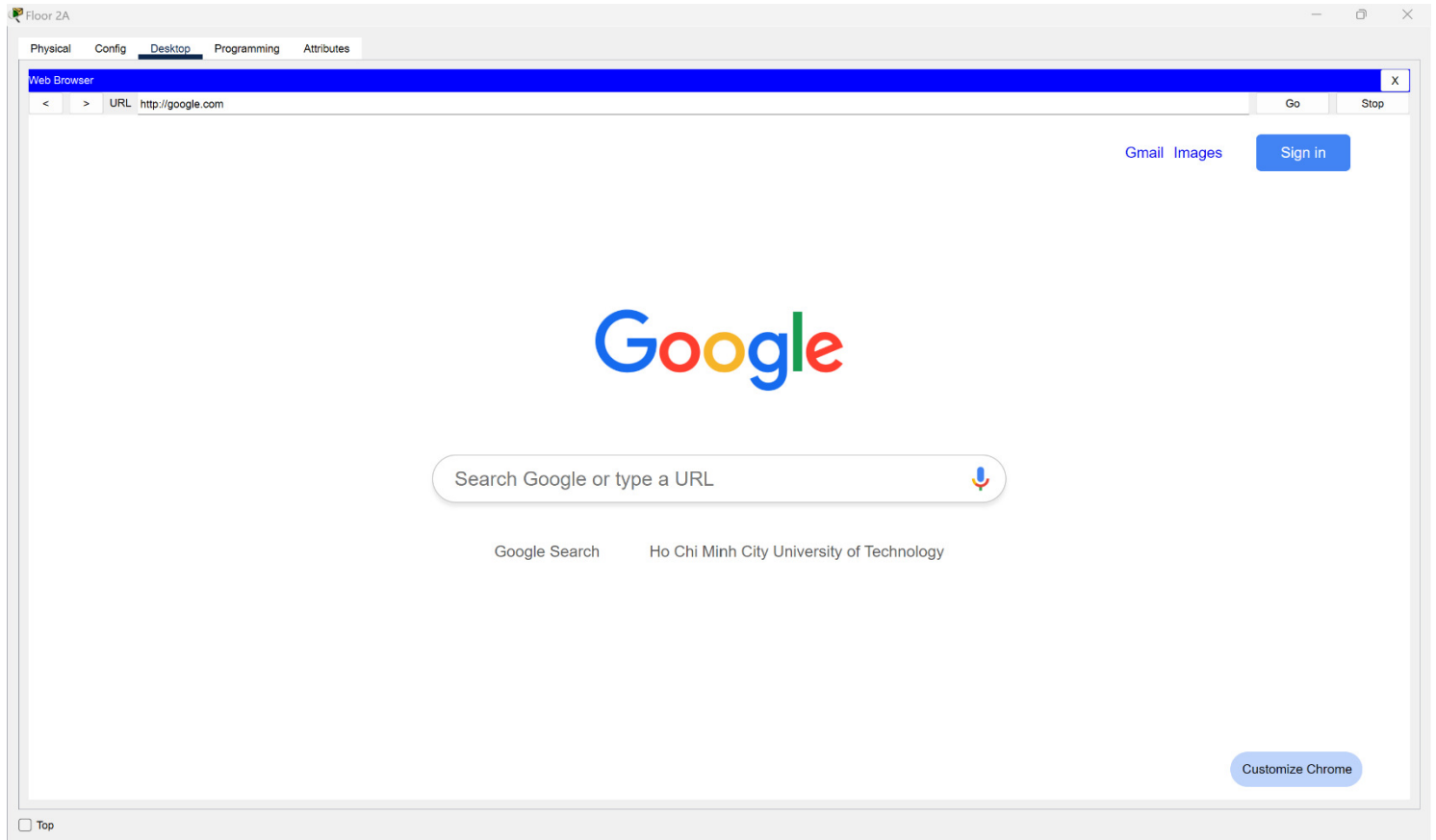


Figure 35: Access to Internet (Google)

As you can see, we can access to the Internet. This Google Homepage is set up on web server with HTML and CSS.

5.0.9 Network Address Translation (NAT)

PDU Information at Device: ASA0

OSI Model Inbound PDU Details Outbound PDU Details

At Device: ASA0
Source: Floor 5A
Destination: 10.10.10.3

| In Layers | Out Layers |
|--|--|
| Layer7 | Layer7 |
| Layer6 | Layer6 |
| Layer5 | Layer5 |
| Layer4 | Layer4 |
| Layer 3: IP Header Src. IP: 192.168.5.12, Dest. IP: 10.10.10.3 ICMP Message Type: 8 | Layer 3: IP Header Src. IP: 192.168.5.12, Dest. IP: 10.10.10.3 ICMP Message Type: 8 |
| Layer 2: Ethernet II Header 0002.4A69.8250 >> 0010.1196.0D02 | Layer 2: Ethernet II Header 0010.1196.0D01 >> 0090.2BAE.0CB9 |
| Layer 1: Port GigabitEthernet1/2 | Layer 1: Port(s): GigabitEthernet1/1 |

1. The CEF table has an entry for the destination IP address.
2. The device decrements the TTL on the packet.
3. The packet is going from an inside to an outside network. The device looks up its NAT table for necessary translations.
4. The NAT table does not have a matched entry for this packet. It passes the packet through without translations.

Challenge Me << Previous Layer Next Layer >>

Figure 36: Network Address Translation

5.0.10 Surveillance Camera System - IoT Server

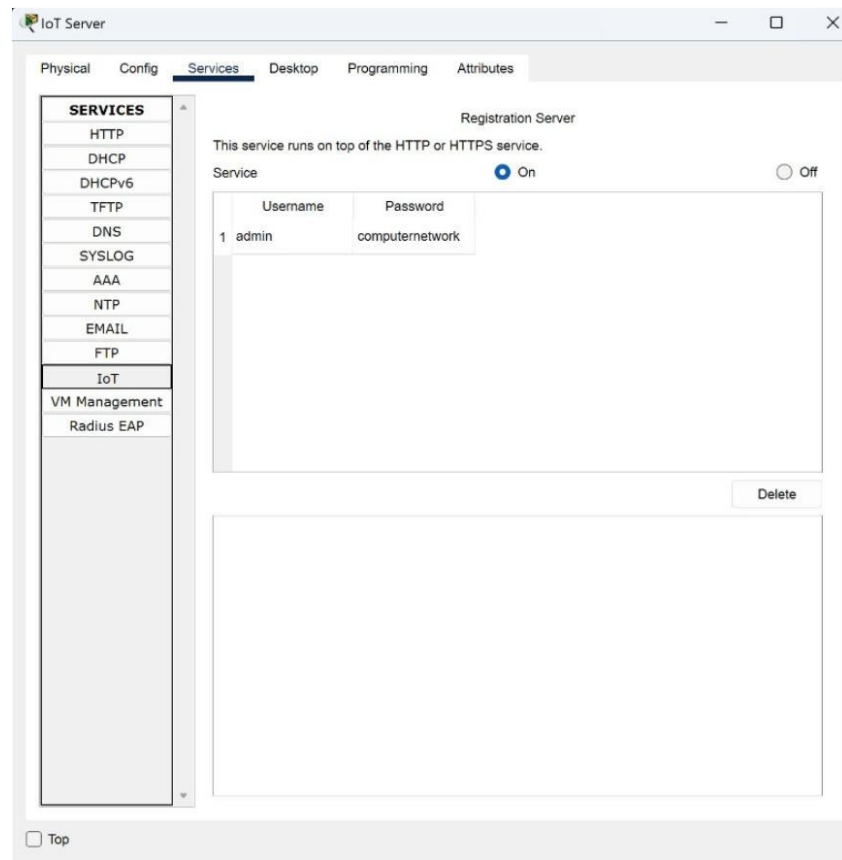


Figure 37: IoT Server



Figure 38: Surveillance Camera System on IoT Server



8 Conclusion

Consequently, we set up a network infrastructure for a hospital with 3 sites with basic configuration. Although we tried our best performance, there are still many things we need to consider due to our lack of knowledge in computer network field. At least, the system meets almost requirements and we consider this as a success. We gain many invaluable lessons and experiences via completing this Assignment in Computer Network Course and we hope that we can develop the performance of the system in a foreseeable future.