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

COMPUTER NETWORK
ASSIGNMENT 02

COMPUTER NETWORK DESIGN FOR UNIVERSITY

Lecturer: Nguyen Le Duy Lai
Author: Vuong Le Huy
Nguyen La Thong
Tran Vu Hong Thien

June, 2020

Table 1: GROUP'S MEMBERS

No.	Name	ID	Contribution
1	Vuong Le Huy	1652252	33.3%
2	Nguyen La Thong	1752522	33.3%
3	Tran Vu Hong Thien	1752506	33.3%

Table 2: ACTIVITY LOG

Day	Changes	Member
05/06/2020	Create project; Analyze system requirement;	Tran Vu Hong Thien
10/06/2020	Physical design.	Vuong Le Huy
19/06/2020	Logical design.	Tran Vu Hong Thien
19/06/2020	Calculate bandwidth.	Nguyen La Thong
20/06/2020	IP addresses range investigate.	Vuong Le Huy
23/06/2020	Network configuration; Budget calculation.	Nguyen La Thong

Contents

1 System requirement analysis

1.1 Synopsis

These days smart technology is everywhere in the world and for the objective to make BKU-Bach Khoa University become a modern and friendly university. CSE faculty has been researched and build a monitoring system with surveillance camera and many other devices (measuring humidity, temperature and light in classes). This system is implemented in buildings at H6 (Binh Duong - Di An). For this system to work efficiently, our faculty need to design new network in these buildings. Because of their important roles, the students in the faculty is asked to propose ideas for solving this problem.

1.2 System description

H6 Building already has camera system at some floors and running with current network. This system is stable, and data is stored in each camera. When new system is built, all the data will be stored in one server in room 106H6. The building also has many laboratories and classes (with many computers) at 6th and 7th floor. For the monitoring purpose, our university will invest an IoT kit for each class in H6 building include:

- Big area room - over 60m2: 6 temperature sensors, 6 light sensors, light remote control
- Other rooms: 3 temperature sensors, 3 light sensors, light remote control
- At each hall: 4 cameras
- Each theory classroom: 1 PC
- Each floor: 1 access point router

1.3 Assumption

In order to design the network for H6 building, we are going to assume the following details, including the building architecture, IP address usage and others, as explained in the following sections.

1.3.1 H6 building Architecture

Table below describes the overall design of H6 building and the equipment list based on the requirements.

ID	Floor	Room type	Room quantity	Device	Device quantity	Note
1	1-5	Admin	1	Computer	10	106H6
		Small room	45 (9x5)	PC	45 (1x45)	
				Temperature sensor	135 (3x45)	
				Light sensor	135 (3x45)	
				Light control equipment	45 (1x45)	
		Big room	15 (3x5)	PC	15 (1x15)	
				Temperature sensor	90 (6x15)	
				Light sensor	90 (6x15)	
				Light control equipment	15 (1x15)	
				Light control equipment	15 (1x15)	
		Hall	5 (1x5)	Camera	20 (4 x 5)	
				Access point router	5 (1x5)	
2	6	Computer lab	6	PC	192 (32x6)	

				Temperature sensor	36 (6x6)	
				Light sensor	36 (6x6)	
				Light control equipment	36 (6x6)	
		Small room	9	PC	9 (1x9)	
				Temperature sensor	27 (3x9)	
				Light sensor	27 (3x9)	
				Light control equipment	9 (1x9)	
		Big room	3	PC	3 (1x3)	
				Temperature sensor	18 (6x3)	
				Light sensor	18 (6x3)	
				Light control equipment	3 (1x3)	
		Hall	1	Camera	4 (4x1)	
				Access point router	1 (1x1)	
3	7	Computer lab	6	PC	192 (32x6)	
				Temperature sensor	36 (6x6)	
				Light sensor	36 (6x6)	

				Light control equipment	36 (6x6)	
		Small room	9	PC	9 (1x9)	
				Temperature sensor	27 (3x9)	
				Light sensor	27 (3x9)	
				Light control equipment	9 (1x9)	
		Big room	3	PC	3 (1x3)	
				Temperature sensor	18 (6x3)	
				Light sensor	18 (6x3)	
				Light control equipment	3 (1x3)	
		Hall	1	Camera	4 (4x1)	
				Access point router	1 (1x1)	

Also, there is a Server Room with 1 server PC and this room is located in the first floor, 105H6.

1.3.2 IP address range

To avoid collision because of the seamlessly integration into another existing network. We can assume the IP range(written in CIDR (Classless Inter Domain Routing) format) of each network is:

- Current network uses IP range : 192.168.0.0/24
- LTK campus network uses IP range: 192.168.1.0/24
- Maybe in the near future, there will be more devices attach (sensor, camera,..), we need to use many unique addresses , here we use IP class B: 172.168.0.0/16, there will be 65536 (256x256) unique addresses.

1.3.3 Extra requirements

Although the original requirements state that each floor will be configured with a different VLAN to save IP resources, we personally find that not adequate for several reasons:

- For security, like some rooms don't want to share its information to the outside (Like doing an important project).
- Similarly, sensors' and cameras' data should each be on their own VLANs, and only the server can access them. Additionally, they should only send the data directly to the server, without any medium.
- The students using computer lab rooms on floor 6th and 7th may bring their personal PCs to use, and will want to connect to the faculty's network. Therefore, the must be a DHCP server to assign IPs to new computers.
- Most of the traffic is from the time between 7:30 - 11:30, and 12:30-17:30. For convenience, we will assume they take 85% of the daily traffic.

2 Bandwidth Calculation

In this section, we will calculate the bandwidth required for Internet and local connections, in order to choose the appropriate ISP bandwidth and equipment to minimize cost

2.1 Computer

According to the table and the additional assumptions as described in Section 1, we obtain the following information:

- Number of PCs in classrooms and computer lab: 492
- Number of PCs in administrator room: 10
- Peak hours: 7:00 to 17:30 (10 hours), about 80% of people download in this range of hours.
- Average data download per day: 200MB for PCs in classrooms and computer rooms, 300MB for administrator room because computers in this room also send 10 mails with 10MB/email.

So, we can calculate the estimated bandwidth:

$$B = ((492*200+10*300)*8*0.8)/(10*60*10)=18 \text{ Mbps.}$$

However, in reality, 80% of download is not in the range of peak hours, the traffic is really busy during about 20 minutes of class time (4 periods long, 2 mornings and 2 afternoons). Therefore, we decrease the time for calculate bandwidth and we obtain:

$$B = ((492*200+10*300)*8*0.8)/(20*60)=540 \text{ Mbps}$$

Therefore, we will choose 600 Mbps ISP plan for Internet access (for 10% more)

2.2 Room

According to the table and the requirements, it is clear that every room (theory classrooms, computer rooms) has sensors which are all managed by IoT kit and computers.

- Sensors: 32 Kbps each, it fits with Fast Ethernet (100 Mbps) which is most commonly found in networks using Category 5 copper twisted-pair cable, also work with fiber-optic cable.
- IoT board:
  - Small rooms: (6 sensors): 32*6 = 192 Kbps = 0.192 Mbps.
  - Big rooms (12 sensors): 32*12 = 0.384 Mbps.
- Computers:
  - With calculations for all computers, each computer of classrooms and computer rooms would need a bandwidth of (200*8)/(15*60) = 1.8 Mbps, and 2.7 Mbps for computer in administrative room.

2.3 Floors

According to table and requirements, there are 4 cameras in each lobby and there is one switch for each room that we calculate bandwidth for the whole room.

- Cameras: It is reported that there are 4 cameras in each lobby and there are 4*7 = 28 cameras for the whole building.

Also, all cameras store the data directly to a central server with data transfer rate of 1000 Mbps.

- Switch for each room:
  - Small theory room has 1 desktop computer on teacher's desk, 3 pairs of sensors: 1.8 + 0.192 = 1.992 Mbps.
  - Big theory room has 1 desktop computer on teacher's desk, 6 pairs of sensors: 1.8 + 0.384 = 2.184 Mbps.
  - Computer lab room has 32 computers and 6 pairs of sensors: 32*1.8 + 0.384 = 57.984 Mbps.
  - Administrator's room has 10 computers with 2.7 per each: 2.7*10 = 27 Mbps.

So, we can still use Fast Ethernet to connect switch of each room to switch of floor.

2.4 Whole building H6

There are 7 floors:

- Floor 1 to 5 have 15 big theory rooms, 45 small theory rooms (cameras added later): 15*2.184 + 45*1.992 = 122.4 Mbps.
- Floor 6 and 7 have 6 big theory rooms, 18 small theory rooms, 12 computer lab rooms: 6*2.184 + 18*1.992 + 12*57.984 = 744.768 Mbps.

For the whole, apart rooms on floors, we also have 28 cameras, 10 computers on administrative room. Besides we estimate that there are about 500 students or staves accessing Internet through access point router with speed of 256 Kbps = 0.256 Mbps.

Total Bandwidth is: 122.4+744.768+1000+27+500*0.256 = 2022.168 Mbps.

Therefore, we will use Gigabit Ethernet which can work with twisted pair (Cat-6 or Cat-7 cable) and fiber-optic cables for connecting main switch to main server at room 106H6.

3 Physical Design

3.1 Room Design

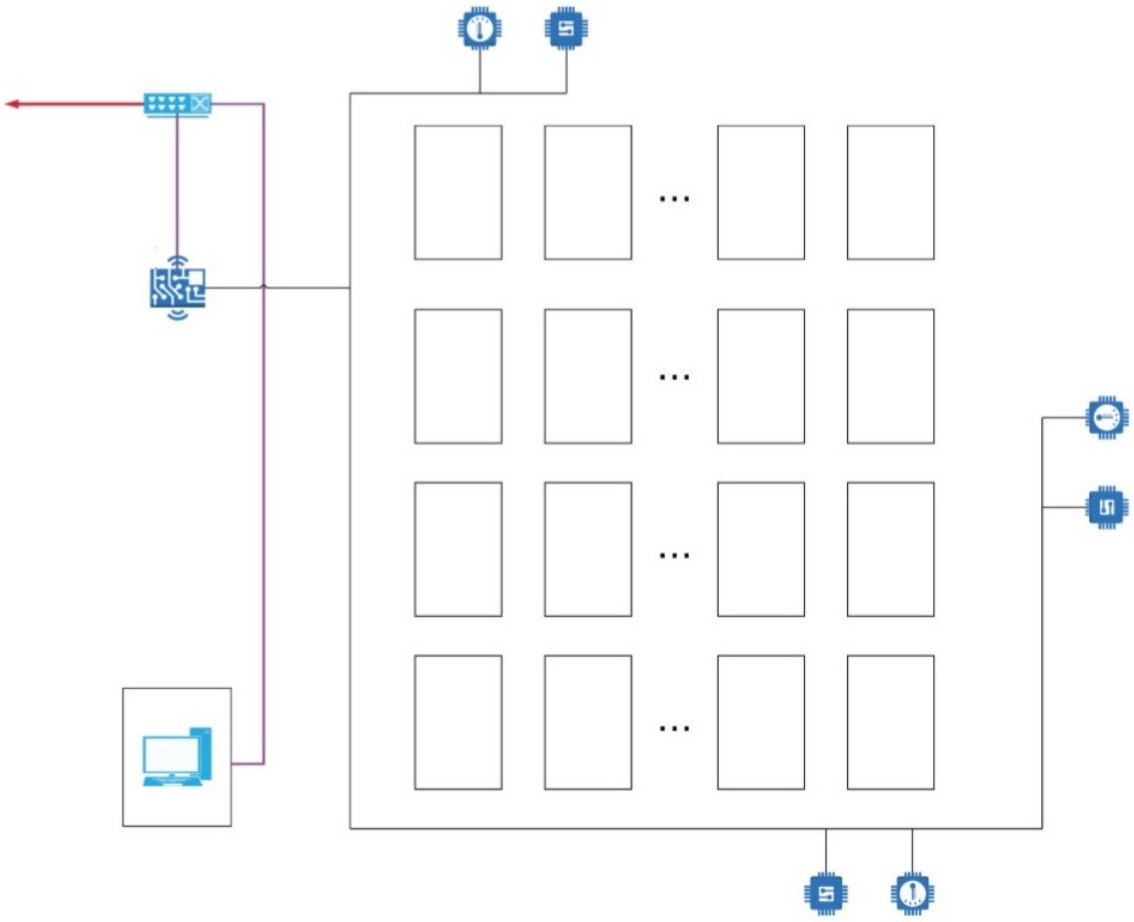
3.1.1 General Requirements

- Control board is always in the room for ready and convenient to use and supervise.
- Wires are fixed to the walls or ceiling that protects from outside affects.
- We need to number all wires or use wires with appropriate order in order to be easier to maintain.
- We can use air hole for connecting switch in room to floor switch.

3.1.2 Small Size Classroom

Each classroom has 1 PC at teacher desk, an IoT board for managing 6 sensors (3 pairs). So, following the design in the figure below:

- The switch has 8 ports, but 2 of them are used that one for PC and one for IoT board.
- The switch will connect to outside which is the switch of floor.
- 6 sensors are located throughout the room, each pair is put in one side of the room.
- All sensors connect to Arduino board for easy management, control and decreasing number of ports that are used in switch of room.
- IoT board is Arduino board which is connected to switch with the violet line (the Arduino is the illustration for real Arduino).
- IoT board is placed in the circuit switch box for protection and maintain if need.
- There is also one PC one teacher's computer in teacher's desk which is connected to switch with another violet line.
- We do not put remote control of light in this figure because it can be a part of our network that it does not contribute to total bandwidth much.

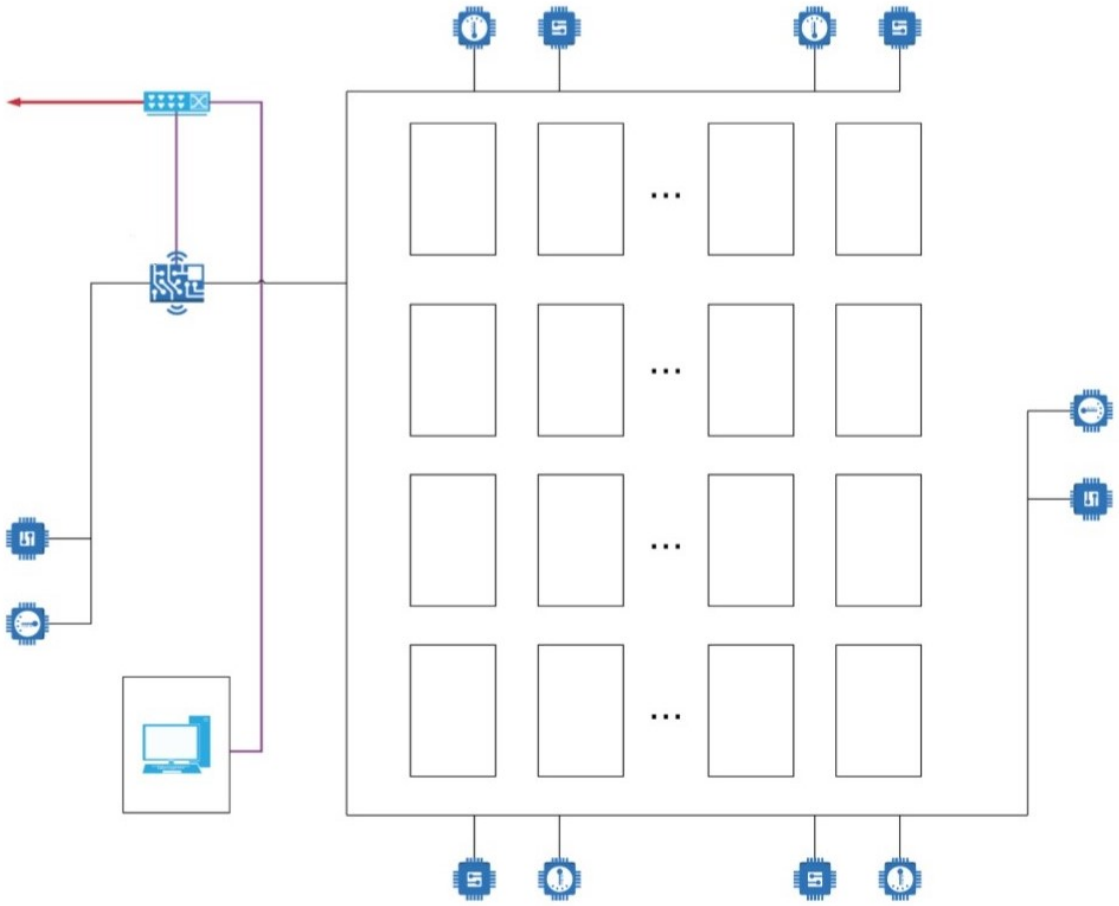


3.1.3 Medium Size Classroom

Each classroom has 1 PC at teacher desk, an IoT board for managing 12 sensors (6 pairs). So, following the design in the figure below:

- The switch has 8 ports, but 2 of them are used that one for PC and one for IoT board.
- The switch will connect to outside which is the switch of floor.
- 12 sensors are located throughout the room, every side of the room.
- All sensors connect to Arduino board for easy management, control and decreasing number of ports that are used in switch of room.
- IoT board is Arduino board which is connected to switch with the violet line (the Arduino is the illustration for real Arduino).
- IoT board is placed in box for protection.

- There is also one PC one teacher's computer which is connected to switch with another violet line.
- We do not put remote control of light in this figure because it can be a part of our network that it does not contribute to total bandwidth much, but it still exists in this room.

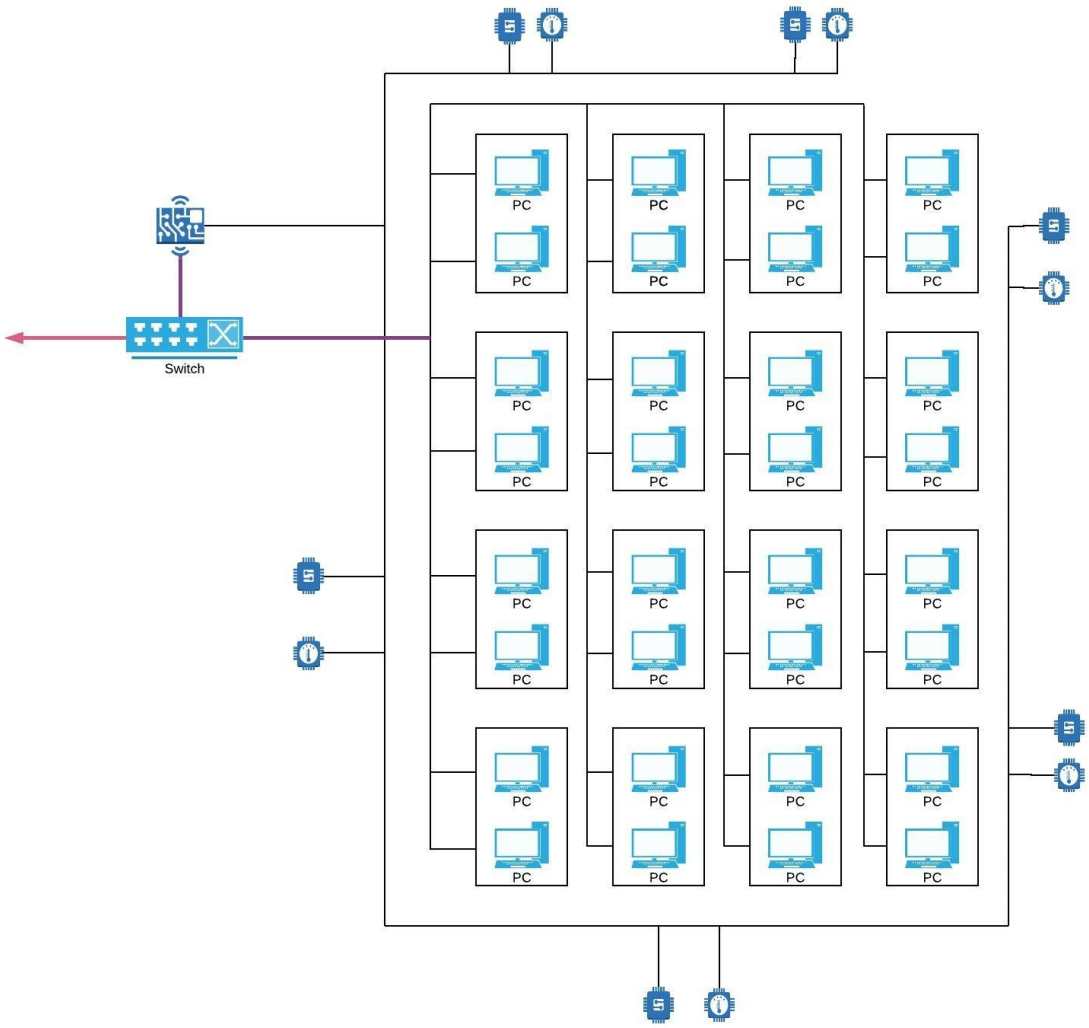


3.1.4 Laboratory Room

Each computer lab has 32 PCs, 12 sensors (6 pairs), IoT board and remote control for air conditioner.

- We use switch with 48 ports, 32 ports are used for 32 computers, and 1 port for IoT board (purpose of using this is explained above).
- PCs connect directly to switch (as illustrated in figure below).
- There are 12 sensors because each computer lab room is considered as a big theory room that they are connected to IoT main board.

- The IoT board connect to switch of room with violet color line in the figure.

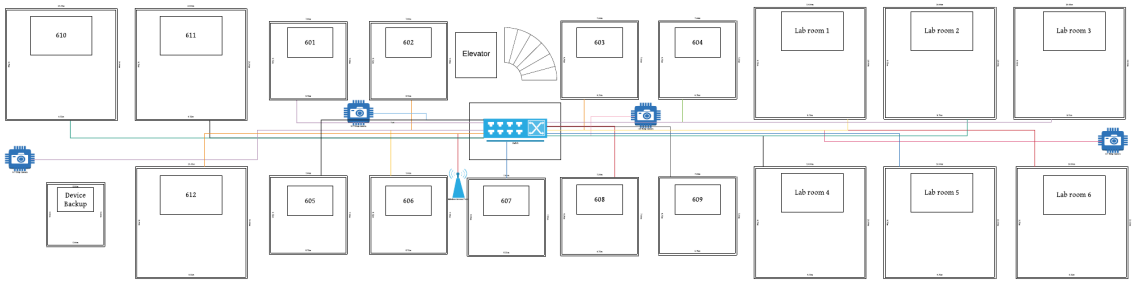


- We do not put air conditioner control device to this figure because, it can be not related much to our network, but it still exists in this room.
- Each pair of computers is put on the table which is placed appropriately.
- 6 pairs of sensors are placed through the room, 2 pairs are in 2 sides and 4 remaining are located in other 2 sides for measuring accurately.

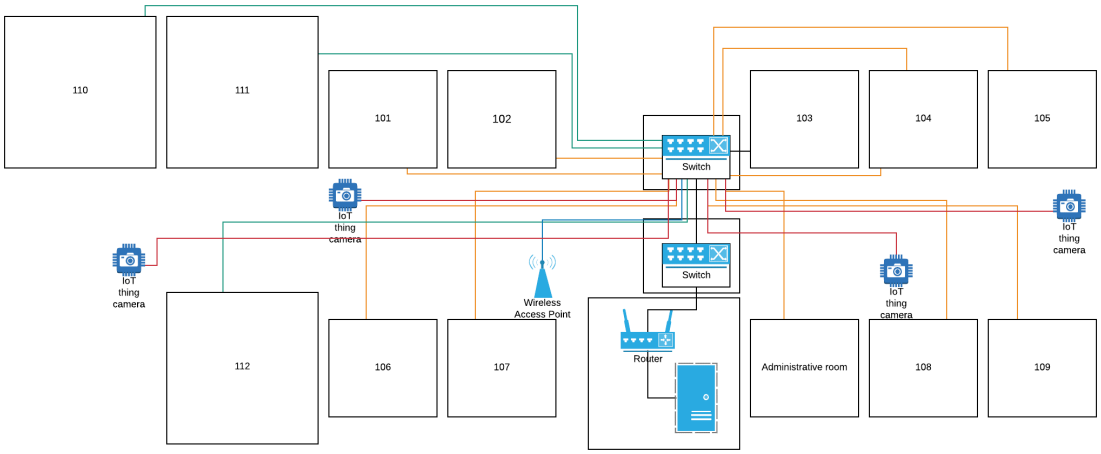
3.2 Floor physical design

- The figure shows a design for sixth floor which is the same for seventh floor.
- Every room's switch connects to the main router of the floor.

- There are also four cameras which connect directly to the floor switch.
- The floor switch is placed on the box next to the elevator and it should be placed in the hall in order to be easy to connect to main router.
- Wires are fixed to walls that we illustrate with different colors for easy to view.
- Seventh floor is the same as this figure.
- First to fifth floor (apart from server room) are also similar that we just eliminate lab rooms.
- By the way, first floor has administrative room, which can be considered as other rooms that connect to switch of first floor.



First Floor



Sixth Floor

4 Logical design

4.1 Fundamentals theories

4.1.1 VLAN

VLAN (Virtual Local Area Network) is logical grouping of devices in the same broadcast domain. Those devices are grouped by their functions, rooms or by purpose of use that they are

limited to just communicate other devices in the same VLAN.

About the purpose of use: VLANs increase the number of broadcast domains while decreasing their size, can create more lexible network designs that group users by department instead of by physical location, also reduce security risk.

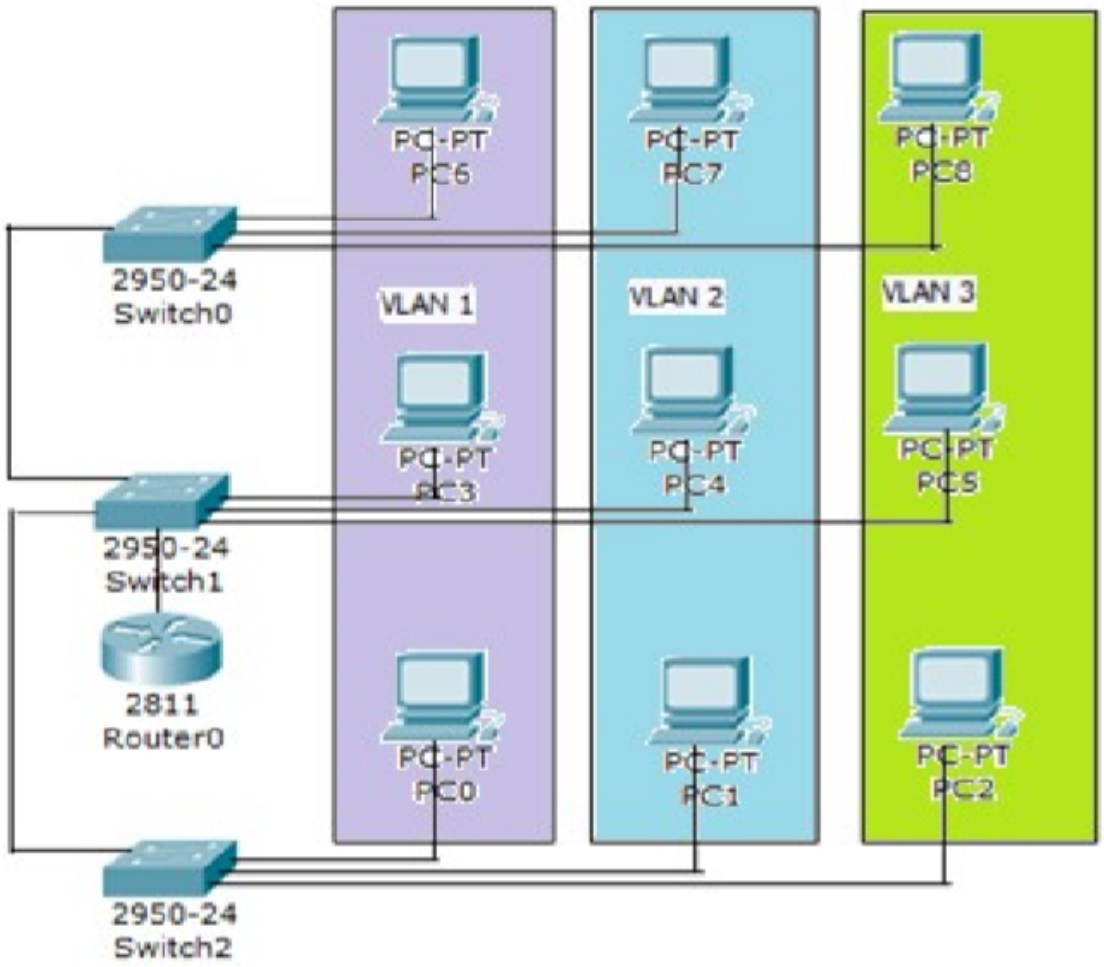


Illustration Image

4.1.2 INTER VLAN ROUTING

Different VLANs can connect and transfer data to each other, we need one router layer 3, or Switch layer 3 or we can call Multilayer Switch. We will create one trunk link that all communications of VLAN operate through this trunk.

In router, we create sub-interface corresponding to VLANs and connect those to trunk of switch.

In Switch layer 3, we use SVI (Switch Virtual Interface or Interface VLAN) to route between VLANs.

4.1.3 DHCP

Every device in the network which uses TCP/IP protocol must have unique IP address. For supporting to provide accurate IP addresses, IETF (Internet Engineering Task Force) developed DHCP protocol (Dynamic Host Configuration Protocol) that allows to provide IP addresses for Clients.

DHCP protocol works based on Client/Server model that communication for providing IP as follows:

- Client sends DHCPDISCOVER to Server and requests providing IP.
- Server sends back DHCPOFFER for renting IP.
- If Client accepts and chooses a DHCPFFER, it will send back DHCPREQUEST to accept to rent that IP.
- If Server is accepted, it will send back again DHCPACK for validating about IP provision. Also, it also sends some information about configuration like: Default Gateway and DNS Server.

4.1.4 VPN

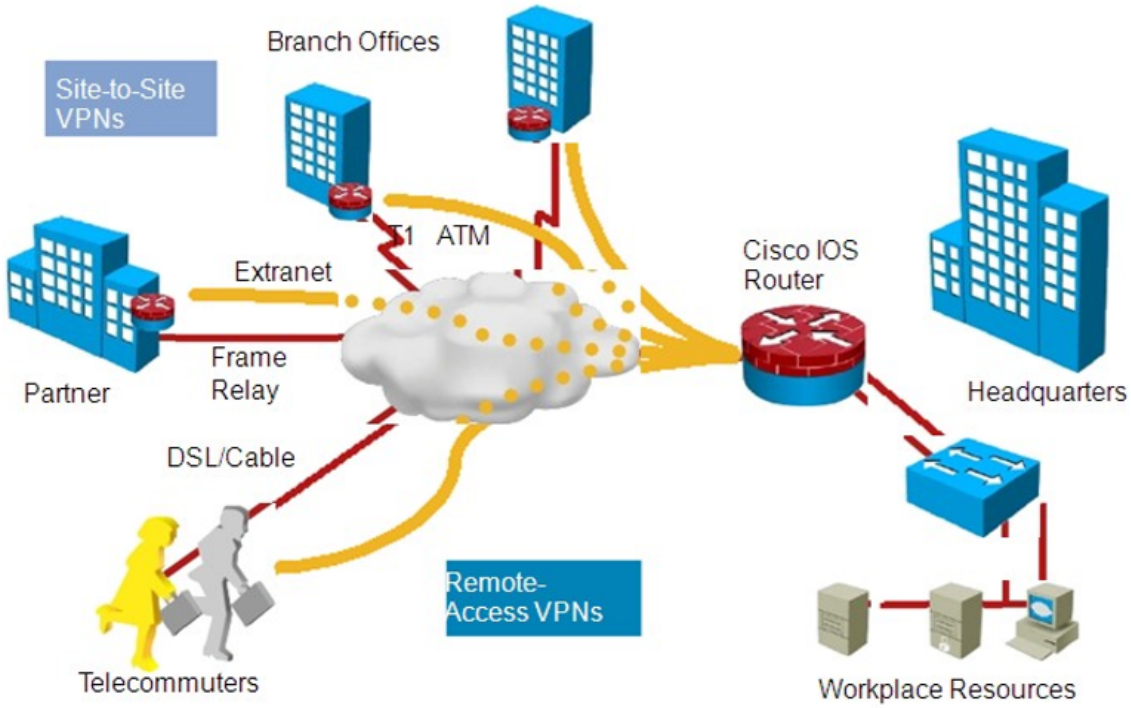
VPN (Virtual Private Network) is extension of private networks by public network. VPN is used for connecting office branches, people who are very far from main office can access. It is divided into 2 types: Site-to-Site VPN and Remote Access VPN

Site-to-site VPN is the model for connecting networks from different places to create the whole system. In this model, first validation depends on first and last device in Site, and they operate like Gateway and it is the place to put a lot of security policies for transferring data safely.

Remote Access VPN is usually applied for staves who are far from their office or would like to work at home safely. Also, it can be applied for far small branches connect to main office that can be considered as User-to-LAN.

VPN's Advantages:

- Low cost: Cost for constructing VPN is much lower than other WAN like: Frame Relay, ATM, Leased Line.
- More secure: it uses some algorithms for encoding and validation methods.
- It overcome some geographical barriers and it is ready to connect private networks by using Internet environment.



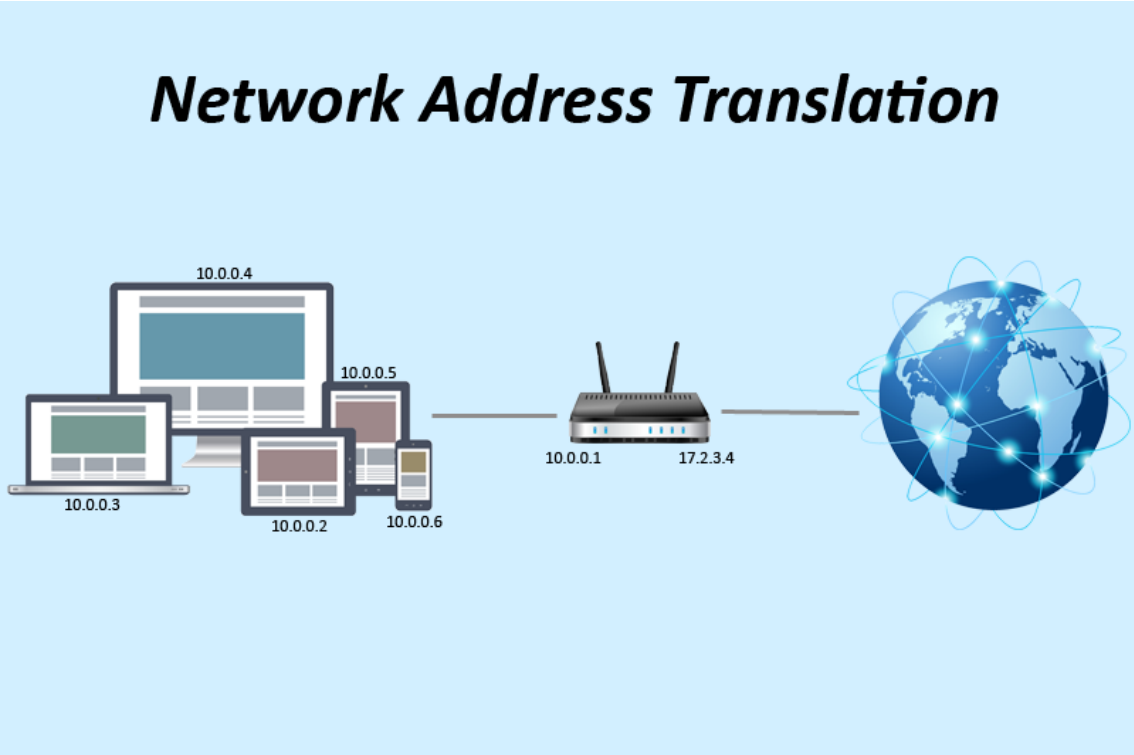
4.1.5 NAT

Network Address Translation (NAT) is designed for IP address conservation. It enables private IP networks that use unregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network.

As part of this capability, NAT can be configured to advertise only one address for the entire network to the outside world. This provides additional security by effectively hiding the entire internal network behind that address. NAT offers the dual functions of security and address conservation and is typically implemented in remote-access environments.

PAT: the Internet Service Provider (ISP) assigns a single IP address to the home network's router. When Computer X logs on the Internet, the router assigns the client a port number, which is appended to the internal IP address. This, in effect, gives Computer X a unique address. If Computer Z logs on the Internet at the same time, the router assigns it the same local IP address with a different port number. Although both computers are sharing the same public IP address and accessing the Internet at the same time, the router knows exactly which computer to send specific packets to because each computer has a unique internal address.

We use PAT in this report.



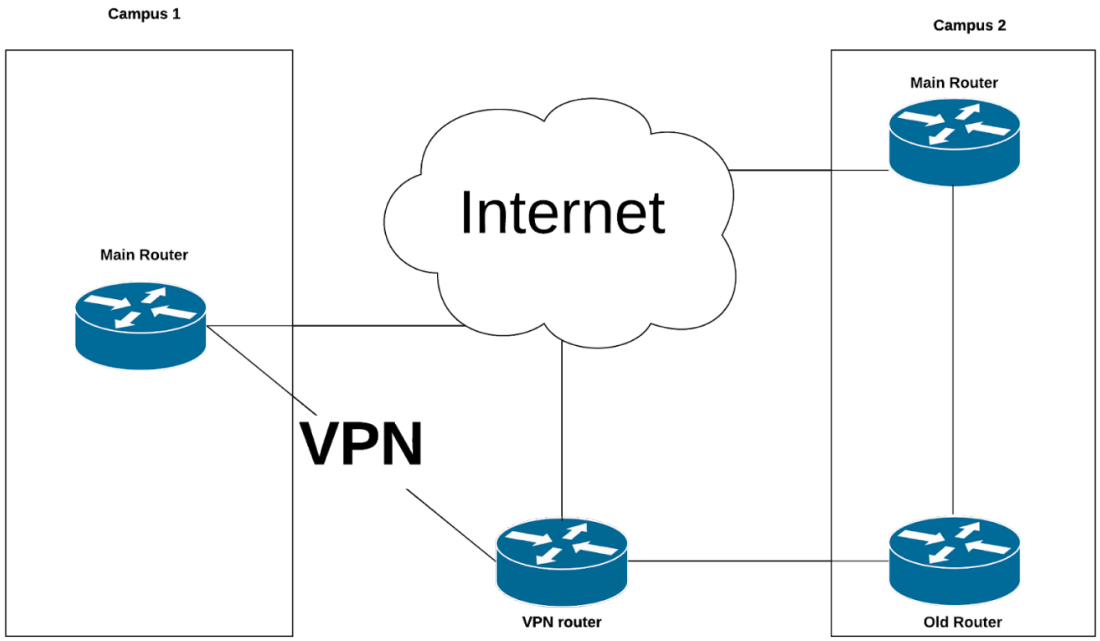
4.2 Logical design architecture

In this section, we will list out all components to our network design at different levels: overall design, building, floor and finally each individual room.

4.2.1 Preliminary Design

Main components of new computer network:

- New Main Router: This is the centerpiece of our new computer network. It handles data routing between devices of the new system, as well as communicate with the existing system and allows Internet access to the PCs.
- Communication with existing computer network system: New main router will connect to the old main router of the old computer network system.
- Connection with Ly Thuong Kiet campus via VPN using VPN Router: Data going to and from Ly Thuong Kiet campus will go through VPN Tunnel to enhance security.
- Connection with ISP's router to enable Internet access: There are 2 connections to the Internet, one from main router to access internet and another from VPN router to implement site-to-site VPN.

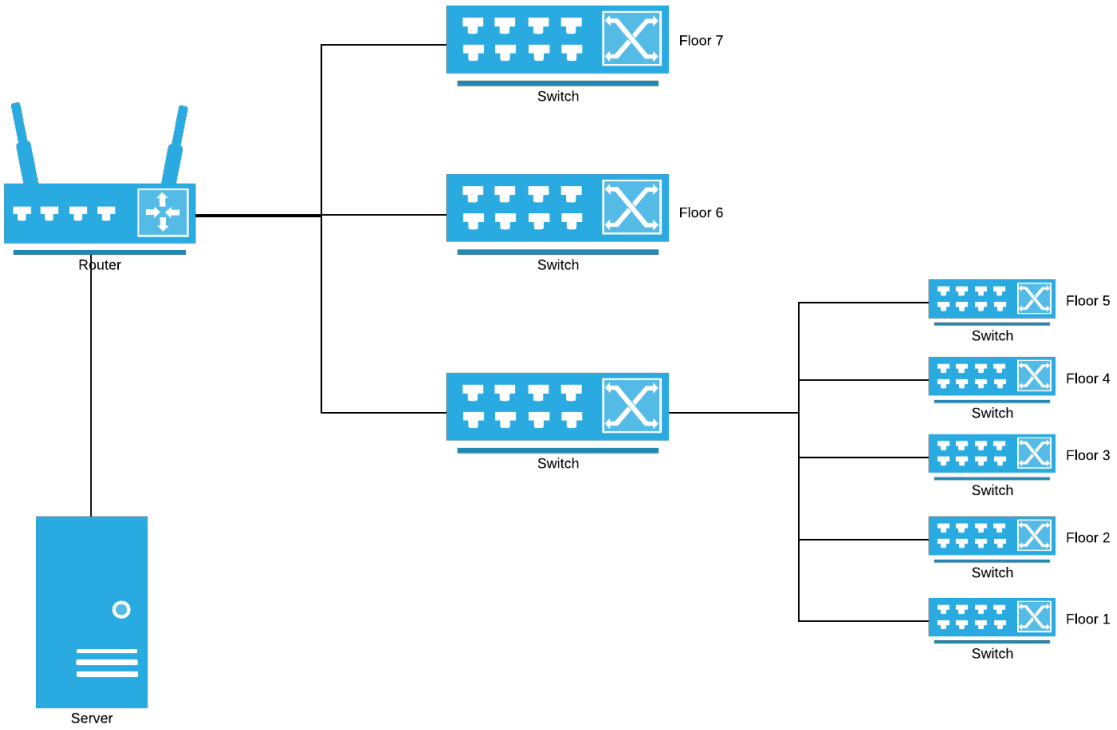


4.2.2 H6 Building Design

Beside the physical design, we present the design in more detail:

- Switches of Floor 1-5 will be connected to a common switch, since their network design are very similar, therefore doesn't require direct connection to MAIN ROUTER.
- Each of the Floor 6-7 switches will be connected to the MAIN ROUTER, these floors have many computer labs, therefore it would be better if them connect to the MAIN ROUTER independently.
- The main switch at Server room will be connected to the MAIN ROUTER as well.

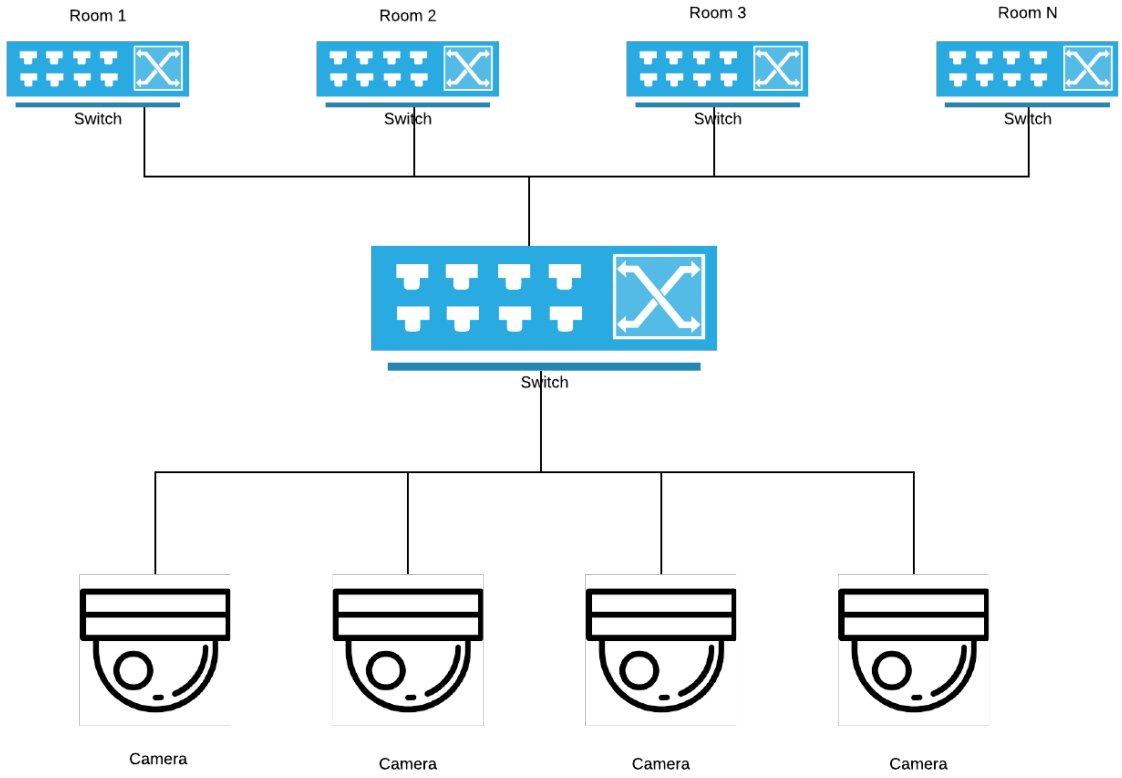
Thus, there is a total of 5 connections to the MAIN ROUTER. This connection scheme reduces the amount of ports needed, reduce load on MAIN ROUTER and allows easier maintenance.



4.2.3 Overall Floor Design

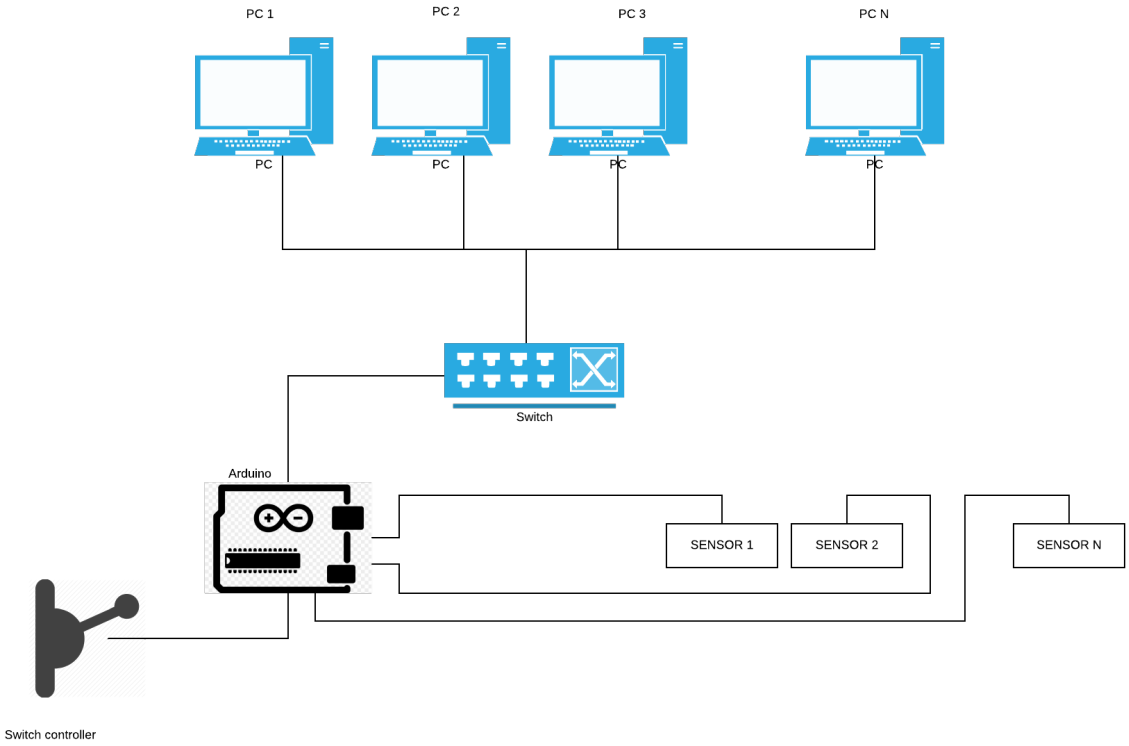
Each rooms' switch is connected to the main floor Switch.

The 4 cameras are connected directly to the main floor Switch.



4.2.4 Room Design

Each PCs is connected directly to room's Switch. The IoT devices and remote controls are connected to an IoT board. This help us to configure them more easily, and also save IP resources.



4.3 Network Configuration

Let's take an overview at the the number of devices we have to configure in our design:

- Computer Lab: total 32*12=384 PCs, sensor + camera = 44 devices.
- Theory Classroom: total 60 PCs, sensor + devices = 80 devices.
- Office: 1 PC, 1 IoT board.
- Hall: 4 cameras each floor.

4.3.1 VLAN Segmentation

We are going to segment the devices into VLANs based on their functionalities, then by each floor in order to reduce load on the switch and enhance security. In particular:

- Sixth and seventh Floor: These floors share the same overall structure, so the below design is applicable to all of them.
  - All Computer Labs will be segmented into their respective floor's VLANs.
  - All sensors/cameras require very high security due to their nature of monitoring.

  Therefore, we propose to segment the cameras and IoT boards into a VLAN, sharing with other floors as well.

- First to fifth floor: These floors share the same overall structure, so the below design is applicable to all of them.
  - All PCs will be segmented into their respective floor's VLANs. (1 for each classroom).
  - All sensors/cameras require very high security due to their nature of monitoring.

  Thus, we segment the cameras and IoT boards into a VLAN that shared connection with other floors.
- Server Room: Will have its own VLAN to enhance security. We will configure Inter-VLAN Routing for MAIN ROUTER, because Server has to monitor all other VLANs.

4.3.2 IP Address Range

In this section, we will allocate IP resources to the devices. As discussed in Section 1.3.3, we will use the IP address range 172.168.0.0/16. The details are described in below.

Floor	Type	Quantity	IP Range	DHCP	VLAN
1-5	Server	1	172.168.4.96/30		Default
	Theory room	60	172.168.0.128/26		2
	Sensor & Cam	80	172.168.0.0/25		3
6	Lab 1	32	172.168.0.192/26	X	2
	Lab 2	32	172.168.1.0/26	X	3
	Lab 3	32	172.168.1.64/26	X	4
	Lab 4	32	172.168.1.126/26	X	5
	Lab 5	32	172.168.1.192/26	X	6
	Lab 6	32	172.168.2.0/26		7
	Theory room	12	172.168.4.64/28		8
	Sensor & Cam	22	172.168.4.0/27		9
7	Lab 1	32	172.168.2.64/26	X	2
	Lab 2	32	172.168.2.128/26	X	3
	Lab 3	32	172.168.2.192/26	X	4
	Lab 4	32	172.168.3.0/26	X	5
	Lab 5	32	172.168.3.64/26	X	6
	Lab 6	32	172.168.3.128/26	X	7
	Theory room	12	172.168.4.80/28		8
	Sensor & Cam	22	172.168.4.32/27		9
1	Admin	10	172.168.4.112/28		

4.3.3 IP Address Allocation Scheme

We decide to allocate IP addresses to device based on their properties:

- Server: Static IP, because it is the place that receives all the data.
- PCs in Computer Labs: Dynamic IP served with DHCP server, because students may bring their devices to connect to the faculty's network.
- Sensors/Cameras: Static IP. These devices will not change so often.

4.3.4 VPN Routing

The network must configured such that if the data is coming to LTK faculty, it has to go through ROUTER VPN, otherwise, it will go to the Internet. The main router must also be configured to interface with the old system.

4.3.5 NAT configuration

As all these IPs are private only, the system will require NAT to translate into a public address when go out to the Internet. This public IP is given by ISP.

5 Budget

Device	Quantity	Price per unit	Note
Router 4 port	1	2.500.000 VND	VPN router
Router 8 port	1	6.000.000 VND	Main router
Switch 48 port	12	10.000.000 VND	Computer lab's switch
Switch 20 port	8	2.500.000 VND	Floor's switch
IoT board	96	300.000 VND	For each room
Cable	5600 (meters)	5.000 VND	
Total			205.300.000 VND

6 Conclusion

During the designing phase, we have come the conclusion the pros and cons of the design:

- Pros:
  - Using one main router reduces maintenance cost.
  - Reasonable amount of VLANs, thus reducing load on router.
  - VPN to Ly Thuong Kiet faculty enhances security over Internet.
  - Using IoT boards like arduino to connect all sensors will save a large IP resources.
- Cons:
  - One main router means that there is whole system downtime when it is under maintenance. In the future, we hope to implement another backup router.
  - Using quite a lot switches. Although 1 switch with more ports is better, it is very expensive so we settle for the proposed design.