**CHI MINH UNIVERSITY OF TECHNOLOGY AND EDUCATION**

**FACULTY FOR HIGH-QUALITY TRAINING**

**COURSE NAME: WINDOW PROGRAMING**

**🙡🙠✵🙢🙣**



**FINAL PROJECT**

**DESIGNING NETWORK INFRASTRUCTURE.**

**Lecturer:** Nguyễn Đăng Quang, PhD

**Course ID:** PROJ215879E\_1\_01\_FIE

**Group:** 2

**Date:** /2022-2023

*Ho Chi Minh City, Jun, 2023*

**LIST OF STUDENTS – GROUP**

**Project:** Designing network infrastructure.

|  |  |
| --- | --- |
| ***ID*** | ***Full name*** |
| 21110802 | Châu Dương Phát Tiến |
| 21110780 | Nguyễn Duy Mạnh |

**Professor’s comment**

Ho Chi Minh city, …. ,… , 2023

Grading

**Contents**

[**PROLOGUE** 4](#_Toc152367352)

[**1.** **INTRODUCTION** 5](#_Toc152367353)

[***Introduce*** 5](#_Toc152367354)

[***Reason for choosing the topic*** 5](#_Toc152367355)

[***Objects and objects of research*** 6](#_Toc152367356)

[**2.** **CONTENT** 7](#_Toc152367357)

[**CHAPTER I: THEORETICAL BASIS OF THE THESIS** 7](#_Toc152367358)

[***Basic knowledge of computer networks*** 7](#_Toc152367359)

[***Knowledge of LAN network design*** 11](#_Toc152367360)

[***Knowledge of security and network safety*** 12](#_Toc152367361)

[***Knowledge of WLAN wireless networks*** 14](#_Toc152367362)

[**CHAPTER 2: DESIGN NETWORK INFRASTRUCTURE FOR 5-STAR HOTELS** 17](#_Toc152367363)

[2.1 analyze the design of the project 17](#_Toc152367364)

[2.2 Requirements analysis 25](#_Toc152367365)

[2.3 Determine network structure 27](#_Toc152367368)

[2.4 Select network equipment and estimate costs 28](#_Toc152367369)

[2.5 Build a simulated network 29](#_Toc152367370)

[CONCLUSION 40](#_Toc152367372)

[REFERENCE 41](#_Toc152367373)

# **PROLOGUE**

Firstly, we would like to express our gratitude to PhD. Nguyễn Đăng Quang for his whole-hearted instructions that helped us finish our final project for the IT Project course. Thanks to the knowledge the professor has provided us, we were able to firmly grasp the basic knowledge and foundation for building database management system. And through this project, our group would like to present the development network infrastructure systems. During the process of executing this project, it will be hard to avoid mistakes. Because of that, we would love to get the professor’s suggestion on improving our work so it would be more functional and complete. We wish you good health and the best of luck pursuing the path of teaching.

Finally, we would like to thank all the teachers and classmates who studied with us on this course and offered us support while we carried out our final project.

# **INTRODUCTION**

## ***Introduce***

In the tourism sector's strong development trend, mini hotel need effective information technology solutions to service their guests. The network system in particular is important since it affects the hotel's connectivity, data transmission capabilities, and information security.

In order to provide a practical network design solution for a mini hotel, the topic "Local area network design for a mini hotelusing VLAN technology" was investigated. The main focus of the discussion is on usxing VLAN technology to satisfy demands for privacy, security, and straightforward administration and use. The project's output is a specific, typical network architecture plan with a VLAN system, network partitioning between guests and employees, for mini hotel

## ***Reason for choosing the topic***

The significance of network infrastructure: Internet services, intranets, and other associated systems are all provided by network infrastructure, which is crucial for the hotel sector. A strong network infrastructure is essential for ensuring the performance, connection, and dependability of hotel operations.

Technology's ongoing advancement has a big impact on the hospitality sector. An adequate network infrastructure is required to take advantage of new opportunities and satisfy customer expectations in the age of online services, AI, and the Internet of Things (IoT).

Increased customer satisfaction: A superior network infrastructure can give customers a better experience. This includes seamless wifi connectivity throughout the hotel, automated systems for managing guest rooms, easy online reservation tools, and more. Putting money into network infrastructure will assist boost customer satisfaction and establish a competitive edge.

Security and confidentiality: The hotel is the home to numerous guests and private data. To safeguard consumer data and reduce cyber security concerns, a reliable and secure network architecture is essential. Modern security technologies like firewalls, encryption, and access control will be incorporated into a well designed network infrastructure.

Based on the aforementioned arguments, I am confident that studying and developing network infrastructure for hotels will have a positive impact on both consumers and businesses.

## ***Objects and objects of research***

Research subjects: Local area network (LAN) system of 5-star hotel.

*Research subjects:*

* LAN architecture and topology are suitable for the hotel environment.
* The solution uses VLAN technology to partition and isolate the network.
* Necessary devices and hardware for this network design.
* IP address plan, subnet configuration, VLAN.
* WLAN wireless access technology.
* Security solutions, network information security.
* Basic network applications and services for hotels.

*Research purposes*

* Research the unique requirements and characteristics of the 5-star hotel environment to propose appropriate LAN/WLAN network design solutions.
* Research and apply VLAN technology to design a LAN with the ability to partition and separate the network between guests and employees.
* Propose reasonable configuration of network devices such as switches, WLAN controllers, WAP... to build LAN & WLAN systems for hotels.
* Evaluate necessary security solutions for the hotel network environment such as firewall, IPS, encryption... to ensure information security.
* Build comprehensive network solutions, meeting connection, speed, reliability and security requirements for hotel operations.

# **CONTENT**

## **CHAPTER I: THEORETICAL BASIS OF THE THESIS**

### ***Basic knowledge of computer networks***

**7-layer OSI model:**

The OSI (Open Systems Interconnection) model is a way of structuring a network system into 7 layers to understand and manage computer networks. Each class has separate functions:

|  |  |  |  |
| --- | --- | --- | --- |
| **Layer** | **Name** | **Function** | **Example Protocols** |
| 7 | Application | Provides application services and interacts with end-users. | HTTP, FTP, SMTP, Telnet |
| 6 | Presentation | Ensures data format compatibility and handles data encryption/decryption. | JPEG, SSL/TLS |
| 5 | Session | Manages session connections between networked computers. | NetBIOS, RPC |
| 4 | Transport | Ensures reliable communication between devices. | TCP, UDP |
| 3 | Network | Routes data, manages IP addresses, and subnetworks. | IP, ICMP |
| 2 | Data Link | Manages access to the networking medium and error detection. | Ethernet, Wi-Fi (802.11) |
| 1 | Physical | Ensures the physical transmission of data through the medium | Ethernet, USB |

**Popular network protocols:**

|  |  |  |
| --- | --- | --- |
| **Protocol** | **Function** | **Operation** |
| TCP/IP (Transmission Control Protocol/Internet Protocol) | Ensures reliable data transmission over the network. | - Divides data into packets. - Checks for errors in packets. - Ensures packets reach their destination by reordering and confirming transactions between source and destination computers. |
| FTP (File Transfer Protocol) | Allows file transfer between a computer and a server. | - Establishes a connection with an FTP server. - Logs into the server with a username and password. - Manages files on the server (upload, download, delete). - Transfers files between a computer and the server via FTP connection. |
| SMTP (Simple Mail Transfer Protocol) | Sends emails. | - Transfers emails between email servers. - Uses SMTP commands to format and send emails. - Relies on TCP/IP for reliable email transmission. |
| Telnet | Enables remote login and control of computers or network devices. | - Establishes remote connections with a computer or network device. - Sends remote commands and data to control and manage the target device or computer. |
| HTTP (Hypertext Transfer Protocol) | Allows web browsing and access to web pages. | - Sends HTTP requests from a web browser to a web server. - The web server receives the request, processes it, and sends the corresponding web page and data back to the browser. - Data is transmitted via the HTTP protocol over a TCP/IP connection. |

**Network devices:**

|  |  |  |
| --- | --- | --- |
| Device | Function | Characteristics |
| Switch | Connects network devices within a LAN, performs switching based on MAC addresses. | - Operates at Layer 2 (Data Link Layer). |
| Firewall | Protects the network from external threats, controls data flow. | - Capable of packet filtering, user authentication, and access rule management. |
| Access Point | Connects wireless devices (such as computers and phones) to a WLAN. | - Typically operates at Layer 2 or Layer 3 and supports Wi-Fi. |

**Concepts in TCP/IP networks:**

* Subnet Mask: A string of bits or decimal numbers that defines the range of a subnet within a subnet.
* Gateway: Device or computer that represents the gateway to the external network and allows devices on the internal network to access the external network.
* Broadcast: Packet sent to all devices on the network, often used to send notifications or search for devices on a LAN.

**Distinguish between types of networks**

* LAN (Local Area Network): Local area network, limited range in an area such as an office or building.
* WLAN (Wireless Local Area Network): Wireless local area network, uses Wi-Fi to connect wireless devices within a specific range.
* WAN (Wide Area Network): A large network, spanning large distances, usually a network connecting many different geographical locations.
* VLAN (Virtual Local Area Network): Virtual LAN, allowing the LAN to be divided into many virtual segments, helping to manage and secure data more effectively.

### ***Knowledge of LAN network design***

**LAN network design principles:**

LAN network design needs to follow some important principles to ensure efficiency and optimization:

* Simplicity: Design your network to be simple and easy to manage. Avoid unnecessary complexity, as it can lead to problems and is difficult to manage.
* Efficiency: The network needs to operate efficiently, with enough bandwidth to meet the needs of users and applications. Make sure that the network is stable and does not experience a lot of congestion.
* Ease of scalability: Design the network with easy scalability so it can adapt to change and scale as needed.
* Cost optimization: Ensure that the network design is cost-optimized, not using too many unnecessary resources.

**Steps to design a LAN:**

* Survey: Collect information about network needs, including number of devices, applications, and Internet connections.
* Requirements Analysis: Investigate and analyze specific network requirements, including bandwidth, security, and scalability.
* Logical - Physical Topology design: Determine the logical structure of the network (VLAN, IP addressing) and physical structure (location of devices, network cables, switches).
* Device selection: Select network devices such as switches, firewalls, and access points based on design requirements.

**Detailed knowledge about VLAN configuration, trunking, spanning tree on Cisco switches:**

VLAN (Virtual Local Area Network): Divides the LAN into virtual segments for data management and security. On Cisco switches, configure VLANs with the "vlan [ID]" command and assign ports to the corresponding VLAN

Trunking: Connecting switches to allow VLANs to communicate over the network. Use IEEE 802.1Q protocol to mark data frames as belonging to specific VLANs.

Spanning Tree: Ensures there are no loops in the network to avoid sending infinite packets in the network. Use Spanning Tree Protocol (STP) to create a closed tree and ensure there is a single path between switches.

**Configure DHCP server to automatically allocate IP addresses:**

Configure a DHCP server to automatically allocate IP addresses to devices on the network. On the DHCP server (usually running on a server), you will configure the IP address range, network options, and address lease period.

**NAT to translate internal IP addresses and share Internet connections:**

Network Address Translation (NAT) is used to convert a LAN's internal IP address into a public IP address so that an Internet connection can be shared. Configure NAT on a firewall to do this.

### ***Knowledge of security and network safety***

**RADIUS, TACACS+ authentication in the network:**

|  |  |  |
| --- | --- | --- |
|  | RADIUS | TACACS+ |
| Function | Used to authenticate and manage user access to the network. | Provides access control and user authentication to network devices. |
| How it works | When a user tries to connect, authentication information is sent to the RADIUS server. The RADIUS server checks and allows or denies access based on credentials. | TACACS+ handles authentication, authorization, and detailed logging of every user behavior. TACACS+ provides a higher level of control and integration with user management and authorization systems in network environments. |

**WEP, WPA2 encryption protocols for wireless networks**

|  |  |  |  |
| --- | --- | --- | --- |
| Encryption Method | Function | Disadvantages | Advantages |
| WEP (Wired Equivalent Privacy) | Used to encrypt data in a wireless network to protect it from unauthorized access. | WEP has serious security vulnerabilities and is no longer considered safe. |  |
| WPA2 | Uses AES (Advanced Encryption Standard) encryption to provide higher security than WPA. |  | WPA2 is considered one of the best security methods for Wi-Fi networks. |

**Firewall: Defines ACLs and network access control policies**

Firewall is a security system used to control and monitor data flow between internal and external networks. To define ACLs (Access Control Lists) and network access control policies, you define rules to manage how data is accessed and forwarded through the firewall. This includes deciding what is allowed and what is denied based on IP address, port, protocol, and other factors.

**Methods to prevent intrusion and network attacks:**

* IDS (Intrusion Detection System):
  + Function: Monitor network activity to detect intrusions or attacks.
  + How it works: IDS uses rules and signatures to detect intrusion patterns or unusual behavior.
* IPS (Intrusion Prevention System):
  + Function: Prevent intrusions and network attacks immediately after detection.
  + How it works: IPS not only detects but also prevents intrusions by blocking data flows or specific attacks.
* Firewall: As mentioned above, a firewall can prevent unwanted connections and control network access to ensure safety.
* Data encryption: Use data encryption to protect important information from unauthorized access.

### ***Knowledge of WLAN wireless networks***

**WiFi 802.11a/b/g/n/ac standards: Speed, Operating frequency**

|  |  |  |
| --- | --- | --- |
| Wi-Fi Standard | Maximum Speed | Operating Frequency |
| 802.11a | 54 Mbps | 5 GHz |
| 802.11b | 11 Mbps | 2.4 GHz |
| 802.11g | 54 Mbps | 2.4 GHz |
| 802.11n | 600 Mbps Both | 2.4 GHz and 5 GHz |
| 802.11ac | Hundreds of Mbps to more than 1 Gbps | Primarily at 5 GHz, usable at 2.4 GHz |

**WLAN design process: Survey, Location selection, AP installation**

* Survey:
  + Investigate requirements: Determine bandwidth needs, number of devices, and installation locations.
  + Determine the frequency: Choose the appropriate frequency band (2.4 GHz or 5 GHz) based on the environment and current situation.
  + Check for noise: Evaluate sources of noise that may affect the signal.
* Select location:
  + Determine AP location: Place Access Points (AP) so that the signal can cover evenly and meet the requirements.
  + Determine the number of APs: Based on the area to be covered and the number of connected devices.
* AP settings:
  + AP Setup: Configure SSID, password, encryption, and network settings.
  + AP Connection: Connect the AP to the LAN and configure it to operate as required.

**Configure SSID, Encryption, Delegate access rights for WLAN**

* SSID (Service Set Identifier):
  + The SSID is the name of the Wi-Fi network and makes the network easily identifiable.
  + Configure the SSID to name the network and identify hidden or visible networks.
* Encode:
  + Encryption protects data in the WLAN from unauthorized access.
  + Encryption methods include WEP, WPA, and WPA2. WPA2 is popular because of its high security.
* Access permissions:
  + Set access permissions: Determine which users or devices are allowed to access the network and where.
  + Use permissions to control role-based network access and sharing.

**Basic knowledge of Access Point operations and working modes**

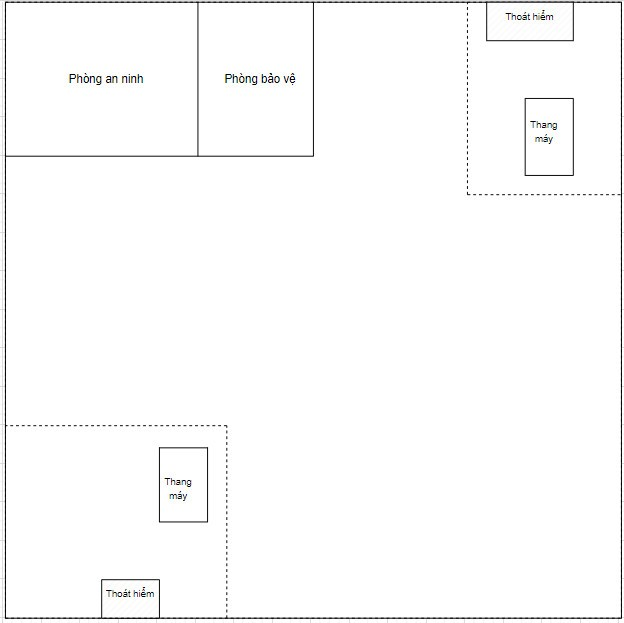
* Access Point (AP) operations:
  + AP is a device that broadcasts Wi-Fi signals to connected wireless devices.
  + The AP transfers data between wireless devices and a wired network (LAN).
* AP working mode:
  + Access Point (AP) mode: In this mode, the AP acts as a Wi-Fi hotspot to connect wireless devices to a wired network (LAN).
  + Repeater (Bridging) mode: The AP can be configured to act as a signal amplifier (repeater) or bridge (bridge) to extend Wi-Fi coverage.
  + Client mode (Wireless Client): In this mode, the AP is configured to connect to another AP as a wireless device, allowing devices without Wi-Fi capabilities to connect to the wireless network. .
  + Mesh Mode (Mesh Networking): Mesh mode is a self-organizing wireless network system in which APs connect to each other to create a large coverage network.
  + WDS (Wireless Distribution System) mode: WDS allows APs to connect to each other wirelessly to expand the wireless network or create wireless mesh networks.

## **CHAPTER 2: DESIGN NETWORK INFRASTRUCTURE FOR 5-STAR HOTELS**

## **2.1 Analyze the design of the project**

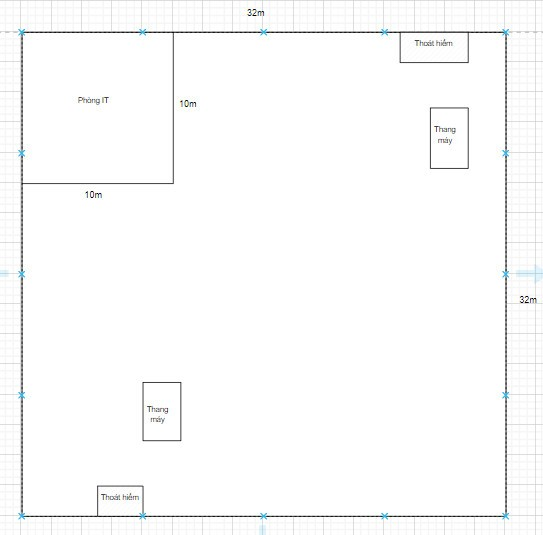
The hotel is designed with careful organization and detail to meet the diverse needs of customers, providing a classy and comfortable stay experience. Below is an in-depth analysis of each floor and space in the building:

Starting from the basement, this is a space mainly planned to meet the needs of parking and technical security. It not only ensures safety but is also an important place to maintain stable operations of the entire hotel.

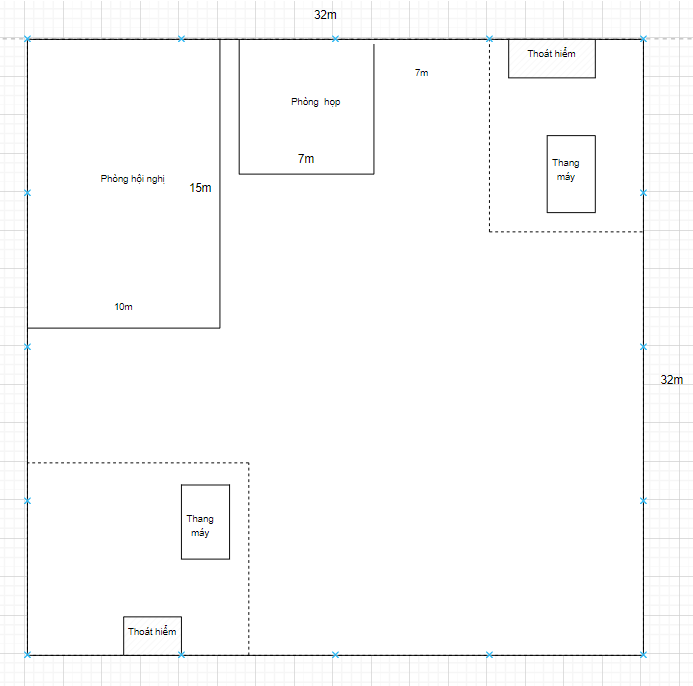


***The Basement***

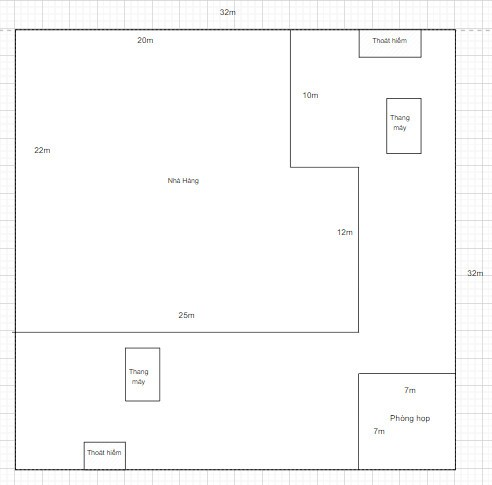
Next is the ground floor, which has an impressive height of 6 meters and is divided into a reception area and IT room. This height creates an open and comfortable space, while also creating a highlight for the hotel's luxury and impression.



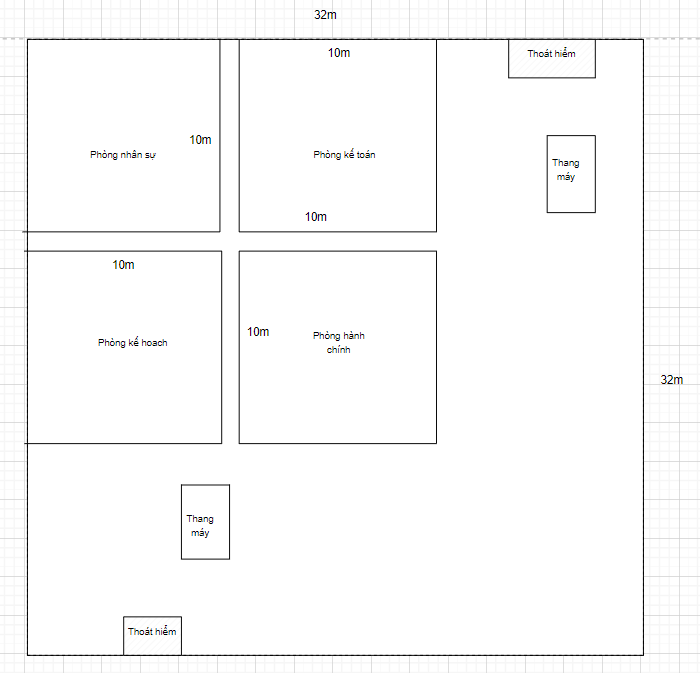
***The ground floor***

The first floor of the hotel is reserved for staff meeting rooms with a capacity of 50 people in 50 square meters and conferences up to 300 square meters, enough room for 200 people. The function of this space is to serve internal events, providing optimal amenities for meetings and conferences.

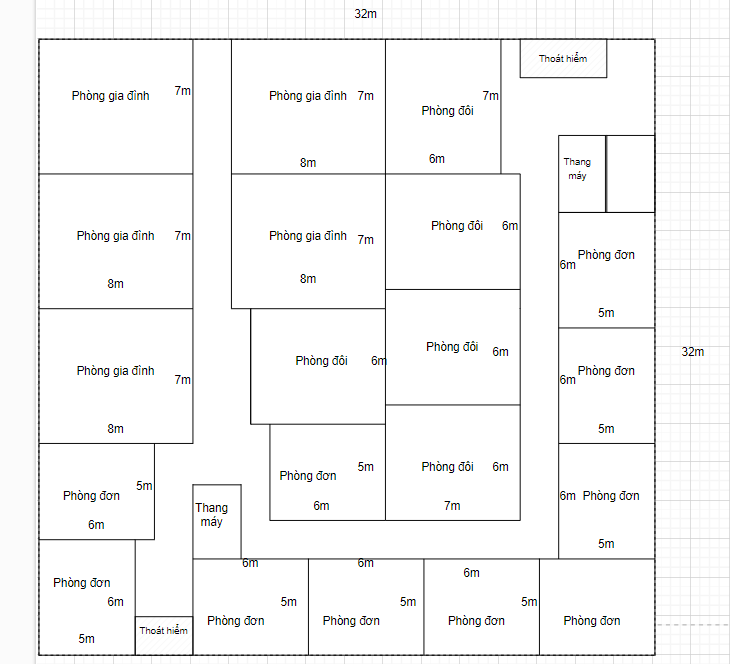
***The first floor***

Moving to the 2nd floor, you will encounter a restaurant area with an area of up to 500 square meters and other services, providing a cozy and comfortable atmosphere for customers to enjoy cuisine andentertainment.

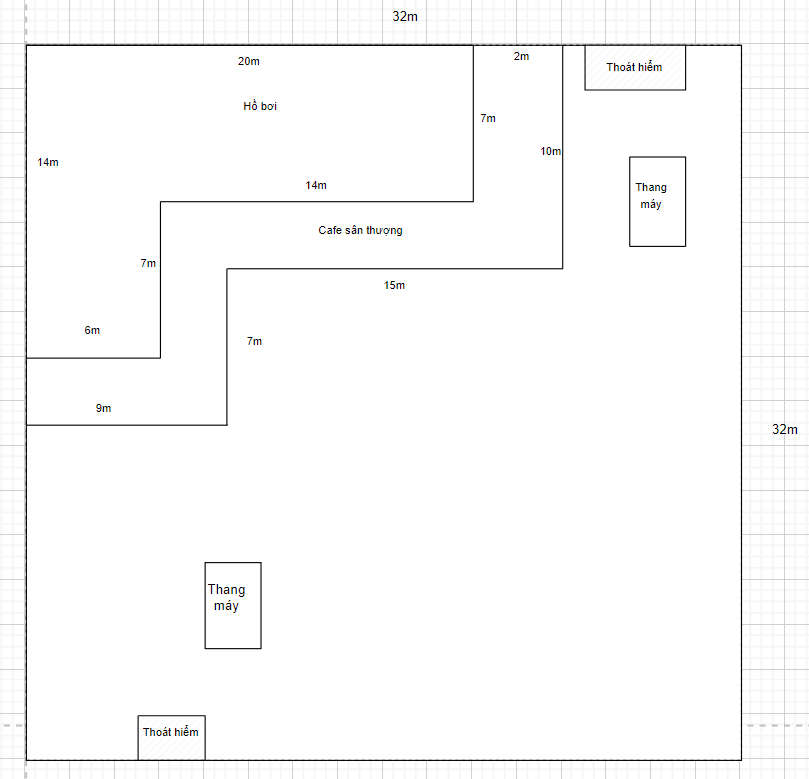
***The second floor***

The 3rd floor is reserved for employees, including offices for accountants, managers, directors, and administrative departments. This helps create a professionally focused and supportive space.

***The third floor***

From floors 4 to 10, each floor has an area of 1000 square meters, divided into a main lobby with a total of 20 rooms. Each of these floors offers flexibility to guests with 10 single rooms (30m²), 5 double rooms (40m²), and 5 family rooms (50m²).

***From 4th floor and up***

The hotel's rooftop terrace is a special feature, where there is a swimming pool and a rooftop cafe. This is a great entertainment space, bringing a relaxing and enjoyable experience to customers, while also creating an interesting highlight for the overall architecture of the hotel.

***The rooftop***

## 2.2 Requirements analysis

* The guest network must be separate from the internal network using VLAN technology to divide the **internal network** and **public network** internal network address with network address 192.168.0.0/16 (InteralVLAN) public network address 172.168. 0.0/16 (ExternalVLAN). Allows access to the internet via Viettel provider using a router to connect the internal network to the external network. Ensure network security with a firewall to manage access from the Internet
  + - Each department uses a separate VLAN
      * VLAN\_Personal 192.168.0.0
      * VLAN\_accountant 192.168.10.0
      * VLAN\_Plan 192.168.20.0
      * VLAN\_administrative 192.168.30.0
      * VLAN\_IT 192.168.40.0(responsible for maintaining computers and software in the hotel)
      * VLAN\_meeting hop room 192.168.50.0
    - The technical department is responsible for server management, network security and direct connection to the server on the same network as the server with address 1.1.1.0 also with DNS, WEB, IoT server room with address 1.1.1.0
    - Security room connects to surveillance cameras on the same network with VLAN 10.10.10.0
    - The conference room accesses the public network and a computer connects to the internal network in the same VLAN as the meeting room
    - Provide enough bandwidth for all users in the hotel. The hotel has 7 floors for guests, each floor accommodates a maximum of 60 guests. So there are about 420 guests including staff, the hotel has about 200 staff There are a total of about 620 visitors, including personal devices, about 700 accesses. If these 700 people access and send a 0.1MB email, there will be 700\*0.1MB/1s=70MBs, so we get 100MBs of bandwidth.
    - Ensure a backup plan for the internal network
* Data Backup: Perform periodic backups of important network data such as network configuration, databases, and important documents. Backups can be stored across multiple devices or the cloud to ensure data is available when needed.
* Redundant devices: For primary network devices such as routers, switches, servers, use redundant devices to ensure that the network remains operational when one device fails crash.
* Ensure coverage for access points
* Location of access points: Choose the location of access points to ensure wide and uniform coverage throughout the hotel. Access points should be placed in strategic locations such as the ceiling, near the door, or near areas where many customers use the network such as halls, restaurants, and reception areas. We use an access point (AP) using Wi-Fi 802.11ac technology, operating at 2.4GHz frequency. This AP is equipped with an integrated antenna and has a maximum transmit power of 20dBm. The physical environment is an open space, without major obstacles, the coverage range of this access point can reach about 30 to 50 meters in the open space, where each floor is wide, placing the access points at different locations. central location and use relay technology (repeater/extender) to extend coverage using load management techniques such as channel division, rate limiting, and load balancing between APs to ensure every user receives good access speeds.
* Limit clashes

VLANs (Virtual Local Area Networks) divide networks, minimizing collisions by allowing direct communication within segments and restricting communication between them without a router or switch.

* **Data Segregation:** VLANs facilitate the separation of data between departments or floors, enhancing security by preventing unauthorized access.

## **Collision Reduction:** Network segmentation lowers the risk of collisions. Devices within the same VLAN communicate directly, averting conflicts with devices in other VLANs.

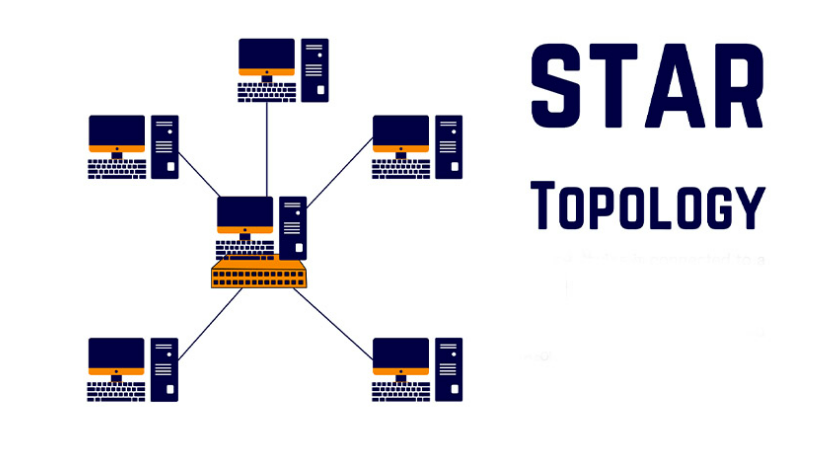
## **Flexible Management:** VLANs allow for agile network management, dividing the network into smaller, manageable segments. Each VLAN can have distinct rules, policies, and configurations, enhancing overall flexibility.

## 2.3 Determine network structure

The hotel's LAN network will be organized as follows:

* On each floor there will be a Switch connected to a central swith switch located on floor 5 to ensure the length of the switch cape is saved, connecting directly to a server room switch and connecting to the internet via a router and a Firewall. The ports on the central Switch are configured for each VLAN, and there is a DHCP service that automatically assigns IP addresses to separate servers with static IPs for ease of management.
* There is a backup switch of the central switch to ensure safety in case of physical problems. This room switch is configured exactly the same as the main one and is pre-wired to the branch switches.
* Network devices are connected by fiber optic cables and there is a backup cable for each wire. This backup cable is installed in parallel with the main cable in case the main cable is broken or physically damaged.
* In this design we do not use routers but use VLAN technology to divide the network

## 2.4 Select network equipment and estimate costs



**Advantage:**

- Star architecture provides resources and centralized management. When a cable segment is damaged, it only affects the machine using that cable segment, the network still operates normally.

- This architecture helps us easily expand the network when required.

- Easy administration and maintenance (because the network is designed according to a centralized processing model).

**Disavantage:**

- Using multiple cables requires finding a good centralized connection device to avoid damage.

- It is necessary to have a skilled technical team to ensure that network management needs are met.

->Because the star network has many outstanding advantages, it is widely used in real life international

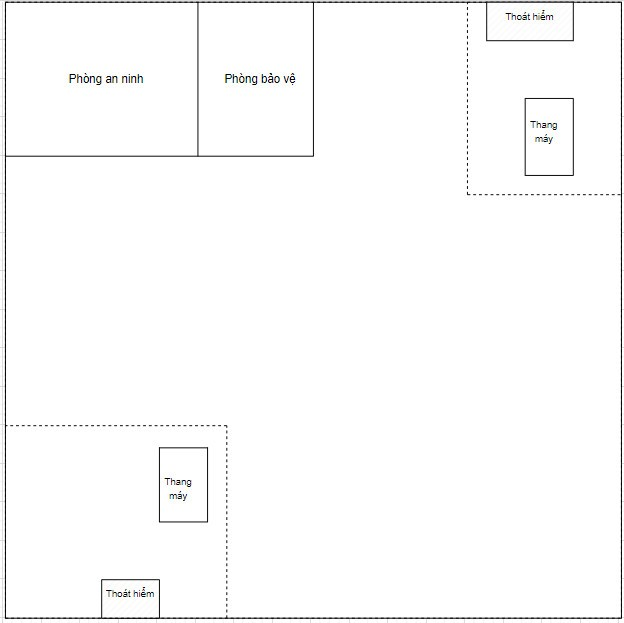
cab: the central switch is located on the 5th floor so the longest wire is the wire connecting from the central switch to the basement switch.

* From basement to 5th floor: 26m so the cable length must definitely be greater than 26m
* From the ground floor to the 5th floor is: 20 meters so the cab must be larger than 22 meters
* From 1st floor to 5th floor is: 16m
* From the 2nd floor to the 5th floor is 12m
* From 3rd floor to 5th floor is 8m
* From the 4th floor to the 5th floor is 4 meters
* From the 5th floor to the 6th floor is 4m
* From 5th floor to 7th floor is 8 m
* From 5th floor to 8th floor is 12m
* From 5th floor to 9th floor is 16m
* From the 5th floor to the 10th floor is 20m

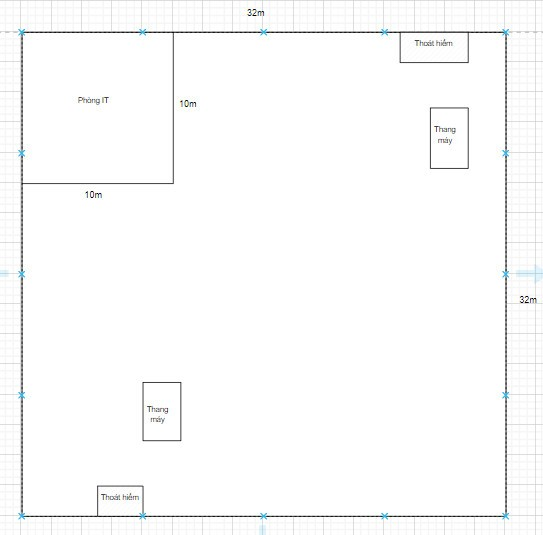
=> 26+20+16+12+8+4+4+8+12+16+20=146m minimum cab to connect Switches to Switch center.

We use Single-mode (suitable for longer transmission distances, often used in large enterprise environments. However, SM cables require laser lights that cost more)

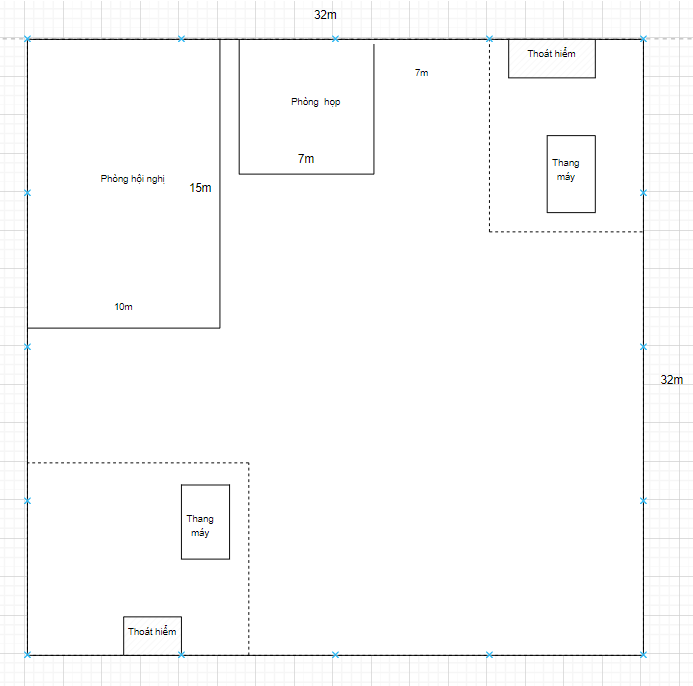
## 2.5 Build a simulated network

***************The basement***

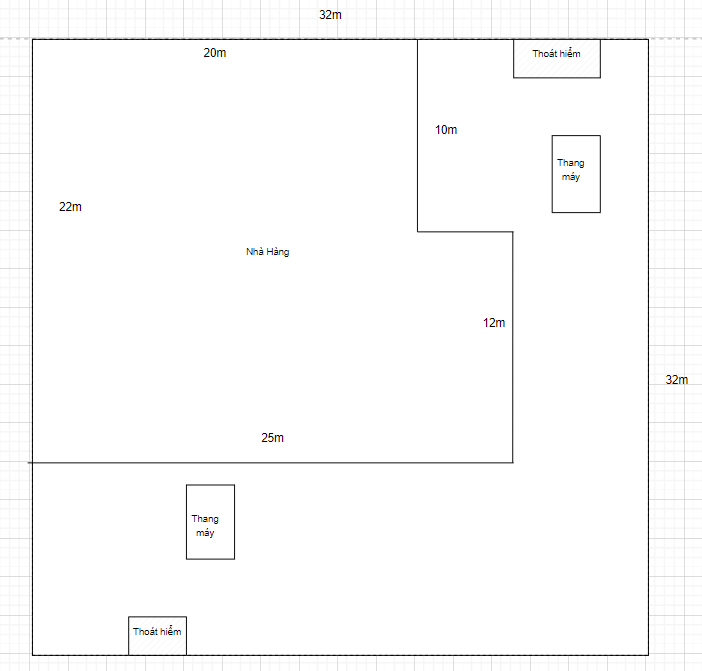
The security room will include 2 servers, 10 computers and 1 access point for network security, and a security room to monitor cameras of the entire hotel. The switch of this floor will connect to the main switch of the floor 5

*********The ground floor***

 On the ground floor , the switch will similarly connect to the main switch on floor 5, the access point will be configured with VLAN address 40 for the IT department, to create internal security and optimize resources.

*********The first floor***

Similar to the first floor with the meeting room with VLAN address 50. The conference room will use an accesspoint connected to the public network. And in the middle of the first floor there will be an access point to broadcast free wifi

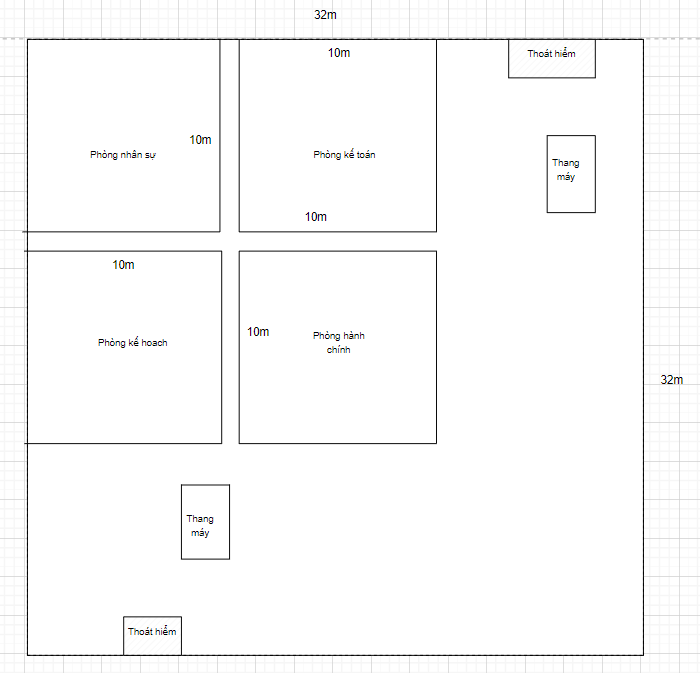
***The second floor***



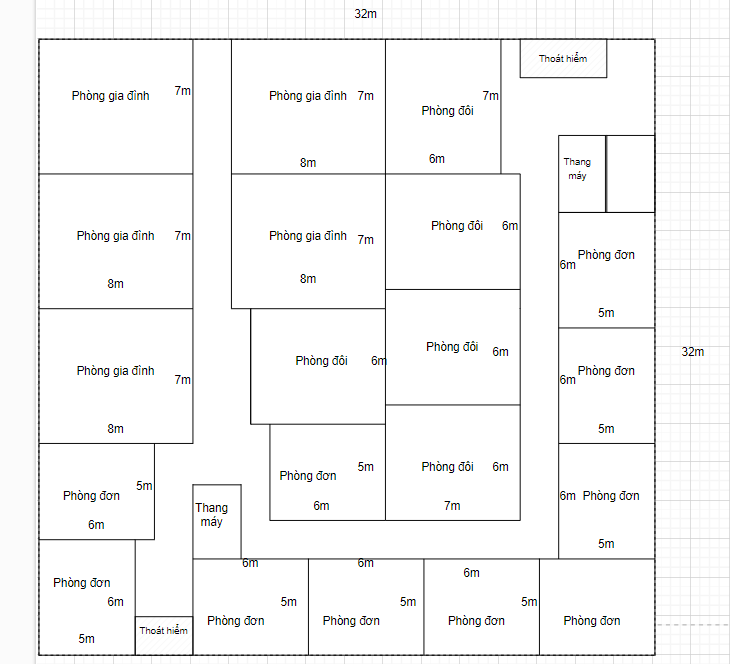




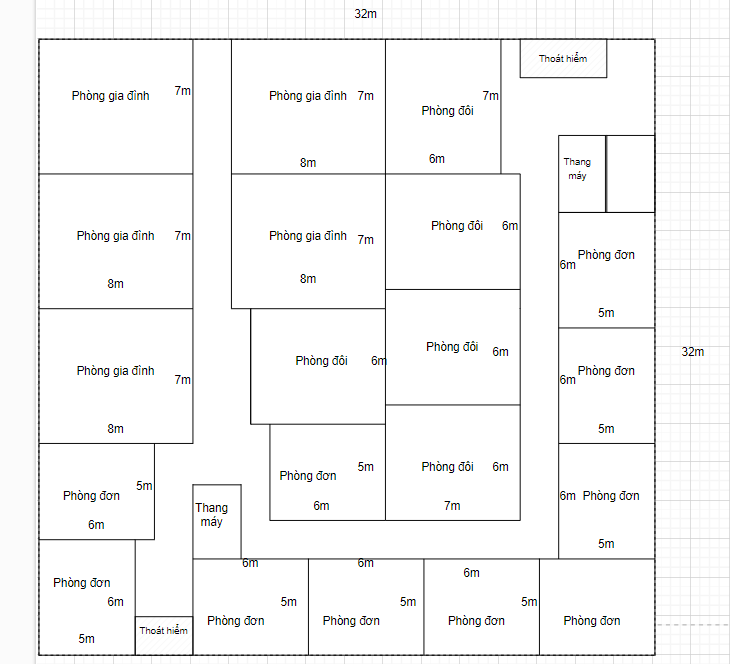
On the 2nd floor, there will be 1 access point in the middle of the restaurant and 1 outside the restaurant to receive the best wifi signal.

****** ***The third floor***

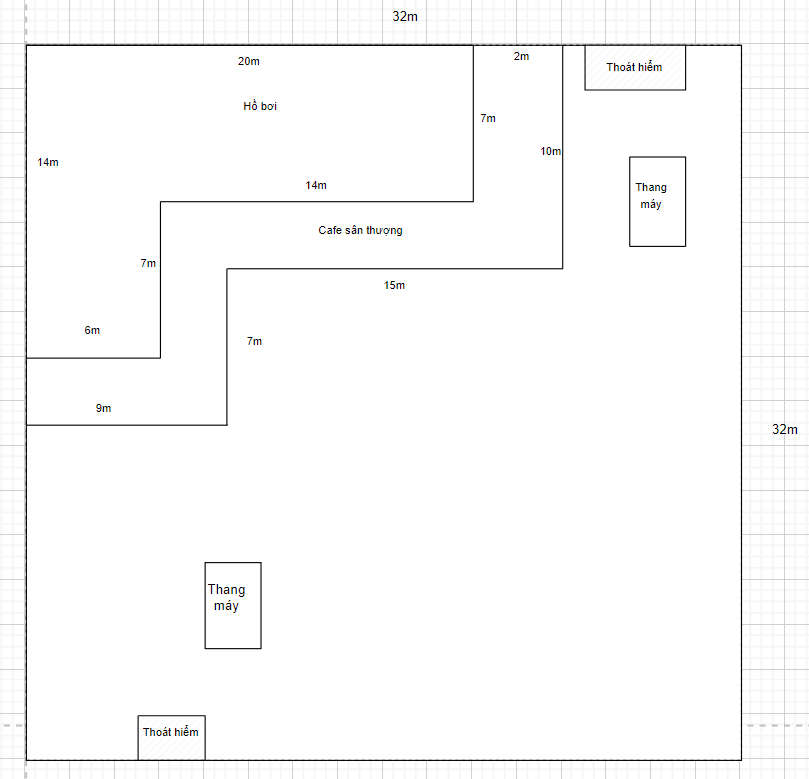
The 3rd floor is divided into 4 departments with different VLAN settings from VLAN 0 - 30 to easily secure information, minimize resource competition and make management easier and 1 access point to broadcast wifi. for guests

 ***The remain floors expect the fifth floor***

From floors 4 to 10, except for floor 5, each floor has 1 switch, 1 access point and 1 repeater to be able to broadcast wifi everywhere, ensuring the signal is always stable and can connected everywhere

*********The fifth***  ***floor*** 

From floor 5, there will be a main switch with a firewall connecting out through the Viettel router. At the same time, the main switch will connect to the switch, the switch will connect to the access point from there to broadcast wifi and there will be a repeater that will absorb wifi to bring wifi to dead spots. A special point is that each room will have a place to plug in a lan cable to be able to serve computers when there is no wifi card

****** ***The rooftop***

For the rooftop, we will use 1 switch and 1 access point to connect to wifi in areas where phones are mainly used.

### ***Necessary equipment:***

* + - 2 Server (1 for primary and 1 for IoT server)
    - 1 firewall 5506-X
    - 2 main Switch 3560-24PS
    - 12 switch 2960-24TT
    - 20 Access Points PT
    - 60 Computer AIO HP Eliteone 840
    - 44 Camera IP Panasonic E-SERIES
    - 30 Repeater AC 1200

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Category | Name | Price(USD) | Quantity | Total |
| Server | SuperStorage Server 6048R-E1CR60L | 16.000 | 2 | 32.000 |
| Switch | WS-C3560-24PS | 3.795 | 2 | 7590 |
| Switch | WS-C2960-24TT-L | 95 | 17 | 16492 |
| Access Points | Cisco 3745 CISCO3745 | 55 | 44 | 2420 |
| Computer | AIO HP Eliteone 840 G9 76N54PA | 1.148.95 | 60 | 6893700 |
| Camera | IP Panasonic E-SERIES | 108 | 59 | 6379 |
| Repeater | AC1200- totolink | 30 | 7 | 210 |

# CONCLUSION

Result:

* Through the steps of learning about the hotel structure, analyze the required capacity of the hotel
* Choose the network architecture type, draw models between layers
* Create different VLANs in a network with many applications, to achieve the goal of dividing the physical network into independent management and operation units.
* Provide ways to limit wifi signal overlap
* Understand more about the network system and the necessary equipment current network user needs.

# **REFERENCE**

* Network Analysis, Architecture, and Design(James D. McCabe)
* Cisco - Campus Network Design Fundamentals.2005
* Amazon.com
* Wikipedia