

ASSIGNMENT FRONT SHEET

Qualification	BTEC Level 5 HND Diploma in Computing		
Unit number and title	Unit 2: Networking		
Submission date		Date Received 1st submission	
Re-submission Date		Date Received 2nd submission	
Student Name	Nguyễn Chí Thanh	Student ID	BHAF190076
Class		Assessor name	
Student declaration I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.			
		Student's signature	Thanh

Grading grid

[illegible]

⚙ **Summative Feedback:**

⚙ **Resubmission Feedback:**

Grade:

Assessor Signature:

Date:

Signature & Date:

Contents

I. Introduce.....	5
II. Examine networking principles and their protocols(p1)	5
1. Discuss the benefits and constraints of different network types and standards.	5
a. The benefits and constraints of different types of networks.....	5
♦ Local Area Network (LAN)	6
♦ Metropolitan area network (MAN)	7
♦ Wide Area Network (WAN)	9
b. Discuss various network standards.....	10

♦ OSI reference model	10
♦ TCP/IP reference model	12
2. Explain the impact of network structure, communication and bandwidth requirements	15
a. Impact of network structure requirements	15
♦ Physical topology	16
STAR topology	16
STAR topology	16
BUS topology	17
RING topology	18
TREE topology	20
MESH topology	20
HYBRID topology	21
♦ Logical topology	22
b. Impact of communication and bandwidth	23
3. Compare common network principles and how efficient protocols allow networked systems	23
a. Compare common network principles	23
b. How protocols allow the efficiency of networked systems	24
♦ TCP and IP	25
♦ UDP	25
♦ Other protocols	25
III. Explain networking devices and operations	26
1. Discuss the operating principles of network devices and server types	26
a. Discuss the operating principles of network devices	26
♦ Repeater	27
Hub	27
Bridge	28
Switch	29
Router	29
Gateway	29
b. Discuss the operational principles of server types	30
2. Explore a variety of server types and demonstrate server selection, considering a certain scenario regarding cost optimization and performance	38
a. Factors to consider when choosing a server	38
b. Select server for business	40
3. Discuss the interdependence of workstation hardware with related network software	41
IV. Design efficient networked systems	42
1. Design a networked system to meet a certain specification	42

a. Request	42
Design plan and expected cost	42
2. Check and evaluate the design to meet the requirements and analyze user feedback.....	46
a. Check and evaluate the design for requirements	46
Check and evaluate costs	46
3. Installing and configuring network services and applications	50
a. Basic configuration.....	50
b. VLAN.....	50
c. DHCP	50
d. Static routing	51
e. NAT	52
f. ACL	52
V. Deploy and diagnose networked systems	53
a. Implement a network based on a prepared design	53
1. Basic configuration.....	53
Set password	54
VLANs	55
Routing between VLANs.....	56
DHCP	57
1. Static routing.	57
4. NAT.....	58
5. Recommend potential enhancements for the networked systems. (M4)	58
VI. Document and analyse test result (p8).....	60
1.SSH protocol.....	60
2.Vlan.....	61
3.DHCP	61
4.Static routing and NAT	62
5.ACl.....	63
VII. Conclude.....	64
VIII. References.....	65

I. Introduce

- In this article, I will explain network principles, protocols, and devices, including the benefits and limitations of network solutions, the impact of network configuration, communication and bandwidth requirements, network system efficiency, the principles of operation of network equipment and server type and network software.
- Furthermore, I will design the network and deploy and diagnose networked systems.

II. Examine networking principles and their protocols(p1)

A network is a series of independent computer systems that are interconnected to exchange data. For this to happen, the networked systems must be properly foreignized. It is then established by special network protocols, such as TCP (Transmission Control Protocol). Even just two computers connected to each other can be classified as a network.

1. Discuss the benefits and constraints of different network types and standards.

a. The benefits and constraints of different types of networks

- A network is set up to transfer data from one system to another or to share resources, such as servers, databases, and printers on the network. Depending on the size and scope of your computer network, you may be able to differentiate different network sizes. The most important types of networks include:

Personal Area Network (PAN)

Local Area Network (LAN)

Urban area network (MAN)

Wide area network (WAN)

Global Area Network (GAN)

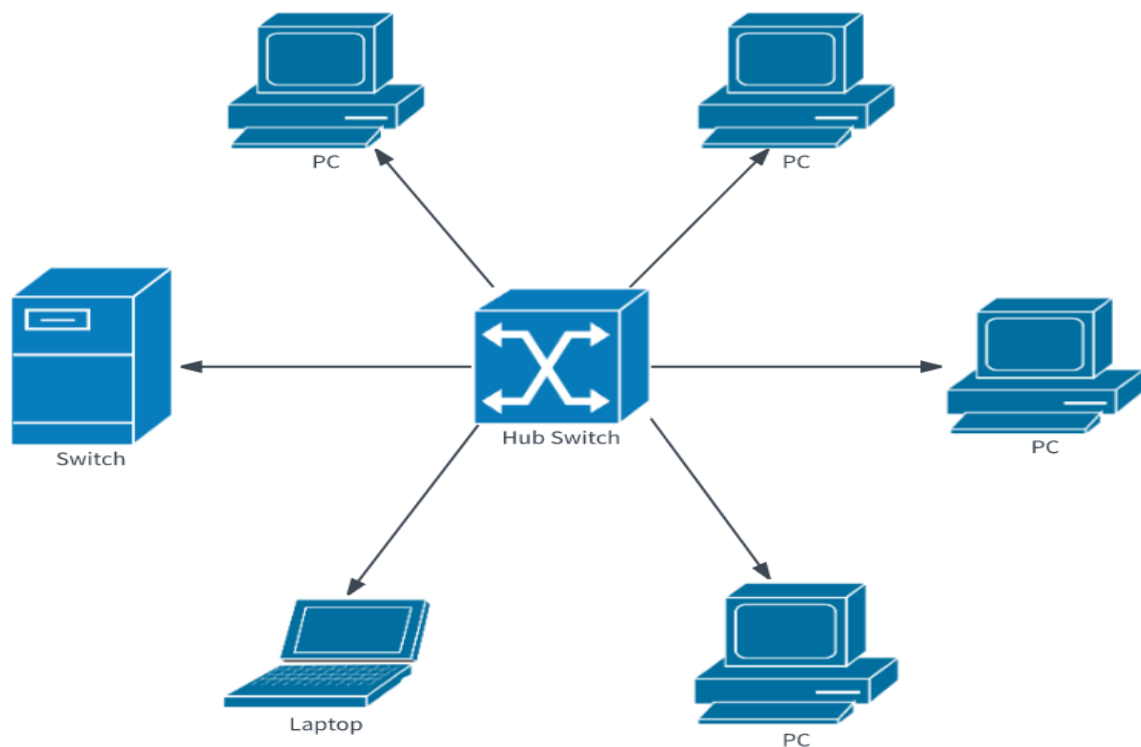
Physical connections based on these types of networks can be connected by cable or made wirelessly. The physical communication network often forms the basis for some logical communication network, known as a virtual private network (VPN). They use an ordinary physical medium, for example fiberglass, when transmitting data and are logically assigned to different virtual networks using tunneling software.

Each type of network is developed for specific areas of application, based on specific techniques and standards, and offers different advantages and disadvantages.

◆ Local Area Network (LAN)

A LAN is a local area network with high speed but short transmission line and can only operate in a certain area: offices, buildings, universities, ... Computers are connected to the assigned network. Available in the form of a server or workstation. LAN works with TCP / IP protocol.

LANs are also divided into two categories that are large LANs and small LANs. For the smallest LAN, it is only used to connect two computers together. By contrast, the largest LAN can connect thousands of computers. LANs are often used to share resources, such as data storage and high bandwidth printers, and can run online applications connected via the network such as conferences, movie projection ... Micro-connections have a relatively small limit but low cost and simple network administration.



LAN Network

Advantages:

-Share resources:

All resources are attached to a network and if any computer needs any resources, it can be shared with the computer needed. Types of resources are DVD drives, printers, scanners, modems and hard drives. Therefore, there is no need to purchase separate resources for each computer and it saves money.

-Relationship between client and server:

All data from the attached computers can be stored in a server. If any computer (client) needs data, that computer user only needs to log in and access data from the server.

-Share on the internet:

In offices and network cafes, we can see that an internet connection is shared between all computers. This is also the type of LAN technology in which the main internet cable is attached to a server and the computers are distributed by the operating system.

-Centralized data:

Data of all network users can be saved on the computer's hard disk. This will help users to use any network workstation to access their data. Because data is not stored on the local workstation. But it is stored on a server computer. Users will access their own data by logging into their account from any client in the network.

-Easy and cheap:

The biggest advantage of a local area network is that it is easy to set up and also cheap compared to other options and therefore, if the company is trying to set up a network at a lower cost and easier than a local area network is the answer. Such companies.

Disadvantages

+ The big disadvantage with LAN is inherent in its name. The "local" area network is only good as far as you can reach with an Ethernet cable or Wi-Fi signal. Simply put, you cannot buy an Ethernet cable that will reach throughout the entire building and the Wi-Fi connection is quickly canceled when you go a few dozen meters further then.

The downside is that the network is slow and when there is a problem on the cable, the entire network will stop working

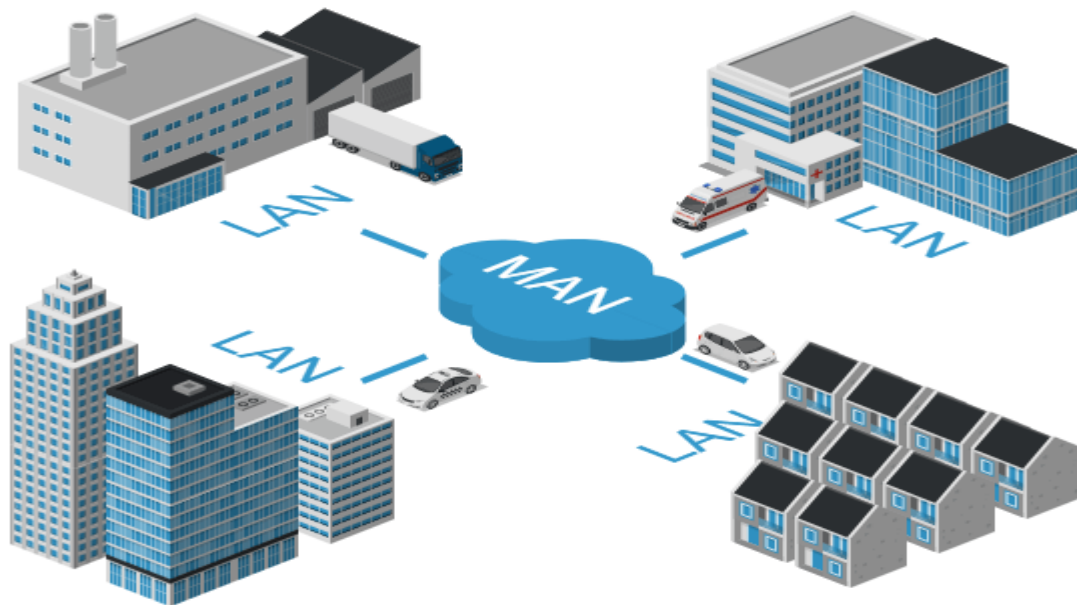
In addition, when there is a problem, it is difficult to check and detect the error, when there is a cable problem, the entire network will stop working and this type of network sign only consumes wires and network equipment. Middlemen are more expensive

♦ Metropolitan area network (MAN)

MAN stands for "Metropolitan Area Network" which is an urban network. The maximum distance between two nodes (nodes) on the MAN network is 100 Km. MAN network is a combination of multiple LANs. The MAN range can cover entire provinces / cities and nationwide.

In addition, a large university may have a very large network that it can be classified as MAN. And MAN networks often exist to provide connectivity to large corporations.

Metropolitan area network (MAN)



Advantages

MAN is capable of creating high-speed connections, up to hundreds of Mb / s, expandable up to 1 Gb / s to: direct work, public administration, exchange information, provide executive services. righteousness, e-commerce development,

Multi-service trend with high bandwidth demand is really becoming an urgent need in big cities like Hanoi, Ho Chi Minh City or industrial zones - high technology. The MAN broadband urban network service will provide customers with a variety of value-added services, bringing significant profits to service providers.

Utilize the Man network with various types of services by maximizing traffic over current bandwidth, diversifying services by offering both existing and new services in the future, increasing capabilities providing services on a large scale to meet future needs.

Disadvantages

Have medium bandwidth to run applications, e-commerce services, applications in the banking system.

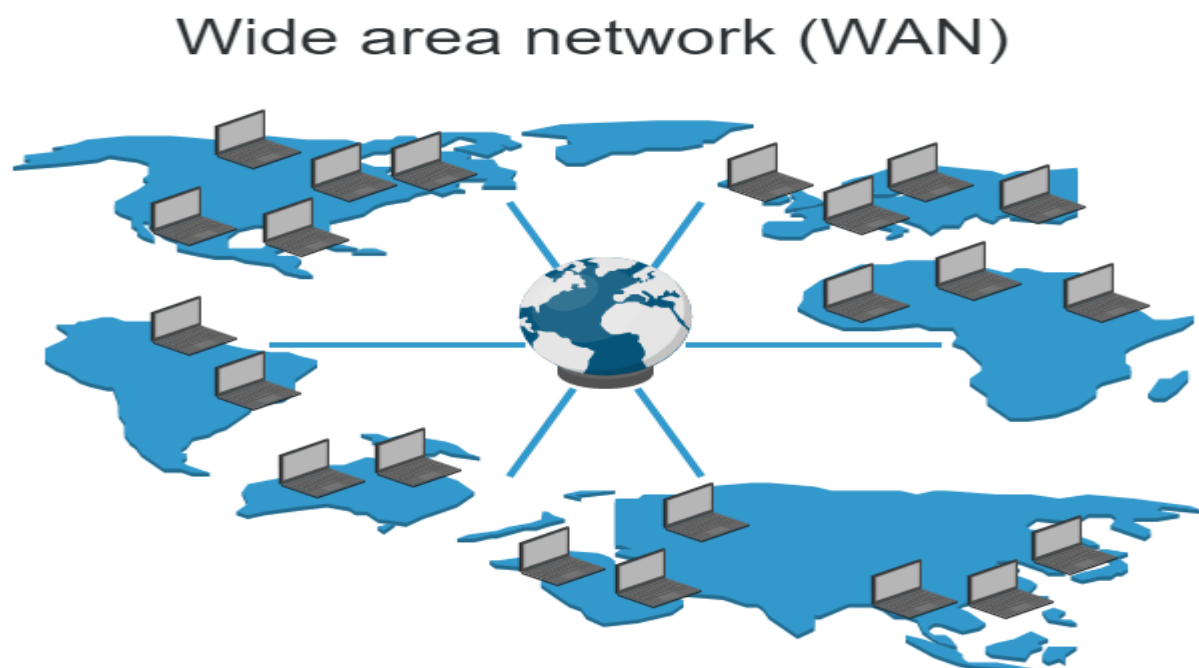
The range of connections is relatively large.

High cost

MAN network administration is more complex.

◆ **Wide Area Network (WAN)**

WAN is a combination of LAN and MAN network connected together through satellite, fiber optic cable or wire cable. This wide area network can both be connected to a private network and can create a large connection, covering an entire country or globally.



Advantages

WANs can be connected to the private network of an organization, or may have to connect across many public network infrastructures and different telecommunications companies.

On the WAN, the information can have different paths, which allows maximum use of the capacity of the transmission line and improves safety in data transmission.

Disadvantages

Low bandwidth so weak connection easily lose connection suitable for applications like E-Mail, Web ...

Wide range of activities, not limited.

Very high cost.

Complex WAN management

b. Discuss various network standards

Network standards define the data communication rules required for the interoperability of network technologies and processes. Standards help create and maintain open markets and allow different suppliers to compete on the basis of the quality of their products while also being compatible with the products currently on the market.

The computers in the network can use different software, hardware, and protocols. In order for two computers to communicate with each other, they need to adhere to certain communication standards. The two standards are:

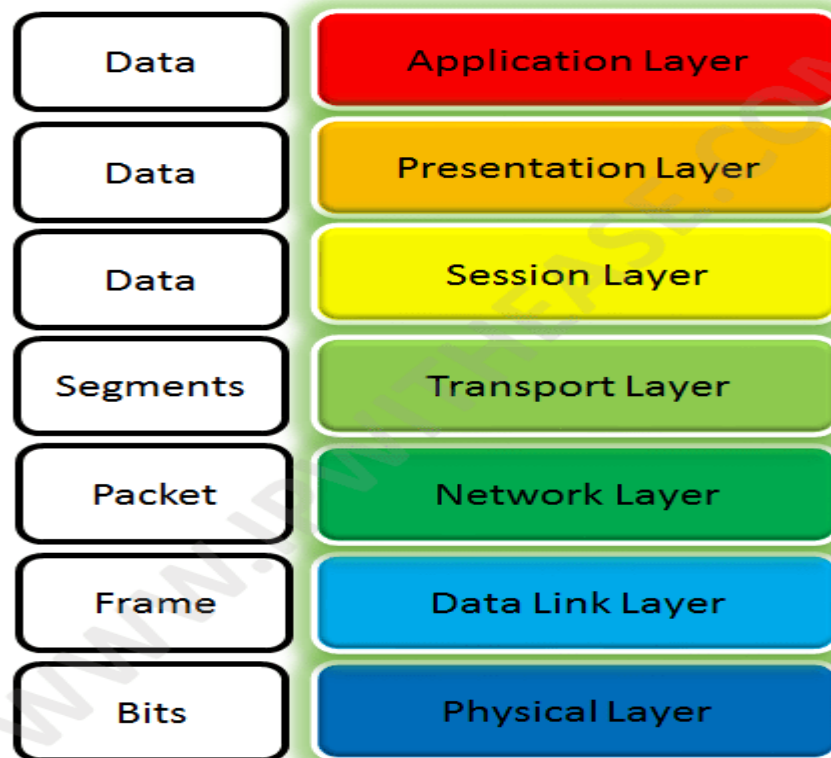
- OSI reference model
- TCP / IP reference model

◆ OSI reference model

The OSI (Open System Connection Model) model is a conceptual framework used to describe the functions of a network system. The OSI model describes computational functions as a set of common rules and requirements that support interoperability between different products and software. In the OSI reference model, communication between a computer system is divided into seven different layers of abstraction: Physics, Data Link, Network, Transport, Session, Presentation, and Application.

Created at a time when network computing was in its infancy, OSI was published in 1984 by the International Organization for Standardization (ISO). Although it doesn't always map directly to specific systems, the OSI Model is still in use today as a means to describe Network Architecture.

The Open System Connection (OSI) model has seven layers. The top layer is the "Application Layer" while the 'lowest' layer in the hierarchy is the Physical layer. The classes in the hierarchy are as follows:



Layer 7: Application Layer: Allows a user (human or software) to interact with an application or network whenever the user chooses to read messages, transfer files, or perform other network-related activities. Web browsers and other internet-connected applications, such as Outlook and Skype, use the Layer 7 application protocol.

Layer 6: Presentation layer: Translates or formats data for the application layer based on semantics or syntax that the application accepts. This layer can also handle the encryption and decryption required by the application layer.

Layer 5: Session layer: Establishing, coordinating and ending conversations between applications. Its services include authentication and reconnection after an interruption. This class determines how long a system will wait for another application to respond. Examples of session layer protocols include X.225, AppleTalk, and Regional Information Protocol (ZIP).

Layer 4: Transport layer: Responsible for transmitting data over the network and providing error checking and data flow control mechanisms. It determines how much data to send, where to send it, and how fast it should be. The transmission control protocol is the best known example of the transport layer.

Layer 3: Network Layer: The main function is to move data into and through other networks. Network layer protocols do this by encapsulating the data with the correct network address information, selecting the appropriate network routes, and forwards the packed data onto the stack to the transport layer.

Layer 2: Data link layer: The protocol layer in the program handles the movement of data in and out of a physical link in the network. This class handles the problems that occur due to bit transmission errors. It ensures that the speed of the data stream does not overwhelm the sending and receiving devices. This layer also allows data transfer to Layer 3, the network layer where it is addressed and routed.

Layer 1: Physical layer: Transfer data by electrical, mechanical or procedural interfaces. This layer is responsible for sending computer bits from one device to another along the network. It defines how physical connections to the network are established and how bits are represented as predictable signals as they are transmitted electrically, electrically, or over radio waves.

Advantages

It is considered a standard model in computer networking.

Supports connectionless and connection-oriented services. Users can leverage connectionless services when they need faster data transfers over the internet and a connection-oriented pattern when they are looking for reliability.

Has flexibility to adapt to many protocols

More adaptive and secure than wrapping all services in one layer.

Disadvantages

Do not define any specific protocol.

The session layer, which is used to manage session and presentation layer, handles user interaction not as useful as other layers in the OSI model.

Some services are replicated in different layers, such as the transport and data link layers, each with an error control mechanism.

Classes cannot operate in parallel; Each class has to wait to receive data from the previous layer.

♦ TCP/IP reference model

The TCP / IP model is the network model used by computer networks today. It was created in the 1970s by DARPA (the Defense Progressive Research Project Agency) as a vendor-neutral, open public network model. Like the OSI reference model, the

TCP / IP model provides general guidelines for the design and implementation of network protocols.

The TCP / IP model has fewer layers than the OSI model, only four layers. These layers describe different network functions and have their own standards and protocols. The classes are:

TCP/IP MODEL	OSI MODEL
Application Layer	Application Layer
Transport Layer	Presentation Layer
Internet Layer	Session Layer
Network Access Layer	Transport Layer
	Network Layer
	Data Link Layer
	Physical Layer

Layer 1: Layer from host to network

Lowest grade of all.

Protocol is used to connect to the server, so that packets can be sent over it.

Change from host to host and network to network.

Layer 2: Internet layer

Selecting a packet switched network based on the network layer that does not connect to it is called the internet layer.

It is the layer that holds the whole architecture together.

It helps the packet move independently to its destination.

The order in which packets are received differs from the way they are sent.

IP (Internet Protocol) is used in this class.

The different functions performed by the Internet Layer are:

- +Provide IP package
- +Perform routing

+Avoid bottlenecks

Layer 3: Transport layer

It determines whether data transmission should be in parallel or single line.

Functions such as multiplexing, segmenting or splitting data are performed by the transport layer.

Applications can read and write to the transport layer.

The transport class adds header information to the data.

The transport layer breaks the messages (data) down into small units so that they are processed more efficiently by the network layer.

The transport layer also sorts the sent packets in order.

Layer 4: Application layer

The TCP / IP specifications describe a lot of applications at the top of the protocol stack. Some of them are TELNET, FTP, SMTP, DNS, etc.

TELNET is a two-way communication protocol that allows connecting to a remote computer and running applications on it.

FTP (File Transfer Protocol) is a protocol that allows file transfer between users of computers connected over a network. It is reliable, simple and effective.

SMTP (Simple Mail Transport Protocol) is a protocol used to transport email messages between source and destination, oriented through a route.

DNS (Domain Name Server) resolves the IP address to a textual address for the Host that is connected to the network.

It allows peer-to-peer entities to initiate a conversation.

It defines two end-to-end protocols: TCP and UDP

+**TCP** (Transmission Control Protocol): A reliable connection-oriented protocol that processes the byte stream from source to destination without error and controls the flow.

+**UDP** (User-Datagram Protocol): An unreliable little connection protocol that doesn't want TCP, sequencing, and flow control. Example: Type of service that responds to a one-time request.

Advantages

It helps you to establish / establish connections between different types of computers.

It works independently of the operating system.

It supports many routing protocols.

It allows internet connection between organizations.

The TCP / IP model has a highly scalable client-server architecture.

It can work independently.

Supports several routing protocols.

It can be used to establish a connection between two computers.

Disadvantages

TCP / IP is a complex model to set up and manage.

The exhaustion / cost of TCP / IP is higher than that of IPX (Internetwork Packet Exchange).

In this, transport layer modeling does not guarantee distribution of packets.

Replacing protocols in TCP / IP is not easy.

It has no clear separation from its services, interfaces, and protocols.

2. Explain the impact of network structure, communication and bandwidth requirements

a. Impact of network structure requirements

Network topology refers to how the various nodes, devices, and connections on your network are physically or logically arranged in relationship to each other. Think of your network as a city and your topology as a road map. And there are many ways to organize and maintain a city - for example, making sure boulevards and boulevards can facilitate travel between areas of town that get the most traffic. There are several ways to organize a network. Each has pros and cons, and depending on your company's needs, certain arrangements can give you a higher level of connectivity and security.

There are two approaches to network topology: physical and logical. The physical network topology, as the name suggests, refers to the physical connections and connections between nodes and networks - wires, cables, etc. A slightly more abstract and strategic network topology, refers to a conceptual understanding of how and why the network is arranged in its way, and how data moves through it.

◆ Physical topology

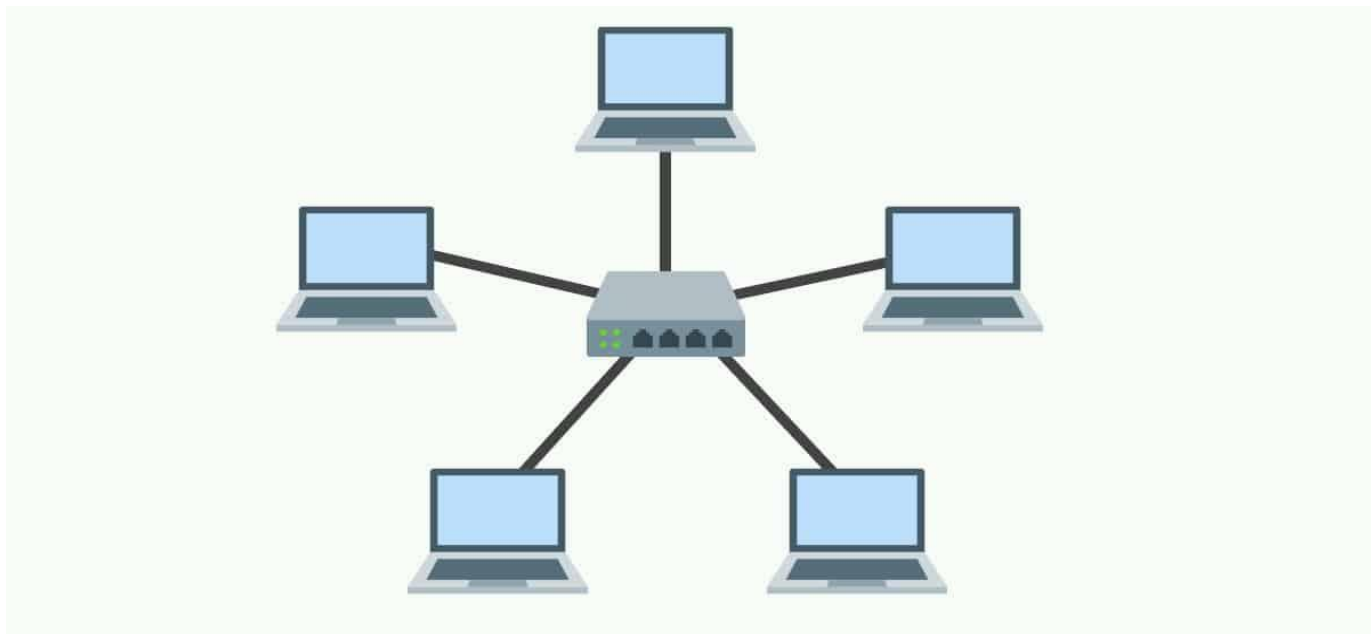
Physical network topology refers to the actual connections (wires, cables, etc.) in terms of how networks are arranged. Setup, maintenance, and provision tasks require detailed physical network information.

There are 6 different types of physical topologies:

- + BUS topology
- + RING topology
- + STAR topology
- + MESH topology
- + TREE topology
- + HYBRID topology

STAR topology

The star topology, the most common network topology, is set up so that every node in the network is connected directly to a central hub via coax, twisted-pair or optical. Acting as a server, this central node manages the data transmission - since information sent from any node on the network must go through the central node to reach the destination - and act as a repeater, helping to prevent data loss.



STAR topology

Advantages

Star topologies are very popular because they allow you to conveniently manage your entire network from a single location. Because each node is connected independently of the center, if one node goes down, the rest of the network will continue to function unaffected, making the star topology a layout. stable and secure network.

In addition, you can add, delete and modify devices without connecting the entire network.

Physically, the topology of the star topology uses relatively few cables to connect the entire network, allowing for both simple setup and management over time as the network expands or contracts. The simplicity of the network design also makes the life of administrators easier as it is easy to locate errors or performance issues.

Disadvantages

On the other hand, if the hub has malfunction, the rest of the network cannot function. But if the center is properly managed and kept in good condition, the administrators won't have too many problems.

The overall bandwidth and network performance are also limited by the central node configuration and specifications, making the star topology expensive to set up and operate.

BUS topology

The bus topology directs all of the devices on the network along a cable that runs in a single direction from one end to the other end of the network - which is why it is sometimes referred to as a "topology. sugar bonds "or" spine topology ". The data flow on the network also follows the cable's route, moving in one direction.



Advantages

A bus topology is a good, cost-effective option for smaller networks because of its simple layout, allowing all devices to be connected via a single coax or RJ45 cable. If necessary, multiple nodes can be easily added to the network by connecting additional cables.

Disadvantages

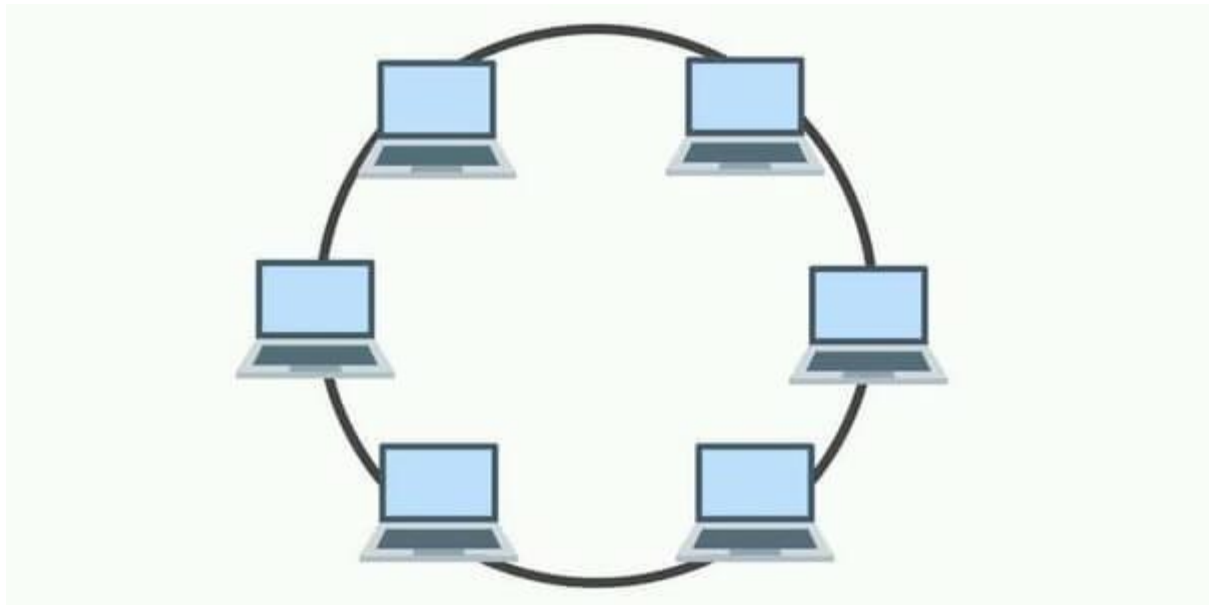
However, since the bus topology uses a single cable to transmit data, they are somewhat vulnerable. If the cable goes down, the entire network will be damaged, restoring can be time consuming and costly, which can cause less problems with smaller networks.

The bus topology is best suited for small networks because there is only so much bandwidth and any additional nodes will slow down the transmission rate.

Furthermore, the data is "semi-duplex", which means it cannot be sent in two opposite directions at the same time, so this layout is not ideal for high traffic networks. .

RING topology

A ring topology is where the nodes are arranged in a circle (or ring). Data can be transmitted over the ring network in either direction or both directions, with each device having exactly two neighbors.



Advantages

Since each device is only connected to the devices on either side, when data is transmitted, packets also move along a circle, moving through each intermediate node until they reach their destination. If a large network is arranged in a ring topology, repeaters can be used to ensure that packets arrive correctly and without data loss.

Only one station on the network is allowed to send data at a time, which greatly reduces the risk of packet collisions, making the ring topology efficient in transmitting data without failure.

In general, the ring topology is cost-effective and inexpensive to install, and the complicated point-to-point connections of the nodes make identifying problems or misconfiguration on the network relatively easy.

Disadvantages

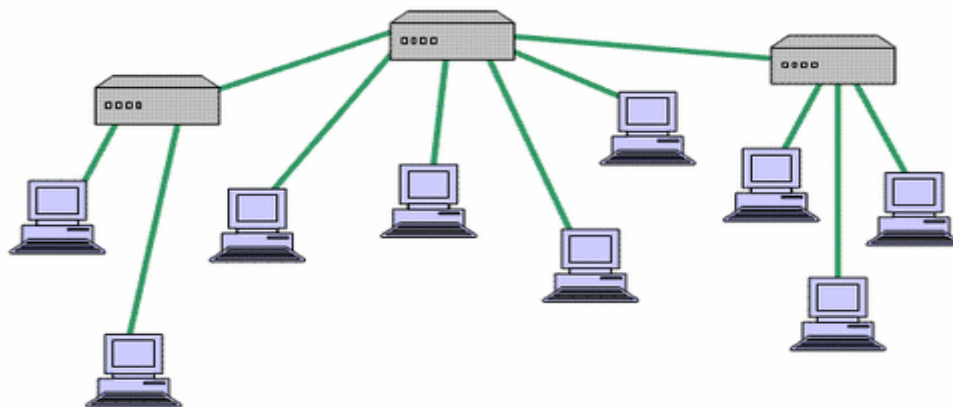
Although it is common, the ring topology is still susceptible to failure without proper network management. Since the data stream moves one way between nodes along each ring, if one node goes down, it can carry the entire network. That is why each node must be monitored and kept in good health. However, even if you are vigilant and attentive to the performance of the node, your network could still be destroyed due to a transmission failure.

The question of scalability also needs to be considered. In a ring topology, all devices on the network share bandwidth, so adding more devices could cause the overall communication delay. Network administrators should pay attention to the devices added to the topology to avoid overloading the resources and capacity of the network.

Additionally, the entire network must be brought offline in order to reconfigure, add or remove nodes. And while it's not the end of the world, scheduling network downtime can be inconvenient and expensive.

TREE topology

The tree topology is named from how the central node acts as a kind of trunk for the network, with the nodes extending outward in a branch-like fashion. However, where each node in the star topology is connected directly to the central hub, the tree topology has a parent-child hierarchy for how the nodes are connected. Connected hubs are connected linearly with the other nodes, so the two connected nodes share only one connection with each other. Because the tree topology is both extremely flexible and scalable, it is often used for wide area networks to support a wide range of devices.



Advantages

The combination of star and bus topology elements allows for easy addition of nodes and network extensions. Network troubleshooting is also a straightforward process, as each branch can be individually evaluated for performance issues.

Disadvantages

As with the star topology, the entire network depends on the health of the root node in the tree topology. If the hub fails, the different branch branches will be disconnected, although connectivity within - but not between - the branch systems will remain.

Due to the hierarchical complexity and linear structure of the network layout, adding more nodes to the tree topology can quickly make proper management difficult to use, not to mention expensive experience. . A tree topology is very expensive due to the amount of cables required to connect each device to the next in a hierarchical layout.

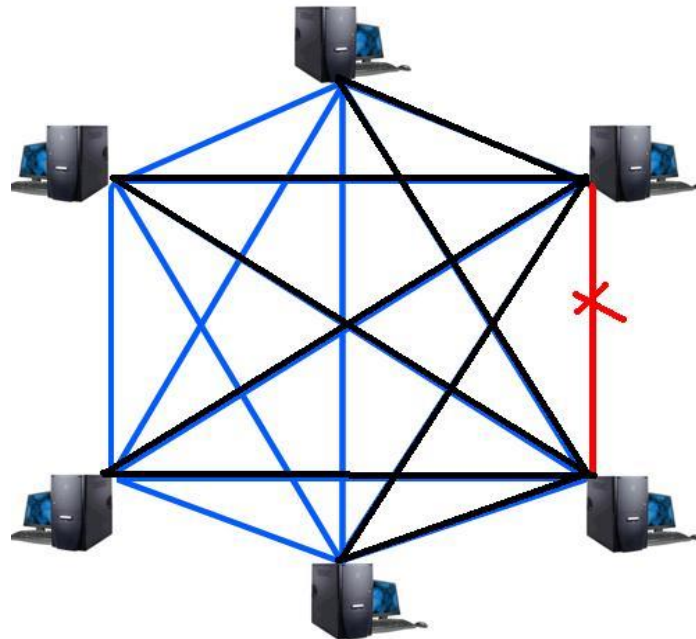
MESH topology

A mesh topology is a complex and complex structure of point-to-point connections where nodes are connected to each other. The network can be either full or partial.

The partial mesh topologies are mostly interconnected, with some nodes having only two or three connections, while the full mesh topology

The web-like structure of a mesh topology provides two different methods of data transmission: routing and flooding. When data is routed, nodes use logic to determine the shortest distance from source to destination, and when data is flooded, information is sent to all nodes in the network without the need for routing logic.

Advantages



Advantages

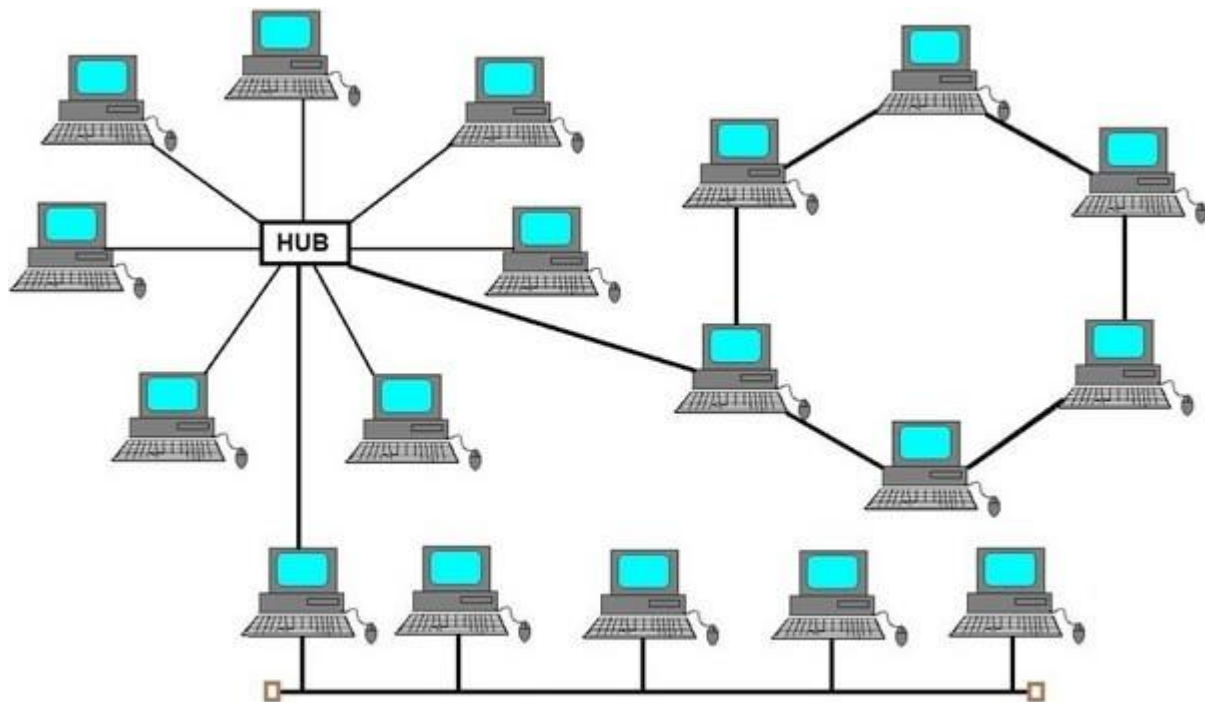
Mesh topologies are reliable and stable, and the complexity of inter-node connections makes the network resistant to failure. For example, not a single device crashes can make the network go offline.

Disadvantages

Mesh topologies are extremely labor intensive. Each connection between nodes requires cabling and configuration when deployed, so setup can also be time consuming. As with other topologies, the cost of cabling increases rapidly, and to say the network requires a lot of cables is an understatement.

HYBRID topology

Hybrid topologies combine two or more different topologies - a tree topology is a prime example, integrating bus and star layouts. Fusion architecture is most commonly seen in larger companies, where individual departments have a personalized network topology that adapts to their network needs and usage.



Advantages

The main advantage of a fusion topology is the degree of flexibility they provide, since the network topology itself has some limitations that the association setup cannot meet.

Disadvantages

However, each type of network topology has its own disadvantages, and as the network gets more complex, experience and know-how is needed on the part of the administrator to keep everything working optimally. There are also monetary costs to consider when creating a network topology.

♦ Logical topology

A logical topology determines how data will be transmitted. Contrast this with the physical topology, including the layout of cables, network equipment, and wiring.

Two of the most common logical topologies are:

Bus topology: Ethernet uses a logical bus topology to transmit data. Under the bus topology, one node transmits data to the entire network. All other nodes on the network hear the data and check if the data is for them.

Ring topology: In this topology, only one node can be allowed to transmit data in the network at a given time. This mechanism is achieved through the token (only the node with the token can transmit data in the network) and thus collisions in the network can be avoided.

b. Impact of communication and bandwidth

The bandwidth can be understood as the maximum speed that can be transmitted in 1 second. We often encounter fiber optic network speeds, copy speed of USB ... In this sense, Bandwidth is understood as Broadband. In the field of website hosting, the term "bandwidth" is often used to describe the maximum amount of data including upload and download back and forth between the website (or server) and users in a unit of time (usually months). In short, bandwidth is the parameter that indicates the maximum amount of traffic your website can circulate each month. In this sense, we understand bandwidth is the sum of 1-month traffic. Another way of understanding Bandwidth is "Broadband" is the size of the transmission line. If the Broadband has a high index, it is possible to serve multiple people online at a time quickly.

3. Compare common network principles and how efficient protocols allow networked systems

a. Compare common network principles

	Bus topology	Ring Topology	Star Topology
Application	- Good for small networks and networks with low traffic and low data traffic.	- Good for cases where the network has a few stations operating at high speed, not far apart or the network has	- Currently the star network is the best way for the case of data and signal integration. Public
		unevenly distributed data.	networks have this structure.
Complexity	- Not complicated.	- Requiring relatively complex installation.	- The complexity depends on the central device, which is generally easy.
Efficiency	- Very good under low load can reduce performance very quickly when loading increases.	- Effective in the case of high traffic volume and is quite stable due to the increase of delay time and degradation compared to other networks.	- Good for medium load case however size and ability, deduce the network performance depends directly on the power of the central device.

Cost	- Relatively low, especially because many devices have been fully developed and sold in the market. Channel redundancy is recommended to reduce the risk of network incidents.	- Must have doubled the resources or have an alternative method when a button does not work if you still want the network to operate normally, very high cost	- The total cost is very high when doing the task of the central device, the central device, although not used for other things. The number of private wires is also high.
Defect	- A broken station does not affect the whole network. Except for incidents on the line.	- A faulty station can affect the whole system because the stations depend on each other. Difficult to find broken network button.	- The reliability of the system depends on the central device, the network only fails when the central device fails.
Ability of extension	- Adding and reshaping this network is easy. However, it is difficult to connect between different computers and devices because they must be able to receive the same address and data.	- Relatively easy to add and subtract workstations without connecting much for each change Cost for change is relatively low.	- Network expansion is quite easy depending on the capacity of the central device.

b.How protocols allow the efficiency of networked systems

A network protocol is a set of directions and regulations that allow devices on a network to communicate with each other. Protocols include means for devices to self-identify and interpret the function and state of other devices on the network. They also usually include instructions or requirements for data transmission, including the types of data packets supported. Without these protocols, your network hardware cannot properly handle the data transmission or communicate with each other.

However, what do network protocols have to do with monitoring performance? Well, many protocols can establish basic performance data for network devices. Checking this data can help network groups understand the current state of their nodes. Regular

monitoring of these protocols ensures that you always have a simple understanding of whether your network is up and running.

◆ TCP and IP

TCP / IP was developed by the US Department of Defense to specify how a computer transfers data from one device to another. TCP / IP places a heavy emphasis on accuracy and it takes several steps to ensure that data is transferred correctly between two computers.

TCP is a system that helps network devices create and maintain connections between each other. It also contains information about how to break data down into packets that can be transmitted over the network. This is a necessary protocol for the networks to function correctly, as it manages the data transmission. TCP monitoring allows your business to analyze TCP response times and availability, letting your network group know how the network's data transmission is performing.

IP addresses each of the devices connected on the network and helps the network route data. Using IP addresses and routing protocols, a network can determine which packet path packets need to go to their destination. You can monitor the IP protocol to ensure that the data is arriving where it needs to go, as well as the delay between the data being sent and the IP system telling it where it is going.

◆ UDP

UDP or User Datagram Protocol is an unbound communication protocol. UDP does not store link state on sender and receiver, so it will not be responsible for the transmitted packet, sender only creates a datagram with IP address, port number of the receiver and then send it. UDP also doesn't have congestion management and flow control like TCP, but UDP has a message format similar to TCP:

With UDP, each packet is accompanied by the length of data that the packet can transmit, this limitation, along with the fact that UDP does not need to establish a link, helps UDP transmit data faster, so it is suitable for The application needs fast data transfer rate.

Along with the advantages of speed, UDP has no congestion control, flow control, so it can clog Internet, incoming packets out of order and especially low reliability. Application development with UDP gets more complicated when developers have to install a reliability control mechanism.

◆ Other protocols

Hypertext Transfer Protocol (HTTP) monitoring can check the availability of web pages and notify you of when mission critical services are down. You can also track

the lag between requesting access to a website and when the request is made. HTTP monitoring NPM alerts you when the network takes too long to access a website.

File Transfer Protocol (FTP) acts as a bridge between the computer and the server regarding file transfer. FTP requests information from the server based on download requests provided by the network. By monitoring your FTP system, your business can verify that you can upload and download files to and from your server. You can also observe upload / download speeds by monitoring FTP requests in real time.

Whenever a device in your network architecture fails, it can rely on Internet Control Management Protocol (ICMP) to generate an error message. It then sends this error message to devices that have requested information from it, such as a website or file. In addition to verifying that the ICMP system is working, ICMP monitoring can also help your business know when an error occurs on your network. The NPM solution can also send ping ICMP requests to check the active status of the devices on the network.

Employees and customers rely on an active network to send and receive corporate emails. There are several network protocols available to handle both incoming and outgoing email across your business network. For incoming mail, Post Office Protocol 3 (POP3) or Internet Mail Access Protocol (IMAP) allows original mail server clients to receive and store email. Monitoring these protocols not only ensures that you maintain constant access to the mail server, but can also track email response times so you know if important emails are handled quickly. For outgoing mail, Simple Mail Transfer Protocol (SMTP) can be monitored to make sure emails are being sent. It's often used in conjunction with POP3 or IMAP, which means you can monitor both your incoming and outgoing mail at the same time.

III. Explain networking devices and operations

1. Discuss the operating principles of network devices and server types

a. Discuss the operating principles of network devices

Network device is a collection of devices used to connect one or more LANs together. They are completely capable of connecting many segments together. However, the number depends on the number of ports on that device as well as the devices used in the network.

Types of network devices list:

- + Hub
- + Switch
- + Router
- + Bridge

- + Gateway
- + Modem
- + Repeater
- + NIC

◆ Repeater

Repeater is a device capable of amplifying, transmitting signals further and more stable. In the OSI model, this device is in class 1. The principle of this device is that it helps the physical signals at the input to be amplified. From there, the wifi transmission line is strong and to the devices that are far away from the Wifi Modem.



Hub

A hub is a multi-port device and is like a multi-port repeater, capable of transmitting signals to many different devices. This means that if one port on the Hub is transmitting, the other ports will also receive the information immediately.

On the market today, there are two popular types of Hubs, Active Hub and Smart Hub, each with its own characteristics and features. Active Hub, for example, is capable of amplifying the signal, helping to stabilize the transmission rate. Smart Hub also has

the same features as Active Hub but also has the ability to detect errors on the network automatically.



Bridge

Bridge is in the second layer of the OSI model. The function of this network device is to connect two Ethernet networks together to form a large network. That means Bridge will help copy the packet and transfer data to the computer to receive even when these two computers use two different networks.



Switch

Switches are more likely to connect depending on the number of ports available on the device. The main function of a Switch is to transfer data from source to destination and build Switch boards.



Router

In the OSI model, the Router is in the third layer. Also known as the router or router, this device is used to encapsulate and transfer data packets from an inter-network to the end devices.

However, in terms of speed, the ability to connect to two networks of the Router is slower than that of Bridge. Because before transmitting, the Router will perform calculations to find the most accurate route for the packets. Especially, if these lines have different transmission rates, the Router has to work harder.

Gateway

The main function of a Gateway network device is to connect computers together easily even when these devices do not use the same protocol. For example, Gateway can connect a computer using IP protocol with a computer using SNA, IPX, ...

In addition, the device is capable of distinguishing protocols. Therefore, it is often used in transferring email from one network to another, including long distance.



b. Discuss the operational principles of server types

A server is a computer, device, or program used to manage network resources. They are so called because they "serve" a computer, device, or another program called a "client" that provides functionality.

There are several types of servers, including print server, file server, network server, and database server. In theory, any time the computer shares resources with the client, they are considered the server.

However, servers are often referred to as dedicated because they do hardly any other tasks than their own.



Web Server

Web server means web server, which is a mainframe connected to an extensive set of computer networks. The server contains all data that it is authorized to manage. Each

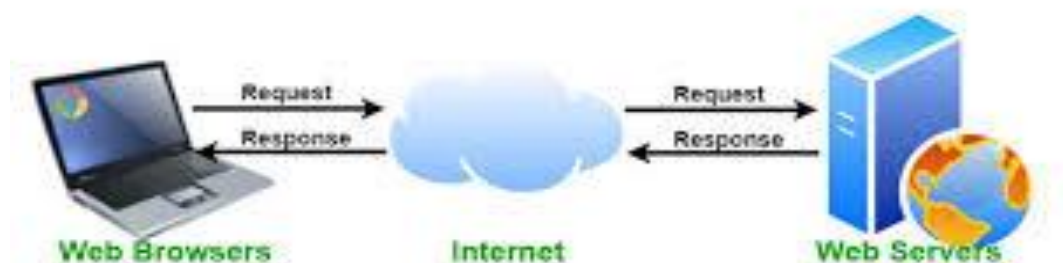
server has its own IP and can read various languages such as HTML, HTM, File, ... The server has large capacity and very high speed to be able to store and operate well data warehouse on the internet. Through each server's separate communication port, the computer system is able to operate more smoothly. The server must ensure continuous operation to be able to provide data to its network of computers.

The web server can be either hardware or software, it can be both.

Hardware: A web server is a computer that stores image files, HTML documents, CSS, and JavaScript files of a website and transfers them to End-user's device. The server is connected to the internet and accessed through a domain name like Mozilla.org.

Software: Web server consists of a number of parts that control user access to files stored on an HTTP server. An HTTP server is a piece of software that can understand website addresses (URLs) and the protocol the browser uses to view websites (HTTP).

Whenever a browser needs a file stored on the server, the browser requests the file over HTTP. When the request reaches the correct server (hardware), HTTP (software) sends the requested document back over HTTP.



Applications Server

An application server, also known as application server software, is a piece of software that provides software applications to a device or workstation, usually over the Internet using HTML protocol.

An application server can be understood differently as a software framework that provides an environment where many applications are capable of functioning whatever they are. An application server differs from a web server by using a lot of server-generated content and tightly integrated with the Database server.

Application server software products often use middleware to aid application communication between dependent applications such as Web servers, database systems, and charting software. . Some Application server software provide an API (application programming interface) that allows them to be independent of the operating system. A portal is a popular application server software mechanism that provides an access point to a variety of applications.



Printer Server

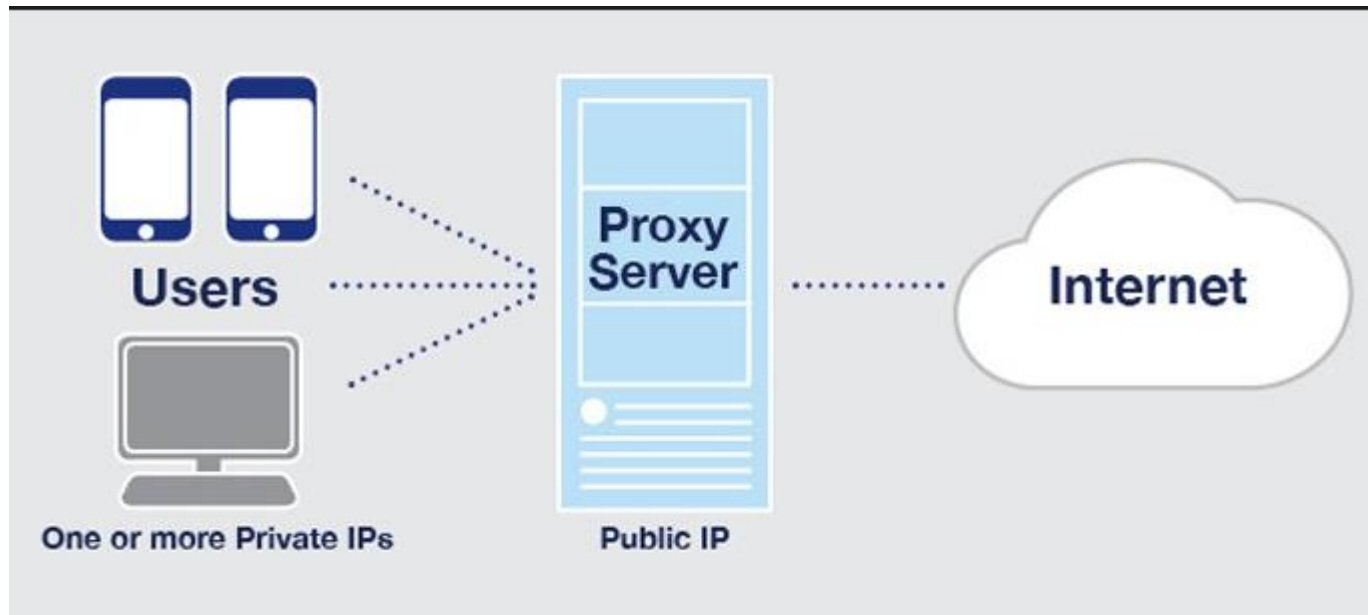
Print server is the print server. This is one of the devices used a lot in modern printing technology that uses new printing technology and incorporates the server operating system indirectly.

The print data will be imported into the print server system and connected to the printer to reduce printing operations. The print server will usually be connected to a USB port to receive data along with a parallel port to connect to the computer to help transmit data from the computer to the printer via the print server's intermediate form.



Proxy Server

Proxy Server is a server that acts as a proxy set-up between station users and the Internet. Connections between sender and receiver will be blocked by Proxy server, not made directly. And the incoming data information received at one port is then forwarded to the rest of the network via a different port than the incoming port. Thanks to such indirect transmission, the proxy server makes it much more difficult for hackers to get the internal address and details of a private server system.



Database Server

Database server or data server is a data warehouse used to store website, data and information. A database server is a LAN computer dedicated to database storage, maintenance and retrieval. Database server includes Database Management System (DBMS) and database. Based on the request from the client computers, the Database server will search the database for the specified records and forward them over the network.

A database server can be defined as a dedicated server providing database services and also as a server running data software. We will often see the database server in a client-server environment, which is the place that provides information that client systems look for.



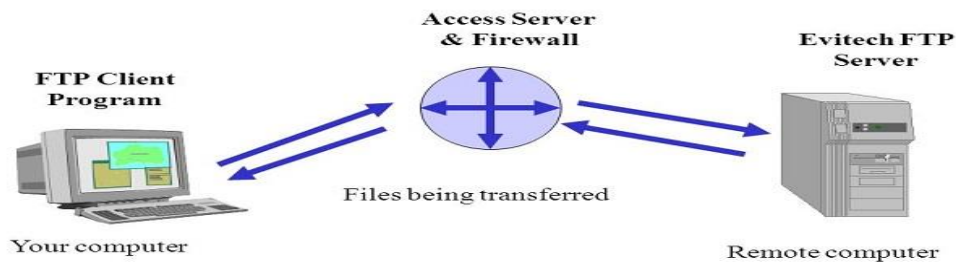
FTP Server

FTP (short for File Transfer Protocol): This is a protocol that transfers files from one computer to another (Usually personal computers and servers) over a TCP network or over the Internet.

At FTP, you will have the right to manage all file and directory data on the host except the database. All hosting packages you buy that support control panel cPanel, DirectAdmin ... are available for FTP via connection port 21 (21 is the default port, this port can be changed if the hosting provider changes the port). Through FTP protocol, users can upload data such as images, documents, media files (music, videos) ... from their computer to a server located somewhere else or download files. on the server to personal computers.

A FTP operation requires two computers, a server and a client). An FTP server, used to run the software providing FTP service (FTP Server), called the server, listens to requests for services from other computers on the network. The client running the FTP client (FTP client) for the service user, called the client, initiates an association with the server. Once the two machines are linked, the client can handle a number of file operations, such as uploading files to the server, downloading files from the server to their own, renaming files, or delete file server etc. Since the FTP protocol is a standard public protocol, any software company, or programmer, can write an FTP server or an FTP client. Almost any computer operating system platform supports the FTP protocol. This allows all computers connected to a TCP / IP-based network, to process files on another computer on the same network, regardless of which operating system the computer is using (if all of these computers allow the access of other computers, using the FTP protocol).

FTP session diagram



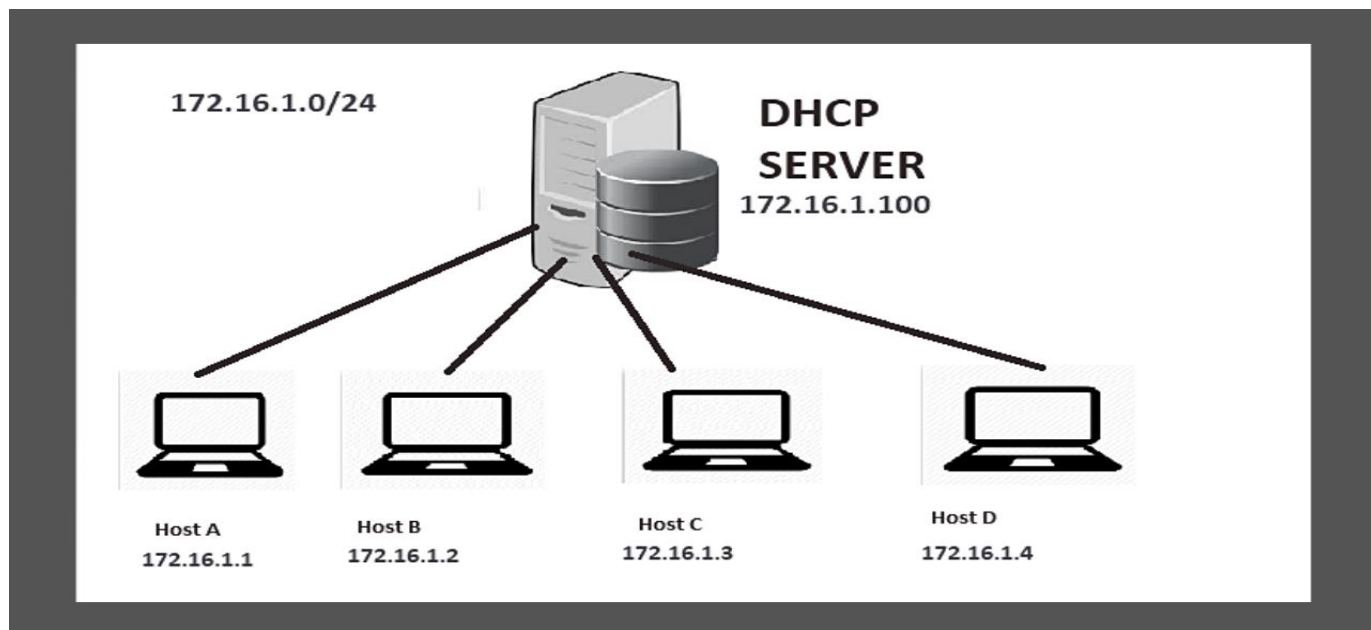
DNS Server

DNS Server, also known as Domain Name System is a naming system in order for computers, services participating in the Internet. It associates various information with the domain name assigned to them so that users can use that domain to find out the information they need to know. It is important to choose a domain name that is meaningful to users, linked to other network devices, to locate and provide information to users around the world.



DHCP Server

DHCP stands for Dynamic Host Configuration Protocol, which is a protocol that automatically assigns IP addresses to devices on the network. The IP addresses provided from the DHCP protocol will allow us to access the internet. It also ensures that no two or more devices have the same IP and also provides configuration information such as DNS, subnet mask, default gateway. "How does DHCP work?" will be answered in the next section.



Virtual Private Server - VPS

VPS, also known as virtual server, is considered as a copy of the operating system, customers can access at the same user levels as the operating system, so when using VPS we can install most software running on that operating system. Depending on the purpose of the user there will be equivalent functionality in a physical server, which is also a defined piece of software and can easily be configured. On the market today, VPS is priced lower than other physical servers so the performance may be slightly lower depending on the workload.



Cloud Server

Cloud server (also known as cloud server) is a virtual infrastructure built to store and process information and applications. Cloud Server is a server product similar to a virtual server (VPS server) but is set up with Cloud Computing technology (cloud computing technology).

What types of servers are when they used to have a certain capacity limit and upgrading more capacity for servers is quite difficult and takes a lot of time to do, at times like servers force must temporarily use activities, causing much influence for businesses as well as users.

Besides, when you have a project to set up a certain application that requires a server to be able to perform, then you are forced to buy, rent one or more new servers, but you cannot use it with servers running other applications or projects.

The resource upgrade of Cloud Sever is very simple and fast, the resource upgrade takes only a few minutes, and during the upgrade, there is no need for server maintenance.

All projects can be deployed on the same server, without enough resources, can be upgraded, with almost no limit.



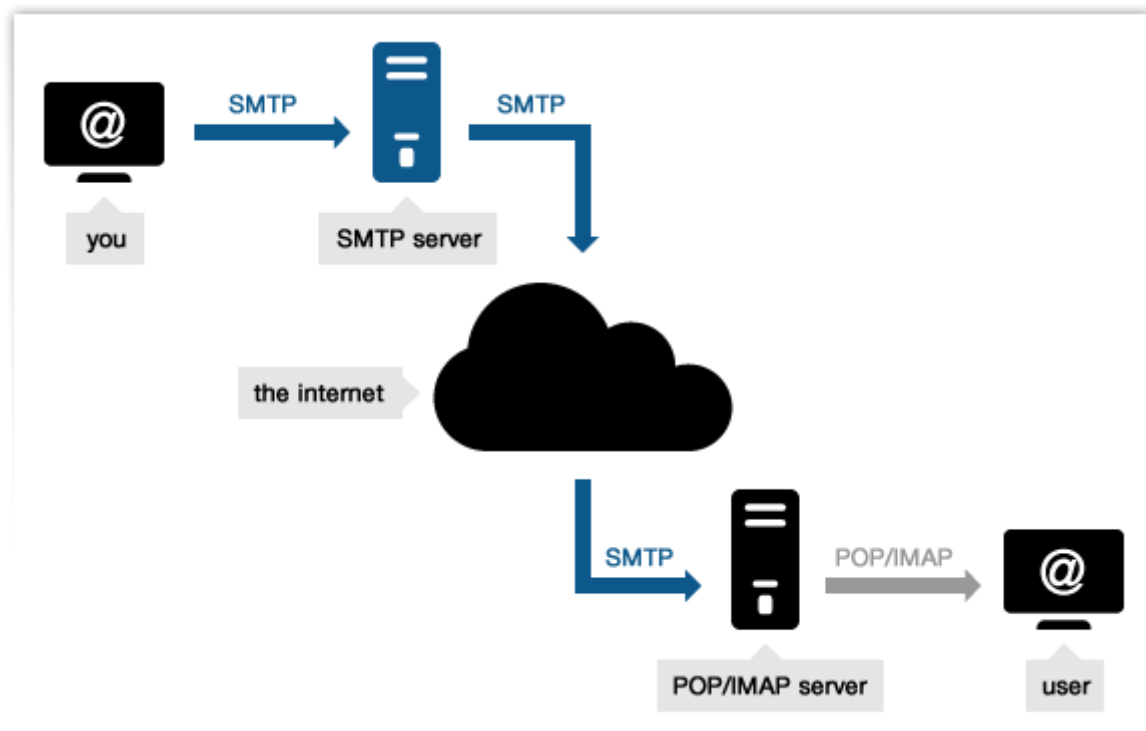
SMTP server

SMTP Server is known by many users as a dedicated server to send mail. This is one of the services that allows businesses to easily send out extremely large and unlimited emails.

This helps SMTP Server to outperform Gmail's free mailboxes or the mail that comes with hosting. Or in a simpler way, the server that helps you send mail is called SMTP server. This service will send mail to you via TCP or IP, ensuring agility, security and convenience.

Normally, SMTP Server can help you to transfer mail through Internet port 25 (TCP). But now, in Europe there is a way for users to send mail more conveniently than X.400.

Besides, there are many email related servers that have gradually been supporting a simpler and more extensive form of mail delivery called ESMTP, which allows users to allow multimedia files to be sent easily. .



2. Explore a variety of server types and demonstrate server selection, considering a certain scenario regarding cost optimization and performance

a. Factors to consider when choosing a server

To choose the right configuration we need to consider factors when choosing a host, including virtual machines (VM) and unified containers. When choosing a host, care should be taken in evaluating the importance of certain features depending on the use case. Remember, security is also extremely important, and consider adding protection, detection, alerting, and recovery features, including native data encryption to protect it on the go, and store the data, update the event log continuously to avoid indelible copies.

Online and regional support services

Select a manufacturer that can provide service and support in your area. Other available methods are online or telephone support. Many server problems can be resolved through a single phone call to the support center or over the Internet. Therefore, it is important to choose a server manufacturer that can support through these methods.

Full warranty and spot

For most servers, going to a repair shop isn't practical. So it's important to choose products that have a good in-house warranty for all parts, that is, the machine and everything in it.

Product quality

You should choose to buy the best machine from a reputable, reliable manufacturer when you need assistance. Don't save money on your initial investment with a product line of unknown origin and low reliability.

Operating system

Microsoft is not the only choice anymore. Make sure your host manufacturer has the resources to support the operating system of your choice, regardless of whether it's Windows or Linux.

Internal skills

Evaluate the skills in the organization and choose to buy the right server for those skills. For example, if your employees know well about Linux but do not know anything about Windows, you should not buy a server using Windows.

Anti-error technology

Select a server with technologies such as RAID (Redundant Array of Independent Disks) storage, hot plugging and error-correction code (ECC) memory. RAID protects data by writing data to more than one disk. Hot-swap technology allows you to replace damaged parts while the machine is running. And ECC memory checks and corrects errors while working.

Redundant parts

The server should also have redundant power, fans, hard drives and network cards (redundant). Any moving parts need a reserve. This will cost more, but it would be a good deal compared to the cost of shutdown when having to replace one of those parts.

Error prediction

The server will run until it no longer works. Error prediction technology gives you up to 48 hours in advance of impending server failure, allowing you plenty of time to prevent.

Automatic data backup

A server holds several gigabytes of data. Don't be the time to reinstall. Make sure your server has automatic data backup program installed.

Compatibility

Select a server manufacturer that tested its product on all of the commonly used applications and hardware. They will give you a list of all the sections for which they have checked for compatibility. This will help you to avoid troubles and fatigue later.

System management

This is an application that monitors the health of the server. It tells you how the machine runs and predicts how it will perform in the future. System management is a complicated business for small businesses, but many manufacturers can provide you with this service.

Product line

As the business grows, equipment upgrades may be required. You need to choose to buy a server from a manufacturer capable of offering a product line that not only meets today's needs but also in the future.

b.Select server for business

◆ For small and medium enterprises

A business purchases a server to handle one or more specific tasks:

- + Share data with file sharing server
- + Provides domain authentication functionality
- + Provide Database service for other application servers.
- + Hosting a website with a web server
- + Provide e-mail services with a mail server.
- + Control shared peripherals, such as printers.
- + Run the shareware on an application server

◆ For big business

The server for large businesses is a necessity because the demand for management capacity and operating speed are always top priorities. Some of the needs that server helps solve for this business object include:

- + Save and manage a large amount of business information, manage project information...
- + Run the software: management, finance ...
- + Backup, data backup
- + Safe and secure data protection
- + Anti-local attack
- + Managing and operating remote systems
- + Increase processing capability, enabling powerful processing capability during peak periods, the need for resources such as RAM, CPU, high speed transmission ...

3. Discuss the interdependence of workstation hardware with related network software

- Network hardware - Computers need network hardware to connect to each other. Routers, hubs, switches and needles are all parts of the network device that can perform slightly different tasks. A router can often combine hubs, switches and wireless access in one piece of hardware..
- Router - A router can form a LAN by connecting the devices in a building. It also makes it possible to connect different networks together. Homes and businesses use a router to connect to the internet. A router can often incorporate a modem in hardware.
- Gateway - it works with different protocols. It is in the network node and interfaces with another network.
- Hub-One hub transmits data to all devices on the network. This can use up a lot of bandwidth as it leads to unnecessary data sending - not all computers need to receive data. A hub would be useful to link several game consoles to a local multiplayer game using a wired LAN.
- Switch contains more intelligent centers. It is capable of checking data, identifying sources and forwarding data. It performs better than the center. The switches are mainly active.
- Bridges A bridge is used to connect two separate LANs. The computer can act as a bridge through the operating system. A bridge looks for the receiving device before it sends the message. This means it will not send the message if the receiving computer is not there. It will check if the recipient has a message. This can help to save unnecessary data transmission, but rather at the performance of the network.
- Modems Modem allows computers to connect to the Internet via phone lines. A modem converts the digital signal from a computer to an analog signal that is then sent down to a phone line. A modem on the other end converts the analog signal into a digital signal that another computer can understand..
- File server - network file server is a computer system used for the purpose of managing file systems, network printers, handling network communication and other functions. A server that can be reserved is such a case, its entire processing power is allocated to the network function or it may not be dedicated, which means that part of the server functions are Allocate as a workstation or DOS-based system.
- Network operating system - it is loaded into the server's hard disk along with system management tools and user utilities. When the system is started, the NOS starts and the other server is under its control.
- Workstations - workstations or nodes are attached to the server via network interface cards and cables; Workstations are usually smart systems, such as IBM computers. But the DUMV terminal is used in mainframe computers.

The concept of distributed processes depends on the fact that the personal computer attached to the network performs its own processing after downloading the program and data from the server. Therefore, a workstation is called an active device on the network. After processing, the files are stored back on the server where other workstations can use them.

- Network interface card - all devices connected to the LAN need a network interface card to plug into the LAN. For example, a PC needs to have an Ethernet card installed in it to connect to Ethernet LAN.
- Network cabling - when the server, workstation and network interface card are set, the network cable is used to connect everything together. The most common type of network cable:
 - + Twisted wire
 - + Coaxial cable
 - + Optical cable.
- These are interdependent to implement the network properly. This is the basic process of complete connection. This is a suitable system for insurance industries to apply this process to operate effectively and efficiently.

IV. Design efficient networked systems

1. Design a networked system to meet a certain specification

a. Request

- *I was recruited to be a network engineer by a high-tech network solution development organization and working on a project for a local educational institution (Specifically, I will act as a network engineer for BTEC FPT International College). I will need to analyze the specification from the organization below to complete this project within a certain time frame with the requirements set out as follows:*
- *People: 200 students, 15 teachers, 12 marketing and administration staff, 5 senior managers including the academic head and program director, 3 computer network administrators.*
- *Resources: 50 student lab computers, 35 staff computers, 3 printers*
- *Building: 3 floors, all computers and printers are on ground floor except for IT lab - one lab is on the first floor and another lab is on the second floor*

b. Design plan and expected cost

◆ Design plan

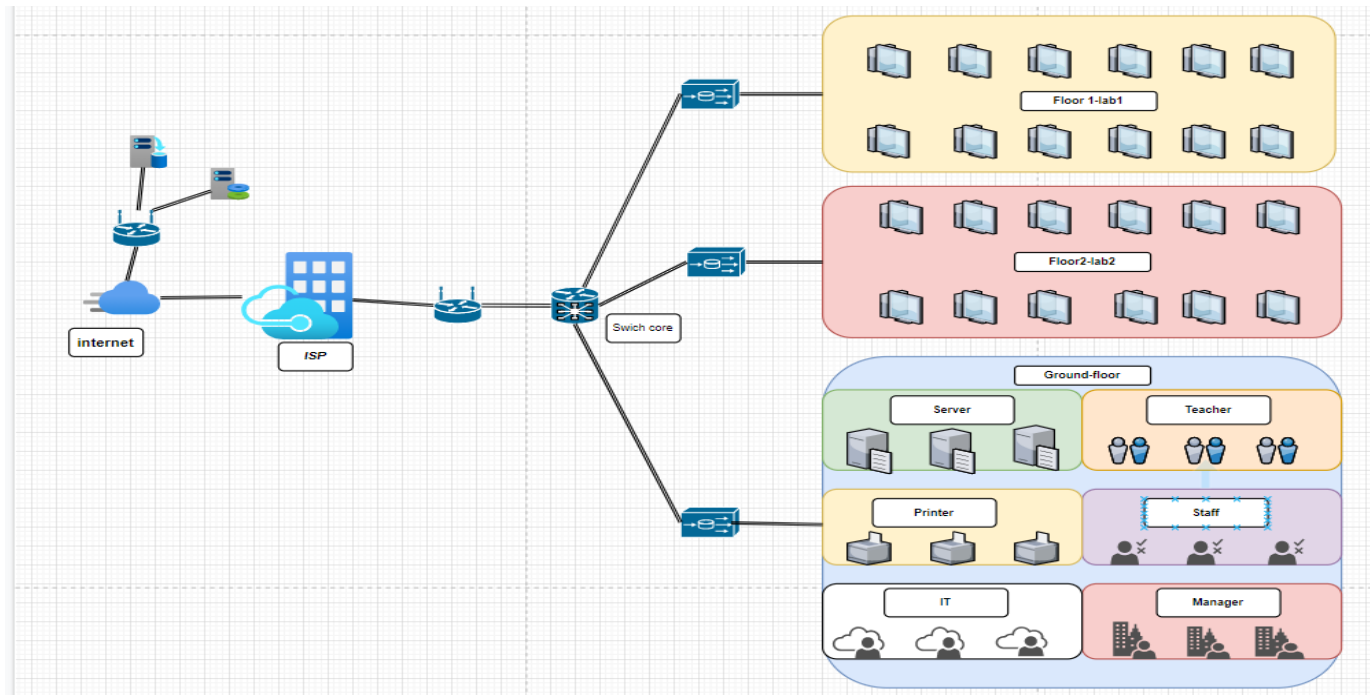
At the request of the lesson, the building consists of 3 floors:

- On the ground floor, teachers and staff at the school will be designed here. Besides, there are rooms for network administrators and managers. The printer is also

designed on the ground floor. In addition, I also propose to add some servers to use as File Server and Web Server. We can also use virtualization technology to save costs (Virtual Private Server).

- Level 1 and 2 are labs. With 50 computers for students, we divided into 2 laboratories, 1 room on the 1st floor and 1 room on the 2nd floor. The number of computers for students per floor is 25 units.

Let's see the physical diagram illustrating the above proposal:



Network physical diagram of the building

- Design plan on ground floor

+ Management Department:

In this room, we will have 5 computers for 5 senior managers, including the academic manager and program manager.

+ Computer network administrator room:

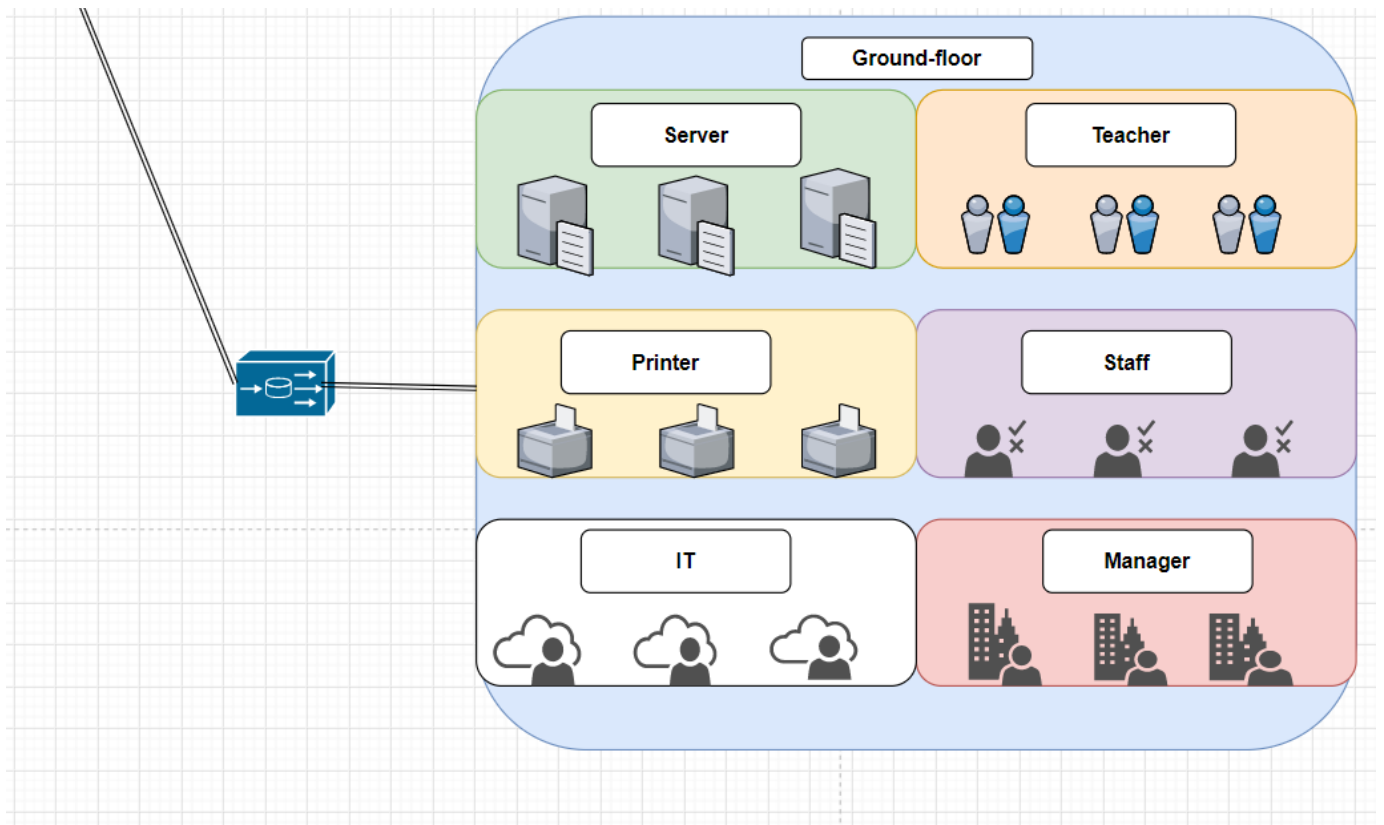
With 3 computers, 3 network administrators will manage the entire network in the school such as switch and router management, server management, security for the intranet, ...

+ Teachers and staff rooms in the school:

Teachers and staff will also be supported by the school and printers to work. These devices are arranged on the ground floor

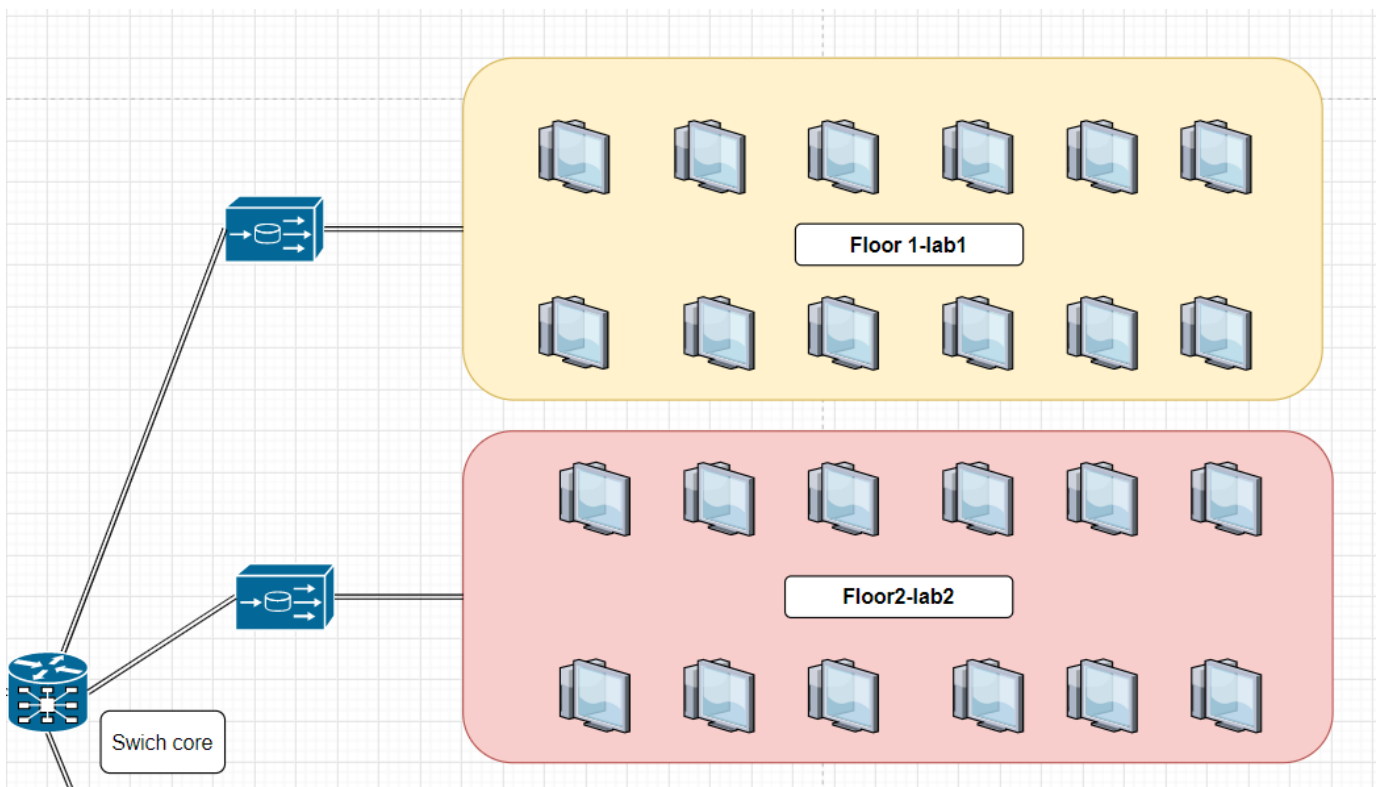
+ Equipment department:

This is the room used to place devices such as switches, routers and servers (as mentioned above, I would suggest installing one or more servers to work internally even though the threads are not required).



• Design plan 2nd and 3rd floor

+ On these two floors there will be the same layout because they are all arranged in a lab for students. With 50 computers divided into 2 labs, each room will have 25 computers. Besides, each room will have 1 computer for teachers to use for teaching as well as to manage students.



2. Check and evaluate the design to meet the requirements and analyze user feedback

Check and evaluate the design for requirements

- Network system of British College BTEC FPT is a network system used for learning purposes and helps improve the quality of school teaching. Since the deployment network must meet some of the following requirements:

♦ Operability:

- - Satisfying the work requirements, the ability to connect between users is always throughput, interaction between the user and the application at acceptable speed and reliability..

♦ Can be managed:

- Easy to monitor and manage to ensure smooth operation of features

♦ Exchange data quickly and safely:

Operate school activities remotely through the network. Therefore, saving travel costs and improving the teaching management efficiency of the school.

♦ Ability to manage centralized data information:

- Building a centralized management model, all data is gathered in one place to both keep information confidential and convenient for managing and backing up data. Simultaneously with centralized management from the central office can easily manage remote offices through the support of application programs.

♦ Remote administration and administration capabilities:

- The school can operate its operations remotely through the network. Therefore, saving travel costs and improving the effectiveness of teaching management of the school.

♦ Ability of extension:

- The network must be expanded, the original design must be expanded without causing a major change in the overall design.

♦ Compatibility:

- The network must be designed with a pair of faces that are always oriented towards new technology and must ensure that it does not prevent the introduction of new technologies in the future.

Check and evaluate costs

Tower: is the main part of the computer. That is the part containing the necessary hardware. In this case I will choose Tower Dell Optiplex 3070MT-42OT370002



Here are a few specifications

Model:	Dell Optiplex 3070MT-42OT370002
Producer:	Dell
Origin:	China
CPU:	Intel Core-i5
CPU type:	9500
CPU speed:	3.0GHz to 4.4GHz
Caching:	9MB Cache
RAM type:	SDRAM DDR3
RAM capacity:	8 GB
Bus speed:	2666 MHz
Hard drive type:	SATA
Hard disk capacity:	1 TB
Optical disc type:	SuperMulti DVD
Graphics processor:	Integrated Intel HD Graphics
Graphics card chipset:	Intel HD Graphics 530
Graphics card capacity:	Share
Sound technology:	High Definition
Audio standard:	High Definition Audio
Wifi standard:	IEEE 802.11 b/g/n
LAN Standard:	10 / 100 / 1000 Mbps
OS	Windows 10 Home SL
Size:	175x426x382 mm
Price:	\$ 350
Weight (kg):	10 kg

It sells for \$ 350 (at the time the network is being designed).

◆ Monitor



Computer screen

- Monitor: if there is no screen, you will not be able to view this website or any other program. I will propose a Samsung LC24F390FHE Curved Monitor - 24 ", FHD, FreeSync.
- Impressive screen performance: Experience superb screen clarity with Full HD (1920x1080) resolution on a 23.8" screen.
- It sell for \$ 250 (at the time the network is being designed). You can refer to many another on the internet.

Mouse and keyboard.

Currently on the market there are many different types of mice and keyboards, which are diverse in types, so I will not recommend specific equipment. The cost for both the keyboard and the keyboard will be about 50 USD.

So for a set of computers we will (including Tower, Monitor, mouse and keyboard) we will spend 500 USD. At the request of the lesson, the school will have 85 computers, so the expected cost is 42 500 USD ($500 * 85 = 42\,500$ USD).

Printer.

At a cost of about 100 USD, we can choose LASER printer CANON IMAGECLASS LBP6230DN

Compact design

Canon Laser ImageClass LBP6230DN laser printer in white color combined with black color gives an elegant, neat design with rounded edges that look a lot like the LBP6030W but slightly larger because the paper tray is upgraded to 250 sheets.



With 3 numbers, we will spend 300 USD to buy a printer

Server

Since this is a small LAN, I will choose the Server for about 1500 USD. The IBM System server x3500 M4 (7383C2A) will be the right choice in this case:



With 2 server machines, we will spend about 3000 USD.

Switch

With 3-storey building, we will use 3 Switch layer 2 and 1 Switch Core. Switch layer 2 will cost 500 USD / unit, Switch Core will be more expensive and cost about 1000 USD.

Thus, we will spend 2500 USD to buy Switch.

Router

For a small network, I would suggest a Router device that costs \$ 100 and just one device is enough.

Thus, the cost for the device will be 49 400 USD.

Other costs

In addition to the cost to buy the equipment, we can also mention some other costs such as initial installation costs, operating costs, ... In order for the network to run smoothly, it will take about 50 000 USD.

3. Installing and configuring network services and applications

Basic configuration

- **Set hostname for router and switch:** Each device needs a name that is easy to manage.
- **Set IP:** Each device needs an IP to easily manage and identify.
- **Set password:** In order to improve security, switches and routers should use access passwords, as well as limit the number of visits for some authorized users. Besides setting a password, we can use SSH remote access method to improve security.
- **SSH configuration:** Besides improving security more than Telnet, SSH helps network administrators easily manage devices.

a. VLAN

◆ VLAN

VLAN stands for Virtual Local Area Network (or Virtual LAN), also known as a virtual LAN. VLAN is a technique that allows the creation of a logically independent LAN on the same switch or the same physical infrastructure. The creation of multiple virtual LANs in the same local network (between departments in a school, between departments in a company, ...) helps to reduce broadcast domains as well as facilitate managing a large local area network. VLANs are equivalent to a subnet.

Because VLANs are based on logic instead of a physical connection, they are extremely flexible.

The Vlan defines the broadcast domains in the class 2 network. The Broadcast domains are the collection of all devices that will receive broadcast frames originating from any device in the region. The Broadcast domains are usually restricted by the Router because the Router does not forward the broadcast domains.

Switch Layer 2 creates the broadcast domains based on the Switch configuration. A switch is a universal bridge that allows you to create multiple broadcast domains. Each broadcast domains are like a separate virtual bridge within a switch. You can define one or more virtual bridges in a switch. Each virtual bridge you create in the switch defines a new broadcast domain (VLAN). The traffic cannot be transmitted directly to another VLAN (between broadcast domain) within the switch range or between two switches. To connect two different LANs, you must use Layer 3 Router or Switch.

◆ Trunk port

- When a link between two switches or between a router and a switch conveys the traffic of multiple VLANs, that port is called trunk port.
- The trunk port must run special communication protocols. The protocol used may be Cisco's proprietary ISL protocol or IEEE 802.1q standard.

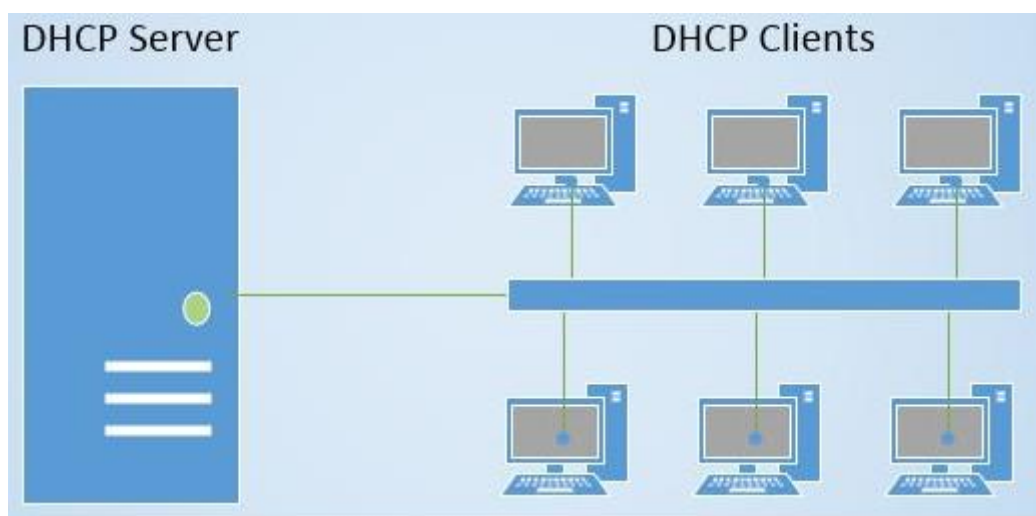
b. DHCP

DHCP server is used to issue unique IP addresses and automatically configure other network information. In most homes and small businesses, the router acts as a DHCP server. In large networks, a single computer can act as a DHCP server.

In short, the process goes like this: A device (client) requests an IP address from a router (host), then the host assigns an available IP address to allow the client to communicate with. network.

When a device is turned on and connected to a network with a DHCP server, it sends a request to this server, called a DHCPDISCOVER request. After the DISCOVER packet reaches the DHCP server, the server will try to keep an IP address the device can use, and then provide the client with that address with a DHCPOFFER packet.

After providing the selected IP address, the device responds to the DHCP server with a DHCPREQUEST packet to accept it, then the server sends the ACK used to confirm the device has that particular IP address and to defines how long a device can use the address before retrieving a new address. If the server decides that the device does not have an IP address, it sends a NACK. Of course this happens very quickly and you don't need to know any of the techniques used to get an IP address from the DHCP server.

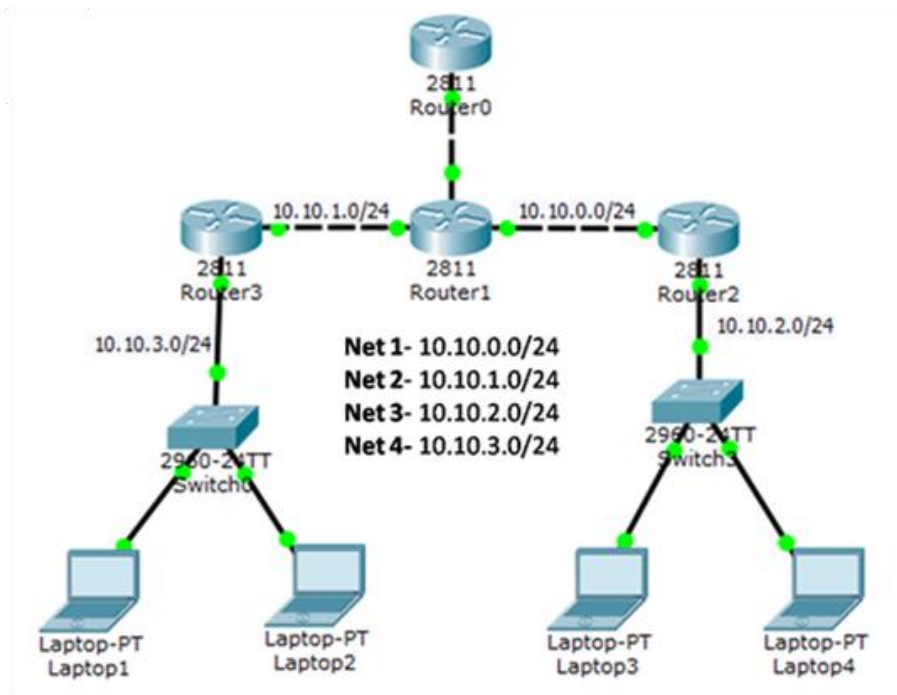


c. Static routing

Static Routing is the routing method in which the administrator will enter all the routing information for the router. So when the network structure has any changes, the administrator will change it by deleting or adding information about the router's path, in other words this path is fixed.

Static Routing operation principle can be understood like this.

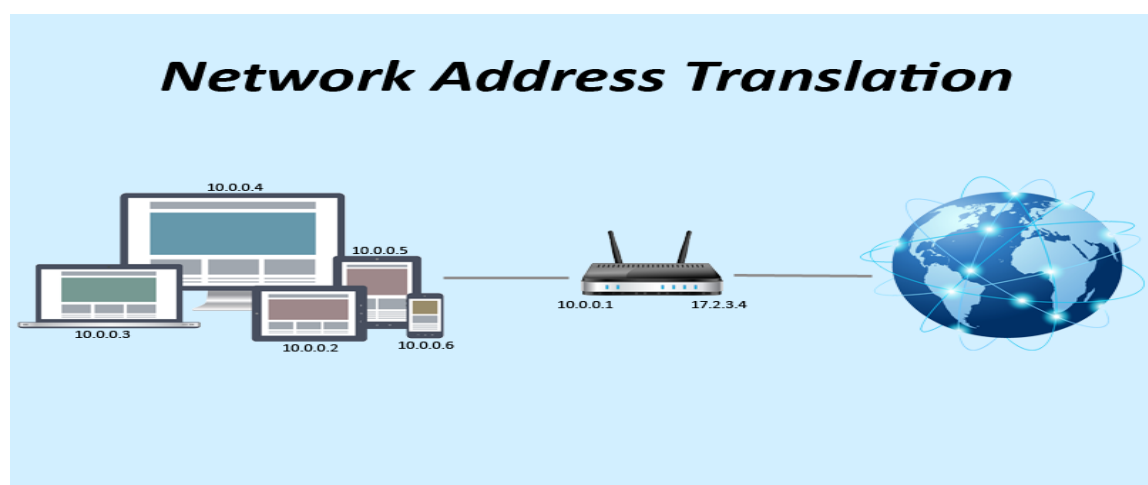
- First, the administrator will configure the fixed routes for the router
- Then the router will install this route into the routing table.
- And the data packet is routed in a fixed route.



d. NAT

NAT is an acronym for Network Address Translation. Usually what the concept of NAT is associated with an internal IP address. Because NAT is a technique that allows one or more local domain IP addresses to be mapped and connected to one or more IP addresses outside of another domain. An IP address is a series of numbers about 32 bits long - IPV4 or 128 bits - IPV6.

To put it simply, NAT is the kind of technology that is built into the router. It allows this router to connect to external internet networks via IP address. At the same time, NAT also allows multiple people to use the same internet by pasting their secondary IP addresses. As defined above, NAT is also known as NAT port.



e. ACL

- An access control list (ACL) contains rules that grant or deny access to certain digital environments. There are two types of ACLs:

- + Filesystem ACLs—filter access to files and/or directories. Filesystem ACLs tell operating systems which users can access the system, and what privileges the users are allowed.
- + Networking ACLs—filter access to the network. Networking ACLs tell routers and switches which type of traffic can access the network, and which activity is allowed.
- Originally, ACLs were the only way to achieve firewall protection. Today, there are many types of firewalls and alternatives to ACLs. However, organizations continue to use ACLs in conjunction with technologies like virtual private networks (VPNs) that specify which traffic should be encrypted and transferred through a VPN tunnel.
- Reasons to use an ACL:
 - + Traffic flow control
 - + Restricted network traffic for better network performance
 - + A level of security for network access specifying which areas of the server/network/service can be accessed by a user and which cannot
 - + Granular monitoring of the traffic exiting and entering the system

V. Deploy and diagnose networked systems

a. Implement a network based on a prepared design

1. Basic configuration

- ◆ Set hostname for devices.

Create a name for Switch

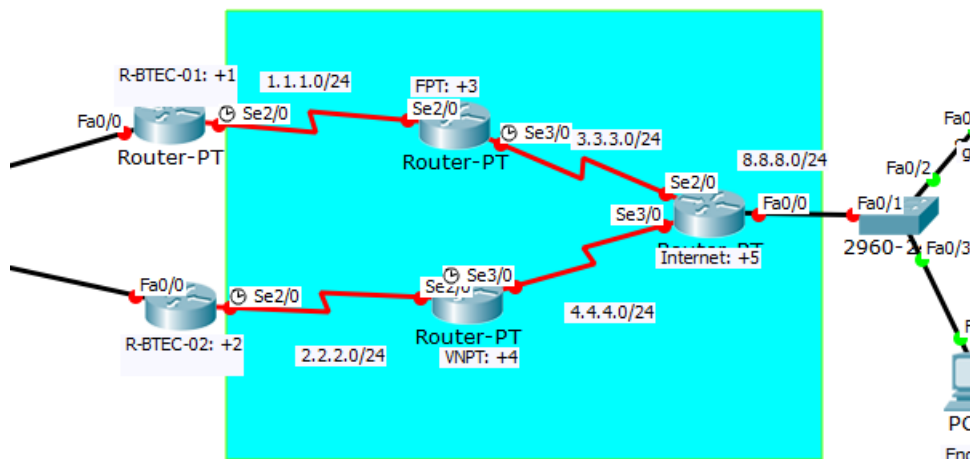
```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End
with CNTL/Z.
Switch(config)#
Switch(config)#
Switch(config)#host BTEC-College
BTEC-College(config)#
BTEC-College(config)#
BTEC-College(config)#
BTEC-College(config)#
BTEC-College(config)#
BTEC-College(config)#
```

Create a name for Router

```
Press RETURN to get started!

Router>
Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End
with CNTL/Z.
Router(config)#host BTEC-R1
BTEC-R1(config)#
```

- ◆ Set IP



We have 2 ip address in port outside in R1 and R2

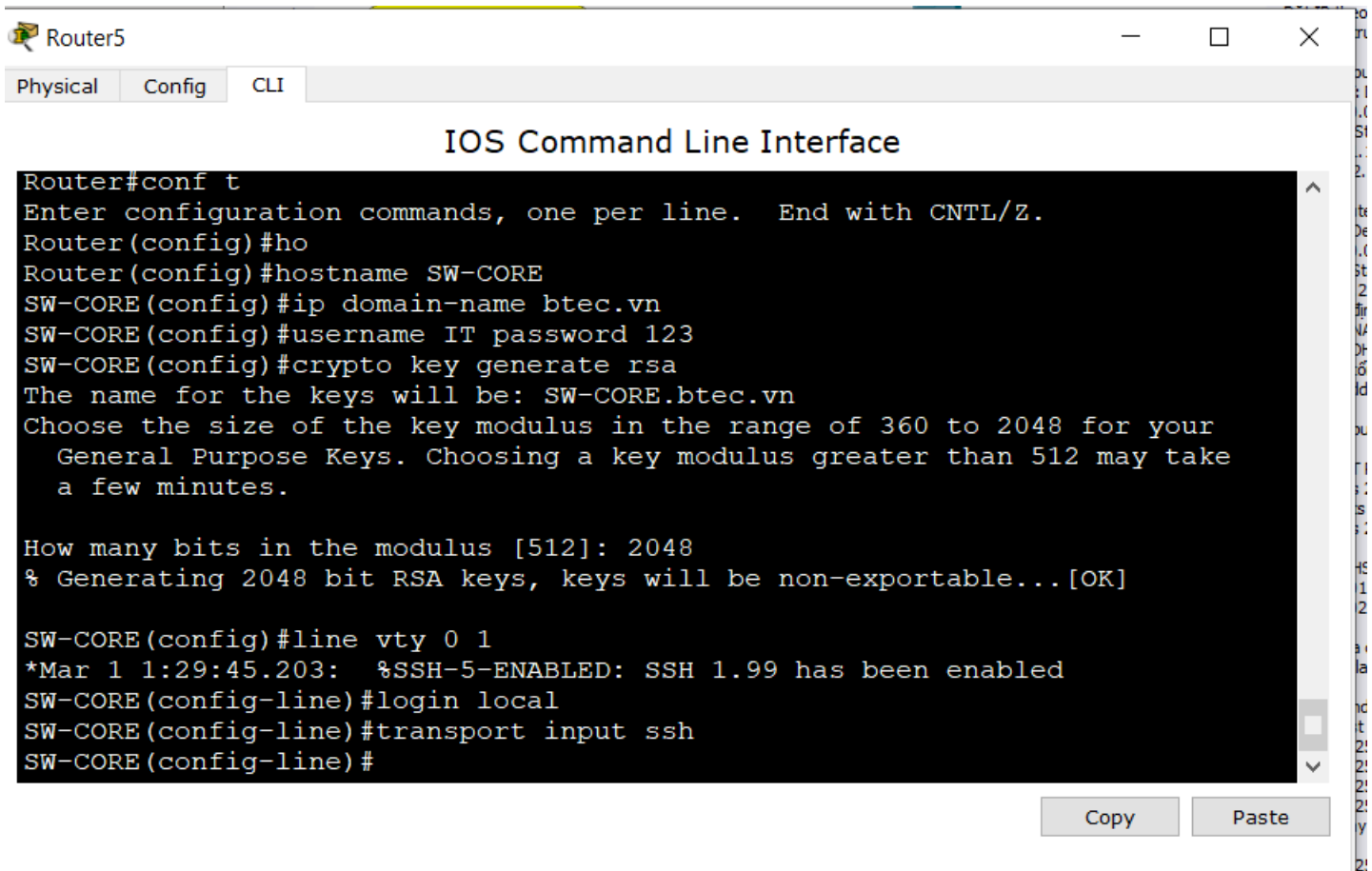
+R1-20.21.30.0/24

+R2-20.31.40.0/24

```
R2(config)#int se2/0
R2(config-if)#ip add 20.31.40.10 255.255.255.0
R2(config-if)#no shut
```

Set password

Create passwords and connection protocols for remote control of IT departments, they are allowed to log in to add, delete and configure the switch.



The screenshot shows a Cisco Router5 CLI window with tabs for Physical, Config, and CLI. The title bar reads "IOS Command Line Interface". The CLI session shows the following commands and output:

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ho
Router(config)#hostname SW-CORE
SW-CORE(config)#ip domain-name btec.vn
SW-CORE(config)#username IT password 123
SW-CORE(config)#crypto key generate rsa
The name for the keys will be: SW-CORE.btec.vn
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

SW-CORE(config)#line vty 0 1
*Mar 1 1:29:45.203:  %SSH-5-ENABLED: SSH 1.99 has been enabled
SW-CORE(config-line)#login local
SW-CORE(config-line)#transport input ssh
SW-CORE(config-line)#
```

At the bottom right of the window, there are "Copy" and "Paste" buttons.

VLANS

Create a Vlan

I will create the following VLANs in turn:

- + VLAN 10 (20.16.10.0/24): Staff
- + VLAN 20 (20.26.22.0/24): Student Lab
- + VLAN 30 (20.36.24.0/24): Teacher
- + VLAN 40 (20.46.30.0/24): IT
- + VLAN 50(20.56.32.0/24): Server
- + VLAN 60 (20.66.41.0/24): Guest

VTP configuration

The VTP protocol plays the role of maintaining the configuration of VLANs and uniformity across the network. VTP is a protocol that uses trunk lines to manage the addition, deletion, and modification of VLANs throughout the network from a central switch located in Server mode.

Conditions for obtaining VTP:

The lines between the Switches must be trunk:

```
Switch(config)#interface f0/3
BTEC-College(config)#
BTEC-College(config)#
BTEC-College(config)#int f0/3
BTEC-College(config-if)#sw mode trunk
BTEC-College(config-if)#
```

Configure VTP mode server on switch core:

```
BTEC-College(config)#vtp domain betc.vn
Changing VTP domain name from NULL to betc.vn
BTEC-College(config)#vtp pass
BTEC-College(config)#vtp password betec@123
Setting device VLAN database password to betec@123
BTEC-College(config)#vtp mode server
Device mode already VTP SERVER.
BTEC-College(config)#
```

Configure VTP mode client on switch:

```
Switch(config)#vtp domain betc.vn
Domain name already set to betc.vn.
Switch(config)#vtp pass betec@123
Setting device VLAN database password to betec@123
Switch(config)#vtp mode clien
Setting device to VTP CLIENT mode.
Switch(config)#
```

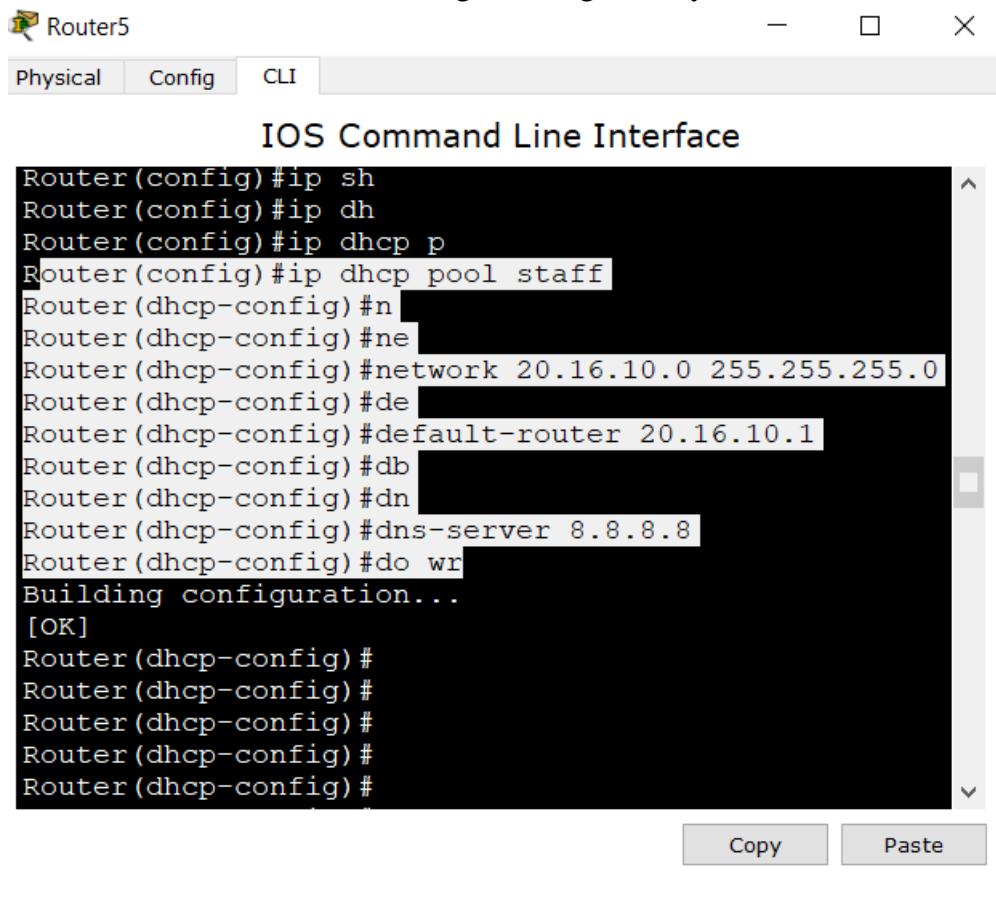
Routing between VLANs

- After creating the VLANs, if something goes wrong the other VLANs cannot communicate. In order for them to communicate, we configure routing between VLANs.
- On SW-L3, configuring the routing image between Vlan ensures that the other VLAN PCs communicate with each other:
- In here I create a subnetting in Router

Port	Link	IP Address
FastEthernet0/0	Up	<not set>
FastEthernet0/0.10	Up	20.16.10.1/24
FastEthernet0/0.20	Up	10.26.22.1/24
FastEthernet0/0.30	Up	20.36.24.1/24
FastEthernet0/0.40	Up	20.46.30.1/24
FastEthernet0/0.50	Up	20.56.32.1/24
FastEthernet0/0.60	Up	<not set>
FastEthernet1/0	Down	<not set>
Serial2/0	Down	<not set>
Serial3/0	Down	<not set>
FastEthernet4/0	Down	<not set>
FastEthernet5/0	Down	<not set>
Hostname: SW-CORE		

DHCP

On router, DHCP configuration grants dynamic IP to VLANs:



```

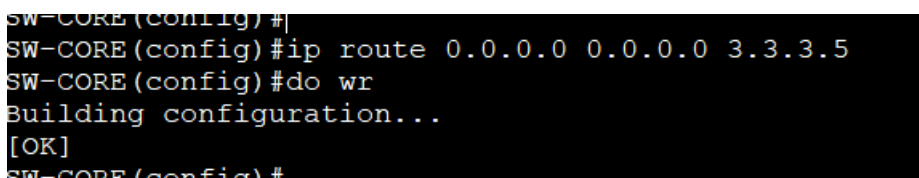
Router5
Physical Config CLI
IOS Command Line Interface
Router(config)#ip sh
Router(config)#ip dh
Router(config)#ip dhcp p
Router(config)#ip dhcp pool staff
Router(dhcp-config)#n
Router(dhcp-config)#ne
Router(dhcp-config)#network 20.16.10.0 255.255.255.0
Router(dhcp-config)#de
Router(dhcp-config)#default-router 20.16.10.1
Router(dhcp-config)#db
Router(dhcp-config)#dn
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#do wr
Building configuration...
[OK]
Router(dhcp-config)#
Router(dhcp-config)#
Router(dhcp-config)#
Router(dhcp-config)#
Router(dhcp-config)#
  
```

In addition to providing dynamic IP for VLAN 10, I also reserve the first 10 IPs of the range to use when needed.

For the remaining VLANs, we perform the same configuration.

Static routing.

Since the ip address range is an unknown number, when the router receives any ip address it will be directed to a certain network address.



```

SW-CORE(config)#
SW-CORE(config)#ip route 0.0.0.0 0.0.0.0 3.3.3.5
SW-CORE(config)#do wr
Building configuration...
[OK]
SW-CORE(config)#
  
```

NAT.

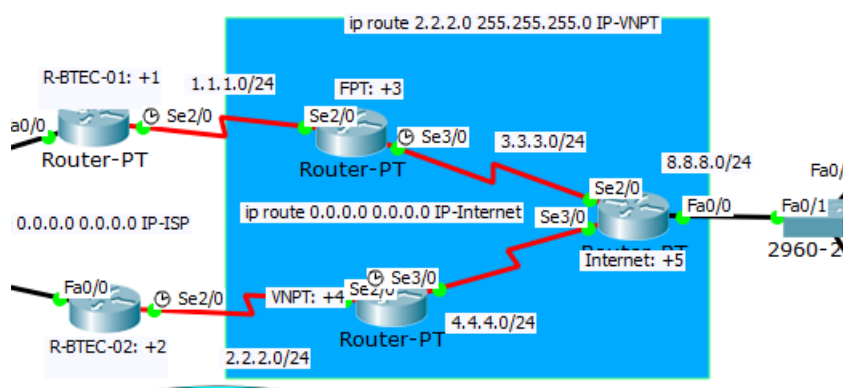
- NAT processing packets from inside a LAN going outside the internet (inside)
- NAT processes packets from outside the internet (outside) to the local network

```
SW-CORE(config)#int fa0/0
SW-CORE(config-if)#ip n
SW-CORE(config-if)#ip nat i
SW-CORE(config-if)#ip nat inside
SW-CORE(config-if)#int fa0/0.50
SW-CORE(config-subif)#ip n
SW-CORE(config-subif)#ip nat i
SW-CORE(config-subif)#ip nat inside
```

Recommend potential enhancements for the networked systems.

On the routers we will configure to create a virtual gateway router as gateway for the LAN to redundant gateways for the system. When a Router is failed, the system still works normally through the other routers. We will choose HSRP protocol to implement the above failover feature. We will also configure the track for the HSRP protocol.

The meaning of using HSRP: is a redundant protocol for a network system. The HSRP protocol in a network system requires at least two routers, a primary router called Active Router and a backup router called Standby Router. When using HSRP, routers work together in a group (group / standby group) to co-manage a Virtual Router. This Virtual Router has a virtual MAC and IP address managed by the Active and Standby Router and when hosts inside the network use the Virtual Router's IP address as the Default Gateway.



This case we have 2 Router R1-R2 and 2 Router company Internet VNPT and FPT, to ensure that the network connection is always stable when unexpected circumstances occur

We should create a subnetting same R1

+ R1: Active for VLAN 10,20,30 standby for VLAN 40, 50

+ R2: Active for VLAN 40,50 standby for VLAN 10,20,30

- **R1:**

- int f0/0.x (x=10,20,30)
- standby x ip VIP
- standby x priority 100
- standby x preempt
- standby x timers 1 3
- int f0/0 (y= 40,50)
- standby y ip VIP
- standby y priority 105
- standby y preempt
- standby y time 1 3
- standby track s2/0

```
R1(config)#int fa0/0.10
R1(config-subif)#standby 10 priority 105
R1(config-subif)#standby 10 preempt
R1(config-subif)#standby 10 timers 1 3
R1(config-subif)#standby 10 track s2/0
R1(config-subif)#
```

```
R1(config)#int fa0/0.20
R1(config-subif)#standby 20 priority 100
R1(config-subif)#standby 20 preempt
R1(config-subif)#standby 20 timers 1 3
R1(config-subif)#
```

- **R2:** we do same step R1

- int f0/0.x (x=10,20,30)
- standby x ip VIP
- standby x priority 100
- standby x preempt
- standby x timers 1 3
- int f0/0 (y= 40,50)
- standby y ip VIP
- standby y priority 105
- standby y preempt
- standby y time 1 3
- standby track s2/0

```
R2(config)#int fa0/0.10
R2(config-subif)#standby 10 priority 100
R2(config-subif)#standby 10 preempt
R2(config-subif)#standby 10 timers 1 3
R2(config-subif)#
```

When we tracer any pc from the inside to the address 8.8.8.8 (DNS address) will default to the ip address from the R1 side but when R1 is disconnected from the network it will immediately switch to R2.

HSRP is a Cisco standard intended to provide high availability of network systems by providing redundancy for hosts on a LAN that has been configured with a default gateway IP address. HSRP routes IP traffic without relying on the availability of a single router. HSRP allows a group of router interfaces to work together to represent the appearance of a virtual router or a default gateway to hosts on the LAN. When the HSRP is configured on a network or segment, it will be able to provide a Virtual MAC address and a shared IP address for a group of routers. HSRP allows two or more routers that have an HSRP feature configured to use the MAC address and IP address of a non-existent Virtual Router; it is represented as a common component for routers that have HSRP functionality configured to provide redundancy for each of those routers. One router is chosen as the Active Router and another will be selected as the Standby Router, and the Standby Router controls the group of MAC addresses and IP addresses if the Active Router fails.

Ip address R1: 20.97.32.1

Ip address R2: 20.97.32.2

VI. Document and analyse test result

1.SSH protocol

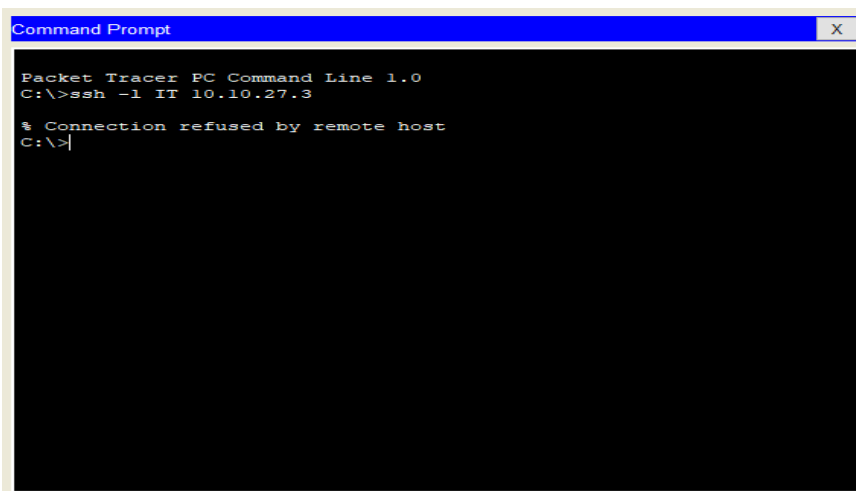
Only the IT staff can establish remote connections to routers and switches:

On a PC IT computer we can use the SSH protocol:

```
C:\>ssh -l IT 10.14.19.1
Password:

R>en
Password:
R#
```

For other VLAN computers, it will not be possible to SSH into the router and switch:

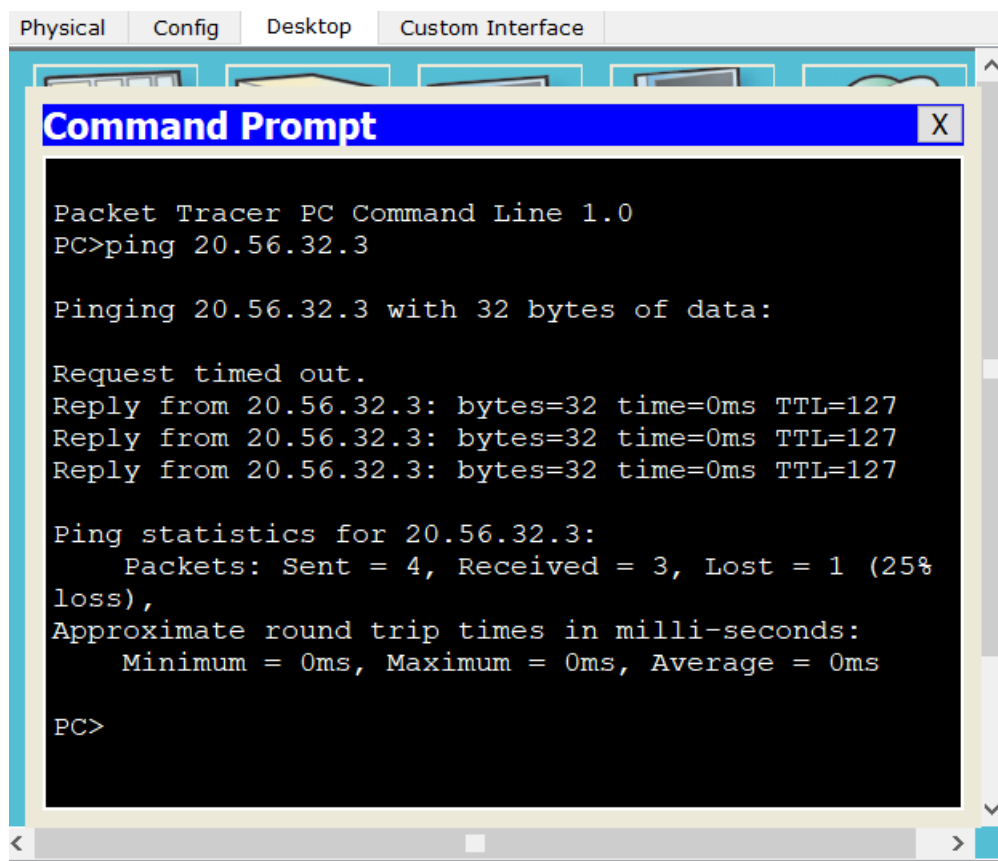


```

Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ssh -l IT 10.10.27.3
% Connection refused by remote host
C:\>
  
```

2.Vlan

After creating VLANs, computers belonging to the same VLAN can communicate with each other. And after routing between VLANs on Switch Core, other VLAN devices can also ping each other



```

Physical  Config  Desktop  Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 20.56.32.3

Pinging 20.56.32.3 with 32 bytes of data:

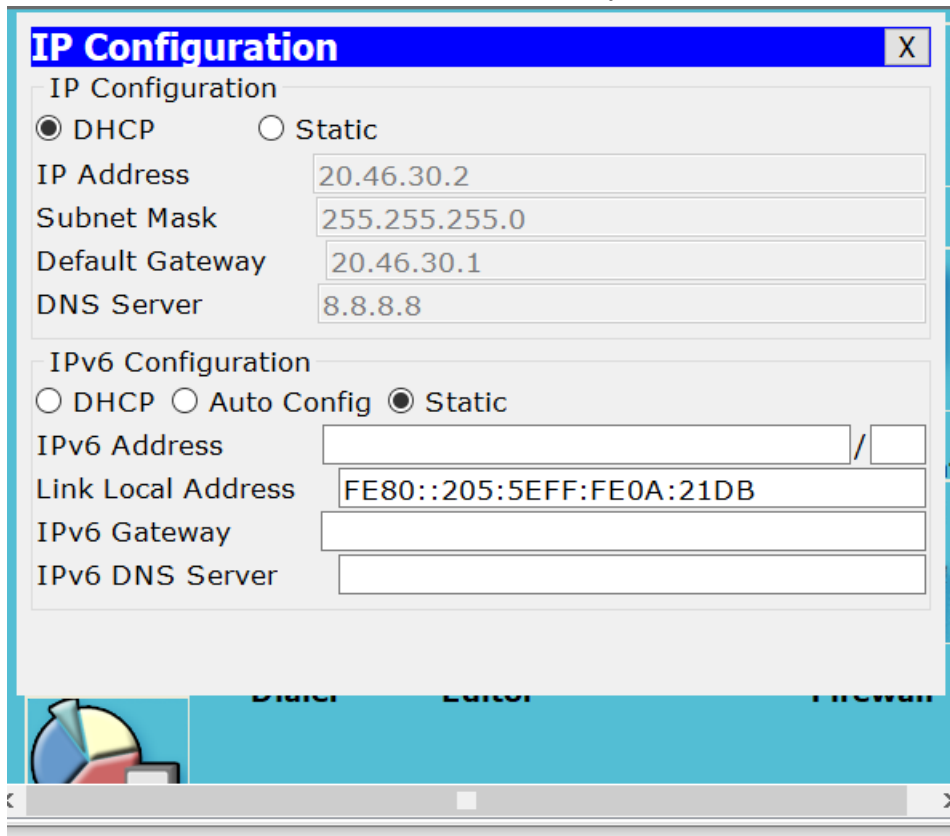
Request timed out.
Reply from 20.56.32.3: bytes=32 time=0ms TTL=127
Reply from 20.56.32.3: bytes=32 time=0ms TTL=127
Reply from 20.56.32.3: bytes=32 time=0ms TTL=127

Ping statistics for 20.56.32.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25%
    loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>
  
```

3.DHCP

After configuring DHCP on the core switch, the devices in the network are completely provided with a free IP corresponding to each VLAN, which reduces the effort for network administrators, no need to install manually.



IP Configuration [X]

IP Configuration

☒ DHCP ☐ Static

IP Address: 20.46.30.2

Subnet Mask: 255.255.255.0

Default Gateway: 20.46.30.1

DNS Server: 8.8.8.8

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address: [] / []

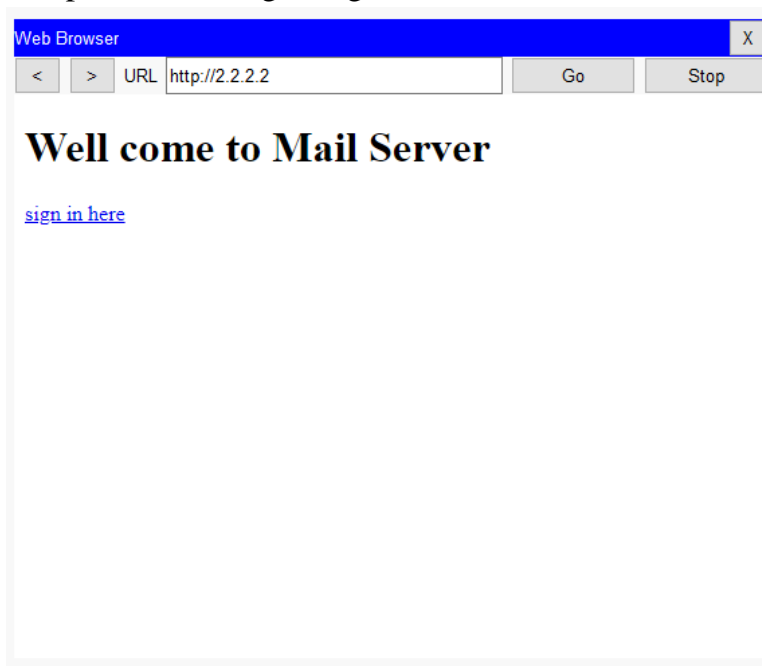
Link Local Address: FE80::205:5EFF:FE0A:21DB

IPv6 Gateway: []

IPv6 DNS Server: []

4.Static routing and NAT

Configuring static routing and NAT helps devices access to the Internet: An example of a computer accessing Google DNS:



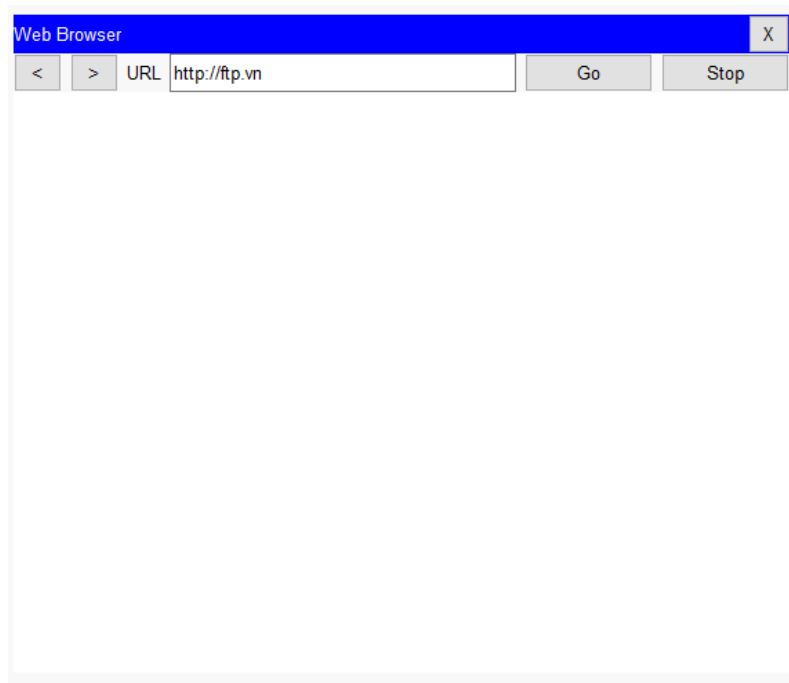
Web Browser [X]

< > URL: http://2.2.2.2 Go Stop

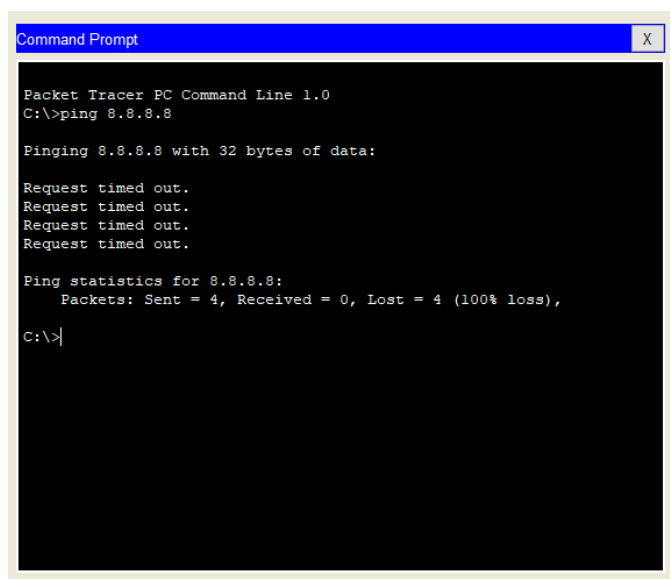
Well come to Mail Server

[sign in here](#)

Another example of internet access, this helps us control any computer that wants to go out to the internet but is not allowed.



Test ping 8.8.8.8 (Google Address):



5.ACI

Configure ACL

Only an IT department is allowed access to perform the function of adding, deleting, and other unrelated parts are not allowed to do so.

```
C:\>ssh -l IT 10.14.19.1

Password:

R>enable
Password:
R#
```

For other VLAN computers, it will not be possible to SSH into the router and switch:

```
Packet Tracer PC Command Line 1.0
PC>ssh -l it 20.46.30.2|
```

V. Proposing potential improvements for networked systems

The network system has been designed relatively completely, so in the event of an upgrade later, we will add a firewall system to make the system more secure.

VII. Conclude

In this report, I have outlined the following key points:

- Check their network rules and protocols.
- Interpret devices and network activities.

- Effective network design.
- Deploying and diagnosing networked systems.
- offer solutions to upgrade the system later.

VIII. References

Forcepoint. 2020. *What Is The OSI Model?*. [online] Available at:

<https://www.forcepoint.com/cyber-edu/osi-model>

2020. *The Advantages And Disadvantages Of Network Topologies*. [online] Available at:

<http://iptcommunications.weebly.com/the-advantages-and-disadvantages-of-network-topologies.html>

www.javatpoint.com. 2020. *Computer Network / TCP/IP Model - Javatpoint*. [online] Available

at: <https://www.javatpoint.com/computer-network-tcp-ip-model>

Hướng Dẫn Hostinger. 2020. *Tên Miền Là Gì? Toàn Bộ Khái Niệm Về Domain Name*. [online]

Available at: <https://www.hostinger.vn/huong-dan/ten-mien-la-gi-toan-bo-khai-niem-ve-domain-name/>

Software Reviews, Opinions, and Tips - DNSstuff. 2020. *What Is Network Topology? Best Guide To Types & Diagrams - Dnsstuff*. [online] Available at: <https://www.dnsstuff.com/what-is-network-topology>