UNIVERSITY of GREENWICH

Alliance with FPT Education

ĐẠI HỌC GREENWICH
(VIỆT NAM)

Liên kết với Tổ chức Giáo dục FPT

# ASSIGNMENT
# NETWORKING REPORT

**Student performance:** TRAN QUANG HUY

**ID:** GCD18457

**Class:** GCD0821

**Teacher:** TRAN DANG MINH KHOA

# Contents

# TABLE, FIGURE, PICTURE

# Part I. Networking principles and their protocols

## 1. The benefits and constraints of different network type and standards

### 1.1. Types of networks

- There are two most common types of network infrastructures are:
  - The local Area Network ( LAN) – LANs are the most frequently discussed networks, one of the most common, one of the most original and one of the simplest types of networks. LANs connect groups of computers and low-voltage devices together across. This types of network are very useful for sharing data likes files, small or big document, play network game etc.
    - Benefit:
      - Ability to share hardware and software resources
      - Individual workstation might survive network failure
      - Component and system evolution are possible
      - Support for heterogeneous forms of hardware and software
      - Access to other LANs and WANs
      - Private ownership
      - Secure transfers at high speeds with low error rates.
    - Constraints:
      - Limited number of systems can only be connected.
      - Cannot cover large area.
      - Network performance degrades as number of users exceeds.

- Wide area Network (WAN) can contain multiple smaller networks such as LANs or MANs. The internet is the best-know example of a public WAN.
  - Benefit:
    - WAN has no limit of area, so it is world wide network.
    - Many country's organizations have facility to form their global integrated network through WAN.
    - WAN support global markets and global business.
    - For a network database, WAN allows users all over a networks to access and update a single, consistent view of data.
  - Constraints:
    - WAN is very big and complex network.
    - It is maybe slow in speed.
    - WAN is not very much secured means not reliable.
    - It is very costly because we have to pay every time for transferring data.
    - Very much dependency on the third party because it is public network.

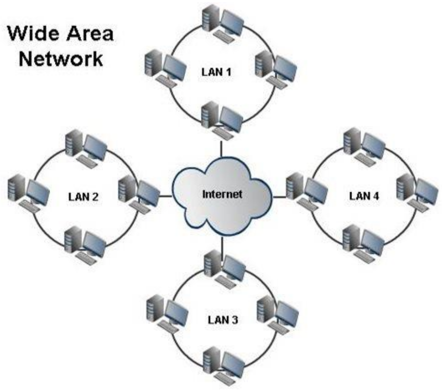
- Other types of network:

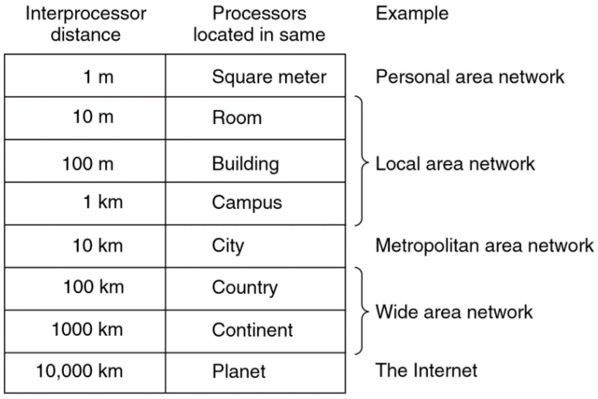
  - MAN: Metropolitan Area Network – MAN is larger than a LAN but smaller than WAN and often used to connect several LANs together to form a bigger network.
  - SAN: Storage-Area Network – As a dedicated high-speed network that connects shared pools of storage devices to several servers, these types of networks do not rely on a LAN or WAN and SANs can be accessed in the same fashion as a drive attached to a server.

- WLAN: Functioning like a LAN, WLANs use wireless network technology such as WiFi.
- PAN – Personal Are Network
- CAN – Campus Area Network
- EPN – Enterprise Private Network
- VPN – Virtual Private Network
- POLAN – Passive Optical Local Area Network
    - Example: WAN = LAN+LAN+LAN + (more)

      INTERNET = WAN+WAN+WAN+ (more)

**Figure 1.1**





| Interprocessor distance | Processors located in same | Example |
|---|---|---|
| 1 m | Square meter | Personal area network |
| 10 m | Room | Local area network |
| 100 m | Building | |
| 1 km | Campus | |
| 10 km | City | Metropolitan area network |
| 100 km | Country | Wide area network |
| 1000 km | Continent | |
| 10,000 km | Planet | The Internet |

**Figure 1.2 : Example network types**

## 1.1. Networking standards

- Ensure the interoperability of networking technology by defining the rules of communication among networked devices. Networking standards exits to help ensure products of different vendors are able to work together in a network without risk of incompatibility.
    - Example about networking standards: IEEE, ISO
        - WPAN: Bluetooth (IEEE 802.15.1)
        - WLAN: WiFi (IEEE 802.11)
        - WWAN: GSM, 3G phone nets
        - Internetwork: Internet Standards

# 2. The impact of network topology, communication and bandwidth requirements

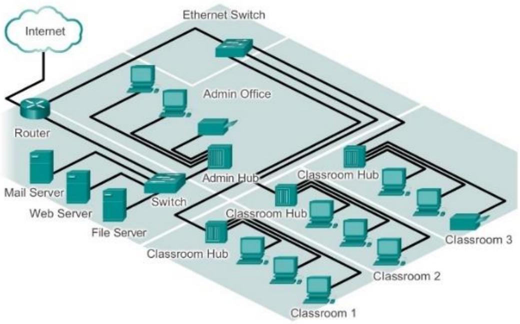
## 2.1. Network topology, communication and bandwidth requirements

### 2.1.1. Network topology

Network topology is the layout of the connection of a computer network. There are two main types of topology. Network topologies may be physical or logical.

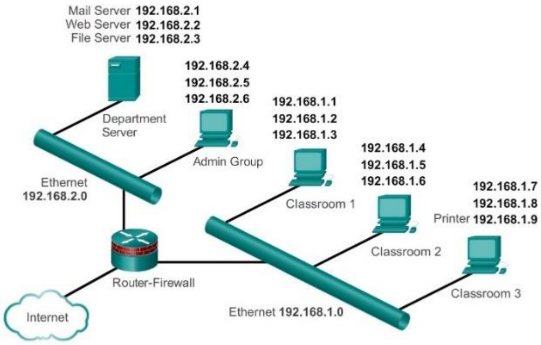
- Physical topology means the physical design of a network including the devices, location and cables.

**Figure 1.3** Physical Topology



- Logical topology is about how data actually move around in a network not its physical design.

**Figure 1.4** Logical Topology



### 2.1.2. Communication

- The Data communication refers to the transmission of the digital data between two or more computers The physical connection between networked computing devices is established using either cable media or wireless media.

- The communication has the rules:

  - An identified sender and receiver.
  - Agreed upon method of communicating.
  - Common language and grammar.
  - Speed and timing of delivery.
  - Confirmation or acknowledgment requirements.

- The message source when was transmitting need to be encoded and decoded when receive

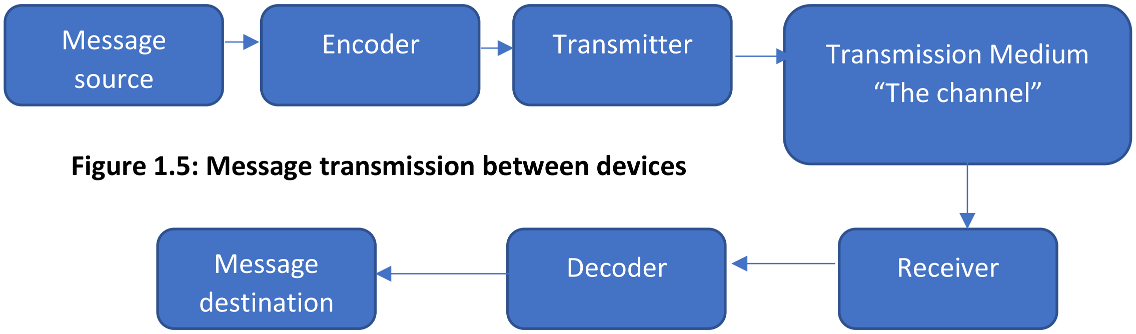


**Figure 1.5: Message transmission between devices**

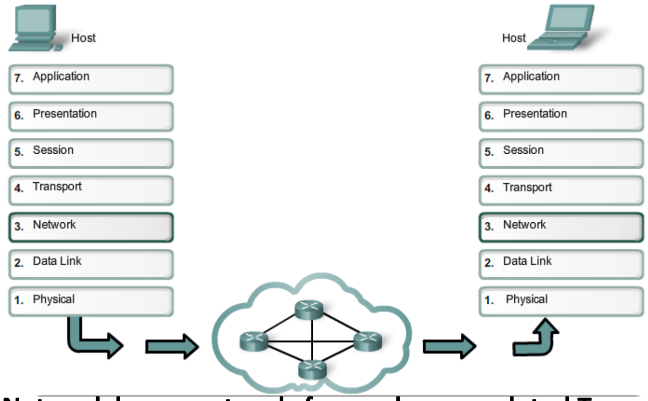
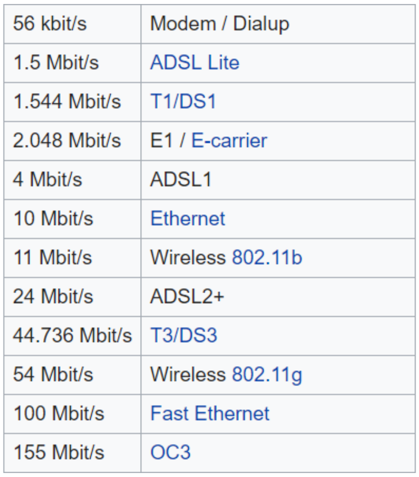


**Figure 1.6: Network layer protocols forward encapsulated Transport Layer**

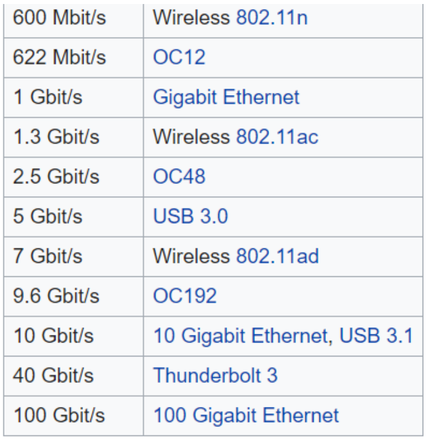
### 2.1.3. Bandwidth

- Bandwidth is the maximum rate of date transfer across give path. Bandwidth may be characterized as network bandwidth, data bandwidth or digital bandwidth

- The maximum bandwidth of common Internet access technologies:



| | |
|---|---|
| 56 kbit/s | Modem / Dialup |
| 1.5 Mbit/s | ADSL Lite |
| 1.544 Mbit/s | T1/DS1 |
| 2.048 Mbit/s | E1 / E-carrier |
| 4 Mbit/s | ADSL1 |
| 10 Mbit/s | Ethernet |
| 11 Mbit/s | Wireless 802.11b |
| 24 Mbit/s | ADSL2+ |
| 44.736 Mbit/s | T3/DS3 |
| 54 Mbit/s | Wireless 802.11g |
| 100 Mbit/s | Fast Ethernet |
| 155 Mbit/s | OC3 |



| | |
|---|---|
| 600 Mbit/s | Wireless 802.11n |
| 622 Mbit/s | OC12 |
| 1 Gbit/s | Gigabit Ethernet |
| 1.3 Gbit/s | Wireless 802.11ac |
| 2.5 Gbit/s | OC48 |
| 5 Gbit/s | USB 3.0 |
| 7 Gbit/s | Wireless 802.11ad |
| 9.6 Gbit/s | OC192 |
| 10 Gbit/s | 10 Gigabit Ethernet, USB 3.1 |
| 40 Gbit/s | Thunderbolt 3 |
| 100 Gbit/s | 100 Gigabit Ethernet |

**Table 1.1: Example about bandwidth**

## 3. Protocols

- **Conceptual models e.g. OSI model, TCP/IP model:**

  - **OSI (Open Systems Interconnection):**

The main concept of OSI is that the process of communication between two endpoints in a network can be divided into seven distinct groups of related functions, or layers. Each layers serves the layer above it and, in turn, is served by the layer below it. If the user send the message, there will be flow of date down through the layers in the source computer, and then up through the layers in the receiving computer.

The seven Open Systems Interconnection layers are:

- Layer 7: The application layer. Network process to application.

- Layer 6: The presentation layer. Data representation and encryption.

- Layer 5: The session layer. This layer sets up, coordinates and terminates communication. Its services include authentication and reconnection after an interruption. On the internet, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) provide these services for most applications.

- Layer 4: The transport layer. The transport layer provides end-to-end data transfer between end-users. The transport layer controls the reliability of a given connection, establishes, maintains, and terminates virtual circuits. The transport layer can monitor the transmission of packets and retransmit the dropped packets.

- Layer 3: The network layer. The network provides functions and processes for the transmission of data strings of various lengths, from one source to another, through one or more networks, while maintaining quality of service ) that the required transport layer, responsible for building the best route for data. The network performs routing functions. Routers operate at this layer, sending routing data over the extended network, making networking possible. IP is the underlying protocol for network layer operations. The data on this layer is called packets.

- Layer 2: The data-link layer. This layer responsible for encoding and decoding of the electrical signal into bits, manage data errors from the physical layer, convert electrical signal into frames. The data link layer divided into two sub-layers: MAC and LLC layer. Some devices like Switch work at this layer.

- Layer 1: The physical layer. This layer responsible for electrical signals, light, signal etc. Some devices like repeater, hub, cables, Ethernet work on this layer.

- **TCP/IP model**

The TCP / IP model is more lightweight than the OSI reference model. For example, the OSI model's transport layer specifies that data transfer must be completely reliable. However, some new applications developed later such as Voice over IP, Video Conference, etc. require high speed and allow to ignore some minor bugs. If the OSI model is still in use, the latency on the network is very high and does not guarantee quality of service. The TCP / IP model, in addition to the main transport layer protocol, is TCP (Transmission Control Protocol), which also provides UDP (User Datagram Protocol) adaptability for high speed applications. TCP/IP model has 4 layers:

- The Link layer: is the lowest layer of the TCP/IP model. This link layer is the combine of physical and datalink layer into one single layer. This layer include modulation, line coding and bit synchronization. Some protocols include: ARP, NDP, IEEE 802.3 and IEEE 802.11
- The Internet layer: is the next layer to the link layer and this layer work with the network layer of the OSI model. Functions of this layer are traffic routing, traffic control, fragmentation and logical addressing. Some protocols include: IP, ICMP, IGMP.
- The Transport layer: this layer has the same name and relate to transport layer in OSI model. Functions of this layer are traffic control, session multiplexing, segmentation, error detection and correction, and message reordering. Some protocols include TCP, UDP.
- The Application layer: this is the highest layer in TCP/IP model and it is related to the session, presentation and application layer in the OSI model. This layer’s functions include session establishment, character code, maintenance, termination and handle all process to process communication functions.

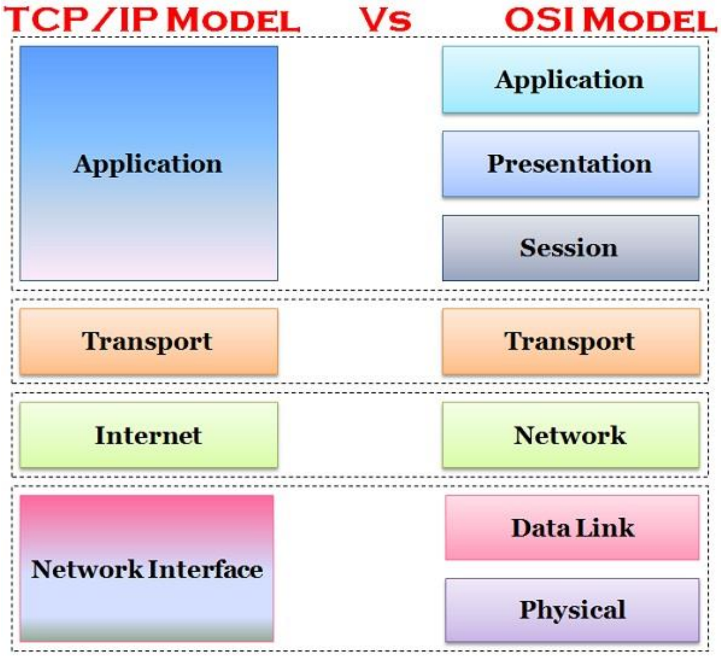
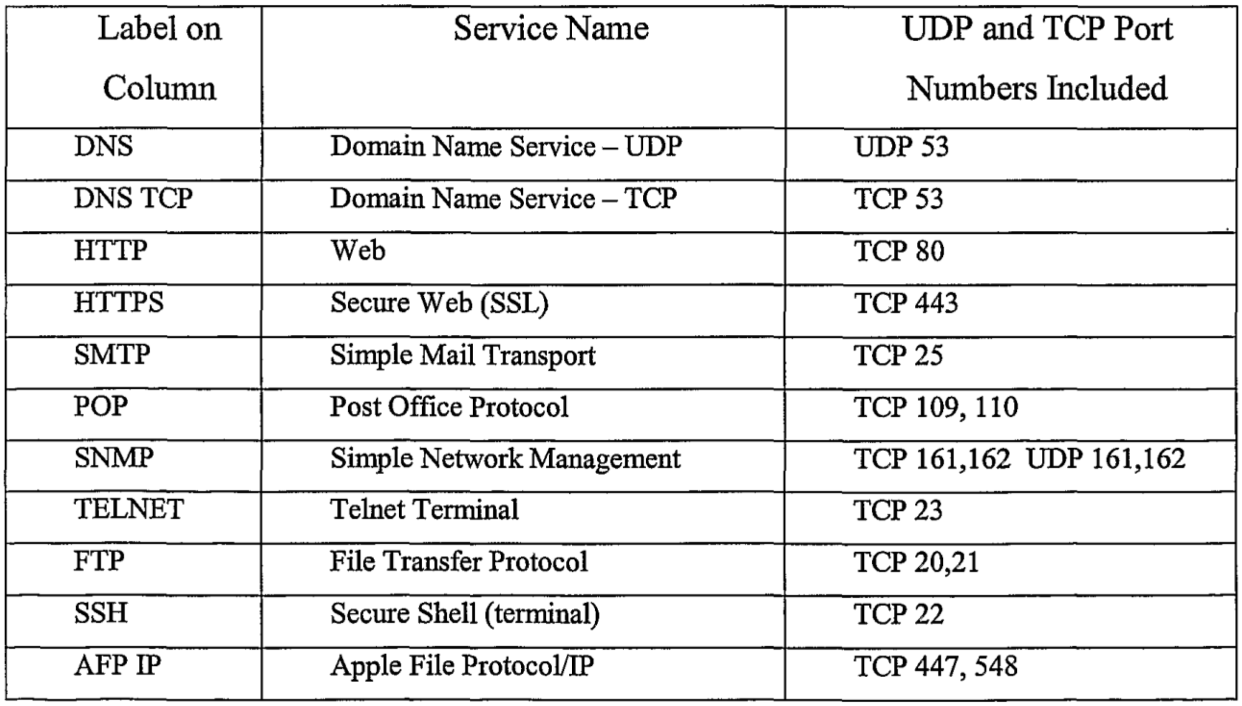


**Figure 1.8: TCP/IP model and OSI model**



| Label on Column | Service Name | UDP and TCP Port Numbers Included |
|---|---|---|
| DNS | Domain Name Service – UDP | UDP 53 |
| DNS TCP | Domain Name Service – TCP | TCP 53 |
| HTTP | Web | TCP 80 |
| HTTPS | Secure Web (SSL) | TCP 443 |
| SMTP | Simple Mail Transport | TCP 25 |
| POP | Post Office Protocol | TCP 109, 110 |
| SNMP | Simple Network Management | TCP 161,162 UDP 161,162 |
| TELNET | Telnet Terminal | TCP 23 |
| FTP | File Transfer Protocol | TCP 20,21 |
| SSH | Secure Shell (terminal) | TCP 22 |
| AFP IP | Apple File Protocol/IP | TCP 447, 548 |

**Figure 1.9: Protocol and Port**

## 4. Compare common networking principles and how protocols enable the effectiveness of networked systems.

### 4.1. Common networking principles:

- If the IP packet loss, packet delay and delay variation. Therefore, you need to enable most of the Quality of Service (QoS) mechanisms available on switches and routers throughout the network. For the same reasons, redundant devices and network link that provide quick convergence after network failures or topology changes are also important to ensure highly available infrastructure.

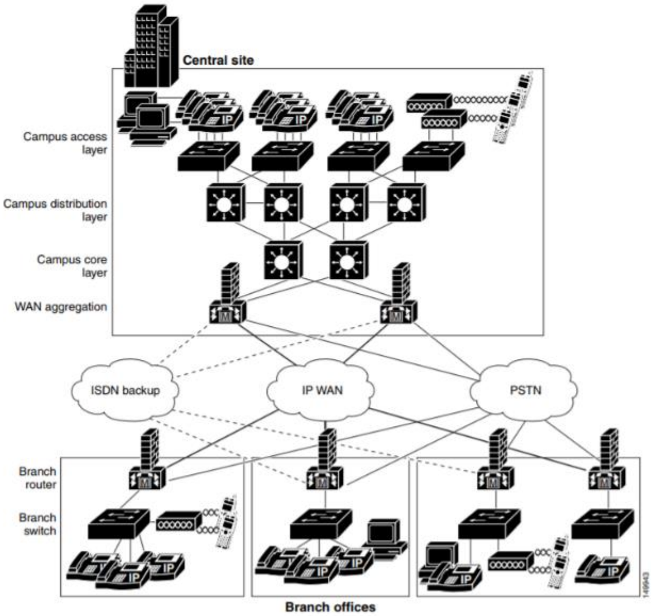
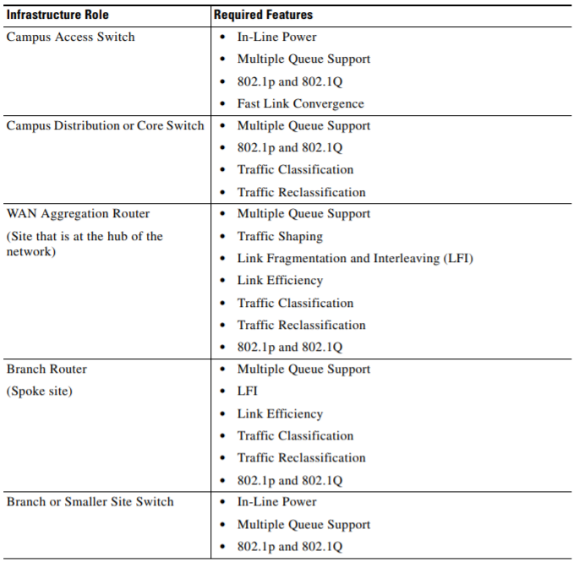


Figure 1.10 : Typical Campus Network



| Infrastructure Role | Required Features |
|---|---|
| Campus Access Switch | • In-Line Power<br>• Multiple Queue Support<br>• 802.1p and 802.1Q<br>• Fast Link Convergence |
| Campus Distribution or Core Switch | • Multiple Queue Support<br>• 802.1p and 802.1Q<br>• Traffic Classification<br>• Traffic Reclassification |
| WAN Aggregation Router<br>(Site that is at the hub of the network) | • Multiple Queue Support<br>• Traffic Shaping<br>• Link Fragmentation and Interleaving (LFI)<br>• Link Efficiency<br>• Traffic Classification<br>• Traffic Reclassification<br>• 802.1p and 802.1Q |
| Branch Router<br>(Spoke site) | • Multiple Queue Support<br>• LFI<br>• Link Efficiency<br>• Traffic Classification<br>• Traffic Reclassification<br>• 802.1p and 802.1Q |
| Branch or Smaller Site Switch | • In-Line Power<br>• Multiple Queue Support<br>• 802.1p and 802.1Q |

Figure 1.11 : Required Features for Each Role in the Network Infrastructure

**- Core layer:** Provides optimal transport between sites and high-performance routing. Due the criticality of the core layer, the design principles of the core should provide an appropriate level of resilience that offers the ability to recover quickly and smoothly after any network failure event with the core block.

- **Distribution layer:** Provides policy-based connectivity and boundary control between the access and core layers.

- **Access layer:** Provides workgroup/user access to the network. The two primary and common hierarchical design architectures of enterprise campus networks are the three-tier and two-tier layers models.

## 4.2. Protocols enable the effectiveness of networked systems

- A network protocol defines rules and conventions for communication between network devices. Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received. Some protocols also support message acknowledgment and data compression designed for reliable and/or high-performance network communication.

- Internet Protocol: The Internet Protocol family contains a set of related (and among the most widely used) network protocols. Beside Internet Protocol itself, higher-level protocols like TCP, UDP, HTTP, and FTP all integrate with IP to provide additional capabilities.

- Wireless Network Protocols: Wireless networks have become commonplace. Network protocols designed for use on wireless networks must support roaming mobile devices and deal with issues such as variable data rates and network security.

- Network Routing Protocol: Routing protocols are special-purpose protocols designed specifically for use by network routers on the internet. A routing protocol can identify other routers, manage the pathways between sources and destinations of network messages, and make dynamic routing decisions.

# Part.2 Networking devices and operations

## 1. The operating principles of networking devices and server types

### 1.1. Networking devices:

- Repeater: A repeater operates at physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. Sometime when repeater sent many messages that will cause a collision and we use CSMA/CD to reduce collision. Repeater just has maximum 4 ports and range up to 80m.

- Hub: A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, simply a convenient means of connecting host and extending segments of Ethernet and other broadcast local network technologies. Hubs cannot filter data, so data packets are sent to all connected devices.

- Bridge: A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. Bridges also means link networks of different types.

- Switch: Switches perform a similar function to routers, but for local networks (normally Ethernets) only. Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only (Correct MAC on mac-table).

- Router: A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

- Access Point: A wireless access point (WAP) is a networking hardware device that allows a Wi-Fi device to connect to a wired network. In Access Point, SSID is the most important which people can connect AP, beside that we can set Security and mana option in AP. If we put too much AP nearly, the signal maybe is unstable so we need to set Standard Channel away 5 channel of each.

- Fire Wall: Firewall is a network security system that monitors and control incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as Internet.

- Gateway: A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer.

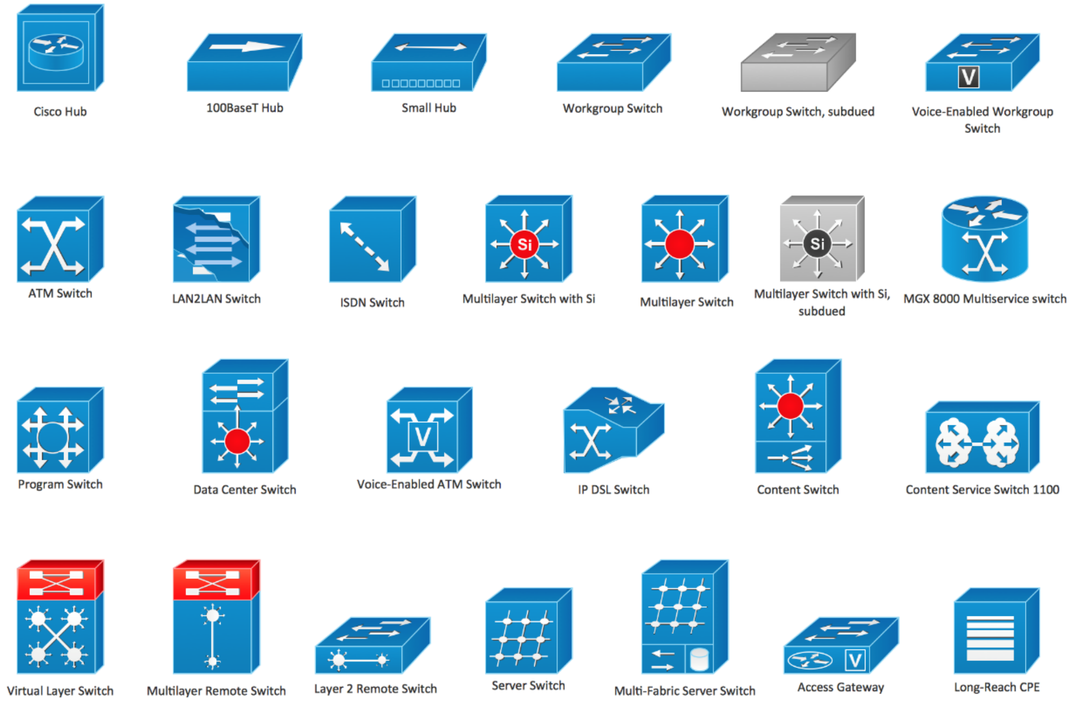


**Figure 2.1 : Network Devices icon**

## 1.2. Server types:

- Servers are often dedicated, meaning that they perform no other tasks besides their server tasks. Different servers do different jobs, from serving email and video to protecting internal networks and hosting Web sites.

- Proxy Server: A proxy server sits between a client program (typically a Web browser) and an external server (typically another server on the Web) to filter requests, improve performance, and share connections.

- Mail Server (Port: 25, 109 and 110): Almost as ubiquitous and crucial as Web servers, mail servers move and store mail over corporate networks (via LANs and WANs) and across the Internet.

- Server Platforms: A term often used synonymously with operating system, a platform is the underlying hardware or software for a system and is thus the engine that drives the server.

- Web Server (Port: 80): A Web server serves static content to a Web browser by loading a file from a disk and serving it across the network to a user's Web browser. This entire exchange is mediated by the browser and server talking to each other using HTTP.

- Application Server: Sometimes referred to as a type of middleware, application servers occupy a large chunk of computing territory between database servers and the end user, and they often connect the two.

- Real-Tome Communication Server: Real-time communication servers, formerly known as chat servers or IRC Servers, and still sometimes referred to as instant messaging (IM) servers, enable large numbers users to exchange information near instantaneously.

- FTP Server (Port: 20,21): One of the oldest of the Internet services, File Transfer Protocol makes it possible to move one or more files securely between computers while providing file security and organization as well as transfer control.

- Virtual Server: The number of virtual servers deployed exceeded the number of physical server and server virtualization has become near ubiquitous in the data center.

## 1.3. Network design topology infrastructure based on a prepared design and list the different type of topologies:

### 1.3.1. Network design topology infrastructure based on a prepared design

- Enterprise:

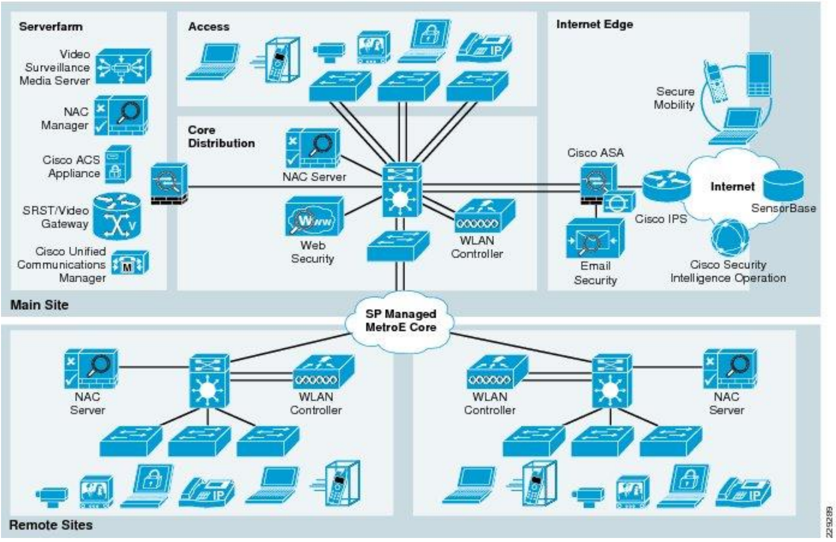


**Figure 2.2 : Network design topology for small Enterprise**

- Small business:

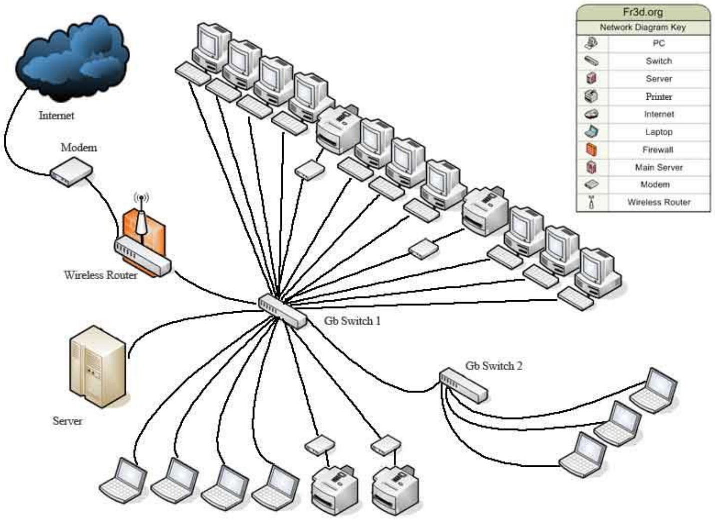


**Figure 2.3 : Network design topology for small business**

### 1.3.2. Types of topology:

- Bus: All devices are connected to one cable called the bus.
    - Advantages:
        - Low cost.
        - Easy to expand.
        - If one device down, the system still working.
    - Disadvantages:
        - If the cable fail, all of the system will stop working.
        - Will make data collision.

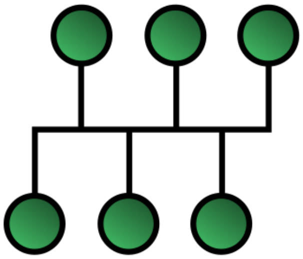


**Figure 2.5 : Topology Bus**

- Star: In local area networks, each network host is connected to a central hub with a point-to-point connection. All traffic on the network passes through the central hub.
    - Advantages:
        - Easy to install, configure, manage and expand.
        - Centralized management.
        - It doesn't be effected when you add or remove a device.
    - Disadvantages:
        - Need more cable than bus topology
        - If the hub is down, all the network will be down.
        - Higher cost.

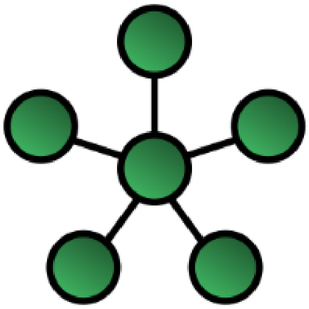


**Figure 2.6 : Topology Star**

- Ring: Set-up in a circular fashion in which data travels around the ring in one direction and each device on the ring acts as a repeater to keep the signal strong as it travels.
    - Advantages:
        - No collision.
        - Reliable and offer greater speed.
        - Can handle large amount of data.
    - Disadvantages:
        - More cable required.
        - Device have to wait for its turn.
        - The more device exists, the more slow data is transferred.
        - One device works incorrectly will affect the network.

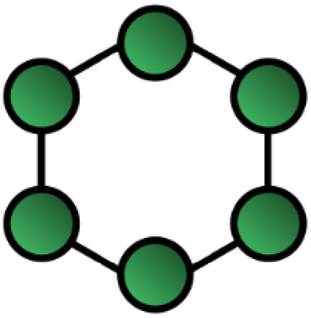


**Figure 2.7 : Topology Ring**

- Mesh: The network are connected to more than one other node in the network with a point-to-point this makes it possible to take advantage of some of redundancy that provided by a physical fully connected mesh topology. All data is transmitted between nodes in the network takes the shortest path between nodes

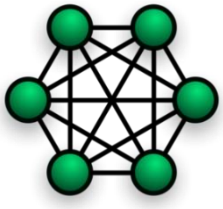


**Figure 2.8 : Topology Mesh**

- Tree: A central 'root' node is connected to one or more other nodes that are one level lower in the hierarchy with a point-to-point link between each of the second level nodes and the top level central 'root' node

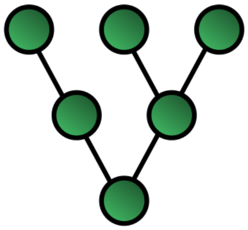


**Figure 2.9 : Topology tree**

## 2. The interdependence of workstation hardware with relevant networking software

- Network interface card (NIC): is a computer hardware component that connects a computer to a computer network. The network controller implements the electronic circuitry required to communicate using a specific physical layer and data link layer standard such as Ethernet of WiFi. This provides a base for a full network protocol stack, allowing communication among computer on the same LAN and larger-scale network communication through routable protocols, such as Internet Protocol (IP) by using cables or wirelessly.
- Permissions: Network access control ( NAC): NAC is the access control – who or what has authorized permission to access the network. This includes both users and devices. The NAC network intercepts the connection requests, which are then authenticated against a designated identity and access management system.
- System bus: is a single computer bus that connects the major components of a computer system, combining the functions of a data bus to carry information, an address bus to determine where it should be sent, and a control bus to determine its operation.
- Local systems architecture: Is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system.
- Network device memory: One of the most important components of network infrastructure and the longevity of system. Network memory dictates the amount of data stored or transferred on a device and can disrupt the performance of a network by acting as a bottleneck.
- I/O devices ( Input/ Output devices): is any hardware used by human operator or other systems to communicate with a computer. As the name suggests, input/

output devices are capable of sending data to a computer and receiving data form a computer

- Processor devices: When a computer receives data form an input device the data must go through an intermediate stage before it can be sent to an output device. A processing device is any device in a computer that handles this intermediate stage such as Network Card

## 3. Explore a range of server types and justify the selection of a server, considering a given scenario regarding cost and performance optimization

- This network system use cable: UTP CAT5
- This cable link Server to Router, Router to Router, Router to Switch, Switch to Switch and Computer to Switch.

| QTY | Line | Length (m) |
|---|---|---|
| 1 | Server → Router | 14m |
| 2 | Router → Router | 70m |
| 3 | Router → Switch | 24m |
| 4 | Switch → Switch | 15m |
| 5 | Computer → Switch | 500m |
| **Total** | | **623m** |

**Table 2.1: The length of Cable**

- **Computer:**

  - Staff computer:

| QTY | Devices | Specific Information | Quantity | Price | Amount |
|---|---|---|---|---|---|
| 1 | Mainboard | Asus H81 | 1 | $55 | $55 |
| 2 | CPU | CPU Intel® i3 - 4160 | 1 | $77 | $77 |
| 3 | HDD | 500Gb, SATA, 7200Rpm, 3.0Gbs | 1 | $21 | $21 |
| 4 | Case | Small Form Factor | 1 | $8 | $8 |
| 5 | Power | 350W - ELITE - PSU001 | 1 | $23 | $23 |
| 6 | RAM | 4Gb, 1333Mhz, DDR3 | 1 | $17 | $17 |
| 7 | Keyboard | A4 tech | 1 | $6 | $6 |
| 8 | Mouse | Mitsumi | 1 | $4 | $4 |
| 9 | LCD | Dell 19 Monitor 18.5 inch | 1 | $57 | $57 |
| **Total** | | | | | **$268** |

**Table 2.2: Information about Staff Computer**

- Student computer:

| QTY | Devices | Specific Information | Quantity | Price | Amount |
|---|---|---|---|---|---|
| 1 | Mainboard | Asus H81 | 1 | $55 | $55 |
| 2 | CPU | CPU Intel® i3 - 3220 | 1 | $77 | $40 |
| 3 | HDD | 200Gb, SATA, 7200Rpm, 3.0Gbs | 1 | $9 | $9 |
| 4 | Case | Small Form Factor | 1 | $8 | $8 |
| 5 | Power | 350W - ELITE - PSU001 | 1 | $23 | $23 |
| 6 | RAM | 4Gb, 1333Mhz, DDR3 | 1 | $17 | $17 |
| 7 | Keyboard | A4 tech | 1 | $6 | $6 |
| 8 | Mouse | Mitsumi | 1 | $4 | $4 |
| 9 | LCD | Dell 19 Monitor 18.5 inch | 1 | $57 | $57 |
| **Total** | | | | | **$219** |

**Table 2.3: Information about Student Computer**

- **Network devices**

| QTY | Name devices | Quantity | Price | Amount |
|---|---|---|---|---|
| 1 | Access Point (WRT 300N) | 3 | $240 | $720 |
| 2 | Cable UTP (Dintek CAT5.5E UTP)- 305m/box | 3 | $80 | $240 |
| 3 | Connector RJ45 CAT5 100c/box | 1 | $14 | $14 |
| 4 | Printer (Dell C1760NW) | 3 | $190 | $570 |
| 5 | PC client (Staff) | 35 | $268 | $9380 |
| 6 | PC client (Student) | 50 | $219 | $10950 |
| 7 | Server | 2 | $2000 | $4000 |
| 8 | Switch (WS-C2960-24TT-26 Port) | 5 | $250 | $1250 |
| 9 | Router (Cisco 2621 XM) | 7 | $220 | $1540 |
| **Total** | | | | **$28664** |

**Table 2.4: Information about network devices**

## 4. Considering a given scenario, identify the topology protocols selected for the efficient utilisation of a networking system.

- This network system need the bandwidth : 100 Mbps data transfer so the Protocol: Fast Ethernet (100Mbs), Gigabit Ethernet (1Gbs) and Cable Twisted Pair (CAT5) were used and we should use the Star Topology for network:

  - Advantages:
    - Easy to install, configure, manage and expand.
    - Centralized management.
    - It doesn’t be effect when you add or remove a device.
    - The system ensure work well with maximum rate of data transfer.

    - Reduce the bottleneck in network system when too much data transfer in network system.

- Disadvantages:
    - Need more cable
    - If the Switch is down, all the network will be down.
    - Higher cost.

# Part 3: Design efficient networked systems

## 1. Design a network system to meet a given specification

### 1.1. General network system

- The network system that I design is a project for a local educational institution.
  - Purpose:
    - Everyone in the building can use computer to service different mission.
    - All computer can connect together.
    - Construction cost is appropriate.
    - Ensure aesthetics: the equipment and the line are arranged in accordance .
    - This network has web server and file Server.
- The building has 3 floors and structure are:
  - Ground floor: 35 computers and printer used for staff (IP: 192.168.1.0/24)
    - Room 1: 15 staff computers + 1 Switch (WS-C2960-24TT-26 Port) + 1 printer.
    - Room 2: 20 staff computers + 1 Switch (WS-C2960-24TT-26 Port) + 2 printers.
    - Room 3 (Rest room): 1 wireless router + 1 Router (Cisco 2621 XM).
  - First floor: 30 Computers at Lab 1 for student. (IP: 192.168.2.0/24)
    - Room 1 (Lab 1): 30 student lab computers + 2 Switch (WS-C2960-24TT-26 Port).
    - Room 2 (Library): 1 wireless router + 1 Router (Cisco 2621 XM)

- Second floor: 20 Computer at Lab 2 for student and server Room. (IP: 192.168.3.0/24)
  - Room 1: 20 student lab computers + 1 Switch (WS-C2960-24TT-26 Port) .
  - Room 2 (Rest room): 1 wireless router + 1 Router (Cisco 2621 XM).
  - Room 3 (Server room): 1 File Server + 1 Mail Server + 4 Router (Cisco 2621 XM).

- We use Star topology for this network.
- Data transfer in the network with bandwidth: 100Mbs and 1Gbs.
- The Cable we use is UTP – Dintek CAT5.5E UTP and Connector RJ45 CAT5.
- The computer are configured to suit work and study.
- Each computer has a specific private IP and connect each together.
- This system has web server and file server located in second floor.
- Based on a prepared design that I have to implement a network system for 3 floor with specific functions.
- This Network System use 3 different IP on each floor for devices. So we can easy manage the system through IP and troubleshoot problem.

### 1.2. Design the network system:

- **Second floor: (20 Computer, 1 Wireless, 5 Router, 2 Server).**

- This Floor we connect 20 Student computers with 1 switch 26 Ports (Have vlan 40, IP: 192.168.3.16/26, topology: Star) through port Fast Ethernet, this switch connected to Sub Router through port Giga Ethernet at nearly Room (Rest Room) and wireless (Rest Room 2nd Floor, IP: 192.168.3.80/25) also.
- At Room server, there are 2 Server: File Server (IP: 8.8.8.8/28) and Mail Server (IP: 9.9.9.9/28) connect with 2 Router. This core layer is Three Router Server connected (IP: 10.10.10.0/28, 12.12.12.0/28, 11.11.11.0/28, topology: Tree) to make sure that if one line has trouble the network is still working.
- The third router of core layer (IP: 13.13.13.0/28) and sub router in Rest Room (IP: 192.168.3.0/28) connect to Main router at Server Room. This Main Router is important with the network system, which connect 3 floor.

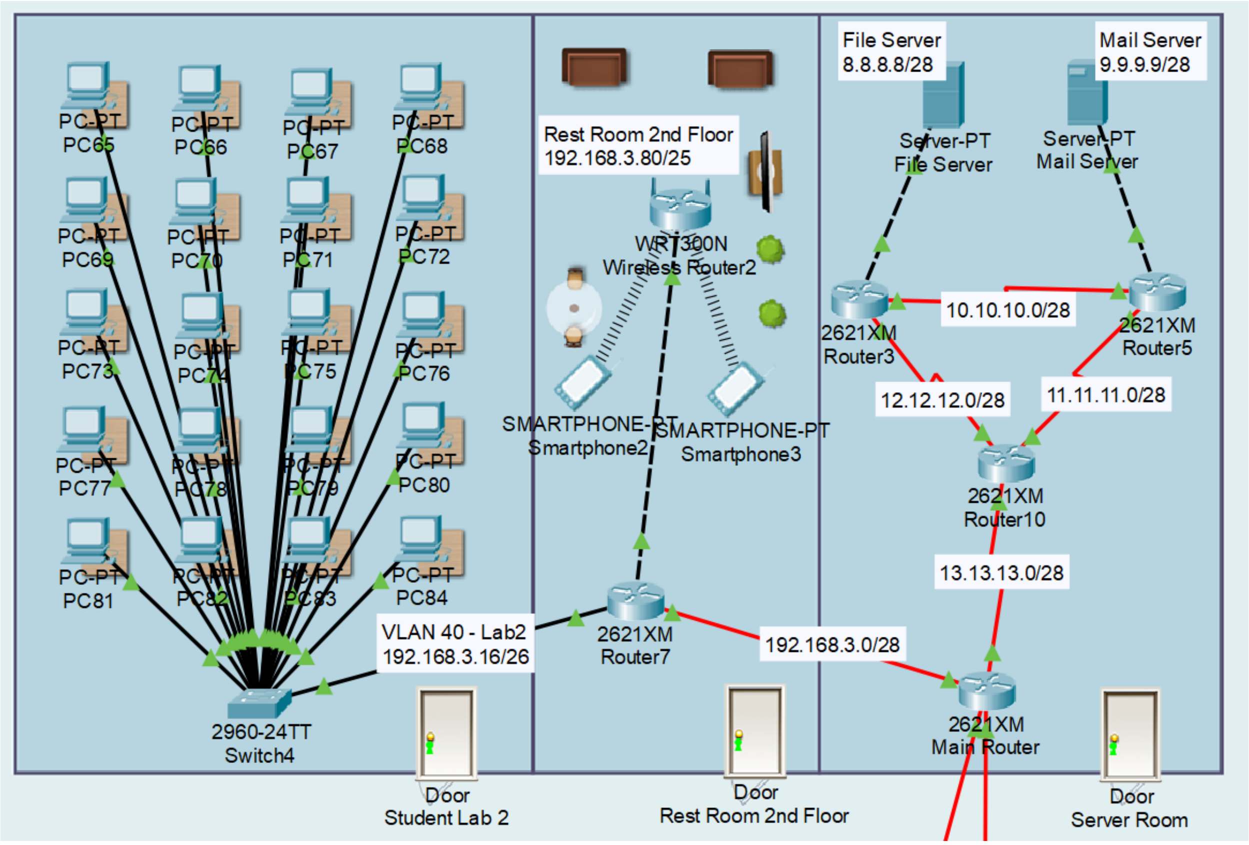


**Figure 3.1 : Design of 2nd Floor**

- **First floor: ( 30 Computer, 1 Wireless, 1 Router)**

- This Main Router connect Sub Router First Floor at Library (IP: 192.168.2.0/28).
- In first floor we connect 30 Student computers with 2 switch (26 Ports/Switch) that 15 computer will connect in one switch (VLAN 30 – Lab1, IP: 192.168.2.16/26).
- Two switch connected together and connect to sub router at Library.
- The Wireless Router at Library connect to sub router (IP: 192.168.2.80/25).

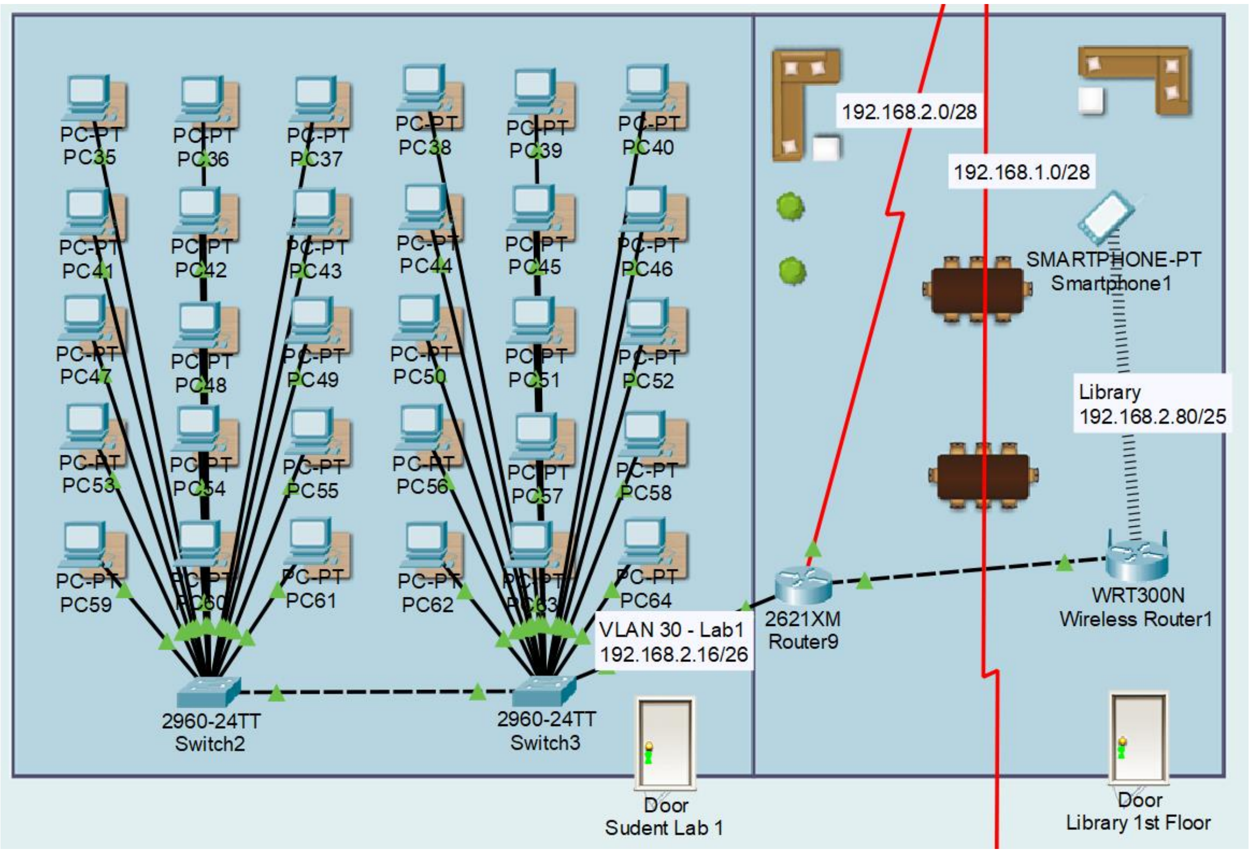


**Figure 3.2 : Design of 1st Floor**

- **Ground floor: (35 Computer, 3 Printer, 2 Switch, 1 Router, 1 Wireless):**

- This floor has three rooms: Staff Room 1, Staff Room 2 and Rest Room Ground Floor.
- The Main Router at second floor connect Sub Router at Rest Room Ground Floor (IP: 192.168.1.0/24). And the Wireless has IP: 192.168.1.44/25.
- The Staff room 1 has 20 computer divide into 3 VLAN (VLAN10 – Marketing IP: 192.168.1.16/27, VLAN 100- Manager IP 192.168.1.48/27:, VLAN 200- Administrator and IP: 192.168.1.80/27) and this Staff Room 1 also has two printer connect to switch (26 Ports).
- The Staff room 2 has 15 computer used for teacher (VLAN 20 – Teacher, IP: 192.168.1.112/27) connect to switch and this Staff Room 2 has one printer connect to switch (26 Ports).
- Two switch at 2 Staff Room connect together and connect to sub Router at Rest Room Ground Floor.

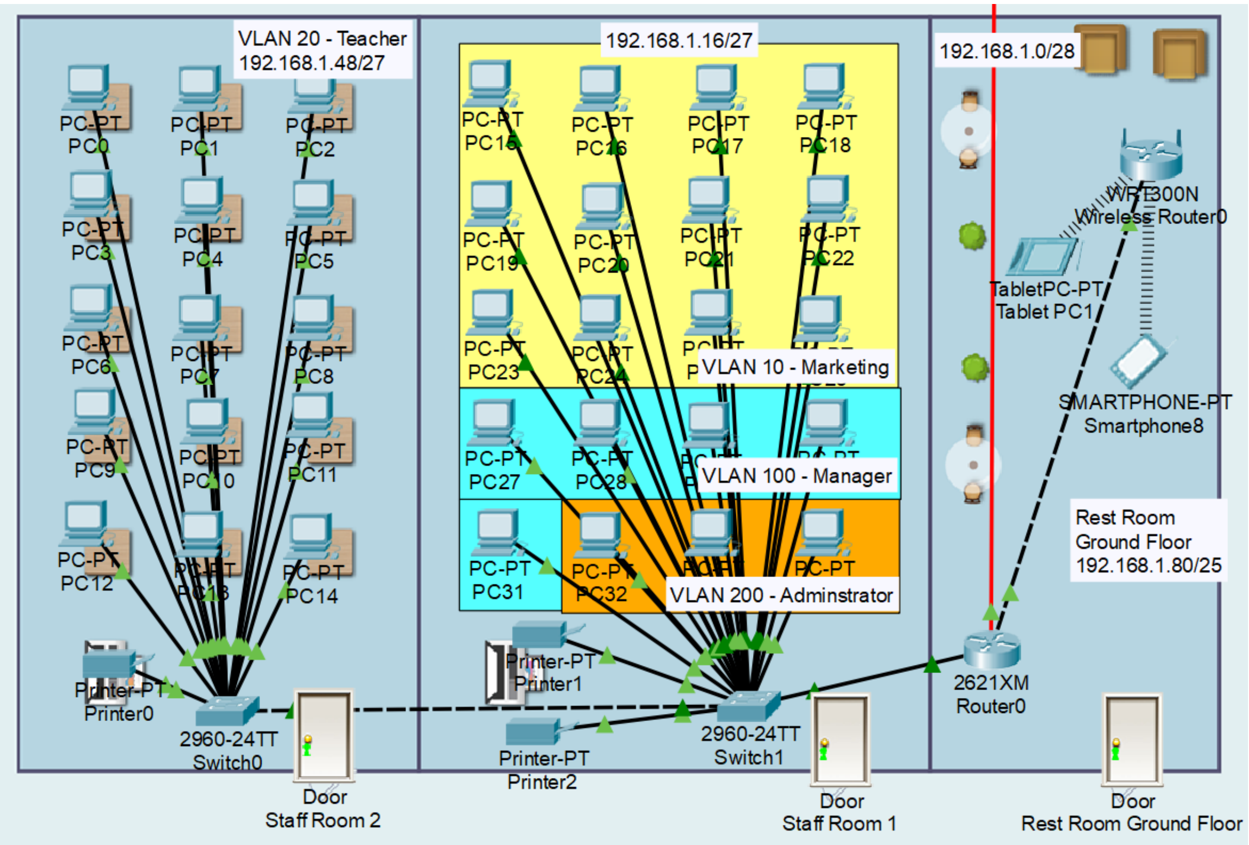


**Figure 3.3 : Design of Ground Floor**

## 2. Test and evaluate the design to meet the requirements and analyses user feedback

- When the network system have a big data transfer in system which cause bottleneck. This makes the system in danger. The solution is changed the connection between switch and router from Fast Ethernet to Giga Ethernet. This solution means change bandwidth from 100Mbs to 1Gbs.

- There are some ways to test the network performance, reliability and security. From host stations use ping to student or staff computer and see the reply times, if it shows a steady time then network utilization and bandwidth are in good shape. When using network traffic just disconnect one uplink cable from access switch to check the reliability of network. Check the see the access list hits that traffic it filtering according to the rule. If subnet wise policy applied then shift a user PC from one subnet to another and check the access policy shifted or not.

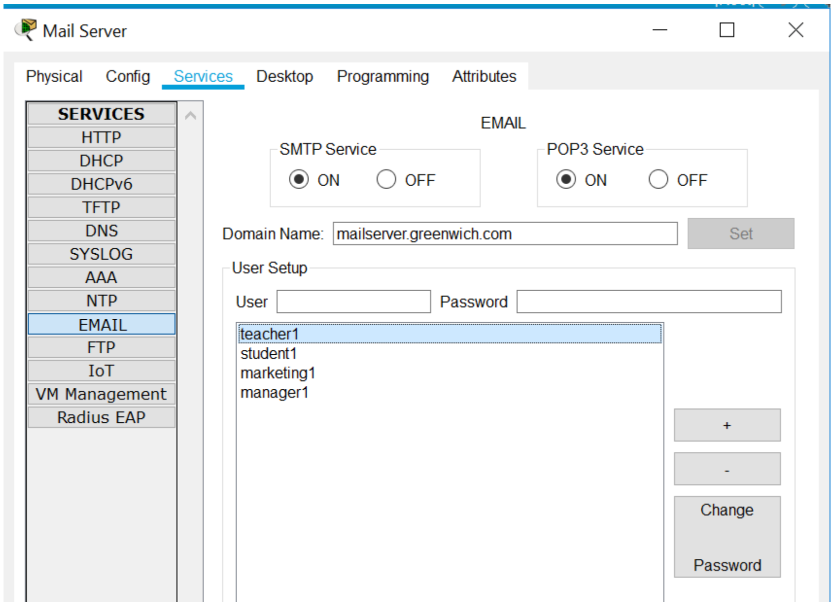
- From Student or Staff PC send exteneded ping to the servers and see checks the alarm from firewall. Using traffic generator software from host PC to check IDS is working or not. Use a authorize device to plug into a switch port and check it getting connection or not.

- When we need for network maintenance services and check maintain the system. We can easy contact the supplier though hotline with staff has experience in the field of network, telecommunications, engineers specializing in network in FPT, Viettel will ensure to fix in the fastest time with cheapest cost.

## 3. Install and configure network services and applications on your choice

### 3.1. Network services:

- Email: Simple Mail Transfer Protocol (SMTP - Port 25 – TCP) is used for email transmission. Mail server and other mail transfer agents use SMTP to send and receive mail message. Post Office Protocol (POS - Port 109,110 – TCP) is used to sent mail message.



Mail Server

EMAIL

SMTP Service ● ON ○ OFF

POP3 Service ● ON ○ OFF

Domain Name: mailserver.greenwich.com

User Setup

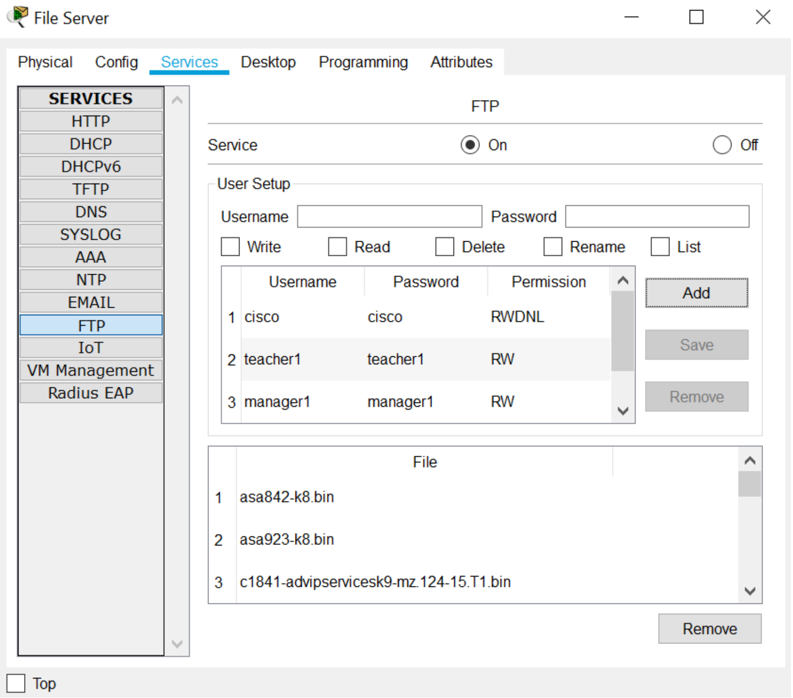
User

Password

teacher1
student1
marketing1
manager1

**Picture 3.1: Mail Services**

- File transfer: File Transfer Protocol (FTP – Port 20,21 - TCP) is a standard network protocol used for the transfer of computer files between a client and server on network system.



FTP

Service ● On ○ Off

User Setup

Username Password

□ Write □ Read □ Delete □ Rename □ List

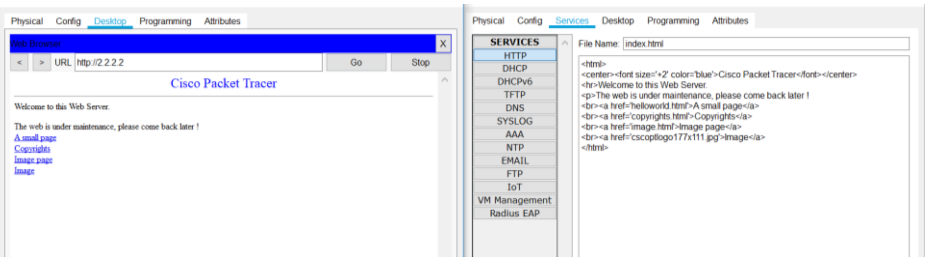
| | Username | Password | Permission |
|---|---|---|---|
| 1 | cisco | cisco | RWDNL |
| 2 | teacher1 | teacher1 | RW |
| 3 | manager1 | manager1 | RW |

| | File |
|---|---|
| 1 | asa842-k8.bin |
| 2 | asa923-k8.bin |
| 3 | c1841-advipservicesk9-mz.124-15.T1.bin |

□ Top

**Picture 3.2: File Transfer Services**

- Web: We use HTTP (Port 80 -TCP) to go to simple web for reading or searching information and HTTPS (Port 443 – TCP) to go to secure web such as login mail and the application important.



URL http://2.2.2.2

Cisco Packet Tracer

Welcome to this Web Server.

The web is under maintenance, please come back later !
A small page
Copyrights
Image page
Image

File Name: index.html

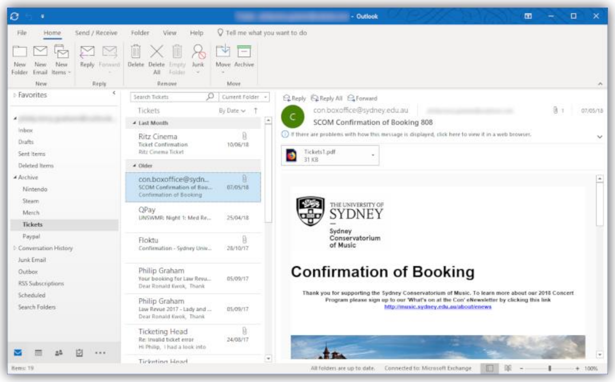
```
<html>
<center><font size='+2' color='blue'>Cisco Packet Tracer</font></center>
<hr>Welcome to this Web Server.
<p>The web is under maintenance, please come back later !
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscoptlogo177x111.jpg'>Image</a>
</html>
```

**Picture 3.3: Web Services**

- Telnet Terminal (Port 23 – TCP): This service allows people to access the network devices.
- Simple Network Management (SNMP Port 161,162 TPC UDP): This service allows administrators to check, manage or troubleshoot problem form far away.

### 3.2. Application:

- Microsoft Outlook: is a personal information manager from Microsoft often used mainly as an email application. This app connect to your Email on Internet or some Site and download into computer, after that people can read, delete, or sent email with this application.



Ritz Cinema
Ticket Confirmation 10/06/18
Ritz Cinema Ticket

con.boxoffice@sydn...
SCOM Confirmation of Boo... 07/05/18
Confirmation of Booking

QPay
UNSWMR: Night 1: Med Re... 25/04/18

Floktu
Confirmation - Sydney Univ... 28/10/17

Philip Graham
Your booking for Law Revu... 05/09/17
Dear Ronald Kwok, Thank

Philip Graham
Law Revue 2017 - Lady and ... 05/09/17
Dear Ronald Kwok, Thank

Ticketing Head
Re: Invalid ticket error 24/08/17
Hi Philip, I had a look into

Ticketing Head

con.boxoffice@sydney.edu.au [redacted] 07/05/18
SCOM Confirmation of Booking 808

If there are problems with how this message is displayed, click here to view it in a web browser.

Tickets1.pdf
31 KB

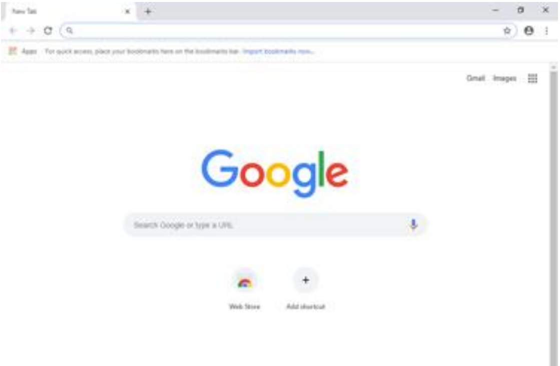
THE UNIVERSITY OF SYDNEY
Sydney Conservatorium of Music

Confirmation of Booking

Thank you for supporting the Sydney Conservatorium of Music. To learn more about our 2018 Concert Program please sign up to our 'What's on at the Con' eNewsletter by clicking this link
http://music.sydney.edu.au/about/enews

**Picture 3.4: Microsoft Outlook Application**

- Google Chrome: is a freeware web browser developed by Google LLC. This application help people surf the web faster than another application and has many useful extension.


New Tab
Apps
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
Gmail
Images
Google
Search Google or type a URL
Web Store
Add shortcut

**Picture 3.5: Google Chrome Application**

### 3.3. Design a maintenance schedule to support the networked system

- Routine maintenance: This is a package maintenance service based on the annual contract with the supplier. Every month we send technicians to test the entire system and to troubleshoot problems that fall under maintenance on a given day.

- Server:
  - Control access to network or server
  - Test and configure network security services (Microsoft ISA, Firewall, Checkpoints)
  - Test, install and update the latest versions of antivirus software, trojan software, adware Spyware for computer systems.
  - Optimized for garbage files and optimization of application software, office software, and security software on computer systems.
  - Ensure the operation of the system Email, File, Document, Printing regularly, stable, safe for work.
  - Backup server configuration ensures that the server always operates properly.
- Student and Staff PC:
  - Check client and staff PC which make sure that each PC can connect to server.
  - All client and staff PC can receive mail and connect each another.
  - Update the latest versions of antivirus software, trojan software, adware Spyware for computer systems.
  - All computer operates properly**.**

- Network:
    - Configure the network to access.
    - Review the entire network cabling system, ensure the cable system is designed and placed in the environment standards.
    - Test all cables and connectors to ensure satisfactory signal. transmission.
    - Satisfactory signal transmission with bandwidth: 100mbs.

- In addition to periodic system checks, when the network has a problem or any question about the system, we will send technical support to within 2 hours. During the inspection we will have replacement products to ensure the operation of the company during that time.

# 4. Implement and diagnose networked systems

## 4.1. Implement a networked system based on a prepared design:

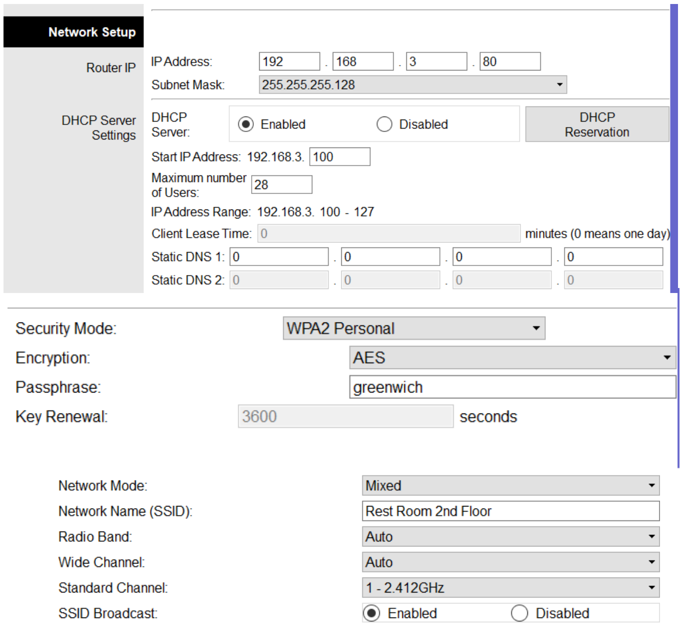
- Wireless Router:

○ Internet Setup: We use DHCP.

○ Network Setup: It is the IP of the Access Point and the AP transmits it to the wireless devices. And the IP Address and Subnet Mask we follow the structure of the network that we design.

○ SSID: This name follow each room and floor such as: Rest Room Floor 1, Library Floor 2, Rest Room Floor 3.

○ Security Mode: WPA2 Personal: "greenwich".



Network Setup

Router IP
IP Address: 192 . 168 . 3 . 80
Subnet Mask: 255.255.255.128

DHCP Server Settings
DHCP Server: ● Enabled ○ Disabled

Start IP Address: 192.168.3. 100
Maximum number of Users: 28
IP Address Range: 192.168.3. 100 - 127
Client Lease Time: 0 minutes (0 means one day)
Static DNS 1: 0 . 0 . 0 . 0
Static DNS 2: 0 . 0 . 0 . 0

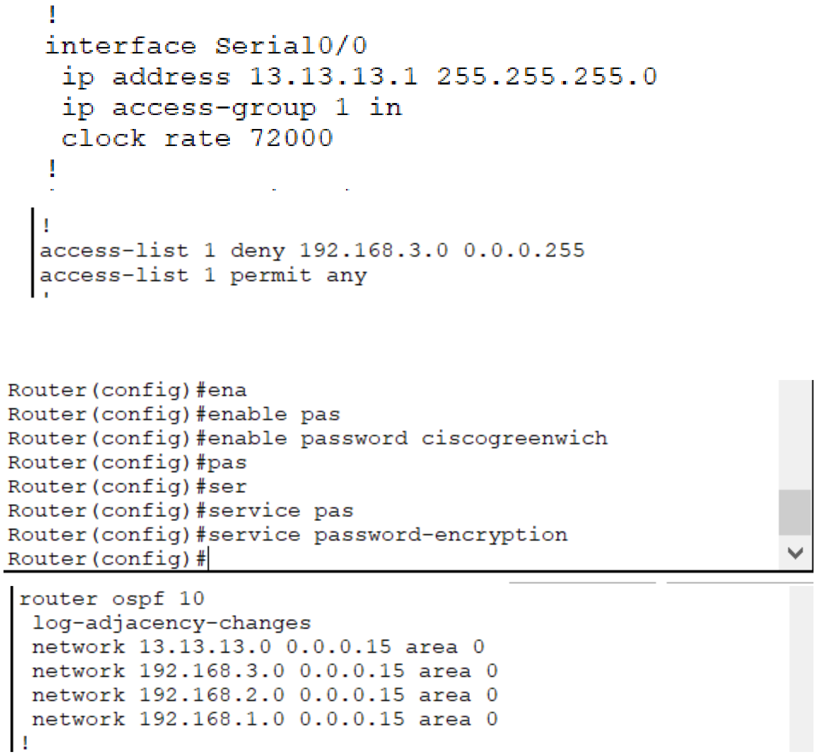
Security Mode: WPA2 Personal
Encryption: AES
Passphrase: greenwich
Key Renewal: 3600 seconds

Network Mode: Mixed
Network Name (SSID): Rest Room 2nd Floor
Radio Band: Auto
Wide Channel: Auto
Standard Channel: 1 - 2.412GHz
SSID Broadcast: ● Enabled ○ Disabled

**Picture 3.6: Wireless Router Configure**

- Router:

  - Router on Stick: Each Floor have one Sub Router so we need configure Router to connect the computer with different vlan through switch.
  - IP Address for each line and when port DCE we set clock rate.
  - Router OSPFv2 Area 0: This configure make all computer can connect each together and server.
  - Access control list (ACL): This make Student Computer cant connect Server.
  - Password: We set password: “cisco” for Sub Router at each floor and Password: “ciscogreenwich” for Main Router ( Router at Server Room). All password are encryption.



```
!
interface Serial0/0
 ip address 13.13.13.1 255.255.255.0
 ip access-group 1 in
 clock rate 72000
!
```

```
!
access-list 1 deny 192.168.3.0 0.0.0.255
access-list 1 permit any
```

```
Router(config)#ena
Router(config)#enable pas
Router(config)#enable password ciscogreenwich
Router(config)#pas
Router(config)#ser
Router(config)#service pas
Router(config)#service password-encryption
Router(config)#
```

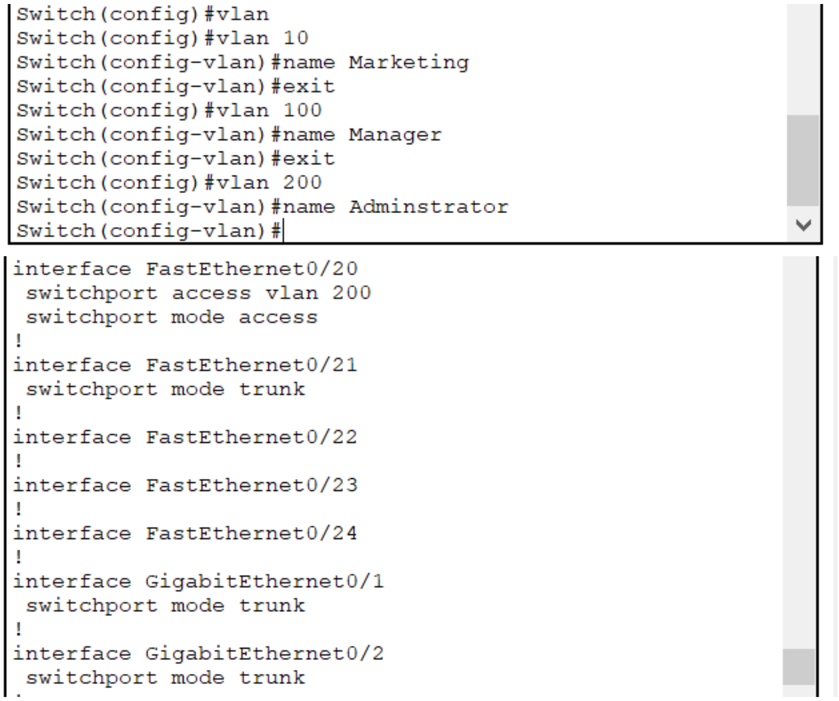
```
router ospf 10
 log-adjacency-changes
 network 13.13.13.0 0.0.0.15 area 0
 network 192.168.3.0 0.0.0.15 area 0
 network 192.168.2.0 0.0.0.15 area 0
 network 192.168.1.0 0.0.0.15 area 0
!
```

**Picture 3.7: Router Configure**

- Switch:

  - Vlan: We set Vlan to specific room such as Vlan 20 for Teacher Computer, Vlan 10 for Marketing, Vlan 100 for Manager, Vlan 200 for Administrator, Vlan 30 for Lab Room 1, Vlan 40 for Lab Room 2.

  - Vlan trunking protocol (VTP): we set VTP at the ground floor.

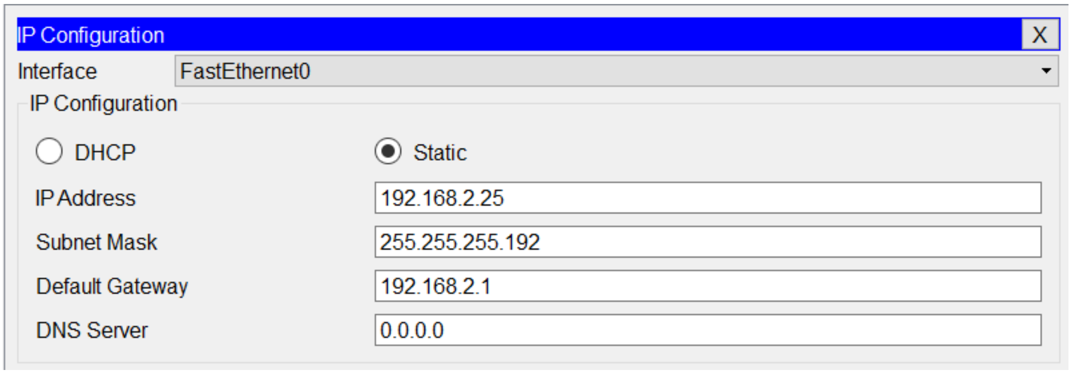


```
Switch(config)#vlan
Switch(config)#vlan 10
Switch(config-vlan)#name Marketing
Switch(config-vlan)#exit
Switch(config)#vlan 100
Switch(config-vlan)#name Manager
Switch(config-vlan)#exit
Switch(config)#vlan 200
Switch(config-vlan)#name Adminstrator
Switch(config-vlan)#
```

```
interface FastEthernet0/20
 switchport access vlan 200
 switchport mode access
!
interface FastEthernet0/21
 switchport mode trunk
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport mode trunk
```

**Picture 3.8: Switch Configure**

- Computer:
  - IP Address and Default Gateway are setup for each computer.



IP Configuration X

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IP Address: 192.168.2.25

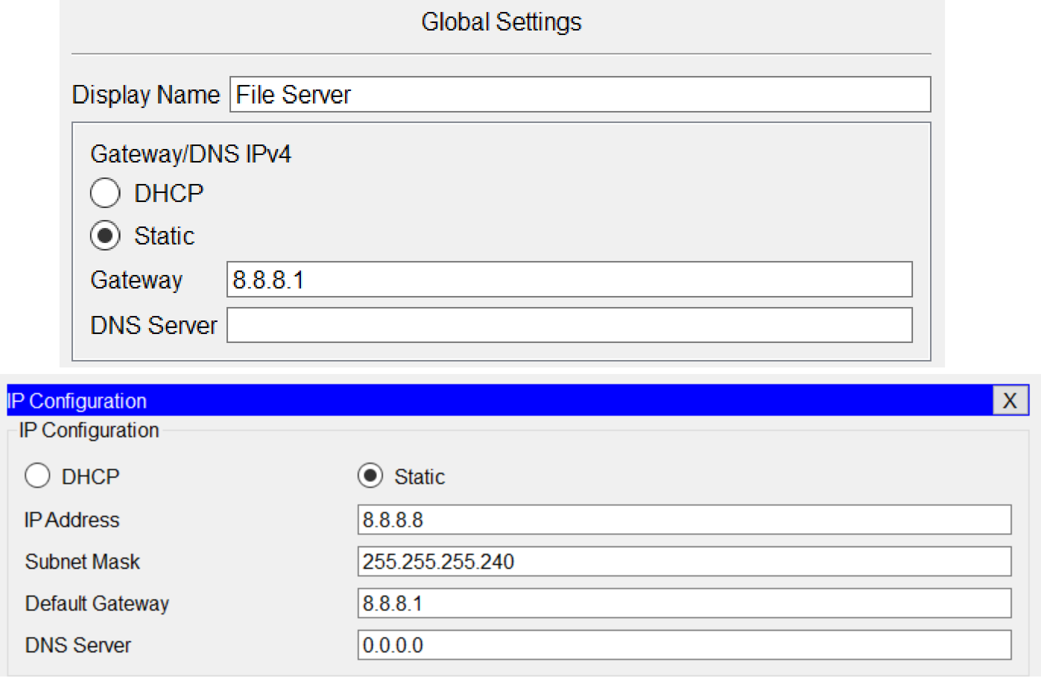
Subnet Mask: 255.255.255.192

Default Gateway: 192.168.2.1

DNS Server: 0.0.0.0

**Picture 3.9: Computer IP Configure**

- Server:
  - IP Address and Default Gateway are setup for File Server and Mail Server.



Global Settings

Display Name: File Server

Gateway/DNS IPv4

○ DHCP

● Static

Gateway: 8.8.8.1

DNS Server:

IP Configuration X

IP Configuration

○ DHCP ● Static

IP Address: 8.8.8.8

Subnet Mask: 255.255.255.240

Default Gateway: 8.8.8.1

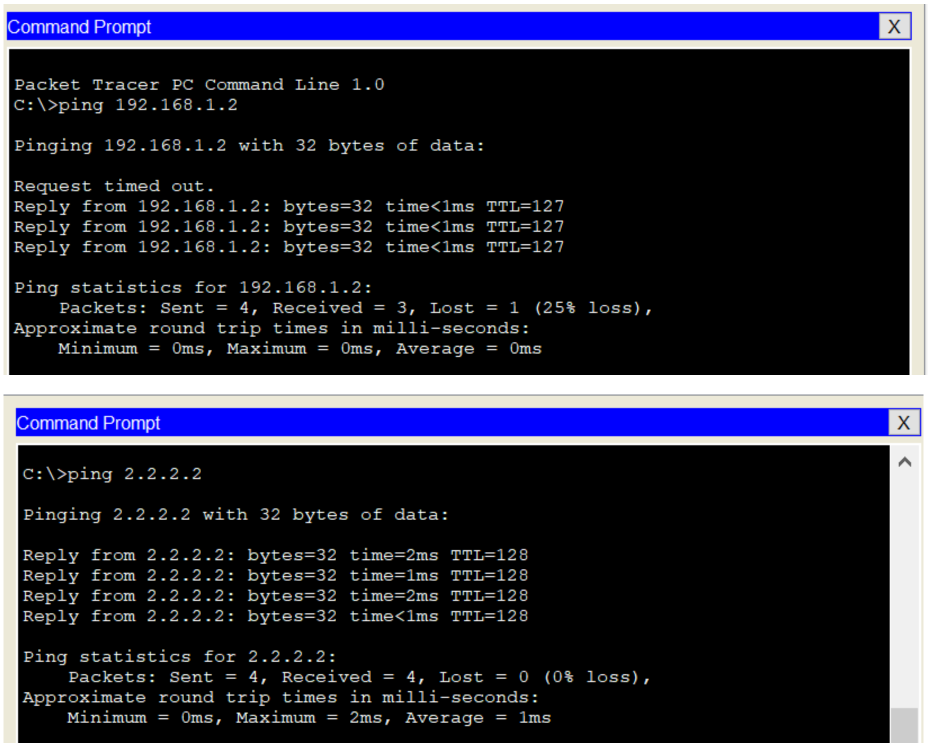
DNS Server: 0.0.0.0

**Picture 3.10: Server IP Configure**

## 4.2. Document and analyses test results against expected results.

- All computer can connect computer. This network system is conducting verification with Ping to test this case:

  - Ping from Computer 1 (Staff Room 2 – VLAN 20 – Teacher) to Computer 1 (Staff Room 1 – VLAN 10 – Marketing) ; Computer 2 ( Lab Room 1 – VLAN 30 – Lab1); Computer 3 ( Lab Room 2 – VLAN 40 – Lab2); File Server and Mail Server ( 2nd Floor):



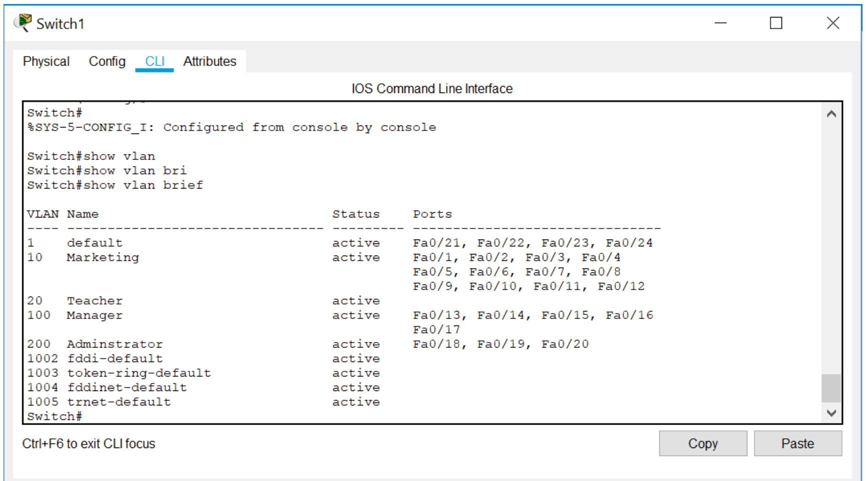
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ping 2.2.2.2

Pinging 2.2.2.2 with 32 bytes of data:

Reply from 2.2.2.2: bytes=32 time=2ms TTL=128
Reply from 2.2.2.2: bytes=32 time=1ms TTL=128
Reply from 2.2.2.2: bytes=32 time=2ms TTL=128
Reply from 2.2.2.2: bytes=32 time<1ms TTL=128

Ping statistics for 2.2.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

**Picture 3.11: Computer test Ping**

  - The results show that the whole computer can connect to each other and connect to the server.

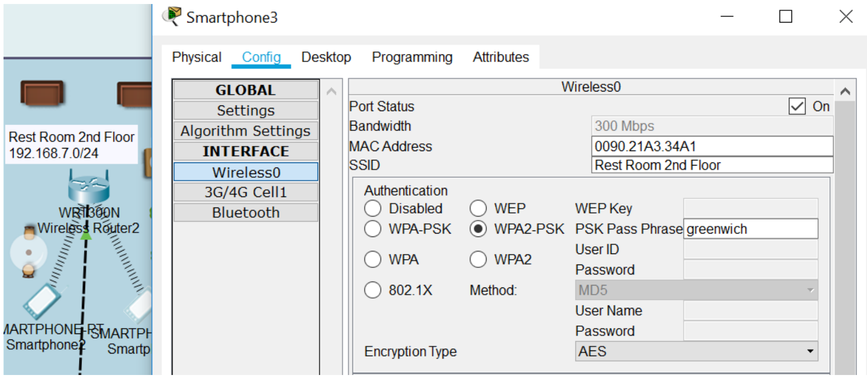
- Each roles of computer has a specific vlan that makes manager or administrator can easy control the network system:
  - At Switch in Ground Floor show us what vlan for computer.



```
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan
Switch#show vlan bri
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   Marketing                        active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
20   Teacher                          active
100  Manager                          active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17
200  Adminstrator                     active    Fa0/18, Fa0/19, Fa0/20
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

**Picture 3.12: Switch vlan**

- The WiFi at Rest Room and Library is worked:
  - We check the wireless on Smartphone with SSID and WPA-PSK same with Wireless, the result show the mobile phone is connecting Wireless Router



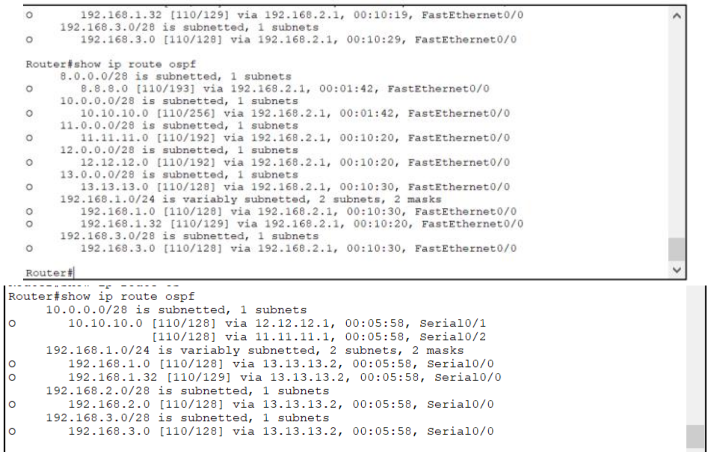
Wireless0

Port Status ☑ On
Bandwidth 300 Mbps
MAC Address 0090.21A3.34A1
SSID Rest Room 2nd Floor

Authentication
○ Disabled ○ WEP WEP Key
○ WPA-PSK ● WPA2-PSK PSK Pass Phrase greenwich
○ WPA ○ WPA2 User ID
Password
○ 802.1X Method: MD5
User Name
Password
Encryption Type AES

**Picture 3.13: Mobile phone connect to Wifi**

- Network system has router were configured OSPFv2 so router can sent/receive data fluent:
  - Checking the Sub Router at 2nd Floor and Core Router that show the router “was learn” all IP in network system through OSPFv2.

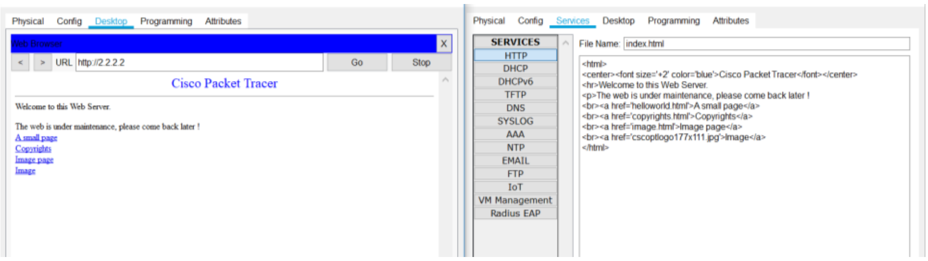


```
O        192.168.1.32 [110/129] via 192.168.2.1, 00:10:19, FastEthernet0/0
     192.168.3.0/28 is subnetted, 1 subnets
O        192.168.3.0 [110/128] via 192.168.2.1, 00:10:29, FastEthernet0/0

Router#show ip route ospf
     8.0.0.0/28 is subnetted, 1 subnets
O        8.8.8.0 [110/193] via 192.168.2.1, 00:01:42, FastEthernet0/0
     10.0.0.0/28 is subnetted, 1 subnets
O        10.10.10.0 [110/256] via 192.168.2.1, 00:01:42, FastEthernet0/0
     11.0.0.0/28 is subnetted, 1 subnets
O        11.11.11.0 [110/192] via 192.168.2.1, 00:10:20, FastEthernet0/0
     12.0.0.0/28 is subnetted, 1 subnets
O        12.12.12.0 [110/192] via 192.168.2.1, 00:10:20, FastEthernet0/0
     13.0.0.0/28 is subnetted, 1 subnets
O        13.13.13.0 [110/128] via 192.168.2.1, 00:10:30, FastEthernet0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
O        192.168.1.0 [110/128] via 192.168.2.1, 00:10:30, FastEthernet0/0
O        192.168.1.32 [110/129] via 192.168.2.1, 00:10:20, FastEthernet0/0
     192.168.3.0/28 is subnetted, 1 subnets
O        192.168.3.0 [110/128] via 192.168.2.1, 00:10:30, FastEthernet0/0

Router#
```

```
Router#show ip route ospf
     10.0.0.0/28 is subnetted, 1 subnets
O        10.10.10.0 [110/128] via 12.12.12.1, 00:05:58, Serial0/1
                    [110/128] via 11.11.11.1, 00:05:58, Serial0/2
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
O        192.168.1.0 [110/128] via 13.13.13.2, 00:05:58, Serial0/0
O        192.168.1.32 [110/129] via 13.13.13.2, 00:05:58, Serial0/0
     192.168.2.0/28 is subnetted, 1 subnets
O        192.168.2.0 [110/128] via 13.13.13.2, 00:05:58, Serial0/0
     192.168.3.0/28 is subnetted, 1 subnets
O        192.168.3.0 [110/128] via 13.13.13.2, 00:05:58, Serial0/0
```

**Picture 3.14: Router OSPFv2**

- Computer can connect to Server with Web Browser:



URL http://2.2.2.2

Cisco Packet Tracer

Welcome to this Web Server.

The web is under maintenance, please come back later !
A small page
Copyrights
Image page
Image

File Name: index.html

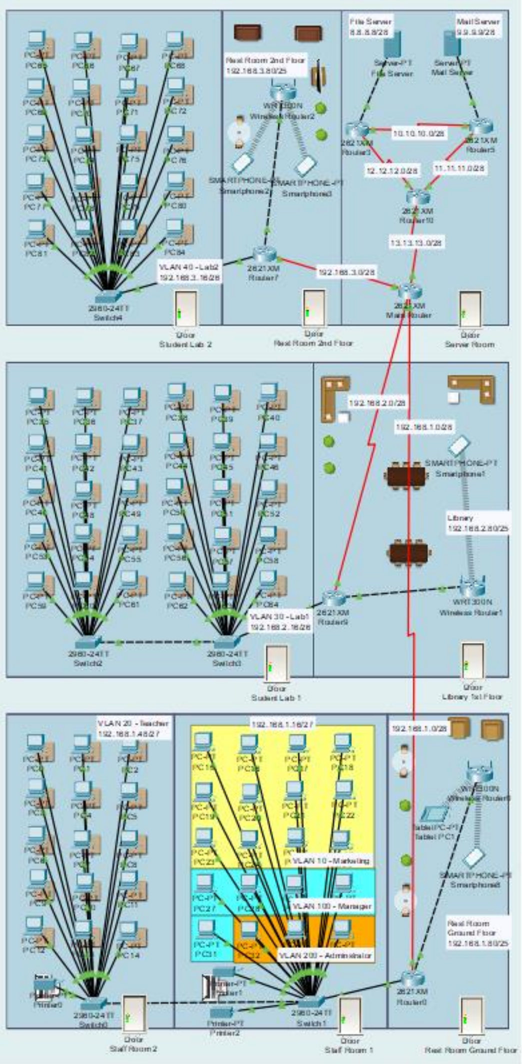
```
<html>
<center><font size='+2' color='blue'>Cisco Packet Tracer</font></center>
<hr>Welcome to this Web Server.
<p>The web is under maintenance, please come back later !
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscoptlogo177x111.jpg'>Image</a>
</html>
```

**Picture 3.15: Computer connect to Server with Web Browser**

### 4.3. Recommend potential enhancements for the networked systems.

- In this system, we have many router and switch(26 port) and the IP for each line are easy for system to have more computer, any devices or upgrade system.
- Them internet This system need connect to Internet and purchasing services form Internet Service Providers (Viettel) with Name of Data: Fast 100 - Bandwidth in national and international: 100Mbs / 2Mbs – Price: $190.
- When we have Internet, so we need to upgrade our security by add a firewall (ASA550 – Price: $250) and purchase anti-virus software with license is update every year.
- When the network is operating that we realize Staff and Student have many devices such as mobile phone, tablet, laptop, etc. So we need to have more Wireless router at Staff Room and Student Room.
- In order to upgrade the network, we should establish the Leased Line to increase speed and security.
- At Ground Floor this building just has 3 room and except all Teacher Computers in Staff Room 2 but Marketing Computer, Manager Computer and Administrator Computer are in Staff Room 1. This problem makes staff will not satisfied when they are working. So we need to divide Staff Room 1 to 3 small room.
- At Ground Floor, there are two switch which connected and just switch in Staff Room 1 connect with Sub Router at Rest Room Ground Floor, if this switch have trouble that will make all teacher computer in Staff Room 1 cant connect to network system.

## 4.4. Use critical reflection to evaluate own work and justify valid conclusions.



**Picture 3.16: Network System in Building**

- When I was an employee as a network engineer by a high-tech networking solution development organization and working on a project for local educational institution. I had designed the network system for 200 students, 15 teacher, 12 marketing and administration staff, 5 higher managers including the head of academics and the programmer manager, 3 computer network administrators in a building 3 floor.

    - This project requires meticulousness in each stage and this project requires meticulousness in each stage and in order for the system to work properly, I have provided general design details for each device. Besides, the configuration for each device is relatively complicated, it takes a lot of time to monitor whether the system works well or not?
    - After completion of the project, the system has worked well, meeting the technical and quality requirements.
    - Handover of documents as well as equipment configuration information and solution suggestions and opinions are also given direction for the future.

- Equipment for the system must meet the following Lan construction standards:
  - Network cables used for the project must ensure durability, quality, meet requirements such as: anti-interference, bearing force when stretching, good signal transmission ...
  - The equipment used must have such genuine origin to be able to measure the most accurate results.
  - Design and construction must meet international standards: ANSI / TIA / EIA 568B, ANSI / TIA / EIA-607, ANSI / TIA / EIA-569A and ISO / IEC 11801
  - Network construction standards must meet professional procedures.
  - Receive survey requests from customers
  - Give staff to the live survey site to have the best construction plan
  - Get ideas and detailed plans for each construction phase.
  - Send a specific quote on the diagram of the design drawing, the quantity of supplies needed, the time for completion for the customer.
  - Carry out the installation according to the agreed plan between the two parties and report the progress of the project for customers to follow.
  - Check the system and proceed to take over the work handed over to the management
  - Maintenance operating system by warranty card

# References

| | Title | Source |
|---|---|---|
| 1 | 11 Types of Networks Explained: VPN, LAN & More | https://www.belden.com/blog/smart-building/11-types-of-networks-explained-vpn-lan-more |
| 2 | Networking Standards | https://www.webopedia.com/Networks/Networking_Standards#<br>https://www.ukessays.com/essays/computer-science/benefits-and-constraints-of-different-networking-computer-science-essay.php<br>http://what-when-how.com/data-communications-and-networking/network-standards-data-communications-and-networking/ |
| 3 | Networking and communication | http://www.contrib.andrew.cmu.edu/~dabousen/Default%20-%20Copy%20(2).html |
| 4 | Network Devices | https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/ |
| 5 | Server Types | https://www.webopedia.com/quick_ref/servers.asp |
| 6 | Network Access Control | https://www.esecurityplanet.com/network-security/network-access-control.html |
| 7 | System bus | https://en.wikipedia.org/wiki/System_bus |
| 8 | System architecture | https://en.wikipedia.org/wiki/Systems_architecture |
| 9 | Network Memory | https://www.connection.com/category/network-device-memory/204416 |
| 10 | I/O Device | https://www.computerhope.com/jargon/i/iodevice.htm |
| 11 | Processing device | https://www.computerhope.com/jargon/p/procdevi.htm |
| 12 | Principles and Protocol | http://cnp3book.info.ucl.ac.be/2nd/cnp3bis.pdf<br>https://resources.saylor.org/wwwresources/archived/site/wp-content/uploads/2012/02/Computer-Networking-Principles-Bonaventure-1-30-31-OTC1.pdf |