# Building and securing a small network


**Presented by:**

**Hassan Gamal**
**Youssef El Sambry**
**Salma Samir**

# Introduction

In today's world, building and securing small networks is very important. As businesses and individuals rely more on technology for communication, data storage, and daily operations, having a strong network is essential. This project report explains how to design and set up a secure small network that meets the needs of a small organization.

The main goal of this project is to create a reliable network that allows easy connections while keeping it safe from potential threats. We will look at different parts of network design, such as choosing hardware, configuring software, and implementing security measures.

By the end of this report, readers will learn best practices for building networks and security steps to protect important information and ensure smooth operations. This project is a key step toward creating a secure digital environment for small businesses in our connected world.

# Project Steps

LYA University is a large university which has two campuses situated 20 Km apart. The university's students and staff are distributed in 4 faculties; these include the faculties of Health and Sciences; Business; Engineering/Computing and Art/Design.

Each member of staff has a PC and students have access to PCs in the labs.

Requirements:

**1] Create a network topology with the main components to support the following:**

- Main campus:

- Building A: Administrative staff in the departments of management, HR and finance. The admin staff PCs are distributed in the building offices and it is expected that they will share some networking equipment (Hint: use of VLANs is expected here). The Faculty of Business is also situated in this building

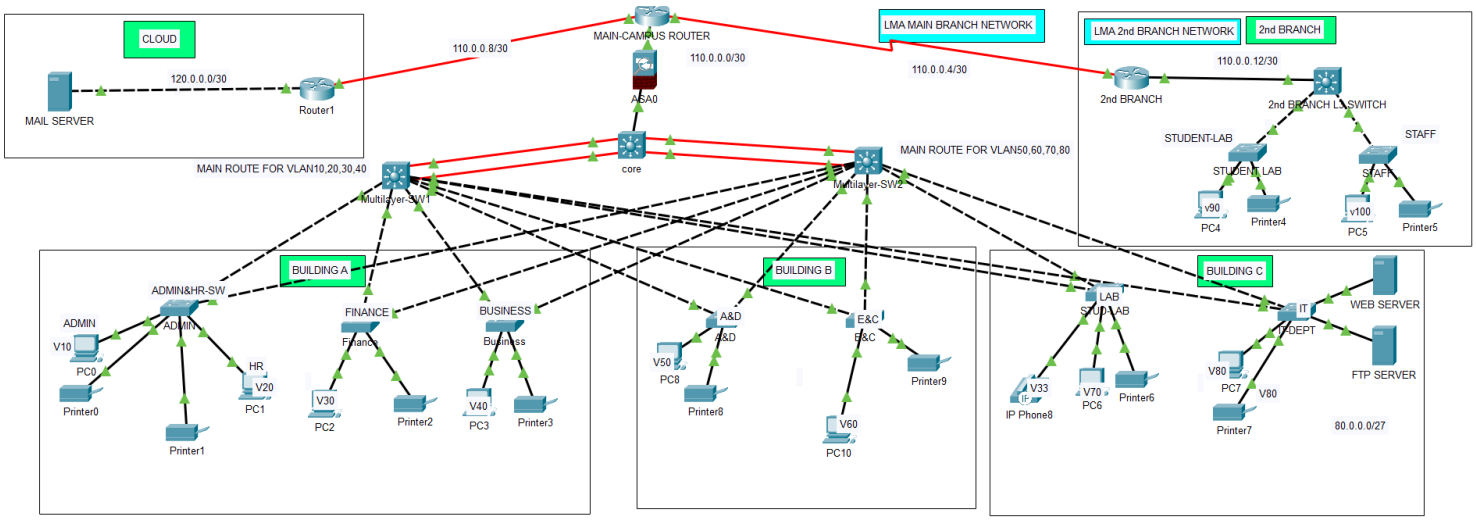
- Building B: Faculty of Engineering and Computing and Faculty of Art and Design
- Building C: Students' labs and IT department. The IT department hosts the University Web server and other servers
- There is also an email server hosted externally on the cloud.

-Smaller campus:

- Faculty of Health and Sciences (staff and students' labs are situated on separate floors)

**2] You will be expected to configure the core devices and few end devices to provide end-to-end connectivity and access to the internal servers and the external server.**

- Each department/faculty is expected to be on its own separate IP network
- The switches should be configured with appropriate VLANs and security settings
- eigrp will be used to provide routing for the routers in the internal network and static routing for the external server.
- The devices in building A will be expected to acquire dynamic IP addresses from a router-based DHCP server.



# Used components

●Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command-line interface. Packet Tracer makes use of a drag-and-drop user interface, allowing users to add and remove simulated network devices as they see fit.

● Router: is a device like a switch that routes data packets based on their IP addresses. The 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 divides broadcast domains of hosts connected through it.

● Switch (also called switching hub, bridging hub, officially MAC bridge is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer (layer 2) of the OSI model. Some switches can also forward data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

● Network Packet is a formatted unit of data carried by a packet-switched network. A packet consists of control information and user data.

● Wireless Network broadcasts an access signal to the workstations or PCs. This enables mobility among laptops, tablets, and PCs from room to room while maintaining a firm network connection continuously. A wireless network also presents additional security requirements.

● Server is a computer or system that provides resources, data, services, or programs to other computers, known as clients, over a network. In theory, whenever computers share resources with client machines they are considered servers. There are many types of servers, including web servers, mail servers, and virtual servers. Many networks contain one or more of the common servers. The servers used in our project are as follows:

➢ DNS Server stands for Domain Name System servers which are application servers that provide a human-friendly naming method to the user computers in order to make IP addresses readable by users. The DNS system is a widely distributed database of names and other DNS servers, each of which can be used to request an otherwise unknown computer name. When a user needs the address of a system, it sends a DNS request with

the name of the desired resource to a DNS server. The DNS server responds with the necessary IP address from its table of names.

➢ WEB Server One of the widely used servers in today's market is a web server. A web server is a special kind of application server that hosts programs and data requested by users across the Internet or an intranet. Web servers respond to requests from browsers running on client computers for web pages, or other web-based services.

➢ EMAIL Server is a server that handles and delivers e-mail over a network, using standard email protocols. For example, the SMTP protocol sends messages and handles outgoing mail requests. The POP3 protocol receives messages and is used to process incoming mail. When you log on to a mail server using a webmail interface or email client, these protocols handle all the connections behind the scenes.

● Ethernet is the backbone of our network. It consists of the cabling and is typically able to Transfer data at a rate of 100mb/s. It is a system for connecting a number of computer systems to form a local area network, with protocols to control the passing of information and to avoid simultaneous transmission by two or more systems. Among the different types of ethernet, we have used Gigabit Ethernet, which is a type of Ethernet network capable of transferring data at a rate of 1000 Mbps and fast Ethernet is a type of Ethernet network that can transfer data at a rate of 100 Mbps.

● Computing Devices are the electronic devices that take user inputs, process the inputs, and then provide us with the end results. These devices may be Smartphones, PC Desktops, Laptops, printer, and many more.

# Used protocols

- Select Root and Secondary: In a network using Spanning Tree Protocol (STP), the **root bridge** is the central switch that all other switches in the network reference for path selection. The **secondary root bridge** serves as a backup in case the primary root bridge fails, ensuring network stability and redundancy.

- Port Fast is a feature in Cisco switches that allows a port to transition directly to the forwarding state, bypassing the listening and learning states of STP. This is useful for ports connected to end devices (like computers) to reduce the time it takes for them to start communicating on the network.

- Rapid Spanning Tree Protocol (RSTP), also known as IEEE 802.1w, is an evolution of STP that provides faster convergence times when network topology changes occur. It improves upon traditional STP by allowing switches to quickly transition ports to forwarding or blocking states.

- Port Security is a feature on network switches that restricts input to an interface based on MAC addresses. It helps prevent unauthorized devices from connecting to the network by limiting the number of MAC addresses that can be learned on a port and taking action (like shutting down the port) if violations occur.

- VTP is a Cisco protocol used to manage VLANs across multiple switches in a network. It allows for centralized management of VLAN configurations, enabling changes made on one switch to be propagated automatically to other switches in the same VTP domain.

- DTP (Dynamic Trunking Protocol) is a Cisco protocol that automatically negotiates trunk links between switches. It allows switches to dynamically determine whether a link should operate as an access port or a trunk port based on the connected device's capabilities.

- BPDU Guard is a feature that protects against loops in a network by disabling ports that receive Bridge Protocol Data Units (BPDUs) when they are not expected (e.g., on access ports). This helps prevent misconfigurations from causing network issues.

- VLAN (Virtual Local Area Network) is a logical grouping of devices within a physical network, allowing them to communicate as if they are on the same local network, regardless of their physical location. VLANs improve security and reduce broadcast traffic by segmenting networks.

- **C**hannel group refers to a configuration that combines multiple physical links into a single logical link (also known as EtherChannel) between switches or devices. This increases bandwidth and provides redundancy, as traffic can be load-balanced across the links.

- DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to automatically assign IP addresses and other network configuration parameters (like subnet mask and default gateway) to devices on a network, simplifying IP address management.

- Routing Protocol OSPF (Open Shortest Path First)**:** A link-state routing protocol used for routing IP packets within an autonomous system. It uses Dijkstra's algorithm to find the shortest path and supports hierarchical routing through areas.

- Routing Protocol EIGRP (Enhanced Interior Gateway Routing Protocol)**:** A Cisco proprietary distance-vector routing protocol that uses metrics like bandwidth, delay, load, and reliability to determine the best path for data packets. It combines features of both distance-vector and link-state protocols for efficient routing.

- Internet Protocol (IP) is one of the fundamental protocols that allow the internet to work. IP addresses are a unique set of numbers on each network and they allow machines to address each other across a network. It is implemented on the internet layer in the IP/TCP model.

# Conclusion

We started our discussion with the word “digitalization” and in order to achieve it, we aimed to start with an educational institute, and finally, we designed a network for a University, which is wireless.

As we mentioned, mobility and efficiency are the key aspects of wireless networks, which were our main goal, and hence, we decided to shift to a wireless network instead of a wired one, making our network clean and less chaotic.

In this project, we designed a University Network using Cisco Packet Tracer that uses a networking topology implemented using servers, routers, switches, and end devices in a multiple area networks. We have covered all the necessary features that are required for a network to function properly. We have included a DNS server and a web server for establishing a smooth communication system between different areas of our network and specifically for the communication between students and teachers. We have included an email server to facilitate intra university communication through emails within the domain. We have used console passwords and ssh protocol to ensure a safe and secure transfer of data.

Future Work The configuration and specifications are for the initial prototype and can further be developed and additional functionality can be added to increase support and coverage of our existing network.

***Thank you***