

**Graduation Project**

**Logo

Description automatically generatedProject Name : Design and implement network infrastructure of company**

**A Project Submitted in Partial Fulfillment**

**of the Requirements for the Degree of Bachelor of Science**

**in Systems and Computer Engineering**

**Submitted By**

|  |
| --- |
| * **Mohamed Ahmed Mohamed Nour Eldean 89** |
| * **Mohamed Ahemd Mostafa AbdElrahman 90** |
| * **Mohamed Atef Mohamed Saber 105** |
| * **Mostafa Sobhy Mahmoud Saleh 134** |
| * **Mohamed AbdElkareem Hamed 158** |

**Supervised by**

**Prof.Dr. Khalel mohamed**

**2023**

design and implement network infrastructure of company

Design and implement network infrastructure of the company

The project is an infrastructure for a company consisting of a main branch and two other branches. All devices can communicate with other devices through switches and routers in the network. It is also possible to control remotely in this network. There are also some servers such as WEB and FTP servers.

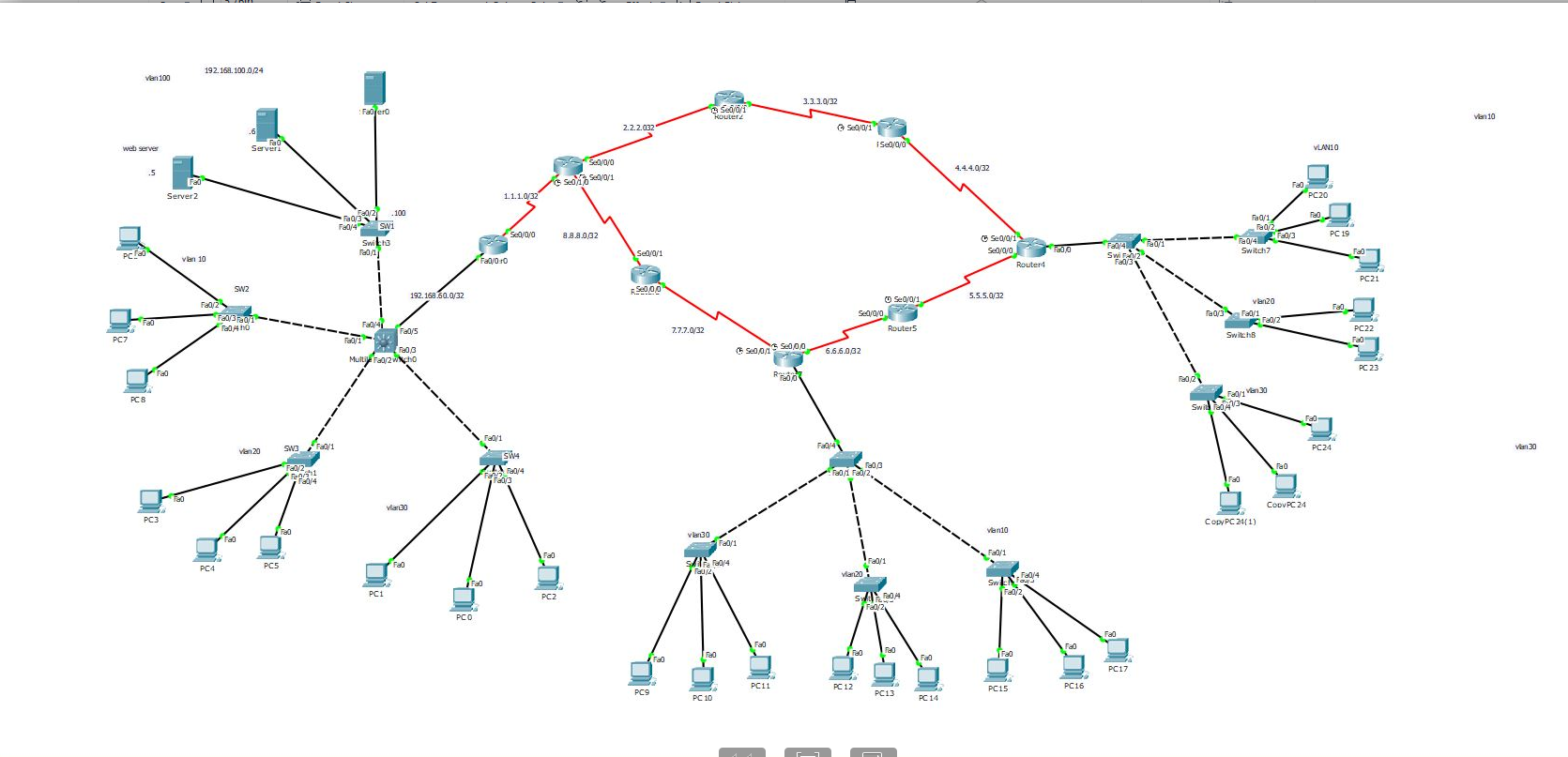
The network is activated by ACL Access Control List

To control some of the internal signals and prevent or allow access

Tools

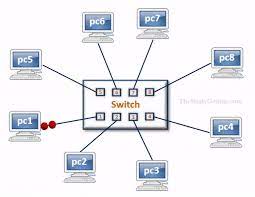
* 1-pc
* 2-Switchs
* 3-core switch
* 4-Routers
* 5- servers
* 6-packet tracer

**Picture from the projec**t

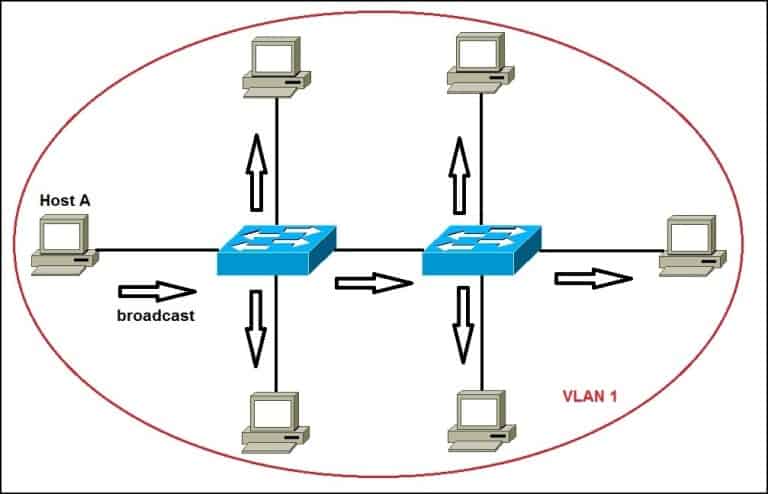


**switching**

Switching in IT and computer networking is the transfer of data packets, or blocks of data, through a network switch. Switches transfer data from source ports on devices such as computers to destination ports on devices such as routers.

****

**VLAN**

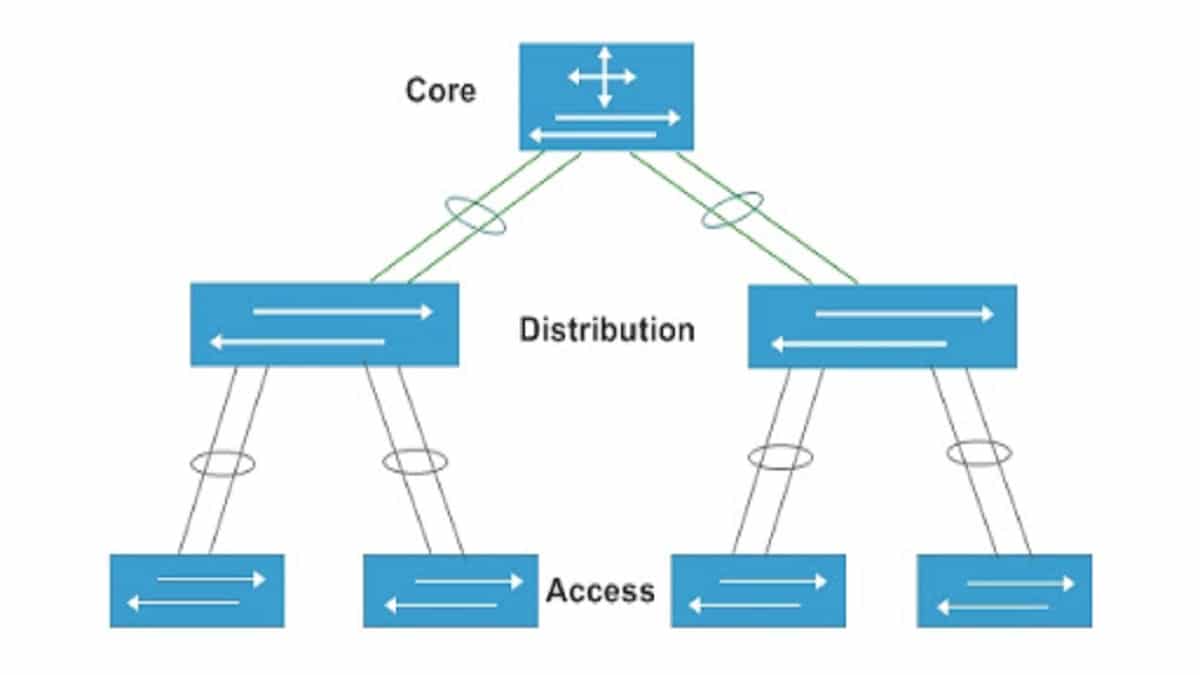
****

**VLANs (Virtual Local Area Networks) are an important concept in networking that provide numerous benefits and enhance network functionality. Here are some key reasons why VLANs are significant in network environments:**

**benefits of vlan**

* **Enhanced Network Security: VLANs help improve network security by isolating and segregating traffic. By logically dividing the network into separate VLANs, it becomes more difficult for unauthorized users to gain access to sensitive data or resources. VLANs can be used to isolate different departments, guest networks, or critical infrastructure, reducing the attack surface and limiting the propagation of potential security breaches.**
* **Improved Performance and Bandwidth Management: VLANs allow network administrators to prioritize and manage bandwidth according to specific requirements. By separating traffic into different VLANs, network congestion can be reduced, ensuring that critical applications or services receive the necessary bandwidth. This helps prevent bandwidth-hungry applications from affecting the performance of other network resources.**
* **Simplified Network Administration: VLANs provide logical grouping of devices, regardless of their physical location. This simplifies network administration tasks, such as configuration changes, security policies, and network monitoring. Rather than managing each individual device, network administrators can apply policies and settings to entire VLANs, streamlining network management processes.**
* **Flexibility and Scalability: VLANs offer flexibility in network design and scalability. New devices can be easily added or moved within VLANs without the need for physical reconfiguration. This flexibility simplifies network expansion, especially in dynamic environments where changes in network topology are frequent.**
* **Broadcast Control: VLANs reduce the propagation of broadcast traffic. Broadcast messages sent by devices within a VLAN are limited to that VLAN, preventing unnecessary broadcast traffic from overwhelming the entire network. This improves network efficiency and reduces bandwidth consumption.**

**core switch**

****

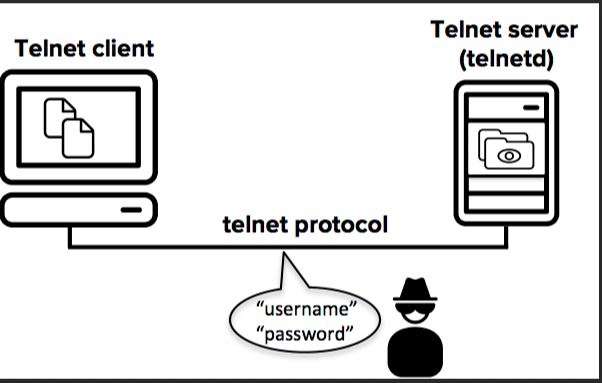
**A core switch, also known as a network core switch or backbone switch, is a high-performance networking device that serves as the central point of connectivity for multiple network segments or devices within a local area network (LAN) or wide area network (WAN). It is typically used in large-scale enterprise networks or data centers where high-speed and reliable connectivity is required.**

**The core switch plays a crucial role in directing network traffic and facilitating communication between various devices, such as servers, routers, switches, and other network devices. It acts as a central point of aggregation for multiple access switches or distribution switches within the network infrastructure.**

**Key features and functions of a core switch include**

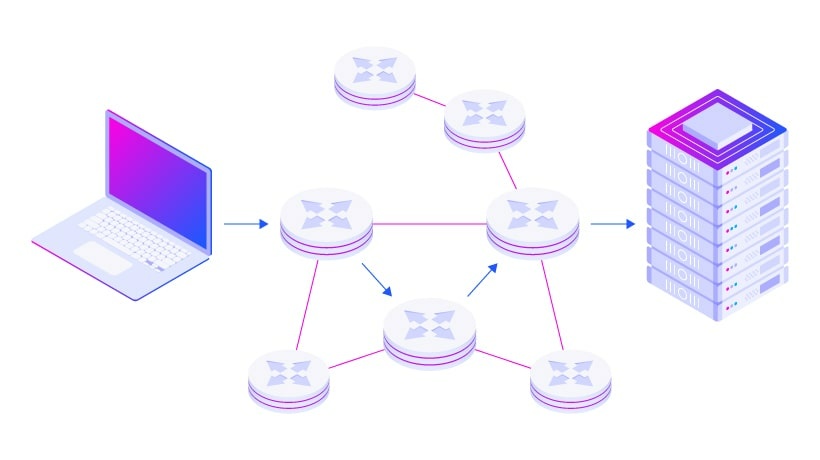
* **High Port Density: Core switches have a large number of ports to accommodate the connection of multiple devices and network segments.**
* **High Bandwidth: They are designed to provide high-speed data transfer rates to handle large volumes of network traffic efficiently.**
* **Redundancy and High Availability: Core switches often support redundancy features, such as link aggregation and redundant power supplies, to ensure continuous network operation and minimize downtime.**
* **Advanced Switching Technologies: Core switches employ advanced switching techniques, such as virtual LAN (VLAN) support, Quality of Service (QoS) capabilities, and multicast routing, to optimize network performance and manage traffic efficiently.**
* **Security and Access Control: Core switches may include features like Access Control Lists (ACLs), port security, and other security mechanisms to control access to the network and protect against unauthorized acces**

**Telnet (remote control)**

****

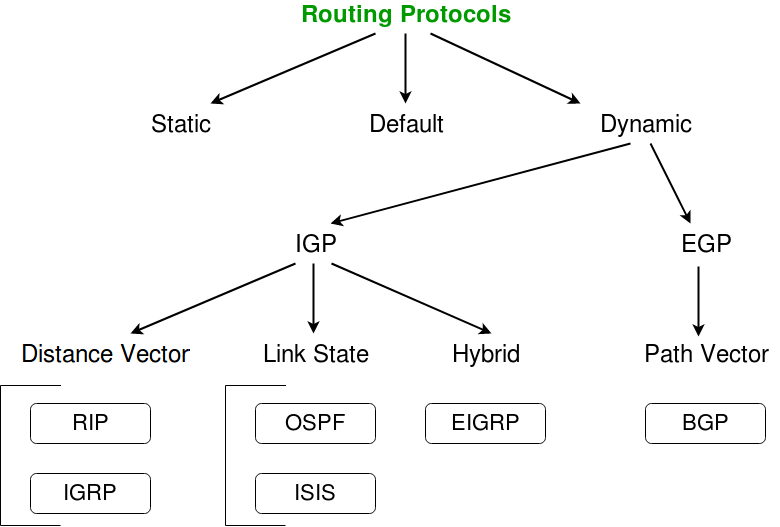
* **Telnet is a network protocol that allows remote access to devices or systems over a network. It enables users to establish a terminal session and interact with a remote device as if they were physically connected to it. Here are some key points about Telnet:**
* **Remote Access: Telnet provides a means to remotely access and manage devices such as servers, routers, switches, and network appliances. By establishing a Telnet session, users can execute commands, configure settings, and retrieve information from a remote device.**
* **Terminal Emulation: Telnet emulates a text-based terminal interface on the local computer, allowing users to interact with the remote device using command-line interfaces (CLI) or text-based menus.**
* **Port 23: Telnet operates using TCP/IP as its underlying protocol and typically uses port 23 for communication. The client establishes a connection to the Telnet server running on the remote device, initiating a session.**
* **Insecure Protocol: It's important to note that Telnet sends data, including usernames, passwords, and commands, in clear text format, making it vulnerable to eavesdropping and interception. Consequently, Telnet is considered an insecure protocol and is not recommended for use in environments where data security is a concern.**
* **Alternative: In modern network environments, Telnet has largely been replaced by more secure protocols like SSH (Secure Shell). SSH provides encrypted communication, authentication, and secure remote access to devices, offering improved security compared to Telnet.**
* **Telnet Clients: To initiate a Telnet session, a Telnet client is required. There are several Telnet client applications available, both as standalone software and as built-in features of operating systems. Users can establish Telnet sessions by specifying the IP address or hostname of the remote device they wish to connect to.**
* **Configuration and Management: Telnet is commonly used for configuration, management, and troubleshooting purposes. Network administrators may use Telnet to remotely configure routers, switches, and other network devices, allowing them to make changes or retrieve information without physically accessing the devices.**
* **In summary, Telnet is a protocol that enables remote access and management of devices over a network. However, due to its lack of encryption, it is not recommended for use in secure environments. SSH is often preferred as a more secure alternative to Telnet for remote access to device**

**Routing**

****

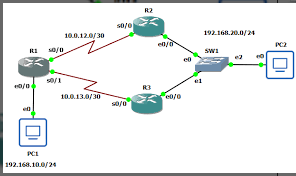
* **Routing in a network refers to the process of directing data packets between different networks or subnets. Routers are network devices that operate at the network layer (Layer 3) of the OSI model and are responsible for forwarding packets based on their IP addresses. Here are some key points about routing in a network:**
* **Packet Forwarding: Routers receive data packets from one network and determine the best path to forward them to their destination network. They use routing tables, which contain information about network addresses and the corresponding next-hop routers, to make forwarding decisions.**
* **Network Interconnectivity: Routers connect different networks together, enabling communication between devices in different subnets or across different physical locations. They facilitate the exchange of data between networks by forwarding packets based on IP addresses.**
* **Routing Protocols: Routing protocols are algorithms or sets of rules that routers use to exchange routing information and update their routing tables. Common routing protocols include RIP (Routing Information Protocol), OSPF (Open Shortest Path First), and BGP (Border Gateway Protocol). These protocols help routers dynamically learn about network changes, determine optimal paths, and maintain updated routing information.**
* **Routing Tables: Each router maintains a routing table that contains information about known networks, including the network addresses and the corresponding next-hop routers. The routing table is used to determine the appropriate outgoing interface or next-hop router for forwarding packets.**
* **Routing plays a critical role in network communication by enabling devices in different networks to communicate with each other. Routers make intelligent forwarding decisions based on network addresses, allowing data packets to traverse multiple networks and reach their intended destinations.**

**Routing Protocol**

****

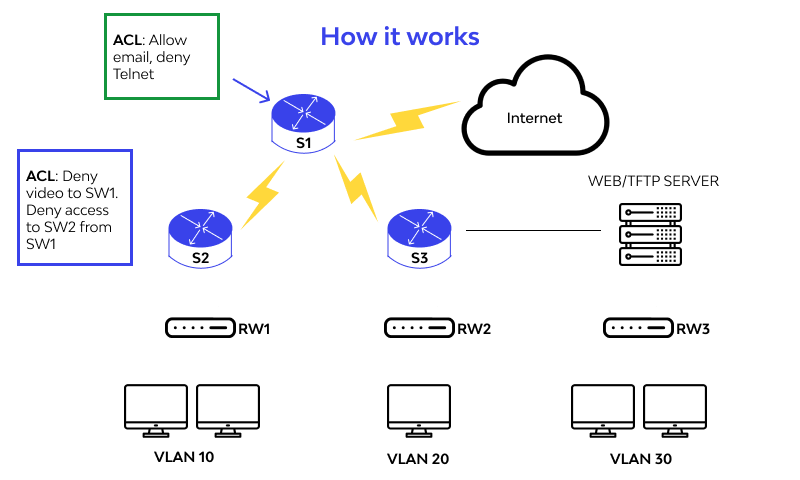
**Ospf Protocol**

**(Open Shortest Path First)**

****

* **OSPF (Open Shortest Path First) is a dynamic routing protocol used in computer networks. It is an Interior Gateway Protocol (IGP) designed to facilitate routing within an autonomous system (AS), such as a single organization's network. Here are some key points about OSPF:**
* **Link-State Protocol: OSPF is a link-state routing protocol. It builds and maintains a detailed map of the network's topology by exchanging link-state advertisements (LSAs) among OSPF routers. Each router has a complete picture of the network, allowing for more accurate route calculations.**
* **Shortest Path Calculation: OSPF uses the Dijkstra's algorithm to calculate the shortest path to reach different network destinations based on the cost associated with each link. The cost is typically based on the bandwidth of the link, with higher bandwidth links having lower costs.**
* **Hierarchical Design: OSPF supports a hierarchical design known as Areas. The network is divided into areas, with each area having its own OSPF topology database. This hierarchical structure reduces the size of the routing tables, enhances scalability, and improves network efficiency**

**ACL (access control list)**

****

**An Access Control List (ACL) is a set of rules or filters used to control and manage network traffic in a network device, such as a router or firewall. ACLs define what types of traffic are allowed or denied to pass through the device based on various criteria, such as source/destination IP addresses, protocols, ports, and other packet attributes. Here are some key points about ACLs:**

* **Traffic Filtering: ACLs are primarily used for traffic filtering, allowing network administrators to permit or deny specific types of traffic based on defined rules. ACLs can be configured to control inbound or outbound traffic, or both, depending on the desired network security and access policies.**
* **Rule-Based Structure: ACLs are composed of individual rules or entries, each specifying a set of criteria and an associated action (permit or deny). The rules are evaluated sequentially, and the first matching rule determines the action to be taken for a particular packet.**
* **Criteria for Matching: ACL rules can include various criteria for matching packets, including source/destination IP addresses, source/destination ports, IP protocols (such as TCP, UDP, ICMP), specific protocols (such as HTTP, FTP), and other packet attributes like VLAN tags. These criteria help define the conditions under which a rule should be applied to incoming or outgoing traffic.**

**It's important to carefully design and configure ACLs to ensure they meet the intended security objectives while avoiding unintended restrictions or vulnerabilities. Proper testing and monitoring are crucial to maintaining the effectiveness and accuracy of ACLs in a network environment.**