



Veermata Jijabai Technological Institute, Mumbai 400019

Experiment No.: 03

Aim: 1) Design the campus wide network for the campus of the engineering college.
2) To design a Data center Architecture

Group : Kiran Patil - 211070904
Mayuresh Murudkar - 211070903
Pratiksha Sankhe – 201071049

Branch: Computer Engineering

Batch: D

Theory:

A. Design the campus wide network for the campus of the engineering college.

Design Fundamentals: Campus Wired LAN

The LAN is the networking infrastructure that provides access to network communication services and resources for end users and devices spread over a single floor or building. You create a campus network by interconnecting a group of LANs that are spread over a local geographic area. Campus network design concepts include small networks that use a single LAN switch, up to very large networks with thousands of connections.

The campus wired LAN enables communications between devices in a building or group of buildings, as well as interconnection to the WAN and Internet edge at the network core.

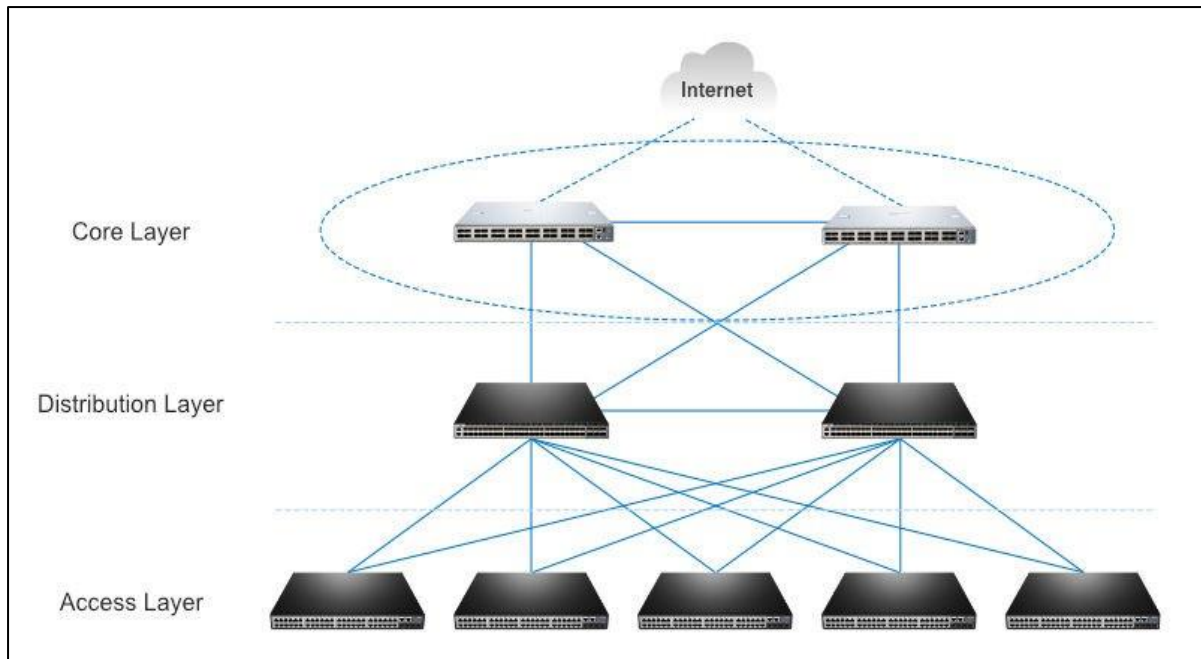
Specifically, this design provides a network foundation and services that enable:

- Tiered LAN connectivity.
- Wired network access for employees.
- IP Multicast for efficient data distribution.
- Wired infrastructure ready for multimedia services.

Location of the core switch, distribution switch and access switch.

1. Core switch:

- A core switch is a high-capacity switch generally positioned within the backbone or physical core of a network. Core switches serve as the gateway to a wide area network (WAN) or the Internet.
- The high-capacity core switch plays an important role in delivering frames/packets as fast as possible in the center of the network.

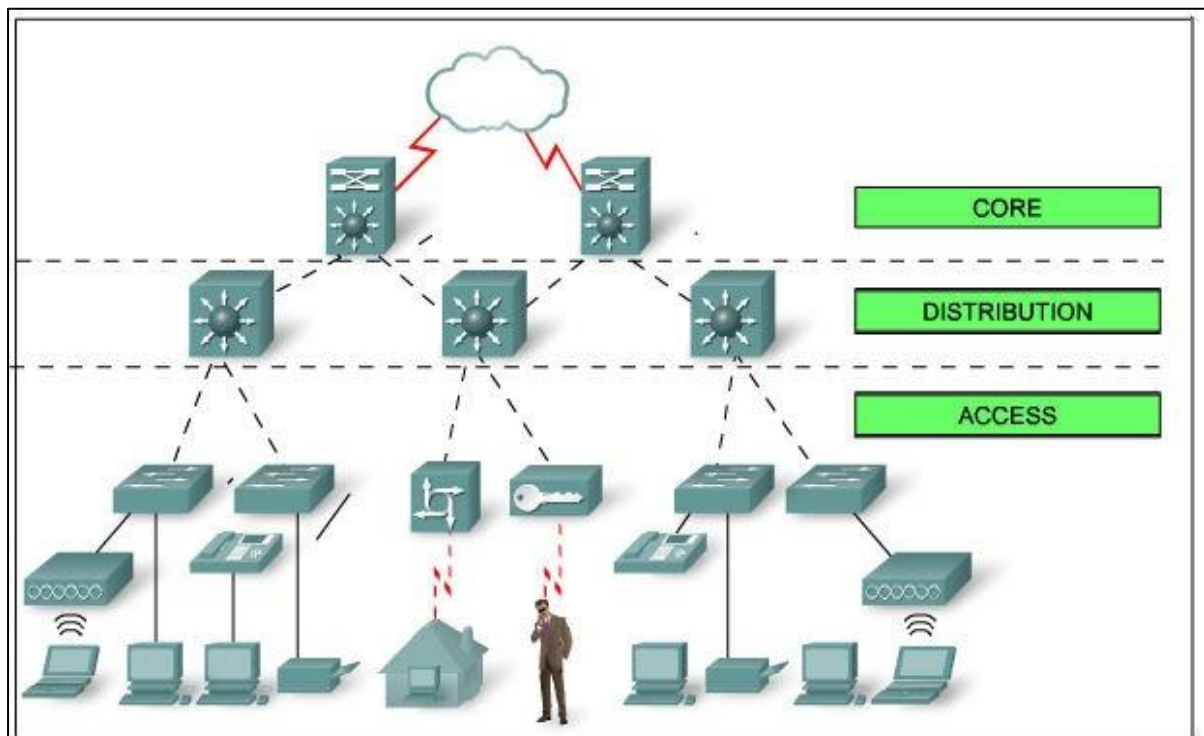
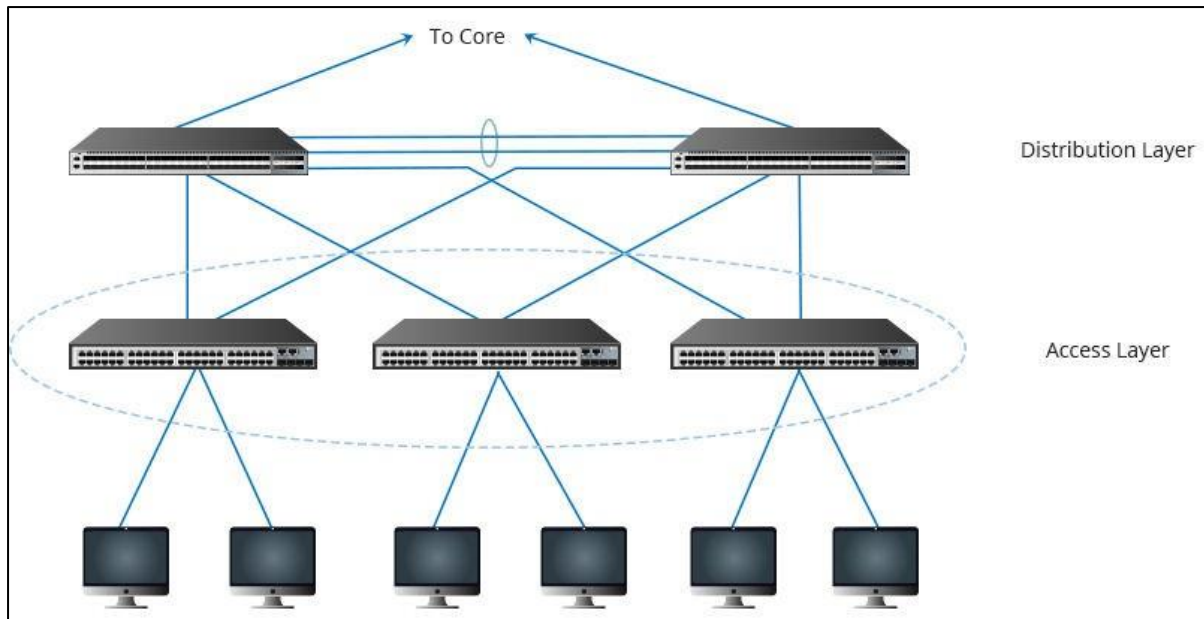


2. Distribution switch:

- A distribution switch is a distribution layer switch which plays an important role of bridge and link between the core layer switch and the access layer switch.
- This is also the reason why a distribution switch is called an aggregation switch.
- In addition, the distribution switch ensures the packets are properly routed between subnets and VLANs.
- Distribution switch usually supports higher performance and is mainly responsible for routing and policy-based network connectivity.

3. Access switch:

- It is the basic device in the access layer.
- The access layer is the lowest level and most fundamental layer in all these three layers.
- An access layer switch is usually a Layer 2 switch and facilitates the connection of end node devices to the network.
- In general, it is not a high-powered switch when compared with those at the distribution layer.



Cables

--- Crossover

— Straight-through

⚡ WAN Link

Devices and End Users



Access Server



Access Switch



Core Multilayer Switch



Distribution Multilayer Switch



Home Office



Teleworker

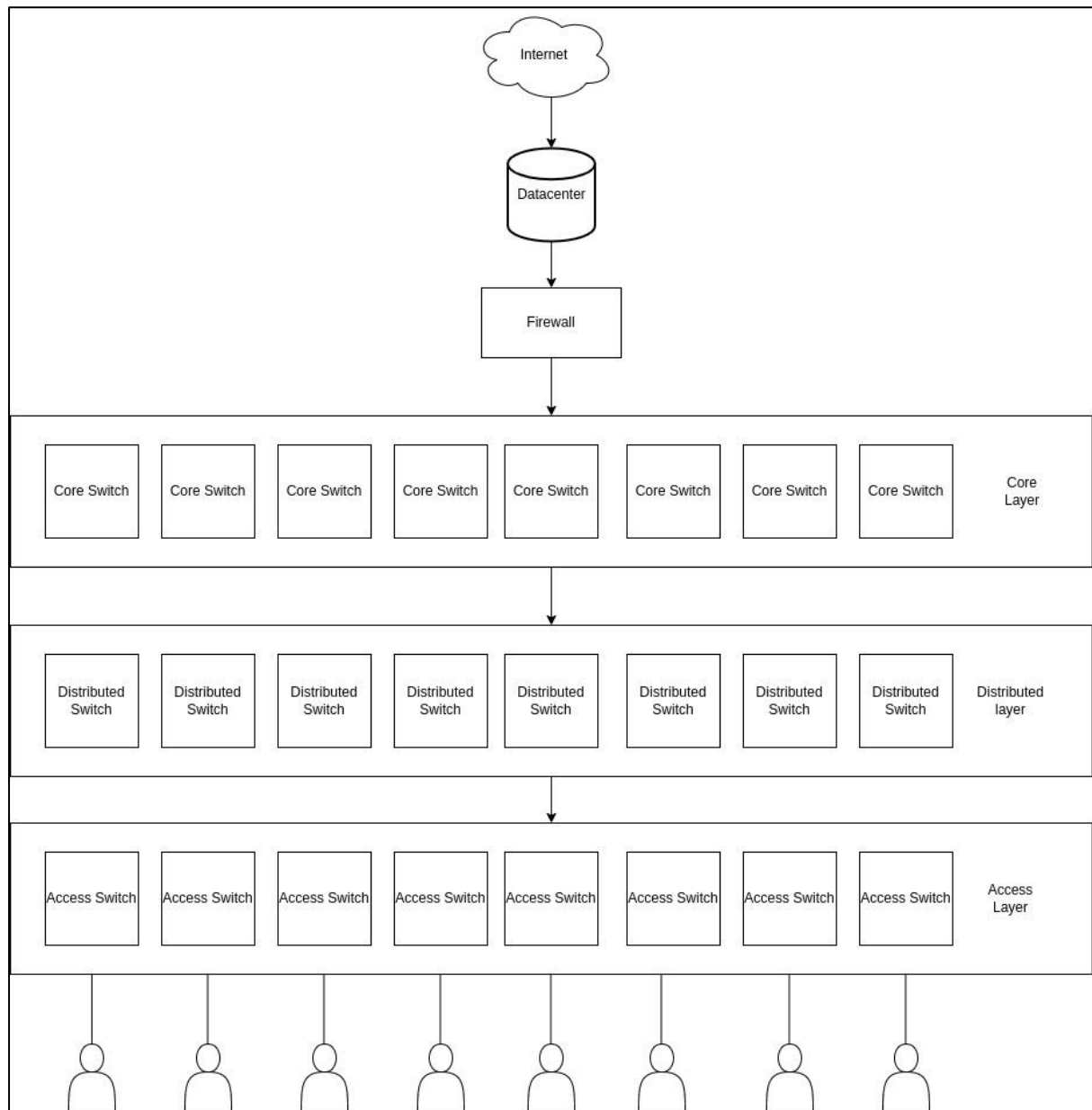


VPN Gateway

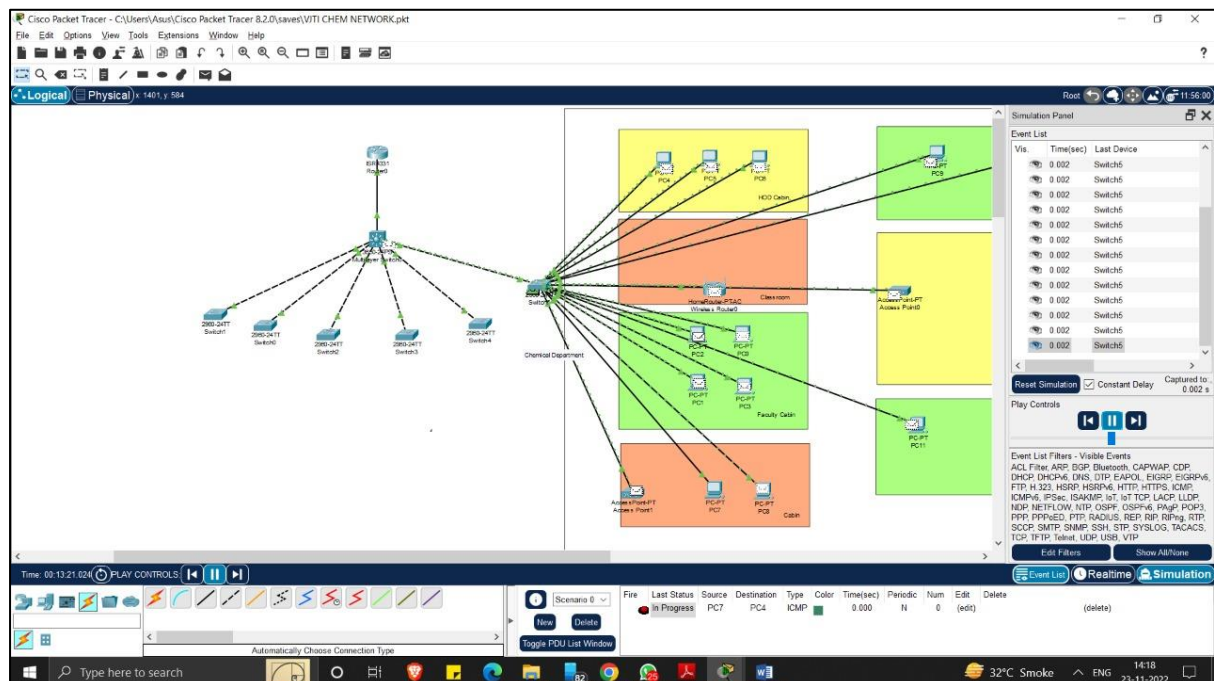
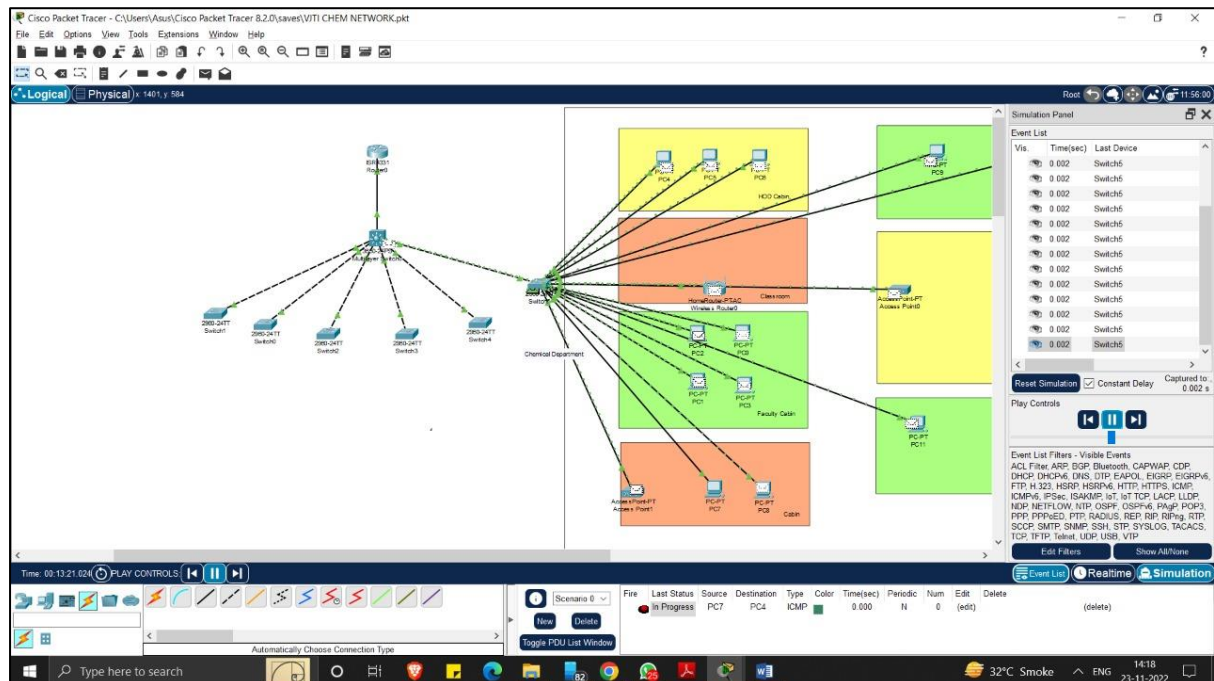


Wireless Router

Block Diagram for the campus network:



Campus Network design using cisco packet tracer



The typical hierarchical design model is broken up into three layers:

Access, Distribution and Core.

1) Access Layer:

provide a means of connecting devices to the network and controlling which devices are allowed to communicate on the network Devices: PCs, printers, and IP phones, routers, switches, bridges, hubs, and wireless access points (AP)

2) Distribution Layer:

aggregates the data received from the access layer switches before it is transmitted to the core layer for routing to its final destination. The distribution layer controls the flow of network traffic using policies and delineates broadcast domains by performing routing functions between virtual LANs (VLANs) defined at the access layer. Devices: high-performance switches to ensure reliability

3) Core Layer:

high-speed backbone of the internetwork Devices: routers, switches capable of forwarding large amounts of data quickly

Benefits of a Hierarchical Network

- Scalability /Hierarchical networks scale very well
- Redundancy/Double distribution and core switches
- Performance/High-performance distribution and core switches guarantee wire speed between all devices
- Security/Various policies at access, advanced security policies at distribution
- Manageability/Fast new deployment and simplified troubleshooting
- Maintainability/Scale very easily

B. Design a Data center Architecture

Requirements for setting the data center, firewall, IPS, Routing.

1. Infrastructure/ Hardware Requirements

An infrastructure represents the vast array of IT gear deployed within the facility. This is the equipment that runs applications and provides services to the business and its users. A typical IT infrastructure includes the following components:

- **Servers.** These computers host enterprise applications and perform computing tasks.
- **Storage. Subsystems,** such as disk arrays, are used to store and protect application and business data.
- **Networking.** The gear needed to create a business network includes switches, routers, firewalls and other cybersecurity elements.
- **Cables and racks.** Miles of wires interconnect IT gear, and physical server racks are used to organize servers and other gear within the facility space.
- **Backup power.** Uninterruptible power supply (UPS), flywheel and other emergency power systems are critical to ensure orderly infrastructure behavior in the event of a main power disruption.
- **Cooling Systems.** Data centers require that multiple servers be placed in close proximity to one another, in a limited space. That being the case, there are high chances of equipment overheating rapidly, in spite of the units' internal fans. Server rooms must therefore be maintained at a specific temperature as prescribed and planned during setup, through the use of external HVAC equipment, for smooth functioning.

In data centers that don't use a hot/cold aisle design, the cooling units aren't always able to efficiently cool equipment.

Active and passive components specifications.

Active components:

- Switches: Core switches, Distribution switches and Access switches
- Repeaters
- Routers
- Firewall (UTM)
- IPS
- Servers

Passive components:

- Switch boards
- Plugs
- Connectors
- Cables (coaxial/fiber optic/LAN)
- Patch points

Vulnerabilities, attacks and defence mechanisms

1. Router

- **Vulnerabilities**

1. If there are inconsistencies in router software i.e. outdated versions of software or patches are not upgraded frequently. There is weak authentication.

- **Attacks**

1. Syn Flood attack
2. Brute Force attack
3. Disgruntled Employee

- **Defence Mechanism**

4. Keep your router software up-to-date, upgrade patches.
5. Limit the authoritative access to required people only.

2. Switch

- **Vulnerabilities**

- 1) Improper configuration of switches.
- 2) Allowing to acquire ports for each dhcp action.
- 3) Making entries for MAC addresses without inspection

- **Attacks**

- 1) Mac Flood attack
- 2) DHCP spoofing
- 3) Arp spoofing

- **Defence Mechanism**

- 1) Port Scanning / Port based authentication
- 2) DHCP snooping
- 3) Dynamic ARP Inspection

3. Firewall

- **Vulnerabilities**

- 1) Outdated firewall software exists.
- 2) Lack of Documentation leading to failure of activating controls.
- 3) Insider attack possibility.
- 4) Inspection protocols are too basic.

- **Attacks**

- 1) Denial of Service exploiting old vulnerabilities.
- 2) IP spoofing is possible if anti spoofing controls are not turned on.
- 3) Fragmentation attacks.

- **Defence Mechanism**

- 1) Keeping the firewall software up-to-date / upgrading the patches.
- 2) Configuring required controls appropriately.
- 3) Setting up proper inspection protocols to detect any kind of malicious packet.

1) Design a Data Center Architecture.

We have 20 TB storage with a redundant controller having 4 FC ports on each controller. We are having 2 48-port Switch [4/48] in a Data Center, we also have 4 HP UNIX servers with 2 single port HBA, 3 Linux servers with 2 dual port

HBAs and 2 Windows servers with 1 single port HBA. Please create a solution design for the Data Center, having the highest level of redundancy.

Available Devices:

- 20 TB Storage Array
- 2 48-port Switch [4/48]
- 4 HP-Unix Servers with 2 Single Port HBA
- 3 Linux Servers with 2 Dual Port HBA
- 2 Windows Servers with Single Port HBA

Theory:

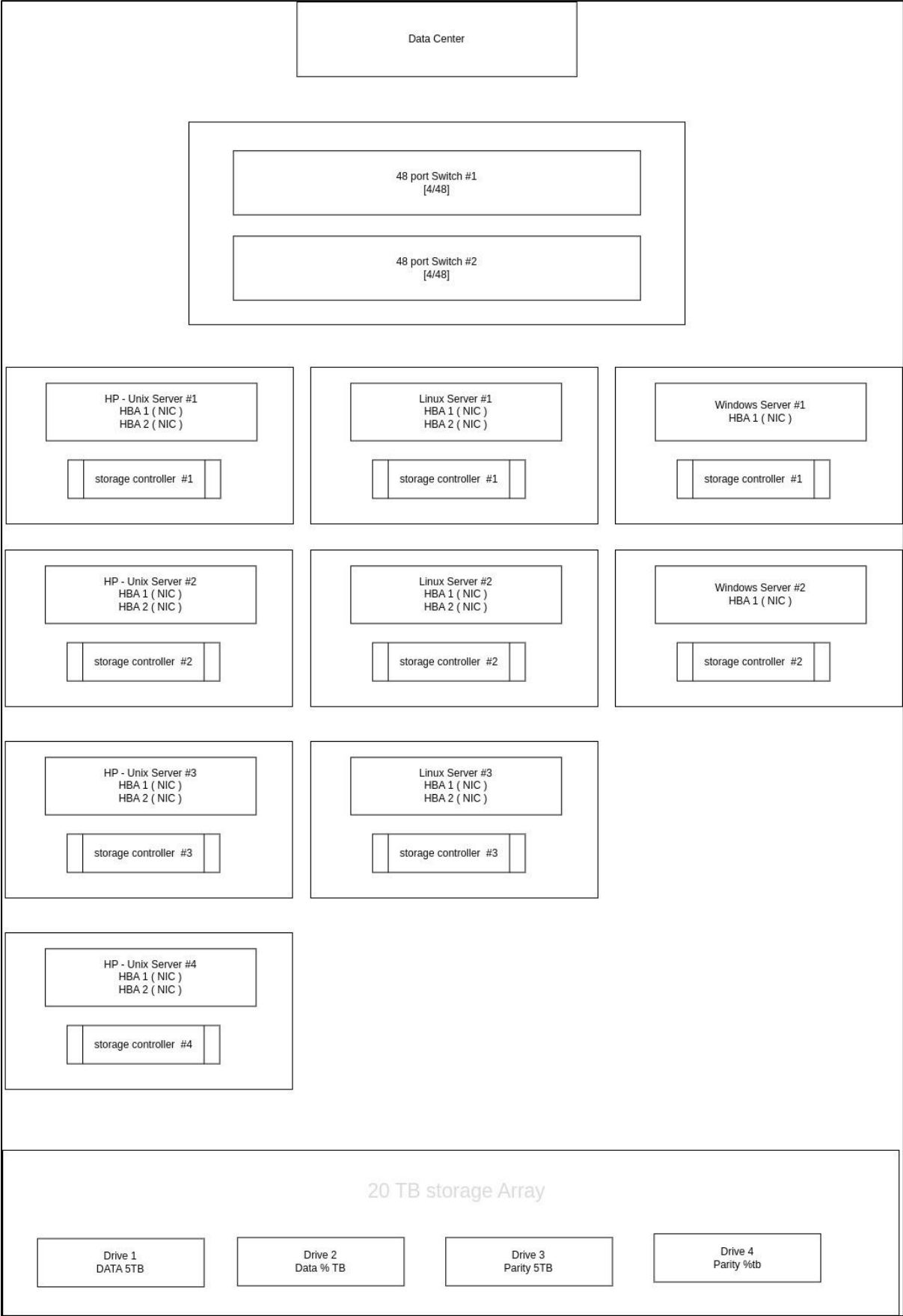
What is redundancy in a data center?

Redundancy refers to a system design where a component is duplicated so that in the event of a component failure, IT equipment is not impacted. For example, having redundant power in case there's a power outage.

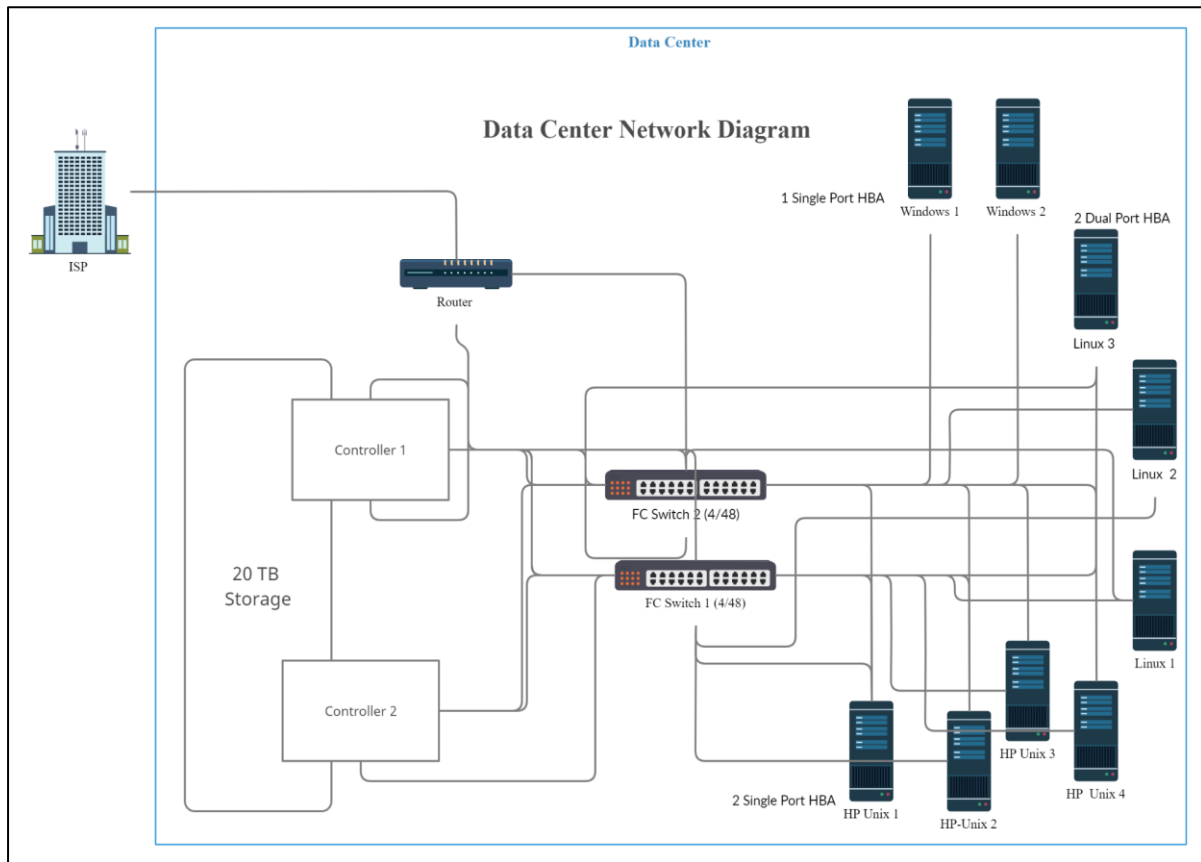
Network Design Principles

- **Network Diameter:** the number of devices that a packet has to cross before it reaches its destination. Keeping the network diameter low ensures low and predictable latency between devices.
- **Bandwidth Aggregation:** allows multiple switch port links to be combined so as to achieve higher throughput between switches (called EtherChannel from Cisco).
- **Redundancy:** double up the network connections between devices, or you can double the devices themselves.
- **Convergence** is the process of combining voice and video communications on a data network.

BLOCK DIAGRAM FOR DATA CENTER



DATA CENTER ARCHITECTURE



Conclusion:

Thus, with the help of this assignment we learnt about secure network design by formulating a plan to design a campus network for an engineering college, specified all the requirements as well as designed the data center architecture.