Group No. 4 - Team Members	Navya Sharma - 191071049
Cyber Security Lab Assignment 3	Esha Shah - 201071902
Final Year B.Tech Computer Engineering	Srushti Fuldeore - 201071908

Secure Network Design For Organization

AIM:

1) Design the campus wide network for the campus of the engineering college.

A. Analyze the location of the **core** switch, **distribution** switch and **access** switch and departmental requirements for connectivity of the computers.
B. Also Specify the requirements for setting the data center and **firewall** and **IPS**, **Routing** Requirements.
C. Identify **active** and **passive components** specifications for the design of the network.
D. Identify the **vulnerabilities, attacks and defense** mechanisms for the security of an organization's enterprise network.
E. Formulate the **organizational guidelines** for network and computing infrastructure usage.

2) To design a Data Center Architecture.

THEORY:

1) 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.

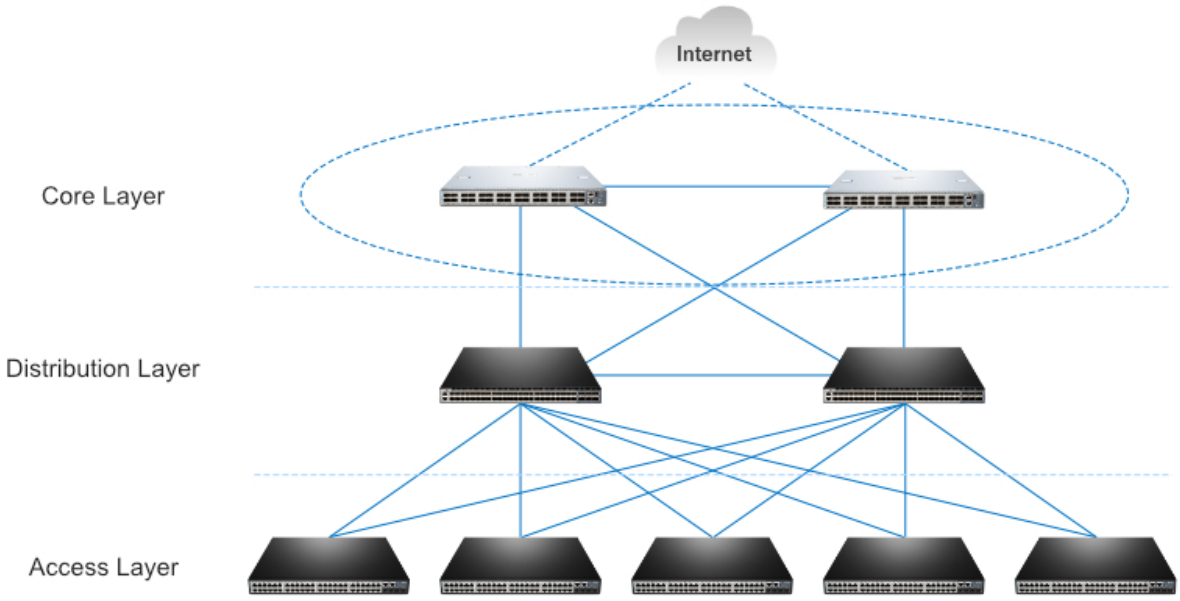
The campus wired LAN enables communications between devices in a building or group of buildings, as well as interconnection to the WAN and Internet edge at the network core.

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.

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

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.

Distribution switch:

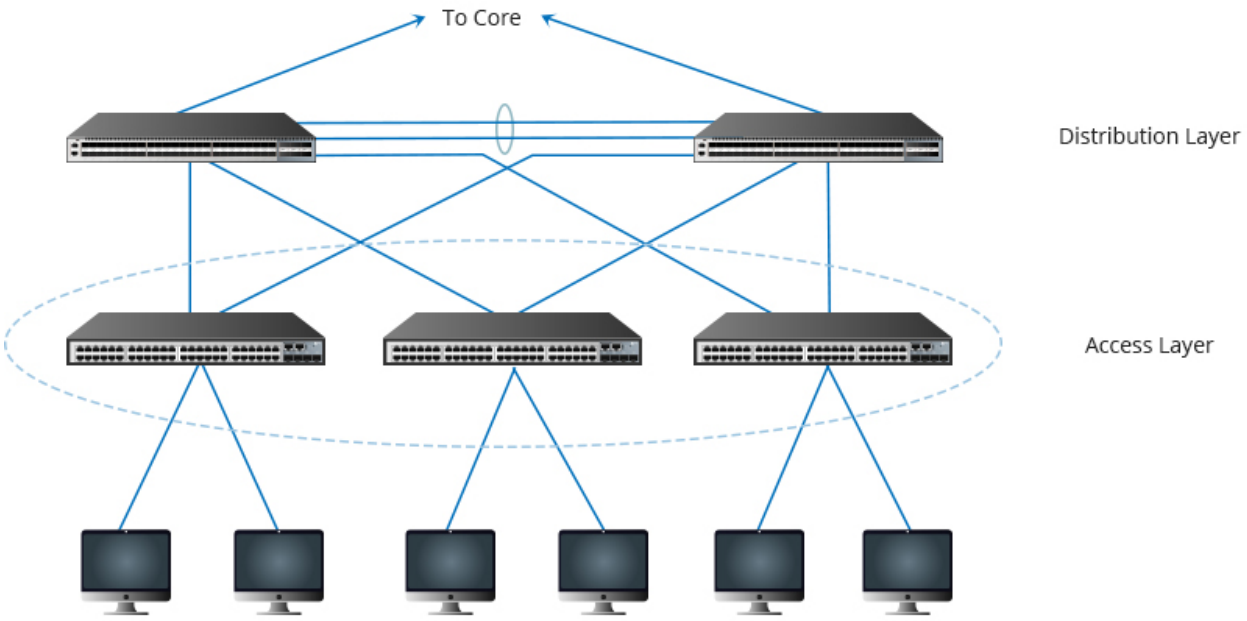
● A distribution switch is a distribution layer switch which plays an important role of bridge and link between the core layer switch and the access layer switch.

● 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.

Access switch:

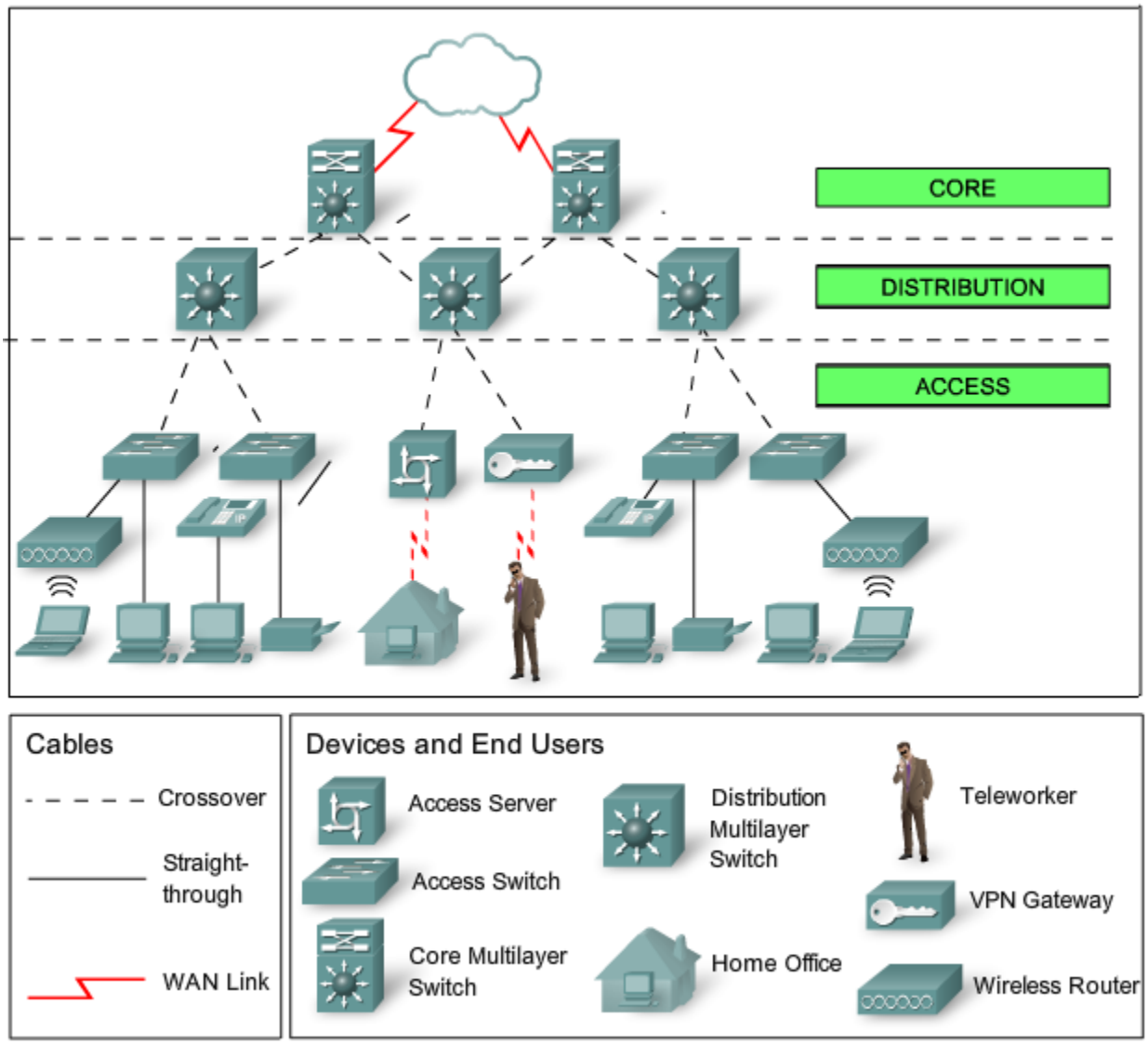


● It is the basic device in the access layer.

● 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.



The typical hierarchical design model is broken up into three layers: *Access, Distribution and Core.*

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

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

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

Benefits of a Hierarchical Network

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

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

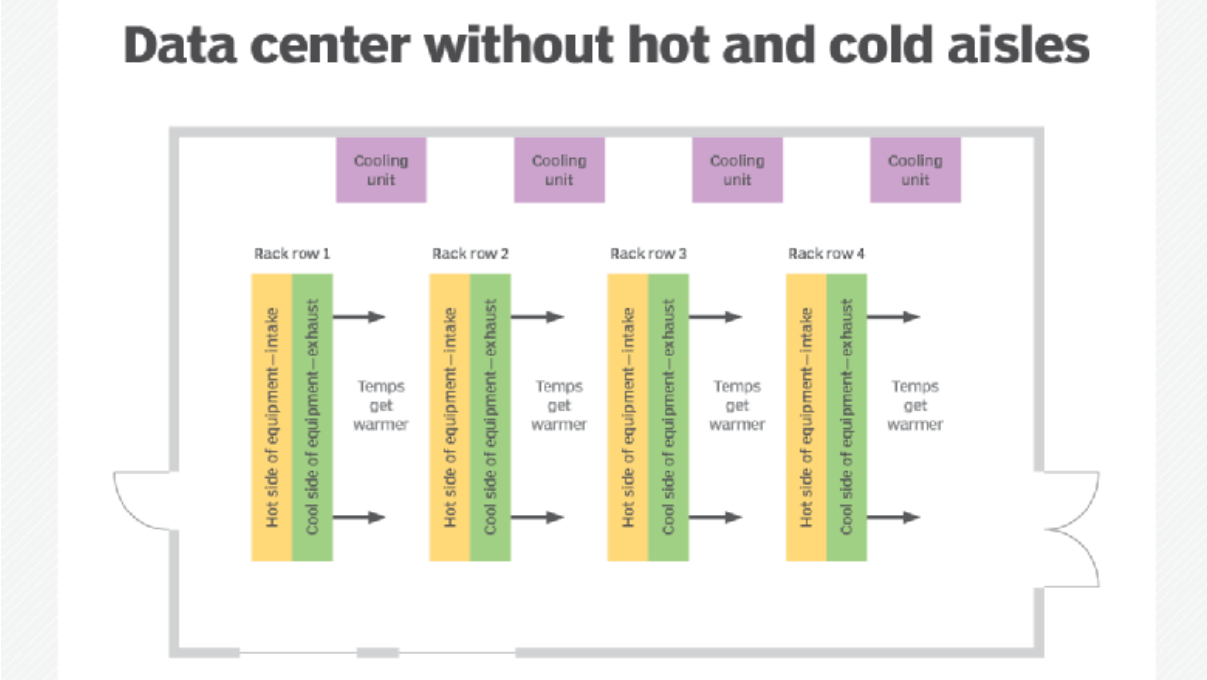
Requirements for setting the data center

1. Infrastructure/ Hardware Requirements

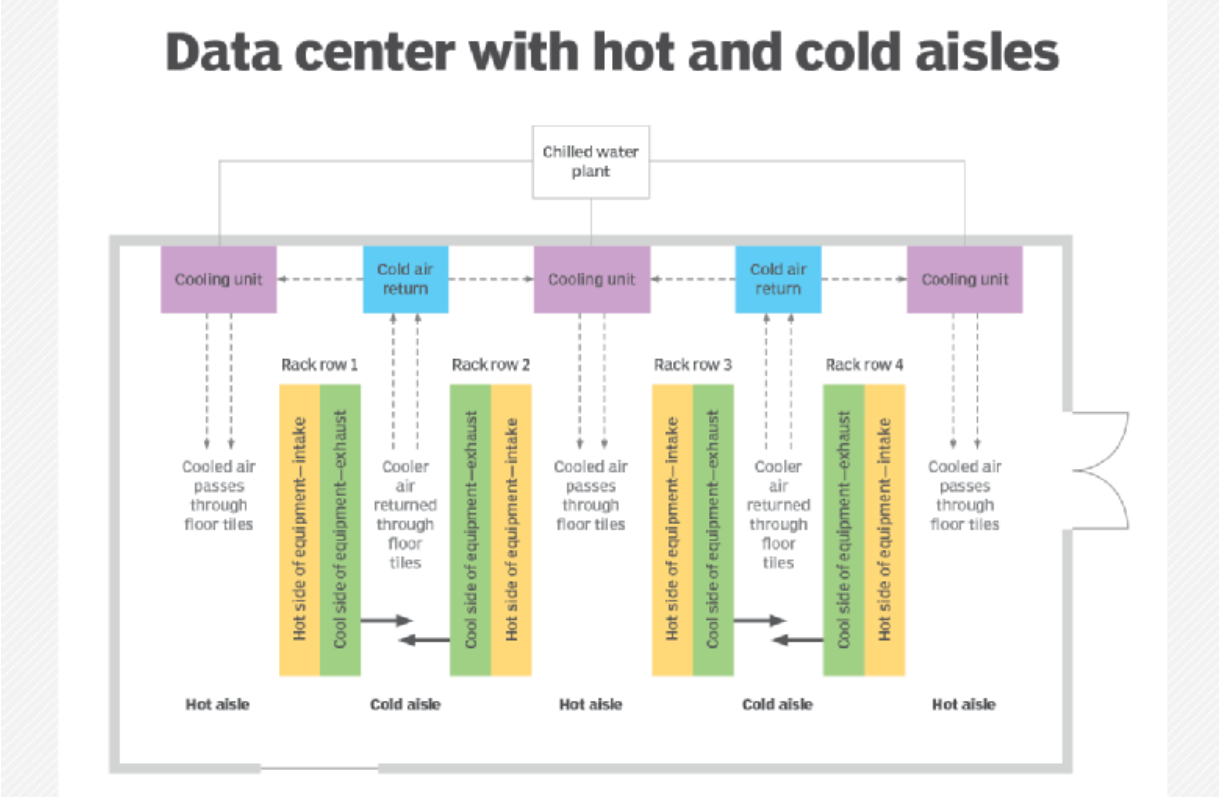
An infrastructure represents the vast array of IT gear deployed within the facility. This is the equipment that runs applications and provides services to the business and its users. A typical IT infrastructure includes the following components:

- **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.



In data centers designed around hot/cold aisles, the cooling units are able to more efficiently cool equipment.



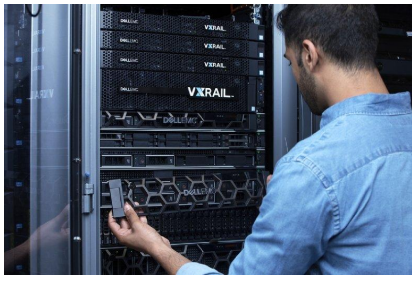
- **Management platforms.** One or more data center infrastructure management (DCIM) platforms are needed to oversee and manage the IT infrastructure reporting on system health, availability, capacity and configuration.

2. Physical space and data center organization

Perhaps the most significant and perplexing space issue is right-sizing the data center for the business. Data centers are incredibly expensive. It's critical to establish a facility that offers capacity for growth yet optimizes utilization. Myriad other factors to consider within a data center space include the following:

- **Lighting.** Most data center lighting is low or off without human presence.
- **Temperature.** Cooling demands can keep temperatures low, so humans might need some protective clothing.
- **Noise.** The cooling fans in dozens -- even hundreds -- of servers can produce a cacophony that requires hearing protection.
- **Weight.** Equipment is heavy, and flooring must be designed to bear the extreme weight. Special weight considerations might be needed for raised flooring used to handle cooling airflows.

The most common feature of any data center layout is the *server rack* -- or, simply, *rack*. Racks also play a vital role in data center cooling schemes. Racks of gear are commonly organized to create hot and cold aisles that can improve cooling efficiency by allowing the introduction of cooled air into a cold aisle, which is heated by gear and delivered into a hot aisle, where the heated air can be effectively removed from the room.

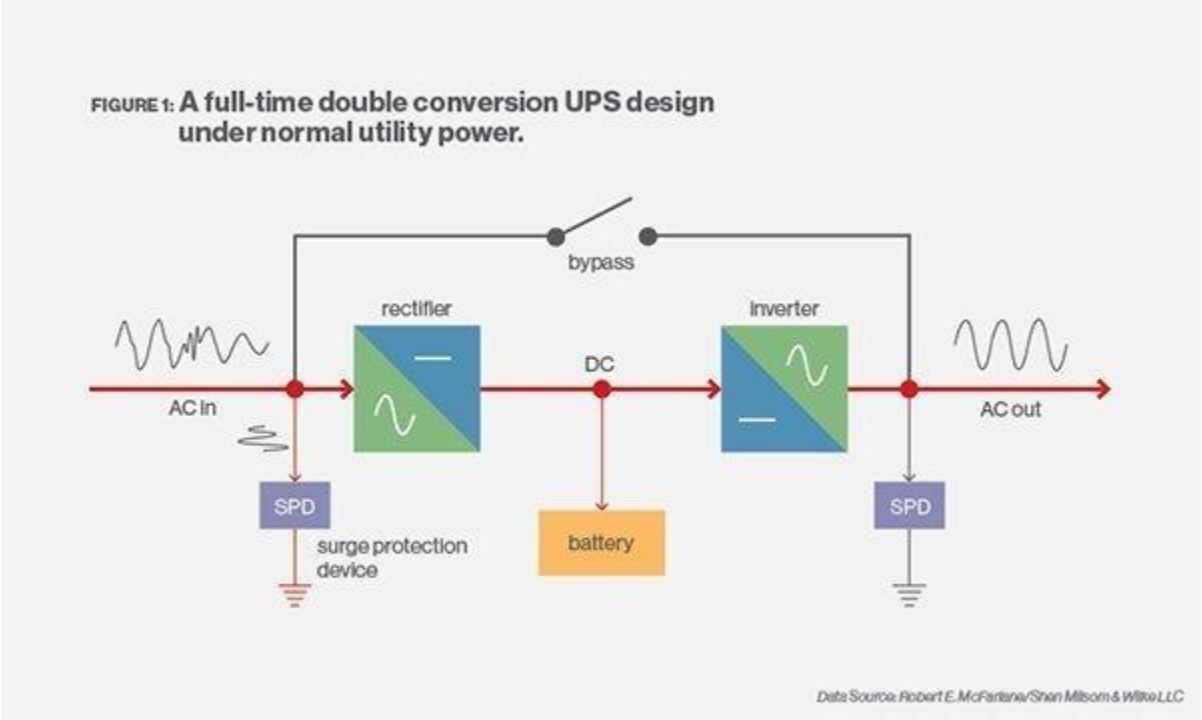


This image shows an IT professional installing and maintaining high-capacity, rack-mounted systems in a data center.

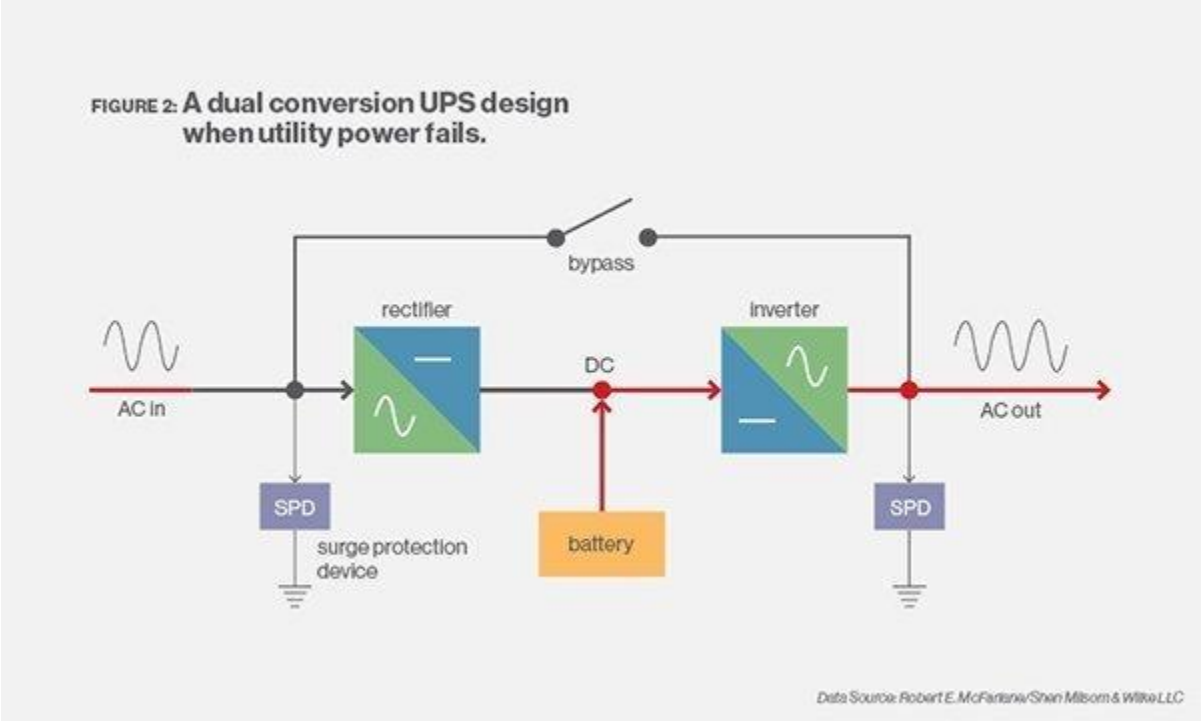
3. Data center power and performance demands

Power is a perpetual challenge for any enterprise-class data center. A large facility can consume about 100 megawatts -- enough to power around 80,000 homes. Therefore, data center operators place the following demands on utility power:

- **Capacity.** There must be adequate power to run the data center.
- **Cost.** Power must be as inexpensive as possible.
- **Quality.** Power must be electrically clean (i.e., free of undesirable electrical noise, surges and spikes).
- **Reliability.** Power must be free of brownouts, blackouts or other disruptions.



A full-time double conversion UPS design under normal utility power.



A dual conversion UPS design when utility power fails.

4. Physical Security

In terms of physical security, a data center should have:

- Gated grounds.
- Perimeter security with 24/7 guard posts.
- Access controls with locked doors and racks.
- Video monitoring of each rack row.
- Closed-circuit security monitoring.
- Live technical surveillance by expert NOC staff.
- Mantraps with multi-factor authentication.
- Windowless environments.

The physical space where the data center is set up must be resistant to natural disasters like flooding, earthquakes, fires, etc. This is of course in addition to physical security systems and access control systems to keep the data private.

Requirements for Managed (Hardware) Firewalls

For the purposes of this document, a firewall is defined as any device which:
a) sits between multiple computers and the College network, and
b) filters traffic or translates network addresses.

- All firewalls must be registered with IT Security.
- Firewalls may not be placed in front of networking equipment managed by IT Services.
- The organization installing the firewall agrees to act as the first line of support for all networking issues involving machines behind the firewall. If IT Services is contacted by someone trying to connect through the firewall, that person may be directed to contact the firewall administrators.
- If the firewall runs any sort of address translation for more than one machine, the maintainers must keep at least six months of logs indicating which machine made every connection through the firewall. The maintainers must provide this information to IT Security upon request.
- The firewall must allow through the firewall any connections from IT Services that are necessary to ensure the integrity of the data network and to allow for vulnerability scans by IT Security.
- If a machine behind the firewall is in violation of the Acceptable Use Policy and would normally be removed from the network, the firewall will be removed from the network (isolating all machines behind it.)
- The organization installing the firewall understands that many modern threats to security are specifically designed to bypass firewalls. Machines behind firewalls must be kept secure.

IPS:

- An IPS can be deployed in a few different ways. The most common deployment model for an IPS is as a **network-based IPS (NIPS)**.
- A **NIPS** is deployed to protect an **entire network** unlike a host-based IPS (HIPS), which protects a single computer.
- A NIPS is deployed at the network boundary alongside or as part of a network firewall.

- All traffic entering and leaving the protected network is inspected by the NIPS, and the NIPS has the ability to block connections or drop packets if malicious or suspicious content is detected.

Router Operation and Maintenance Requirements:

The following kinds of activity are included under router Operation & Maintenance:

- Diagnosing hardware problems in the router processor, in its network interfaces, or in the connected networks, modems, or communication lines.
- Installing a new version of the routers software.
- Restarting or rebooting a router after a crash.
- Configuring (or reconfiguring) the router.
- Detecting and diagnosing Internet problems such as congestion, routing loops, bad IP addresses, black holes, packet avalanches, and misbehaved hosts.
- Changing network topology, either temporarily (e.g., to diagnose a communication line problem) or permanently.
- Monitoring the status and performance of the routers and the connected networks.
- Collecting traffic statistics for use in (Inter-)network planning.

C. Active and passive components specifications.

Active components:

1. Switches: Core switches, Distribution switches and Access switches
2. Repeaters
3. Routers
4. Firewall (UTM)
5. IPS
6. Servers

Passive components:

1. Switch boards
2. Plugs

3. Connectors
4. Cables (coaxial/fiber optic/LAN)
5. Patch points

D. Vulnerabilities, attacks and defense mechanisms

Router

Vulnerabilities

i. If there are inconsistencies in router software i.e. outdated versions of software or patches are not upgraded frequently.

ii. There is weak authentication.

Attacks

i. Syn Flood attack

ii. Brute Force attack

iii. Disgruntled Employee

Defense Mechanism

i. Keep your router software up-to-date, upgrade patches.

ii. Limit the authoritative access to required people only.

Switch

Vulnerabilities

i. Improper configuration of switches.

ii. Allowing to acquire ports for each dhcp action.

iii. Making entries for MAC addresses without inspection

Attacks

i. Mac Flood attack

ii. DHCP spoofing

iii. Arp spoofing

Defense Mechanism

i. Port Scanning / Port based authentication

ii. DHCP snooping

iii. Dynamic ARP Inspection

Firewall

Vulnerabilities

i. Outdated firewall software exists.

ii. Lack of Documentation leading to failure of activating controls.

iii. Insider attack possibility.

iv. Inspection protocols are too basic.

Attacks

i. Denial of Service exploiting old vulnerabilities.

ii. IP spoofing is possible if anti spoofing controls are not turned on.

iii. Fragmentation attacks.

Defense Mechanism

i. Keeping the firewall software up-to-date / upgrading the patches.

ii. Configuring required controls appropriately.

iii. Setting up proper inspection protocols to detect any kind of malicious packet.

E. Formulate the organizational guidelines.

More information can be found here**:** **Policies and Guidelines for Effective Network Management**

Table 1: **Guidelines for implementing IT security policie**s

Guideline	**Description**
Create awareness	Create user awareness using the following methods: · Notify employees about the new security polices. · Update employees on the progress of new security policies. · Publish policy documentation electronically and on paper. · Develop descriptive security documentation for users. · Develop user-training sessions. · Require new users to sign a security acknowledgement.

Maintain awareness	Maintain user awareness of ongoing and new security issues using the following methods: · Web site · Posters · Newsletters · E-mail for comments, questions, and suggestions

- Assign responsibility for reviewing policies and procedures.
- Implement a reporting plan in which departments report security incidents to designated security personnel
- Implement regular reviews to evaluate the following:
    - Nature, number, and impact of recorded security incidents.
    - Cost and impact of controls on business efficiency, including third-party vendor compliance.
    - Effects of changes to organizations or technology.

Information Management

This section contains guidelines for the following policies: Handling information & Disposing of media.

Handling Information

Electronically stored information should be protected from unauthorized access or misuse. Each department in an institution should establish internal procedures for the secure handling and storage of its electronically stored information to prevent unauthorized access or misuse. The guidelines for handling electronically stored information are:

- Develop procedures to invoice and manage the following:
  Documents, Computing systems, Networks, Mobile users, Postal services, E-mail, Voice mail, Voice communications, Fax machines, Multi-media and Other sensitive items
- Develop methods for handling and storing media.
- Develop access restrictions to identify unauthorized users.
- Maintain formal records of the recipients of data.
- Store media in accordance with manufacturer's specifications

- Restrict distribution of information.
- Indicate the authorized recipient of all copies of data.

Disposing of Media

To ensure the security of information, Institutions should develop procedures to render information unrecoverable before disposing of media. Each department should develop a media disposal process based on the sensitivity of the data as determined by law and the data owners. Guidelines for disposing of media are:

- Dispose of paper media
- Cleanse magnetic or optical media
- Develop disposal procedures

Conclusions

Once an institution has agreed upon a set of security policies, then the procedure, plans, guidelines and standards that support those policies should be documented and disseminated to the appropriate managers and users. In addition, a back-up plan is necessary to ensure that essential stored data be recovered in the event of a system failure or disaster.

---

2) Design a Data Center Architecture.

Question: 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:

1. 20 TB Storage Array
2. 2 48-port Switch [4/48]
3. 4 HP-Unix Servers with 2 Single Port HBA
4. 3 Linux Servers with 2 Dual Port HBA

5. 2 Windows Servers with Single Port HBA

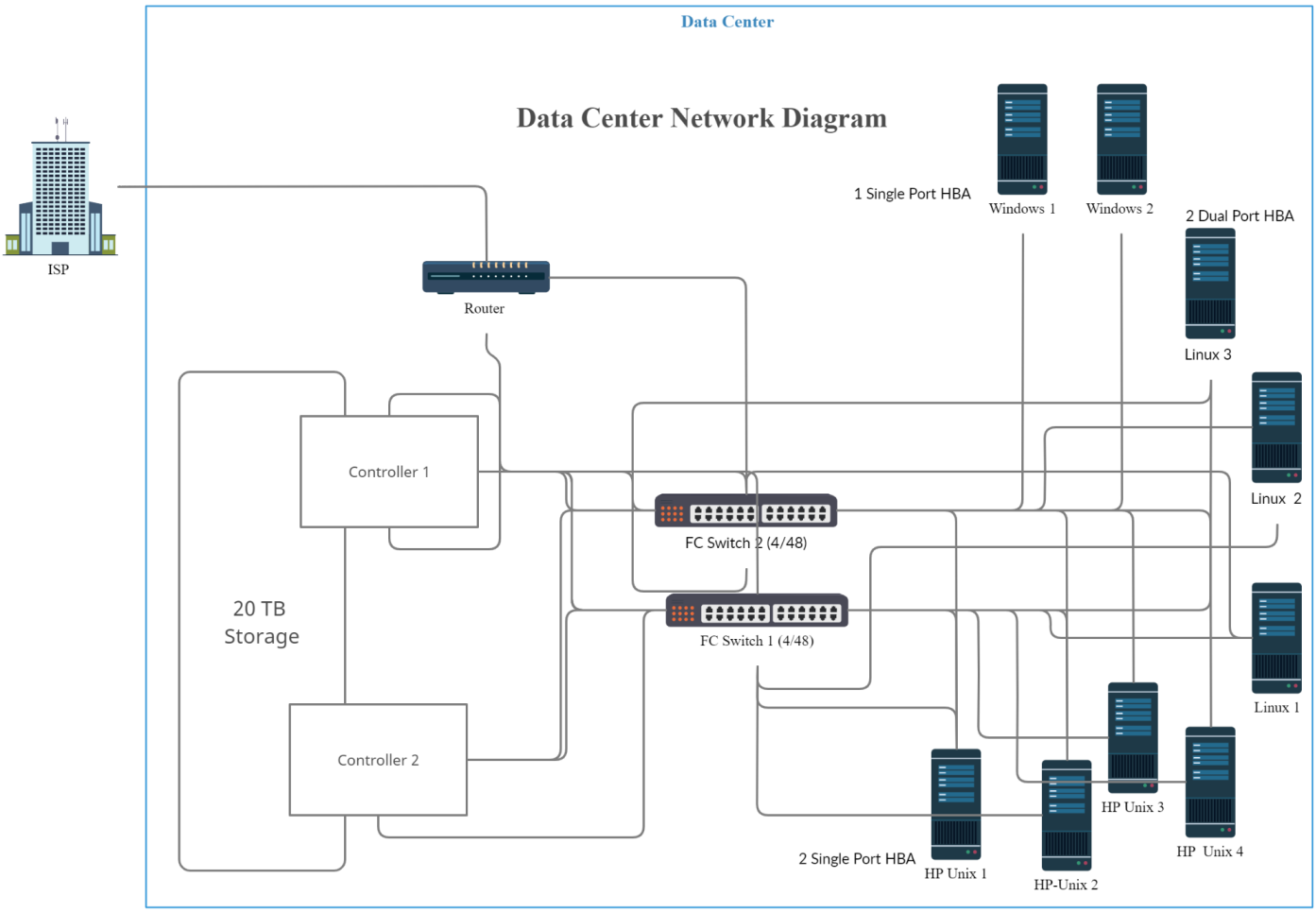
Theory:

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

1. **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.
2. **Bandwidth Aggregation**-allows multiple switch port links to be combined so as to achieve higher throughput between switches (called EtherChannel from Cisco).
3. **Redundancy**-double up the network connections between devices, or you can double the devices themselves.
4. **Convergence** is the process of combining voice and video communications on a data network.



- Made using creately

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.
- Also, we have got hands-on experience of designing a network and have studied the fundamentals of network design and architecture

---