

**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

# Aim:

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

Analyze the location of the core switch , distribution switch and access switch and departmental requirements for connectivity of the computers and also specify the requirements for setting the data center and firewall and IPS, Routing Requirements. Identify active and passive components specifications for the design of the network. Identify the vulnerabilities, attacks and defense mechanisms for the security of an organization's enterprise network. Formulate the organizational guidelines for

network and computing infrastructure usage.

# To 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:

Design Considerations:

1. Location of Core, Distribution, and Access Switches:
   * Place the Core Switch centrally within the campus for optimal connectivity to all parts of the network.
   * Deploy Distribution Switches in strategic locations, one per building or department, to aggregate connections and minimize cable runs.
   * Access Switches should be placed within each department or area to provide connectivity for computers and devices.
2. Departmental Connectivity Requirements:
   * Analyze the specific needs of each department to determine the number of ports required on access switches.
   * Consider future growth and scalability when designing the network to accommodate additional devices.
3. Data Center, Firewall, and IPS:
   * Set up a Data Center with redundant power, cooling, and network connectivity to host servers and critical resources.
   * Place the Firewall at the network perimeter to protect against external threats and configure security policies.
   * Implement an Intrusion Prevention System (IPS) strategically within the network to monitor and detect malicious activities in realtime.
4. Routing Requirements:
   * Utilize a dynamic routing protocol (e.g., OSPF, BGP) to manage routing within the campus network for efficient data traffic.
5. Active and Passive Component Specifications:
   * Specify network equipment including switches, routers, and access points based on capacity and performance requirements.
   * Use high-quality passive components like Cat6 or better cabling infrastructure, patch panels, and cable management solutions for reliable connections.
6. Security Measures:
   * Identify Vulnerabilities: Conduct regular network vulnerability assessments to identify weaknesses.
   * Defense Mechanisms:

Implement network segmentation to isolate critical resources and reduce the attack surface.

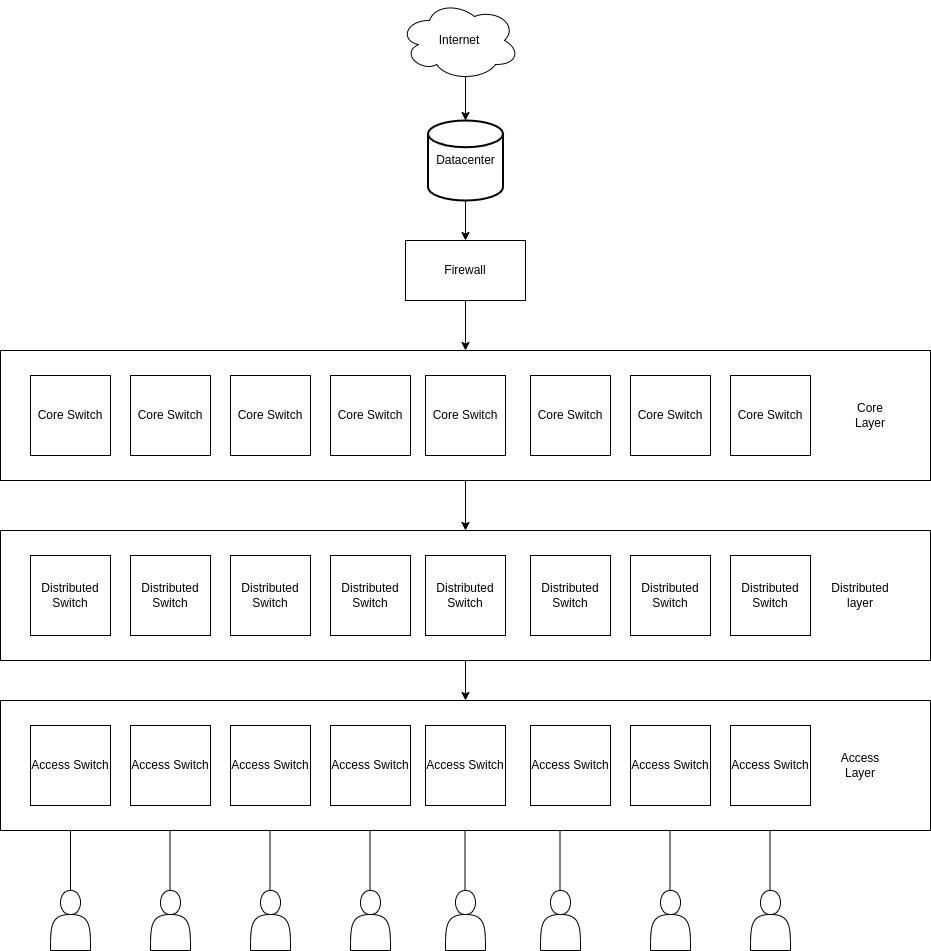
Employ intrusion detection systems (IDS) in addition to IPS for comprehensive threat detection.

Encrypt sensitive data in transit and at rest to protect confidentiality. Regularly update and patch network devices to mitigate known vulnerabilities.

Provide cybersecurity training to staff and students to prevent social engineering attacks.

1. Organizational Guidelines:
   * Develop clear guidelines and policies for network and computing infrastructure usage, covering areas such as acceptable use, data handling, password management, and incident reporting.
   * Educate the campus community about these guidelines and enforce them consistently.
2. Core, Distribution, and Access Switch Placement:
   * Core Switch: Place the core switch in a central location within the campus to ensure efficient connectivity to all parts of the network. It should be highly redundant and capable of handling the entire campus's data traffic.
   * Distribution Switches: Deploy distribution switches strategically throughout the campus, typically one per building or department. These switches aggregate connections from access switches and provide a link to the core switch.
   * Access Switches: Place access switches within each department, classroom, and office to provide connectivity for computers and devices. The number and placement of access switches will depend on the size and layout of each department.
3. Departmental Connectivity Requirements:
   * Analyze the specific needs of each department to determine the number of ports required on access switches.
   * Consider future growth and scalability when designing the network to accommodate additional devices.
4. Data Center, Firewall, and IPS:
   * Data Center: Set up a centralized data center to host servers, storage, and other critical resources. It should be equipped with redundant power, cooling, and network connectivity.
   * Firewall: Place firewalls at the network perimeter to protect against external threats. Implement security policies and rules to control incoming and outgoing traffic.
   * Intrusion Prevention System (IPS): Deploy IPS devices strategically within the network to monitor and detect malicious activities, providing realtime threat protection.
5. Routing Requirements:
   * Implement a dynamic routing protocol (e.g., OSPF, BGP) to manage routing within the campus network and ensure efficient data traffic.
6. Active and Passive Component Specifications:
   * Specify network equipment, including switches, routers, and access points, based on capacity, scalability, and performance requirements. Choose reputable vendors.
   * Passive components include cabling infrastructure (Cat6 or better), patch panels, and cable management solutions to ensure organized and reliable connections.
7. Security Measures:
   * Identify Vulnerabilities: Conduct regular network vulnerability assessments to identify weaknesses in the infrastructure.
   * Defense Mechanisms:
8. Implement network segmentation to isolate critical resources and reduce the attack surface.
9. Use intrusion detection systems (IDS) in addition to IPS for comprehensive threat detection.
10. Encrypt sensitive data in transit and at rest to protect confidentiality.
11. Regularly update and patch network devices to mitigate known vulnerabilities.
12. Train staff and students in cybersecurity best practices to prevent social engineering attacks.
13. Organizational Guidelines:
    * Develop clear guidelines and policies for network and computing infrastructure usage, covering areas such as acceptable use, data handling, password management, and incident reporting.
    * Educate the campus community about these guidelines and enforce them consistently.

Block Diagram:



# Data Center Architecture:

1. Storage Configuration:
   * Redundant Controllers: Redundant controllers in a storage array refer to having two or more controller modules to manage data access and ensure high availability. If one controller fails, the other can seamlessly take over.
   * RAID (Redundant Array of Independent Disks): RAID is a technology that combines multiple hard drives into an array to improve performance, data redundancy, or both. Common RAID levels include RAID 0 (striping for performance), RAID 1 (mirroring for redundancy), and RAID 5/6 (striping with parity for both performance and redundancy).
2. Networking:
   * Redundant Configuration: Redundancy in networking involves setting up duplicate or backup components to ensure uninterrupted connectivity in case of hardware or network failures.
   * Link Aggregation (LACP): LACP is a protocol that allows you to bundle multiple physical network links into a single logical link. This improves network bandwidth and provides redundancy.
   * VLANs (Virtual Local Area Networks): VLANs segment a physical network into multiple isolated virtual networks, improving security and management. In this context, VLANs are used to separate different types of servers for better network organization and security.
3. Server Configuration:
   * HBA (Host Bus Adapter): An HBA is a hardware device that allows servers to connect to a storage network. It is commonly used in storage area networks (SANs). The number of ports on an HBA determines how many connections a server can make to the SAN.
   * Redundancy: Redundancy in server configuration means having multiple network connections, adapters, or components to prevent a single point of failure.
4. Redundant Paths:
   * Multipath I/O (MPIO): MPIO is a technology that allows a server to use multiple physical paths to access storage devices. It enhances redundancy and load balancing, improving both performance and fault tolerance.
5. High Availability:
   * Clustering: Clustering is a technique where multiple servers work together as a single system to provide high availability. If one server fails, another can take over its workload.
   * Failover: Failover is the process of switching to a backup system or component when the primary one fails.
6. Backup and Disaster Recovery:
   * Backups: Regularly creating copies of data to protect against data loss due to various reasons, including hardware failures, data corruption, or accidental deletion.
   * Disaster Recovery: Planning and procedures to recover data and IT infrastructure in the event of a disaster, such as fires, floods, or major hardware failures.
7. Monitoring and Management:
   * Centralized Monitoring: The use of a centralized system or software to monitor the health and performance of various components in the data center, including storage, servers, and networking equipment.
   * Alerting and Reporting: Setting up notifications and reports to proactively identify and address issues in the data center.
8. Security:
   * Firewall: A security device or software that controls incoming and outgoing network traffic, allowing or blocking data based on a set of security rules.
   * Security Policies: Guidelines and rules that define how systems and networks should be secured. They can include access controls, encryption, and authentication methods.
   * Patch Management: Regularly applying software updates (patches) to fix security vulnerabilities and improve system stability.
9. Documentation:
   * Configuration Documentation: Detailed records of how various components are configured, including IP addresses, network settings, and hardware configurations.
   * Network Diagrams: Visual representations of the data center's network topology, including connections between servers, switches, and storage.
   * Procedures: Step-by-step instructions for performing maintenance tasks, disaster recovery, and troubleshooting.

To design a high-redundancy data center architecture for your 20 TB storage array and the servers with various HBAs,we can follow these steps:

1. Storage Configuration:
   * Configure your 20 TB storage array with redundant controllers and use RAID technology (e.g., RAID 1, RAID 5, or RAID 6) to ensure data integrity and high availability.
   * Utilize all 4 FC ports on each controller for redundancy and performance. Configure these ports in failover mode.
2. Network Design:
   * Utilize the 2x 48-port switches for network connectivity. To ensure redundancy, connect each device (storage array, servers) to both switches.
3. Server Configuration:
   * For HP-Unix Servers (4 servers):
   * Each server has 2 single-port HBAs. Connect one port to each switch, ensuring redundancy.
   * For Linux Servers (3 servers):
   * Each server has 2 dual-port HBAs. Connect one port from each HBA to each switch for redundancy.
   * For Windows Servers (2 servers):
   * Each server has 1 single-port HBA. Connect each port to both switches for redundancy.
4. Redundant Paths:
   * Enable Multipath I/O (MPIO) on all servers to ensure data can take multiple paths. This enhances redundancy and load balancing between the storage array and servers.
5. High Availability:
   * Implement server clustering for your critical applications or services, such as Windows Failover Clustering for the Windows servers and a suitable clustering solution for Linux. This allows for automatic failover if one server becomes unavailable.
6. Backup and Disaster Recovery:
   * Implement regular backups of critical data to the storage array. Additionally, set up a backup solution to offsite storage for disaster recovery.
7. Monitoring and Management:
   * Utilize centralized monitoring tools to keep track of the health and performance of all components, including storage, switches, and servers. Configure alerting and reporting for proactive issue resolution.
8. Security:
   * Implement firewall and security policies to restrict access to your data center. Ensure that only authorized personnel can access sensitive areas and systems.
   * Regularly update and patch all systems and networking equipment to address security vulnerabilities and maintain the highest level of security.

Data-center Architecture:

