ACN ASSIGNMENT – 1

College LAN network design

(Iteration 3)

Vijayraj Shanmugaraj

20171026

Objective

The purpose of this assignment is to design the IIIT-Hyderabad Campus Network and provide a IP addressing scheme for the same.

Basic Network Requirement:

The aim is to provide a network that is:

- Having a topology that satisfies the need of IIIT-Hyderabad Campus
- Using the latest technology and future proofing
    - Scalable – so that future requirements can be met with graceful addition/minimal reconfiguration of existing network
    - Future technologies can be incorporated without disturbing the existing network.
    - Provide cabling and connecting equipment as per the Structured Cabling System based on ANSI/TIA-568-C.0 (Generic Telecommunication Cabling for Customer Premises) and ANSI/TIA-568.C.1(Commercial Building Telecommunications Cabling Standard) – so that the cabling and connectivity is future proof.
- Having good bandwidth, to service the various requirements of different user groups within the campus
- Having a high availability
- Secure
- Easy to troubleshoot
    - Selecting an architecture that supports easy troubleshooting
    - Provide inbuilt monitoring support in the design.
- Cost Effective
    - Avoid very high cost equipment – which may be technologically superior but not required to satisfy the network requirements of the design being done.
    - Minimalistic design – but scalable with enough free capacity.

Assumptions

1. The layout of IIIT-Hyderabad campus was studied. The following points were notes:
    a. The area of the campus is manageable using a Local Area Network (LAN) and Wide Area Network (WAN) is not required. Hence, the design will consider the LAN technology and ISP provided Internet connectivity – using secure connectivity.
    b. There are not many remote areas in the campus – hence, microwave or other type of radio-based connectivity is not considered. However, Wi-fi connectivity will be provided through Access points (AP) at various facilities.
    c. The complete campus will be provided with intranet access, and to provide this the network will be extended through Optical cabling.
2. The campus requirements will be broadly classified into following groups:
    a. Casual users in various facilities in all facilities, who will get Internet access and restricted Intranet access through Wi-fi
    b. Hostels where the intranet will be used extensively, and Internet will be provided through Wi-fi and Wired network as per the requirement.
    c. Academic and Research facilities
    d. Administrative and Financial department

3. The network diagram provided will indicate the various network equipment and may not include a detailed layout of the equipment – However, general guidelines will be provided for cabling and layout of network equipment.
4. No study of existing network or server count has been done, but the various servers and computer counts shown are tentative and representative.
5. The tentative user count is based on the following assumptions:
    a. Student count – 2500
    b. Academic staff count – 125
    c. Support Staff count – 250
6. No bandwidth requirement (Internet and Intranet) are calculated. But the relative bandwidth ratios are maintained between various levels and connections.
7. It is assumed that all the civil facilities in the campus are designed with separate secure area for hosting network connection and equipment and have enough cabling trays for routing the network cables – that are distinct from power cables.

Network Design Goals

The requirements specified in the network requirements section, translate into the following design goals

- Availability: The first requirement of a Campus network is high availability. Unlike other enterprise networks, campus networks are used 24x7. Hence, the campus network should be designed for consistent, reliable performance for 24x7 use. Also, failure of a single link or a piece of equipment should no significantly degrade the performance of the network.
- Scalable and Future Proof: The network should be able to gracefully grow to include new user groups, new facilities, new application without impacting the Quality of Service (QoS) being delivered to the existing users.
- Security: As IIIT-Hyderabad Campus is a Academic cum Research facility, its data servers hosts information which has huge Intellectual Property (IP) value. Hence, the segmentation and security of the network design is very important.
- Manageability: Management and Troubleshooting of the installed network is an important requirement. Hence, the network monitoring features should be in-built in the network design. Also, the topology should allow easy troubleshooting without affecting the availability of the network.
- Cost Effectiveness: Though cost calculations are not part of this design, every design should be cost effective, as budget is scarce in a Campus scenario.

Network Design

The design follows a top-down approach (i.e.) first topology is decided, then the architecture is decided and based on the architecture the network components are selected.

When we go through the various LAN topologies, the following stand out:

- Bus Topology
- Ring Topology
- Star Topology
- Tree Topology
- Mesh Topology

The bus and ring topologies are outdated.

Mesh topology is not required for campus networks as it is not a cost-effective solution and is not easy to troubleshoot. But partial mesh topology can be created at higher-tiers of the tree topology.

If we scan the latest technologies, most of the LANs are designed with Switched Ethernet due to the availability of fast ASIC based Layer2 switches and related cabling hardware.

This Switched Ethernet based LAN technology has the following advantages:

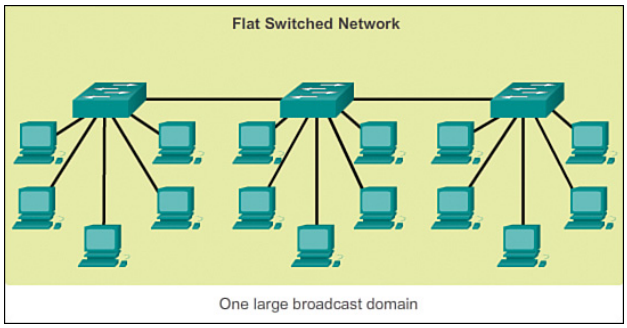
1. As far as the cable and connectivity hardware is concerned, it is future proof. It uses the UTP Cat 5 cables and standard connectivity hardware as per structured cable standards.
2. It is a Tree Topologies (with partial mesh at upper-tiers to improve availability) – which has the following topological advantages:
    a. Easy to setup and modify
    b. Easy to troubleshoot – as failure of one node or one segment does not affect the working of other segments of the network
    c. Provides definite hierarchy in the network – Hence, in future when the technology changes or the bandwidth requirement increases then the higher levels can be altered without affecting the lower levels. Hence, it is highly scalable and future proof.
    d. Multiple links (partial mesh) can be provided and hence the availability of the resulting network will be high.
    e. Troubleshooting and monitoring are in-built into the network hardware.
3. Though the initial cost of cabling and hardware is high, due to the long life of the architecture the Return on Investment (ROI)[##] will be high.

By definition, ROI is a performance measure used to evaluate the efficiency of an investment or compare the efficiency of a number of different investments. It is true that the college is not a business that uses its network to make profit. In a case of a tech-driven college like ours, students, teachers and administrators may rely heavily on network uptime for the success of the classroom initiatives. So if we translate 24 x 7 uptime as zero downtime – then we need to log all the downtime. If we assign a dollar value to each hour of downtime – as it is affecting the productivity of staff, students and support staff, then we will be able to monitor the loss in dollars. Saving money by making the network less dependent on network admin staff and making it future proof (avoiding future investment) also translates to an increase in ROI.

High Level Architecture

The Switched Ethernet based LAN design supports many architectures. The following is based on literature of one of the major suppliers of network solutions – CISCO:

Flat Switched Network



- Switches are added as more devices need to connect
- Provides little opportunity to control broadcasts or filter undesirable traffic
- As more devices and applications are added, response times degrade, making the network unusable.
- As we need a scalable, future-proof network this is not a good architecture.

Three-Tier Architecture

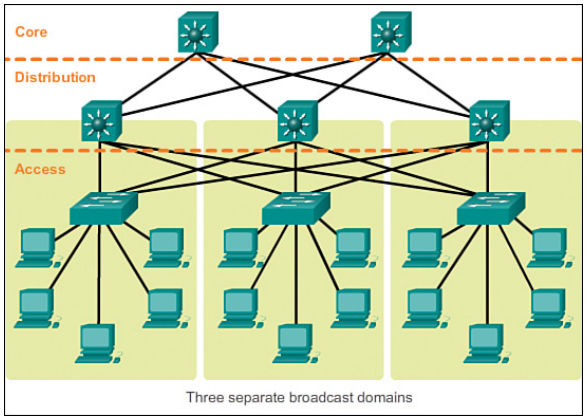
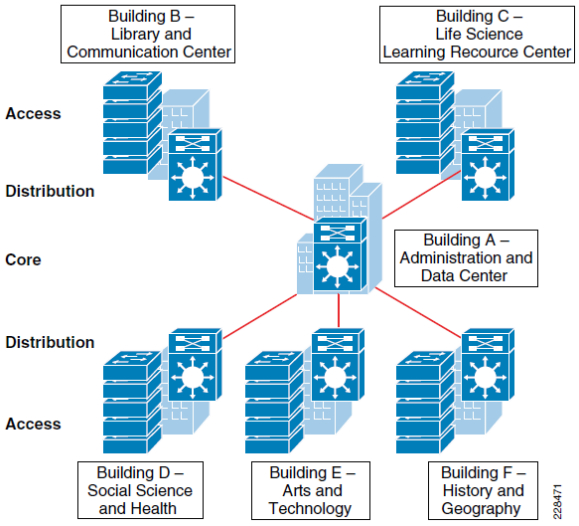


Figure 4 Three-Tier LAN Network Design Example



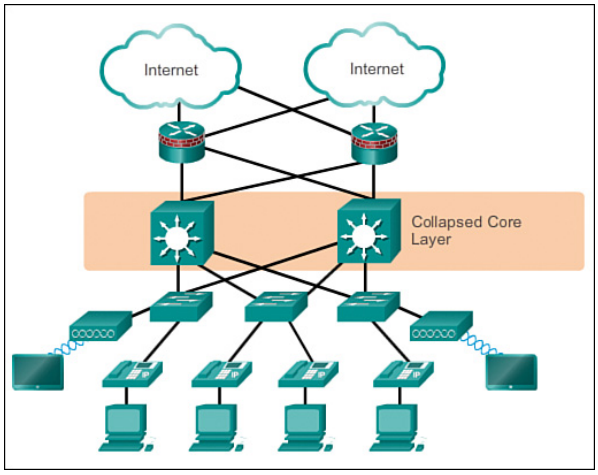
A hierarchical network design involves dividing the network into discrete layers. Each layer or tier, in the hierarchy provides specific functions that define its role within the overall network. In each block the local traffic remains local. Only traffic that is destined for other networks is moved to a higher layer.

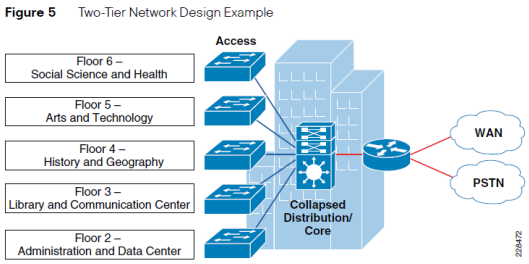
A typical enterprise hierarchical LAN campus network design includes the following three layers:

- Access Layer – Represents network edge, where traffic enters or exits the network. All the hosts (desktop, laptop, phones etc.,) are connected here. The Wi-fi Access points are also connected to this layer.
- Distribution Layer – Provides policy-based connectivity and controls the boundary between the access and core layers. Generally, this is a boundary between Layer-2 switching and Layer-3 switching.
- Core Layer – Provides fast transport between distribution switches within the campus. This acts as the backbone of the network. This also provides connectivity to the external network through router and firewall combination.

Two-Tier Architecture (or) Collapsed Core Architecture

When the network growth is not significantly larger or if the main components of the network are concentrated in a single large building or within a set of buildings that are close to each other, then the core and distributed layers can be collapsed and kept inside the Equipment room of a single building instead of distributing it across the campus. This reduces the network cost, while maintaining most of the benefits of the three-tier hierarchical model.





Final decision on Hierarchical Architecture

From the above discussion it is clear that if we are designing a network for only the Himalaya and Vindhya building cluster, then the Collapsed-Core architecture would have been the right choice. But the network involves other distributed areas like hostels, Nilgiri building area etc., Three tier architecture with network segmentation at Distribution layer is a good choice. The distribution tier will help us in easy segmentation of the network.

The physical distribution of the "Distribution Tier" switches is an important decision. There are two choices:

- We can have Distribution Tier switches along with access layer switches in large network segments
- We can have Distribution Tier switches along with core switches in a centralized, climate controller facility.

The option of keeping **Distribution Tier switches along with core switches** is a good decision as:

- It helps in maintenance and troubleshooting
- As these switches are high throughput switches, they are better to be in a climate-controlled environment
- If there is a technological change and the Distribution and Core tier is modified, it is easier to do if they are present in a centralized location.
- Only disadvantage will be that optical cables need to run from the access level switches to the distribution tier switches.

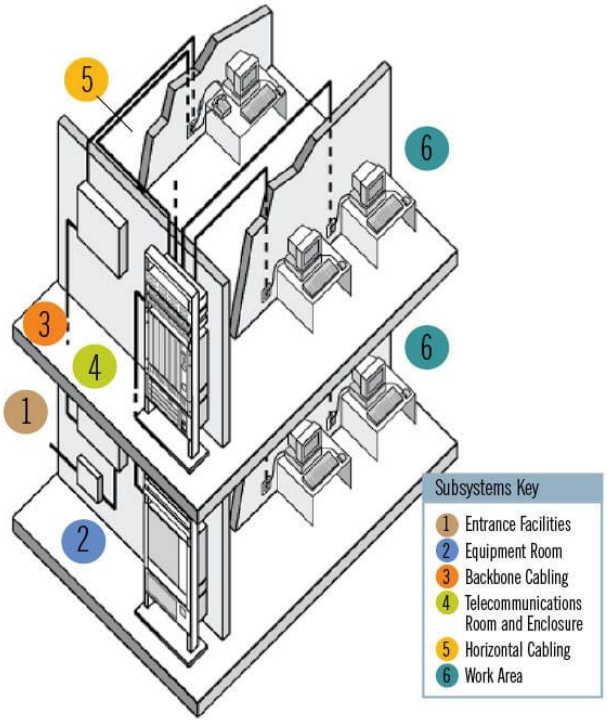
As we have finalized the architecture the next step is cabling guidelines and selection of components.

Cabling Guidelines:

As mentioned before the cabling has to be performed as per the Structured cabling system (SCS)

Need for Structural Cabling:

- Consistency: A structured cabling system can use the same cabling system for everything. Standardizes systems for phone, Ethernet, and ISDN cabling in order to simplify troubleshooting issues and streamline future cabling updates.
- Long Life: Supports multivendor equipment. So it is future proof.
- Simple to Modify: Moving of equipment like desktop, printer etc., across rooms or if the complete layout is modified it is easy to reconfigure the system.
- Simplify troubleshooting: Problems are easily traceable and more straight forward to fix.
- Support for future applications: It will support future applications like multimedia, video conferencing etc., with little or no upgrade pain.



As per the TIA-568 standard there are six sub-systems:

- **Entrance Facility:** Point at which the telephone company network ends and connects with the on-premises wiring belonging to our network. For the campus, the entrance facility shall be in the building where the Core Tier Equipment, Routers and Firewalls are placed.
- **Equipment Rooms:** house equipment and wiring consolidation points that serve the users inside the building or campus.
- **Backbone cabling:** is the inter-building and intra-building cable connections in structured cabling between entrance facilities, equipment rooms and telecommunication closets. Backbone cabling consists of the transmission media, main

and intermediate cross-connects and terminations at these locations. This system is mostly used in data centers.

- **Horizontal cabling:** wiring can be standard inside wiring (IW) or plenum cabling and connects telecommunications rooms to individual outlets or work areas on the floor, usually through the wireways, conduits or ceiling spaces of each floor. A horizontal cross-connect is where the horizontal cabling connects to a patch panel or punch up block, which is connected by backbone cabling to the main distribution facility.
    - Cabling between Work Area's telecommunication's information outlet to telecommunication room (TR) or (TE)
    - Uses Multiuser telecommunications outlet assemblies (MUTOAs) and consolidation points (CP).
    - Maximum horizontal cable length shall be 90m – independent of media type.
    - If MUTOAs are used the twisted pair cable length shall be reduced.
- Telecommunications room or telecommunications enclosure connects between the backbone cable and horizontal cabling.
- Work Area (WA): components connect end-user equipment to outlets of the horizontal cabling system.
    - A minimum of two telecommunications outlet (permanent links) should be provided for each work area
    - Multiuser telecommunications outlet assemblies (MUTOAs) if used, are part of WA
    - The maximum cable length between outlet and the WA equipment in 3m.

Cables Used:

Unshielded Twisted Pair (UTP) cables are used for Horizontal cabling between the switch ports and the MUTOAs. The maximum length can be 90m.

Optical Cables

There are three types of optical Cables:

1. Multi-Mode optical cables
    a. Graded Index
    b. Step Index
2. Single Mode Optical Cables

Single mode optical cables are used when the transmission distance is high. These cables are costly. We need to use laser sources.

In Multimode cabling system, when LEDs are used as sources then multiple modes of the cable can be used for transmission. These cables are used for short distance transmission. These cables are cheaper and the LED sources are also cheaper than the Laser sources.

As in the IIIT-Hyderabad campus, the distance between various locations are not more than 2 km, the **multimode cables can be used**.

There are various connector types available on the optical connectors available on network equipment. This can be standardized or patch-chords of right type need to be used.

Component Selection

Here the components are selected from CISCO range of network equipment. The selection criteria mentioned here can be used to select products of other vendors also:

Access Switches:

Criteria for selection:

- Centrally manageable – updating of OS, configuration etc.,
- 802.1X port-based network access control – for high scalability and dynamic role-based access control.
- Stacking options should be available.
- Less power consumption and hibernation mode
- Optical Uplink port support

So, for Access switches I have selected CISCOs 2960 Series – WS-C2960X-48LPD (48 port switch) and these switches can be stacked (or) WS-C2960XR-24PD (24 port) can be used for consolidated the 48 port switches in a particular building. SFPs are added to the top-level access switch from which the optical cables should be run to the Distribution level switches.

Distribution Tier Switches:

These switches act as aggregators of access switches connected to them. These Distribution Tier switches can be selected as per the size of the access network connected to them directly.

- Layer2 and Layer 3 Capability (Switching and Routing support)
- High switching bandwidth
- High Mac address table size
- 1 Gbps and 10 Gbps optical ports

Cisco Catalyst 3850 Series or Catalyst 4500 Series will suit the requirements of the Distribution-tier. Here 4500 series is selected.

Core Switches:

These switches are similar to Distribution-tier switches but with a higher capacity. The main requirement at this level is high availability and redundancy support.

Cisco Catalyst 6500 Series is a good choice – as it supports redundancy using the VSL link. This makes the two switches to act as a single virtual switch. ‘

Router:

As the internet connectivity is an integral part of campus network and everyone need internet for day to day working and for various research functions, a good gateway router is a basic requirement. To this router the ISP is connected through Point-to-Point connectivity.

- Redundant power-supplies (AC or DC)
- Pay as you go performance
- Modular design with optional modules
- Extendable I/O
- Support for DMZ Layer

The CISCO ASR 1002-HX Router is selected, as a high-performing edge solution for an ISP provided internet access.

Firewall:

The latest technology in firewalls is Next-Generation Firewalls (NGFWs), that incorporate:

- Policy enforcement for applications and user control
- Intrusion prevention
- Deep packet inspection
- Sandboxing
- Threat intelligence feeds

A firewall from one of the top vendors, such as *Fortinet*, *Barracuda*, *Juniper* or *Check Point* can be selected for our design. If single vendor product is to be selected then CISCO's Firepower which offers or integrates the following features:

Intrusion prevention, advanced malware protection, cloud-based sandboxing, URL filtering, endpoint protection, web gateway, email security, network traffic analysis, network access control.

Wireless Access Points:

Wireless access points are meant for providing wi-fi to large number of users. I have selected CISCO APs – which can handle 400 users and maximum bandwidth of 5Gbps. Some models of 2960 series switches provide power supply for APs.

Network Architecture Diagram

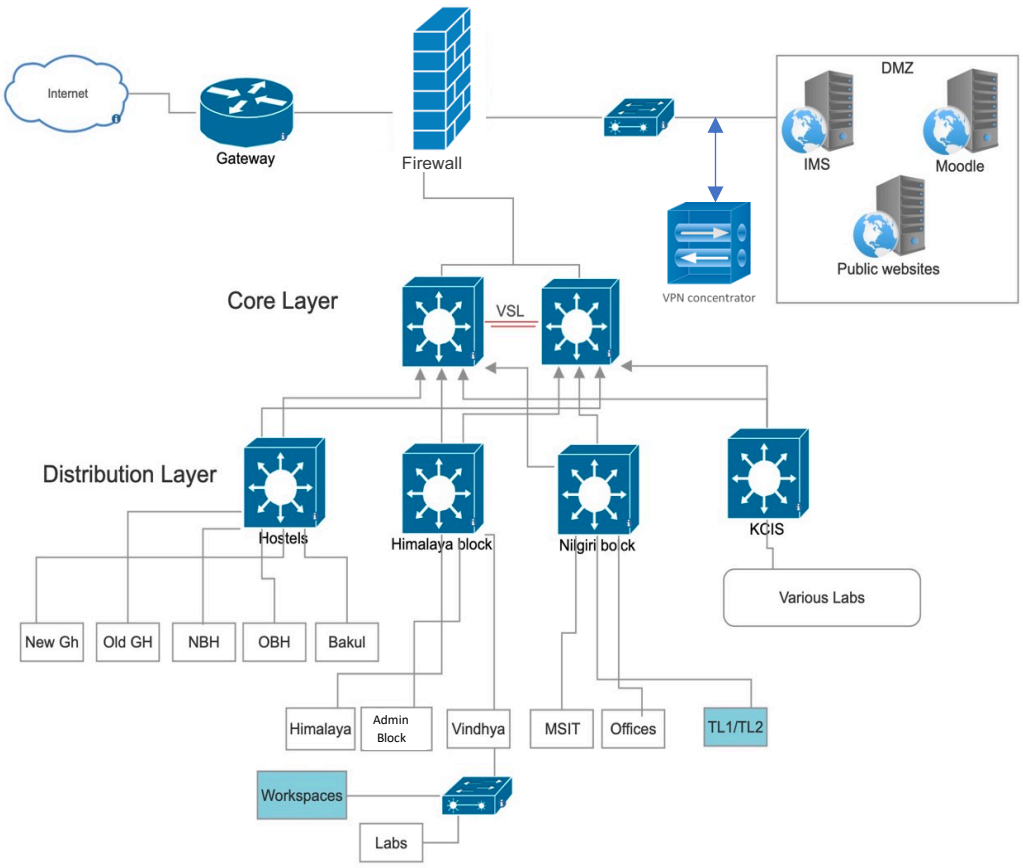


Figure 1: Overall Network

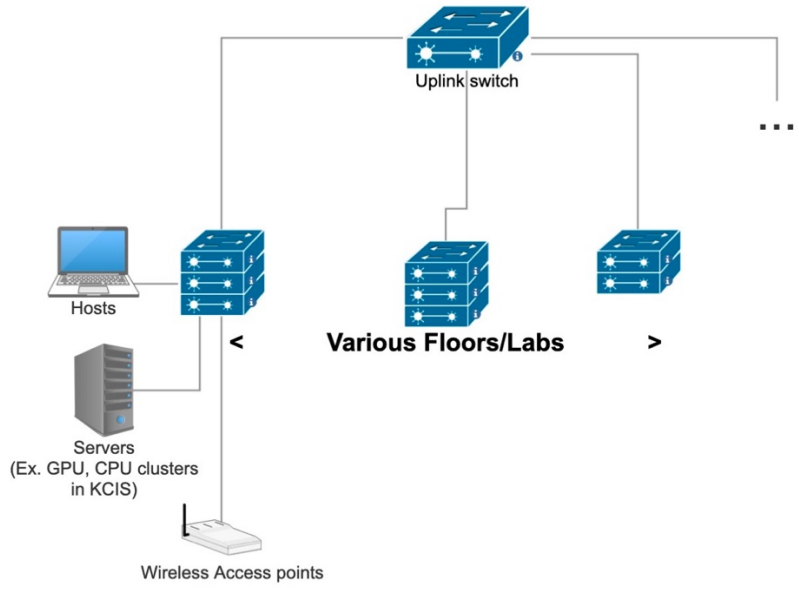
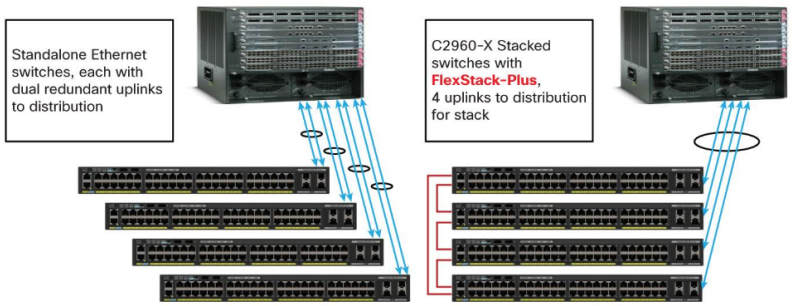


Figure 2: Network design in a building

Implementation of the 3-Tier Architecture

1. There are many network intensive facilities inside IIIT-Hyderabad. These include Hostels where there are 120 ports per floor and 5 floors in the building, Workspaces, Library, and research laboratories and offices.
    a. Hence in each building the access switches are 48-port Cisco Catalyst 2960 switches are selected. These switches provide backplane stacking facility, which allows the nearby switches inside the same rack can be connected to each other using stacking cable. These switches are mounted in a network rack or a cabinet and kept under lock and key to avoid any physical intrusion.
    b. The switches in each floor have been stacked, providing the network administrator with the following benefits:
        i. Single point of management:
        All switches in the stack are managed as one
        ii. Built-in redundancy and high availability:
        The connections between switches provide redundant communication for each stack member to the other
        iii. Scalability to fit network needs:
        If the need for additional access ports grows, adding a new switch to the existing stack is easier and faster than adding a new standalone switch to the network.

Figure 1. Comparison of FlexStack and Nonstacked Configurations



    c. The stacked switches are connected to a Link switch, which is a 24 port switch from Cisco Catalyst 2960 family. This switch is provided so that only **two pairs of optical cables are extended from a building to the distribution switch** which is kept in the controlled environment in a centralized facility in the research area.

2. The distribution switches are not kept in individual buildings due the following reasons:
    a. The network connection and load needed for various buildings are does not warrant a separate distribution tier switch
    b. More than one building can be combined into a single distribution tier switch. If the related servers and the research labs are connected on the same distribution switch, then all the traffic between server and clients can be restricted within the distribution switch and need not be sent up to the core level switch.

c. Also, the troubleshooting, maintenance and upkeep of the distribution tier can be done from a single room which is climate controlled.
d. The Optical cable uplinks from various buildings are connected to the SFP port (Small form factor fiber port) of the distribution switch.
e. For the distribution switch, Cisco's catalyst 4500 family switches are used. While selecting the switch, the Layer 2 and Layer 3 capabilities are considered. Also, the MAC table size is also kept in mind. This series of switches have a MAC table size of 55K entries.

3. The distribution switches are connected to two numbers of Cisco Catalyst 6500 series Core switches using SFP links. Both these switches are connected using a VSL link, so that these switches work as one. These switches act as backbone for the network. These switches have a MAC table size of 128 K entries.
4. The Core switch is connected to a Firewall and a Router so that the entire LAN can be connected to Internet.
    a. The firewall provides the DMZ edge, in which the servers like Moodle, IMS etc., are place which need access from the internet. One 2960 switch is provided to connect all these servers.

IP addressing scheme and VLAN design

The assumption that is being made is that the entire campus is run on IPv4.
The 10.0.0.0 network is being subnetted and used for the internal network. The assumption is that the PAT is set up for the college for internet access. In this network, subnetting is done mainly to reduce traffic due to broadcast messages. Additionally, any internet-related restrictions also can be effected with this subnetting.

The purpose of VLANs (Done using IP addresses and port switches in certain cases) in addition to subnetting is to divide the LAN logically to implement various policies related to security, privacy and internet access. As a rule, the DMZ is provided a separate VLAN. For example, if we can group all ports of 1st year students in the hostels, we can provide a separate VLAN, to provide them intranet access, but deny internet access. Since definite rooms are allocated for first years, other students and staff, VLANs here can be set up based on the ports in the L2 switches in the interior of the hostel buildings. Workspaces and labs can be put in a separate VLAN to avoid cheating during lab examinations. IP addresses cannot be set manually by individuals on their system. Inter-VLAN routing can be set up wherever required in the distribution layer, as these are L3 switches. In addition to all these measures, security will also be implemented through login and authentication.

10.1.0.0/20 - Bakul
(VLAN 10 for first years, VLAN 20 for other students, VLAN 30 for staff)
10.1.16.0/20 – OBH
(VLAN 20 for students, VLAN 30 for staff)
10.1.32.0/20 – NBH
(VLAN 20 for students, VLAN 30 for staff)
10.1.48.0/20 - Old GH
(VLAN 40 for students, VLAN 30 for staff)
10.1.64.0/20 - New GH
(VLAN 40 for students, VLAN 30 for staff)

10.2.0.0/16 – Himalaya (VLAN 50)

10.3.0.0/16 - Admin block (VLAN 30)
10.4.0.0/16 – Vindhya (VLAN 50 for common area, separate VLANs for each lab)
Workspaces: 10.4.0.0/24, 10.4.1.0/24, 10.4.2.0/24 * (VLAN 60)

10.5.0.0/16 – Nilgiri
(VLAN 50 for common area, separate VLANs for each lab, VLAN 30 for staff)
Labs: 10.5.0.0/24, 10.5.1.0/24* (VLAN 60)

10.6.0.0/16 – KCIS (separate VLANs for each lab)

192.168.0.0/24 - DMZ** (VLAN 100)
10.7.0.0/16 – Network devices$ (VLAN 1)

The only public addresses subnet of the Institute is present at the gateway router that connects the institute's internal network to the outer network.

(Giving 4000-odd addresses per hostel, for easy expansion or in the case of introducing wireless access points in hostels)

^ More addresses have been given to Himalaya expecting the varying number of visitors, who mainly involve themselves in events, usually happening in Himalaya block

* The labs and worskspaces have been given certain dedicated subnets within their building-based subnet since they hold more than 50 people at a time. Lab examinations are conducted in these rooms, and setting a separate subnet for these rooms will make it easier for monitoring

** DMZs have sensitive servers, and hence deviating from the normal IP address pattern may avoid attackers from guessing the IP address of these servers from the IP addresses of the LAN

$A separate subnet has been allocated for all networking devices so that it can be easily managed from a centralized location and they have been put in the default VLAN for the same purpose.

Network Security (Firewall & VPN)

As there are no remote sites we have not considered site to site connectivity using VPN. But considering mobile and remote users, who want to connect externally through Internet – VPN can be used.

We have added the Next General Firewall (NGFW) as an Intrusion Protection System. Using this firewall we have created the DMZ (Demilitarized Zone) where the servers which needs to be accessed through the Internet are placed. Also, the VPN concentrator is placed in the DMZ, which the best configuration as far as security is concerned.