Information Security Audit and Assurance

Secure LAN design IIIT-H Campus

(Revised)

Team members

Member Name	Roll No.
Nitin Kumar	2021202020
Sudipta Halder	2021202011
Karan Negi	2021201039

OBJECTIVE:

- To design a Secure Network for IIIT Hyderabad.
- Design bare minimum infrastructure.
- The system should be scalable.
- The budget is limited and hence high tech technologies cannot be deployed.
- Biometric and other security devices should be connected to the network also.

REVISION:

- Added Central Synchroniser, which manages all the software/firmware updates of all the devices to make sure every device's software and firmware is not manually updated and all are in synchronization.
- Has been noted that during heavy load the router abruptly restarts and hence becomes unavailable for some time, we wanted to solve this issue as well, we realized that the bottleneck was the processor used in the router could not handle too much request and was causing the issue, only solution was to have a backup router(which was connected to Lan port of original router, from our experience we have noticed that the lan port was able to provide service even if the wifi goes down for few moments) . or we can buy a router with higher processing power.

- We forgot to make a committee that will. The committee should develop network rules and policies that are clear, concise, and easy to understand. These rules should be communicated to all members of the college community.
- Network failure response team: The role of a network failure response team is to quickly respond to and resolve network failures in an organization. The team is responsible for identifying the cause of the failure, isolating the affected systems, and restoring service as quickly as possible.
- The Network Engineering Team is in charge of creating, executing, and maintaining the campus network infrastructure. Their main duty is to make certain that the network is dependable, secure, and can be expanded as needed.
- The Network Operations Team is responsible for overseeing and maintaining the network on a daily basis. They are accountable for ensuring that the network is accessible and performing at its best.
- The Help Desk Team is responsible for providing technical assistance to end-users who are experiencing network-related problems. They are accountable for identifying and resolving issues related to network connectivity, access, and performance.
- The Security Team is responsible for ensuring the security of the campus network. They are accountable for implementing and maintaining security measures such as firewalls, intrusion detection and prevention systems, and access controls.
- The Application Support Team is responsible for supporting the various applications and services that run on the campus network. They are accountable for ensuring that these applications are available and performing optimally.

Note: the changes are minute and hence not visible in the figure that we have drawn, because the figure is mostly high level design.

ASSUMPTION:

- The main objective of IIIT Hyderabad is academic excellence, hence the network design mainly revolves around fulfilling this requirement.
- The Number of Network users is around 3000, and not everyone will need Internet service at the same time.

INFRASTRUCTURE OVERVIEW:

We have to provide internet access to following places:

- We have one Admin Block where all the administrative work is done.
- We have quite a few classrooms and some teaching labs.

- We also have several dedicated laboratories for various departments along with faculty/Staff cabins. They also contain Servers of respective departments.
- There are 3 Hostel (Two of which are boys hostel and one girl hostel).
- There is one Faculty and one PhD residence area.
- We have Security Blocks\Desks and Security Devices (CCTV, Biometric Devices, etc) Which have to be connected to the Network.
- Rest of the infrastructure includes Canteens, Music Room bb-instant, Medical room (aarogya), Sports room, Yoga room, Guest House, Amphitheater, Workspace, T-Hub, etc.

DEVICES/TECHNOLOGIES USED:

- Cables (From ISP to Multi-WAN Routers): Fiber optic cables.
- Cables (From Multi-WAN Routers to Switches): Copper cables.
- Cables (From Switches to Hosts): Twisted Pair cables.
- CCTV: Honeywell Performance Series IP Camera
- Biometric Device: Mantra MFS100
- Wifi Device: Cisco Aironet 3800 Series
- FireWall: Cisco Adaptive Security Appliance (ASA)
- Router: Cisco ISR 4000 Series
- IDS/IPS: Snort
- L3 Switches: Cisco Catalyst 3650 series
- L2 Switches: Cisco Catalyst 2960-X series
- Sensors: Thermal Sensors
- Log tool: Syslog-ng
- DNS Server: BIND (Berkeley Internet Name Domain)
- Reverse Proxy: NGINX

All Images GDrive Link:

https://drive.google.com/drive/folders/1ZhDpXdaKlf_i3O_2rCQWWwc5AhoXMYnd?usp=sharing

NETWORK DESIGN EXPLANATION:

Central Routing System:

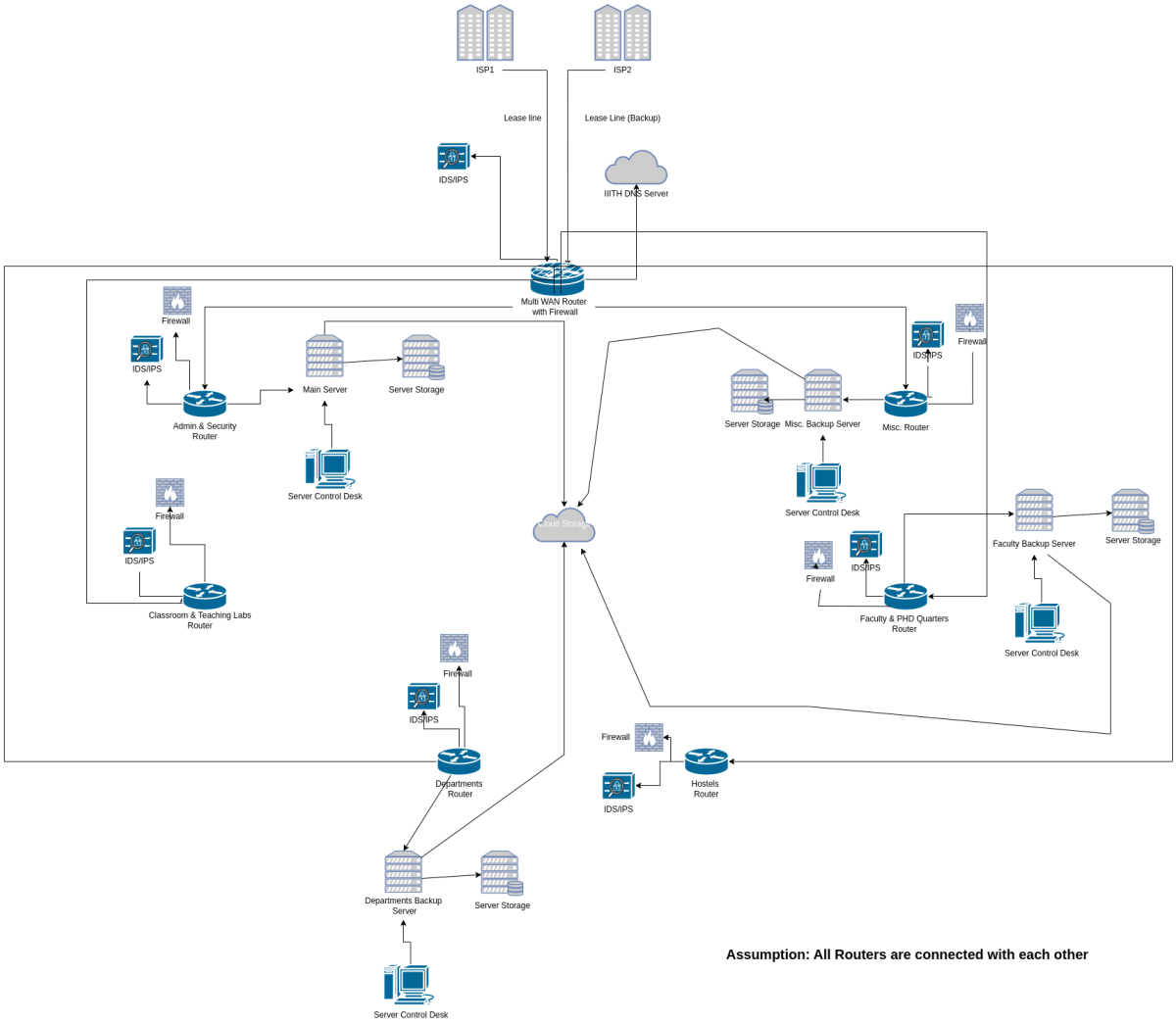

Figure 1) Central Routing System

Leased-Line Connection:

The internet is provided to IIIT Hyderabad from ISP through a leased line connection. A few reliable ISPs that provide Leased Line connections in India are Airtel, Reliance Jio, Tata Communications, Spectranet, ACT Fibernet, BSNL, You Broadband.

We will prefer BSNL's Leased Line Connection for this because of its High-speed connectivity, Symmetric Bandwidth, Scalability, Cost-effective ,Network Up Time and Customer Support for 24x7.

The reason for using Leased line connection from ISP is that it provides a dedicated communication line that is high-speed, reliable, scalable and secure. The bandwidth is not shared with external users also, security can be provided via encryption.

We will be having connection from two ISPs, both of which will provide internet via Leased Line, ISP1 will be used as a primary provider for Internet service and ISP2 will only be used when ISP1 is down. The Network speed we need from ISP1 for our network will be around 1GBps.

For ISP2 the pricing will be usage-based. And charges for ISP1 will be based on the amount of bandwidth required. The purpose of ISP2 is to provide internet connection when ISP1 is down to ensure availability.

Router:

This Multi-WAN Router is connected to 6 routers.

Router 1) Connected between Multi-WAN Router and Admin Block\Security Block.

Router 2) Connected for all the classrooms and teaching labs (connection source being Multi-WAN Router).

Router 3) Connection for all Departments (connection source being Multi-WAN Router).

Router 4) Connection for all Hostels (connection source being Multi-WAN Router).

Router 5) Connection for all Faculty and PhD Quarters (connection source being Multi-WAN Router).

Router 6) Connection for all the remaining buildings like library, canteens, bb-instant, music room, aarogya, amphitheater (connection source being Multi-WAN Router), Workspace , T-hub.

All these routers have to be connected in a mesh topology in order to provide fault tolerance so that if one router goes down another can take its place. Apart from this

everywhere else we follow star topology. Making the entire topology as hybrid topology.

All these routers have the capability of IDS/IPS to prevent attack from inside the network as well. All these routers are kept under surveillance of CCTV cameras and are locked where not everyone can go. Router 1 and 3 have the highest security and a lot more power backup has been allocated to them as compared to Router 2, 4, 5 and 6.

The Router that we have used for this purpose is **Cisco ISR 4000 Series** router.

The estimated number of hosts required per router are (based on their requirements) **:**

Router 1) 512 hosts, **Router 2)** 1024 hosts, **Router 3)** 2048 hosts,

Router 4) 4096 hosts, **Router 5)** 2048 hosts, **Router 6)** 2048 hosts.

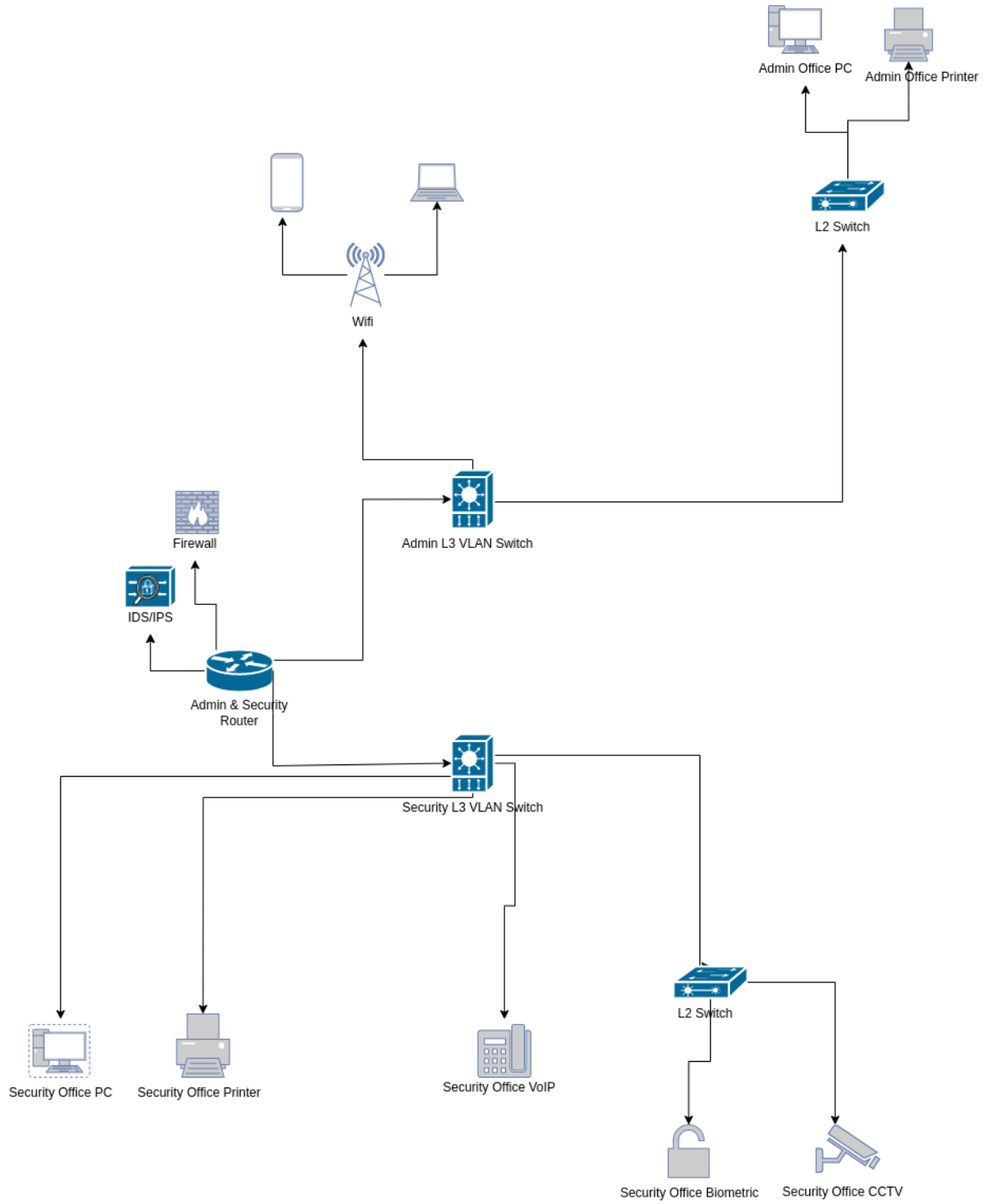

Figure 2) Router 1: Admin & Security Block

Router 1 (Admin & Security):

- The router is connected with a separate IDS/IPS system.
- 2 L3 switches are connected with the router for Admin and Security respectively.
- **Admin L3 Switch:** A wifi connection is generated from the L3 switch which takes care of Mobile, Laptop connections.

- A L2 switch is placed in front of the L3 Switch for scalability. It takes care of the huge number of LAN connections possible in Admin Block. Mainly, Admin office PCs and Admin Office Printers are connected through this L2 switch.
- **Security L3 Switch:** Security Office PCs, printers, voip connections are directly connected to L3 switch since they won't be very large in number.
- A L2 switch is also deployed in front of the L3 switch which takes care of biometric and CCTV connections. Since, biometric and CCTV can be very large in number, L2 switch is used which can cater for a large number of connections(scalability).

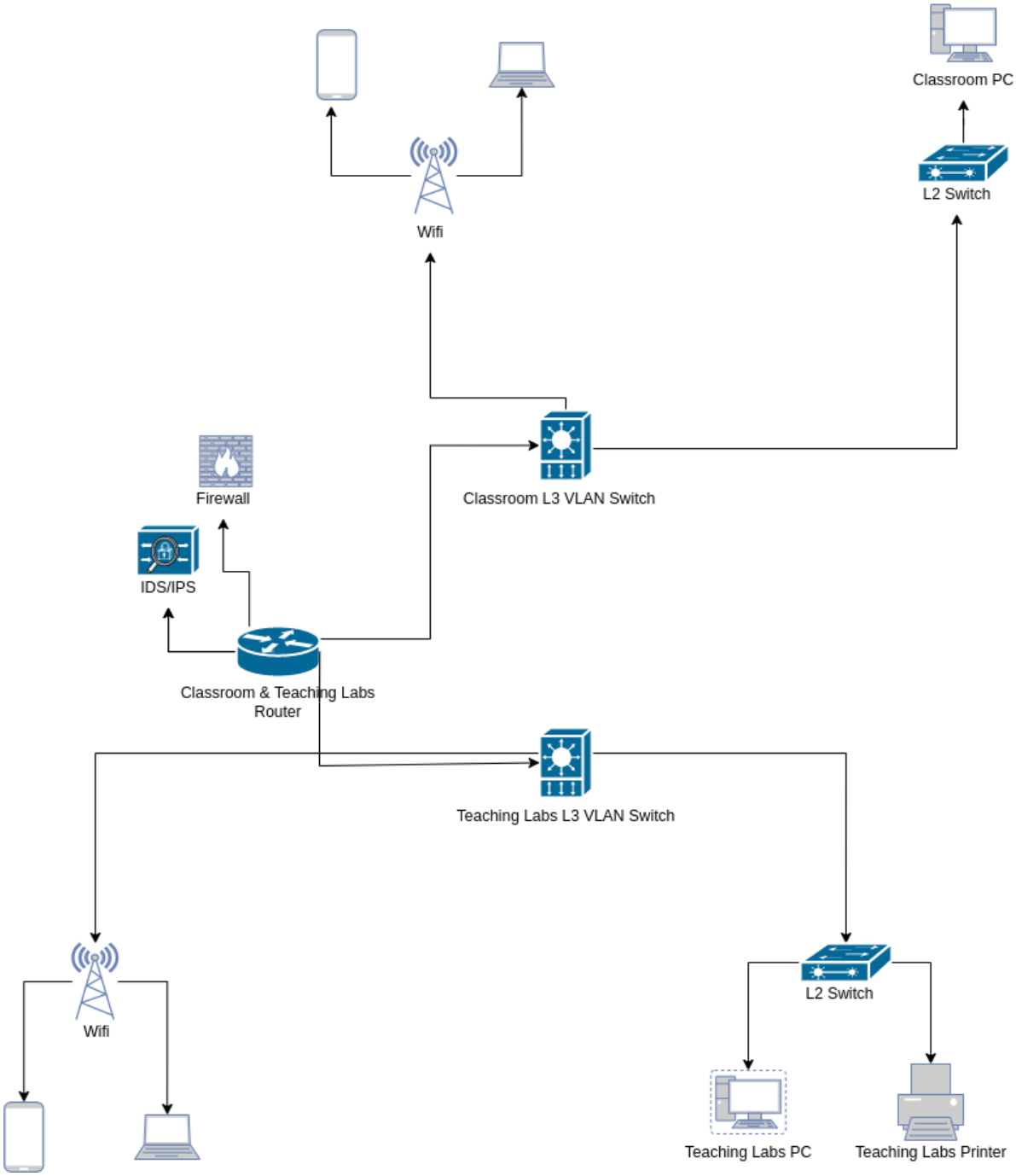

Figure 3) Router 2: Classroom & Teaching Labs Router

Router 2 (Classroom & Teaching Labs):

- The router is connected with a separate IDS/IPS system.
- 2 L3 switches are connected with the router for classroom and teaching labs respectively.
- **Classroom L3 Switch:** A wifi connection is generated from the L3 switch which takes care of Mobile, Laptop connections.
- A L2 switch is placed in front of the L3 Switch for scalability. It takes care of the huge number of LAN connections possible in the classroom. Mainly, classroomPCs are connected through this L2 switch.
- **Teaching Labs L3 Switch:** A wifi connection is generated from the L3 switch which takes care of Mobile, Laptop connections.
- A L2 switch is also deployed in front of the L3 switch which takes care of PC and Printer connections. Since, PC and printer can be very large in number, L2 switch is used which can cater for a large number of connections(scalability).

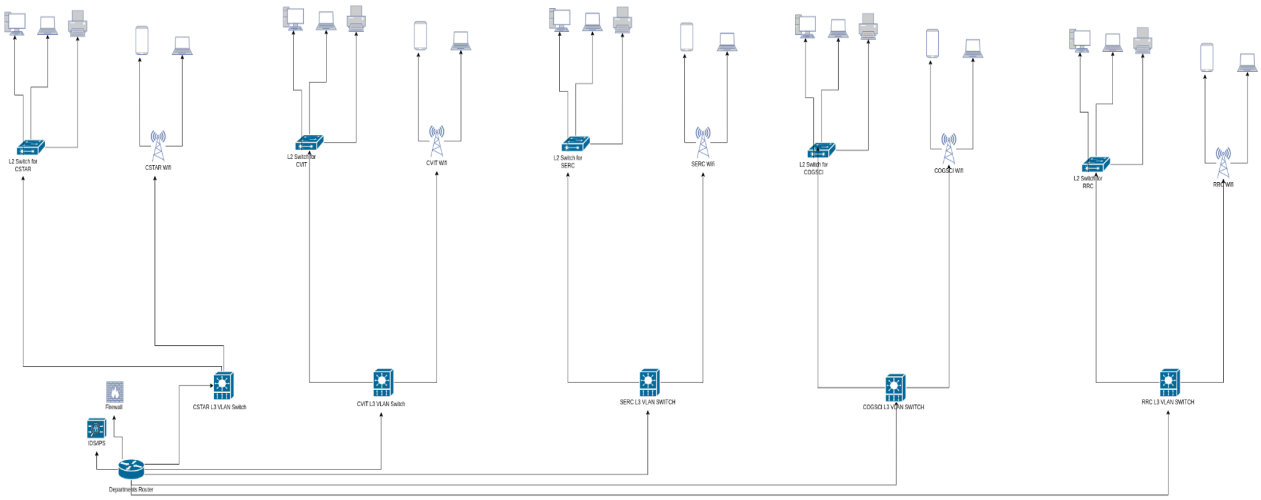

Figure 4) Router 3: Departments Router

Router 3 (Departments):

- The router is connected with a separate IDS/IPS system.
- 5 L3 switches are connected with the router for **CSTAR, CVIT, SERC, COGSCI and RRC respectively.**
- **CSTAR L3 Switch:** A wifi connection is generated from the L3 switch which takes care of Mobile, Laptop connections.
- A L2 switch is placed in front of the L3 Switch for scalability. It takes care of the huge number of LAN connections possible in the **CSTAR** lab. Mainly PCs, Laptops, printers are connected through this L2 switch.
- **CVIT L3 Switch:** A wifi connection is generated from the L3 switch which takes care of Mobile, Laptop connections.
- A L2 switch is placed in front of the L3 Switch for scalability. It takes care of the huge number of LAN connections possible in the **CVIT lab**. Mainly PCs, Laptops, printers are connected through this L2 switch.
- **SERC L3 Switch:** A wifi connection is generated from the L3 switch which takes care of Mobile, Laptop connections.

- A L2 switch is placed in front of the L3 Switch for scalability. It takes care of the huge number of LAN connections possible in the **SERC lab**. Mainly PCs, Laptops, printers are connected through this L2 switch.
- **COGSCI L3 Switch:** A wifi connection is generated from the L3 switch which takes care of Mobile, Laptop connections.
- A L2 switch is placed in front of the L3 Switch for scalability. It takes care of the huge number of LAN connections possible in the **COGSCI lab**. Mainly PCs, Laptops, printers are connected through this L2 switch.
- **RRC L3 Switch:** A wifi connection is generated from the L3 switch which takes care of Mobile, Laptop connections.
- A L2 switch is placed in front of the L3 Switch for scalability. It takes care of the huge number of LAN connections possible in the **RRC lab**. Mainly PCs, Laptops, printers are connected through this L2 switch.

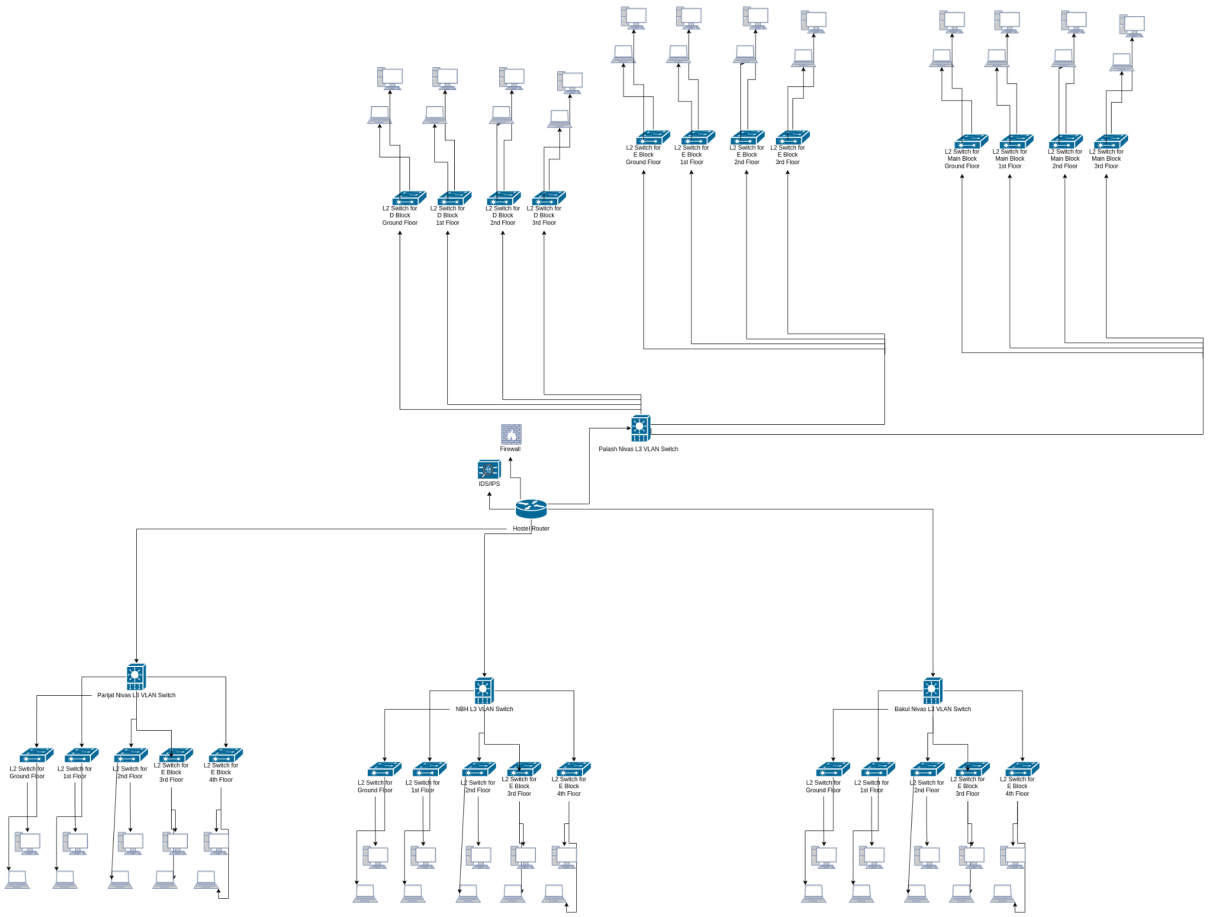

Figure 5) Router 4: Hostel Router

Router 4 (Hostels):

- The router is connected with a separate IDS/IPS system.
- 5 **L3 switches** are connected with the router for **Palsh Nivas, Parijat Nivas, NBH, Bakul Nivas** respectively.
- **Palsh Nivas L3 Switch:** 12 L2 switches are placed in front of the L3 Switch for scalability. There are 3 blocks **Main, D, E**. And the number of floors are 4. So, each

block has one L2 switch for a floor. So, in total there are 12 switches. Each switch takes care of the huge number of LAN connections possible in each block in each floor. Mainly PCs, Laptops are connected through these L2 switches.

- **Parijat Nivas L3 Switch:** 5 L2 switches are placed in front of the L3 Switch for scalability. The number of floors is 5. So, each floor has one L2 switch in it. So, in total there are 5 switches. Each switch takes care of the huge number of LAN connections possible in each block in each floor. Mainly PCs, Laptops are connected through these L2 switches.
- **NBH L3 Switch:** 5 L2 switches are placed in front of the L3 Switch for scalability. The number of floors is 5. So, each floor has one L2 switch in it. So, in total there are 5 switches. Each switch takes care of the huge number of LAN connections possible in each block in each floor. Mainly PCs, Laptops are connected through these L2 switches.
- **Bakul Nivas L3 Switch:** 5 L2 switches are placed in front of the L3 Switch for scalability. The number of floors is 5. So, each floor has one L2 switch in it. So, in total there are 5 switches. Each switch takes care of the huge number of LAN connections possible in each block in each floor. Mainly PCs, Laptops are connected through these L2 switches.
- There is no Wireless Internet access in the hostels.

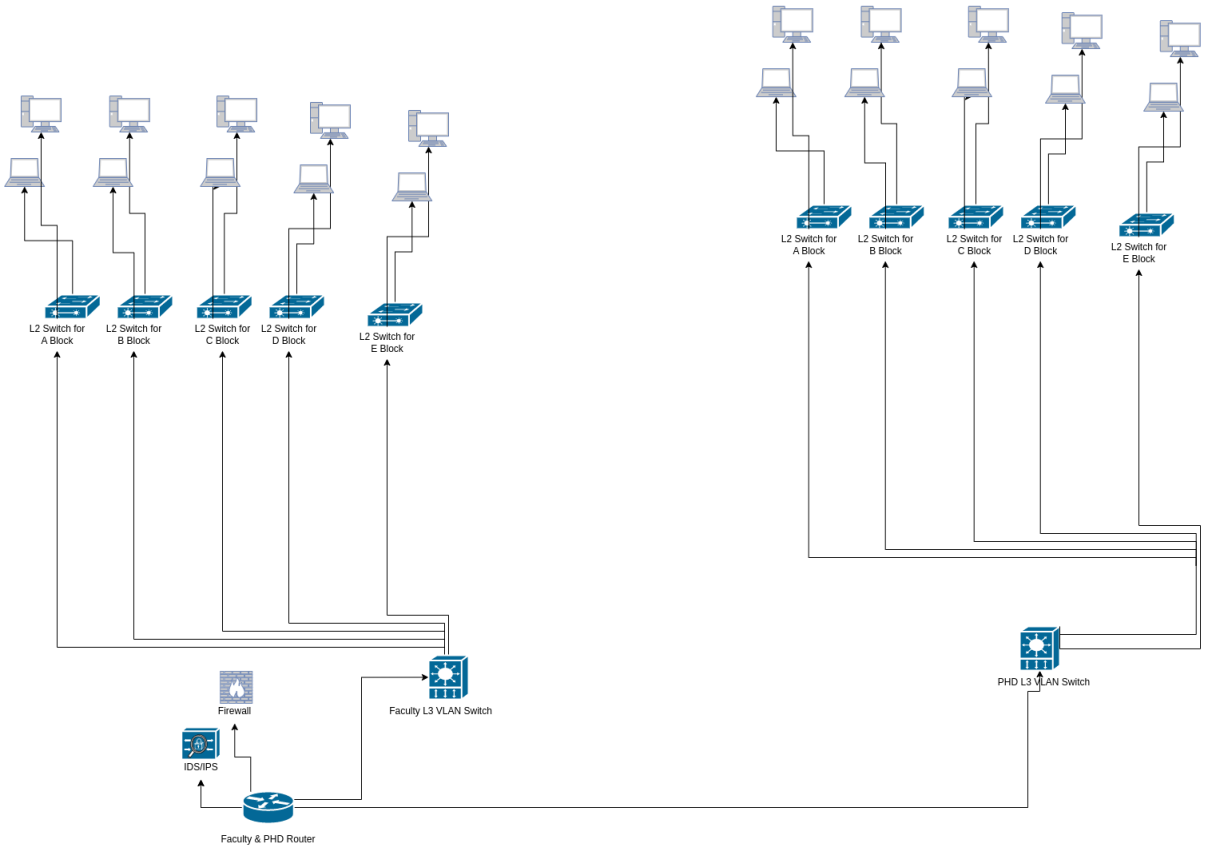

Figure 6) Router 5: Faculty & PHD quarters Router

Router 5 (Faculty & PHD quarters):

- The router is connected with a separate IDS/IPS system.
- 2 L3 switches are connected with the router for Faculty quarters and PHD quarters respectively.

- **Faculty quarters L3 Switch:** 5 L2 switches are placed in front of the L3 Switch for scalability. There are 5 blocks A, B, C, D, E. So, each block has one L2 switch in it. So, in total there are 5 switches. Each switch takes care of the huge number of LAN connections possible in each block in each floor. Mainly PCs, Laptops are connected through these L2 switches.
- **PHD quarters L3 Switch:** 5 L2 switches are placed in front of the L3 Switch for scalability. There are 5 blocks A, B, C, D, E. So, each block has one L2 switch in it. So, in total there are 5 switches. Each switch takes care of the huge number of LAN connections possible in each block in each floor. Mainly PCs, Laptops are connected through these L2 switches.

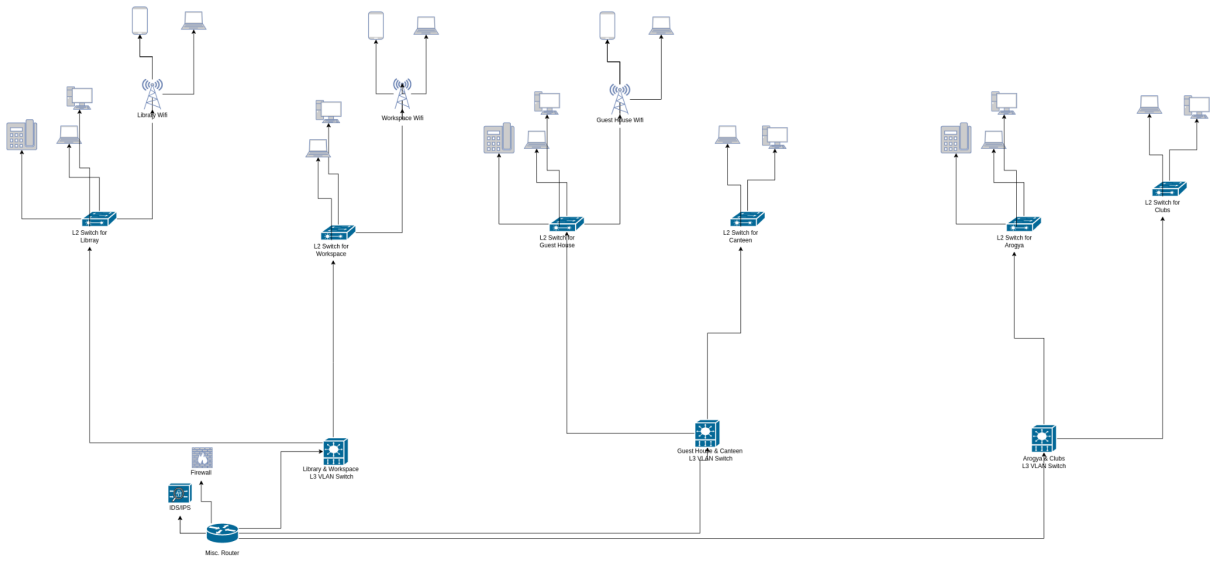

Figure 7) Router 6: Misc. Router

Router 6 (Miscellaneous):

- The router is connected with a separate IDS/IPS system.
- 3 L3 switches are connected with the router for Library & Workspace, Guest House & Canteen and Arogya & Clubs respectively.
- **Library & Workspace L3 Switch:** 2 L2 switches are placed in front of the L3 Switch for scalability. One takes care of Library connections and another takes care of Workspace connections. From each L2 switch there is a wifi connection for mobile devices and also in general LAN ports present for PC, Laptop, VOIP.
- **Guest House & Canteen L3 Switch:** 2 L2 switches are placed in front of the L3 Switch for scalability. One takes care of Guest House connections and another takes care of Canteen connections. From each L2 switch there is a wifi connection for mobile devices and also in general LAN ports present for PC, Laptop, VOIP.
- **Arogya & ClubsL3 Switch:** 2 L2 switches are placed in front of the L3 Switch for scalability. One takes care of Guest House connections and another takes care of Canteen connections. From each L2 switch there are general LAN ports present for PC, Laptop and(or) VOIP.

- ## IP Addressing Schema Design, Subnetting

Scheme: CIDR (Classless Inter-Domain Routing or supernetting)

We have 6 routers. They are as follows:

Router 1 (Admin & Security Block)

No of IP's = 512 (2^9) (/23)

Subnet Mask: 255.255.254.0

IP Range: 192.168.2.0 -> 192.168.3.255

Network ID: 192.168.2.0

Directed Broadcast Address: 192.168.3.255

Gateway Address: 192.168.2.1

Router 2 (Classroom & Teaching Labs)

No of IP's = 1024 (2^{10}) (/22)

Subnet Mask: 255.255.252.0

IP Range: 192.168.4.0 -> 192.168.7.255

Network ID: 192.168.4.0

Directed Broadcast Address: 192.168.7.255

Gateway Address: 192.168.4.1

Router 3 (Departments)

No of IP's = 2048 (2^{11}) (/21)

Subnet Mask: 255.255.248.0

IP Range: 192.168.8.0 -> 192.168.15.255

Network ID: 192.168.8.0

Directed Broadcast Address: 192.168.15.255

Gateway Address: 192.168.8.1

Router 4 (Hostels)

No of IP's = 4096 (2^{12}) (/20)

Subnet Mask: 255.255.240.0

IP Range: 192.168.16.0 -> 192.168.31.255

Network ID: 192.168.16.0

Directed Broadcast Address: 192.168.31.255

Gateway Address: 192.168.16.1

Router 5 (Faculty & PHD quarters)

No of IP's = 2048 (2^{11}) (/21)

Subnet Mask: 255.255.248.0

IP Range: 192.168.32.0 -> 192.168.39.255

Network ID: 192.168.32.0

Directed Broadcast Address: 192.168.39.255

Gateway Address: 192.168.32.1

Router 6 (Miscellaneous)

No of IP's = 2048 (2^{11}) (/21)

Subnet Mask: 255.255.248.0

IP Range: 192.168.40.0 -> 192.168.47.255

Network ID: 192.168.40.0

Directed Broadcast Address: 192.168.47.255

Gateway Address: 192.168.40.1

CONNECTING INFRASTRUCTURE TO NETWORK:

We have to provide internet access to following places:

- We have one Admin Block where all the administrative work is done, offices inside Admin Block are connected to the Network via L3 Switches which is connected to **Router 1.** The network can be scaled up by just adding an extra L2 switch connected to L3 switch or to Router 1 and if demand for new connection is less then we can use the already existing free port of switches.
- Similarly all the security devices such as CCTV, Biometric devices and Networked devices at the security desk are also connected to L2 Switch of **Router 1.**
- We have quite a few classrooms and some teaching labs (Each Teaching Labs has a lot of desktops) where network is provided via LAN port as well as Wifi. The network can be scaled up by just adding an extra L2 switch to L3 switch or to **Router 2** and if demand for new connection is less then we can use the already existing free port of switches.
- We also have several dedicated laboratories for various departments along with faculty/Staff cabins which connect to this network via LAN ports or Wifi. The network can be scaled up by just adding an extra L2 switch to L3 switch or to **Router 3** and if demand for new connection is less then we can use the already existing free port of switches. Servers of respective departments run here **[Needs proxy server]**. Each laboratory and faculty/Staff Cabin has a Biometrics device. All the Labs and cabin doors have Vibration sensors. All the Labs and Server are under CCTV surveillance which starts recording whenever thermal sensors detect some activity.
- There are 3 Hostel (Two of which are boys hostel and one girl hostel) and 1 Faculty quarters which gets connected to the network via L3/L2 Switches connected to **Router 4**. We can increase the number of L2\L3 switches for scalability purposes.

- There is one Faculty and one PhD quarters which get connected to the network via L3/L2 Switches connected to **Router 5.** We can increase the number of L2\L3 switches for scalability purposes.
- Rest of the infrastructure includes components such as Canteens, Music Room, bb-instant, Medical room (aarogya), Sports room, Yoga room, Guest House, Amphitheater, etc. Users can access the Internet here via Wifi/LAN port which gets its connection from **Router 6.**

Note: Each Biometrics device and CCTV is connected to Network via L2 switch which is connected to **Router 1**.

FIrewall:

A Multi-WAN Router is connected to this ISP, the router has capability of IDS/IPS and also acts FIrewall (Hybrid Device) we need firewall to protect the network from various attack such as Denial-of-service (DoS), Spoofing attacks, Phishing attacks, SQL injection attacks, Remote code execution attacks, Man-in-the-middle (MitM) attacks, Brute force attacks, Virus and malware attacks.

Choice of Firewall:

In this design we will use Cisco Adaptive Security Appliance (ASA) because other than just firewall it also provides the following features

1. Trusted by many organizations.
2. Can be used by organizations of any size.
3. Highly scalable and stable.
4. Provides Remote access VPN.
5. Manageability and monitoring capability.
6. Ability to control access based on application i.e. Application Visibility and Control (AVC).
7. Antivirus, AntiSpyware, antispam.
8. Filtering based on URL.
9. High Availability.

Choice of IDS/IPS:

In this design the IDS/IPS we will be using is **Snort** because of its highly optimized performance for large traffic, Open source nature, large community support, high scalability, signature based detection, Real-time detection, ease of integration, and low-cost. Although we already used Cisco Adaptive Security Appliance (ASA) which comes with its own IPS, we still used Snort because it does not cost anything and is not too resource intensive.

Choice Between Router/L3 Switch/SDN:

We use **L3 Switches** in most places which will be connected to these 6 routers. This choice is largely based on the fact that Layer 3 switches are designed for small or medium sized networks which is cost effective and also provides high performance, since they rely on hardware based switching they are faster and also more efficient as compared to router, for the same reason we didn't used SDN based Network within the campus because simple routing using L3 switch will do the required the task within the network.

The L3 Switch that we will be using is Cisco Catalyst series L3 switches because of it's Good Quality of Service (QoS), High availability, Easy Management (GUI and CLI), tools such as Cisco Prime Infrastructure, Scalability, Protocol-Independent Multicast (PIM) and ability to handle load-intensive multicast applications (like video streaming), VLAN, Also provides Security by offering features like access control lists (ACLs), authentication and port security.

Securing Server:

We have decided not to have common server room for all the server which are running in the server room to avoid attacker tampering with other's servers, every department has to keep their respective server (if any) in their lab that should be connected to Backup Power supply and access to servers is restricted to only authorized personals (and they need **biometric/RFID** authentication to access the server), the Lab should have **CCTV surveillance** and **thermal sensors** are used to tell when and what to record. Also The Server which are outside departments like Admin Block they will also require similar security. And the servers running in Faculty quarters will get security provisioning in the form of software but won't be having any separate room to secure the servers. To protect

the server's data from data loss in case of any attack we are storing the data on cloud storage as well as on local backup storage.

Application/Services Blocking:

Various Services such as **VNC** (usually [not always] running on port 5900 or 5800) or similar services which enable users to remotely use someone else's device must be blocked.

Torrent Services can be blocked by **blocking Port** number 6881-6889, but not always since some torrent applications can run using any of the ports.

So for these and similar applications we will have to make use of **content filtering Firewall**.

Blocking Porn sites, adware, malware, fake news, gambling:

Network admin can edit the hosts file in the Routers to contain URL and IP mapping to redirect popular porn sites, adware, malware, fake news, gambling sites to local hosts and hence no connection can be initiated to them within the network (without the use of VPN). The mapping of URL and IP address can be fetched from https://github.com/StevenBlack/hosts .

Maintaining Logs: We can use tool like **Syslog-ng** to keep the logs of your network, it not only stores the logs it can also process them and do analysis on the data to identify security breaches. The reason for using this tool over others is that it is open-source. Other Features include Scalability, high-performance, highly configurable, Integrability with other tools such as Kafka, Elastic Search, Splunk, etc.

DNS Server: In order to increase the security we would like to have our own DNS server as well, for this we can use several tools one of which is **BIND (Berkeley Internet Name Domain)** because it is open source software. Other features include Caching, Dynamic Updates, DNSSEC (Domain Name System Security Extensions) [for security of DNS from DNS Tampering or DNS spoofing], IPv4 and IPv6 Support. Having a separate DNS server of our own in the network makes sure that the malicious code is not able to connect to its remote command line interface to get instructions on what to execute next.

Reverse Proxy: In order to protect the servers that need to be accessed from outside the campus, for those servers we will be using proxy servers to provide a layer of security for these servers. Due to this no client can directly talk to the server. Other benefits that we get using Reverse Proxy includes SSL Encryption, Caching, Load Balancing, Protection against various attacks. The software solution for reverse proxy that we will be using is **NGINX**.

The reason for using NGINX is that it is open source. Also, it can take care of a huge amount of connections and requests, as it can manage huge traffic easily. Can also act as load balancer. It is highly configurable.

We are avoiding any hardware appliance for reverse proxy to avoid the increased cost of the system. The software solution that we will be using is open source so it won't cost anything. But the hardware appliances that we could have used are Citrix NetScaler, F5 Network BIG-IP, Barracuda Load Balancer ADC, etc but we would not use them as they increase the cost of network infrastructure a lot and are usually used for large organizations only.

Let us name the computers which are involved in the illustration:

- D: This refers to the user's computer.
- E: Reverse Proxy Server
- F:These are the Origin servers

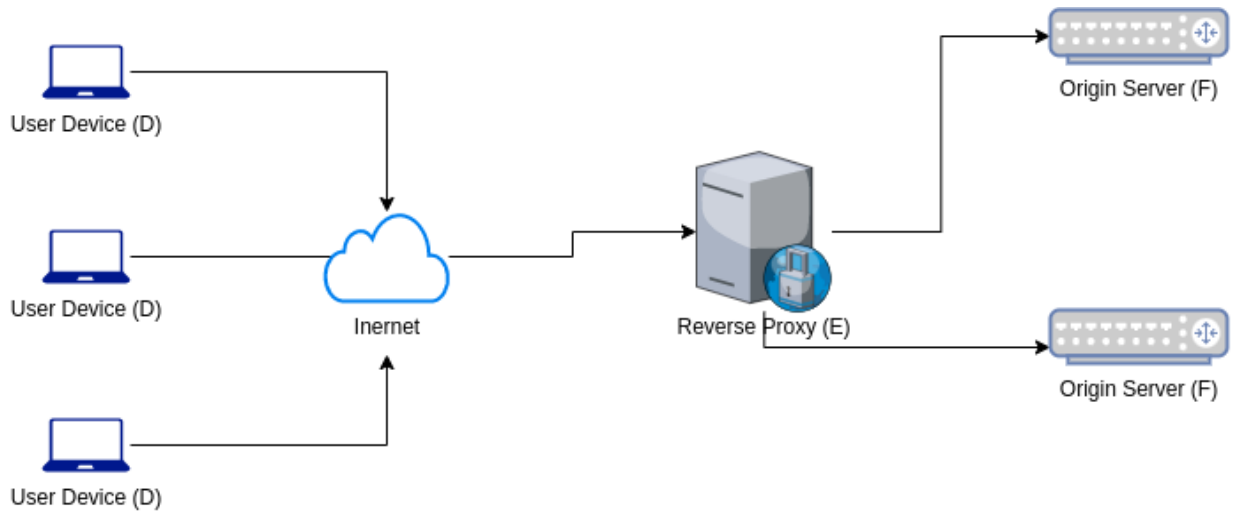

Figure 8) Reverse Proxy Flow

In the general scenario, all the requests from D would go directly to F and F would respond back to those requests directly to D. But when reverse Proxy is involved, the requests from D would go to E, which in turn send those requests to F. F would then respond back to those requests to E, and E will send those responses back to D.

Choice of L3 Switch: The device that we will be using for L3 switch is **Cisco Catalyst 3650 Series** because it can support 480 Gbps switch throughput and 40 Gbps stacking bandwidth. Has security features like ACLs (Access Control Lists), MACsec, TrustSec. It can be used to create VLANs. It supports Simple Network Management Protocol (SNMP). Multiple options for management such as GUI, CLI and Cisco Prime. It can support upto 96 ports per device which is more than what we will ever require and serve the purpose at most of the places in the Campus Network.

Choice of L2 Switch: The device that we will be using for L2 switch is **Cisco Catalyst 2960-X Series** because it has 48 ports per devices which server the purpose at most of the places in the Campus Network and at places where 48 ports are insufficient we will buy that variant which has more ports. Other benefits that it provides are easy management, good quality of service, energy efficient, high security and support from Cisco. Devices can be directly connected to L3 Switch but we connect them to L2 switch for scalability (it means that L2 Switches are connected to L3 Switch, so that connection from L2 switch to other host/devices can be added).

VLAN Design: We cannot have network segregation based on LAN only due to security reasons, so we will segregate the network using VLAN so that we can control where the broadcast message can go. VLANs (Virtual LANs) also have other security advantages. To create VLAN we will use L3 Switches which are directly connected to Router 1,2,3,...6. It segregates the traffic but the virtual LANs reside in the same Physical LAN, i.e. the VLANs behave as if they exist in different switches.

We will be using a Dynamic VLAN in which we can use username/computer to determine which VLAN a user belongs to, due to which the user can move to various places and still belong to the same VLAN.

The Different VLAN that are created are for:

- Admin Block where all the administrative work is done.
- Classrooms and Teaching labs
- Laboratories for various departments along with faculty/Staff cabins.
- Servers running at various places are part of the same VLAN, as they have the same level of security.
- Each Hostel is part of a different VLAN (to make it difficult to initiate an attack from one hostel to another Hostel).
- Faculty residence areas are part of a VLAN and PhD residence areas are part of different VLAN.
- Security Blocks\Desks and Security Devices (CCTV, Biometric Devices, etc) are part of one VLAN.
- Rest of the infrastructure such as Canteens, Music Room bb-instant, Medical room (aarogya), Sports room, Yoga room, Guest House, Amphitheater, Workspace, T-Hub, etc are part of different VLAN.

Security Threats in Wi-Fi:

- Since the range of Wi-Fi can extend and it does need to be physically connected, if someone gets close enough to the access point, they can connect to you and can capture the personal files and data.
- There is something known as evil twin attacks in which the attacker gathers information about the public access point and tries to impersonate it and then sending a stronger broadcast signal stronger then the legitimate access point luring the users to connect to stronger signal and can read the users data easily which is being sent over internet including username, passwords, credit card numbers etc.
- Most of the data which is being carried by the public access points is not encrypted so anyone can sniff and obtain sensitive information.

WiFi:

How can we Enhance security in Wifi:

- There is a feature of guest accounts in wireless routers which grants access to the guest users on a separate channel with a separate password.
- We can restrict access to the Wi-Fi by configuring the network such that only allowed mac addresses can connect to the access point and filtering out the others.
- There are various encryption protocols such as Wi-Fi Protected Access (WPA), WPA2, and WPA3 which can be used to encrypt the information which is transmitting over the channels.

We can use Cisco routers or Juniper networks which provide routers with advanced security features such as packet filtering, intrusion prevention, and SSL VPN support.

SERVER STORAGE:

How can we Enhance security in Server Storage:

- Install SSL (Secure Socket Layer) certificates so that these security protocols guard communication between two systems over the internet. SSL certificates scramble the data in transit and even if someone succeeds in accessing the data it will not be able to decipher its meaning.
- We can change the default ports or well-known ports to access the data, we can use the dynamic ports in order to increase the security of our storage Server.
- We should also avoid placing the user input directly into the sql statement and prefer parameterized queries to avoid attacks like SQL injection on our storage.
- The database files of Sql Server and Azure Sql can be encrypted using TDE(Transparent Data Encryption).This encrypts our sensitive data in the database and also protects the keys which are used to encrypt the data.

We can use tools such as Nagios or Zabbix for monitoring the server, both of them are open source, highly customisable and highly scalable and can be used to monitor various aspects such as CPU usage, disk space and network traffic.

SERVER CONTROL DESK:

How can we Enhance security in Server Control Desk:

- We can use SSH based authentication instead of password to connect with my server, which in turn increases the security of the server as attackers cannot authenticate as easily as in case of traditional password-based mechanisms.
- We can monitor the number of login attempts to my server so that i can prevent my server from intrusion of brute force attacks.
- We also need to set up some password expiration policy, so that the user needs to keep changing the password within some time period.

We can use tools such as Fail2Ban which is a popular intrusion prevention tool that monitors log files and blocks IP addresses with malicious activity such as users having multiple failed login attempts.

MAIN SERVER:

How can we Enhance security in Main Server:

- We can disable the DNS recursion in order to restrict the recursion such that DNS will not query any other DNS server apart from its own cache or information available within its local DNS server. This disabling of DNS recursion protects our server from DoS (denial of Service) attacks (only addresses queries of registered sites).
- We can also use FTPS (File Transfer Protocol Secure) to transfer files to and from the server and protect the file during transfer. FTPS encrypts the file using command and data channels.
- We should also not provide root access as if someone gets root credentials then he can attack the server and bring it down easily, boiling down the security of my server to root access. Instead, we can create some limited access accounts which have the same privileges as the root user and perform the administrative tasks and then take away the access privileges once the task is over.
- We can also install some application firewalls such as mod security or mod_evasive.

- We can use sophos which is an intrusion detection system (IDS) used to detect unauthorized activity by monitoring processes running on your server.

We can use tools like OpenSSL to encrypt files and folders as well as implement SSL/TLS to encrypt network traffic.

MAIN BACKUP SERVER:

- Disabling all inbound ports except the port the backup software needs to perform the backup needs to be left open and even this port should be accessed via VPN. Disabling ports secures my backup server both from any vulnerability in my server or through logging credentials.
- In order to make our backup server secure we need to separate our backup network into security zones (a group of servers with the same level of security requirements) and these security zones are protected by layer3 firewall or through VLAN segmentation. In essence, we must ensure that the backup server should not be connected to any centralized authentication system and should be accessed only by a limited set of users.

We can use tools like Veritas NetBackup which is a backup encryption software which provides advanced encryption capabilities using encryption algorithms such as AES-256 and 3DES.

CLOUD SERVER:

- We need to secure the API Interfaces which are provided by the cloud service provider as the documentation designed for the customer can also be used by a cybercriminal to identify and exploit potential methods for accessing and exfiltrating sensitive data from cloud servers. The Certified Cloud Security Professional (CCSP) certificate is most valued in cloud security certification, so to make your cloud server secure ensure that the cloud service provider has a CCSP certificate.

There are various Cloud Service Providers such as AWS(Amazon Web Services) and Microsoft Azure which offer built in firewall features.

How does LDAP work?

LDAP (Lightweight Directory Access Protocol) authentication is a method of authentication that allows users to log in to a network or application using their LDAP credentials, which are stored in a centralized directory.

This is how LDAP works:

1. The user enters his username and password on the login page of the application/ network he wants to access.
2. The application sends an authentication request to the LDAP server which stores and manages the user credentials.
3. LDAP server searches for the username and password in its directory and sends back a positive or negative response based on whether the credentials match or not indicating whether the access is granted or denied.

Thus, LDAP provides a centralized way to store and manage user credentials and can be easily integrated with other authentication methods to provide an extra layer of security.

USING LDAP FOR CAS:

LDAP is a protocol which is used to retrieve user accounts and other information associated with that account after talking to a directory while CAS is a software which uses LDAP to find users accounts and do other things with that information.

VPN And Intranet/Mess Access.

IIITH Intranet: We have an intranet in the campus along with a mess portal which is only accessible using network of university network or through VPN from outside the Network.

VPN setup for remote accessibility of IIITH intranet: We'll use Remote Access VPN for this purpose since the resources(servers) are not hosted in the cloud. Remote Access VPNs will help to access college's intranet from anywhere outside college campus. The two most widely used technologies in remote access VPNs are SSL and IPsec.

We'll use SSL vpn for this purpose since SSL VPNs are more secure than IPSEC VPNs.After a user logs into the network, SSL becomes more secure. IPsec users are treated as complete

network members while SSL VPNs only allow access to a limited number of apps. Hence, SSL makes it simpler to limit user access.

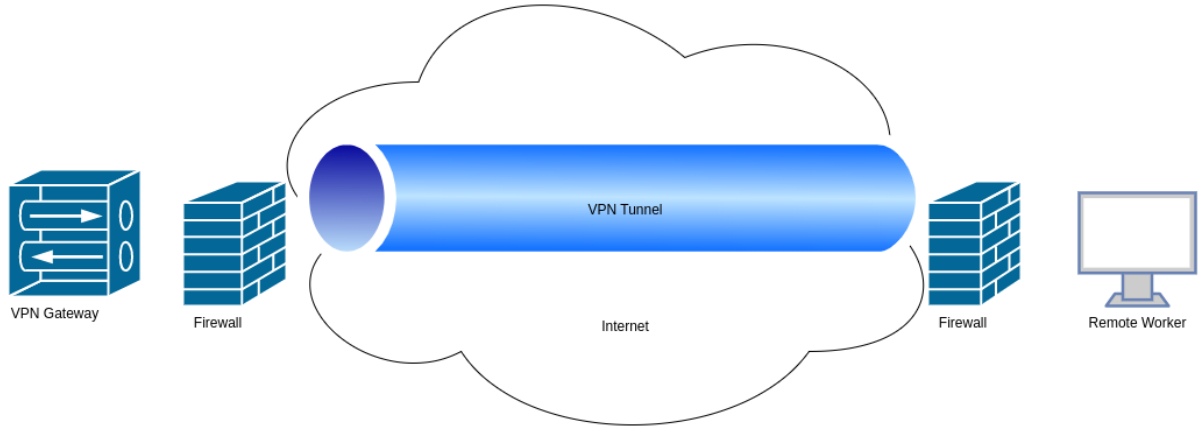

Figure 9) VPN Tunneling Process