



Computer Networks

Assignment 4

CS5001

Name-Nipun Patel

Enrolment ID-AU19B1009

Bachelor of Technology

(2021 – 22)

Design A Small Enterprise Network

❖ **Problem Statement: -**

As a Network Manager in an organization given task to design Network Architecture for their IT Infrastructure. Please consider following 10 network design steps to create a sustainable and future-proof network design:

1. Outline the requirements
2. Draw out the network topology
3. Keep a register of the hardware
4. Label the hardware
5. Keep a record of the software used
6. IP addresses and subnets
7. Test the network
8. Allow room for redundancy
9. Network security
10. Plan for the future

Small Enterprise / Organization :

ABC Ltd (IT Solutions Provider) has departments/sections like

HR

Finance

Client Engagement

Software Development

Marketing

Project and Technical Support Team

have members of 10,10,30,60,30,30 and 40, respectively.

ABC has corporate offices at Pune and Regional offices at Delhi and Bengaluru. Employees Count at Delhi and Bengaluru will be less compared to corporate office. (50 % Only). For example, Software Development Team has 60 at Corporate Office 30 at Regional Offices.

The Corporate Office has 6 Floors, and the regional office has 3 Floors. Each Floor has capacity of 150 Seats. Expected growth will be 100% increment on the employees count each section every year from the startup count. For example, HR Employees' count in the third year will be 40. (0 Year – 10 1-Year –20 2 Year –30 and 3 Year –40). Network Design scalable for up to 3 years and reliable too.

Assume that office has structured cabling with plenty of MM fiber between the floors. Each Floor has a length of 75 Meters. The regional office and corporate office connected with 1000 Mbps MPLS Cloud for Intranet and for the internet they connected with 500 Mbps Leased Line with their location Internet Service Provider.

Corporate Office has Server Farm with Network Hub has network devices with 20 Physical Servers for the office automation and testing environment for Software development Team, 2 web servers facing with internet for development team to test their applications.

Since you are being a Network Manager - you must design the Network Hierarchical Model and Security too. If you encounter ambiguities, make reasonable assumptions, and proceed. For all tasks, use the initial customer scenario and build on the solutions provided thus far. You can use all documentation, books, white paper, and so on.

In each step, you act as a network design consultant. Justify your ideas when they differ from the solutions provided. Use any design strategies you feel are appropriate.

❖ Requirements and budget estimation: -

a. User Requirements:

User Requirements	Description
Location and number of workstations	<ul style="list-style-type: none">• 2 regional offices Delhi and Bengaluru, 1 corporate office.• Server room for corporate office,• MPLS line and local ISP for all offices connectivity.• 3 years scalability of employees on network.
Availability	An uninterruptible network is required for user operations
Scalability	The network implemented should be scalable to endure any future expansions.
Affordability	ABC Ltd has a limited budget and network design and implementation should be done within the said budget.
Security	The LAN should be secured with restricted access. The network should have the capability of filtering what enters and leaves the network.

b. Network devices requirements: –

Device	Specification	Qty.	Location
Cisco Nexus 93180LC-EX (Core Switch)	Up to 32 x 40/50-Gbps QSFP+ ports OR 18 x 100-Gbps QSFP28 ports CPU: 4 cores System memory: 24 GB SSD drive: 64 GB	3	Corporate, Regional offices
Cisco ISR4431/K9 (Router)	1 x 10/100/1000 Mb/s RJ45 Port 1 x 10/100/1000 Mb/s SFP Port 1 x 10/100/1000 Mb/s Management Port	3	Corporate, Regional offices
Cisco Nexus 7700 4-Slot Switch (Corp Distribution)	one I/O module slots, supports up to 48 x 1 and 10 Gigabit Ethernet ports, 24 x 40 Gigabit Ethernet ports, or 12 x 100 Gigabit Ethernet ports	8	Corporate office
FortiGate F600D (Firewall)	Site-to-site ADVPN – Dynamic VPN tunnels, policy-based VPN, IKEv1, IKEv2, DPD, PFS, ESP and ESP/HMAC support, Symmetric Cipher support (IKE/ESP): AES-128 and AES-256	5	Corporate and regional offices, server room
Cisco SG250-08HP (regional primary switch)	Support for IEEE 802.3ad Link Aggregation Control Protocol (LACP) <ul style="list-style-type: none"> Up to 4 groups Up to 8 ports per group with 16 candidate ports for each (dynamic) 802.3ad LAG 	6	Regional office
Cisco Nexus 93120TX (Sub Switch)	2.4 Tbsp. of bandwidth in a 2 RU form factor 96 fixed 10-Gbps BASE-T ports that can operate at 100 Mbps, 1 Gbps, or 10 Gbps speeds Six fixed 40-Gbps QSFP+ for uplink connectivity that can be turned into 10-Gbps ports Latency of 1 to 2 microseconds	14	Regional Office
Cisco Aironet 2800 (Access Point)	– 4x4 MU-MIMO with three spatial streams – MRC – 802.11ac Beamforming – 20-, 40-, 80, 160-MHz channels	15	Corporate, regional office

Cisco IP Phone 7821	The handset is Hearing Aid-Compatible (HAC) and meets Federal Communications Commission (FCC) loudness requirements for the Americans with Disabilities Act (ADA). You can achieve Section 508 loudness requirements by using industry-standard inline handset amplifiers such as Walker Equipment W-10 or CE-100 amplifiers. The dial pad is also ADA-compliant.	420	Corporate, Regional office
Ethernet CAT-7 and Multimode Fiber Cable	support 10 Gbps, but laboratory testing has successfully shown its ability to transmit up to 40 Gb at 50 meters and even 100 Gb at 15 meters. The multimode optical fiber cable is designated as 50/125 or 62.5/125 (OM1). This defines the core to cladding diameter as 50 or 62.5 to 125 microns.	-	Corporate, Regional office all floors

c. Estimated budget:

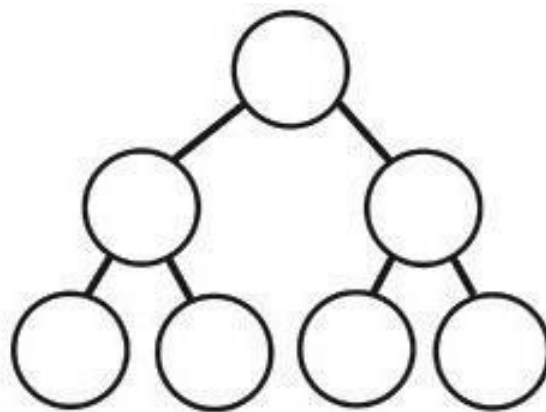
Device	Quantity	Price
Cisco Nexus 93180LC-EX (Core Switch)	3	32200
Cisco ISR4431/K9 (Router)	3	4437
Cisco Nexus 7700 4-Slot Switch (Corp Distribution)	8	32,902
FortiGate F600D (Firewall)	5	10000
Cisco SG250-08HP (regional primary switch)	6	399
Cisco Nexus 93120TX (Sub Switch)	14	6999
Cisco Aironet 2800 (Access Point)	15	1728
Cisco IP Phone 7821	420	270
Ethernet CAT-7 and Multimode Fiber Cable	-	10000
Total	474	98935
Grand Total		46,895,190

❖ Network Topology of our network: -

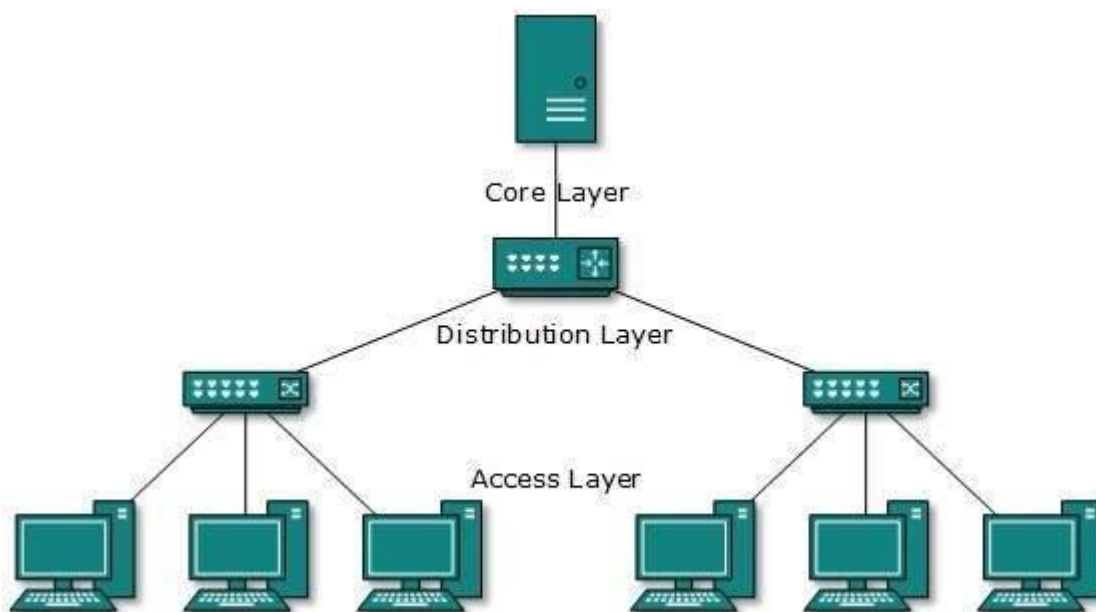
We will be using **Tree Topology** for our network design.

Tree Topology: A tree topology is a special type of structure where many connected elements are arranged like the branches of a tree. Tree topologies are frequently used to organize the computers in a corporate network, or the information in a database.

It is also known as hybrid topology because it is combination of star and bus topology, it has fast/same data transfer speed and is easy to install.



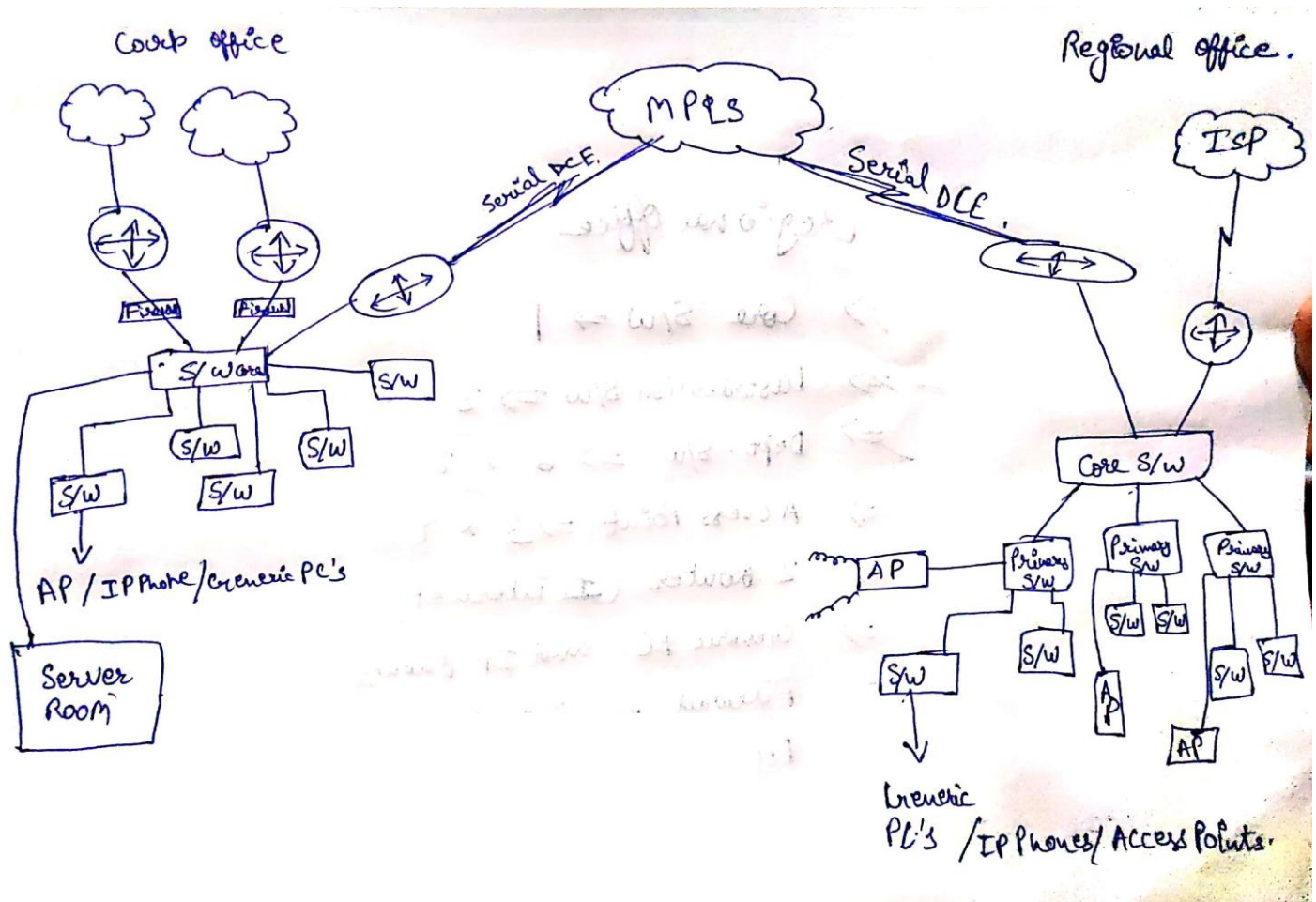
A basic representation of tree topology



Tree topology in computer network architecture.

The reason why we chosen this topology is because in our case we are communicating with 3 different types of network through MPLS line and each network has several departments and each one of them are interconnected through core and distribution switch. Therefore the network architecture/structure comes out to be in the form of a tree.

Below is our network hierarchy,



CS Scanned with CamScanner

In the above diagram we can see that the network hierarchy is forming a tree where both bus and star topology is concurrently coming in the scenario, we have 3 networks intercommunicating via MPLS leased Line which is coming in STAR topology and while router firewall etc. are in BUS therefore the series/parallel combination of these networking devices creates a tree hierarchy.

❖ Hardware Register table: -

Corporate Office (PUNE)					
Location	Core Switch	Supply Switch	Access Point	IP Phone	Data
Ground Floor	1	2	1	10	10
1 st Floor	0	1	1	10	10
2 nd Floor	0	1	1	30	30
3 rd Floor	0	1	1	60	60
4 th Floor	0	1	1	30	30
5 th Floor	0	1	1	30	30
6 th Floor	0	1	1	40	40
Total	1	8	7	210	210
Network Room (Ground Floor)					
Router (MPLS)	Internet Router Primary 500Mbps	Internet Router Backup 100Mbps	Physical Servers	Web Servers	Firewall
1	1	1	20	2	3

Regional Office (Delhi)						
Location	Core Switch	Supply Switch	Access Point	IP Phone	Data	Distrib. Switch
Ground Floor	1	2	1	20	20	1
1 st Floor	0	2	1	25	25	1
2 nd Floor	0	2	1	30	30	1
3 rd Floor	0	1	1	30	30	0
Total	1	7	4	105	105	3
Network Room (Ground Floor)						
Router (MPLS 1000Mbps)			Internet Router Primary 500Mbps		Firewall	
1			1		1	

Regional Office (BENGALURU)						
Location	Core Switch	Supply Switch	Access Point	IP Phone	Data	Distrib. Switch
Ground Floor	1	2	1	20	20	1
1 st Floor	0	2	1	25	25	1
2 nd Floor	0	2	1	30	30	1
3 rd Floor	0	1	1	30	30	0
Total	1	7	4	105	105	3
Network Room (Ground Floor)						
Router (MPLS 1000Mbps)			Internet Router Primary 500Mbps		Firewall	
1			1		1	

❖ Hardware Label's: -

DEVICE NAME	LABELS
Router MPLS 1000Mbps (Corporate office PUNE)	R-Corp
Router MPLS 1000Mbps (Regional office DELHI)	R-DEL-Reg
Router MPLS 1000Mbps (Regional office BENGALURU)	R-BLR-Reg
Core Switch (Corporate Office PUNE)	CSW-P
Core Switch (Regional Office DELHI)	CSW-D
Core Switch (Regional Office BENGALURU)	CSW-B
Distribution Switch (Corporate Office PUNE)	DSW-P
Distribution Switch (Regional Office DELHI)	DSW-D
Distribution Switch (Regional Office BENGALURU)	DSW-B

Sub Switch (Regional Office DELHI)	SSW-D
Sub Switch (Regional Office BENGALURU)	SSW-B
Access Point (PUNE)	AP-P
Access Point (DELHI)	AP-D
Access Point (BENGALURU)	AP-B
Physical Servers	P-Server
Web Servers	W-Server
IP Phones	VoIP
Generic Data PC (LAN Connection)	PC
FortiGate Firewall	Firewall

❖ **Software's Used: -**

1. Cisco Packet Tracer (for designing the network architecture)
2. Photoshop (Editing purpose)
3. Lucid Chart (Network Blueprint creation)
4. Draw.io (Network Blueprint creation)
5. SolarWinds (Network structure, IP addressing, Topology creation)



❖ IP addresses and Subnets: -

For our Network design we will use B-Class IP addresses and use subnetting on the private IP address provided as **172.16.0.0**, thus for subnetting calculation below are some formulas to calculate,

1. (Na) Network per subnet = 2^n where n is the no. of bits. Purchased.

This formula calculates how many subnets we can have over same network.

2. (Hs) Host per subnet = $2^x - 2$ where x is the no. of unused bits or OFF bits.

This formula calculates how many hosts we can have in a subnet.

3. (B) Block size = 256 - new subnet mask, this formula shows from which IP new host can be connected over every new subnet.

For corporate office we will use **B-26** and **B-27** subnets for respective departments as mentioned in the IP subnet table.

26th Bit calculation:

Na : $2^{10} = 1024$, since we have purchased 10 bit therefore, **n = 10** thus total subnet on new subnet will be 1024.

Ha : $2^6 - 2$, x = 6 (OFF bits)

$$2^6 - 2 = 62$$

We can have over 62 new hosts per subnet in a network.

B = 256 - 192 = 64, thus new hosts on new network subnet will start from 64

B-26 - Subnet: 255.255.255.192

27th Bit calculation:

Na : $2^{11} = 2048$, since we have purchased 11 bit therefore, **n = 11** thus total subnet on new subnet will be 2048.

Ha : $2^5 - 2$, x = 5 (OFF bits)

$$2^5 - 2 = 30$$

We can have over 30 new hosts per subnet in a network.

B = $256 - 224 = 32$, thus new hosts on new network subnet will start from 32

B-27 – Subnet: 255.255.255.224

Corporate Office (PUNE)	
Dept. name	Hosts Required
HR	10
Finance	10
Client	30
Software	60
Marketing	30
Project	30
Technical	40

Corporate Office - PUNE (network:172.16.0.0)						
Dept. Name	Vlan ID	Network Subnet	Subnet Mask	Host range	Broadcast ID	No.of hosts
HR	10	172.16.0.0	255.255.255.224	1-30	172.16.0.31	29
Finance	20	172.16.0.32	255.255.255.224	33-62	172.16.0.63	29
Client	30	172.16.0.0	255.255.255.192	1-62	172.16.0.63	61
Software	40	172.16.0.64	255.255.255.192	65-126	172.16.0.127	61
Marketing	50	172.16.0.128	255.255.255.192	129-190	172.16.0.191	61
Project	60	172.16.0.192	255.255.255.192	193-254	172.16.0.255	61
Technical	70	172.16.1.0	255.255.255.192	1-62	172.16.1.63	61

For regional office we will again use B-26 and B-27 Subnetting, subnetting calculation mentioned above already.

Regional Office (DELHI)	
Dept. name	Hosts Required
HR	5
Project	15
Finance	5
Technical	20
Client	15
Marketing	15
Software	30

Regional Office - DELHI (network:172.30.0.0)						
Dept. Name	Vlan ID	Network Subnet	Subnet Mask	Host range	Broadcast ID	No.of hosts
HR	10	172.30.0.0	255.255.255.224	1-30	172.30.0.31	29
Project	20	172.30.0.32	255.255.255.224	33-62	172.30.0.63	29
Finance	30	172.30.0.64	255.255.255.224	65-94	172.30.0.95	29
Technical	40	172.30.0.96	255.255.255.224	97-126	172.30.0.127	29
Client	50	172.30.0.128	255.255.255.224	129-158	172.30.0.159	29
Marketing	60	172.30.0.160	255.255.255.224	161-190	172.30.0.191	29
Software	70	172.30.1.0	255.255.255.192	1-62	172.30.1.63	61

Hence we have successfully created the IP tables and assigned the range of IP to the respective VLAN's of different departments, based on the calculation we did for IP address assigning and subnet selected for various departments.

Regional Office (BENGALURU)	
Dept. name	Hosts Required
HR	5
Project	15
Finance	5
Technical	20
Client	15
Marketing	15
Software	30

Regional Office - BENGALURU (network:172.28.0.0)						
Dept. Name	Vlan ID	Network Subnet	Subnet Mask	Host range	Broadcast ID	No.of hosts
HR	10	172.28.0.0	255.255.255.224	1-30	172.28.0.31	29
Project	20	172.28.0.32	255.255.255.224	33-62	172.28.0.63	29
Finance	30	172.28.0.64	255.255.255.224	65-94	172.28.0.95	29
Technical	40	172.28.0.96	255.255.255.224	97-126	172.28.0.127	29
Client	50	172.28.0.128	255.255.255.224	129-158	172.28.0.159	29
Marketing	60	172.28.0.160	255.255.255.224	161-190	172.28.0.191	29
Software	70	172.28.1.0	255.255.255.192	1-62	172.28.1.63	61

❖ Routing Protocols: -

We will be using 2 different protocols they are as BGP (Border Gateway protocol) and EIGRP (Enhanced Interior Gateway Routing Protocol).

- BGP Protocol:** BGP Protocol is a multiple system Autonomous number. It transfers packet information between different A.S. no. system. It is designed to distribute routing information between A.S. System.

BGP enables the internet function, BGP uses router ID, which sets in 4 blocks x.x.x.x and it will be different in every router and neighbor router information must be feeded.

- b. **EIGRP Protocol:** EIGRP is a dynamic routing protocol, it is a hybrid protocol which combines with IGRP, it is a classless routing protocol, it supports CIDR and VLSM. EIGRP has maximum network support and host count of 255.

Multiprotocol Label Switching (MPLS): It is a routing technique in telecommunications networks that directs data from one node to the next based on short path labels rather than long network addresses, thus avoiding complex lookups in a routing table and speeding traffic flows. The labels identify virtual links (*paths*) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols, hence the "multiprotocol" reference on its name. MPLS supports a range of access technologies, including T1/E1, ATM, Frame Relay, and DSL

- So as we are using MPLS secured communication line in that case we definitely require BGP protocol in dealing with because we are using Internet also by different ISP at different locations so role of BGP is to control the access, it itself acts as security filter protocol which is best suitable and reliable protocol for any enterprise network.
- MPLS is a common link between **PUNE-----DELHI-----BENGALURU** therefore any information coming through MPLS secured line face BGP for security check and then pass that information to destination router id with the AS number.
- While for our internal communication we have several departments in both regional and corporate office, situated at different floors as well thus in order to facilitate the

internet facility to the allotted VLAN's respectively EIGRP which Cisco's own protocol would be best suitable as it supports CIDR and VLSM to which we deals for our respective VLAN's created, below are the benefits listed,

- Easy transition to IPv6 with multi-address family support for both IPv4 and IPv6 networks.
- Superior scaling of Interior Gateway Protocol (IGP) for large dynamic multipoint (DM) VPN deployments
- Very fast rapid convergence times for changes in the network topology
- Only routing table changes, not the entire routing table, are propagated, when a change occurs
- More efficient use of links, through equal cost multipath (ECMP) and unequal cost load sharing

Thus BGP and EIGRP will be best suitable protocols for our network.

❖ **Network Security: -**

For Enhancing the security of our network we will be using following security measures and protocols they are as follows,

1. Access Control List (ACL):

Access control lists perform packet filtering to control the movement of packets through a network. Packet filtering provides security by limiting the access of traffic into a network, restricting user and device access to a network, and preventing traffic from leaving a network. IP access lists reduce the chance of spoofing and denial-of-service attacks, and allow dynamic, temporary user-access through a firewall.

Router(config)# Access-list [acl type] [permission] [Protocol] host [IP address applying permission] [Providing IP] eq [protocol port no]

2. Enable secret: enable password is used to set in the previous mode, it provide protection to router to configure it or going to configure in terminal port and secret encrypts the password we add.

Router(config)# enable password [secret]

Router(config)# enable secret [secretpassword]

Router(config)#exit

3. Firewall Integration: -

These firewalls include all the capabilities of a traditional NGFW and also provide advanced threat detection and remediation. With a threat-focused NGFW you can:

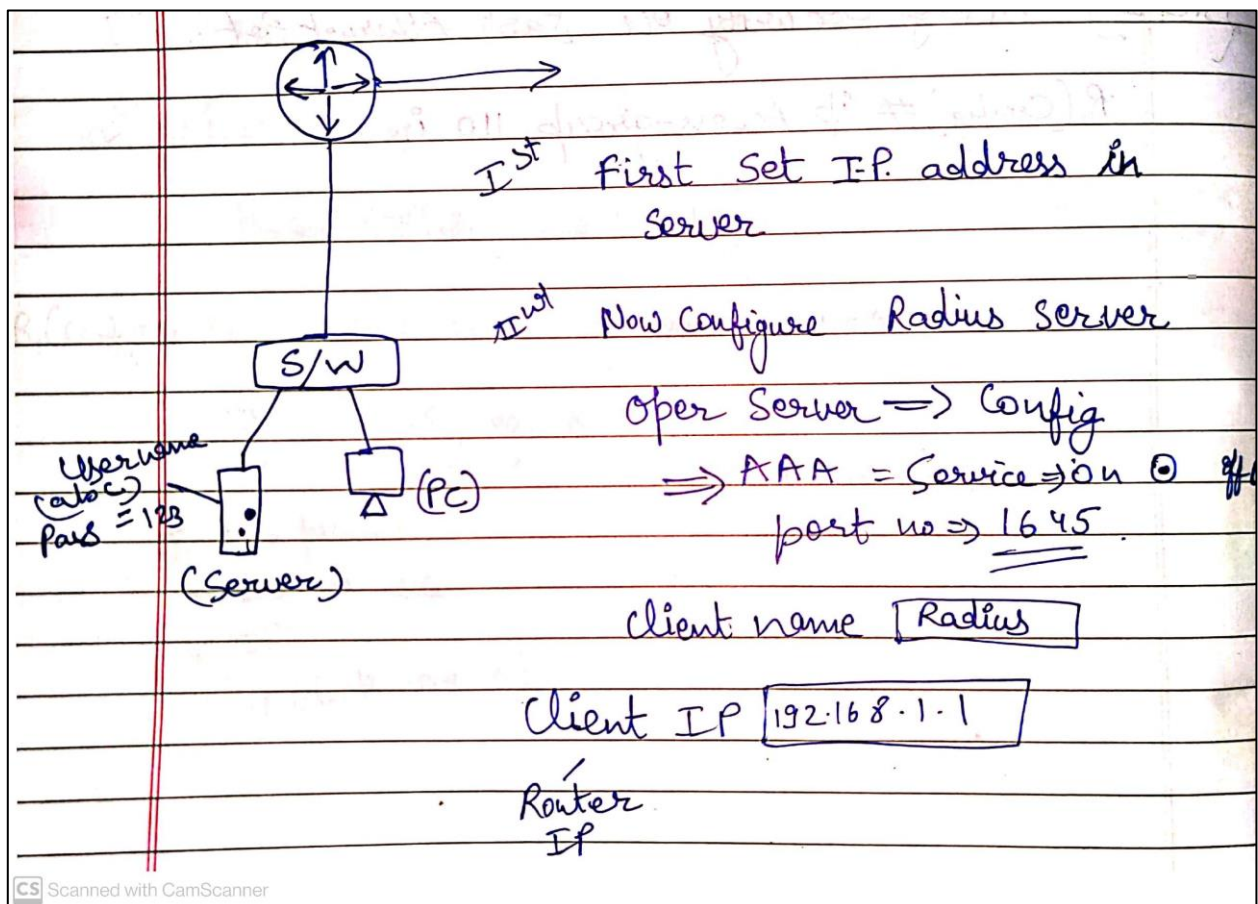
- Know which assets are most at risk with complete context awareness
- Quickly react to attacks with intelligent security automation that sets policies and hardens your defenses dynamically
- Better detect evasive or suspicious activity with network and endpoint event correlation
- Greatly decrease the time from detection to cleanup with retrospective security that continuously monitors for suspicious activity and behavior even after initial inspection
- Ease administration and reduce complexity with unified policies that protect across the entire attack continuum.

4. Radius and AAA (remote authentication dial in user service) & (Authentication Authorization Accounting):

Radius is a networking protocol, provide centralized authentication, authorization and accounting management for user who connect and use a network service. Radius server provide security for router to avoid unauthorized access and login to the router. In radius we can set user name and password for logging in the user.

It is high level security for router, in this router is connected to a **server** via gateway switch, unless until server is powered on the router will respond and if any user has to access to the router he/she needs to provide the **authentication credentials to server** and then **login to router**.

Below is the configuration of the AAA Radius security,



Secret 123 or any name Server Type Radius

Link provide to which Router for access + add

Now Set the Username password.

Username abc Password 123 + add

Scanned with CamScanner

In the above diagram we can see a router connected to a server via switch, where the login credentials of server are as **username – abc** and **password – 123** we have to add it in GUI provided, Router IP – 192.168.1.1, AAA Port no – 1645.

Router configuration:

```
R1(config)# int fa0/0
R1(config-if)# ip add 192.168.1.1 255.255.255.0
R1(config-if)# no shut
R1(config-if)# exit
```

Radius Authentication Configuration:

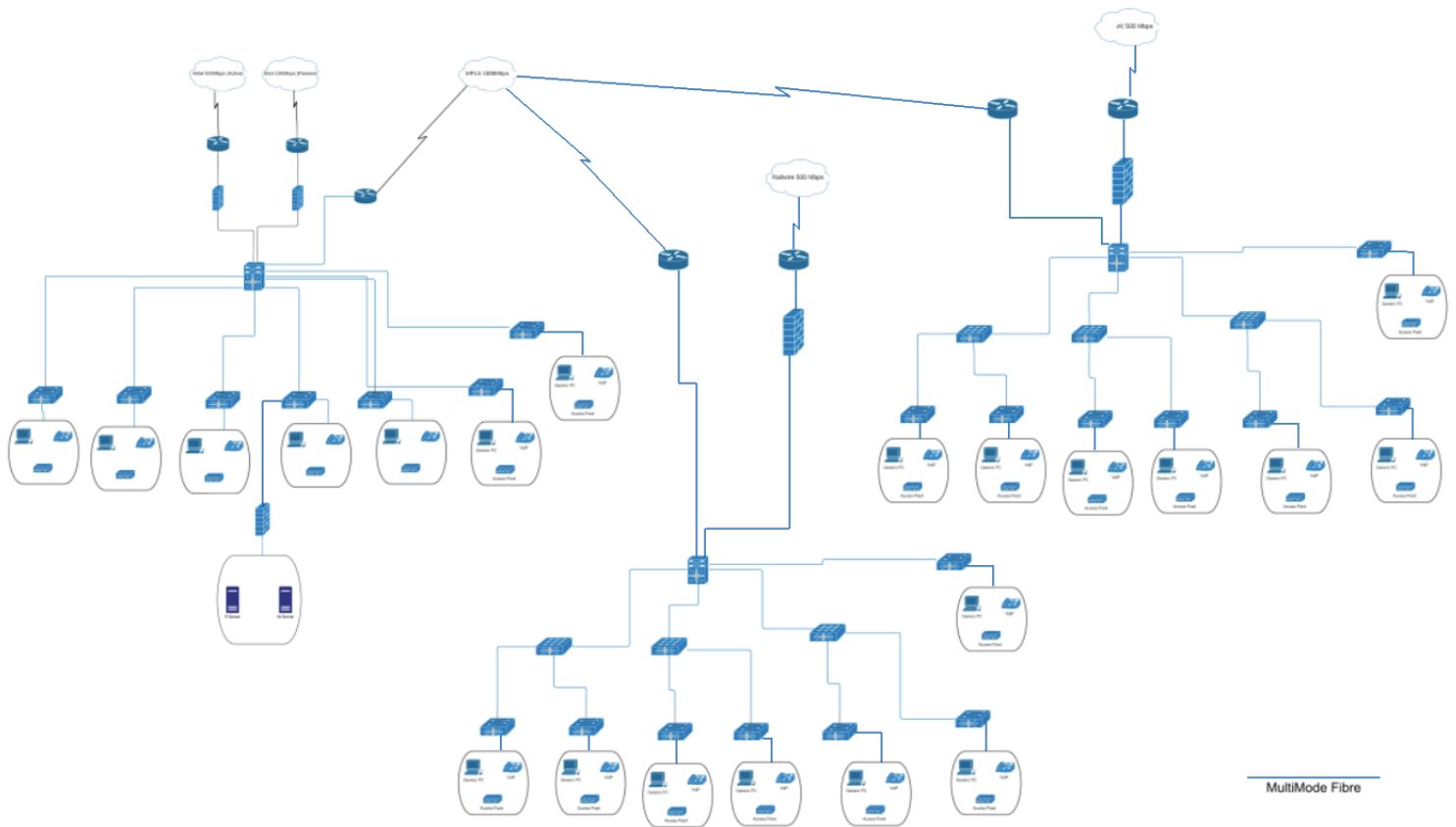
```
R1(config)# AAA new-model
R1(config)# radius-server host 192.168.1.2 auth-port 1645 key nipun
R1(config)# aaa authentication login default group radius local
R1(config)# exit
```

192.168.1.2 is the server IP to whom which we are syncing the router, and **nipun is the password** for the server login and redirection to router login.

▪ **Conclusion: –**

So in order to filter the internal communication we will use Access Control List and For the Servers and additional Firewall we require advance security as AAA and radius which allow routers to operate and login over a Device if that device is in on state the routers will work and if it is in OFF state then not work and even anyone has to access the router they have to do login first in that device and then in the router i.e. what we call as **2 factor authentication**. While Router password and firewall devices will more enhance the security by blocking and filtering Spam contents.

❖ Network Design and Blueprints: -



Network blueprint

In the above network blueprint we will explain it briefly in the below schematic diagram in 2 different parts.

Part – I (corporate office):

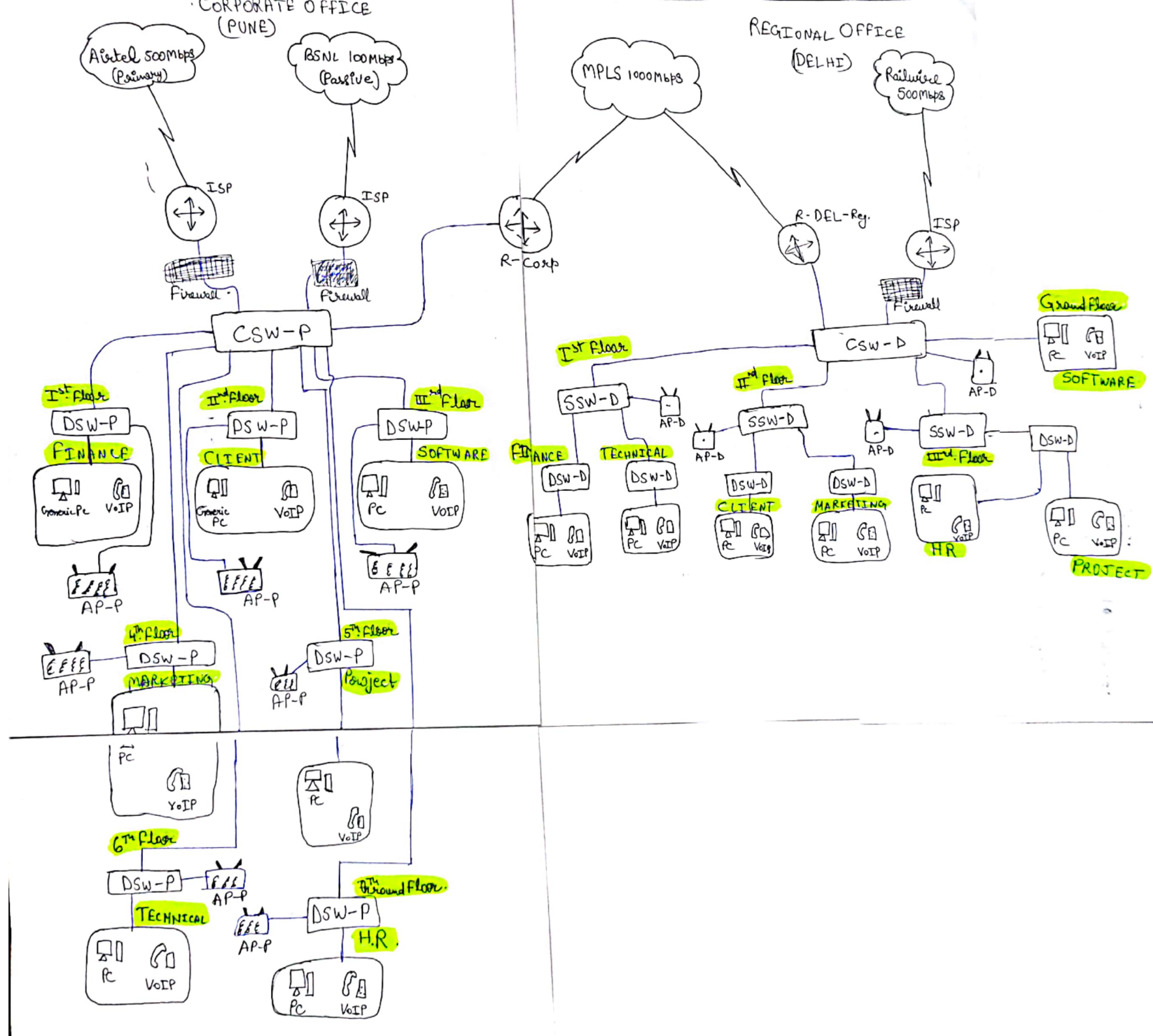
For corporate Office at PUNE we have 7 departments at each department is having specific number of employees and each department has its separate floor for operation.

So in the below diagram **Core switch** at Pune is distributed to **7 different distribution switches at all 6 floors and ground floor**.

These distribution switch provide connection to **each department at each floor** via **Multimode fiber cable**.

For better enhancement we have added **VoIP phone for every employee and 1 access Point each at every floor** for any common wireless connection.

For development and testing purpose 20 physical servers and 3 web servers are connected via **firewall** and has given access to **floor 3rd distribution switch** which has **Software Team** on that floor.



Pune Office is getting 2 Internet connections 1 is from **Airtel** and another from **BSNL** which is a backup in case if any network fails other takes over. Pune Office is connected to Delhi and Bengaluru office via 1000Mbps MPLS line.

Part II (regional Offices):

Regional offices both **Delhi and Bengaluru** have Internet connections from **rail wire and JIO** which are connected via **Firewall** which prevents/block unauthorized access or remove unwanted spams/contents.

Here we have 3 floors only and departments are 7 only so we have divided team of 2 branches at every floor in such a manner that capacity is distributed

Ground Floor – HR and Project

First Floor – Finance and Technical

Second Floor – Client and Marketing

Third Floor – Software

As we have **150 of capacity each floor** to handle, the above case conveniently fits our case.

Here the core switch is lined to **3 sub-switches located at all 3 different floors** for departments we have teamed. Each **sub switch has a Wireless access point connection** for any common wireless connection.

Each **sub-switch is giving access to distribution switch for 2 departments per floor** lined up, **at 3rd floor we have only software team**, no other department is teamed with it up as it itself is a whole.

▪ Conclusion:

Hence we have successfully completed all the task of network design and created a well-structured network and assigned them accordingly to different floors as per the given criteria, and created VLAN as well for the network provided.

❖ **Future Scope: -**

For the future purpose as it is mentioned that this network is scalable and reliable up to 3 years and each year 100% employee increment is there so we have already designed the network in such a manner that the administrator won't get any problem for configuration the things.

Below are the key features which are already prepared for the future,

1. IP and Subnet spaces available
2. Security Firewall available for any external future Domain lining up in organization.
3. Regional offices are paired up in such a manner that if employee grows in departments, sufficient space will be available and occupied by the new user
4. Pre-Configuration VLAN ID's and Subnets groups available to provide for future use as we B-27, B-26 subnet having 30, 62 hosts per subnet and there are around 3000 subnet spaces available which is more than enough.
5. Connecting our network over an International Sea link is the future implementation of our company ABC Ltd.

❖ **Appendix, Reference and On-Paper Calculations: -**

----- **Next page** -----

Corporate Office

Pune

HR (10), Finance (10), Client (30)
Software (60), Marketing (30)
Project (30), Technical (40)

Regional Office


Delhi and Bengaluru

HR (5), Finance (5)
Client (15), Software (30),
Marketing (15), Project (15)
Technical (20)

Corporate Office Floor Plan

Grand	1 st Floor	2 nd Floor	3 rd Floor	4 th Floor	5 th Floor	6 th Floor
HR	Finance	Client	<u>Software</u>	Marketing	Project	<u>Technical</u>
10/150	10/150	30/150	60/150	30/150	30/150	40/150
3Y	3Y	3Y	3Y	3Y	3Y	3Y
⇒ +30	+30	+30	+180	+90	+90	+120

* Regional Office @ Delhi & Bengaluru.

Ground	1 st floor	2 nd floor	3 rd floor	4 th floor	5 th floor
HR	Finance	Client	Software		
5 / 150	5 / 150	15 / 150	30 / 150		
3Y + 15	3Y + 15	3Y + 45	3Y + 90		
Project	Technical	Marketing			
15 / 150	20 / 150	15 / 150			
3Y + 45	3Y + 60	3Y + 45			
				X 2 (for 2 offices)	

Fibre Cabling

Fibre Cabling

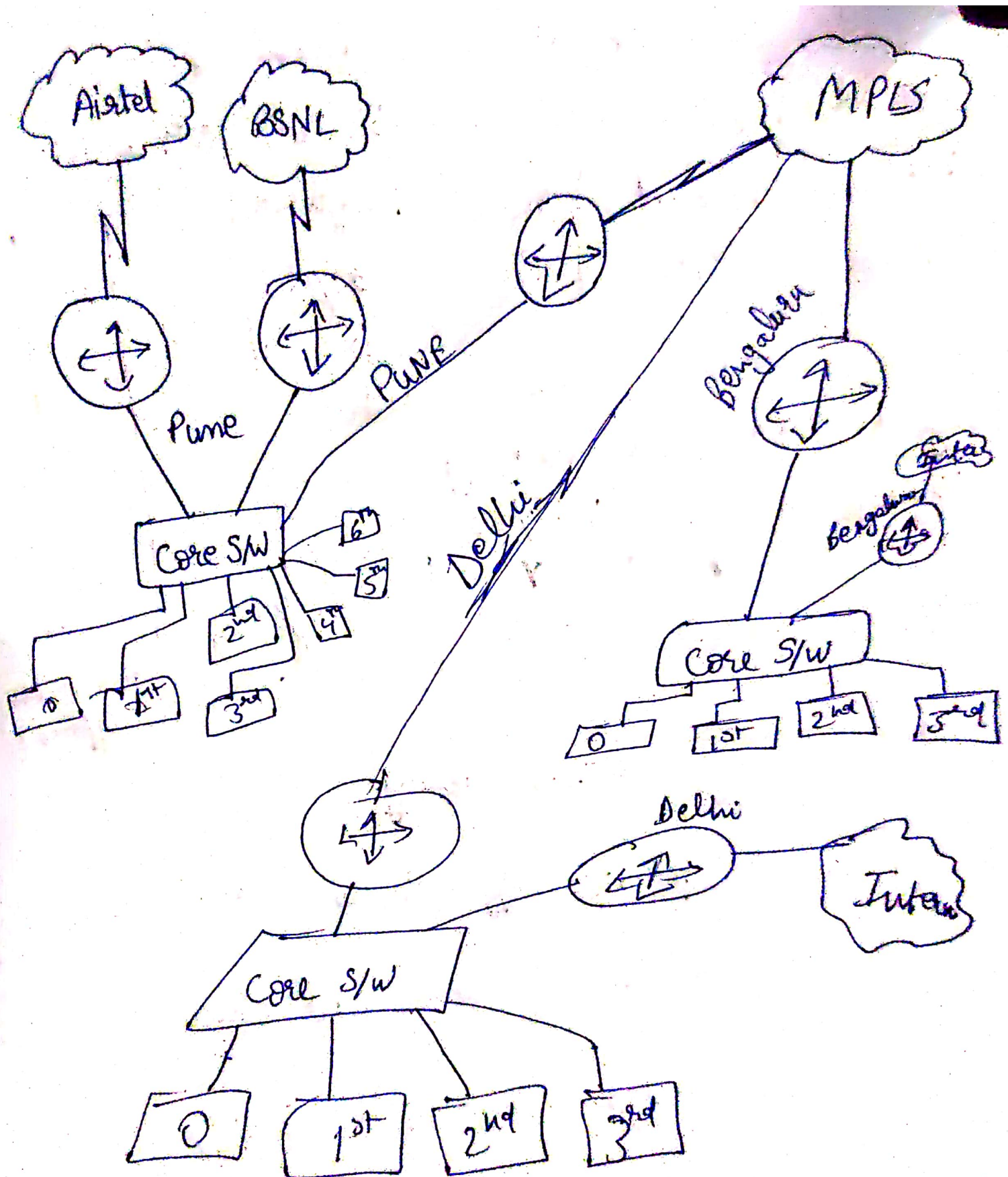
For Corporate office: we have 6 Floors
75 Mtrs of cable to cover each floor.

$$\therefore 6 \text{ Floors} = 6 \times 75 = \underline{450 \text{ Mtrs.}}$$

For Regional office: we have 3 Floors

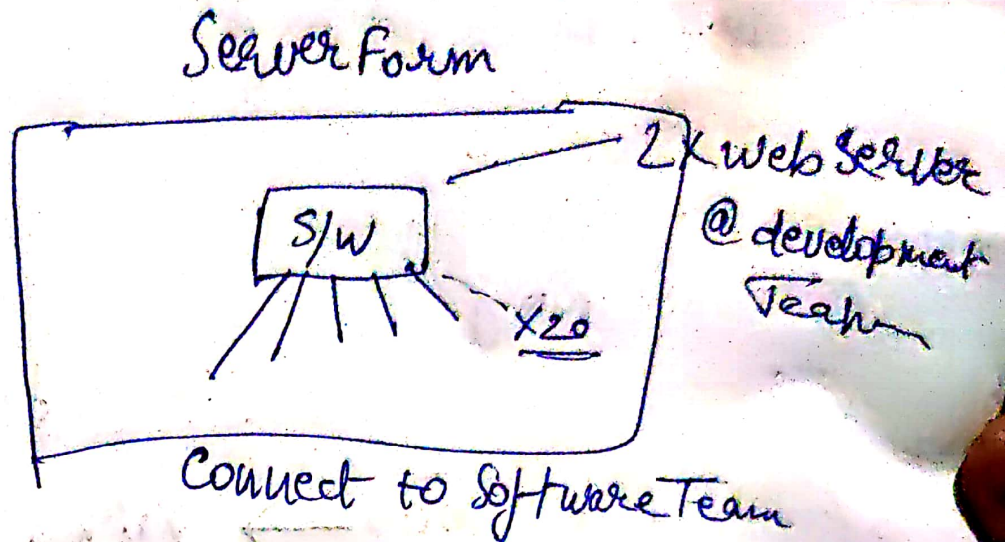
$$\therefore 3 \text{ Floors} = 3 \times 2 \times 75 = 450 \text{ Mtrs}$$

each office: 225 Mtrs



Devices \Rightarrow Data/lam, IP Phone, Access Point

* Corporate office; Server room



* Hardware Req.

Corporate. (All POB)

✓ 2 Firewall on 2 Internet Router

✓ ① Core S/W.

② Distribution S/W x6 + 1 24 Port S/W Server Room

③ Firewall to Server Room. (AAA radius to MPLS)

④ Access Point each floor $\therefore 1 \times 6 = \underline{6}$.

⑤ ~~Data~~ PC Generic & IP Phone for Internal communication

⑥ Ethernet Cat 74 MM fibre.

⑦ 3 Routers

⑧ 20 Physical Servers & 2 Web Servers.

Regional Office

- ⇒ Core S/w ⇒ 1
- ⇒ Distribution S/w ⇒ 3 x 2
- ⇒ Dept. S/w ⇒ 6 x 2
- ⇒ Access Point ⇒ 3 x 2
- ⇒ 2 Router (1 Internet)
- ⇒ Generic P.C. and IP Phones
- ⇒ Firewall to Internet.
- ⇒ Ethernet cat 7 and MM Fibre