॥ सिद्धिः भूषयते विद्याम् ॥

avantika
UNIVERSITY

Discipline

Design a Small Enterprise Network

CS5001

Assignment-4

Sheikh Muhammed Tadeeb (AU19B1014)

❖ Problem Statement:

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 start-up 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 fibre 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 Form 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.

❖ Solution:

1. Requirement Analysis:

Before designing the enterprise network, we need to decide upon the following things:

Snos.	Required Product / Service	Why we need it?
1	Hardware	They are required for communication and interaction between devices on a computer network. Specifically, they mediate data transmission in a computer network.
2	Software	Networking software is a foundational element for any network. It helps administrators deploy, manage, and monitor a network virtually to check its performance and other aspects.
3	Network topology	Network topology helps us understand two crucial things. It allows us to understand the different elements of our network and where they connect. Two, it shows us how they interact and what we can expect from their performance.
4	Network Diagram	A project network diagram is an important tool because it helps teams visualize the activities that need to be completed over the duration of a project. It also gives crucial context like task duration, sequence, and dependency.
5	Ip address and Subnets	Because an IP address is limited to indicating the network and the device address, IP addresses cannot be used to indicate which subnet an IP packet should go to. Routers within a network use something called a subnet mask to sort data into subnetworks.
6	Security	A solid network security system helps reduce the risk of data loss, theft and sabotage.

7	Scalability	Scalability for a network matter because: It impacts how well a business will be able to keep up with ever-evolving demands for network infrastructure. If a business' growth outpaces its network capabilities, this can cause service disruptions that drive customers away.

2. Network Topology:

- **Brief:**

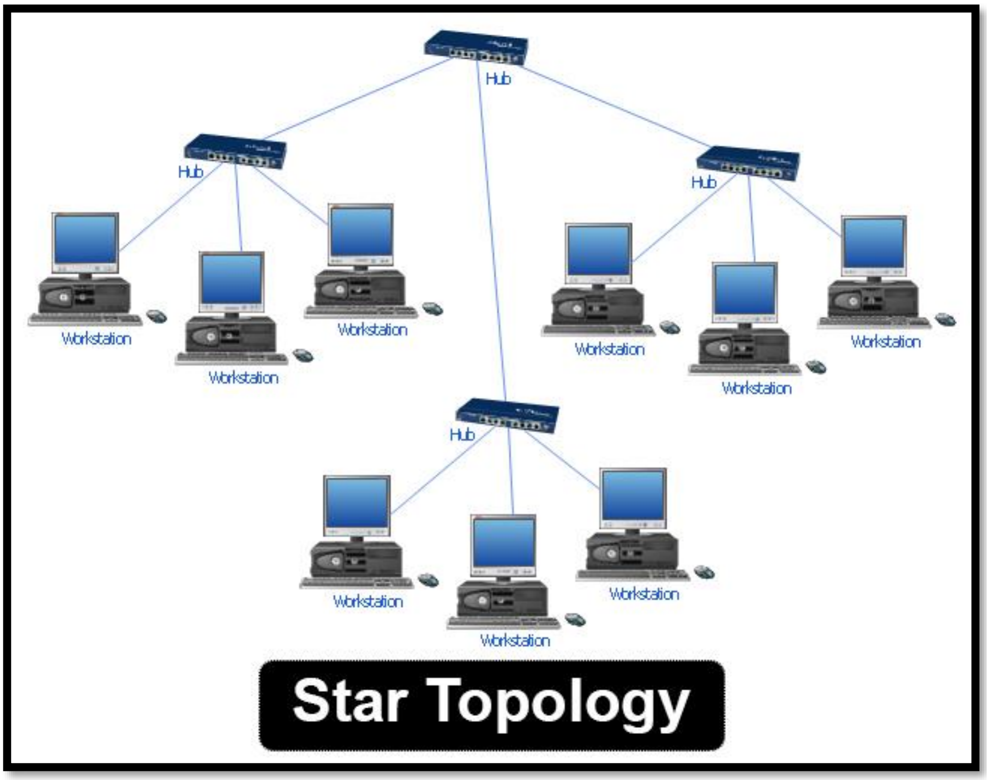
In the term of a communication network, the term topology refers to that way in which the end points, or stations, attached to the network are interconnected or it is the arrangements of systems in a computer network.

- **Why Network Topology?**

The network topology can be categorized into bus, ring, star, tree, and mesh. On the starting of this project, I am going to architect a small enterprise network, first I am going with the future proof, scalable, availability & less cabling model. By using these things, we design a security proof diagram then after we are going to implement it in the Cisco packet tracer.

- **Deciding Right Topology:**

  - **Star Topology:** In star topology, each computer is connected to a central hub using a point-to-point connection. The central hub can be a computer server or firewall that manages the network, or it can be a much simpler device that only makes the connections between computers over the network possible. Star topology is very popular because the startup costs are low. It is also easy to add new nodes to the network. The network is robust in the sense that if one connection between a computer and the hub fails, the other connections remain intact. If the central hub fails, however, the entire network goes down. It also requires more cable than bus topology and is, therefore, more expensive.



- **Pros:**

- If one node or connection breaks, the rest of the network remains unaffected. Other computers and their connections can continue working with zero downtime.

- It's highly scalable i.e., new computers/machines can be added or removed without disturbing the whole network.

- Heavy loading = no sweat. Star networks can accommodate lots of different machines, which means it's possible to create a large network.

- Star networks are safer in the event of a cyber-attack. Consider the case of the enterprise for which I am designing network with several branches. If one branch or office comes under attack, the server will be notified and prevent a second. One branch goes down, but the others continue running in complete safety.

- **Cons:**

- Each cable is individually connected to the central server, which means we’re going to need A LOT of cables. And that doesn’t come cheap. Although it’s worth noting that the upfront cost of cables is a fraction of the cost of downtime in the event of a total system failure. Most network designers think this benefit far outweighs the cable cost.
- The hub is a single point of failure, which means that if it stops, it brings the whole lot down.
- There are only so many machines you can connect to a central server before you start running out of cable length and ports. One way to get around this is to extend the star topology into multiple stars with a new central server in the middle. In this situation, messages from each system are transferred to its star, which then transfers it to the core server, then back out to the star and then to the destination system.

3. Hardware Analysis:

Snos.	Name	Model Number	Quantity	Why we are using this
1.	ASR	Cisco ASR-920-12SZ-IM	3	Effective Cisco IOS XE Release 3.16S, the Cisco ASR-920-12SZ-IM Aggregation Services Router supports Power over Ethernet (PoE). PoE is the ability for any LAN switching infrastructure to provide power over copper Ethernet cable to an endpoint or powered device.

2.	Switch 	3650 switches	Total 18 (6 in each office)	The 3650 switch gives you smart, simple, and highly secure unified access with an integrated wireless controller. Support up to 50 access points and 1000 wireless clients on each switching entity (switch or stack)
3.	Firewall 	Cisco ASA5506 series	Total 3 (1 in each office)	The Cisco ASA5506 series is Cisco's follow up of the Cisco PIX 500 series firewall. However, the ASA is not just a pure hardware firewall. The Cisco ASA is a security device that combines firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities. It provides proactive threat defense that stops attacks before they spread through the network. Therefore, the Cisco ASA firewall is the whole package and fit for our enterprise.
4.	RJ45 Cable 	–	–	RJ45, which incidentally stands for registered jack 45, is the ubiquitous Ethernet style data port found on switches, routers, and network cards. The RJ45 style connectors and ports are also commonly found on Ethernet, serial and ATM IMA cards and interfaces. However, the most common use by far is with Ethernet data connections from desktop PC network cards, Wi-Fi access points, data switches and routers in home and corporate networks.
5.	Multi-Mode Fiber cable 	–	–	A fiber-optic cable contains anywhere from a few to hundreds of optical fibers within a plastic casing. Also known as optic cables or optical fiber cables, they transfer data signals in the form of light and travel hundreds of miles significantly faster than those used in traditional electrical cables.

Note: Other device could be PC, laptops and Mobile phones.

4. Software Analysis:

Cisco Packet tracer

Packet Tracer offers an effective, interactive environment for learning networking concepts and protocols.

Key Features:

- Unlimited devices
- Customize single/multi-user activities
- Interactive Environment
- Visualizing Networks
- Real-time mode and Simulation mode
- Supports majority of networking protocols

5. Ip Address & Subnets:

○ Pune Office:

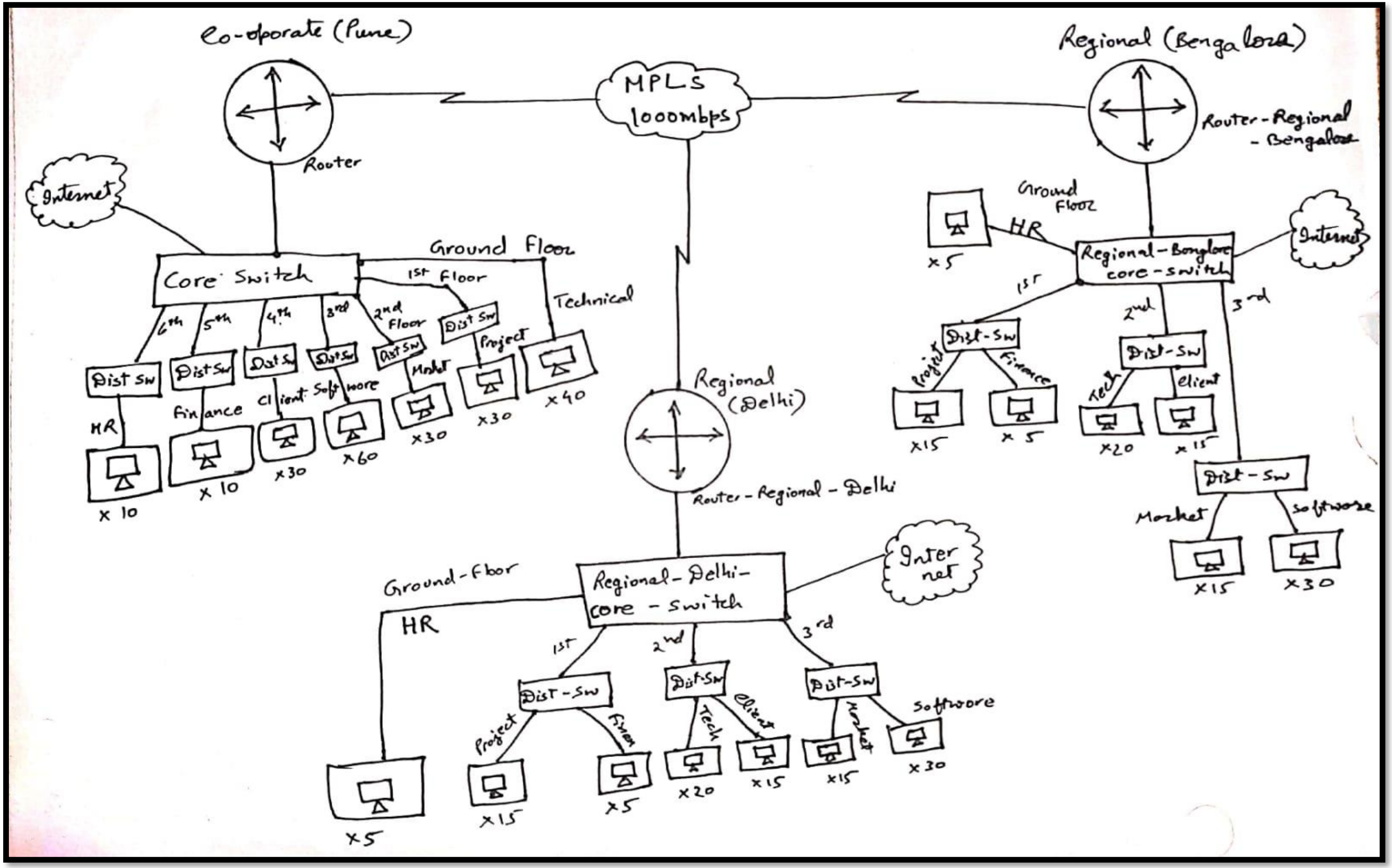
Class A IP address will be used which is ideal for industrial and corporate networks.

IP = 10.0.0.0

Subnets = 255.255.255.192 or /26

Department Name	Nos of hosts
HR	10
Finance	10
Client Engagement	30
Software Development	60
Marketing	30
Project	30
Technical Support Team	40

- **Network Diagram:**



- **Subnet Division for Corporate Office (Pune):**

Department	Network Subnets	Host Range	Nos of Host connected
HR	10.0.0.0	1-62	61
Finance	10.0.0.64	65-126	61
Client	10.0.0.128	129-190	61
Software	10.0.0.192	193-254	61
Marketing	10.0.1.0	1-62	61
Project	10.0.1.64	65-126	61
Technical	10.0.1.128	129-190	61

- **Future Scope for Rooms at Corporate Office (Pune):**

Since for this network we have 2,62,144 subnets and host per subnet are 61 (with valid IP). Therefore, subnets left will be 2,62,137

Department	Network Subnets	Host Range	Nos of Host connected
Room 1	10.0.1.192	193-254	61
Room 2	10.0.2.0	1-162	61

… so on

- **Regional Office Bengaluru:**

Here the number of hosts in each department will be half to that in the corporate office.

IP = 12.0.0.0

Subnets = 255.255.255.224 or /27 and 255.255.255.192 or /26

Department Name	Nos of hosts
HR	5
Finance	5
Client Engagement	15
Software Development	30
Marketing	15
Project	15
Technical Support Team	20

- **Subnet Division for Regional Office (Bengaluru):**

Department	Network Subnets	Host Range	Nos of Host connected
HR	12.0.0.0 /27	1-30	30
Finance	12.0.0.32 /27	32-62	30
Client	12.0.0. 64 /27	64-94	30
Software	12.0.0.96 /27	96-126	30
Marketing	12.0.0.128 /27	128-158	30
Project	12.0.0.160 /27	160-190	30
Technical	12.0.0.0 /26	1-162	61

- **Future Scope for Rooms at Regional Office (Bengaluru):**

Since for this network we have 5,24,288 subnets and each subnet has 30 hosts connectivity. We have used 7 subnets in total therefore remaining subnets are 5,24,281. This much subnets are abundant for our company so we don't need to worry for future if our company gets bigger in network size.

Department	Network Subnets	Host Range	Nos of Host connected
Room 1	12.0.0.192	192-222	30
Room 2	12.0.0.224	224-254	30
Room 3	12.0.1.0	1-30	30

… so on

- **Regional Office Delhi:**

Here the number of hosts in each department will be half to that in the corporate office.

IP = 16.0.0.0

Subnets = 255.255.255.224 or /27 and 255.255.255.192 or /26

Department Name	Nos of hosts
HR	5
Finance	5
Client Engagement	15
Software Development	30
Marketing	15
Project	15
Technical Support Team	20

- **Subnet Division for Regional Office (Delhi):**

Department	Network Subnets	Host Range	Nos of Host connected
HR	16.0.0.0 /27	1-30	30
Finance	16.0.0.32 /27	32-62	30
Client	16.0.0. 64 /27	64-94	30
Software	16.0.0.96 /27	96-126	30
Marketing	16.0.0.128 /27	128-158	30
Project	16.0.0.160 /27	160-190	30
Technical	16.0.0.0 /26	1-162	61

- **Future Scope for Rooms at Regional Office (Delhi):**

Since for this network we have 5,24,288 subnets and each subnet has 30 hosts connectivity. We have used 7 subnets in total therefore remaining subnets are 5,24,281. This much subnets are abundant for our company so we don't need to worry for future if our company gets bigger in network size.

Department	Network Subnets	Host Range	Nos of Host connected
Room 1	16.0.0.192	192-222	30
Room 2	16.0.0.224	224-254	30
Room 3	16.0.1.0	1-30	30

… so on

6. Network Security:

- **Enable MAC Address Filtering:**

  Most broadband routers will have a unique identifier called the physical address or Media Access Control (MAC) address. This address aims to improve security by limiting the number of devices that can hook up to the local area network. LAN users have the option to type in the MAC addresses of all devices in the LAN and this restricts the network to only allow connections from these approved addresses. This provides another layer of security to help keep hackers at bay.

- **Next-GEN Firewall:**

  A traditional firewall provides stateful inspection of network traffic. It allows or blocks traffic based on state, port, and protocol, and filters traffic based on administrator-defined rules.

  A next-generation firewall (NGFW) does this, and so much more. In addition to access control, NGFWs can block modern threats such as advanced malware and application-layer attacks. According to Gartner's definition, a next-generation firewall must include:

  - Standard firewall capabilities like stateful inspection
  - Integrated intrusion prevention
  - Application awareness and control to see and block risky apps
  - Threat intelligence sources
  - Upgrade paths to include future information feeds
  - Techniques to address evolving security threats

- **Benefits of Next GEN firewall:**

  The best next-generation firewalls deliver five core benefits to organizations, from SMBs to enterprises. Make sure your NGFW delivers:

1. Breach prevention and advanced security:

   The No. 1 job of a firewall should be to prevent breaches and keep your organization safe. But since preventive measures will never be 100 percent effective, your firewall should also have advanced capabilities to quickly detect advanced malware if it evades your front-line defenses. Invest in a firewall with the following capabilities:

   - ✓ Prevention to stop attacks before they get inside
   - ✓ A best-of-breed next-generation IPS built-in to spot stealthy threats and stop them fast
   - ✓ URL filtering to enforce policies on hundreds of millions of URLs

2. Comprehensive network visibility:

   You can't protect against what you can't see. You need to monitor what is happening on your network at all times so you can spot bad behavior and stop it fast. Your firewall should provide a holistic view of activity and full contextual awareness to see:

   - ✓ Threat activity across users, hosts, networks, and devices
   - ✓ Where and when a threat originated, where else it has been across your extended network, and what it is doing now

3. Fastest time to detection:

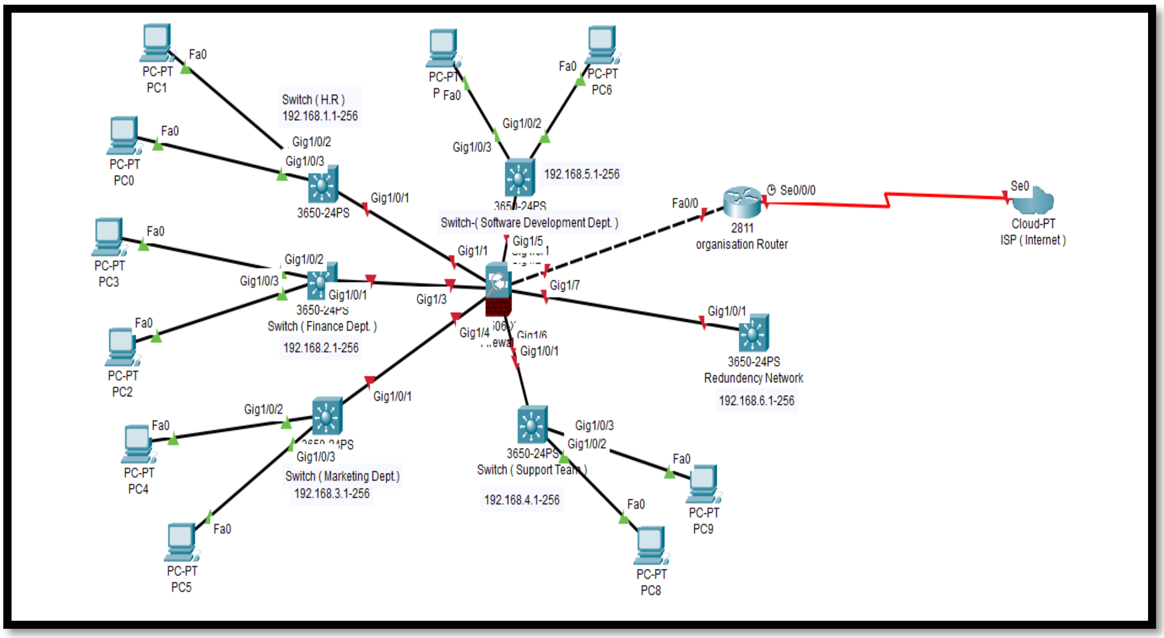
   The current industry standard time to detect a threat is between 100 to 200 days; that is far too long. A next-generation firewall should be able to:

   - ✓ Detect threats in seconds.
   - ✓ Detect the presence of a successful breach within hours or minutes.
   - ✓ Prioritize alerts so you can take swift and precise action to eliminate threats.

7. Alternative Approach to Network Design:

NOTE: This approach is different from the one explained above. I made this approach keeping or considering different networks for each department within an enterprise.

- **Network Diagram (For Alternative Approach):**



- **Explanation:**

So, in this star topology network diagram a router I used for a small organization is called the edge router and it is connected with the firewall which is connected with the different IT Department switches and then it's connected with the help of cable to desktop computers and laptops for the end user.

For accessing the internet, I gave the different IP or subnet it to the different departments like in the HR department I am using the subnet of 192.168.1.1-256 IPS which is now scalable up to 256 desktop or digital devices. Same as given to the Finance department 192.168.2.1-256, For marketing department 192.168.3.1-256, For support team 192.168.4.1- 256, For Software development dept. 192.168.5.1-256. And 192.168.6.1-256 for the redundancy.

- **Room for Redundancy:**

  All the departments have their different switches like HR, Finance, Software Development, Support Team etc. and one switch is left for redundancy purpose like if any of the network or switch will fail so it directly connects to the redundancy switch and continues their work in less than 1 minute.

- **Network Security:**

  All the connections are connected with the firewall which helps to secure our network. After the setup of Firewall, I am making some policy rules to stop the interrupted malicious activities in our network and secure as much from the hacker and their hacking activities.

  Now the firewall connects to the main router which is called Edge Router / ASR. All the main routers have some static public IP which is 103.39.133.186. It is also known as gateway IP. And it is directly connected with your ISP Which is an Internet service provider. After configuring all the things your End user devices take DHCP IP automatically from any department switch after connecting the cable or Wi-Fi in our Network.