CS425 Assignment 3 - Group 13

Arham Chopra, 14130
Gopichand Kotana, 14249
Nikhil Vanjani, 14429

Building Structure And Assumptions Underlying the Design

For the basis of our design we have considered the following building structure: Our hypothetical organization will be running in multistory building with each floor having employees of different departments. Departments will on average have around 50 employees. The total number of employees being 500 ie around 10 floors.
We assume that all the departments are mostly independent, and there comparatively less communication between the departments(ie floors) as compared to within the departments.
We assume that each floor is divided into offices/meeting rooms/public areas. All offices will have a fixed desktop PC.

Design

The building will need the following services:

- LAN for internal communication
- Wifi throughout the building
- Internet Connection
- Services like DNS, Mail Server, VPN Server
- Gateway, Firewall

Wired and Wireless Internet connection

Topology

We propose a hierarchical star topology network for connecting all the floors. All the machines within a floor will be connected by a switch through a star topology. There will be a single router to connect to the switches on all the floors in a star topology. If the floor is very large then we can create a further hierarchy of switches and routers. Thus all internal machines will be connected to each other through this tree like structure. Thus for each machine(PC, Wifi Routers) on floor, there will have a wired connection to a switch.
We propose this as star topology is more reliable and fault tolerant. Faults at any point in the topology will only disconnect that part(corresponding subtree) from the whole network and other can continue without issues. It is also easier and quicker to discover the actual locations of the faults. Using switches rather that hubs as they improve the bandwidth usage and reduce the collisions for the underlying medium used for communication.

Cabling

For the cabling inside the building we propose using coaxial cabling(thinnet) for all the connections within a floor and thicknet for connections between the floor switches and the root router.
These cables are resistant to signal interference. The thinnet cables support a distance of 185 meters, which should be okay for a floor. Between floor, thicknets will be used as they more durable and they support larger distances(500 meters).

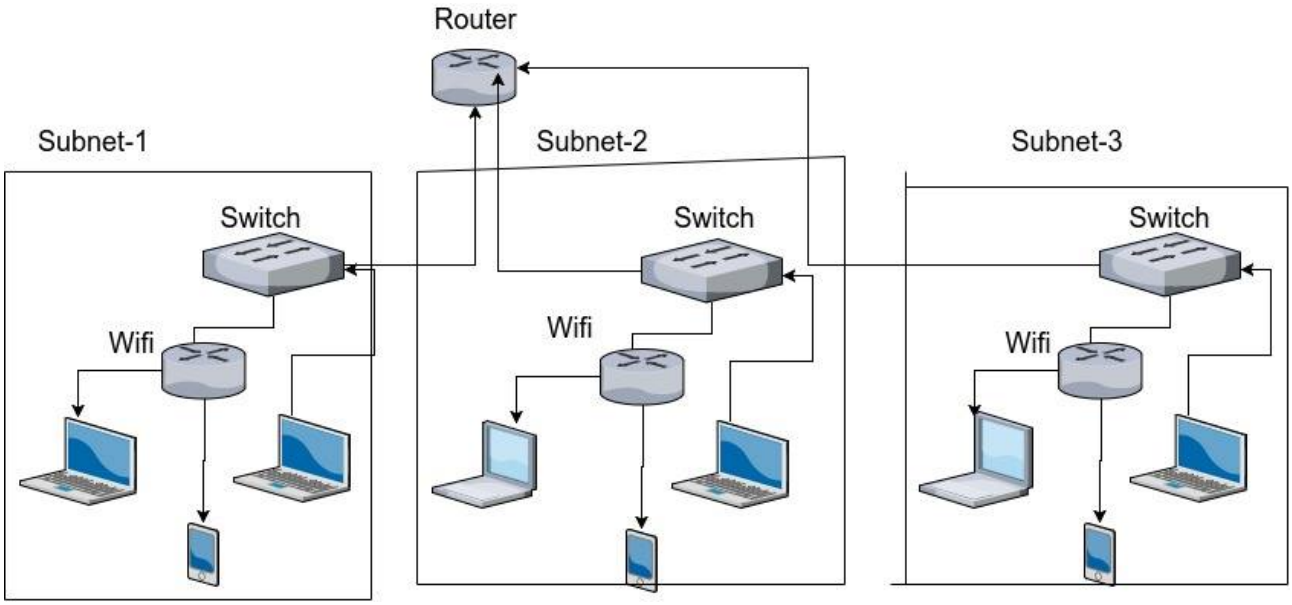

Figure 1: Overview of the Network Topology

IP Addressing

We propose dividing the overall network into different subnets on the basis of the hierarchical topology of the network. Each floor will have a separate subnet. A subnet for a floor would comprise of the switch and all children machines connected to the switch. Since the number of nodes in a subnet will be around 80, subnet masks in the range of 24-25 would suffice.
We also propose using a static ip addressing for all ports in the switches. Thus each machine(PC, wifi routers) connected by will have a static ip assigned to it. Each switch being configured to properly redirect requests in its subnet and otherwise passing on the request to its parent router. The parent router will be configured to redirect requests between the subnets(ie departments/floors)
The NAT enabled wifi routers will also provide ip addresses to the connected clients. The request from wifi clients will be "NATted" to the ip of the router in the subnet.
For certain services we will need to use static ips like the mail server and dns. Subnetting will help differentiate between the departments and thus will make packet redirection faster and easier. This would allow faster communication between all machines in a floor. Also, a logical separation of various parts of the network makes the network more secure and manageable. Using a static ip addressing will remove the need of a DHCP server and thus reduce the cost and maintenance for the company.

Internet Connection

We propose having the root router act as a gateway. Since all internal ips will be private ips, this router will perform NAT. Also, the gateway will be connected to DNS Server, Mail Server, Web Server, etc. We can then have a NAT device connecting the root router(gateway) to the outside world. We also propose to have a firewall placed after the NAT for security purposes.
Given the number of employees, 1 Gbps link to the Internet would suffice.
Gopichand elaborate a bit here The root router will be aware of all ip addresses in the network. For any destination address not present in the private it can redirect the request to the NAT. The NAT is used as there has to be some means to translate the private ips to the public ips. The NAT will also store some static ip mappings such as for the mail server and the DNS. The firewall can be used to filter the packets going in and out of the private network thus allowing control over the packets being requested from the Internet.

DNS Server, Mail Server, Web Server

The DNS Server, Mail Server, Web Server will be directly connected to the root router (gateway) for providing their service. Other similar servers will also be connected this way.

VPN Server

Often it is the case that someone from the organization is outside the building, for example at home or is traveling and he/she wants to access the network. For providing such access, a VPN Server needs to be setup. Apart from Firewall, this will be the only other public facing component so that people can directly connect to it. VPN server will have two network cards- one for the public IP and one for the private IP. Once the user authenticates himself/herself correctly, VPN server will allocate a port on private IP for the user just like DHCP does and forward the request to the root router(gateway).

Perimeter Security: Firewall/Proxy

For security at the perimeter, firewall is a must. It should be placed between the NAT and the public. The common usage of the term firewall is that of packet filter which acts on the network layer. For better security, we can replace with a application layer firewall, ie, a proxy server. As proxy servers can inspect at application layer as well, hence can take better decisions.

Demilitarized Zone (DMZ)

If the building wants to host some service which the outside world needs to access, a DMZ (demilitarized zone), isolated from the internal network should be set up for the same between the firewall and the outside world.

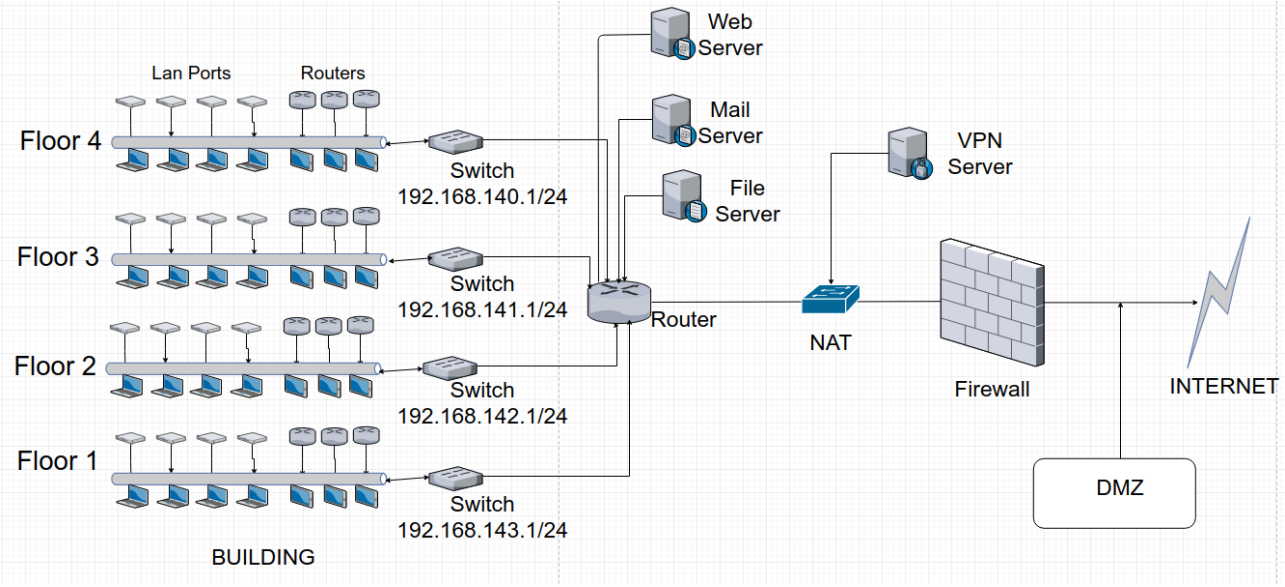

Figure 2: Overview of the Network Topology