Indian Institute of Technology Kanpur

Department of Computer Science and Engineering

Computer Networks : CS425A

Design of Network

Prepared By:

Avinash Choudhary	14158
Sagar Chand	14579
Shivam Yadav	14655

Supervisor:

Professor Dheeraj Sanghi

1 Introduction

This report deals with designing a network layout with all the nitty-gritty used in the network. Aim of this to give a comprehensive report of laying out a network for a big building organization and explain how everything is connected to each other, how is wiring done, how is communication taken place, how are we able to connect to outside world while also connecting internally, use of firewall to ensure security in the system and other technical details.

2 Wiring in every room

We would be using Star-Ring topology for connecting the computers to the network. The computers would be connected to the central switch, and also, these are wired to one another to form a ring structure. Expansion and administration of the network will be easier. Signals to and from the outside network would be transmitted and received through the central switch. Devices would be separately connected to the network through the switch and also to one another through the circle cabling which would be make broadcasting simpler and also, it is cost efficient since less cabling is required for the ring connection.

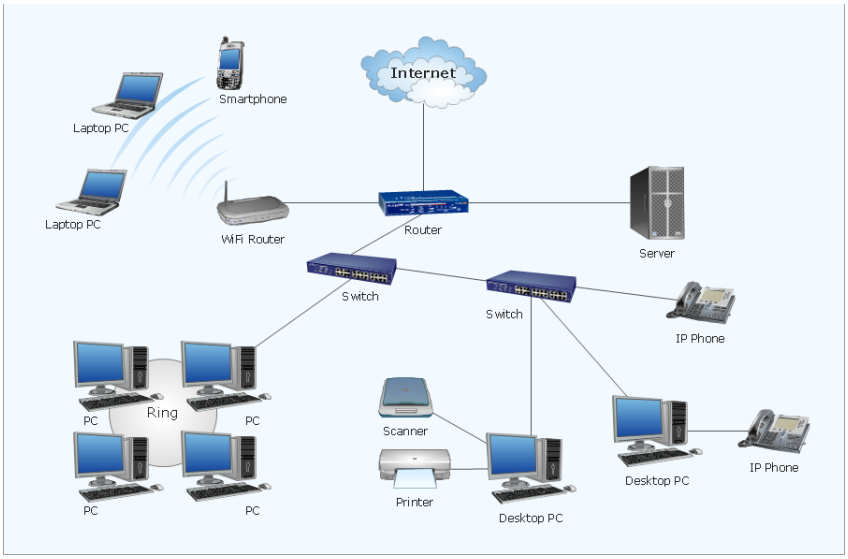

Figure 1: Basic idea of our network design

For cabling, we would be using unshielded twisted pair (UTP) CAT7 cables which support a dataspeed of upto 10Gbps over a length of 100 meters. These cables are very easy to install and expand and supports high network traffic.

sectionInternal and External Network There would be an internal database with username and passwords, which ensures that only when a user is there in that database, he can connect to internet. To connect to internal network, no authentication is required as it is trusted that there is nothing malicious in here. New user has to go to admin to get his name entered in the database.
When a user tries to connect to external network, this request goes to the router, which forwards the request to the server who in turn checks if the user is currently logged in or not. If he is not, then a session is created for the user in a particular gateway for a particular time with particular IP address. Now till the time expires, user has can access internet from that IP. It can be renewed again(more on it on DHCP) once it expires and user can keep on accessing the internet.
So in all there would be just one main router.

3 Wireless Access For Mobiles & other devices

For wireless connection, there would be a wifi router on each floor (maybe more depending upon the number of user and reach of the router) which would be connected to a switch which would then be connected to the main router. When a device connects to a wifi router, the request is then forwarded to main router and similar procedure as discussed in the Internal and External Network section would follow.

4 Accessing the internet

The main router connects the network to the internet. It connects all devices within the network to the outside internet and finds the best route for the information to be sent. It protects information and sets priority order to the devices for an information packet. Since all devices in the network would be given a private IP, a lookup table is created with entries as privateIP and port and corresponding publicIP and port. Now when a request from a device is sent to outside world, router checks if it has session running or not and then changes the source IP in packet header to a public IP and send sends the request to destination server. An entry is created for this in this table. Now when a reply comes back with addressing its public IP and a port, this is looked up into the table, corresponding private IP and port number is found, packet header is changed with destination address to private IP and packet is forwarded there.

5 Switches

Switching is a very essential part of the network. They would connect the devices on the network within the building. They would allow devices to share information and talk to each other. Managed switches would be used for the network as they are customizable. They can be accessed and programmed as per the needs of the organization, this would give the organization control over the network traffic and network access.
Thus best grade switches like TP-Link 5-Port Gigabit desktop switch TL-SG1005D would be installed in the network with sufficient data transfer rate. These switches would be easy to use and manage. They would have inline power which allows to place wireless access points (to improve the reach of the wireless access) or any other equipment which would spare the cost of installing extra electrical outlets or wiring for some functioning.
Although a router can be used to perform task of a switch but they are expensive and slower(due to higher complexity) for internal communication. Therefore good qualities switches are used for internal connection.

6 Subnet

We would divide the network into sub-networks as per the departments of the organization. It would help in simplifying troubleshooting as the network problems could be rooted down to their specific subnet. It would also conserve a large amount of IP addresses.
Subnetting divides IP addresses into two fields. One part is to identify the subnet and the other is to identify the broadcast address within the subnet. Traffic is exchanged between the two subnetworks through the switch or the router if the subnet address of the source and the destination is different, else it is confined to that particular subnet, thus reducing the broadcasting traffic over the entire network since now, there are less broadcasting domains.

7 DHCP servers, DNS, Mail server, webserver

DHCP server assigns different IP adrresses to the networked devices upon request from the devices from the range of IP addresses assigned to it by the network administrator. DHCP server would be located in the main router. So whenever a new connection is established, it will give a private IP to that device for a fixed amount of time which have to be renewed again for further continuous use.
When a client/device on the network requests a URL , the DNS server would translate this URL to a IP address and then send it back to the device.
The device then sends a message to the IP address given by the DNS server requesting the webpage. The webserver then replies by sending the webpage to the IP address of the device given by the DHCP server.
A mail server receives mails from local users as well as remote sender and transfer them to their respective clients within the network and also forwards outgoing emails for delivery. There might be more than one mail servers. So load balancing is done here. Servers which can handle more load are contacted more frequently than others.
All the servers would be connected in the main router.

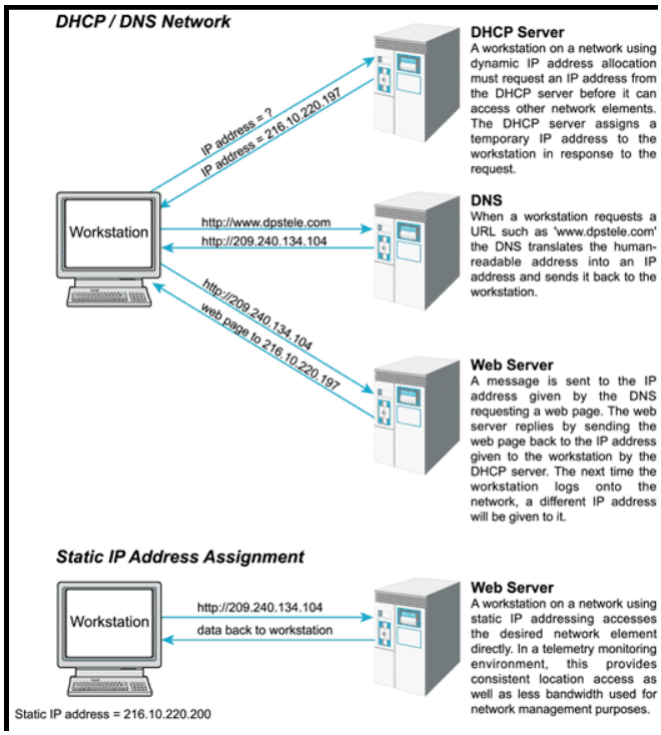

Figure 2: Wiring

8 Firewall

We will use Application Level Firewall or proxy servers as a security mechanism as they provide reasonable security compared to their price(in comparison to other types of firewall techniques like circuit level firewall, network level firewall and stateful multilayer firewall). They work on particular applications only. Their main function is to protect the internal network of an organization from trojans, malware, viruses, keyloggers, and other types of malicious programs. So instead of protecting individual hosts, they protect entire network as such. Network firewalls forward traffic to and from computers on an internal network, and filter that traffic based on the criteria the administrator has set.

A gateway from your firewall, proxy is setup to the rest of the internet. When they are setup as a web proxy, various functionalities like gopher, telnet, ftp, torrent, etc. are not allowed through the firewall. They can also be used to block a website based on the content. The downside of application level firewalls is that they are slow because they examine each data packet in a thorough manner; hence, it takes more time for the data to be filtered.

References

[1] Help from man pages, stackoverflow and various documentations are taken for the completion of this project.

[2] Article of a IT security and consulting company -Swiss Ns, has been taken as a reference for designing firewall.

[3] Article of a Technet,Microsoft has been taken as a reference for designing firewall.

[4] A figure from conceptdraw has been used to explain network connections.