Planning, Designing and Implementation of IT Networks using Network Infrastructure and Security measures

Er.Gagandeep Singh Kahlon[1] Er.Sukhwinder Kaur[2] Dr. R.C Gangwar[3]
[1,2,3]Department of Computer Science and Engineering and Information Technology
[1,2]CT Group of Institutions[3]Beant College of Engg. & Tech

Abstract— This paper gives you a brief idea about how we can design, plan and implement computer networks. The knowledge of this makes you a solid, well-rounded network designer. It trains you in multiple levels and areas regarding the ability to work with routed and switched networks. It includes the decision about which networking device to choose. How to assign IP addresses and what are the various schemes available for the same. What are the various security measures which are there for a network? It includes detailed knowledge about all the devices which we can use for designing a network. It fully develops your networking knowledge and helps you add value to any organization's network.

Key words: IDS, Router, switch, Subnetting

I. INTRODUCTION

Welcome to the exciting world of internetworking which have made data sharing very easy and fast ranging from big multinational corporations to a single user and is a widely used practice which provides multiple benefits to the people utilizing it. By reading this paper you will develop a complete understanding of the network devices, protocols, security measures which are necessary to plan, design and implement a complete computer network. The network design and planning is a step by step process in which we are concerned with the topological design of the network, the size and number of network components to be used and also calculating the capacity requirements and how to ensure reliability within a network. The task of a network engineer is first of all to choose the right devices needed for setting up the network. The different networking devices which are required to set up a network are routers, switches, hubs, networking cables, firewalls, modems, access points, clients and servers. To efficiently and effectively set up a network using these networking devices require a rational decision to be made for using them.

A. Function of each networking device and the place where it can be used:

1) Routers

A router is a device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. A router is simply a device which connects two different networks together. The main functions of a router is to forward data packets from source to destination which is known as routing and packet filtering which is avoiding those requests and packets which are useless for the intended network. The router is having number of ports in it which can be used for router to router connectivity and router to switch connectivity. The console port of the router is used to do all the configurations on the router. The picture 1 depicts the ports a router is having.

```
Router#
Router#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        192.168.100.10  YES manual up                    down

FastEthernet1/0        10.0.0.1        YES manual up                    down

Serial2/0              unassigned      YES unset  administratively down down

Serial3/0              unassigned      YES unset  administratively down down

FastEthernet4/0        unassigned      YES unset  administratively down down

FastEthernet5/0        unassigned      YES unset  administratively down down
```

Fig. 1:

The router works on the command line interface and this picture(Fig 1) shows how many ports a router is having and whether the IP address is given to a particular port or not? The router is having its own operating system installed in it which is IOS (Internetworking Operating System). The router is the most important component of the network on which different routing protocols are assigned depending upon the requirements of the network. Router is only used when we have to connect different networks together.

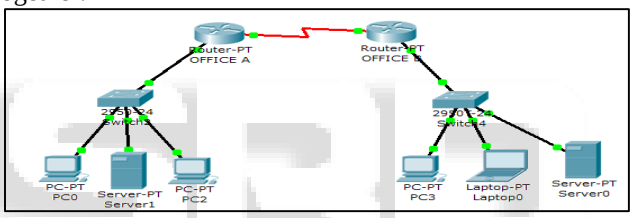

Fig. 2:

This figure shows the basic layout of a network components attached. In this figure if we want to have connectivity between departments or we want to have connectivity within a network then we will make use of switches as the network components but if we want to connect two different networks then we can proceed with the help of a router. In this figure you can see that there are two routers, one is at the Office A and the other is at the Office B. There are total three networks present in the above figure. One network is between two routers. The other two networks are connected to the routers with the help of switches, one is on the left hand and other is at the right hand side. In this research paper all the explanations are given based on the above scenario.

2) Switches

Switches are the networking devices which works on MAC addresses assigned to them. Switches work on data link layer. Switches are used when we want to have connectivity within a department, within a network, within a lab of a college. Switches are intelligent devices which are having their own operating system installed in it. Switches store all the MAC addresses in their memory. Just like routers switches are having ROM, buffer memory installed in them. Switches make use of store and forward technology to send data among different computers. All the MAC addresses of computers are stored in the MAC table of the computers and the data is sent using MAC addresses assigned to the PC. The quality of a switch is that they don't send data to all the

computers connected to them whereas in case of hubs they are performing broadcasting. The data is sent to the entire PC connected with it. Hence in case of hubs there is wastage of bandwidth of the network. In case of switches the data is sent to only the intended receiver of the message and it is not sent to the entire network. Switches can work by sending data in multicasting and unicasting manner. We can define VLANs in the switches which is a very important aspect of networking. An Ethernet switch operates at the data link layer (layer 2) of the OSI model to create a separate collision domain for each switch port. Each device connected to a switch port can transfer data to any of the other ones at a time, and the transmissions will not interfere – with the limitation that, in half duplex mode, each switch port can only either receive from or transmit to its connected device at a certain time. In full duplex mode, each switch port can simultaneously transmit and receive, assuming the connected device also supports full duplex mode.

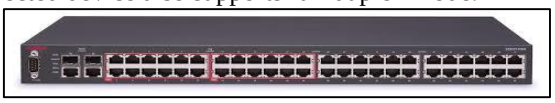

Fig. 3:

3) How to assign IP addresses to the computers in a network

There are two schemes used in subnetting, one is fixed length subnet mask and the other is variable length subnet mask. In fixed length subnet mask when we are assigning the IP addresses to the computers then some IP addresses got wasted. But in case of variable length subnet mask there is very less wastage of IP addresses because we are providing IP addresses according to their requirements. There are many reasons to perform subnetting. Some of the benefits of subnetting include the following:

4) Reduced network traffic

We all appreciate less traffic of any kind. Net- works are no different. Without trusty routers, packet traffic could grind the entire network down to a near standstill. With routers, most traffic will stay on the local network; only packets destined for other networks will pass through the router. Routers create broadcast domains. The smaller broadcast domains you create, the less network traffic on that network segment.

5) Optimized network performance

This is a result of reduced network traffic.

6) Simplified management

It's easier to identify and isolate network problems in a group of smaller connected networks than within one gigantic network.

To assign IP addresses to all the networking devices a network engineer have to first identify the number of networks and hosts present in the network. In the second step, the numbers of bits are reserved according to the number of networks. Let us take the given scenario and assign IP addresses to them accordingly. The method to assign the IP addresses is as given below.

- Numbers of networks are: 3
- Formula for finding out the number of networks is 2n. (Where n is the number of Ones in the network).
- 2n=3. Here we choose the value of n to be 2 because we can consider a slightly greater value but if we take n to be 1 then it will not satisfy the equation.
- Now let us suppose that we have given the class C for performing subnetting then we will first of all consider its subnet mask. The mask of class C is 255.255.255.0
- 255.255.255.0 is converted into binary form which become 11111111.11111111.11111111.00000000.
- Now we are having the value of n to be 2. Then the subnet mask for this will become 11111111.11111111.11111111.11000000.
- Convert the above subnet mask into decimal for that comes out to be 255.255.255.192.
- Then block size is calculated which comes out to be 256-192=64.
- Now the subnets are: If we are taking class C for subnetting

1) 192.168.10.0
2) 192.168.10.64
3) 192.168.10.128
4) 192.168.10.192

- If we want to find out how many hosts are there in a subnet then the formula for the same will be 2n-2. Here the number of hosts comes out to be 62.
- Now we can assign address to three networks given in the above scenario by using the calculated subnets and hosts.

Network security is a very complex area which can only be tackled by people who are well trained in this. There are many types of network threats which are there in the field of network security. With cyber-threats becoming a daily headache for IT security staff, it helps to have some advice, or at least know what to look out for. The ways that the networks can be compromised five years ago internally, certainly still exist. It's just that today, that list is really growing, and that's why this is ongoing research. The various threats are as follows:

The top 10 internal network vulnerabilities are:

1) USB drives.
2) Laptops and netbooks.
3) Wireless access points.
4) Miscellaneous USB devices (digital cameras, MP3 players, etc.)
5) Employees borrowing others' machines or devices.
6) The Trojan Human (attackers who visit sites disguised as employee personnel or contractors)
7) Optical media (CDs, DVDs, etc.)
8) Lack of employee alertness.
9) Smartphone.
10) E-mail.

There is a simple method of defining the Access Control Lists on the routers so as to filter the unwanted IP addresses to the network. An access control list (ACL), with respect to a computer file system, is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

7) Types of IP ACLs

a) Standard ACLs

Standard ACLs are the oldest type of ACL. Standard ACLs control traffic by the comparison of the source address of the IP packets to the addresses configured in the ACL. The standard access control lists in common do the filtering based on IP addresses of the computers.

b) Extended ACLs

Extended ACLs control traffic by the comparison of the source and destination addresses of the IP packets to the addresses configured in the ACL. The extended access control lists does the filtering based on protocols also.

Cisco Access Lists

access-list number	protocol/function
1 - 99	Basic IP List
100 - 199	Extended IP List
200+	Additional Protocols

Fig. 4:

The following table shows the numbers which we can assign to the access control lists. We can use numbers from 1 to 99 for standard access control lists. Moreover we can use firewalls and Intrusion detection systems for protecting our network from unauthorized access. A firewall is a hardware or software system that prevents unauthorized access to or from a network. They can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet. All data entering or leaving the Intranet pass through the firewall, which examine search packet and blocks those that do not meet the specified security criteria.

Internet security has become a major concern as many businesses now make their transactions online. It therefore means that the internet must be secured for business to be done. An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavours" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. So nowadays to keep our databases and knowledge bases secure is the most important criteria of designing computer networks. The main difference between a firewall and an intrusion detection system is that the firewall cannot detect an attack which arises from within a network but on the other hand an intrusion detection system is capable of detecting an attack that arises from within a network.

II. CONCLUSIONS

The main concern is the choice of right networking devices and if proper implementation of a network is done it acts as a system that provides unique capabilities to its users. In today's computer world it had become mandatory for an engineer to properly administer and maintain the computer network. The important criterion while designing is that network must be robust, scalable and reliable. It validates one's ability to work in small and medium sized businesses and organizations that use less extensive networks.

REFERENCES

[1] The DBLP Computer Science Bibliography. http://dblp.uni-trier.de/
[2] UCINET, https://sites.google.com/site/ucinetsoftware/home
[3] Pajek, http://vlado.fmf.uni-lj.si/pub/networks/pajek

