Enterprises Network

Mohd Nadeem[1], Mredul Sharma[2], Aditi Chaudhary[3], Sanjeev Kumar[4]

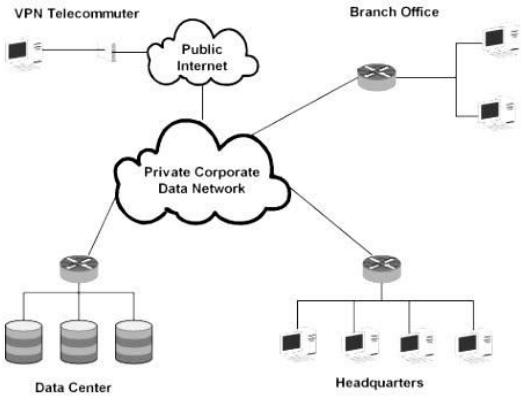
Abstract- *In this paper we are going to explain about the campus network. Campus network is an important part of campus life and network security is oriental for campus. In this network all devices are palced in right place so that all devices work well and make this network secured and optimized. A hierarichical architecture of the campus network is configured with different type of protocol. Device like router, switch L2 and switch L3, servers or PC. In this campus network there are different branch and different staff. How they communicate with its related field. Cisco packet Tracer latest version was used to design and simulate this design. Using Cisco packet tracer we can simulate application layer protocols, basic routing with RIP, OSPF and EIGRP.*

Keywords- Enterprise network, VLAN,ACL,DHCP,DNS, VLSM,NAT, different servers like g mail, face book, Network Switch, Cisco Packet Tracer.

I. INTRODUCTION

The main purpose of an enterprise network is to reduce isolated users and workgroups. All systems should be capable of communicate and provide and desired information. Campus network is essential and it plays important role for any organization network architecture and its security are important we design this network by keeping in mind the right device at place with as much as less possible cost, in today's expensive world. The devices are taken according to the network infrastructure. A campus network is an autonomous network under the control of a university. Which is within a local geographical place. The network infrastructure design has become a critical part for some IT organization in recent year.

An important network design consideration for today's network is creating the potential to support feature expansion in a reliable, scalable and secure manner. The project has been designed to create a fully equipped network. Who's whole coding and command will be properly done in the project as per requirement for the configuration of devices and required protocol. The devices are right place with as much as less possible cost in today's expensive world. The devices are taken according to the network infrastructure. A campus network is an autonomous network under the control of a university.



II. BASIC DIAGRAM OF ENTERPRISES NETWORK

Enterprise network includes:

- Networking Hardware:
  - Routers
  - Switches
  - LAN cards
  - Cables
- Networking Software:
  - Network operations and management
  - Operating systems
  - Firewall
  - Network security applications

III. PROPOSED SYSTEM

Our proposed is "Collect-experiment-analysis-decision". Based on the framework, we collected information relevant to the objectives of this paper, we implemented configuration based on the collection, analyzed the output after implementation, and proposed our decision on this paper towards optimization of network performance and security based on the analysis. The project provides a virtual working model of the network which can be implemented in the organization. This simulation of packets from each and every location in the network helps in easy detection of any error or problem in the network and also provides in checking the feasibility of any feature in the network which the organization management wants to add.

DHCP (Dynamic Host Configuration Protocol)

The Dynamic Host Configuration Protocol is basically a Network protocol which is based on a client server model. The DHCP is a concept which is based on Network management protocol used in the layer of TCP/IP protocol networks where a DHCP server dynamically allocates IP addresses to our computers. The main functioning of DHCP server is to enable computers to request IP addresses from the server, the IP addresses are provided by the ISP (Internet Service Provider) although it makes the task of administrator easier to allocate automatically IP addresses to the computers when we are having several in numbers in our network, and if we enable DHCP server then the administrator of our network should not manually assigned our IP addresses. In this a router or a residential gateway can be configure to act as a DHCP server. If we talk more about it then a DHCP server assigns a local IP address within a local network to each device connected to the network. DHCP server can also communicate with an IP network and it also provides configuration information which is related to subnet mask and default gateway. In Cisco Packet Tracer the DHCP server works as the DHCP client makes a request of an IP address by broadcasting a DHCP, as it discovers a message to the local subnet. Hence through DHCP the client is provided with an IP address through DHCP server as it responds with a DHCP offer message which is containing IP address and configuration information for lease to the client.

Hence the advantage of using DHCP server in our project is that it provides easier management of IP addresses. Without using DHCP server the administrator has to manually configure IP addresses to each device and hence if we are not using it the administrator must be careful to assign IP to each client and to configure each client individually.

DNS (Domain Name System)

Domain Name System which can be abbreviated in short as DNS. It is considered as one of the world's largest distributed databases whose main aim or function is to translate IP addresses to their corresponding human understandable or readable domain names. All internet services mainly rely on DNS as an infrastructure, which makes it as very much essential and fundamental in its nature. As all computers and systems on the Internet use addresses that look similar to 192.168.10.1. A computer always needs to understand what numerical IP address of user alphanumeric address such as www.google.comwhich is accomplished through DNS servers.
we can used the method of DNS can be used on systems without a public network connection by resolving domain name queries which are outside the perimeter of trusted hosts through a series of internal and external name servers. Hence DNS is relatively a simple protocol in which the queries which are made by a DNS client and the response which are provided by the DNS server use the same basic DNS message format.

DNS Server

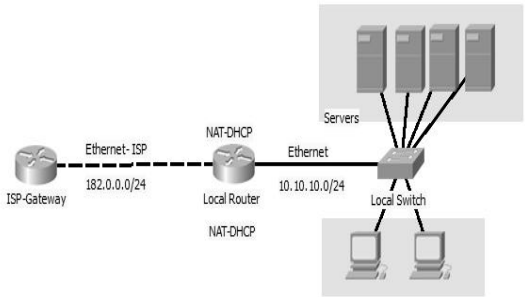
Hence now we conclude that DNS (Domain Name Server) is a server which is used to assign names to IP addresses as remembering IP addresses of each website or network is a typical task for human beings so for our simplicity we provide domain names to them. So, here in this way DNS helps us by converting our IP address number into a name. Now through DNS server we just type only name instead of IP of any website and network to search it on the browser or internet.

IV. VLAN (VIRTUAL LOCAL AREA NETWORK)

Before go to VLAN, We need to understand the working of switch and how it works.

Multiple collision domain: There are 48 port of switch which have seen in fig. has 44 collision domain that means of those port and devices that communicates with another devices with another port without coding. If multiple devices are connected with multiple ports of this switch. If one of those devices sends the broadcast that broadcast is sent by active port of that switch. There are broadcast loud. So, this is not an efficient communication. If one of the devices has IP address 192.168.1.0/24.then other devices should be the part of this IP network in a switch. For Efficient communication we use the concept of VLAN.

VLAN means breaking down this large switch into smaller switch.



ACL (ACCESS CONTROL LIST)

V. ACL (ACCESS CONTROL LIST)

In this ACL protocol, we study about the controlling of traffic flow. Suppose there are people in Sales and they want to access the server. We do not want that everybody in this team to access the server. Manager needs access to the server so manager can be able to access the server. If there is new hire and he want to access the server then the packet should be dropped and he should not get access to the server. ACL (ACCESS CONTROL LIST) is a mechanism by which we can filter the traffic depending different parameters. We can filter them according to source IP address, Destination IP-address, port number and protocols are the different mechanism by which we can identify traffic and take action according to them. If we need to block anybody from access the server. We need to deny the traffic so that he cannot access the server. The important thing when filtering to identify the traffic flow. ACL is qualifying list which contains the qualified parameter that is used to identify the traffic. ACL are of two types:-

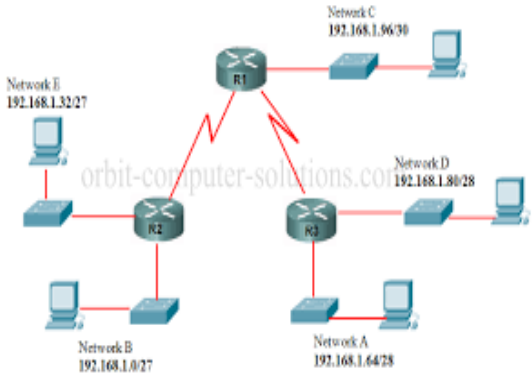
Standard Access control list
Extended Access control list

Standard Access control list is the ACL which has identification number 1-99. These are just names that identify the number of version. There is no priority. The classification is based on source IP address. So, every time when you use extended ACL, you want access traffic depending on destination IP address. You can tell only when packet coming from destination.

Extended Access control list is the ACL with number 100-199. Extended list is classified based on source IP address or destination IP address. So, every time when you use extended ACL, you want access traffic depending on destination IP address. You can tell only when packet coming from destination. It is totally depends on the data flow. It checks only the ingoing traffic. After identify the condition (incoming or outgoing). There are two possible action permit/deny. When we use the deny condition then the traffic automatically implicit deny at the end. If there is standard ACL it should apply as possible as close to the destination. If there is an extended ACL apply it as possible as close to source.

VI. VLSM (Variable length Subnet mask)

VLSM refers to summarization builds up on subletting. It was required to use the same subnet mask across the network. This was called class full networking. With increase in complexity of networks and decrease in available IP address. It becomes obvious that class full networking causes the waste valuable of IP address. To avoid wasting of IP address, classless networking was introduced by way of VLSM. VLSM allow you to use different subnet masks across the network for the same class of address.
There are few restrictions you need to consider when planning to use VLSM. You need to use fixed block size. Start by finding the largest subnet in your network. The number of host address needed to decide the size of the subnet. Next we have to assign an appropriate mask to the largest subnet using the block size. Take the next subnet that is available and then again subnet it to accommodate your smaller subnet. Repeat the smallest segment



VLSM DIAGRAM

EIGRP (enhanced interior gateway routing protocol)

EIGRP is advanced distance vector routing protocol it means it has two quality distance vector and as well as link state routing protocol. It is standard protocol initially it was CICSO proprietary. EIGRP is class less routing protocol it means it support FLSM, VLSM and CIDR. EIGRP includes all features of IGRP , IGRP was class full protocol. Maximum hop count is 255 (by default 100), administrative distance is 90. It uses DUAL (diffusion update algorithm) to find best route , it support IP,IPX and APPLE TALK protocol. EIGRP convergence rate is faster than RIP and OSPF. update are through multicast (224.0.0.10). EIGRP use split horizon rule by default in its algorithm its mean it not accept the traffic which are generated by own. It is hundred percent loop free class less routing protocol.

EIGRP MAINTAIN THREE TABLE which are neighbor table, topology table and routing table. Neighbor table contains list of directly connected routers, Topology table contains list of all the best routes learned from each neighbor, Routing table contains the best route to the destination.

EIGRP depend upon 5 things bandwidth,delay loading, reliability,MTU.-

EIGRP MAINTAIN FIVE PACKETS :-

1 Hello
2 Update
3 Query
4 Reply
5 Acknowledgement

VII. CONCLUSION

The process of design a good network requiresConcerted efforts by network designers and technicians, who identify network requirements and select the best solutions to meet the needs of a business. The four fundamental technical requirements of network design are scalability, availability, security, and Manageability. Our Purpose is to just design an enterprise network only for software based not practically.

The main Purpose of this paper is:

- Enterprise network design overview.
- The benefits of enterprise network.
- New design methodology

This is the small model which can be used for packet transmission over the network which is secure and optimized with the help of protocols used here. Placing the right device at the right place with the different functionalities of the protocols creates the secure and optimized network which helps in the packet transmission over it.

REFERENCES

[1] Andrew S.Tanenbaum, D.J. (2010). Computer Networks (5^{th} edit.)
[2] Todd lammle (routing and switching).
[3] www.packettracertrivia.com-
[4] www.en.wikipedia.org
[5] http://www.ciscopress.com/articles/article.asp?p=31276
[6] [R1]: Sarabjeet Singh Chugh “Impact of Network Address Translation on Router Performance ” . ity,” Characterization Study of VLANs in a Campus Network” .
[7] [R2]: Minli Zhu and Mart Molle Computer Science Department University of California, Riverside mzhu@cs.ucr.edu ,” Design and Implementation of Application-based Secure VLAN” .