SECURE AND OPTIMIZED NETWORK FOR RESEARCH ORGANISATION

Nisha Rani, Gauri Kamboj, Abhinav Goel and Prof. Sanjeev Kumar

[1]Department of Computer Science and Engineering, ABES Institute of Technology, Uttar Pradesh, India

ABSTRACT: In this paper, we are going to explain that how to make a secure and optimized network for research organization. In this network we will explain that right device should be placed at a right place so that all devices work well and make this network secured and optimized. In, this network we have used different types of protocols that are used to provides security. We have used various devices in this network such as routers, switches, servers, personal computers and different types of protocols.

KEYWORD *-Security,Optimization,Protocols,ACL,DNS,DHCP,NAT,VLSM,TELNET,TFTP and Simulation.*

1. INTRODUCTION

This paper "Secure and optimized Network for a Research Organization" has been created as putting the right device at the right place with as much as less possible cost has now become essential in today's expensive world. The requirements according to the infrastructure and the overall cost are major factors in determining the idealness of the designed Network. There are a lot of factors which play a major role in the efficiency and security for a research organization. After designing it is also necessary to check whether there is any error or flaw in the design of the network. For this we also have to simulate the network. The project has been designed to create a fully equipped network for a research organization who's whole coding and commands will be properly done in the project as per requirement for the configuration of devices and required protocols.

2. Abbreviations and Acronyms

ACL(Access Control List),DNS(Domain Name System),DHCP(Dynamic Host Configuration Protocol),NAT(Network Address Translation),VLSM(Variable Length Subnet Mask),TFTP(Trivial File Transfer Protocol).

3. Proposed System

The goal of the project is to design a safe, secure and efficient network for a research organization to get a whole understanding about which device will be best to be placed in which section of the organization so as to get best at least such that all required functionalities of the organization are not compromised. 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.

3. PROTOCOLS USED

3.1 VLSM (Variable Length Subnet Task)

VLSM refers to summarization builds up on subletting. It was required to use the same subnet mask across the network. This was called classful networking. With increase in complexity of networks and decrease in available IP address. It becomes obvious that classful 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.

3.2 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.com which 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.

3.3 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.

3.4 ACL (Access Control List)

For 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 is 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 and 1300-1999. 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 and 2000-2199. 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 ingoingtraffic. 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.

3.5 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.

Logically group

Segment broadcast

Subnet correlation

VLAN means breaking down this large switch into smaller switch.

3.6 VTP (Virtual Local Area Network Trunking Protocol)

VLAN is a logical way of grouping. suppose we have two switch and we have put them in trunk when any packet goes out of the network then trunk send all the traffic coming from switch to the next switch. Trunk is a communication that is used to connect from one switch to another switch.

3.7 NAT (Network Address Translation)

The **Network Address Translation** can be abbreviated as NAT. In Network Address translation we talk about addresses which are assigned dynamically. As it name suggests it translates our IP addresses. NAT consists of two types which are Static NAT and Dynamic NAT configurations. Static NAT is used when a network device which resides inside a private network is used to be accessed from the internet. Dynamic NAT can be used for mapping purposes like for example in this private IP address are mapped with public IP address from a group of public IP addresses and it is also called as "NAT pool". It also allows hosts on a

private network that have IP addresses to access a public network such as the internet. Dynamic NAT functioning also explains or occurs when a router assigns an outside global address form a predefined address, or pool of address to an inside private network device. The NAT advantage is that it hides our PC's from external networks, so that no unauthorized person can determine the IP addresses of the private computers or that individual hosts are not directly accessibly from the public internet. There are a couple of main concepts that also must be reviewed and understood before configuring NAT.

Inside and Outside Address

In typical NAT configurations, interfaces are being placed into one of the two categories or locations which are: *Inside or Outside.* Inside indicates that the traffic which is coming from an internal network is from within the organizational network and Outside indicates traffic that is coming from an external network that is outside the organizational network.

Inside local address: As its Name suggests this is the inside address which we seen and used and observe within the organizational network.

Inside global address: This is the inside address as it is seen and used on the outside of the organizational network.

Outside local address: This is the address which is used in outside as it seen and used within the organizational network.

Outside global address: This is the outside address as it is seen and used on the outside of the organizational network.

3.9 TFTP (Trivial File Transfer Protocol)

TFTP can be stand as a version of FTP that is FILE TRANSFER PROTOCOL. In creating a secure and optimized network, we have used TFTP to transfer the data or information between two devices. The data can be send and receive between the two devices or computers using TFTP. User authentication is not supported by TFTP. The objective behind the creation of secure and optimized network is to provide a network which is well efficient and cost effective so at this point, fewer resources are used by TFTP which can be counted as an advantage over the FTP. Transferring of file between client and server but doesn't provide user authentication is the task. It uses UDP. In this Network, TFTP is also used for the router backup.

As if any fault creates and there is a loss of router data so we can have a solution to a problem with the help of TFTP. It is used for the backup of the router. As if there will be the backup so there will be no limitation i.e. Loss of the data or information which will help to make the created network secure and more efficient. On the other side FTP used to send and receive files from the remote computers .Difference is that here, initially authentication need to be done by the way of validating username and password . Once it is done we can transfer the files between two systems.

3.10 TELNET

Across the network, a device can be remotely connected with the help of TELNET. Basically in simpler way, we can say telnet is used for the communication. Telnet stands for the telecommunication network. Telnet can be used for full access. Data sending and data receiving is the working of telnet with the credentials user id and password. Telnet used in LAN (local area network) to provide a bidirectional interactivity which helps in communication facility.

Communication over the network can be justified with the full access of the data or a file. Through Telnet, an administrator or another user can access someone else computer remotely. Using Telnet, we can log on as a regular user with privileges.We may have been granted to the particular application and data on that computer. On using telnet protocol a user can log on to any other device or computer on the network.

4. RESULTS AND DISCUSSION

This section all the results of the modules is discussed. The packets are if successfully transferred from one location to another as we can see clearly in the simulation after full connection and configuration then we can conclude that those locations are properly connected. Thus for final validation we just have two drop packets from select packets option and check the proper connectivity using the simulation mode for each location in the designed network and we can say that the network that we designed become a secured and optimized. All the packets are transmitted in optimized way. They selected the best way using these protocols and transmitted the packets.

5. CONCLUSION

Lastly we can conclude that it is very difficult to estimate the transferring of the packets or information over the network without any secure and optimized way. So this model of the network can allow an organization to test the transmission of the packets over it and can use it for their benefit. As it is cost effective and efficient way to come over the limitations and also helps to check whether there is any fault or error in the path of data flow. 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

- A Tutorials attached with CISCO Packet Tracer.
- Vocational Training material provided by ALTTC.
- Andrew S.Tanenbaum, D.J. (2010). Computer Networks (5th edit.)
- Routing TCP/IP by Jeff Doyle
- Wireless Home Networking For Dummies.

- www.learningnetwork.cisco.com- Last sited on (Date)
- www.freeccnalab.com
- www.en.wikipedia.org
- www.packettracertrivia.com-
- www.whatismyip.com
- www.cisco.com/web/learning/PacketTracer.html