FAULT TOLERANT ENTERPRISE NETWORKS FOR LARGE SCALE ORGANIZATIONS

BY

NITESH KUMAR

108CS074

Under the Guidance of

Prof. P. M. KHILAR

Department of Computer Science & Engineering

National Institute of Technology, Rourkela

Rourkela-769 008, Odisha, India

CERTIFICATE

This is to certify that the thesis entitled, "**FAULT TOLERANT ENTERPRISE NETWORKS FOR LARGE SCALE ORGANIZATIONS**" submitted by **Nitesh Kumar (108CS074)**in partial fulfilment of the requirements for the award of **Bachelor of Technology degree** in **Computer Science & Engineering** at National Institute of Technology Rourkela is an authentic work carried out by him under my supervision and guidance.

To the best of my knowledge, the matter embodied in the thesis has not been submitted to any University/Institute for the award of any Degree or Diploma.

Prof. P. M. Khilar

Department of Computer Science & Engineering

National Institute of Technology

Rourkela-769008

ACKNOWLEDGEMENT

I avail this opportunity to extend our hearty indebtedness to our guide Prof. P M Khilar, Computer Science Engineering Department, for his valuable guidance, constantencouragement and kind help at different stages for the execution of this dissertation work.

Nitesh Kumar

108CS074

Department Of Computer Science & Engineering, 2012

NIT Rourkela

ABSTRACT

Enterprise Networks are private computer networks that are owned by a single organization in order to connect their various offices in order to share computer resources.

Enterprise Networks are different from other networks in a sense that an enterprise network may or may not completely comprise of uniform type of network. Often it is a combination of different type of networks like Ethernet, wireless, Voice over IP, etc.

Enterprise Networks are very secure and robust in nature. An attempt has been made to provide different examples of how a network designer or a network manager can make good use of the available protocols and known methodologies. Enterprise networks vary from other networks in terms of their sophistication and robust nature.

As far as the design principles of Enterprise Networks are concerned a network designer must ensure the security of the network along with all the properties mentioned in this document. These networks require a lot of configuration expertise and experience from the network designer and the network manager.

This document explains the best practices done in the designing and troubleshooting of Enterprise Networks for Large Scale Organization.

List of Figures:

Index

CHAPTER 1

Introduction to the basics of Networking

1.1 Introduction:

Enterprise networks are computer networks owned by a single organization in order to connect its various offices across a wide area. The enterprise networks are often very complicated and sophisticated networks.Enterprise Networks are more often called Enterprise Private Network in order to differentiate them from pubic networks and explicit clarification Enterprise Private Networks are complex and use a combination of various different types of networks like wireless, IP Telephony, Ethernet, etc.

Designing a network is the first step of fault diagnosis and probably the trickiest one too. At this stage a network designer has to keep in mind many aspects of this process. In order to give a detailed explanation of how one should start designing a robust and secure network the process is divided into three parts. These parts are enumerated as follows:

- Things to consider while designing the network
- Steps involved in designing the network
- Troubleshooting the network

1.2 Things to consider while designing a network:

1.2.1 No. of independent Departments or Offices

These are the designs a network designer has to make when he has to design a network for some company or institutionhaving a huge infrastructure including many sub-sections or departments. This is where the concept of Virtual Local Area Network comes into play.

Every organisation, be it an enterprise or an educational institute comprises of various different departments or offices. Each of these departmentsmust have users that need the organisations resources.

Hence they must be connected to the enterprise network. So, the first step is to consider the number and the type of users that work at different locations and departments in the organisation.

1.2.2 Categorization of nodes for creating VLANs

A network designer must see all its users or hosts as nodes that have certain requirements and rights. All the users in a network cannot be given equal access rights. For example, the workers at lower departments might not be allowed to know or have access to higher level news or resources. On the other hand managerial staffs who are higher in the concerned hierarchy must have more privilege, hence more access to the network resources. The designer has to divide the network in such a way that every one gets access as per his or her clearance level.

Virtual Local Area Network is a very useful way of doing that. It comes with a lot to offer and can really come in handy. It is easy to configure and debug. We can do the user classification using this method.

VLANs also quarantine the broadcast storms. Broadcast storms cause a lot of traffic problems in IPv4. Using VLAN method we can break broadcast domains. Hence the broadcasts are limited to their own broadcast domains.

Other benefits of VLANs include the flexibility and security that comes with it. Users from different geographical location can be put in same VLAN. Hence they get same kind of accessibility. This gives a lot of flexibility to the network designer. Also if the network designer does not intend to give access to some particular users he can do that using VLANs. This enhances security of the network from internal hosts too.

1.2.3 The Big Question: IPv4 or IPv6?

One of the most important decision that a network designer hast to take these days is the selection of the version of Internet Protocol.

Internet Protocol is essentially the network layer. Almost all of the tasks related to routing the packets from sender to receiver is done by this protocol. The logical addressing of devices based on which they are recognised in an internetwork is done by the Internet Protocol. Other protocols at the network layer just exist to support the Internet Protocol. So, choosing the version of this protocol is really an important decision.

The current version of Internet Protocol i.e. IPv4 is almost 30 years old. It is working extremely well and provides all the features that are actually required to run and maintain a network. The main problem associated with the use of IPv4 is the lack of available IPv4 addresses. It is depleting at a very fast rate. Hence it is hard to get. Moreover, Internet Protocol's new version i.e. IPv6 comes with a lot of promises. It gives a network designer a lot of new features and flexibility. There are many things that IPv6 has to offer in the field of computer networking. The main problem associated with the use of IPv6 is the lack of support but recently many device vendors have added the support for IPv6. It is only a matter of time before IPv6 becomes the Internet Protocol in use. Another problem associated with the use of this protocol is that the network designer has to take care of the fact that all the devices used in the network are new. Older devices lacked the support for IPv6.

1.2.4 Subnetting – No. of users per subnet

Subnetting is one of the most crucial parts of network design.Subnetting, by definition, means dividing a network in partsforassigning IP addresses in an optimal way so as to optimizethe utilization of network address space.Users in a network which need to communicate using switchingmust be in the same subnet.

Subnetting is very important step in planning for a network. The network designer must have complete information about the total

number of users. This makes his job easy as he is supposed to use this information to create VLANs and do the subnetting process. Subnetting helps to utilize the address space more efficiently. Classless Inter domain Routing (CIDR) is used to achieve this. Using CIDR the network designer gets the flexibility to use classless addresses. This way he can decide which subnet gets how many users.

1.2.5 Block size of every subnet

Every subnet needs to have proper no. of IP address available forevery valid host. For every subnet the 1st address correspondsto the subnet ID and the last address corresponds to the broadcast address of that subnet. Hence it is safe to say that every address in a subnet excluding the subnet ID and broadcastaddress can be a valid host address.The network designer has to decide the subnet mask based on the number of hosts available or no. of addresses required forassignment to nodes.

1.2.6 Available Global IP addresses

Global IP addresses are provided by the ISP which reallycosts a lot. Not every host in a network can be providedwith a global IPaddress. This is why we use private IP addressinside a network and global IP's are converted to local IP while packets are received and vice versa.This is where the concept of Network Address Translationcomes into play. NAT is run on the external routerwhichhandles the translation. It is important to understand thatprivate IP addresses are not recognizable across the Internet.

1.2.7 Managing Spanning Tree Protocol

There are often times when a network designer might encounterloops in his network. It happens very often that certain active links have to be shut down to avoid the loops.In a huge network it is vary hard to find loops and shut specificlinks in order to avoid them. So this is done dynamically usingSpanning Tree Protocol. These days most of the switches availablein the market have STP enabled. This is a great boon for network managers.

1.2.8 Which routing protocol to use?

There are a bunch of routing protocols available some of which are proprietary others are open to all.Some of these are enumerated below:

1) RIP – Classful, Max. Hop Count = 15, Broadcast based.

2) RIPv2 – classless, Max Hop Count = 15,

Multicast (224.0.0.4) based

3) EIGRP – Enhanced Interior Gateway Routing Protocol.

Cisco Proprietary.

4) OSPF – Open Shortest path First (open standard)

Suitable for huge networks.

1.3 Steps involved in designing the network:

1.3.1 Deciding which types devices to be used

It is a very important decision to make. The network designer is supposed to choose from a big list of vendors who make networking devices. Most important among the many constraints that remain on board are the financial ones along with the technical expertise of the

network designer himself. The network designer has to choose on the basis of cost, availability and services. He must choose from the best alternative.

1.3.2 Deciding the required network topology

In theory there are many networking topologies available but practically, it is very hard to stick to a single topology such as mesh or start topologies. So, the network designer must try to make the best choice possible by choosing a hybrid network topology. Hybrid network topologies are a combination of different topologies. The network is designed based on the network requirements. Hence, sticking with a single network topology might not be the best way to go about it.

1.3.3 Connecting these devices with proper cables

The network designer must have enough expertise and experience to know what kind of cable would suit to the needs of the network depending on traffic at a particular interface and compatibility issues. Some of the options are Straight-through cable, cross over cable and serial links. As far as connecting layer 3 switches is concerned, there are two types of devices. One router acts as a Data Communication Equipment (DCE) and the other as a Data Terminal Equipment (DTE). The device acting as DCE must provide the clock rate to the DTE so that the two devices have synchronised clocks.

The network designer must configure the DCE with a standard clock rate value.

1.3.4 IP Addressing

IP addressing is the main task in the network designing process. The concepts of Classless Inter Domain Routing and Variable Length Subnet Mask are used for subnetting. All the devices are configured with the corresponding value of IP address Subnet Mask and Default Gateway either statically or dynamically. Doing the IP addressing manually for a large scale organization can prove to be a really hectic task. In order to do this dynamically a very widely used protocol is used. It is called Dynamic Host Configuration Protocol (DHCP). The default gateway is made to act like a DHCP server. All the host connected to it get their default configurations from the router acting as default gateway.

1.3.5 Implementation of Variable Length Subnet Mask

VLSM is implemented during the process of subnetting. VLSM being a conceptual method is very widely used or subnetting. The whole concept of subnetting is based on the method of VLSM.

1.3.6 Assigning other details like hostname, passwords etc.

Every node in the network must have a hostname, a password etc. These details are for the purpose of convenience of the network manager. Every switch and the routers must be configured with passwords so that no one could make any changes to the configurations of these devices.

1.4Troubleshooting the Network:

This is the phase where packet is send from every host to every other host to check if there is any problem in the desired transmissionscheme. Packet Internet Groper (PING) is mostly used. Every Network design needs to be troubleshoot before it can actually be implemented.

There is a list of steps to be taken to troubleshoot a network. These will be discussed in the upcoming few slides.

1.4.1 Open DOS and ping 127.0.0.1

This is domestic, or loopback address. If it is successful that means your IP stack is considered to be initialised. If an unsuccessful result is obtained that means your IP stack has failed and you need to reinstall TCP/IP on the host.

1.4.2 From the DOS window ping the local host

If this is successful, it means that your Network Interface Card (NIC) is functioning. If it fails, there is a problem with the NIC.

Success here doesn't mean that a cable plugged into the NIC, only that the IP protocol stack on the host can communicate to the NIC(via the LAN driver).

1.4.3 From the DOS window ping the default gateway

If the ping works, it means that the NIC is plugged into the network and can communicate on the local network. If it fails, you have a local physical network problem that could be anywhere from the NIC to the router.

1.4.4 If steps 1 through 3 were successful, ping the remote server

If that works, then you know that you have IP communication between the local host and the remote server. You also know that the remote physical network is working.

If the user still can't communicate with the server after steps 1 through 4 are successful, you have some type of name resolution problem and need to check your Domain Name System (DNS) settings.

1.5 Motivation

The field of computer networks is growing at a very fast rate. New technologies are emerging almost everyday. Thousands of volunteers work together everyday to discuss and form new standards and conventions. This field has always fascinated me because of its simplicity and scope. Also, there is a lot of scope of learning in this area of Computer Science.

1.6 Problem Statements

- To design an Enterprise Network in a manner which will minimize the occurrence of faults.
- Designing the network in such a way that nodes can be added to or removed from any secondary node.
- To address the Fault Tolerance issues in Enterprise Networks for Large Scale Organizations.
- To detect and diagnose the faulty nodes.

1.7 Thesis Organization

1). Introduction: This chapter deals with the basics of network design. It also emphasizes the steps taken to troubleshoot a network after the design is completed.

2). Properties of ENLSO:This chapter deals with the most common properties that an Enterprise Network for Large Scale Organization must have. In this chapter emphasis is given to how an Enterprise network should be designed.

3). Fault Tolerance :This chapter explains the most common types of faults that can occur in a network. A Network Designer must works towards avoiding these types of faults.

4). Implementation:In this chapter a discussion on the actual scenarios and designs created by me is done. Here I have tried to explain and implement all the properties that have been talked about in the previous chapters. Also a complete description of two network scenarios is produced in the form of case studies.

5). Conclusion:This chapter presents the detailed conclusions that I want to produce. Here a discussion on what properties are to be implemented in what fashion has been made.

6). References:This chapter contains all the references that has been helpful in doing this project. I have tried to mention all the relevant references.

1.8 Summary

This chapter contains information on how to design and troubleshoot a network. I have enumerated all the points to keep in mind while planning the network. After that a discussion on the steps to follow while designing a network has also been done. Finally, the chapter is concluded with steps towards troubleshooting the designed network. No computer network can be said to be designed completely unless all the nodes and devices are working properly. Hence, this step is a must for all the Network Designers.

CHAPTER 2

Properties of Enterprise Network for Large Scale Organization

2.1 Introduction

Any network which is big in size and is owned by a single organization cannot be called an enterprise private network. It is very important to know that enterprise networks have different architecture and design. Hence, it has different properties also. Enterprise networks are the networks owned by large scale organizations in which a high performance network is required. They cannot afford to have their network down even for few seconds. Hence, some of the properties that make enterprise networks what they are are as follows:

2.1.1 Redundancy:

Enterprise networks are highly redundant. There always is at least one more path to reach a host. Redundancy is a good way of providing backup routes. This helps to protect the network from link failures. Redundancy can be of two types:

- Switch redundancy:- Layer 2 redundancy
- Router Redundancy: - Layer 3 Redundancy.

Redundancy helps to tackle network faults specifically related to nodes and links.

2.1.2 Router Redundancy protocol

Some of the protocols used for router redundancy is implemented in order to remove the single point of failure. Some of the protocols used to achieve this are:

Hot Standby Router Protocol, Virtual Router Redundancy Protocol, etc.

2.1.3 Use of fast converging routing protocols.

Fast convergence implies the time taken by a router to find a new path to a node in case the old one is down. This can be achieved by using Dynamic routing protocols. We have to make sure to minimize the convergence time.

2.1.4 Requirement of high availability

Enterprise networks are highly available networks. Rapid Spanning Tree protocol is used to achieve high availability.

2.1.5 Use of ACL to balance load in case of failure

Access Control Lists are used for load balancing operations.

2.1.6 Link Aggregation to avoid traffic congestion

Link Aggregation or Etherchannel is used to equip a network with high capacity for data transfer.

2.2 Detailed Description of these properties

2.2.1 Redundancy

Redundancy is the key property of an enterprise network. Enterprise networks are designed in such a way that for every path there must be an alternate one.In case a node or a link goes down, the Enterprise networks are equipped with backup routes. Hence it is only a matter of seconds for back up routes to be discovered and the network to be back on track.

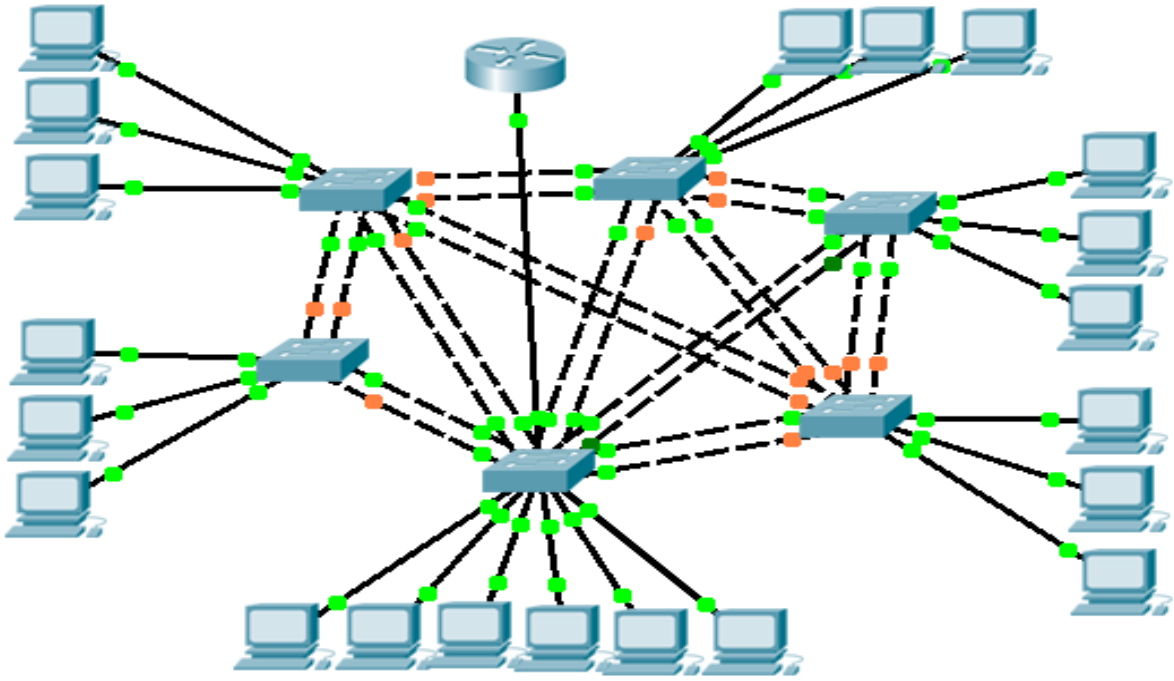

Fig 2.1 Redundancy in Layer 2 Switches

2.2.2 Router Redundancy

- Router Redundancy is an important property of an Enterprise network. It is a method which is extensively used in enterprises.
- Basically, Hot Standby Router Protocol removes the need for the old design called “router on a stick”.
- Once you have this protocol running the fear of a single point of failure is completely eliminated. A back up default gateway becomes available.
- Alternatives:
  - Virtual Router Redundancy Protocol (VVRP)
  - Common Address Redundancy Protocol (Open Source)

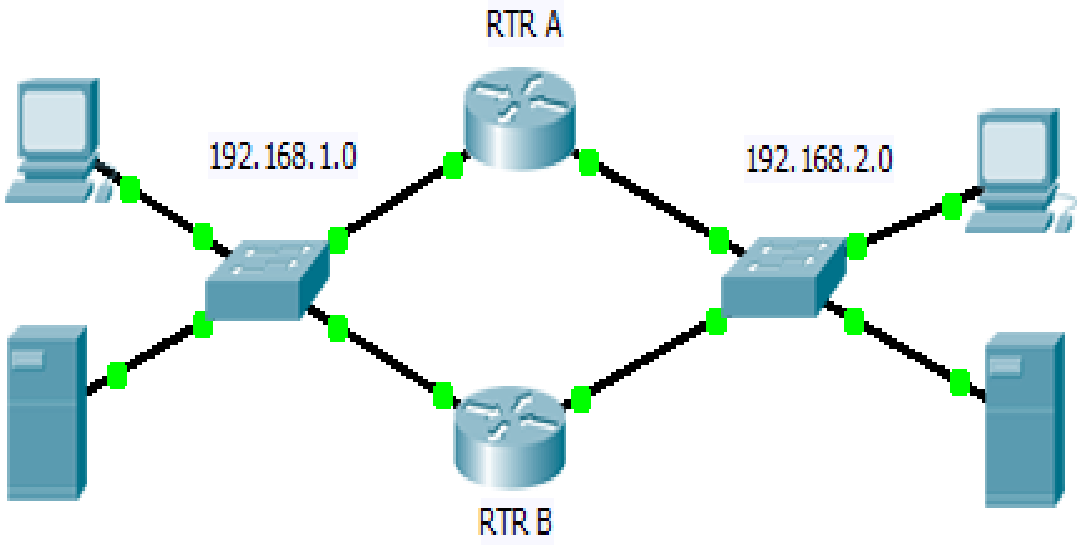

Fig 2.2 An example of router redundancy

2.2.3 Fast Convergence

- In an Enterprise network it is very important to keep running without a breakdown even for a second. Hence routing protocols with fast convergence become an unavoidable necessity.
- The routing protocols used in Enterprise networks are

  RiPv2, OSPF, EIGRP, BGP, IS-IS, etc.

These protocols have faster convergence and lower administrative distances. Hence these routing protocols are preferred.

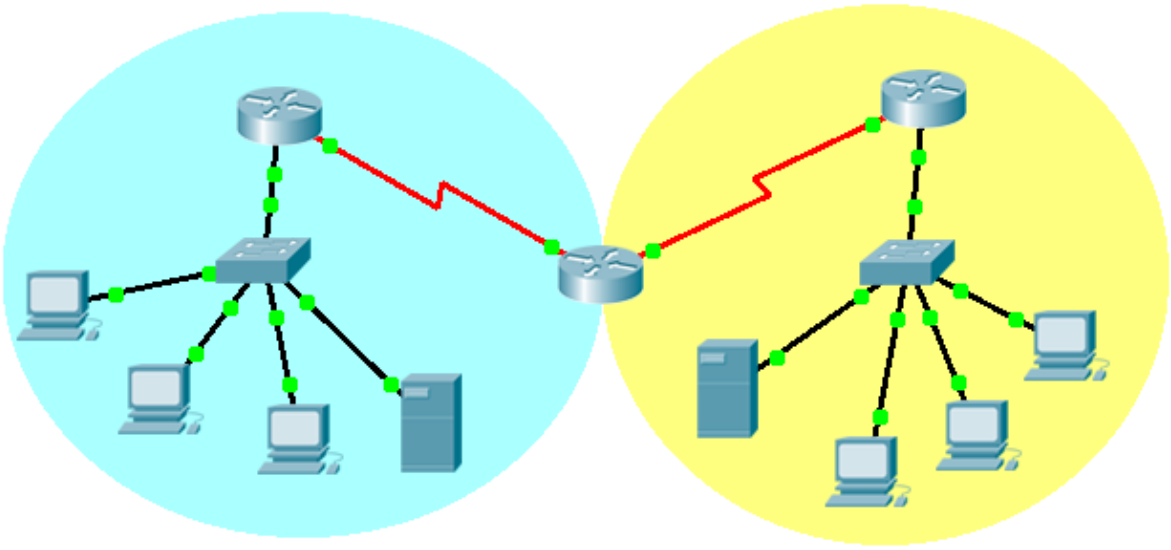

Fig 2.3 An example of fast converging Routing Protocols

Fast converging routing protocols like Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) can be represented as shown above.

2.2.4 High Availability

- Providing high availability in the enterprise site can involve deploying highly fault-tolerant devices, incorporating redundant topologies, implementing STP, and configuring HSRP.
- Network designers must incorporate high-availability features throughout the network.
- Adopting a high-availability strategy for an enterprise site is a must.

2.2.5 Use of ACL

- Access Control Lists are very useful and extensively used in enterprise networks.
- ACL's are used to filter traffic as well as manage them.

- ACL's are also used to load balance in case of a failure. Dynamic ACL's can be configured on layer 3 switches which get triggered in case a node is down.

2.2.6 Ether Channel

- Ether channeling is a way of logically bundling the transmission link in order to load balance. The bundled links behave as one interface with large transmission capacity. This process is called Link Aggregation.
- Cisco's version of Ether Channel is called Port Aggregation Protocol(PAgP)
- IEEE calls it Link Aggregation Control Protocol (LACP orIEEE802.3ad)
- Even though there are 6 links between each of the switches, they behave as one. It is obvious that their transmission capacity is six times more than that of a single link.

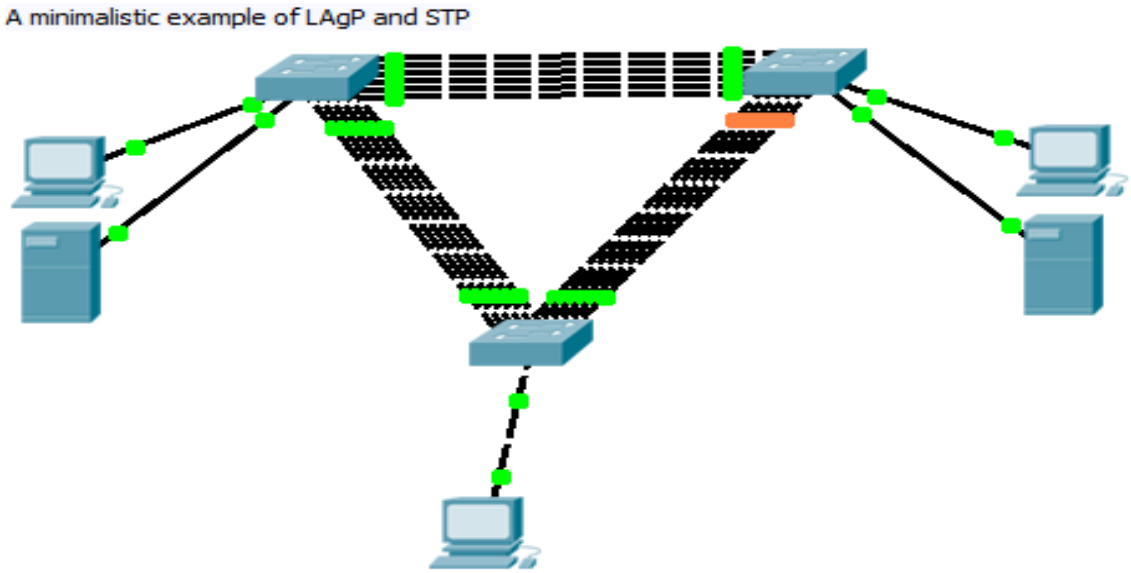

Fig 2.4 A minimalistic example of Ether channel and STP

Even though there are 6 links between each of the switches, they behave as one. It is obvious that their transmission capacity is six times more than that of a single link.

2.3 Enterprise Network Guidelines for High Availability

- Implement Spanning Tree Protocols to avoid loops
- Use uplinkFast and portFast enhancements for better results.
- Rapid Spanning Tree Protocol (IEEE 802.1w) and Multiple Spanning Tree Protocol (IEEE 802.1s) offer benefits such as faster convergence and more efficiency over traditional Spanning Tree Protocol (IEEE 802.1d)

2.4 Summary

This chapter deals with the properties that an Enterprise Network must poses in order to be robust and secure. It starts with the enumeration of these properties followed by a detailed explanation of the same including some new ones. All the Enterprise networks must have these properties and the Network Designers must use the discussed methods and protocols to make their network design more fault tolerant. Finally, the chapter is concluded with some guidelines that should be followed to make the network more productive.

CHAPTER 3

Fault Tolerance

3.1 Introduction

Fault tolerance is a term used to describe the ability of a network to continue to function in a manner acceptable to the network users despite the occurrence of one or more faults or failures within the network itself.

It is also desirable that in the event of a part of a network suffering a failure, information concerning the failed network elements is available to the functioning remainder of the network.

3.2 Types of faults:

There are four types of basic faults that can occur in a network:

1) Transient

2) Persistent

3) Intermittent

4) Byzantines

3.2.1 Transient Faults:

Transient faults are faults that appear for a very small time. These are temporary in nature. These can be caused by lightening, or voltage fluctuations. These faults are non persistent in nature and remain in the network for a very small time.

3.2.2 Persistent Faults:

Persistent Faults are like permanent faults. These faults have to be corrected as soon as they occur. There can be various reasons for these faults. Once they occur, persistent faults continue to keep the network segment down unless corrected as early as possible.

3.2.3 Intermittent Faults:

Intermittent faults are caused by repetition of transient faults. Unlike transient faults, these faults remain in the network. These faults are

crucial as they are hard to pin point. Intermittent faults create noise in the network and can also bring down the network segment in specific network scenarios.

3.2.4 Byzantine Faults:

Bisentine faults are faults that occur due to a combination of transient, intermittent and persistent faults.

Bisentine faults are hard to correct and have the capacity to bring down a network segment as it includes persistent as well as intermittent faults.

These four basic faults do not usually occur in their defined forms. The most common type of faults originating in a network are as follows:

- Transient leading to Persistent
- Intermittent leading to Persistent
- Transient, Intermittent, Persistent

3.3 Summary

This chapter explains the various kinds of basic faults that can occur in a network. Every Network Designer must work towards avoiding these types of faults. Any network that is not fault tolerant is not practical enough to be implemented. Every network should be capable enough to avoid or at least work in case of a node or link failure. A little light on this topic was necessary to complete the range of the problem statements.

CHAPTER 4

Implementation

4.1 Introduction

As a part of the implementation process I have created various simulations and explained the use of each of the techniques mentioned in the previous chapters. A combination of these methods and protocols gives us a very robust and fault tolerant network without compromising the security.

4.2Details ofTools UsedforDesigningthe Networks

PACKET TRACER:

Packet Tracer is a powerful network simulation tools which helps students to get a hands on approach on various networking devices and concepts. This hands-on capability is a fundamental component of learning how to configure routers and switches from the command line.

Supported Protocols: Packet Tracer supports HTTP, Telnet, SSH, TFTP, DHCP, and DNS;TCP and UDP; IPv4, IPv6, ICMPv4, and ICMPv6; RIP, EIGRP, multi-area OSPF, static routing, and route redistribution; Ethernet/802.3, 802.11, HDLC, Frame Relay, and PPP; ARP, CDP, STP, RSTP, 802.1q, VTP, DTP, and PAgP.

4.3 A case study

The following is a typical Enterprise Private Network. Some of the components of this network are:

Demilitarised Zone (DMZ): That part of a network which gives the outside users access to the internal network is called a DMZ. Usually this is the most vulnerable area of any network. The network managers must be careful about the Demilitarized Zone.

Branch Office: Branch Office is obviously the office located at the scene.

Corporate WAN: This is the actual internal network of the corporation.

The green circle represents the Internet. The internet users may need to have access to the servers because some of the company's resources might be public e.g. the company's website, ftp server etc.

No Internet user should have access to the corporate WAN. This network is completely segregated from the outside network. It is important to note that the users from the branch office can use Internet resources but the internet users cannot access the branch office. To achieve this routers are configured with Access Control Lists.

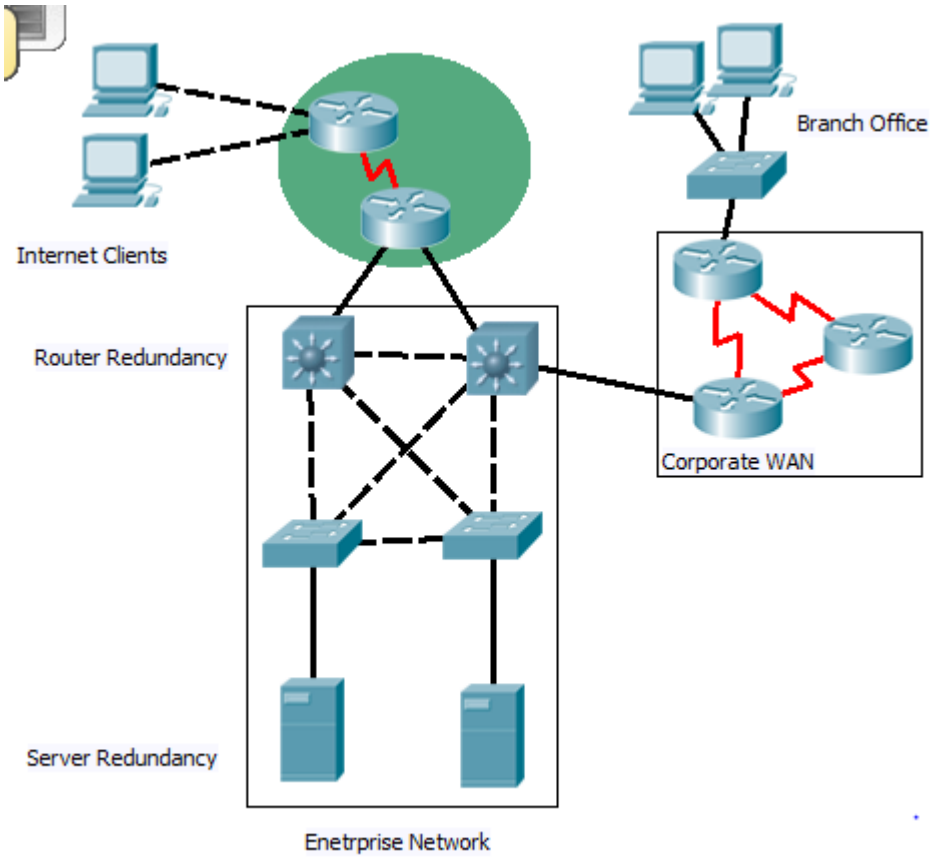

Fig 4.1 Example of an Enterprise Private Network

The two types of redundancies discussed in the last chapter have also been clearly shown. These are router redundancy and server redundancy. The enterprise network has no single point of failure. Router Redundancy Protocol is running on the two uppermost switches. Also there is a backup server in case the active server goes down.

4.4 The corporate WAN

The corporate WAN is the actual internal network which connects all the departments of the corporations. As one can see the switches are extensively connected. This is done to protect the internal network from link as well as node failures. If any node in the network goes down, only the devices connected to it directly will loose connection, the rest of the network will work without fault. In case a link goes down, there always is a backup route to the destination.

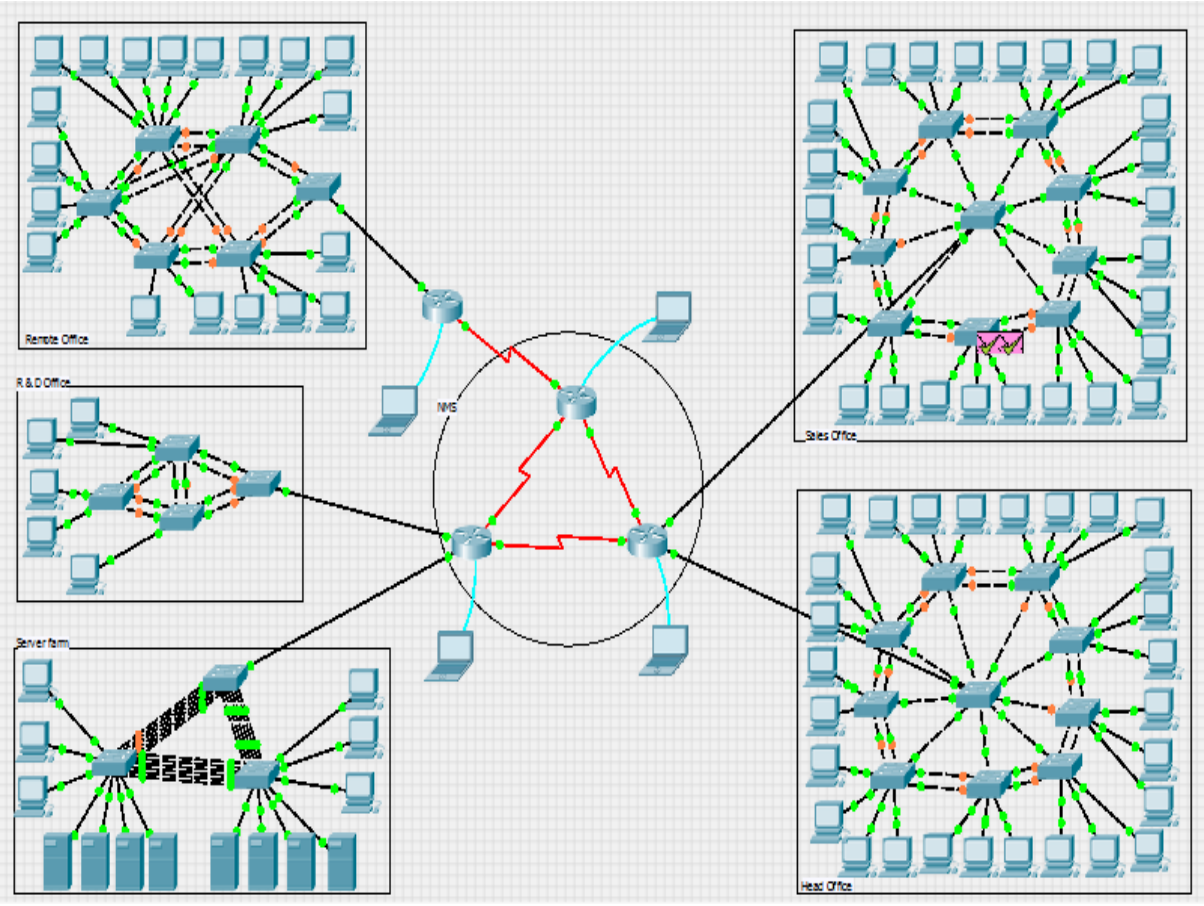

Fig 4.2 A Local corporate WAN

In the server farm, the traffic is supposed to be considerably very high. This is the reason why Port Aggregation Protocol is used in the network. For fast convergence at switch level Rapid Spanning Tree Protocol has been used. For fast convergence at the router level Enhanced Interior Gateway Routing Protocol is used.

4.5 Summary

In this chapter I have implemented all the properties that have been mentioned in the previous chapters. Fig 4.1 gives us a general scenario of how an Enterprise Network should be designed. The following figure i.e. Fig 4.2 explains in details the Corporate WAN part of the Enterprise network shown in Fig 4.1. A brief discussion of these two networks has been done in order to explain all the protocols and methodologies used in the network scenarios.

CHAPTER 5

Conclusions

5.1. Detailed Conclusions

- Redundancy can prove to be very helpful in order to reduce link related faults. Anytime a link goes down, a backup link must be available in order for communication to take place. Redundancy is done at
- Looping is extremely helpful in order to avoid node related faults. When looping is done in a smart way, loops can be very helpful in avoiding node related faults. Once a node goes down, only the devices directly connected to the faulty node loose connection.
- Etherchannel can be used to handle large amount of data traffic. At network segments where traffic is relatively high we can use Link Aggregation. A method of logically bundling the Ethernet cables. This process is most commonly known as Ether Channel.
- Hot Standby Routing Protocol removes single point of failures. HSRP is a way of achieving router redundancy. This protocol removes the most common problem of single point of failure. When HSRP is running on the routers directly connected to the network segment, the default gateway is actually a virtual interface.
- High availability can be achieved by using Fast convergence techniques. Fast convergence at switch level can be achieved by using Rapid Spanning Tree Protocol. At router level, fast convergence is achieved by using dynamic routing protocols. A Network Designer must choose the best of the best routing protocols when it comes to designing an Enterprise Network.

7. References:

[1]Simon Edwin Crouch "Fault Tolerance in Ethernet Networks"

PUB. NO. US 2005/0022048 A1

[2]P. Bahl, R. Chandra, A. Greenberg, S. Kandula, D. A. Maltz, M. Zhang, "Towards highly reliable enterprise network services viainference of multi-level dependencies." In SIGCOMM, Aug. 2007.

[3]P.M.Khilar and et. al. "Evaluation of Computer Networks in TCP/IP Environment—a Review", Proceedings of Annual Technical Session, OEC-2003, Bhubaneswer, EECS-1 to EECS-6,January 2003.

[4]P.M.Khilar and et. Al. " Evaluation of flow control in group communication", CSI 2002, SRIJI College, AP

[5]Michael Galea, "Rapid Spanning Tree in Industrial Networks", RuggedCom Inc. - Industrial Strength Networks Woodbridge, Ontario, Canada

[6]S. Yemini, S. Kliger, E. Mozes, Y. Yemini, and D. Ohsie, "High speed and robust event correlation". IEEE Communications Mag., 1996.

[7]Cisco Press Book : http://www.ciscopress.com/articles/article.asp?p=375501&seqNum=2

[8]Cisco Study Guide By Todd Lammle, chapter 8 and 9