Department of Networking and Communications

COURSE PROJECT REPORT
ACADEMIC YEAR:2021-2022
EVEN SEMESTER

PROJECT TITLE: Small Business Network Design with Secure E-Commerce Server

Program(UG/PG):UG
Semester: IV
Course Code:18CSC202J
Course Title: COMPUTER COMMUNICATIONS
Student Name: Saloni Smriti,Aditi Mishra,Riya Singh
Register Number: RA2011031010021, RA2011031010041, RA2011031010044
Faculty Name: Dr.P.Visalakshi
Branch with Specialization: CSE- INFORMATION TECHNOLOGY
Section: O1

SCHOOL OF COMPUTING

COLLEGE OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR - 603203

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR-603203

BONAFIDE CERTIFICATE

Certified that this course project report titled **"LAN Network Design with Redundancy"** is the bonafide work done by **" Riya Singh (RA2011031010044)"**who carried out the course projectwork under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form part of any other work.

SIGNATURE
Dr.P.Visalakshi
Asst.Professor(Selection Grade)
Course Handling Faculty

INDEX

APPENDIX

REFERENCES

What is LAN Network?

A local area network (LAN) is a computer network which extends in a small coverage of geographical area (ex-home, school, computer laboratory, office building or group of buildings)

A LAN is composed of internally connected functional workstations and pc', each capable of accessing and sharing data and devices inside the network (ex- printers, scanners and data storage devices, anywhere on the LAN).

LANS are characterized by data transfer rates and various other characteristics such

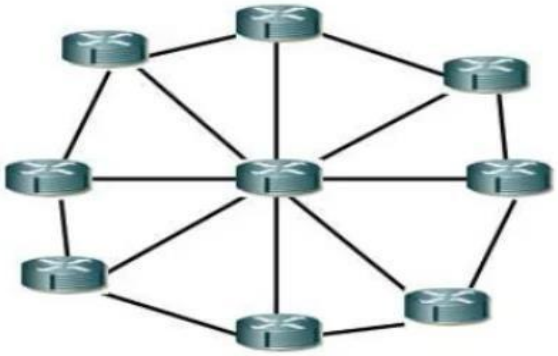
as leased lines.

History

In the 1960s, large colleges and universities had the first local area networks (LAN). In the middle of 1970, The Chase Manhattan Bank in New York used the LAN Network commercially in December 1977.

In the late 1970s and early 1980s, it was common to see and experience hundreds of individual computers located in the same site. Many individual users and network administrators were attracted to the basic concept of multiple computers which are sharing economically expensive disk space and laser devices.

What is Network Redundancy?



The sole concept of network redundancy is to provikle alternate and efficient paths for

data to travel along in case a cable is broken or a connector accidentally un-plugged.

Ethernet as standard does not have rings or loops in the network because it will cause

broadcast stoms and can ultimately cause the network to stop functioning.

To withstand with redundancy, network building structure mainly the switches and routers used in the network must support redundancy protocols designed to avoid the usual problems of putting bops into a network.

Importance of Network Redundancy

In our 21 century all networks are high-tech build and high speed. A simple example would be if you have a single network (ex TI) connection from your core site to each remote office you connect with. What will happen if the link went down?? In this section we will find the solution of this scenario to help designing and plan for a backup solution that you can count on and one that is cost effective and will not break the bank.

Network redundancy is very simple concept. If there is a single point of failure and it fails the network, then there is nothing to rely on.

Solution

The first and foremost step in building network redundancy is to follow a scheduled and perfect project plan to reconstruct the current architecture

of the network.

1. Plan for a way to make it redundant.

2. Plan for a way to deploy it and then set up a way to test it.

Final step will be applying all the policies and processes that allow to monitor it and be alerted when things do fail and actions can be taken. A company's various policy(security policy, disaster recovery plan, business continuity plan and/or incident response plan) will leave room for this type of solution.

Always have a scheduled procedure regardless of automatic or manual. This means. when implementing the practical redundancy into systems or network, there will be need to take action immediately even if all the operations continue to take place to verify that everything went scheduled or not.

Analysis is critical to building a good redundancy plan. Almost every network created is unique in some way of operations. This is why understanding the core concept is a must needed quality to acquire network redundancy.

Important steps

1. A risk analysis assessment must take place.

2. The core sites must be taken into consideration if that is where the bulk of network resources are located.

3. Routing and routing protocols need to be considered.

4. Solutions exist only when specific routing and switching (ex- MPLS) protocols are applied the designing of the network to achieve redundancy.

1.5 Various Topologies of a LAN Network:

At first we have to know that what exactly network topology means. We can say Topology is basically the construction of the network. Theoretically we can say it's the schematic description of how the network is arranged including its nodes and the connecting lines.

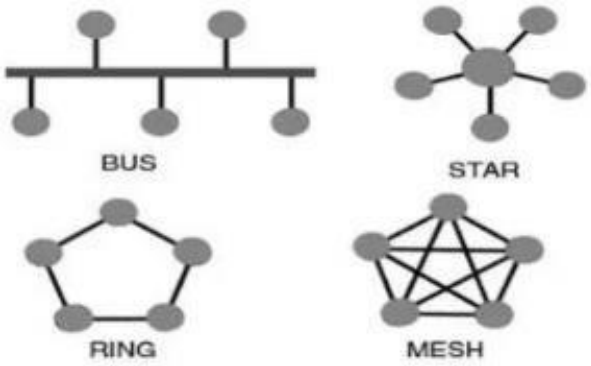
The Network topology can be of two types

1. Physical Topology

2. Logical Topology

LAN network can be created by various network topologies, which are

1. Bus Topology
2. Star Topology
3. Ring topology
4. Mesh Topology



The mostly used and common LAN topobgy is a "star." In which each computer, or node is connected to a central hub. This is reliable than a "ring" topology, because failing of a node will not break down the whole network. A bus topology is conceptually more reliable, but has poorer performance than ring.

Redundant LAN Connection

To handle a system communication failure that use to occur within or outside of a server's local subnet.

The server's are the main potential points of network breakdown, but redundancy can be added in variety of ways.

1. NIC Card
2. Default gateway

Multiple NIC cards on the same subnet

Whether the server system is standalone, clustered, or load-balanced, the Network Interface Card is a potential point of failure.

To provide NIC redundancy, do connect NICs to the same hub or switch or preferably to different switches. The Interface metric property determines which of the active (ie., enabled) NICs the system will use for outbound traffic; the system uses the NIC with the lowest number in the Interface metric field.

Steps

1. Go to Control Panel, Network and Dial-up Connections- Local Area Connection Properties.

2. Select Internet Protocol and click Properties.

3. On the General tab, click Advanced,

4. Clear the Automatic Metric check box at the bottom of resuking dialog box.

5. Enter the metric you want to assign to this NIC.

Multiple Default Gateways

Failure of the default gateway configuration on the subnet will cause the internet traffic to remote subnets to fail. Implementing multiple routers on the subnet provides a measure of fault tolerance to this kind of failure.

The Virtual Router Redundancy Protocol (VRRP) and the Hot Standby Router

Protocol (HSRP) supports such fault tolerance without configuration

changes Multiple default gateways can be implemented at each client by defining

more than one default gateway address on each Network Interface Card.

route p add 0.0.0.0 subnet mask 0.0.0.0 20.20.0.254 metric 10

Add a persistent default gateway for the router at 10.10.0.254 with a metric of 10. Only connection-oriented traffic like TCP will have a default gateway change; UDP and Internet Control Message Protocol (ICMP) traffic such as Ping won't as they are connectionless. Defining different de fault gateways for different NICs in a computer can cause problems when the NICS connect to the internal networks that can't communicate with one another within. Even when de fault gateways are defined on different NICs, only one of a computer's default gateways is active at a time.

Link aggregation

NIC vendors began to offer proprietary solutions to the single-NIC concept.. These solutions give birth to the IEEE 802.3ad Link Aggregation Control Protocol (LACP) standard.

1. Switch-to-switch

2. Server-to-switch connections.

Theme

Network which has redundancy in the design be setup for an organization. The organization is currently having an internet connection, which is setup using a Cisco router. The gateway addresses for users in the LAN is currently provided as an intermediate routers address, which would then forward all internet bound packets to the internet router. The network has to be upgraded by having dual intermediate routers which would automatically failover, and provide high availability access to the internet HSRP is to be used for the depbyment. The project identifies the configurations required on Cisco routers to achieve the same,

Organization

Amity Institute of Telecom Engineering & Management is the prime institute for

Telecommunication situated in Noida. It comes under Amity University, AITEM provides B-Tech. M-Tech and MBA degrees for study in Telecom Field.

Vision

Building global bridges and fora in industry and academia providing total integrated & quality education, being the front-runner in value education & nurturing Indian traditions and ethos.

Mission

To develop the overall personality of students by making them not only "excellent professionals", but also good individuals, with understanding and regards for "human values", pride in their heritage and culture, a sense of right and wrong, and a yearning for perfection.

Materials & Methods

Basic Idea

We will be making a topology on GNS3 which will be a hub and spoke topology in which all the routing protocols will be implemented and a LAN network will be created.

We will be creating SSL VPN ie. the virtual private network on a system which will provide us network and we will be able to access our office computers just by sitting at our home.

To make it secure communication we will be implementing Cisco ASA ie. Cisco Adaptive Security Appliances and will be assigning a public IP to it. Further we will be implementing Network Address Translation so that server can be NAT on ASA and on routers. Through adaptive security appliances we will apply ACL ie. Access Control List.

A Graphical User Interface of ASA firewall will be made to make the connection secure and handle the network more reliably and an easy manner. The topology of network will be Hub and Spoke topology. For eg Hub can be the main headquarter situated in Delhi

Spoke can be different offices in Chennai Jammu & Kashmir etc. All traffic will be routed through the main headquarters and we will get the logs at the Hub. At Hub we will use Multi-Protocol Label Switching Router so that we can route our Voice and Video traffic using different types of protocols that come under MPLS. At the end terminals we will be deploying Cisco Phones and we will show the connectivity between different Cisco Phones by ringing Further if any growth will be there then we will be making an application of the project

Methodology

1: Study different types of routing protocols.

2: Study in detail about firewalls.

3: Start making the topology on GNS3.

4: Study about virtual private network (VPN).

5: Start setting up VPN on the system.

6: Study Adaptive Security Appliance.

7: Study NAT and Implement it on ASA and on router.

8: Apply Access control list through ASA.

9: Study MPLS routing and different types of protocols that comes under it.

Requirements

1. CISCO Packet Tracer for applying basic commands.

2. GNS 3 for making the final network topologies.

3.2 or 3 Laptops.

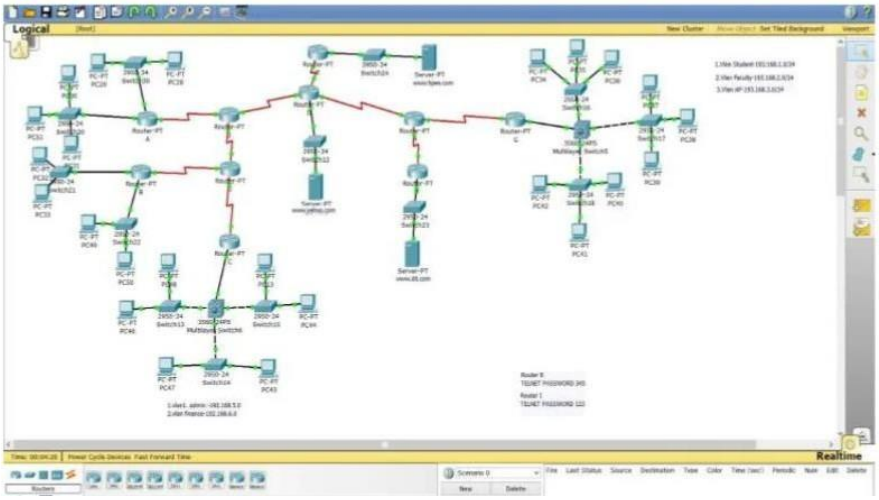
4. LAN Cable for connectivity.

2.5 Different routing Protocols

We will use different routing protocok to establish connection, but in this model

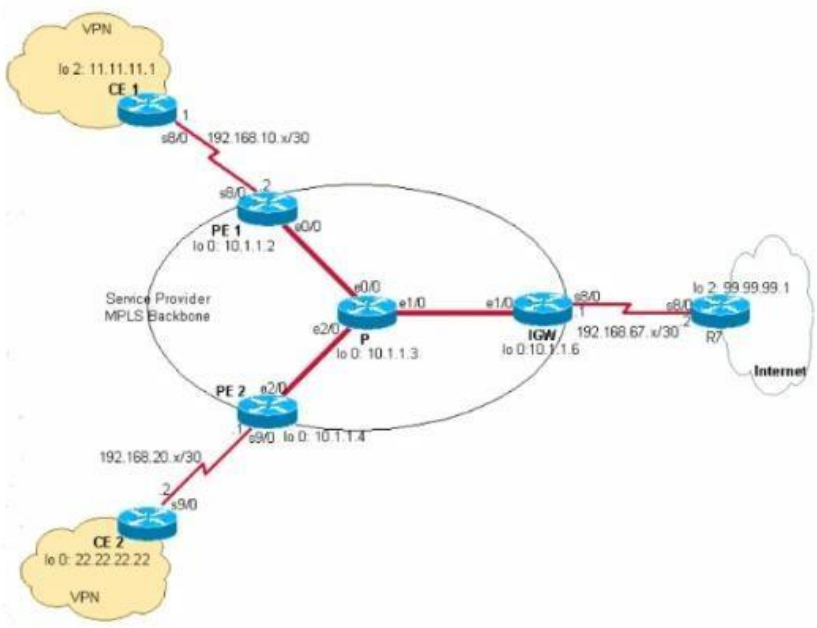
mainly we will use Multi- Protocol Label Switching Protocol

CISCO Packet Tracer Model



MPLS ROUTING:

A Label Switched Path is a path via Label Switched Routers (LSR) in a MPLS enabled network. Packets are switched based on labels applied to the packet. LSP's) may be signaled using the Tag Distribution Protocol (TDP), the Label Distribution Protocol (LDP) and the Resource Reservation Protocol (RSVP).



VPN (Virtual Private Network)

A VPN is a type of a secured network that allows the provisioning of private network services for an organization over the unsecured network using tunneling protocol. By the unsecured network, we mean a public or shared infrastructure such as theinternet or service provider hackbone network. The shared service provider backbonenetwork is also known as the VPN Backbone. It is the VPN backbone which is used to transport the data traffic for multiple VPN's.

VPN is provisioned using technologies such as Frame Relay and Asynchronous Transfer Mode vinual circuits for long time. However over the past few years IP and MPLS based VPN's have been a part of innovations.

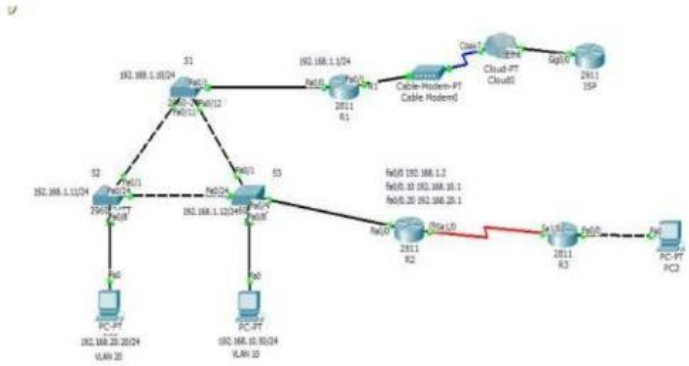


Figure 5: VPN

NAT(Network Address Translation)

Short for Network Address Translation, which is an Internet standard that enables a local-area network (LAN) to use two set of IP address.

1. One set of IP addresses for internal (inbound) traffic. 2. Second set of addresses for external (outbound) traffic.

NAT serves three main purposes:

1. Provides a type of firewall by hiding internal IP addresses in the network.

2. To use more internal IP addresses.

3. Allows to combine multiple ISDN (Internet Switched Digital Network) connections into a single Internet connection.

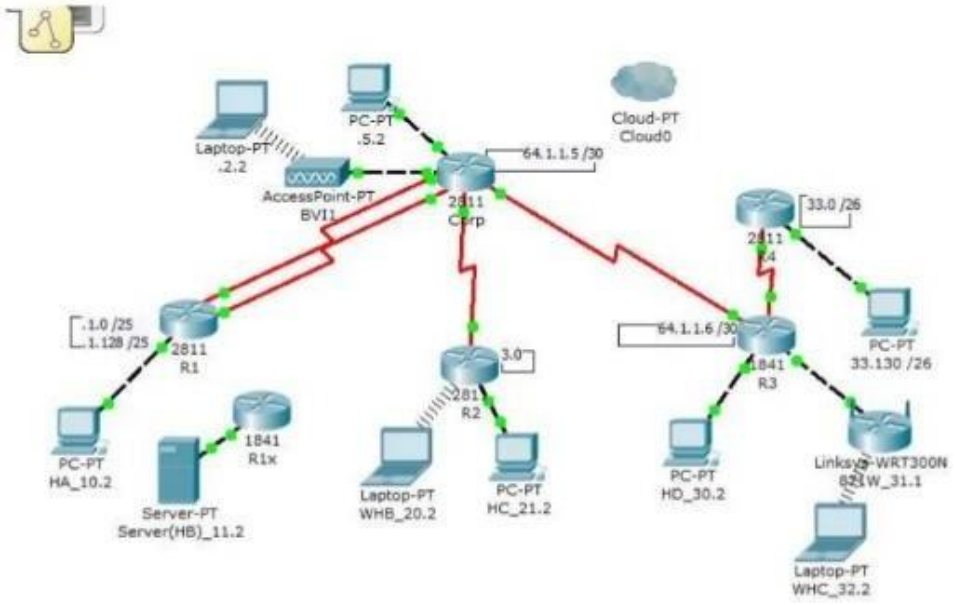


Figure 6: NAT

Configuring Static NAT

[Router (config inte 0/0

Router (config-if)# prat inside

Router (config)# int s0/0

Router(config-if)# ipnat outside.

Router(Config)# ipnat inside source static 172.16.1.51 158.80.1.45

Configuring Dynamic NAT

[Router (config)# inte 0/0

Router (config-if)# pnat inside

Router (config)# int s0/0

Router(config-if)# ipnat outside

Router(Config)# iprat pool AMITY ip address ip address netmask"]

Port Address Translation

Router(config)# interface fastethemet 0/0

Router(config-if)# ip nat inside

Router(config)#interface serial 0/0/0

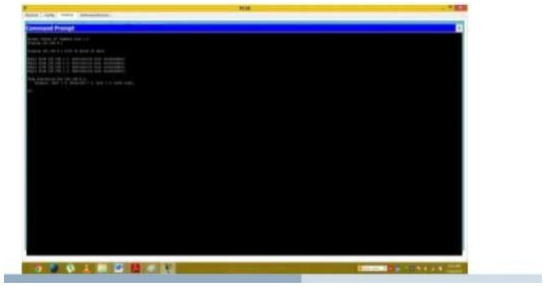
Router(config-if)# ip not outside

Router(config)# ip nat inside source list 10 interface serial 0/0/0 overload

Router(config)# access-ist 10 permit ip add. Subnetmask

Access List

Access list defines a pattern that can be found on IP packet. As each packet comes through an interface with an associated access list, the list can be scanned fro, top to bottom in the exact order that i intended for a pattern that matches the incoming packet. A permit or deny rule associated with the pattern that determines the fate of the packet.



Configuring Access List

Router #config

Router(config)# access-list udp 150 permit any ip address netmask port number

Router(config)# access-list tcp 150 permit any ip address netmask port number

Router(config)# access-list tep 150 deny ip address netmask ip address netmask

Router(config)# access-list tep permit any any

Router(config)# int s1

Router(config-if)# ip access-group 150 in

Router(config-if)# exit

Router(config)#exit

Routing Commands

[Routers Enable

Router# Configure terminal

Router(config)# int fa (0/0, 1/0)

Route (config-if)# ip address (ip address) (subnet mask)

Router(config-if)# no shutdown

Router(config-if)#exit

Router(config)#int serial 20

Router(config-if)# ip address (ip address) (subnet mask)

Router(config-if)# no shutdown

Router(config-if)# ext

Router(config)#int serial 3/0

Router(config-if)# ip address (ip address) (subnet mask)

Router(config-if)# no shutdown

Router(config-if)# ext"]

No Shutdown command is used to change the state of Interface from UP to DOWN or

from DOWN to UP.

RIP V2 Routing

[Router(config)# router rip

Router(config)# version 2

Router(config-router)# (Connected Network! address)

Redundancy Routing Protocols

Virtual Router Redundancy Protocol (VRRP) is a networking protocol that provides for automatic assignment of available Internet Protocol (IP) routers to participate as a host. This increases the availability and reliability of routing paths vi automatic default gateway selections on an IP sub-network.

It is achieved by creation of virtual routers, which are representation of multiple routers, ie, master and backup routers, acting as a group. The default gateway of a participating host is assigned to the virtual router instead of a physical router. If the physical router that is routing packets on behalf of the virtual router fails, another physical router is selected to automatically replace it. VRRP provides information on the state of a router, not the routes processed and exchanged by that router.

How Election of Master Router is performed?

A failure to receive a multicast packet from the master router over a period longer than three times the advertisement timer causes the backup routers to assume that the master router is dead. The virtual router transitions into an unsteady state and an election process gets initiated to select the next muster router from the backup routers. This is fulfilled by the use of multicast packets.

Backup routers are only supposed to send multicast packets during an election process. One exception to this rule 'is when a physical router is configured with a higher priority than the current master, which means that on connection to the network it will preempt the master status. This allows a system administrator to force physical router to the master state immediately after booting, for ex: when the particular router is more powerful than others within the virtual router. The backup. router with the highest priority becomes the master router by raising its priority above that of the current master. It then takes responsibility for routing packets sent to the virtual gateway's MAC address. In cases where backup routers all have the same priority, the backup router with highest IP address becomes the master router.

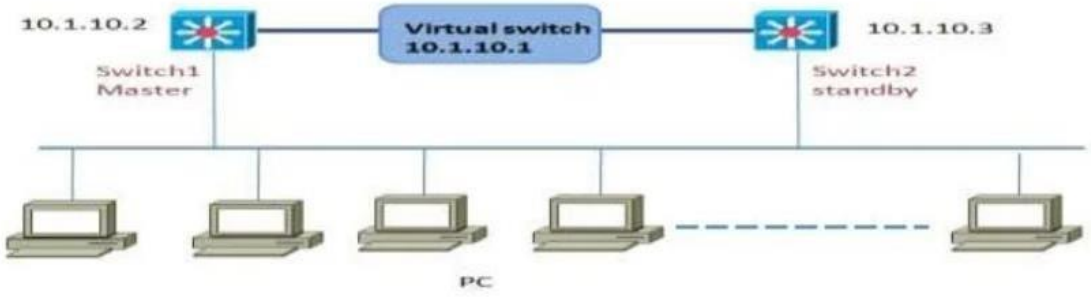


Figure 8: Master Router Election

All physical routers act as a virtual router are in the same LAN segment. Communication within the virtual router takes place periodically. The period can be adjusted by changing advertisement interval timers. The shorter the advertisement interval, shorter the black hole period, though at the expense of more traffic in the network. occurring during election. The skew time is given by the formula (256 Priority/25)(expressed in milliseconds).

HOT STANDBY ROUTER PROTOCOL (HSRP) is a Cisco proprietary redundancy protocol for establishing a fault-tolerant default gateway.

The protocol establishes a framework between network routers in order to achieve defaub gateway failover if primary gateway gets inaccessible, in close association with a rapid-converging routing protocol like EIGRP or OSPF. By multicasting packets, HSRP sends hello messages to the multicast address 22432 (all routers) for version 1, or 224.0.0.102 for version 2, using UDP pon 1985, to other HSRP enabled routers, defining priority between the routers. The primary router with highest configured priority acts as a virtual router with a pre-defined gateway IP address and responds to the ARP request from machines connected to the LAN with the MAC address 0000.0007.ACXX (or 0000.0C9E.EXXX for HSRPV2) where X will be hex representation of the (decimal) group ID. If primary router fails, the router with the next-highest priority takes over the gateway IP address and answers ARP requests with the same MAC address, thus achieving transparent default gateway failover. HSRP is not a routing protocol as it does not advertise IP routes or affect the routing table in any way. HSRP has the ability to trigger a failover if one or more interfaces on the router go down. This is useful for dual branch routers each with a single serial link back to the head end. If serial link of the primary router goes down, the backup router will take over the primary functionality and thus retain connectivity to the head end.

GATEWAY LOAD BALANCING PROTOCOL (GLBP)

Gateway Load Balancing Protocol (GLBP) is a Cisco proprietary protocol that attempts to overcome the limitations of existing redundant router protocol by adding basic load balancing functionality. In addition to being able to set priorities on different gateway routers, GLBP allows a weighting parameter to be set. Based on: this weighting (compared to others in the same virtual router group), ARP requests will be answered with MAC addresses pointing to different routers. Thus, kad balancing is not based on traffic load, but rather on the number of hosts that will use each gateway router.

By default GLBP load balances in round-robin fashion. GLBP elects one AVG (Active Virtual Gateway) for each group. Other group members act as backup in case of AVG failure. In case there are more than two members, the second best AVG is placed in the Standby state and all other members are placed in the Listening state.

FIREWALL

A fire wall is a network security system that controls the incoming and outgoing network traffic based on applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g, the Internet) that is assumed not to be secure and trusted. Firewall exist both as a software solution and as a hardware appliance. Many hardware-based firewalls also offer other functions to the internal network they protect, such as acting as a DHCP server for that network.

Many personal computer operating systems include software-based firewalls which protect against threats from the public Internet. Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions.

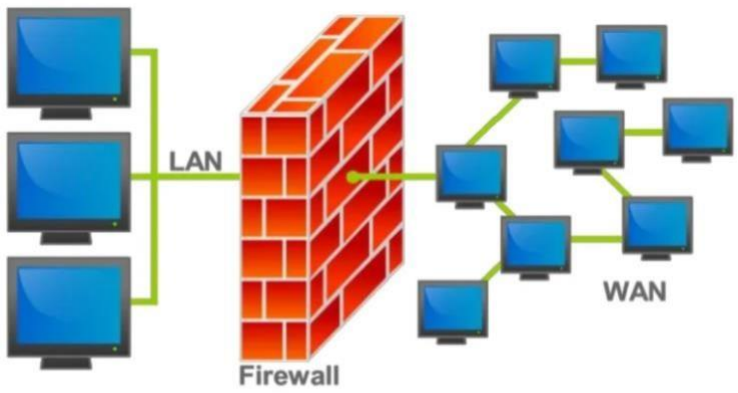


Figure 9: Firewall

HISTORY

First Generation: Packet Filters

The first paper published on firewall technology was in 1988, when engineers from Digital Equipment Corporation (DEC) developed filter system known as packet filter firewalls. This was the first generation of what is now a highly involved and technical internet security feature. At AT&T Bell Labs, Bill Cheswick and Steve Bellovin were continuing their research in packet filtering and developed a working model for their own company based on their original first generation architecture.

Packet filters act by inspecting the "packets" which are transferred between computers on the Internet. If a packet matches the packet filter's set of filtering rules, the packet filter will drop (silently discard) the packet or reject i (discard i, and send "error responses" to the source).

This type of packet filtering pays no attention to whether a packet is part of an existing stream of traffic (ie. it stores no information on connection "state"). It filters each packet based only on

information that is contained in the packet itself (most commonly using a combination of the packet's source and destination address, its protocol, and, for TCP and UDP traffic, the port number).

TCP and UDP protocols constitute most communication over the Internet, and because TCP and UDP traffic by convention uses well known ports for particular types of traffic, a "stateless" packet filter can distinguish between, and control, those types of traffic (such as web browsing, remote printing, email transmission, file transfer), unless the machines on each side of the packet filter are both using the same non-standard ports.

Packet filtering firewalls work mainly on the first three layers of the OSI reference model, which means most of the work is done between the network and physical layers, with a little bit of peeking into the transport layer to figure out source and destination port numbers.

When a packet originates from the sender and filters through a firewall, the device checks for matches to any of the packet filtering rules that are configured in the firewall and drops or rejects the packet accordingly.

When the packet passes through the firewall, it filters the packet on a protocol/port

number basis. For example, if a rule in the firewall exists to block telnet access, then

the firewall will block the TCP protocol for port number 23.

Second Generation: Stateful Filters

Second-generation firewalls performs the work of their first-generation predecessor but operate up to layer 4 (transport layer) of the OSI model This is achieved by retaining packets until enough information is available to make judgments about its state. Known as state full packet inspection, it records all connection passing through it and determines whether a packet is the start of a new connection, a part of an existing connection, or not part of any connection Though static rules are still used, these rules can now contain connection state as one of their test criteria.

Third Generation: Application Layer

The key benefit of application layer filtering is that it can understand certain applications and protocols (such as File Transfer Protocol (FTP), Domain Name System (DNS), or Hypertext Transfer Protocol (HTTP)). This is useful as it is able to detect if an unwanted protocol is attempting to bypass the firewall on an allowed port, or detect if a protocol is being abused in any harmful way. As of

2012, the so-called next-generation firewall (NGFW) is nothing more than the "widen" or "deepen" inspection at application-stack. For example, the existing deep packet inspection functionality of modern firewalls can be extended to include (1) Intrusion prevention systems (IPS);(ii) User identity integration (by binding user IDs to IP or MAC addresses for "reputation"); and/or (iii) Web Application Firewall (WAF). WAF attacks may be implemented in the tool "WAF Fingerprinting utilizing timing side channels.

Types

Network laver or packet filters

Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. The fire wall administrator may define the rules; or defauk rules may apply. The term "packet filter" originated in the context of BSD operating systems.

Network layer firewalls generally fall into two sub-categories, stateful and stateless. Stateful firewalls maintain context about active sessions, and use that "state information" to speed packet processing. Any existing network connection can be described by several properties, including source and destination IP address, UDP or TCP ports, and the current stage of the connection's lifetime (including session initiation, handshaking, data transfer, or completion connection). If a packet does not match an existing connection, will be evaluated according to the rule het for new connections. If a packet matches an existing connection based on comparison with the firewall's state table, it will be allowed to pass without further processing

Stateless fire walls require less memory, and can be faster for simple filters that require less time to filter than to look up a session. They may also be necessary for filtering stateless network protocols that have no concept of a session. However, they cannot make more complex decisions based on what stage communications between hosts have reached.

Newer firewalls can filter traffic based on many packet attributes like source IP address, source port, destination IP address or port, destination service like WWW.or FIP. They can filter based on protocols, TTL values, net block of originator, of the source, and many other attributes.

Application-layer

Application-layer firewalls work on the application level of the TCP/IP stack (ie., all browser traffic, or all telnet or ftp traffic), and may intercept all packets traveling to or from an application. They block other packets (usually dropping them without acknowledgment to the sender).

On inspecting all packets for improper content, furewalar can restrict or prevent outright the spread of networked computer worms. The additional inspection criteria can add extra latency to the forwarding of packets to their destination.

Application firewalls function by determining whether a process should accept any given connection Application firewalls accomplish their function by booking into socket calls to filter the connections between the application layer and the lower layers of the OSI model Application firewalls that hook into socket calls are abo referred to as socket filters Application firewalls work much like a packet filter but application filters apply filtering rules (allow/block) on a per process basis instead of filtering connections on a per port basis. Generally, prompts are used to define rules for processes that have not yet received a connection. It is rare to find application firewalls not combined or used in conjunction with a packet fikers.

Aho, application firewalls further filter connections by examining the process ID of data packets against a rule set for the local process involved in the data transmission The extent of the filtering that occurs is defined by the provided rule set. Given the variety of software that exists, application firewalls only have more complex rule sets for the standard services, such as sharing services. These per process rule sets have limited efficacy in filering every possible association that may occur with other processes. Also, these per process rule sets cannot defend against modification of the process via exploitation, such as memory corruption exploits. Because of these limitations, application fire walls are beginning to be supplanted by a new generation of application firewalls that rely on mandatory access control (MAC), also referred to as sandboxing, to protect vulnerable services.

Proxies

A proxy server (running either on dedicated handware or as software on a general purpose machine) may act as a firewall by responding to input packets (connection) requests, for example) in the manner of an application, while blocking other packets. A proxy server is a gateway from one network to another for a specific network application, in the sense that it functions as a proxy on behalf of the network users.

Proxies make tampering with an internal system from the external network more difficult and misuse of one internal system would not necessarily cause a security breach exploitable from outside the firewall (as long as the application proxy remains intact and properly configured). Conversely, intruders may hijack a publicly reachable system and use it as a proxy for their own purposes; the proxy then masquerades as that system to other internal machines. While use of internal address spaces enhances security, crackers may still employ methods such as IP spoofing to attempt to pass packets to a target network.

Network address translation

Firewalls often have network address translation (NAT) functionality, and the hosts protected behind a fire wall commonly have addresses in the "private address range", as defined in RFC 1918. Firewalls often have such functionality to hide the true address of protected hosts. Originally, the NAT function was developed to address the limited number of IPv4 routable addresses that could be used or assigned to companies or individuals as well as reduce both the amount and therefore cost of obtaining enough public addresses for every computer in an organization. Hiding the addresses of protected devices has become an increasingly important defense against network reconnaissance.

2.12 CISCO ASA

The Cisco ASA Family of security devices are meant to protect all the corporate and individual private networks and data centers. CISCO ASA provides highly secure access network resources. Cisco ASA devices are used more than 15 years of firewall and network security engineering with more than million security appliances.

Features and Capabilities

Cisco Adaptive Security Appliance (ASA) Software is the sole operating system for the Cisco ASA Family in networking and business. CISCO ASA use delivers enterprise class firewall capabilities for ASA devices for any distributed network infrastructure. ASA Software also used with other highly secured critical security technologies to deliver smart solutions that meet continuously increasing security needs.

Cisco ASA Software is used in following categories:

CISCO ASA Offers integrated VPN, and Unified secure Communications capabilities.

. It helps private corporates to increase capacity and improve performance through high-performance, multi-node networking.

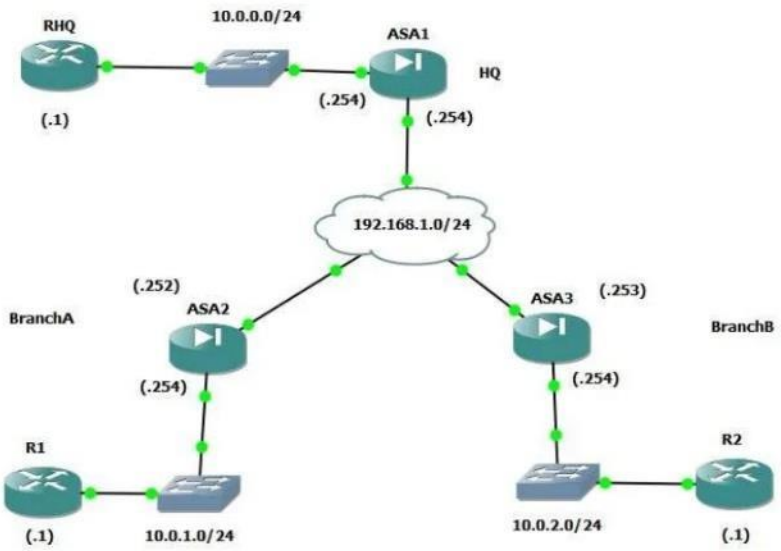
. It delivers high availability for high efficiency networking applications.

. It provides an interface between physical and virtual devices.

. It meets the vibrant needs of the network and the data centers.

. It provides context awareness with Cisco Trust security group tag technology in private corporate organizations.

Configuration



Results and Discussions

As we have completed a minor part during these months of our project, the following results has been reflected

1. Basic Routing Successful
2. RIP Routing Successful
3. Configuring Access List Successful

Conclusion

To conclude we would like to say that we have successfully completed the basic and soul purpose of our project which is to create a Redundant LAN Network which Offers fault tolerance and efficient load balancing across its internal network.

The Basic Fundamentals and aims we think we have successfully achieved and implemented but as nothing can be perfect so as my project, it needs better implications in future.

According to us we have completed our project still we are left with lots of improvements and enhancements of this projected structure. We will try my level best to complete it in our near future.

Recommendations

Although I have completed my project successfully but there can be made few extensions

1. CISCO PACKET TRACER should be updated to next version, as it lags sometimes.

2. Using different colors in the software makes it easy to understand the difficult network architecture.

4. We will try to make a network topology in GNS3 which is precisely broader to realize, means there should be sufficient gap between router, switch and multilayer switches.

Implications for Future Research

We will apply all our described networking topologies and protocols in GNS 3 softaware to make an efficient redundant LAN Network. Going through all the steps it is very easy to configure th whole network in our near future. Two or more laptops will be required to show to network connection and to verify it as it is working ornot in a proper way.

To increase the redundancy quotent Cisco Adaptive Appliance Security we will apply which will work as a security measurement interface in the network. By using firewalls we will be implementing security in the network.

Before setting up the network planning is done in which redundancy is made so we will be providing redundancy in the network so if there is any failure the traffic is routed through different path.

We will be implementing how a user or client can access the resources of office sitting at home which is great advantage according to user point of view.

Appendix

Working in CISCO Packet Tracer Software is very interesting according to me. We know our generation is fond of mobiles and their configuration (Android, IOS, Symbian) Going through the CISCO Packet Tracer software I understood that it is very similar because everything you are configuring is clearly visible as there is not any virtual level, you can test your correctness of

configuration while you are writing the program, may be in routers, in switches or in servers(Command Line Interface or in Global Configuration Mode). It was a nice experience working in this highly customizable Network Simulation Software.

References

1. HP Advanced Concept of Networking Material.

2. Network Convergence-Sridhar Iyer

3. CISCO Packet Tracer Module (v 6.0.1)

5. Internet

THANK YOU