SECURING COMMUNICATIONS BETWEEN DUAL MULTI-CAMPUS CORE

Report

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR
Minor Project

Submitted By:-
Manpreet Kaur
Branch: Information Technology
Univ. Roll No. 1905361
Class Roll No. 1921062

Department of Information Technology
GURU NANAK DEV ENGINEERING COLLEGE,
LUDHIANA, INDIA

SECURING COMMUNICATIONS BETWEEN DUAL MULTI-CAMPUS CORE

Report

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR
Minor Project

Submitted By:-
Manpreet Kaur
Branch: Information Technology
Univ. Roll No. 1905361
Class Roll No. 1921062

Department of Information Technology
GURU NANAK DEV ENGINEERING COLLEGE,
LUDHIANA, INDIA

Student's Declaration

I hereby certify that the work which is being presented in this training report with the project entitled as SECURING COMMUNICATIONS BETWEEN DUAL CORE MULTI-CAMPUS by Manpreet Kaur, University Roll No. 1905361 in partial fulfilment of requirements for the award of degree of B.Tech. (Information Technology) submitted in the Department of Information Technology at GURU NANAK DEV ENGINEERING COLLEGE, LUDHIANA under I.K. GUJRAL PUNJAB TECHNICAL UNIVERSITY is an authentic record of my own work carried out under the supervision of Prof. Mohanjit Kaur. The matter presented has not been submitted by me in any other University/ Institute for the award of B.Tech. Degree.

Student Name: Manpreet Kaur

Univ. Roll No. 1905361

(Signature of Student)

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Signature of Internal Examiner

The External Viva-Voce Examination of the student has been held on

Signature of External Examiner

Signature of HOD

Acknowledgment

I am highly grateful to the Dr. Sehijpal Singh, Principal, Guru Nanak Dev Engineering College (GNDEC), Ludhiana, for providing this opportunity to carry out the four weeks industrial training at IVY Institute of Advanced Education.

The constant guidance and encouragement received from Dr. K. S. Mann, HOD-IT, GNDEC, Ludhiana has been of great help in carrying out the project work and is acknowledged with reverential thanks.

I would like to express a deep sense of gratitude and thanks profusely to our Project guide Mrs. Mohanjit Kaur (Assistant Professor, GNDEC Ludhiana). Without the wise counsel and able guidance, it would have been impossible to complete the report in this manner.

The help rendered by her for experimentation is greatly acknowledged. I express gratitude to other faculty members of Information Technology department of GNDEC for their intellectual support throughout the course of this work.

Finally, I am indebted to all whosoever have contributed in this report work.

Banipreet Singh (1905315)
Manpreet Kaur (1905361)
Komaldeep Singh Mangat (2005011)

Abstract

This project is totally dedicated to the Network Engineer for new and smart learning of the Network Structure. In this concept it is possible for the networker to check the Network Structure of a company spread in the big campus area. The incoming the outgoing traffic can be maintained along with some security concepts as well. In this logic we use the multiple Routing Protocols in different areas of the company. The practical shows us the proper movement of the packet from one part of the company to the other part of the company. The project comprises of the different Departments spread in different buildings of the company. Multiple Routing protocols have been used in different branches and all the departments can communicate with other different departments through the Redistribution among different Routing Protocols. The East Building has a DHCP server for assigning the IP Addresses to the Hosts in

the building as well as a DHCP server has been used in the West Building as well. The Internet Service Provider has been used for Communication of the East West Building with the Data Centre Internet through ISP, using the Frame Relay Switching Technology available for Wide Area Network. Routing Protocols EIGRP along with the Synchronous Number, Static Routing its concepts including the Default Routing as well has been applied. The different Routing Protocols are running and which has been synchronized to work with Frame Relay Switching Technology. This project has designed on large network design data secure e-commerce server.

In this project we are telling that how to forward the data, videos, voice in the network. We also told that how to access data security. We have used different kind of devices in the network like router, switches, pcs, servers and wi-fi. We are explaining that how to access, secure the data on different location, and how company provides data high speed. Whatever we design the network in this project i.e. in different locations but every location is connected to each other. We have used different kind of media like leased line, frame-relay for connecting the network location we are using the IP address with each media. There are four services has been used such as DNS server, Web-server and DHCP server. DNS server is used to resolve the names. And the last DHCP server is used to assign the automatic IP address.

All the services are enabled for the user in this project but web services is secured only for first user, These services has been disabled by us for the first user.

List of Figures

Contents

1 Introduction

1.1 Introduction to Project

We made this project on college campus in which we have shown two different campuses. These campuses are in WAN network. One campus is located in Ludhiana and another one is in Chandigarh. Both are connected with Internet Service Provider (ISP), by which our domains are not secured. It means those domains which are connected with ISP are not secured. In this project we have configured network security which secures our end to end network. The data which is to be transferred in end to end network will be the secured data and it is not read by the center domain. In this we can send our data in encrypted form. To make the data encrypted, we used VPN-GRE (IPSEC) and security algorithm like HMAC(MD5),SHA,3DES. By which we can use separate IP after changing public or private IP. We encrypt our data on this separate IP. Only that person can decrypt the data who will have key. There is one advantage that we can prevent our data from hacking. We are explaining all the security configuration in the project.

IMPORTANCE OF PROJECT:
Wide Area Networks are spread over a (very) wide area so that companies and institutes that are located far from each other are directly connected via the network. Wide Area Networks have – mostly on more than one location – external connections with other big networks. Internet Service Providers (ISPs) and multinationals with many offices frequently own a WAN themselves. Regional education networks and company networks between several establishments are also examples of Wide Area Networks. Two great advantages of WAN are allowing secure and fast data transmission between the different nodes in the network. Many WANs also implement sophisticated monitoring procedures to account for which users consume the network resources. This is, in some cases, used to generate billing information to charge individual user.

1.2 Objectives of the project

1. Objective of the project is to connect various campus of the college by using LAN and WAN technologies.

2. The project aims to assess the security issues related to access control configuration on a Cisco router on the network and to design an upgraded secure configuration using multiple access control techniques.

3. Currently it is observed that the access to the router is exploited using stolen passwords by users on the network.

4. The identified threat has to be mitigated using appropriate feature and technology available on the router and explanation on how it would achieve the requirement such that only the administrator of the network has access to the router.

1.3 Project Category

The network-based project is the process of developing and creating a network using LAN and WAN technologies. The goal of this project is to make communications easier and more effective.

1.4 Existing System

The existing network consists of hubs and there are dial up connections in between various offices of the College campus because of which both LAN and WAN links are very slow and users regularly face problem in transmitting their data over the links.Most of the time there is network congestion in the network because of which the work is suffering and users are not able to perform up expectation.

1.5 Proposed System

In the proposed design, hubs will be replaced with switches so as to improve the LAN connectivity. Switches would be operating at 100 Mbps as compared to hubs which operate at 10 Mbps. Moreover switches are manageable so VLANS can be created on them so as to decrease broadcast traffic and to enhance security as well. As far as WAN is concerned all the dial up links would be replaced with ISDN, Frame-Relay and Leased Line connection so as to improve WAN connectivity and users don't face network congestion during working hours.

2 Requirement Analysis and System Specification

2.1 Feasibility Study

2.1.1 Economic Feasibility

Economic analysis is the most frequently used method for evaluating the effectiveness of a new system. More commonly known as cost/benefit analysis, the procedure is to determine the benefits and savings that are expected from a candidate system and compare them with costs. If benefits outweigh costs, then the decision is made to design and implement the system.

2.1.2 Legal Feasibility

Determines whether the proposed system conflicts with legal requirements, e.g. a Data Processing system must comply with the local Data Protection Acts.

2.1.3 Operational Feasibility

Is a measure of how well a proposed system solves the problems, and takes advantages of the opportunities identified during scope definition and how it satisfies the requirements identified in the requirements analysis phase of system development.

2.1.4 Resource feasibility

This involves questions such as how much time is available to build the new system, when it can be built, whether it interferes with normal business operations, type and amount of resources required, dependencies, etc. Contingency and mitigation plans should also be stated here.

2.1.5 Cultural feasibility

In this stage, the project's alternatives are evaluated for their impact on the local and general culture. For example, environmental factors need to be considered and these factors are to be well known. Further an enterprise's own culture can clash with the results of the project

2.2 Requirements of the system

Hardware :

- Processor: Intel core i3 or above
- Processor Speed: 2.40 GHz CPU
- RAM: 4 GB or above

Network Requirement :

- Network Topology diagram.
- Identify the hardware required like routers, switches, access points (Cisco)
- The network has to be segregated into guest and staff
- The guest network should not have access to the staff network.
- TCP/IP Network design and IP address table.
- Configurations and features which are required to be configured on the devices.

The project aims to assess the security issues related to access control configuration on a Cisco router on the network and to design an upgraded secure configuration using multiple access control techniques. Currently it is observed that the access to the router is exploited using stolen passwords by users on the network. The identified threat has to be mitigated using appropriate feature and technology available on the router and explanation on how it would achieve the requirement such that only the administrator of the network has access to the router

Network and Security requirement:

- Only the administrator should have access to the route.
- The access control should have multiple level of security.
- Users on the network should be unable to access the router.
- Unique passwords should be used wherever appropriate.

3 System Design

3.1 Design Approach

The project ”Securing Communications between Dual Multi- Campus Core” is Function-oriented. System design is to deliver the requirements as specified in the feasibility report. The main objectives of the design are:

1. Security
2. Cost
3. Flexibility
4. Efficiency

3.2 Detail Design

3.2.1 Devices Used

1. 5 Serial Cables
2. 4 Multi Layer Switches
3. 12 Copper Cross over
4. 33 Copper Straight Through
5. 6 Routers
6. 4 Switches (Layer 2)
7. 26 PCs
8. 6 Servers

3.2.2 Protocols Used

1. EIGRP
2. Static Routing
3. Default Routing
4. VTP (VLAN Trunking Protocol) at all Switches
5. Inter VLAN Routing
6. Subnet Masking
7. Wild card MAsking
8. STP (Spanning Tree Protocol)
9. NAT (Network Address Translation)

3.3 System Design

The various devices that are being used in designing the network are as follows:

- **NIC**
  A network interface card, network adapter, network interface controller (NIC), network interface card, or LAN adapter is a computer hardware component designed to allow computers to communicate over a computer network. It is both an OSI layer 1 (physical layer) and layer 2 (data link layer) device, as it provides physical access to a networking medium and provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other either by using cables or wirelessly.

Figure 1: Network Interface Card

Although other network technologies exist, Ethernet has achieved near-ubiquity since the mid-1990s. Every Ethernet network card has a unique 48-bit serial number called a MAC address, which is stored in ROM carried on the card. Every computer on an Ethernet network must have a card with a unique MAC address. Normally it is safe to assume that no two network cards will share the same address, because card vendors purchase blocks of addresses from the Institute of Electrical and Electronics Engineers (IEEE) and assign a unique address to each card at the time of manufacture.

- ROUTER-A router is a device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANS or WANS or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect, and are the critical device that keeps data Flowing between networks and keeps the networks connected to the internet When data is sent between locations on one network or from one network to a second network the data is always seen and directed to the correct location by the router.

  The router accomplishes this by using headers and forwarding tables to determine the best path for forwarding the data packets, and they also use protocols such as ICMP to communicate with each other and configure the best route between any two hosts.

Figure 2: Router

- **SWITCH**
  A switch is an electrical component that can break an electrical circuit, interrupting the current or diverting it from one conductor to another. The most familiar form of switch is a manually operated electromechanical device with one or more sets of electric contacts. Each set of contacts can be in one of two states either 'closed meaning the contacts are touching and electricity can flow between them, or 'open', meaning the contacts are separated and non-conducting. A switch may be directly manipulated by a human as a control signal to a system, such as a computer keyboard button, or to control power flow in a circuit, such as a light switch. Automatically-operated switches can be used to control the motions of machines, for example, to indicate that a garage door has reached its full open position or that a machine tool is in a position to accept another work piece. Switches may be operated by process variables such as pressure, temperature, flow, current, voltage, and force, acting as sensors in a process and used to automatically control a system. For example, a thermostat is an automatically-operated switch used to control a heating process. A switch that is operated by another electrical circuit is called a relay. Large switches may be remotely operated by a motor drive mechanism.

Figure 3: Switch

- **ASA FIREWALL 5505**
  A firewall is a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules. Acting as a barrier between a trusted network and other untrusted networks – such as the Internet – or less-trusted

networks – such as a retail merchant's network outside of a cardholder data environment – a firewall controls access to the resources of a network through a positive control model. This means that the only traffic allowed onto the network defined in the firewall policy is; all other traffic is denied

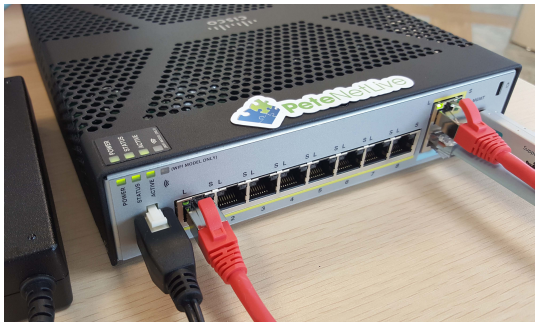

Figure 4: ASA Firewall

- **Optical Fibre Cabe**
  A fiber-optic cable is composed of very thin strands of glass or plastic known as optical fibers; one cable can have as few as two strands or as many as several hundreds of them. These optical fiber cables carry information in the form of data between two places using optical or light-based technology. Once the light beams travel down the optical fiber cable (OFC), they would emerge at the other end. A photoelectric cell will be required to turn the pulses of light back into electrical information the computer could understand.

  While travelling down fiber optic cable, light repeatedly off the walls. The beam of light does not leak out of the edges because it hits the glass at really shallow angles. And then it reflects back again as if the glass was really a mirror. This is called total internal reflection. The other factor that keeps it in the pipe is the cable structure.

The various WAN technologies that are being used in the design of MNC network as follows:

- Leased line - Looking for fast and reliable Net access with zero down time. A leased line may be the answer to your access woes. When you conduct business on the Internet, your company needs access that is dependable and fast. Time is money, and downtime or slow transfers can cost many times more than what you actually pay for your connections. Leased lines addresses these issues.

  Leased lines are dedicated circuits provided by Basic Service Providers (BSP), which provide permanent connectivity to the Internet. Leased lines provide the last mile access from the user premises to the ISP They provide permanent connection as compared to the temporary connectivity through dialup access. The quality of the connection is far superior to what is normally available through dialup, thanks to digital signaling, less noise, fewer exchanges etc.

Leased lines provides a scalable access method, important particularly for organizations with large user groups, including corporate, banks and financial institutions, educational and RD organizations, government, military etc. Starting typically with 64 Kbps, it is possible to deploy a scalable architecture, with multiples of E1 (2 MBPS) pipes, providing the necessary bandwidth. In fact, leased access becomes a must for large organizations in most situations. Since the access is ”always on”, it is possible to associate a pool

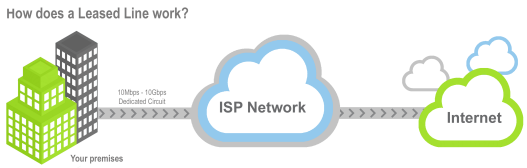

Figure 5: Lease-Line

of permanent IP addresses with a particular leased line. Normally, the ISP would provide 16/32 IP addresses for each 64 Kbps chunk of bandwidth. Using these IP addresses it becomes possible to deploy a variety of services such as mail, FTP, WWW, DNS, and proxy, to name the most common requirements of organizations. In other words, leased lines enable hosting of services of all types, and provide a platform for enterprise intranets and extranets, apart from what we may term as ”entry level” services such as messaging, which still account for over 70 percent of all Internet access.

We can look at two types of equipment requirements. The first set of hardware is required for establishing the last mile link between the customer premises and the ISP. Currently, 64 Kbps and 2 Mbps leased line modems are commonly deployed for terrestrial leased line access to the Net. The equipment required is one pair of leased line modems (one each with V.35 and G.703 interface) and one G.703/V.35 interface converter, supporting either 64 Kbps or 2 Mbps.

The other set of equipment required is at the customer premises. This includes a router and various servers as needed in specific sites. The router establishes the link with the ISP. Typically, users need to consider services like DNS, mail, proxy, firewall, FTP, databases, file servers, and security services which can be set up on the available connectivity.

Applications of Leased Line:

Point-to-Point for data only: One of the widely used applications of leased lines is having a secure dedicated data circuit between two locations via a private line, used to transmit data at a constant speed equal to the bandwidth of the circuit.

Point-to-point: For Voice and Data : This kind of application allows transmission of voice and data over the same connection. Here also two separate locations are joined together. This type of configuration is commonly provided on a higher bandwidth circuit. The bandwidth of the circuit is divided into individual voice channels and data channels.

Multiplexing: Multiplexing basically connects multiple remote sites to a single centralized location. Typically a connection originating at the host location is connected into a

multiplexer at a service provider's end. At the multiplexer, the host circuit is split into smaller individual circuits, and those are then delivered to the remote sites.

Advantages: It provides permanent, reliable, high-speed connectivity as compared to the temporary connectivity of dial up access. The quality of the connection is far superior to what is normally available through dialup, because of the digital signaling, less noise, fewer exchanges etc.

Disadvantages: Leased bandwidth prices are quite high, compared to dialup bandwidth of comparable size. Entry level annual port prices are also high at present, so that this access method is only feasible beyond a fairly high threshold level.

Permanent connectivity to the Net exposes the organization to a variety of threats including hacking, malicious code including active vandals, viruses. Trojan Horses, macros, denial of service attacks etc.

- DNS Server- DNS is a network protocol used to translate hostnames into IP addresses. DNS is not required to establish a network connection, but it is much more user friendly for human users than the numeric addressing scheme. Consider this example - you can access the Google homepage by typing 216.58.207.206, but it's much easier just to type www.google.com.

  To use DNS, you must have a DNS server configured to handle the resolution process. A DNS server has a special-purpose application installed. The application maintains a table of dynamic or static hostname-to-IP address mappings. When a user request some network resource using a hostname. (e.g. by typing www.google.com in a browser), a DNS request is sent to the DNS server asking for the IP address of the hostname. The DNS server then replies with the IP address. The user's browser can now use that IP address to access the webpage.

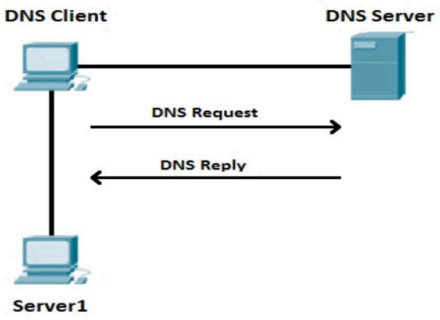

Figure 6: DNS Server

- Web Server- WEB SERVER- A Web server is a program that uses HTTP (Hypertext Transfer Protocol) to serve the files that form Web pages to users, in response to their requests, which are forwarded by their computers' HTTP clients. Dedicated computers and appliances may be referred to as Web servers as well.

The process is an example of the client/server model. All computers that host Web sites must have Web server programs. Leading Web servers include Apache (the most widely-installed Web server), Microsoft's Internet Information Server (IIS) and nginx (pronounced engine X) from NGNIX. Other Webers include Novell's NetWare server, Google Web Server (GWS) and IBM's family of Domino servers. Web servers often

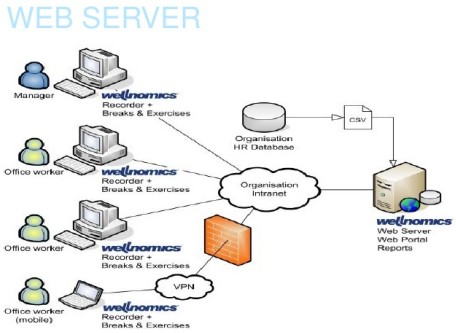

Figure 7: Web Server

come as part of a larger package of Internet- and intranet-related programs for serving email, downloading requests for File Transfer Protocol (FTP)) files, and building and publishing Web pages. Considerations in choosing a Web server include how well it works with the operating system and other servers, its ability to handle server-side programming, security characteristics, and the particular publishing, search engine and site building tools that come with it.

- Frame-Relay- Frame Relay is a high-performance WAN protocol that operates at the physical and data link layers of the OSI reference model. Frame Relay originally was designed for use across Integrated Services Digital Network (ISDN) interfaces. Today, it is used over a variety of other network interfaces as well. This chapter focuses on Frame Relay's specifications and applications in the context of WAN services.

  Frame Relay is an example of a packet-switched technology. Packet-switched networks enable end stations to dynamically share the network medium and the available bandwidth. The following two techniques are used in packet-switching technology:

  1. Variable-length packets
  2. Statistical multiplexing

  Variable-length packets are used for more efficient and flexible data transfers. These packets are switched between the various segments in the network until the destination is reached.

  Statistical multiplexing techniques control network access in a packet-switched network. The advantage of this technique is that it accommodates more flexibility and more efficient use of bandwidth. Most of today's popular LANS, such as Ethernet and Token Ring, are packet switched networks.

Frame Relay often is described as a streamlined version of X.25, offering fewer of the robust capabilities, such as windowing and retransmission of last data that are offered in X.25. This is because Frame Relay typically operates over WAN facilities that offer more reliable connection services and a higher degree of reliability than the facilities available during the late 1970s and early 1980s that served as the common platforms for X.25 WANs. As mentioned earlier, Frame Relay is strictly a Layer 2 protocol suite, whereas X.25 provides services at Layer 3 (the network layer) as well. This enables Frame Relay to offer higher performance and greater transmission efficiency than X.25, and makes Frame Relay suitable for current WAN applications, such as LAN interconnection.

3.4 Methodology

- For safe and secure communication between two buildings, suppose MBA Block and Admin Office. Start by establishing a LAN (Local Area Network) in each building and then connect the two buildings by using WAN (Wide Area Network).
- Connect the WAN of both the buildings through routers by applying following protocols such as, EBGP (External Border Gateway Protocol), OSPF (Open Shortest Path First), ISP (Internet Service Provider) etc.
- After the connection is established, the messages which are to be sent are encrypted thoroughly, using some algorithms such as HMAC (Hash- Based Message authentication Code), 3DES (Data Encryption Standard).
- By symmetric Encryption, the data is encrypted and is sent to VPN-GRE tunnel. When message is received, it is decrypted by using the same key.
- Hence our message is reached successfully. For every message which is to be sent is sent by using the same protocols as mentioned above.
- The biggest benefit of using this is that it is feasible and can be managed easily and provide more security than the existing system.
- As we use tunnel like technique which is G.R.E (Generic Routing Encapsulation).In this the data is encapsulated and is sent through more secure path. Which is hidden from the intruders hence providing less chances of data leakage.

4 Implementation, Testing and Maintenance

4.1 Introduction to Languages, IDE's,Tools and Technologies used for implementation

SIMULATOR

A network simulator is a piece of software or hardware that predicts the behavior of a network, without an actual network being present. Network simulators serve a variety of needs. Compared to the cost and time involved in setting up an entire test bed containing multiple networked computers, routers and datalinks, network simulators are relatively fast and inexpensive. They allow engineers to test scenarios that might be particularly difficult or expensive to emulate using real hardware- for instance, simulating the effects of a sudden burst in traffic or a DoS attack on a network service. Networking simulators are particularly useful in allowing designers to test new networking protocols or changes to existing protocols in a controlled and reproducible environment.

Network simulators, as the name suggests are used by researchers, developers and QA to design various kinds of networks, simulate and then analyze the effect of various parameters on the network performance. A typical network simulator encompasses a wide range of networking technologies and help the users to build complex networks from basic building blocks like variety of nodes and links. With the help of simulators one can design hierarchical networks using various types of nodes like computers, hubs, bridges, routers, optical cross-connects, multicast routers, mobile units, MSAUs etc. The simulator that we have used to create a simulation of the network design is GNS3.

Figure 8: GNS3

GNS 3

GNS3 is used by hundreds of thousands of network engineers worldwide to emulate, configure, test and troubleshoot virtual and real networks. GNS3 allows you to run a small topology con-

sisting of only a few devices on your laptop, to those that have many devices hosted on multiple servers or even hosted in the cloud.

GNS3 is open source, free software that you can download from http://gns3.com

It is actively developed and supported and has a growing community of over 800,000 members. By joining the GNS3 community you will be joining fellow students, network engineers, architects and others that have downloaded GNS3 over 10 million times to date. GNS3 is used in companies all over the world including Fortune 500 companies.

GNS3 can help you prepare for certification exams such as the Cisco CCNA, but also help you test and verify real world deployments. Jeremy Grossman, the original developer of GNS3 originally created the software to help him study for his CCNP certifications. Because of that original work, you can today use to help you do the same without paying for expensive hardware.

GNS3 has allowed network engineers to virtualize real hardware devices for over 10 years. Originally only emulating Cisco devices using software called Dynamips, GNS3 has now evolved and supports many devices from multiple network vendors including Cisco virtual switches, Cisco ASAs, Brocade vRouters, Cumulus Linux switches, Docker instances, HPE VSRs, multiple Linux appliances and many others.

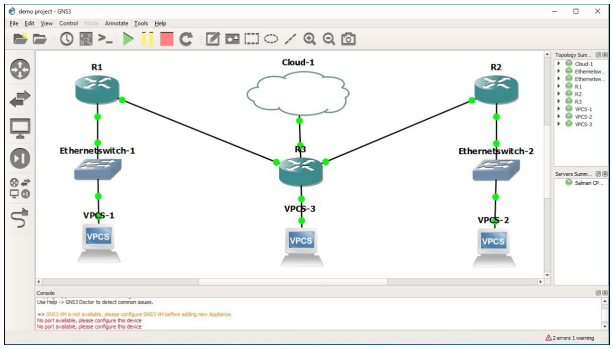

Figure 9: GNS3 Demo Network

Wireshark

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network.

Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

1. Packet Capture: Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.

2. Filtering: Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.

3. Visualization: Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

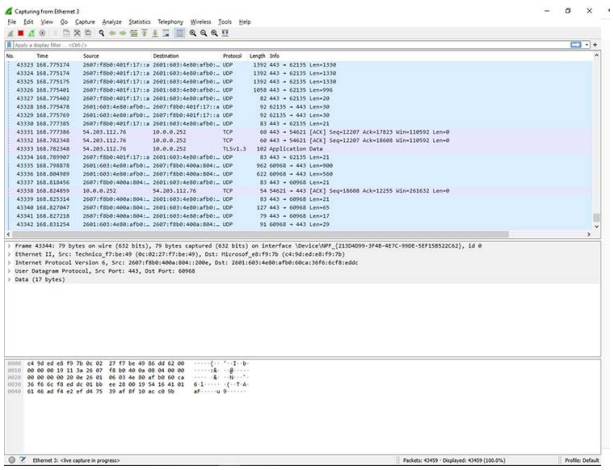

Figure 10: Wireshark

Various Protocols used in the project.

- **EIGRP**
  Historically speaking, the first IPv4 routing protocols used DV logic. RIP Version 1 (RIP-1) was the first popularly used IP routing protocol, with the Cisco-proprietary Interior Gateway Routing Protocol (IGRP) being introduced a little later, as shown in the figure below. By the early 1990s, business and technical factors pushed the IPv4 world

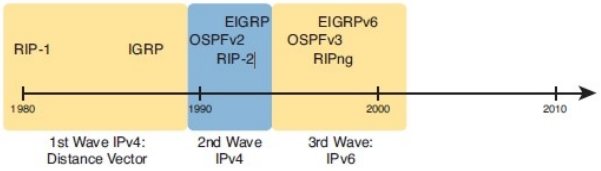

Figure 11: EIGRP Protocol

toward a second wave of better routing protocols. First, RIP-1 and IGRP had some technical limitations, even though they were great options for the technology levels of the 1980s. The bigger motivation for better routing protocols was the huge movement toward TCP/IP in the 1990s.

Many enterprises migrated from older vendor-proprietary networks to networks built with routers, LANs, and TCP/IP. So, with so many IPv4 routing protocols, how would a network engineer choose the right routing protocol? Engineers should consider two key points about EIGRP that drive them toward wanting to use it:

1. EIGRP uses a robust metric based on both link bandwidth and link delay, so routers make more efficient choices about the best route to use.
2. EIGRP converges quickly, meaning that when something changes in the internetwork, EIGRP quickly finds the currently best loop-free routes to use.

EIGRP does not send full or partial update messages based on a periodic timer, as a result EIGRP cannot rely on update messages to monitor the state of its neighbors. So, EIGRP uses the same basic communication method as OSPF does; Hello messages. The EIGRP Hello message and protocol define that each router should send a periodic Hello message on each interface, so that all EIGRP routers know that the router is still working. The font image is a simple illustration of it.

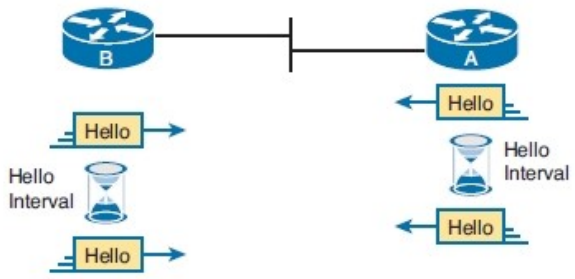

Figure 12: GNS3 EIGRP Working

The routers use their own independent Hello Interval, which defines the time period between each EIGRP Hello message. For instance, routers R1 and R2 do not have to send their Hello messages at the same time. Routers also must receive a Hello from a neighbor after a certain interval called the Hold Interval, with a default value of four times the Hello Interval.

- **OSPF**
  Stands for ”Open Shortest Path First”. OSPF is a method of finding the shortest path from one router to another in a local area network (LAN). As long as a network is IP-based, the OSPF algorithm will calculate the most efficient way for data to be transmitted. If there are several routers on a network, OSPF builds a table (or topography) of the router connections. When data is sent from one location to another, the OSPF algorithm compares the available options and chooses the most efficient way for the data to be sent. This limits unnecessary delays in data transmission and prevents infinite loops.

  OSPF (Open Shortest Path First) is a router protocol used within larger autonomous system networks in preference to the Routing Information Protocol (RIP), an older routing protocol that is installed in many of today’s corporate networks. Like RIP, OSPF is designated by the Internet Engineering Task Force (IETE) as one of several Interior Gateway Protocols (IGPs).

  So that all will have the same routing table information. Unlike the RIP in which the entire routing table is sent, the host using OSPF sends only the part that has Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately multicasts the information to all other hosts in the network changed. With RIP, the routing table is sent to a neighbor host every 30 seconds. OSPF multicasts the updated information only when a change has taken place. Rather than simply counting the number of hops, OSPF bases its path descriptions on ”link states” that take into account additional network information. OSPF also lets the user assign cost metrics to a given

host router so that some paths are given preference. OSPF supports a variable network subnet mask so that a network can be subdivided. RIP is supported within OSPF for router-to-end station communication. Since many networks using RIP are already in use, router manufacturers tend to include RIP support within a router designed primarily for OSPF.

- **BGP**
  Border Gateway Protocol (BGP) is a standardized gateway protocol that exchanges routing information across autonomous systems (AS) on the Internet. Border Gateway Protocol is the protocol that makes the Internet work. Networks or autonomous systems that need to interact with each other do so through peering, which is made possible with BGP.

  When one network router is connected to other networks it cannot determine which network is the best network to send its data to by itself. Border Gateway Protocol considers all peering partners that a router has and sends traffic to the router that is closest to the data's destination. This communication is possible because, at boot, BGP allows peers to communicate their routing information and then stores that information in a Routing Information Base (RIB).

  Border Gateway Protocol was originally created in 1989 as a quick fix for the Internet but it has remained the primary protocol for long distance traffic. Since then, however, cyber threats have evolved and BGP has not kept up. Border Gateway Protocol abuse is called BGP hijacking which is possible because the protocol relies on trusting advertised routes. There have been multiple attempts at making a more secure version of BGP but implementation is extremely problematic. Most of the new versions are unable to communicate with standard BGP which means that every AS across the world would have to adopt the new protocol simultaneously.

- **VPN IPSEC**
  Site-to-Site IPSec VPN Tunnels are used to allow the secure transmission of data, voice and video between two sites (e.g offices or branches). The VPN tunnel is created over the Internet public network and encrypted using a number of advanced encryption algorithms to provide confidentiality of the data transmitted between the two sites.

  IPSec VPN tunnels can also be configured using GRE (Generic Routing Encapsulation) Tunnels with IPsec. GRE tunnels greatly simply the configuration and administration of VPN tunnels and are covered in our Configuring Point-to-Point GRE VPN Tunnels article. Lastly, DMVPNs – a new VPN trend that provide major flexibility and almost no administration overhead can also be examined by reading our Understanding Cisco Dynamic Multipoint VPN (DMVPN), Dynamic Multipoint VPN (DMVPN) Deployment Models Architectures and Configuring Cisco Dynamic Multipoint VPN (DMVPN) - Hub, Spokes , mGRE Protection and Routing - DMVPN Configuration articles. Site 1 is configured with an internal network of 10.10.10.0/24, while Site 2 is configured with network 20.20.20.0/24. The goal is to securely connect both LAN networks and allow full communication between them, without any restrictions.

- **STP**
  Spanning Tree Protocol (STP) is a Layer 2 network protocol used to prevent looping

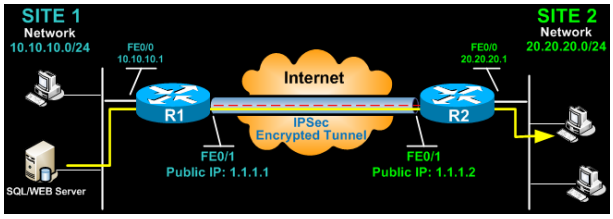

Figure 13: Configuration

within a network topology. STP was created to avoid the problems that arise when computers exchange data on a local area network (LAN) that contains redundant paths. If the flow of traffic is not carefully monitored and controlled, the data can be caught in a loop that circles around network segments, affecting performance and bringing traffic to a near halt.

Networks are often configured with redundant paths when connecting network segments. Although redundancy can help protect against disaster, it can also lead to bridge or switch looping. Looping occurs when data travels from a source to a destination along redundant paths and the data begins to circle around the same paths, becoming amplified and resulting in a broadcast storm.

STP can help prevent bridge looping on LANs that include redundant links. Without STP, it would be difficult to implement that redundancy and still avoid network looping. STP monitors all network links, identifies redundant connections and disables the ports that can lead to looping.

- **NAT**
  To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required. Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on a router or firewall.

  Generally, the border router is configured for NAT i.e the router which has one interface in the local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

  If NAT runs out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.

- **GRE Tunnel**

Tunneling is a concept where we put ‘packets into packets’ so that they can be transported over certain networks. We also call this encapsulation. A good example is when you have two sites with IPv6 addresses on their LAN but they are only connected to the Internet with IPv4 addresses.Normally it would be impossible for the two IPv6 LANs to reach each other but by using tunneling the two routers will put IPv6 packets into IPv4 packets so that our IPv6 traffic can be routed on the Internet. Another example is where we have an HQ and a branch site and you want to run a routing protocol like RIP, OSPF or EIGRP between them. We can tunnel these routing protocols so that the HQ and branch router can exchange routing information. Basically when you configure a tunnel, it’s like you create a point-to-point connection between the two devices. GRE (Generic Routing Encapsulation) is a simple tunneling technique that can do this for us. Let me show you a topology that we will use to demonstrate GRE: Above we have 3 routers connected to

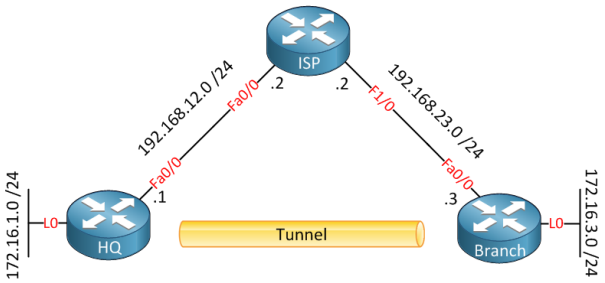

Figure 14: GRE Tunnel Protocol

each other. On the left side we have the “HQ” router which is our headquarters. On the right side there is a “Branch” router that is supposed to be a branch office. Both routers are connected to the Internet, in the middle on top there is an ISP router. We can use this topology to simulate two routers that are connected to the Internet. The HQ and Branch router each have a loopback interface that represents the LAN.

- **Autonomous Number (AS)**
  Autonomous System Number (ASN) is a globally unique identifier that defines a group of one or more IP prefixes run by one or more network operators that maintain a single, clearly-defined routing policy. These groups of IP prefixes are known as autonomous systems. The ASN allows the autonomous systems to exchange routing information with other autonomous systems.
  Benefits of AS Number:

  1. Network operators can have their own network identity internally and externally
  2. The capability of establishing own Border Gateway Protocol with a public ASN
  3. Ability to directly peer with Internet Exchange Points
  4. Flexible Network Management
  5. Network operators can have better control of the traffic
  6. IP Address portability is one of the major benefits of using own IP address and ASN

4.2 Testing Techniques and Test Plans

4.2.1 Ping

Ping can test the speed of your connection, ”distance” to target, and whether or not your connection is even up and running. It tells you how long a packet of data takes to travel from your computer to a specified host, and back again(in this case, the packet is 32 bytes in size).
Ping Tests Once you have your command prompt (or WhatRoute) open, enter ping 127.0.0.1 and press Enter. You should receive 4 responses similar to the lines below. This ping test verifies the operation of the base TCP/IP stack. If TCP/IP is working correctly, there will be no problems with the ping. If you receive a timeout or error message, there is a problem with TCP/IP in which case you may have to uninstall and reinstall TCP/IP.

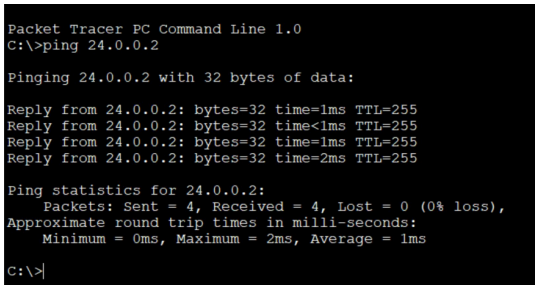

Figure 15: Trouble-Shooting-1

Ping your IP* and press Enter. The ”XXX” indicates your IP address and can be found by using the ipconfig /all command. Pinging your IP verifies that the physical network device can be addressed. If you cannot ping your own IP address, make sure the IP is correctly entered in the Network Control Panel (NCP). If it is correct, replace TCP/IP. If this does not work, the network card may not be properly installed or ’bad’ in which case you may need to reinstall the NIC.

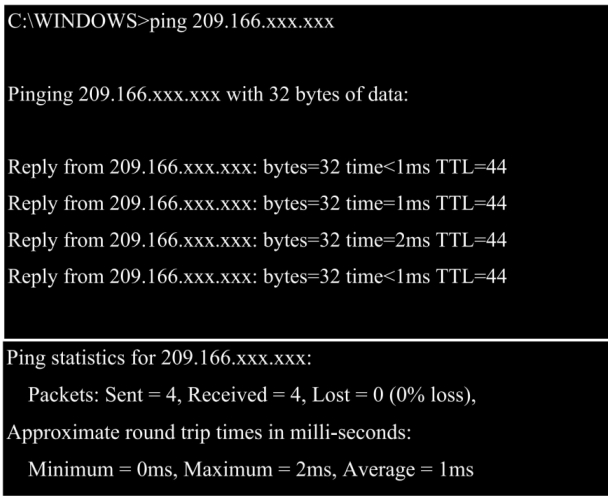

Figure 16: Trouble-Shooting-2

Enter ping 209.166.161.121 and press Enter. This test checks that your connection to the Internet is active and that the network can be accessed. You should receive 4 responses similar to the lines below. Now enter ping www.expedient.net or another server name (e.g.,

```
C:\WINDOWS>ping 209.166.161.121

Pinging 209.166.161.121 with 32 bytes of data:

Reply from 209.166.161.121: bytes=32 time<1ms TTL=44
Reply from 209.166.161.121: bytes=32 time=1ms TTL=44
Reply from 209.166.161.121: bytes=32 time=2ms TTL=44
Reply from 209.166.161.121: bytes=32 time<1ms TTL=44

Ping statistics for 209.166.161.121:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Figure 17: Trouble-Shooting-3

www.yahoo.com) and press Enter. This test checks that your computer is able to translate name addresses (like www.expedient.net or www.yahoo.com) to numbers (like 209.166.165.174 or 64.58.76.224) - DNS resolution. You should receive 4 responses similar to the lines below. If you do not receive responses, check your DNS configuration settings.

```
C:\WINDOWS>ping www.expedient.net

Pinging corp01.web.pitdc1.expedient.net [208.40.175.241] with 32 bytes of
data:

Reply from 208.40.175.241: bytes=32 time<1ms TTL=44
Reply from 208.40.175.241: bytes=32 time=1ms TTL=44
Reply from 208.40.175.241: bytes=32 time=2ms TTL=44
Reply from 208.40.175.241: bytes=32 time<1ms TTL=44

Ping statistics for 208.40.175.241:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

Figure 18: Trouble-Shooting-4

4.2.2 Traceroute

Traceroute tracks the path that a packet takes from your computer to a destination address. A traceroute also shows how many times your packets are being rebroadcast by other servers until it gets to the final destination. For windows users, the command is tracert. For Macintosh OS X users, its traceroute. Example:

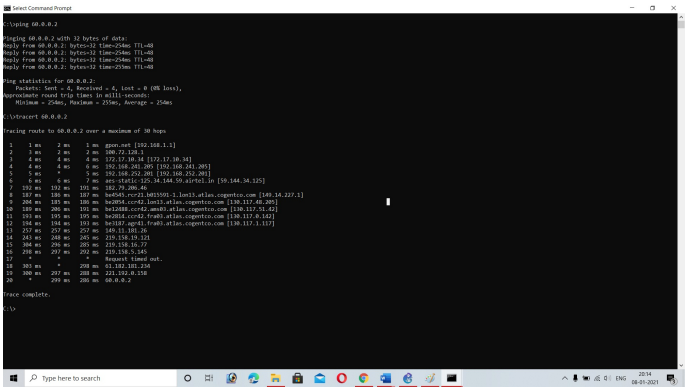

Figure 19: Trouble-Shooting-5

5 Results and Discussions

5.1 User Interface Representation (Of Respective Project)

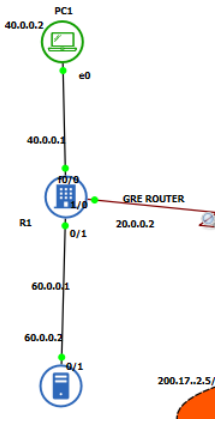

Figure 20: End user PC-1

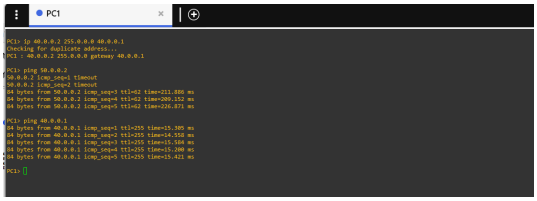

Figure 21: PC-1 ping

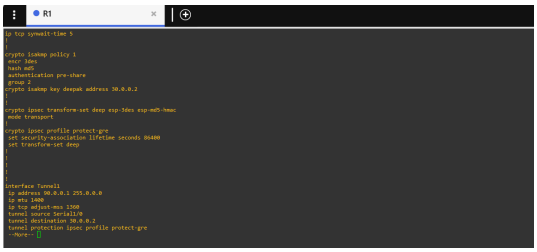

Figure 22: Router 1 configuration

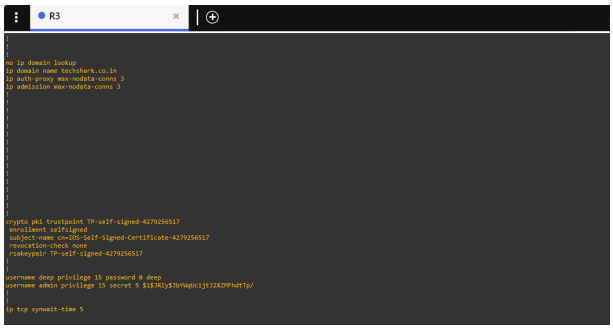

Figure 23: Router 3 (Server) configuration

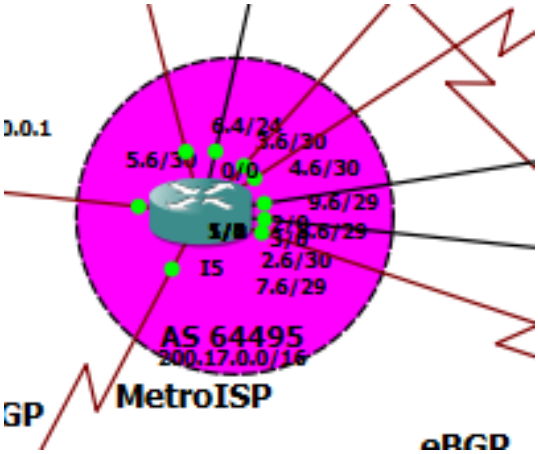

Figure 24: I5 Router

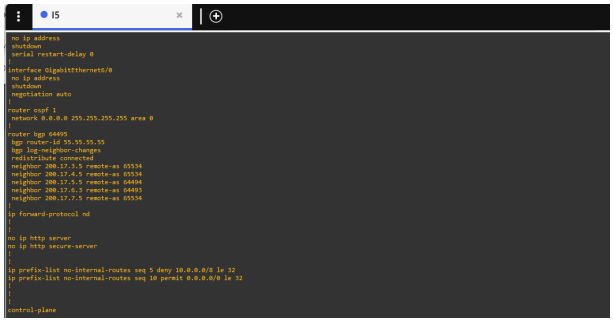

Figure 25: I5 Router Configuration

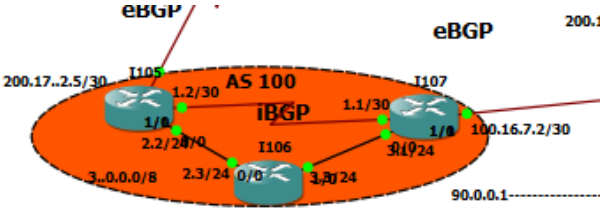

Figure 26: I105 Router

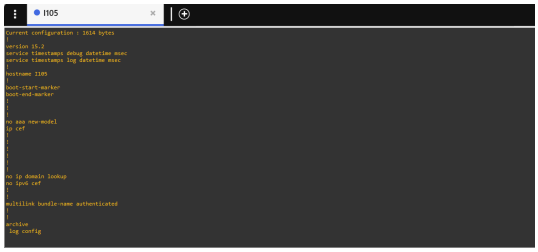

Figure 27: I105 Router Configuration

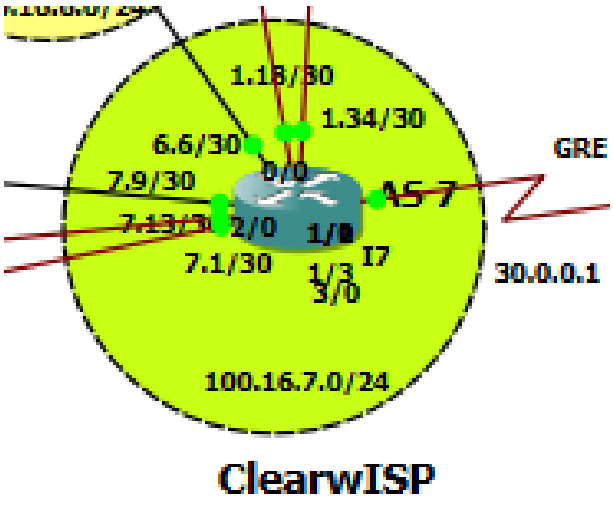

Figure 28: I7 Router

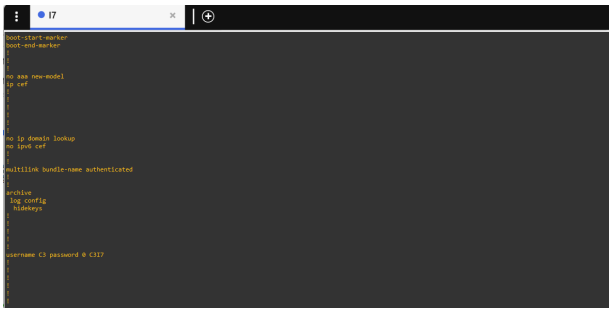

Figure 29: I7 Router Configuration

Figure 30: Router 2 Configuration

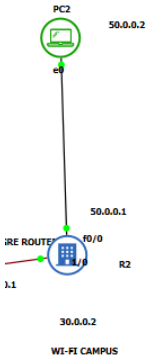

Figure 31: End user PC-2

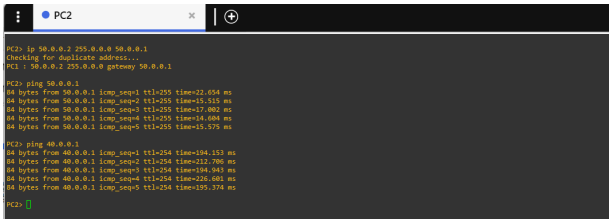

Figure 32: PC-2 ping

5.2 Snapshots of the system

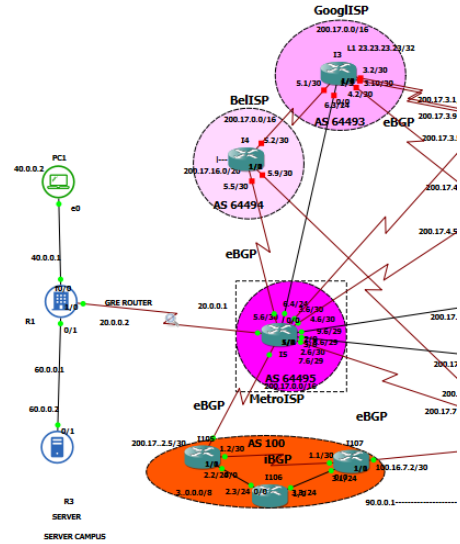

Figure 33: Project (Part-1)

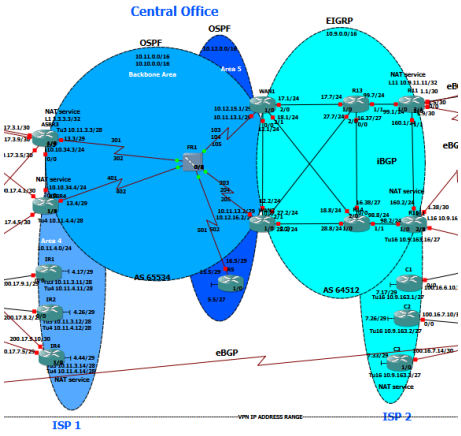

Figure 34: Project (Part-2)

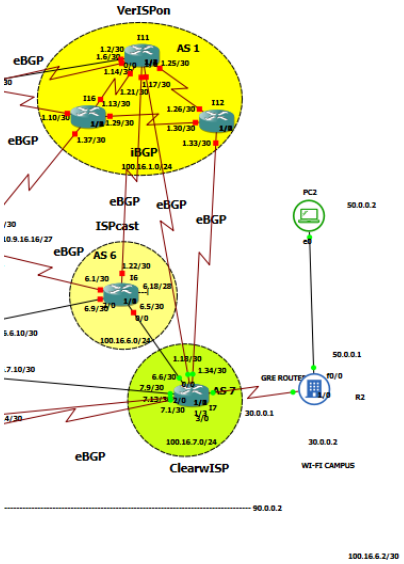

Figure 35: Project (Part-3)

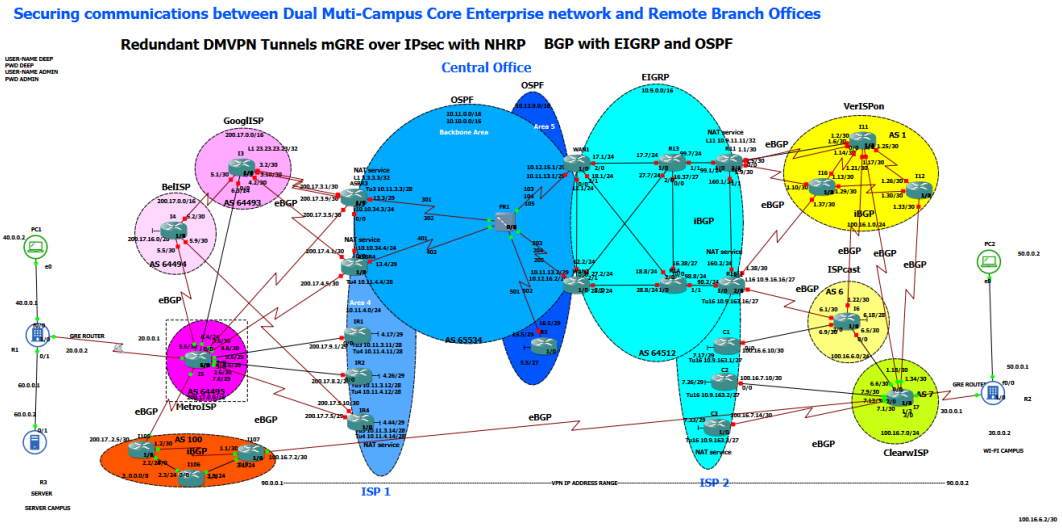

Figure 36: Project

6 Conclusion

Conclusion:
It was a great learning experience while working on the project as we experienced the real taste of networking. The College campus network performance was not up to the mark because of the slow WAN links and hub connectivity in the LANs. The College camps wanted to actually feel the improvement in network performance by replacing the existing WAN technologies and networking hardware devices. They wanted a simulation of the actual network before they decide to actually upgrade their hardware infrastructure.

7 References

[1]Science Direct “Cryptography Techniques” [Online]
Available: https://www.sciencedirect.com/topics/computer-science/cryptographictechnique
[Accessed on: March 15, 2022]

[2] Tutorial Points “Data Encryption Standard” [Online]
Available:https://www.tutorialspoint.com/cryptography/
data_encryption$_s tandard.htm[Acessedon : March22, 2022]$

[3]Hash-based message authentication codes (HMAC) [Online]
Available: https://cryptography.io/en/latest/hazmat/primitives/mac/hmac/ [Accessed on: April 2, 2022]

[4]CiscoPress, [Online] Available: Cisco Press: Source for Cisco Technology, CCNA, CCNP, CCIE Self-Study Cisco Press [Accessed on: May 25, 2022].

[5] Todd Lammle, CISCO CERTIFIED NETWORK ASSOCIATE STUDY GUIDE, Seventh Edition [E-book].