INSTITUTE/ INDUSTRIAL SUMMER TRAINING REPORT

ON

REDISTRIBUTION IN NETWORKING PROTOCOLS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD

OF THE DEGREE OF

BACHELOR OF ENGINEERING

(Computer Science & Engineering)

CHANDIGARH UNIVERSITY GHARUAN, MOHALI

JUNE-JULY,2022

COMPANY NAME: SOLATAIRE INFOSYS

SUBMITTED BY:

NAME: Rujhaan Gupta

UNIVERSITY UID :20BCS9747

SECTION WITH GROUP :WM_902 B

CONTENTS

Topic **Page No.**

Certificate by Company/Industry/Institute *i*

Candidate's Declaration *ii*

Abstract *iii*

Acknowledgement *vi*

About the Company/ Industry / Institute *v*

CHAPTER 1 INTRODUCTION **1-5**

1.1 Introduction and Background of Project 1

1.2 VPN And Its Types 1

1.3 Advantages and Disadvantages of VPN 3

1.4 Software and Hardware tools 5

CHAPTER 2 TRAINIMG WORK UNDERTAKEN **6-17**

2.1 Concept learned 6

2.2 Commands used 16

2.3 Project implementation 17

CHAPTER 3 RESULT AND DISCUSSION **18-22**

3.1 Project screenshot 18

3.2 Project explanation 22

3.3 Discussion 22

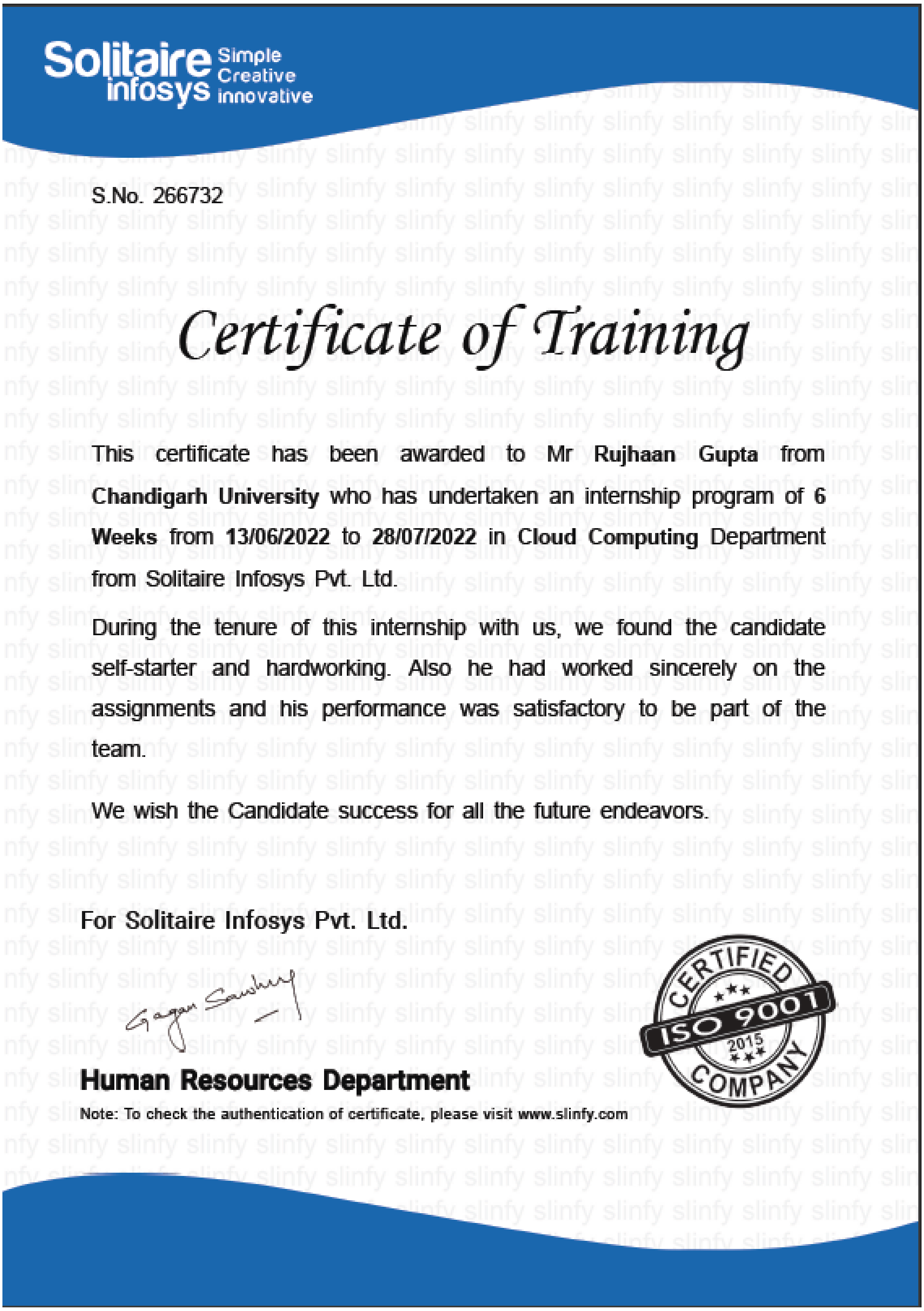
CHAPTER 4 CONCLUSION AND FUTURE SCOPE **23**

4.1 Conclusion 23

4.2 Future scope 23

References **24**

Certificate by Company



Solitaire infosys Simple Creative innovative

S.No. 266732

Certificate of Training

This certificate has been awarded to Mr **Rujhaan Gupta** from **Chandigarh University** who has undertaken an internship program of **6 Weeks** from **13/06/2022** to **28/07/2022** in **Cloud Computing** Department from Solitaire Infosys Pvt. Ltd.

During the tenure of this internship with us, we found the candidate self-starter and hardworking. Also he had worked sincerely on the assignments and his performance was satisfactory to be part of the team.

We wish the Candidate success for all the future endeavors.

For Solitaire Infosys Pvt. Ltd.

Gagan Sawhney

Human Resources Department

Note: To check the authentication of certificate, please visit www.slinfy.com

CERTIFIED ISO 9001 2015 COMPANY

CANDIDATE'S DECLARATION

I RujhaanGupta hereby declare that I have undertaken Institute/ Industrial Summer Training in Solitaire Infosys and developed project titled “REDISTRIBUTION IN NETWORKING” during a period from 14/06/2022 to 29/07/2022 in partial fulfillment of requirements for the award of degree of B.E(COMPUTER SCIENCE & ENGINEERING) at CHANDIGARH UNIVERSITY GHARUAN, MOHALI. The work which is being presented in the Institute/ Industrial Summer training report submitted to Department of Computer Science & Engineering at CHANDIGARH UNIVERSITY GHARUAN, MOHALI is an authentic record of training work.

Rujhaan

Signature of the Student

The training Viva–Voce Examination of__________________ has been held on ____________ and accepted.

Signature of Internal Examiner

Signature of External Examiner

ABSTRACT

"Cloud" is a collective term for a large number of developments and possibilities. It is not an invention, but more of a "practical innovation", combining several earlier inventions into something new and compelling. Much like the iPod is comprised of several existing concepts and technologies (the Walkman, MP3 compression and a portable hard disk), cloud computing merges several already available technologies: high bandwidth networks, virtualization, Web 2.0 interactivity, time sharing, and browser interfaces. Cloud Computing is a popular phrase that is shorthand for applications that were developed to be rich Internet applications that run on the Internet (or "Cloud"). Cloud computing enables tasks to be assigned to a combination of software and services over a network. This network of servers is the cloud. Cloud computing can help businesses transform their existing server infrastructures into dynamic environments, expanding and reducing server capacity depending on their requirements. A cloud computing platform dynamically provisions, configures, reconfigures, and deprovisions servers as needed. Servers in the cloud can be physical machines or virtual machines. Advanced clouds typically include other computing resources such as storage area networks (SANs), network equipment, firewall and other security devices .The cloud computing is a new computing model which comes from grid computing, distributed computing, parallel computing, virtualization technology, utility computing and other computer technologies and it has more advantage characters such as large scale computation and data storage, virtualization, high expansibility, high reliability and low price service.

ACKNOWLEDGEMENT

First and foremost, I would like to thank our trainer who guided us in doing these projects. He provided us with invaluable advice and helped us in difficult periods. His help contributed tremendously to the successful completion of the project.

Secondly, I would like to thank the company Solitaire Infosys for providing this training.

At last but not in least, we would like to thank everyone who helped and motivated us to work on this project.

ABOUT THE COMPANY

Company Name: Solitaire Infosys

Solitaire Infosys Pvt. Ltd. is an acclaimed IT service provider contributing its part in the development of many businesses around the globe. We socialize with our clients to get a superior cognizance of their business and requirements and help them in fabricating websites and applications for their business. Founded in 2011 by a dynamic duo with the same aim and zeal, we have come a long way in satisfying our clients.

We are serving our clients with the world-class services for more than seven years now. The clients are delivered with the best IT solutions after we have developed a great understanding of their business and requirements. Our team works on the client projects like its own and that is the reason why we hold the edge in the league.

With every project that we deliver, we deliver our respect, creativity, quality, transparency, and teamwork to our clients. We have the experience, expertise, and capabilities to enable organizations to accelerate their service processes in every possible way. We are known for our excellent customer satisfaction, cost-effectiveness, and innovative skills that are unparalleled.

CHAPTER 1 INTRODUCTION

1.1 Introduction and Background of Project

Name of Project: Redistribution in Networking

WAN:

A wide area network (also known as WAN), is a large network of information that is not tied to a single location. WANs can facilitate communication, the sharing of information and much more between devices from around the world through a WAN provider.

WANs can be vital for international businesses, but they are also essential for everyday use, as the internet is considered the largest WAN in the world. Keep reading for more information on WANs, their use, how they differ from other networks and their overall purpose for businesses and people, alike.

Purpose of WAN:

If WAN connections didn’t exist, organizations would be isolated to restricted areas or specific geographic regions. LANs would allow organizations to work within their building, but growth to outside areas — either different cities or even different countries — would not be possible because the associated infrastructure would be cost prohibitive for most organizations. As organizations grow and become international, WANs allow them to communicate between branches, share information and stay connected. When employees travel for work, WANs allow them to access the information they need to do their job. WANs also help organizations share information with customers, as well as partner organizations, such as B2B clients or customers. However, WANs also provide an essential service to the public. Students at universities might rely on WANs to access library databases or university research. And every day, people rely on WANs to communicate, bank, shop and more.

1.2 VPN And Its Types

VPN stands for **"Virtual Private Network"** and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in **real time**.

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.

A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host. This means that if you surf online with a VPN, the VPN server becomes the source of your data. This means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online. A VPN works like a filter that turns all your data into "gibberish". Even if someone were to get their hands on your data, it would be useless.

The VPN itself should also be protected against compromise. These are the features you should expect from a comprehensive VPN solution:

Encryption of your IP address: The primary job of a VPN is to hide your IP address from your ISP and other third parties. This allows you to send and receive information online without the risk of anyone but you and the VPN provider seeing it.

Encryption of protocols: A VPN should also prevent you from leaving traces, for example, in the form of your internet history, search history and cookies. The encryption of cookies is especially important because it prevents third parties from gaining access to confidential information such as personal data, financial information and other content on websites.

Kill switch: If your VPN connection is suddenly interrupted, your secure connection will also be interrupted. A good VPN can detect this sudden downtime and terminate preselected programs, reducing the likelihood that data is compromised.

Two-factor authentication: By using a variety of authentication methods, a strong VPN checks everyone who tries to log in. For example, you might be prompted to enter a password, after which a code is sent to your mobile device. This makes it difficult for uninvited third parties to access your secure connection.

TYPES OF VPN

Virtual private networks may be classified by several categories:

Remote access

A *host-to-network* configuration is analogous to connecting a computer to a local area network. This type provides access to an enterprise network, such as an intranet. This may be employed for remote workers who need access to private resources, or to enable a mobile worker to access important tools without exposing them to the public Internet.

Site-to-site

A *site-to-site* configuration connects two networks. This configuration expands a network across geographically disparate offices, or a group of offices to a data center installation. The interconnecting link may run over a dissimilar intermediate network, such as two IPv6 networks connected over an IPv4 network.

Extranet-based site-to-site

In the context of site-to-site configurations, the terms intranet and extranet are used to describe two different use cases. An *intranet* site-to-site VPN describes a configuration where the sites connected by the VPN belong to the same organization, whereas an *extranet* site-tosite VPN joins sites belonging to multiple organizations.

1.3 Advantages and Disadvantages of VPN

ADVANTAGES OF VPN

A VPN connection disguises your data traffic online and protects it from external access. Unencrypted data can be viewed by anyone who has network access and wants to see it. With a VPN, hackers and cyber criminals can’t decipher this data.

Secure encryption:

To read the data, you need an *encryption key*. Without one, it would take millions of years for a computer to decipher the code in the event of a brute force attack. With the help of a VPN, your online activities are hidden even on public networks.

Disguising your whereabouts:

VPN servers essentially act as your proxies on the internet. Because the demographic location data comes from a server in another country, your actual location cannot be determined. In addition, most VPN services do not store logs of your activities. Some providers, on the other hand, record your behavior, but do not pass this information on to third parties. This means that any potential record of your user behavior remains permanently hidden.

Access to regional content:

Regional web content is not always accessible from everywhere. Services and websites often contain content that can only be accessed from certain parts of the world. Standard connections use local servers in the country to determine your location. This means that you cannot access content at home while traveling, and you cannot access international content from home. With VPN location spoofing, you can switch to a server to another country and effectively
“change” your location.

Secure data transfer:

If you work remotely, you may need to access important files on your company’s network. For security reasons, this kind of information requires a secure connection. To gain access to the network, a VPN connection is often required. VPN services connect to private servers and use encryption methods to reduce the risk of data leakage.

DISADVANTAGES OF VPN

While it is true remote access VPN saved the day for some businesses, it’s also true that the increased usage has further magnified some of the biggest VPN disadvantages.

Not designed for continuous use:

The use case for remote access VPN was never to connect an entire enterprise to the WAN. Traditionally, enterprises purchased VPN solutions to connect a small percentage of the workforce for short periods of time. With a shift to large-scale work from home, existing VPN infrastructure is forced to support a continuous workload it wasn’t intended for. This creates an environment where VPN servers are subject to excessive loads that can negatively affect performance and user experience.

Complexity impedes scalability:

Enterprises may try to address the issue of VPN overload with additional VPN appliances or VPN concentrators, but this adds cost and complexity to the network. Similarly, configuring VPN appliances for HA (high availability) adds more cost and requires more complex configuration.

Further, because VPN servers provide remote access, but not enterprise-grade security and monitoring, they must be complemented by management solutions and security tools. These additional appliances and applications lead to even more configuration and maintenance. As each additional solution is layered in, the network becomes more complex and more difficult to scale.

Lack of granular security:

VPN appliances are a textbook example of castle-and-moat security. Once a user connects via VPN, they have effectively unrestricted access to the rest of the subnet. For some enterprises, this means non-admin users have network access to critical infrastructure when they shouldn’t. Further, this castle-and-moat approach increases the risk of malware spread and data breaches. To add granular security controls to remote access VPN, enterprises often have to deploy additional security point-solutions, but this adds additional cost and complexity while leaving plenty of room for misconfiguration and human error.

Unpredictable performance:

VPN connections occur over the public Internet, which means network performance is directly tied to public Internet performance. The jitter and packet loss common to the Internet can wreak havoc on mission critical apps and user experience. Additionally, enterprises with a global footprint know that there are significant latency challenges when attempting to send Internet traffic across the globe, before we even take into account the additional overhead VPN tunneling adds.

Unreliable availability:

Beyond unpredictable performance, enterprises that depend on the public Internet for remote access get no availability guarantees. When public Internet outages mean lost productivity for your entire organization, the risk of depending solely on the public Internet can outweigh the rewards significantly.

1.4 Software and Hardware tools

HARWARE REQUIREMENT

PC with:

1. Processor i3
2. RAM- 4GB
3. System type- 64bits
4. MAC/Linux/Windows-7, 8,9,10,11

SOFTWARE REQUIREMENT

CISCO Packet Tracer Student

Devices:

1. Switch -2960-tt
2. Router-2811
3. Server-pt
4. PC
5. Wireless router
6. VPN interface tunnel

Cabling:

1. Straight Through Cable
2. Serial Cable
3. Cross Over Cable

CHAPTER 2 TRAINING WORK UNDERTAKEN

2.1 Concept Learned

- ✞ Networking
- ✞ Topologies
- ✞ Transmission Mode
- ✞ Devices
- ✞ IP Address
- ✞ Protocols
- ✞ Cables
- ✞ OSI Layer
- ✞ Routing Protocols
- ✞ Redistribution
- ✞ Domain Name System
- ✞ Email Server
- ✞ Dynamic Host Control Protocol
- ✞ Voice Over IP
- ✞ VOIP Redistribution
- ✞ Access Control List
- ✞ Virtual Private Network
- ✞ Network Address Translation

EXPLAINATION Networking

Networking is the exchange of information and ideas among people with a common profession or special interest, usually in an informal social setting. Networking often begins with a single point of common ground.
A computer network can be categorized by their size. A **computer network** is mainly of **three types**:

- LAN(Local Area Network) ○ MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

LAN(Local Area Network) ○ Local Area Network is a group of computers connected to each other in a small area such as building, office.

- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

MAN(Metropolitan Area Network) ○ A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.

- ○ Government agencies use MAN to connect to the citizens and private industries. ○ In MAN, various LANs are connected to each other through a telephone exchange line.
- ○ The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc. ○ It has a higher range than Local Area Network(LAN).

Uses Of Metropolitan Area Network: ○ MAN is used in communication between the banks in a city. ○ It can be used in an Airline Reservation. ○ It can be used in a college within a city.

- ○ It can also be used for communication in the military.

WAN(Wide Area Network) ○ A Wide Area Network is a network that extends over a large geographical area such as states or countries.

- ○ A Wide Area Network is quite bigger network than the LAN.
- ○ A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- ○ The internet is one of the biggest WAN in the world.
- ○ A Wide Area Network is widely used in the field of Business, government, and education.

Topologies

A Network Topology is the arrangement with which computer systems or network devices are connected to each other. Topologies may define both physical and logical aspect of the network. Both logical and physical topologies could be same or different in a same network.

Point-to-Point

Point-to-point networks contains exactly two hosts such as computer, switches or routers, servers connected back to back using a single piece of cable. Often, the receiving end of one host is connected to sending end of the other and vice-versa.

Bus Topology

In case of Bus topology, all devices share single communication line or cable.Bus topology may have problem while multiple hosts sending data at the same time. Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue. It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning.

Star Topology

All hosts in Star topology are connected to a central device, known as hub device, using a point-topoint connection. That is, there exists a point to point connection between hosts and hub.

Ring Topology

In ring topology, each host machine connects to exactly two other machines, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. To connect one more host in the existing structure, the administrator may need only one more extra cable.

Mesh Topology

In this type of topology, a host is connected to one or multiple hosts. This topology has hosts in pointto-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only.

Tree Topology

Also known as Hierarchical Topology, this is the most common form of network topology in use presently. This topology imitates as extended Star topology and inherits properties of bus topology.

This topology divides the network in to multiple levels/layers of network. Mainly in LANs, a network is bifurcated into three types of network devices. The lowermost is access-layer where computers are attached. The middle layer is known as distribution layer, which works as mediator between upper layer and lower layer. The highest layer is known as core layer, and is central point of the network, i.e. root of the tree from which all nodes fork.

Hybrid Topology

A network structure whose design contains more than one topology is said to be hybrid topology. Hybrid topology inherits merits and demerits of all the incorporating topologies.

Transmission Mode

Simplex Mode –

In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit, the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction.

Example: Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.

Half-Duplex Mode –

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time. The entire capacity of the channel can be utilized for each direction.

Example: Walkie-talkie in which message is sent one at a time and messages are sent in both directions.

Full-Duplex Mode –

In full-duplex mode, both stations can transmit and receive simultaneously. In full_duplex mode, signals going in one direction share the capacity of the link with signals going in another direction, this sharing can occur in two ways:

- Either the link must contain two physically separate transmission paths, one for sending and the other for receiving.
- Or the capacity is divided between signals traveling in both directions.

Networking Devices

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

2. Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

3. Bridge – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

4. Switch – A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but broadcast domain remains the same.

5. **Routers** – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

6. **Gateway** – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. Gateway is also called a protocol converter.

7. **NIC** – NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and router or modem. NIC card is a layer 2 device which means that it works on both physical and data link layer of the network model.

8.Firewall –A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.

IP Address

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

Types of IP:

1. IPV4 2.
IPV6

IP stands for **Internet Protocol** and **v4** stands for **Version Four** (IPv4). IPv4 was the primary version brought into action for production within the ARPANET in 1983.
IP version four addresses are 32-bit integers which will be expressed in decimal notation.
Example- 192.0.2.126 could be an IPv4 address. *Parts of IPv4*

- **Network part:**
  The network part indicates the distinctive variety that's appointed to the network. The network part conjointly identifies the category of the network that's assigned.
- **Host Part:**
  The host part uniquely identifies the machine on your network. This part of the IPv4 address is assigned to every host.
  For each host on the network, the network part is the same, however, the host half must vary.
- **Subnet number:**
  This is the nonobligatory part of IPv4. Local networks that have massive numbers of hosts are divided into subnets and subnet numbers are appointed to that.

Characteristics of IPv4

- IPv4 could be a 32-Bit IP Address.
- IPv4 could be a numeric address, and its bits are separated by a dot.
- The number of header fields is twelve and the length of the header field is twenty.
- It has Unicast, broadcast, and multicast style of addresses.

Advantages of IPv4

- IPv4 security permits encryption to keep up privacy and security.
- IPV4 network allocation is significant and presently has quite 85000 practical routers.
- It becomes easy to attach multiple devices across an outsized network while not NAT.
- This is a model of communication so provides quality service also as economical knowledge transfer.
- IPV4 addresses are redefined and permit flawless encoding. Classes in IPV4

Class A:

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The default subnet mask for Class A IP address is 255.0.0.0

The IP range **127.x.x.x** is reserved for loopback IP addresses.

Class B:

Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.

Class C:

Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.

Class D:

Class D has IP address range from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

Class E:

This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

Internet Protocol Version 6 is a network layer protocol that allows communication to take place over the network. IPv6 was designed by Internet Engineering Task Force (IETF) in December 1998 with the purpose of superseding the IPv4 due to the global exponentially growing internet users.

Types of IPv6 Address

Now that we know about what is IPv6 address let’s take a look at its different types.

- **Unicast addresses** It identifies a unique node on a network and usually refers to a single sender or a single receiver.
- **Multicast addresses** It represents a group of IP devices and can only be used as the destination of a datagram.

- **Anycast addresses** It is assigned to a set of interfaces that typically belong to different nodes.

Advantages of IPv6

- Reliability
- **Faster Speeds:** IPv6 supports multicast rather than broadcast in IPv4.This feature allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations all at once.
- **Stronger Security:** IPSecurity, which provides confidentiality, and data integrity, is embedded into IPv6.
- Routing efficiency
- Most importantly it's the final solution for growing nodes in Global-network. *Disadvantages of IPv6*
- **Conversion:** Due to widespread present usage of IPv4 it will take a long period to completely shift to IPv6.
- **Communication:** IPv4 and IPv6 machines cannot communicate directly with each other. They need an intermediate technology to make that possible.

Protocols

- **DNS** - Domain Name System - translates network address (such as IP addresses) into terms understood by humans (such as Domain Names) and vice-versa.
- **DHCP** - Dynamic Host Configuration Protocol - can automatically assign Internet addresses to computers and users
- **FTP** - File Transfer Protocol - a protocol that is used to transfer and manipulate files on the Internet
- **HTTP** - HyperText Transfer Protocol - An Internet-based protocol for sending and receiving webpages
- **POP3** - Post Office protocol Version 3 - a protocol used by e-mail clients to retrieve messages from remote servers
- **SMTP** - Simple Mail Transfer Protocol - A protocol for e-mail messages on the Internet
- **HTTPS -Hypertext Transfer Protocol Secure** (https) is a combination of the Hypertext Transfer Protocol (HTTP) with the Secure Socket Layer (SSL)/Transport Layer Security (TLS) protocol.
- **TFTP -**TFTP Server is used for **simple file transfer (typically for boot-loading remote devices)**. Trivial File Transfer Protocol (TFTP) is a simple protocol for exchanging files between two TCP/IP machines.
- **APIPA -APIPA** stands for **Automatic Private IP Addressing (APIPA).** It is a feature or characteristic in operating systems (eg. Windows) which enables computers to selfconfigure an IP address and subnet mask automatically when their DHCP(Dynamic Host Configuration Protocol) server isn't reachable. The IP address range for APIPA is **(169.254.0.1 to 169.254.255.254)** having **65, 534** usable IP addresses, with the subnet mask of **255.255.0.0**.
- **PPP-** Point - to - Point Protocol is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers.

- **ARP-** Address Resolution Protocol is a protocol or procedure that connects an ever-changing Internet Protocol address to a fixed physical machine address, also known as a media access control (MAC) address, in a local-area network (LAN).
- **RARP-**Reverse Address Resolution Protocol is a protocol a physical machine in a local area network can use **to request its IP address**.

Cables

Mainly there are three types of ethernet cables used in LANs i.e., Coaxial cables, Twisted Pair cables, and Fiber optic cables.

1. **Coaxial Cables:** A coaxial cable is used to carry high-frequency electrical signals with low losses. It uses 10Base2 and 10Base5 Ethernet variants. It has a copper conductor in the middle that is surrounded by a dielectric insulator usually made of PVC or Teflon. The dielectric insulator is surrounded by a braided conducting metallic shield which reduces EMI (Electromagnetic Interference) of the metal and outside interference; and finally, the metallic shield is covered by a plastic covering called a sheath usually made of PVC or some other fire-resistant plastic material. Its maximum transmission speed is 10 Mbps. It is usually used in telephone systems, cable TV, etc.

2. **Twisted Pair Cable:** Twisted pair is a copper wire cable in which two insulated copper wires are twisted around each other to reduce interference or crosstalk. It uses 10BASE-T, 100BASE-T, and some other newer ethernet variants. It uses RJ-45 connectors.

Types of twisted pair cable:

- **Shielded Twisted Pair (STP) Cable:**
- **Unshielded Twisted Pair (UTP) Cable**

3. **Fiber Optic Cable:** Fiber optic cables use optical fibers which are made of glass cores surrounded by several layers of cladding material usually made of PVC or Teflon, it transmits data in the form of light signals due to which there are no interference issues in fiber optics.

OSI Layer

OSI model is not a **network architecture** because it does not specify the exact services and protocols for each layer. It simply tells what each layer should do by defining its input and output data. It is up to network architects to implement the layers according to their needs and resources available.

These are the seven layers of the OSI model −

- **Physical layer** −It is the first layer that physically connects the two systems that need to communicate. It transmits data in bits and manages simplex or duplex transmission by modem. It also manages Network Interface Card's hardware interface to the network, like cabling, cable terminators, topography, voltage levels, etc.
- **Data link layer** − It is the firmware layer of Network Interface Card. It assembles datagrams into frames and adds start and stop flags to each frame. It also resolves problems caused by damaged, lost or duplicate frames.
- **Network layer** − It is concerned with routing, switching and controlling flow of information between the workstations. It also breaks down transport layer datagrams into smaller datagrams.
- **Transport layer** − Till the session layer, file is in its own form. Transport layer breaks it down into data frames, provides error checking at network segment level and prevents a fast host from overrunning a slower one. Transport layer isolates the upper layers from network hardware.
- **Session layer** − This layer is responsible for establishing a session between two workstations that want to exchange data. • **Presentation layer** − This layer is concerned with correct representation of data, i.e.
  syntax and semantics of information. It controls file level security and is also responsible for converting data to network standards.
- **Application layer** − It is the topmost layer of the network that is responsible for sending application requests by the user to the lower levels. Typical applications include file transfer, E-mail, remote logon, data entry, etc.

Routing Protocols Routing information protocols (RIP)

RIP (Routing Information Protocol) is a forceful protocol type used in local area network and wide area network. RIP (Routing Information Protocol) type is categorized interior gateway protocol within the use of distance vector algorithm. Routing information protocols defined in 1988. It also has version 2 and nowadays both versions are in use. Technically it is outdated by more sophisticated techniques such as (OSPF) and the OSI protocol IS-IS.

Open shortest path first (OSPF)

Open Shortest Path First (OSPF) is an active routing protocol used in internet protocol. Particularly it is a link state routing protocol and includes into the group of interior gateway protocol. Open Shortest Path First (OSPF) operating inside a distinct autonomous system. The version 2 of Open Shortest Path First (OSPF) defined in 1998 for IPv4 then the OSPF version 3 in RFC 5340 in 2008. The Open Shortest Path First (OSPF) most widely used in the network of big business companies.

Enhanced interior gateway routing protocol (EIGRP)

Enhanced Interior Gateway Routing Protocol (EIGRP) based on their original IGRP while it is a Cisco proprietary routing protocol. It is a distance-vector routing protocol in advance within the optimization to lessen both the routing unsteadiness incurred after topology alteration, plus the use of bandwidth and processing power in the router which support enhanced interior gateway routing protocol will automatically reallocate route information to IGRP (Enhanced Interior Gateway Routing Protocol) neighbours by exchanging the 32 bit EIGRP (Enhanced Interior Gateway Routing Protocol) metric to the 24 bit IGRP metric. Generally optimization based on DUAL work from SRI which assured loop free operation and offer a means for speedy junction.

Redistribution

Redistribution in networking is the importing and exporting of network routes from one routing protocol (or static routing) to another routing protocol. Routers that run two or more routing protocols can be configured for redistribution.

Domain Name System

The Domain Name System (DNS) Server is a server that is specifically used for matching website hostnames (like example.com)to their corresponding Internet Protocol or IP addresses. The DNS server contains a database of public IP addresses and their corresponding domain names.

Email Server

An email server, or simply mail server, is an application or computer in a network whose sole purpose is to act as a virtual post office. The server stores incoming mail for distribution to local users and sends out outgoing messages.

Access Control List

An access control list (ACL) is a list of rules that specifies which users or systems are granted or denied access to a particular object or system resource. Access control lists are also installed in routers or switches, where they act as filters, managing which traffic can access the network.

Virtual Private Network

VPN stands for virtual private network. In basic terms, a VPN provides an encrypted server and hides your IP address from corporations, government agencies and would-be hackers. A VPN protects your identity even if you are using public or shared Wi-Fi, and your data will be kept private from any prying internet eyes.

Network Address Translation

A Network Address Translation (NAT) is the process of mapping an internet protocol (IP) address to another by changing the header of IP packets while in transit via a router. This helps to improve security and decrease the number of IP addresses an organization needs.

2.2 Commands Used

Router used: 2811

WIC-2T

Routing Protocols 1. Routing Information Protocol router rip Net 10.0.0.0 **2. Open Shortest Path Exist** router ospf 10 net 10.0.0.0 0.255.255.255(wild card mask)

3. Enhance Interior Gateway Routing Protocol

router eigrp 20 net 10.0.0.0 **Redistribution**

router rip redistribute
ospf 10 metric 2
redistribute eigrp 20 metric 2

router ospf 10
redistribute rip subnets
redistribute eigrp 20 subnets

router eigrp 20 redistribute rip metric
2 100 100 100 100
redistribute ospf 10 metric 2 100 100 100 100

DHCP ip dhcp
pool abc net 10.0.0.1
255.0.0.0 default-
router 10.0.0.1
dns-server 20.0.0.6

VOIP ip dhcp pool abc
net 10.0.0.1 255.0.0.0
default-router 10.0.0.1 dns-
server 20.0.0.6 option 150
ip 10.0.0.1 telephony-
service max-ephone 2
max-dn 2 ip source 10.0.0.1
port 2000 auto assign 1 to 2
ephone-dn 1 num 100
ephone-dn 2
num 101

VOIP redistribution dial-
peer voice 1001 voip
destination-pattern 200
session target ipv4:10.0.0.2

VPN

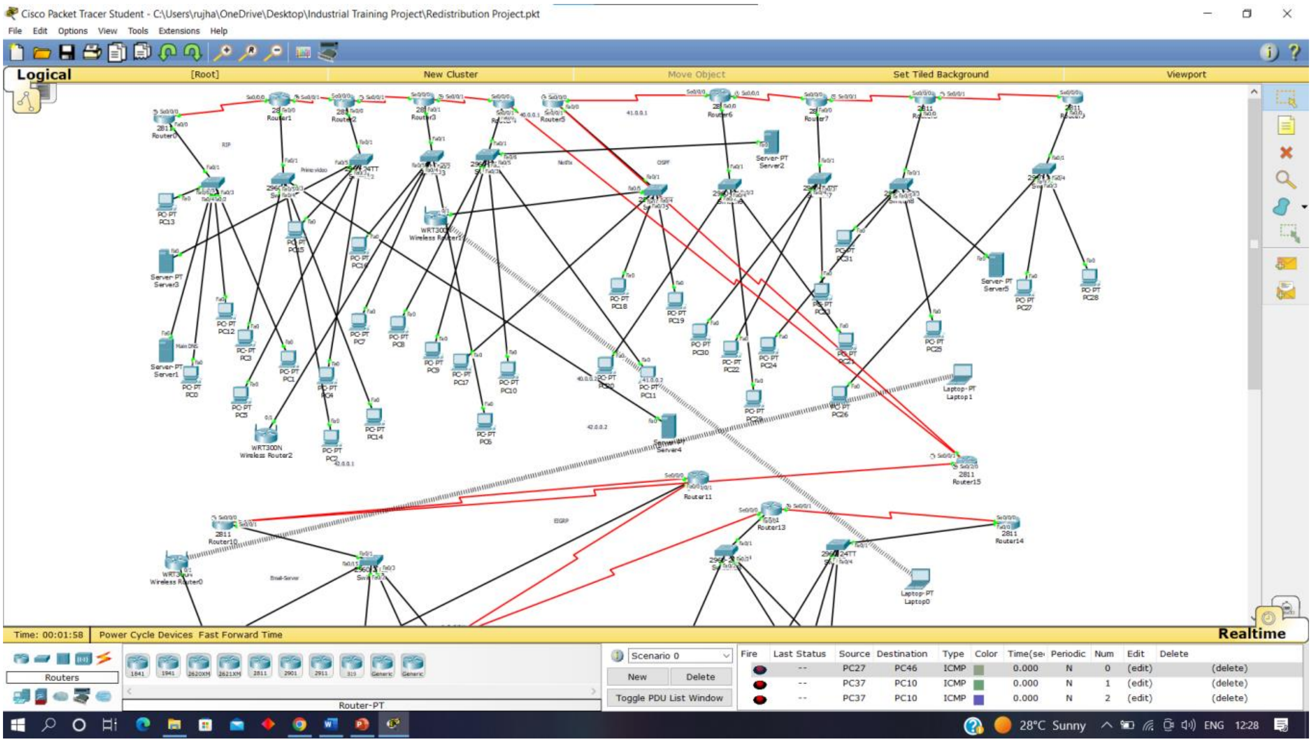
1st Router: int tunnel 0
ip add 100.0.0.1 255.0.0.0
tunnel source se0/0/0
tunnel destination 14.0.0.2

2nd Router: int tunnel 0

```
ip add 100.0.0.2 255.0.0.0
tunnel source se0/0/1
tunnel destination 10.0.0.2
```

2.3 Project Implementation

After implementation of all the commands the project is completed



Cisco Packet Tracer Student - C:\Users\rujha\OneDrive\Desktop\Industrial Training Project\Redistribution Project.pkt

Time: 00:01:58

Scenario 0

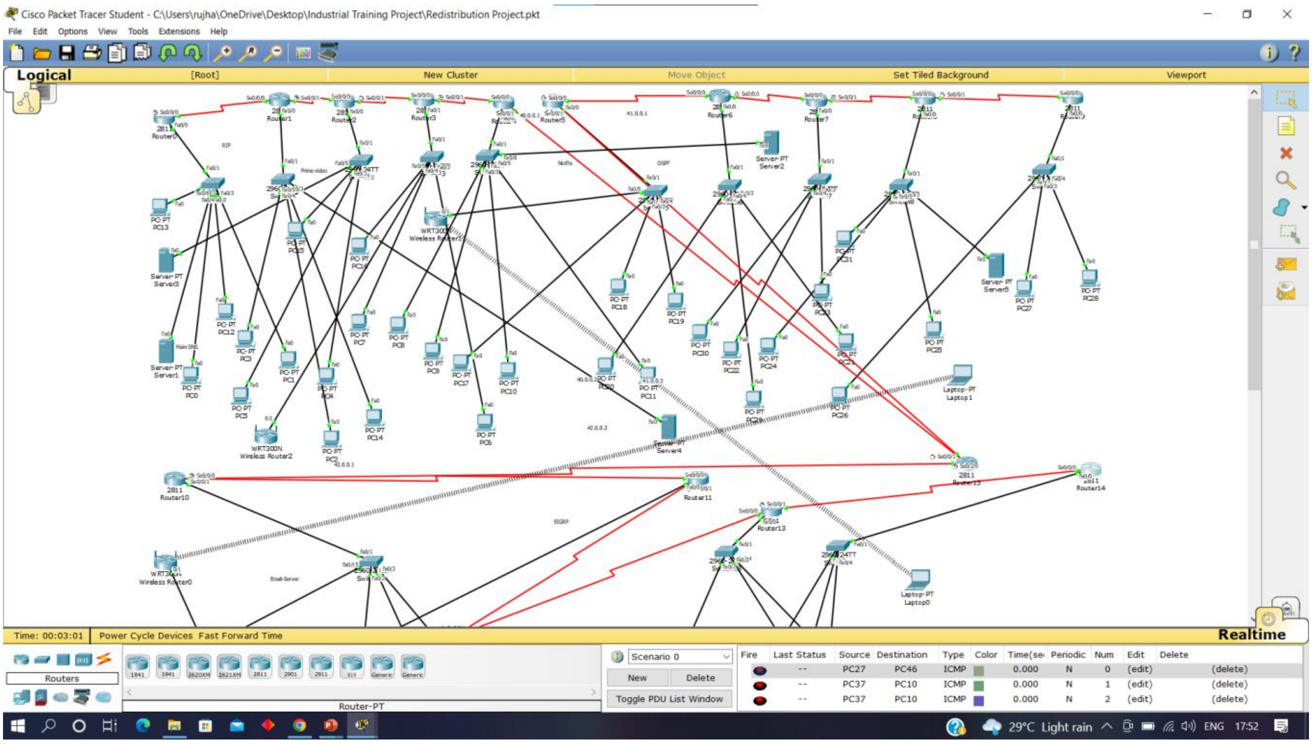
Fire	Last Status	Source	Destination	Type	Color	Time(se	Periodic	Num	Edit	Delete
●	--	PC27	PC46	ICMP	🟩	0.000	N	0	(edit)	(delete)
●	--	PC37	PC10	ICMP	🟩	0.000	N	1	(edit)	(delete)
●	--	PC37	PC10	ICMP	🟦	0.000	N	2	(edit)	(delete)

Fig 2.1 Project screenshot

CHAPTER 3

RESULT AND DISCUSSION

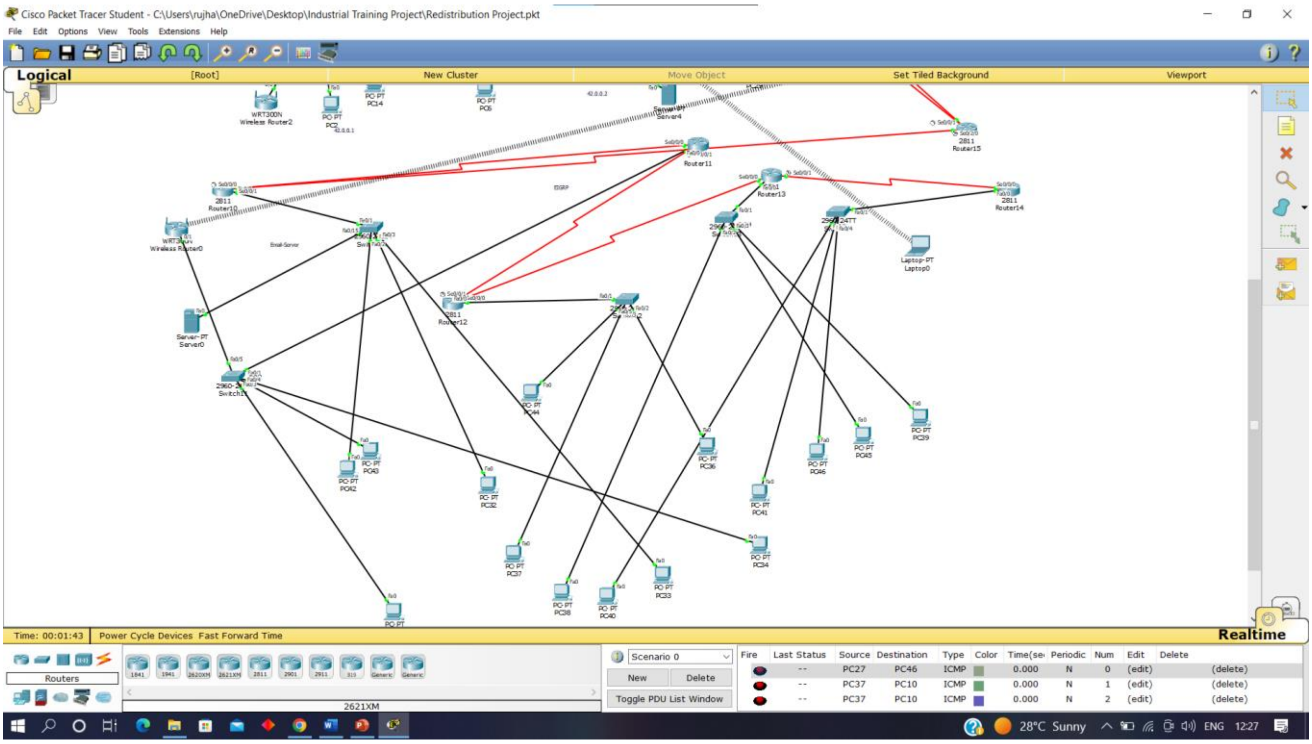
3.1 PROJECT SCREENSHOT



Cisco Packet Tracer Student - C:\Users\rujha\OneDrive\Desktop\Industrial Training Project\Redistribution Project.pkt

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	--	PC27	PC46	ICMP	🟩	0.000	N	0	(edit)	(delete)
●	--	PC37	PC10	ICMP	🟩	0.000	N	1	(edit)	(delete)
●	--	PC37	PC10	ICMP	🟦	0.000	N	2	(edit)	(delete)

Fig 3.1 Project screenshot 1

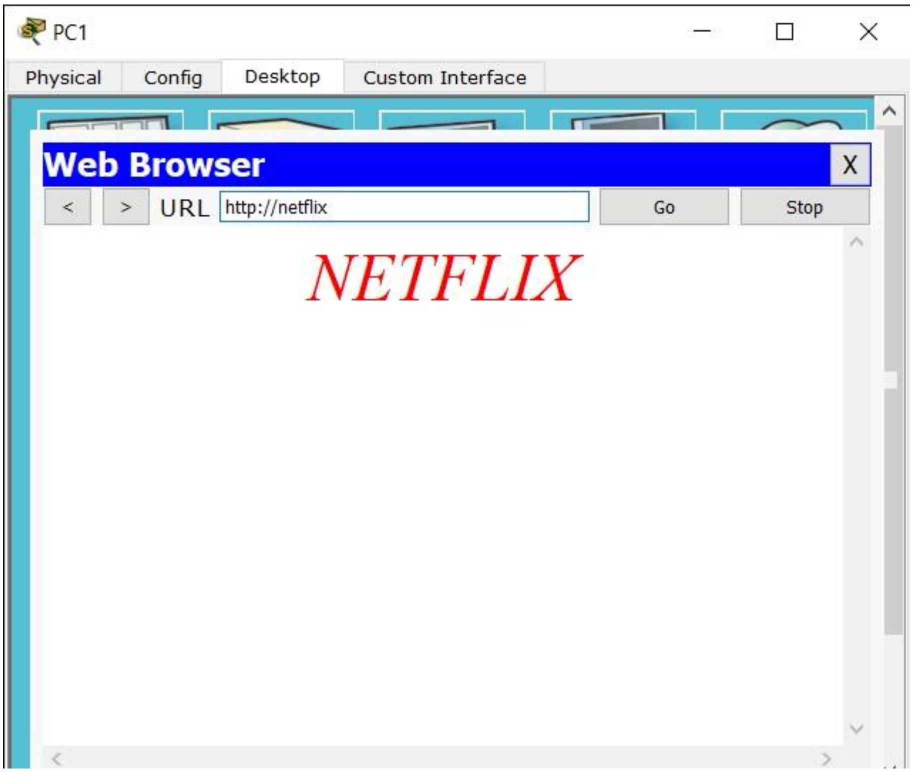


Cisco Packet Tracer Student - C:\Users\rujha\OneDrive\Desktop\Industrial Training Project\Redistribution Project.pkt

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	--	PC27	PC46	ICMP	🟩	0.000	N	0	(edit)	(delete)
●	--	PC37	PC10	ICMP	🟩	0.000	N	1	(edit)	(delete)
●	--	PC37	PC10	ICMP	🟦	0.000	N	2	(edit)	(delete)

Fig 3.2 Project screenshot 2

DNS

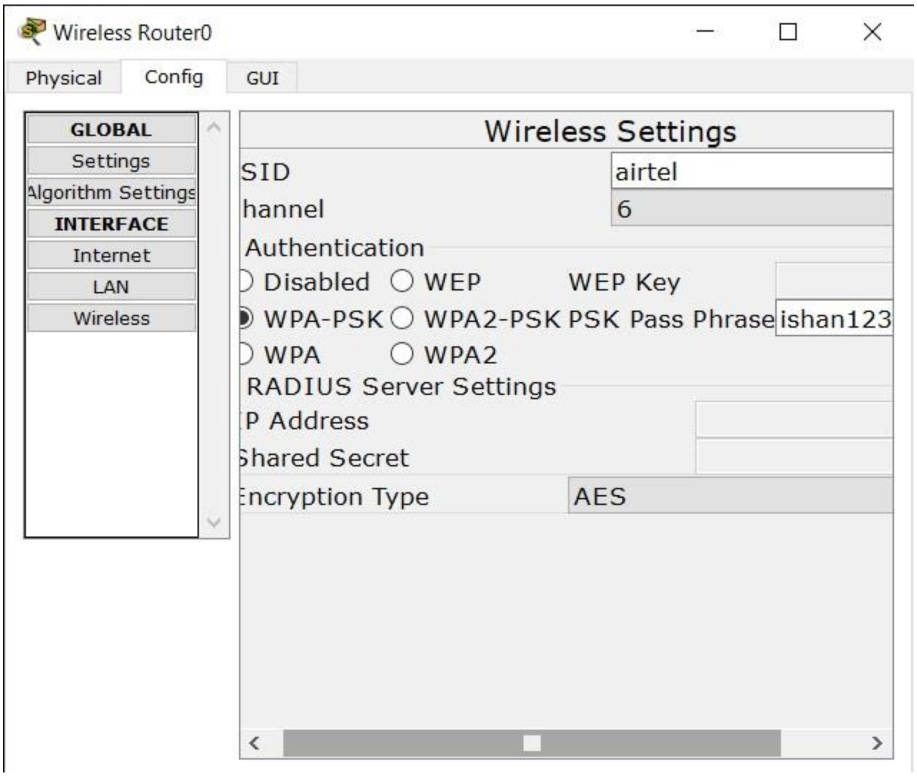


URL http://netflix

NETFLIX

Fig 3.5 DNS using internet

WIFI



Wireless Settings

SID airtel

hannel 6

Authentication

) Disabled ○ WEP WEP Key

● WPA-PSK ○ WPA2-PSK PSK Pass Phrase ishan123

) WPA ○ WPA2

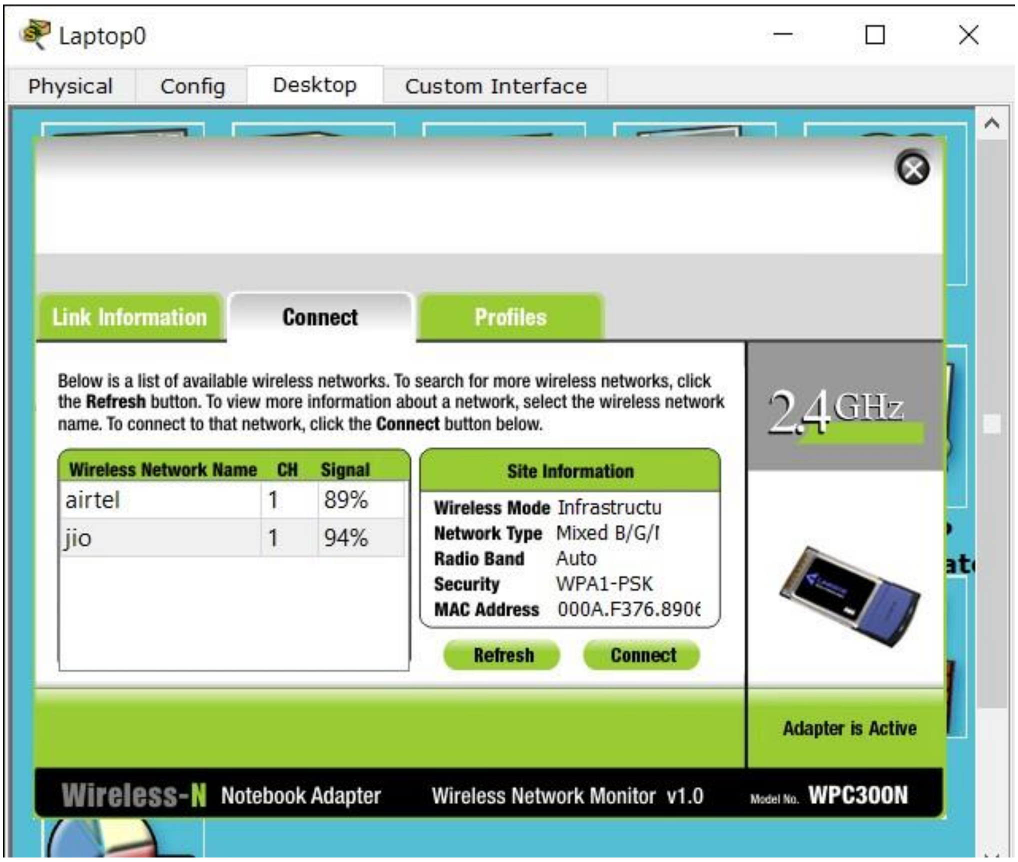
RADIUS Server Settings

P Address

Shared Secret

Encryption Type AES

Fig 3.6 WIFI setup



Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

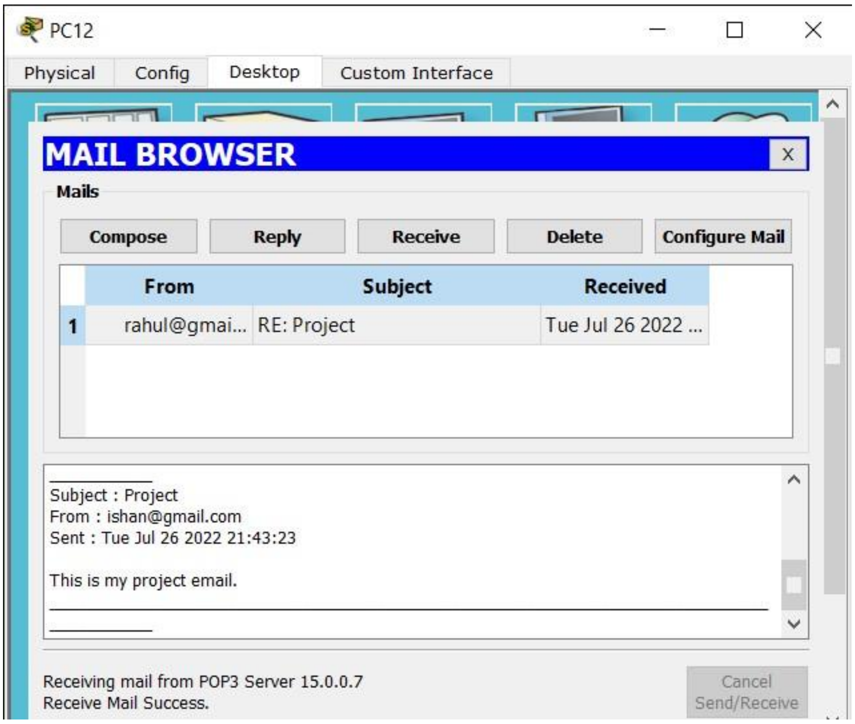
Wireless Network Name	CH	Signal
airtel	1	89%
jio	1	94%

Site Information

Wireless Mode	Infrastructu
Network Type	Mixed B/G/I
Radio Band	Auto
Security	WPA1-PSK
MAC Address	000A.F376.890€

Fig 3.7 WIFI connection

EMAIL Server



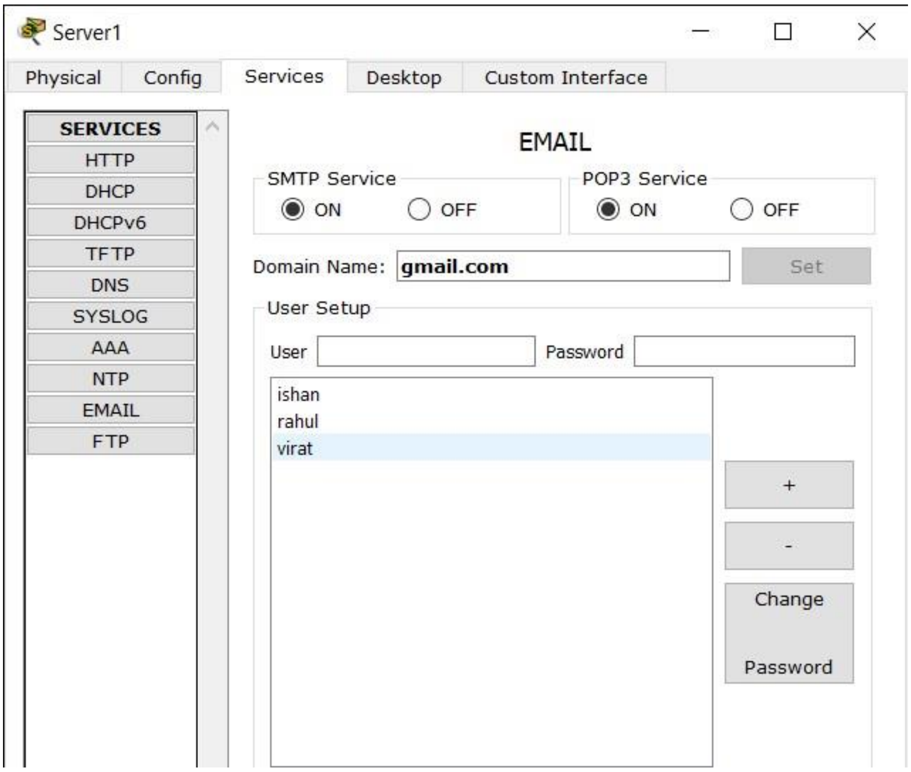
	From	Subject	Received
1	rahul@gmai...	RE: Project	Tue Jul 26 2022 ...

Subject : Project
From : ishan@gmail.com
Sent : Tue Jul 26 2022 21:43:23

This is my project email.

Receiving mail from POP3 Server 15.0.0.7
Receive Mail Success.

Fig 3.8 Email in pc



EMAIL

SMTP Service ● ON ○ OFF

POP3 Service ● ON ○ OFF

Domain Name: gmail.com

User Setup

User | Password

ishan
rahul
virat

Fig 3.9 Email Server

3.2 Project Explanation

VPN also ensures security by providing an encrypted tunnel between client and VPN server.

VPN is used to bypass many blocked sites.

VPN facilitates Anonymous browsing by hiding your ip address.

Also, most appropriate Search engine optimization(SEO) is done by analysing the data from VPN providers which provide country-wise stats of browsing a particular product. This method of SEO is used widely my many internet marketing managers to form new strategies.

3.3 Discussion

VPN offers securities such as: Secure Your Network.

Hide Your Private Information.

Prevent Data Throttling.

Avoid Bandwidth Throttling.

Get Access to Geo-blocked Services.

Network Scalability.

Reduce Support Costs.

CHAPTER 4 CONCLUSION AND FUTURE SCOPE

4.1 Conclusion

VPN stands for **"Virtual Private Network"** and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in **real time**.

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments. A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host. This means that if you surf online with a VPN, the VPN server becomes the source of your data. This means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online. A VPN works like a filter that turns all your data into "gibberish". Even if someone were to get their hands on your data, it would be useless.

The VPN itself should also be protected against compromise. These are the features you should expect from a comprehensive VPN solution:

Encryption of your IP address: The primary job of a VPN is to hide your IP address from your ISP and other third parties. This allows you to send and receive information online without the risk of anyone but you and the VPN provider seeing it.

Encryption of protocols: A VPN should also prevent you from leaving traces, for example, in the form of your internet history, search history and cookies. The encryption of cookies is especially important because it prevents third parties from gaining access to confidential information such as personal data, financial information and other content on websites.

Kill switch: If your VPN connection is suddenly interrupted, your secure connection will also be interrupted. A good VPN can detect this sudden downtime and terminate preselected programs, reducing the likelihood that data is compromised.

Two-factor authentication: By using a variety of authentication methods, a strong VPN checks everyone who tries to log in. For example, you might be prompted to enter a password, after which a code is sent to your mobile device. This makes it difficult for uninvited third parties to access your secure connection.

4.2 Future Scope

For the future of VPNs, end systems' increasing power will facilitate the migration of more software-based VPN technology into endpoints. VPN technologies will evolve to take advantage of local process capabilities, which make VPNs easier for users and network administrators alike. Network admins will control VPN administration through central systems.

REFRENCES

[1] Himanshu Gupta et al: A New Concept in Modern Cryptography, International Journal of Computer Theory and Engineering vol. 5, no. 4, 2013, 638--640.

[2] Baukari N., et al, Security and auditing of VPN. In sdne, IEEE, 1996, 132.

[3] Luo, Zhiyong, et al., Research of A VPN secure networking model.Proceedings of 2013 2nd International Conference on Measurement, Information and Control. 2013, 567--569.

[4] Dhall H, et al (2012), Implementation of IPSec Protocol, Second International Conference on Advanced computing & CommunicationTechnologies.978-0-7695-4640-7/1.2

[5] Gharehchopogh F S, et al 2013), A New Communication Platform for data transmission in Virtual Private Network, International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol. 3, No.2,DOI : 10.5121/ijmnct.2013320101.

[6] Hussein S N et al (2013), The Impact Of Using Security Protocols In Dedicated Private Network And Virtual Private Network, International Journal of Scientific & Technology Research, Volume 2, Issue 11, ISSN 22778616, pp. 170-175.

[7] Kumar N M et al (2013), Proposed Architecture for Implementing Privacy In Cloud Computing Using Grids And Virtual Private Network. International Journal of Technology Enhancements and emerging Engineering Research, Volume 1, Issue 3, ISSN 2347-4289