

**DESIGN AND IMPLIMENTATION OF VIRTUAL PRIVATE NETWORK (VPN)  
OF A CORPORATE OFFICE**

**BY**

**TANJIL MIAH  
ID: 162-15-8150**

**AND**

**FERDUSI AKTHER  
ID: 162-15-8200**

This Report Presented in Partial Fulfillment of the Requirements for the  
Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

**Abdus Sattar**  
**Assistant Professor**  
Department of CSE  
DaffodilInternational University



**DAFFODIL INTERNATIONAL UNIVERSIT**

**DHAKA, BANGLADESH**

**MAY 2019**

## **APPROVAL**

This Project titled “Virtual Private Network” submitted by Tanjil Miah, ID No: 162-15-8150, Ferdusi Akther, ID No: 162-15-8200 to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on May 03, 2019.

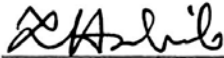
### **BOARD OF EXAMINERS**



**Dr. Syed Akhter Hossain**  
**Professor and Head**

Department of Computer Science and Engineering  
Faculty of Science & Information Technology  
Daffodil International University


**Chairman**



**Md. Tarek Habib**  
**Assistant Professor**

Department of Computer Science and Engineering  
Faculty of Science & Information Technology  
Daffodil International University

**Internal Examiner**



**Moushumi Zaman Bonny**  
**Senior Lecturer**

Department of Computer Science and Engineering  
Faculty of Science & Information Technology  
Daffodil International University

**Internal Examiner**



**Dr. Swakkhar Shatabda**  
**Associate Professor**

Department of Computer Science and Engineering  
United International University

**External Examiner**

©Daffodil international University

## DECLARATION

We hereby declare that, this project has been done by us under the supervision of **Abdus Sattar Assistant Professor, Department of CSE** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

### Supervised by:



---

**Abdus Sattar**  
**Assistant Professor**  
Department of CSE  
Daffodil International University

### Submitted by:



---

**Tanjil Miah**  
ID: 16-15-8150-  
Department of CSE  
Daffodil International University



---

**Ferdusi Akther**  
ID: 16-15-8200  
Department of CSE  
Daffodil International University

## ACKNOWLEDGEMENT

First we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year project/internship successfully.

We really grateful and wish our profound our indebtedness to Supervisor **Abdus Sattar Assistant Professor**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of “*Field name*” to carry out this project. His endless patience ,scholarly guidance ,continual encouragement , constant and energetic supervision, constructive criticism , valuable advice ,reading many inferior draft and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to **Dr. Syed Akther Hossain Professor**, and Head, Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

## **ABSTRACT**

Now a days increasing demand to connect between internal network and distance location. For that reason it is necessary to connect the employees of any organization to internal private network with over the internet. And it's necessary also to maintain the security which could be connect from home, office, university, hostels, airport, and bus station or from any other external network. VPN (Virtual Private Network) is a technology which provides a security to protect the information which will be transmitted over the network and will be allowed by the authenticate users. This paper provides a general guideline of a VPN implementation over the internet with an organization. We elaborated a security risks and how it could be implemented with a virtual private network.

# TABLE OF CONTENTS

<b>CONTENTS</b>	<b>PAGE</b>
<b>DECLARATION</b>	i
<b>ACKNOWLEDGEMENTS</b>	iii
<b>ABSTRACT</b>	iv
<b>CHAPTER</b>	
<b>CHAPTER 1: INTRODUCTION</b>	<b>1-2</b>
1.1 Introduction	1
1.2 Project Objectives	1
1.3 Project Goals	1
1.4 Report Layout	2
<b>CHAPTER 2: COMPUTER NETWORKING</b>	<b>3-12</b>
2.1 Internetworking	3
2.2 Internetworking Device	4
2.3 Network Topology	12
<b>CHAPTER 3: OSI REFERENCE MODEL</b>	<b>13-21</b>
3.1 OSI Reference Model	13
3.2 Transmission Control protocol (TCP) IP Model	15
3.3. Internetwork Addressing	16
3.4 Local Area Network (LAN)	18
3.5 Wide Area Network (WAN)	19
3.6 Firewalls	21
<b>CHAPTER 4: VIRTUAL NETWORKS (VPNs)</b>	<b>22-26</b>
4.1 Overview of VPNs	22
4.2 VPN Device and Technologies	22
4.3 Remote- access VPN	24
4.4 Site-to-Site	25
4.5 Remote Access VPN	25

<b>CHAPTER 5:DESIGN AND IMPLIMENTATION OF VPN</b>	<b>28-29</b>
5.1 VPN Design Proposal	28
5.2 Site-to-site VPN design	28
5.3 Remote access VPN design	29
<b>CHAPTER 6: CONCLUSION</b>	<b>31</b>
<b>REFERENCES</b>	<b>32</b>

## LIST OF FIGURES

<b>FIGURES</b>	<b>PAGE NO.</b>
Figure 2.1.1 An Internetwork Formed from Different Network Segments	3
Figure 2.2.1 Internetworking Devices	4
Figure 2.3.1 Bus Topology Features of Bus Topology	5
Figure 2.3.2 Ring Topology Features of Ring Topology	6
Figure 2.3.3 Star Topology Features of Star Topology	8
Figure 2.3.4 Mesh Topology Types of Mesh Topology	9
Figure 2.3.5 Tree Topology Features of Tree Topology	10
Figure 2.3.6 Hybrid Topology Features of Hybrid Topology	11
Figure 3.1.1 OSI Layers. Reprinted from OSI Model	14
Figure 3.2.1 Transmission Control Protocol Header	16
Figure 3.2.2 Classes of Network Address. Reprinted	17
Figure 3.4.1 Local Area Network (LAN) diagram	18
Figure 3.5.1 WAN Technology Connectivity Options	19
Figure 3.6.1 Firewall Location in the Network. Reprinted from Firewall	20
Figure 4.4.1 Site-to-Site VPN network diagram	24
Figure 4.5.1 Remote Access VPN	25
Figure 5.2.1 site-to-site VPN	28
Figure 5.3.1 Remote access VPN design	29



# CHAPTER 1

## INTRODUCTION

### 1.1 Introduction

Earlier, business organization would appliance leased or dedicated lines to connect to their several branches with their main office or telecommuters so as to established and ensure secure data transfer. Nevertheless, for corporations using dedicated leased line is not practical in terms of cost, space coverage and time needed for installation. Recently several years, the direction of network topology has been changed tremendously and it has changed also rapid development of the network. The internet has become abundant, almost everywhere and every time in any situation. However, the Internet is exposed to attackers sniffing sensitive information. Last several years we see that Virtual Private Networks (VPNs) this concept is more popular and is an alternative solution for any organization to secured their different branches which result in the use of public networks, which is unsecure, for private communications.

As security is the top priority, an established VPN allows packets to tunnel via the public network by providing a secure connection as if they were on private networks. A VPN tunnel implements cryptographic techniques to protect on intercepting VPN packet by attackers when it traverses through the public carrier network. The main VPN technologies that provide secure communication are IPsec VPN and Secured Socket Layer (SSL) VPN.

IPsec is a protocol of suite that is geared around security of data communication. IPsec has several elements which consists of pieces for user authentication, data integrity, confidentiality, and anti-reply attack prevention. IPsec VPN secures the tunnel that is established over a non-secure network.

### 1.2 Objectives

The main objective of this project to establish secure data communication network in a corporate office between their remote branch and main office. Bellow listed are pre-requisite to establish the project:

Below are some of the prerequisites that were specified by the company president:

1. Workers at the remote branch shall be able to connect securely to the main office LAN using their PCs.
2. The remote branch office employees need access to the following services on the main office LAN: client database stored on web server, email stored on local server.
3. The VPN shall be implemented in the most expedient manner possible since the new branch is scheduled to be up and running.

### 1.3 Project Goals:

Our project goals were to configure and test three different types of VPNs in order to confirm that the VPN best suited to meet all of the prerequisites laid out by the company president under the objectives section above is an IPSec Client VPN.

In order to do this, we implemented and tested the following types of VPNs:

- a) **Site-to-site:** Tunnel mode connection between VPN gateways. The process of encrypting and transferring data between networks is transparent to end-users.
- b) **IPSec client:** Network Layer VPN for both network-to-network and remote-access deployments. End-users will need to run either Cisco or Open Source VPN software on their PCs.
- c) **Clientless SSL:** “Remote-access VPN technology that provides Presentation Layer encryption services for Applications through local redirection on the client.” [2] VPN communications are established using a browser rather than specific software installed on the end-user’s device.

### 1.4 Report Layout

In chapter 1: have the purpose of the coaching staff, the participation of the coaching staff and described.

In chapter 2: we have described about Computer Network and Network Topology.

In chapter 3: We have discussed about the OSI Reference models and describe details about them.

In Chapter 4: Discussed about Virtual Network (VPNs) and Technology about VPNs.

In chapter 5: Discussed benefits of VPNs.

In chapter 6: Discussed Conclusion of the report.

# CHAPTER 2

## COMPUTER NETWORK AND NETWORK TOPOLOGY

### 2.1 Internetworking

Recently the Internet has changed the world in the sector of communication channels, where intercommunication has become vital in our daily lives. The computer revolution is a key factor for the dramatic change in the information sector. The Internet encompasses thousands of computer networks that interconnect a bulk of computing devices around the globe [1].

The demand of networks and networking shown an exponential increase in the past two decades. To point out some of the benefits for the telecommuters, headquarters, branch offices, or home offices are to offer connection whether they are located in the same place or a different geo-location and share different services and resources. For example they can share data, printers, video conferences and VoIP services [5].

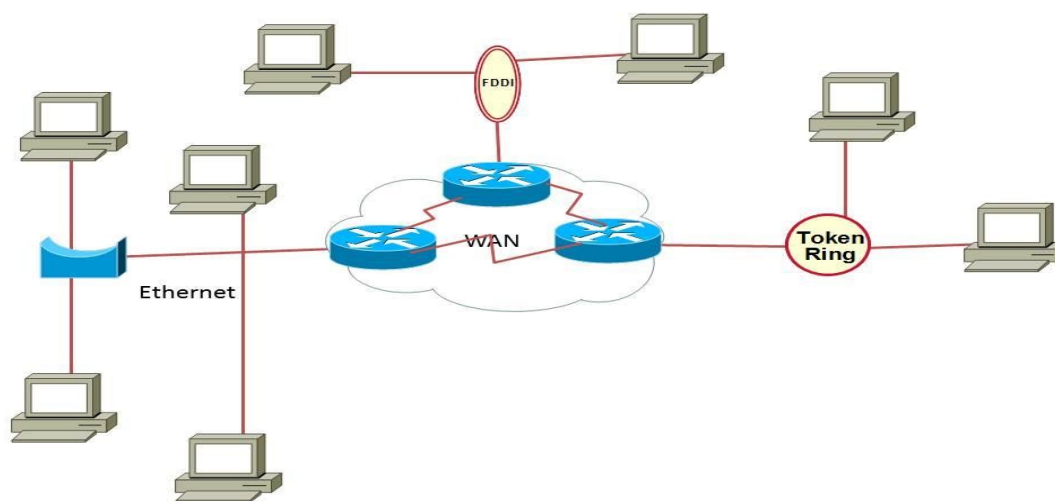


Figure 2.1.1 An Internetwork Formed from Different Network Segments

An internetwork is a combination of multiple local area networks connected through gate-way devices that contribute and forward routing information of packets among the networks. The gateways can be routers, firewall appliances, or layer 3 switches that have configured their interfaces using the IPv4 or IPv6 addressing scheme. Figure 1 below illustrates those different internetworking technologies that are interconnected via routers, bridges and switches. The internetworking technology mentioned in figure 1 will be illustrated in section 2.3 and 2.4 in detail. For example LAN (Local Area Networks) and WAN (Wide Area Networks) and FDDI

and Token Ring are legacy technology which has been replaced with a new technology that are economical and scalable [2].

Establishing a working and efficient internetworking is not an easy task. There are certain areas needed to be addressed to maintain smooth working conditions. Some of the internetworking challenges are listed below:

- Connectivity issue: The issue when connecting different multiple networks is to get successful connectivity to the other end device. For example the end device is implementing a different networking technology and different kinds of media running at various bandwidth levels [2].
- Reliability: Expecting network connectivity of the company to work and services are reachable all the time [2].
- Centralized network management: Additionally, it is good to secure the network from inside and outside users. Most of the security attacks come from users in the internal network. Implementing network management that gives trouble-shooting and managing of security issues, configuration and performance in the network [2].
- Adaptation to change: Internetworks must be flexible to change to this dynamic world, since technology is changing all the time [2].

## 2.2 Internetworking Device

It is time now to introduce some of the commonly used internetworking devices and their functions in the communication system.

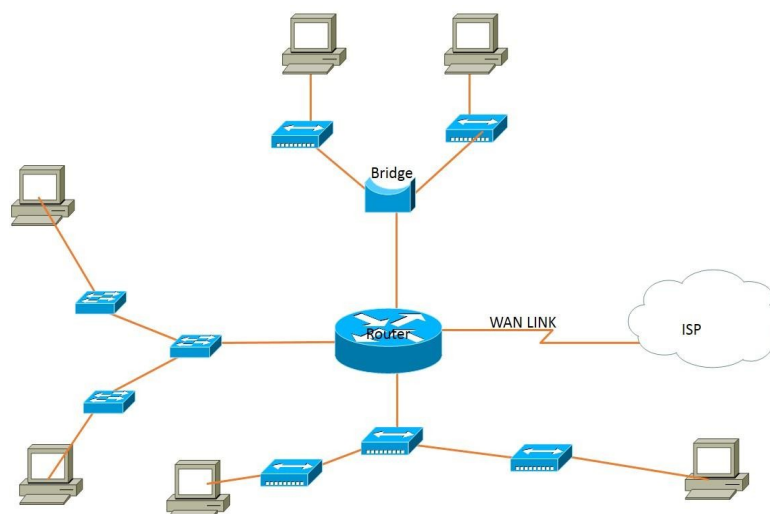


Figure 2.2.1 Internetworking Devices

- i. **Hub:** An Ethernet Hub, which is a multiport repeater, is a device connecting many Ethernet devices into a single logical topology network that can send data across the connected perimeter network. An Ethernet hub is primarily kind of a repeater. When a hub transmits data, it will repeat the signal to all ports and this will create a problem when another port sends traffic at the same time. This broadcast message will be send to all interfaces results as a collision effect. A hub is one collision domain. A collision domain as the name indicates it is a collision of signals in a network segment [6].
- ii. **Switch:** A switch is a layer 2 device which uses Application Specific Integrated Circuits (ASICs) to form and update Media Access Control (MAC) table. Switches and bridges, which are layer 2 devices, are fast compared to routers, because they do not spend time looking at the IP layer header information. Rather they look at the frame header to forward, flood or drop the frame. When a data frame is sent to the interface, the switch will track the connected devices' MAC address and saves the MAC addresses to its Content Addressable Memory (CAM) table. Switches filter data frames based on layer 2 information which is MAC ad-dress [6].
- iii. **Router:** A router is an internetworking device which connects multiple logical networks. Router interfaces are separate broadcast domains and collision domains. They do not forward broadcast traffic to the other network segment and they forward IP packets based on the destination IP address, provided that some of routers' functions in an internetwork are packet selection, packet switching, connecting internetworks and choosing best path for the routing[6].

## 2.3 Network Topology

Network Topology is the schematic description of a network arrangement, connecting various nodes (sender and receiver) through lines of connection.

### 2.3.1 Types of Network Topology:

- i. **BUS Topology:** Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called Linear Bus topology.

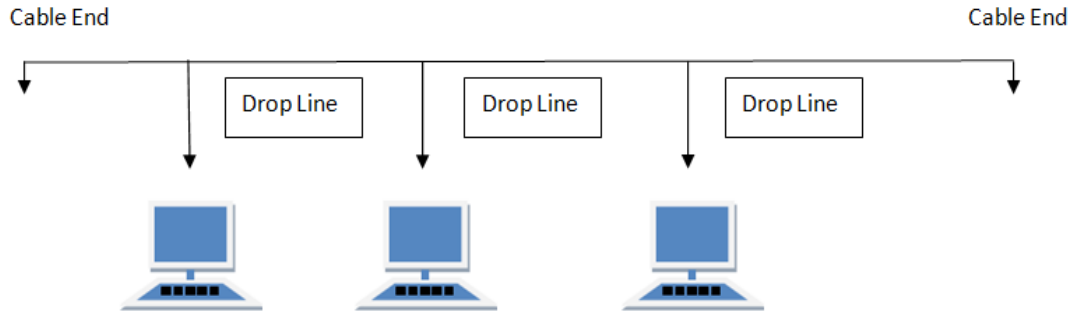


Figure 2.3.1 Bus Topology Features of Bus Topology

- It transmits data only in one direction.
- Every device is connected to a single cable

#### Advantages of Bus Topology

- It is cost effective.
- Cable required is least compared to other network topology.
- Used in small networks.
- It is easy to understand.
- Easy to expand joining two cables together.

#### Disadvantages of Bus Topology

- Cables fails then whole network fails.
- If network traffic is heavy or nodes are more the performance of the network decreases.
- Cable has a limited length.
- It is slower than the ring topology.

- ii. **RING Topology:** It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbors for each device.

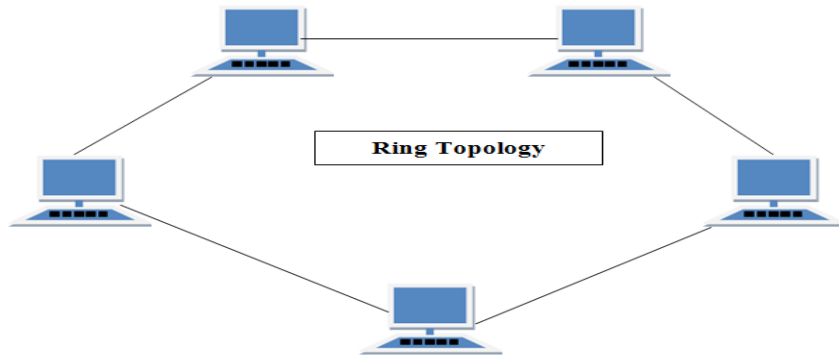


Figure 2.3.2 Ring Topology Features of Ring Topology

- A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
- The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
- In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
- Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

#### Advantages of Ring Topology

- Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
- Cheap to install and expand

#### Disadvantages of Ring Topology

- Troubleshooting is difficult in ring topology.
  - Adding or deleting the computers disturbs the network activity.
  - Failure of one computer disturbs the whole network.
- iii. **STAR Topology:** In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node.

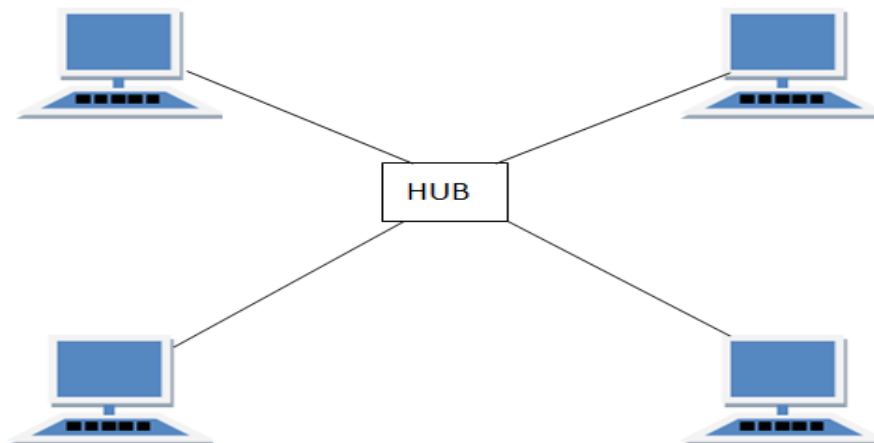


Figure 2.3.3 Star Topology Features of Star Topology

- Every node has its own dedicated connection to the hub.
- Hub acts as a repeater for data flow.
- Can be used with twisted pair, Optical Fiber or coaxial cable.

### **Advantages of Star Topology**

- Fast performance with few nodes and low network traffic.
- Hub can be upgraded easily.
- Easy to troubleshoot.



- Easy to setup and modify.
- Only that node is affected which has failed, rest of the nodes can work smoothly.

### **Disadvantages of Star Topology**

- Cost of installation is high.
  - Expensive to use.
  - If the hub fails then the whole network is stopped because all the nodes depend on the hub.
  - Performance is based on the hub that is it depends on its capacity
- iv. **MESH Topology:**It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has  $n(n-2)/2$  physical channels to link  $n$  devices.

There are two techniques to transmit data over the Mesh topology, they are:

- a) **Routing:** In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.
- b) **Flooding:**In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the it's very unlikely to lose the data. But it leads to unwanted load over the network.

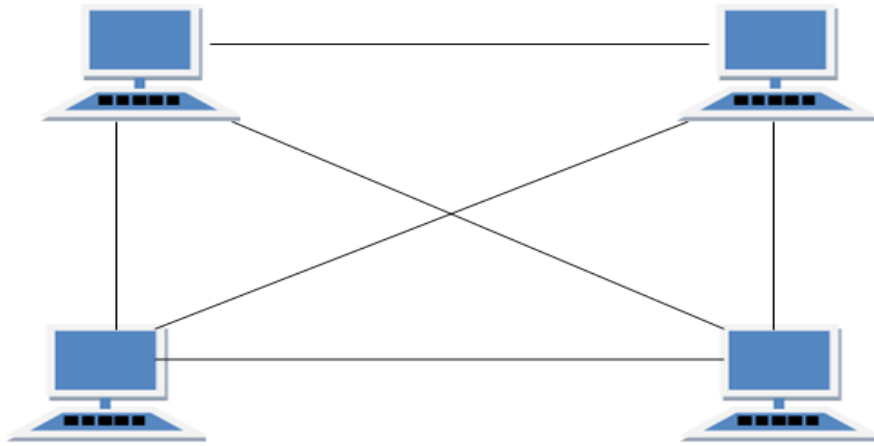


Figure 2.3.4 Mesh Topology Types of Mesh Topology

- **Partial Mesh Topology:** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
- **Full Mesh Topology:** Each and every nodes or devices are connected to each other.

### Features of Mesh Topology

- Fully connected.
- Robust.
- Not flexible.

### Advantages of Mesh Topology

- Each connection can carry its own data load.
- It is robust.
- Fault is diagnosed easily.
- Provides security and privacy.

### Disadvantages of Mesh Topology

- Installation and configuration is difficult.
  - Cabling cost is more.
  - Bulk wiring is required.
- v. **TREE Topology:** It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.

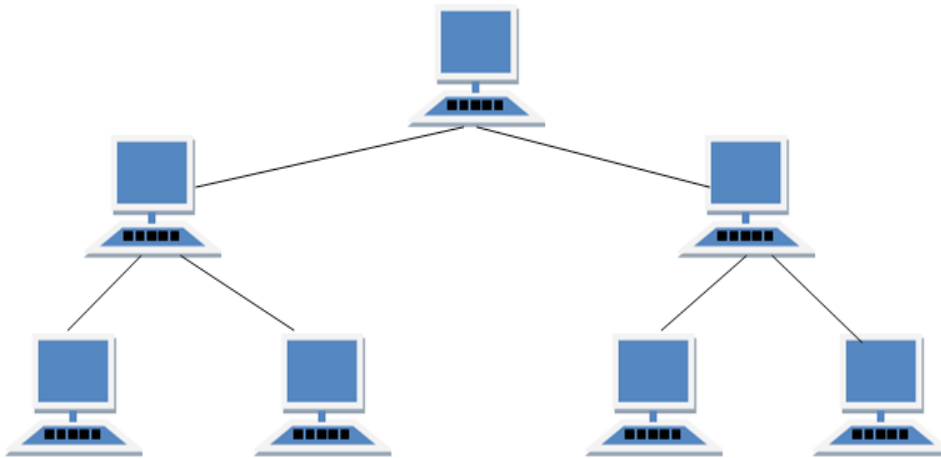


Figure 2.3.5 Tree Topology Features of Tree Topology

- Ideal if workstations are located in groups.
- Used in Wide Area Network.

### Advantages of Tree Topology

- Extension of bus and star topologies.
- Expansion of nodes is possible and easy.
- Easily managed and maintained.

- Error detection is easily done.

### Disadvantages of Tree Topology

- Heavily cabled.
  - Costly.
  - If more nodes are added maintenance is difficult.
  - Central hub fails, network fails.
- vi. **HYBRID Topology:**It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

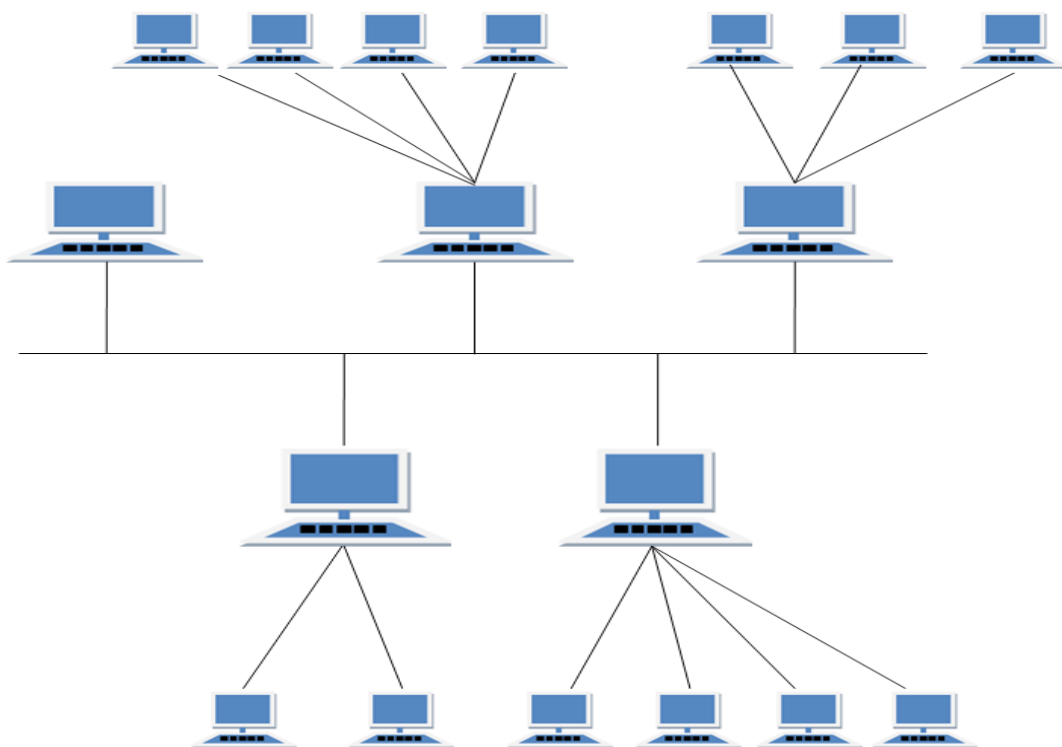


Figure 2.3.6 Hybrid Topology Features of Hybrid Topology

- It is a combination of two or topologies
- Inherits the advantages and disadvantages of the topologies included

### **Advantages of Hybrid Topology**

- Reliable as Error detecting and trouble shooting is easy.
- Effective.
- Scalable as size can be increased easily.
- Flexible.

### **Disadvantages of Hybrid Topology**

- Complex in design.
- Costly.

## CHAPTER 3

### OSI REFERENCE MODEL AND COMPUTER LAN

#### 3.1 OSI Reference Model

The OSI reference model is a standardized architecture defining network communications. It allows cross-platform communication for different vendors like Apple, Dell, or IBM to communicate with each other. The OSI model is a logical or conceptual model that breaks down a communication system into seven abstraction layers [5].

Basically, an OSI reference model is a hierarchical model that comprises seven abstraction layers. Its specific protocols from top to bottom layers are application, presentation, session, transport, network, data-link, and physical layers respectively as shown in figure 6 below. Each layer has its own unique functions and protocols [5].

There are many benefits of OSI model architecture. To mention some of the advantages of the OSI reference models are described below [5]:

- It breaks down network communication into smaller chunks that accelerate de-signing, developing and troubleshooting components.
- It cooperates inter-vendor development by implementing the common standardized component architecture.
- It ensures interoperable technology for different vendors.
- It reduces complications.

Figure 3.1.1 shows a list of OSI model layers, data unit, functions of the layers and some of the corresponding protocols. For example, in layer 7 which is the application layer the unit in this layer is data unit. The functions are high level Application Programming Interfaces (APIs) and protocols such as Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS) and File Transfer Protocol (FTP). Let us discuss each layers of the OSI model.

Layer	Function	Example
<b>Application (7)</b>	Services that are used with end user applications	SMTP,
<b>Presentation (6)</b>	Formats the data so that it can be viewed by the user Encrypt and decrypt	JPG, GIF, HTTPS, SSL, TLS
<b>Session (5)</b>	Establishes/ends connections between two hosts	NetBIOS, PPTP
<b>Transport (4)</b>	Responsible for the transport protocol and error handling	TCP, UDP
<b>Network (3)</b>	Reads the IP address form the packet.	Routers, Layer 3 Switches
<b>Data Link (2)</b>	Reads the MAC address from the data packet	Switches
<b>Physical (1)</b>	Send data on to the physical wire.	Hubs, NICS, Cable

Figure 3.1.1OSI Layers. Reprinted from OSI Model [7].

- i. **Application Layer:** This layer is the layer 7 of the OSI reference model and also it is the nearest layer to the user sitting on the computer host that is trying to browse or use some resources over the network like the servers, email, videos, or voice. This means that users can make communication directly to the OSI application layer through an API. When validating the communication node or host, the application layer identifies and determine whether the intended peer communication partner is available or not prior to data transfer. Some of the examples this layer is using includes Telnet, File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP) [2].
- ii. **Presentation Layer:** The presentation layer engages in translation and format-ting services. This layer helps communication which is sent from one application layer and can be understood on other end application layer. Some of the functionalities of this layer are data compression, decompression, and encryption and decryption services [2].

- iii. **Session Layer:** This layer provides session management. It sets up and tear down connections to other users.
- iv. **Transport Layer:** This layer gives service to host-to-host communication by assuring the communication channel to be either reliable or unreliable communication. The two main protocols used in this layer are TCP (for reliable communication) and UDP (for unreliable communication).It also implements flow control and multiplexing data control mechanisms [5].
- v. **Network Layer:** This layer is layer 3 of the protocol stack of the OSI model and is serving as device addressing. IP is the protocol used for device addressing. This layer is used to connect different networks in an internetwork by implementing a router device for routing and updating purposes [5].
- vi. **Data Link Layer:** This layer engages in physical data transmission and some of this layer's services are flow control, error alerting, and topology scheme [5].
- vii. **Physical Layer:** This layer is the first layer of the OSI model and is located at the bottom layer of the stack list and its function is to send bits and receiving bits [6].

### 3.2 Transmission Control Protocol (TCP) / Internet Protocol (IP) Model

TCP/IP model is a condensed model of the OSI reference model. TCP/IP model shrinks the application, session, and presentation layer into the process layer. TCP/IP layer has four layers: [5]

- o Application
- o Transport
- o Internet
- o Network Access

Transmission Control Protocol (TCP), which is a reliable data communication, receives a chunk of data information from an application layer of the OSI reference model and divides that into smaller chunks of data segments. It adds a sequence number to each data segment so that the destination TCP peer application can build up the data segments back to the original full data. After the data segments are sent from the sender host, the TCP expects an acknowledgment from the recipient peer host, and retransmits the data in case if any data segment is missing or not acknowledged. First the TCP stack forms a connection which is called virtual circuit. During the initial TCP 3-way handshake,



The two TCP peer stack layers must agree on the size of the data information that they are going to exchange before the recipient sends an acknowledgement back. The User Datagram Protocol (UDP) is preferred for unreliable data communication such as real-time video and VoIP [3].

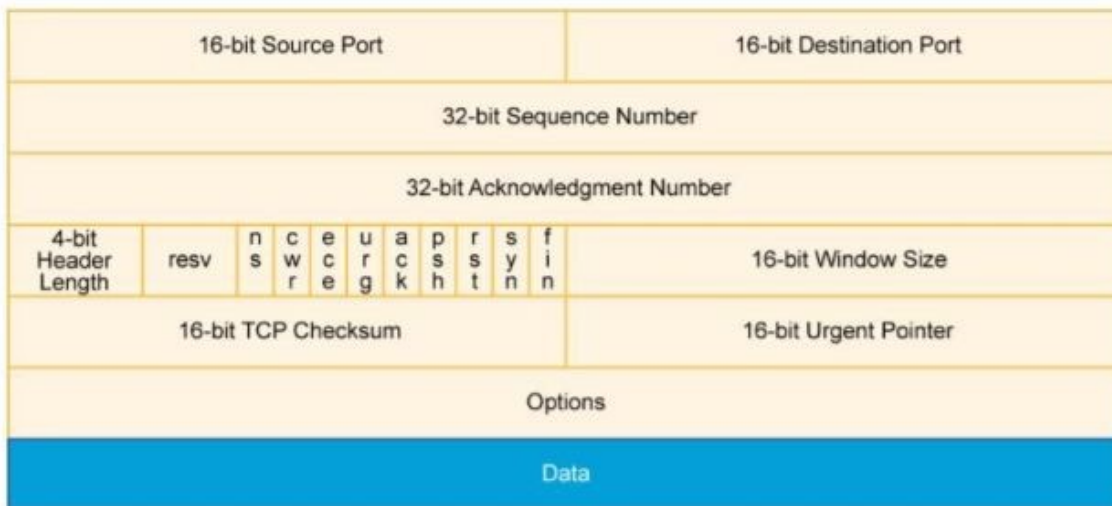


Figure 3.2.1 Transmission Control Protocol Header. Reprinted from Transmission Control Protocol [21].

### 3.3 Internetwork Addressing

Internetwork addressing is the addressing of network devices individually or as a group. The network device addressing scheme varies with the layers they reside as well as the protocols they use. There are three categories of addressing network devices: network layer address, mac address and data link layer address [2].

#### i. Data Link Layer Addresses

A data link layer addresses is layer 2 in the OSI reference model. It can uniquely identify the physical network connection in an internetwork devices. This address is assigned to the devices by the manufacturer to the specific devices [2].

The data link layer has two sub layers, the MAC address sub layer and Logical Link Layer (LLC). The MAC address are assigned by the vendor and they are 48 bits long [2].

#### ii. Network Layer Addresses

The network addresses located at the layer 3 of the OSI model and the relationship to the devices is virtual or logical addresses unlike MAC addresses which are fixed to the devices. In network layers addressing the most common protocols are IPv4 and IPv6 protocols. An IP address is a software address that is designed to identify numerical addresses assigned to each device in an IP network. It allows different devices on an internetwork to communicate regardless of the LANs the nodes reside in. [2]

Class	Leading bits	Size of network number bit field	Size of rest bit field	Number of networks	Addresses per network	Start address	End address
Class A	0	8	24	128 ( $2^7$ )	16,777,216 ( $2^{24}$ )	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 ( $2^{14}$ )	65,536 ( $2^{16}$ )	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 ( $2^{21}$ )	256 ( $2^8$ )	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

Figure 3.2.2 Classes of Network Address [22].

The IP address expression 10.0.0.0/24 is used in this project for describing the IP address ranges. It actually means that the IP address starts with 10.0.0.0 and the right-most 8 bits will vary. The 8 is calculated by using 32 bit. So 10.0.0.0/24 means it covers the address range from 10.0.0.0 to 10.0.0.255. The Request for Comments (RFC) 1918 of private IP network addresses are implemented for the internal networks. Those IP address are not routed over the Internet but they reside in the local network. The private network ranges are: [24]

- 10.0.0.0-10.255.255.255 ( or 10.0.0.0/8)
- 172.16.0.0-172.31.255.255 (or 172.16.0.0/12)
- 192.168.0.0-192.168.255.255 (or 192.168.0.0/16)

### 3.4 Local Area Network (LAN)

A LAN is a group of computer networks confined to a limited geographic area such as home, school building, office building or organizations. It typically connects devices like personal computers, shared printers, and servers. It can be connected to a locally cabled or wireless connection. A LAN is usually a high-speed data communication network. The LAN protocols resides at the data link layer and physical layers of the OSI model. A data link layer formats

the Protocol Data Unit (PDU) message into a frame, and adds headers and trailers into the frame. A physical layer sends and receives bits. [6]

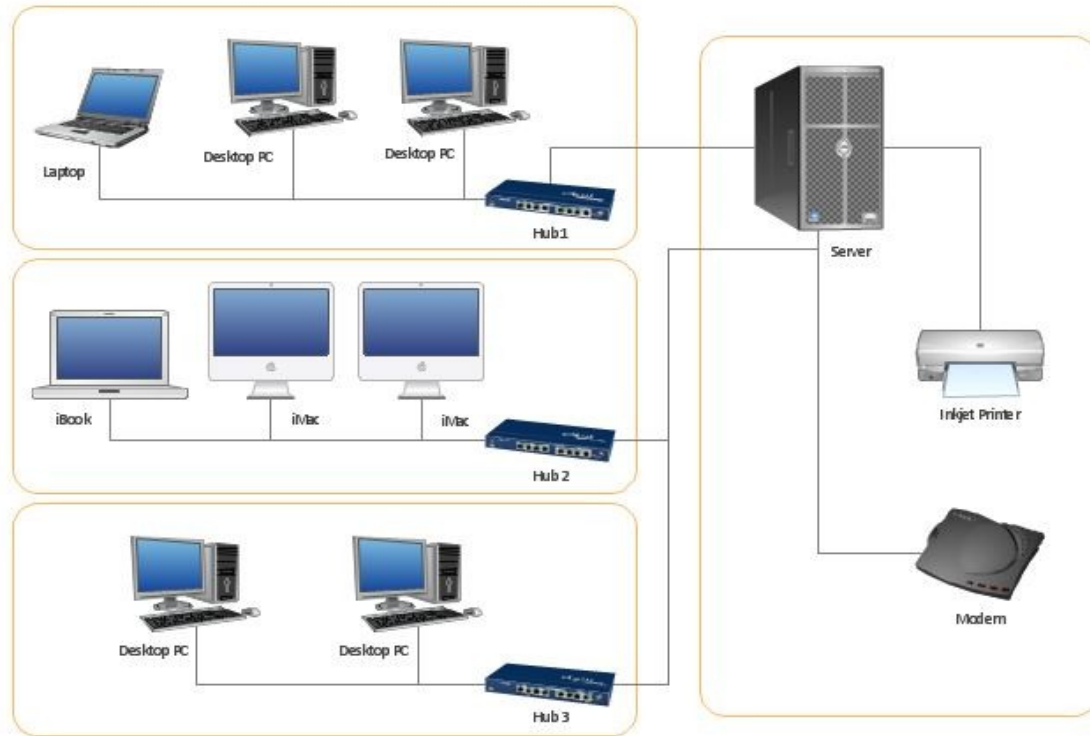


Figure 3.4.1 Local Area Network (LAN) diagram

Basically, for a communication in a LAN there is a standard protocol called the Institute of Electrical and Electronics Engineers (IEEE) 802 family standard. For example, 802.3 is Ethernet, 802.2 Logical Link Control (LLC) or 802.11 wireless LAN or WI-FI. The IEEE 802 standard has two sub layers, LLC and MAC. The MAC is a physical hardware addressing. The Logical Link Control (LLC) is used for identifying network layer protocols and for encapsulation [5].

The LAN data transmission mechanism has three categories: unicast, broadcast, and multicast. When a single packet is transferred from a source to a single destination device it is a unicast transmission, one packet to one. Multicast transmission is sending information to a group of destination nodes, one packet to groups. Broadcast transmission is sending information to all destination nodes, one packet to all. [2]

### 3.5 Wide Area Network (WAN)

A WAN is a network that encompasses a large geographical area and is used to connect multiple networks or LANs for communication. A WAN link defines a new type of the bottom three layers of the OSI model connectivity: the physical layer, the data link layer, and the

network

layer. It allows links to the internet or other offices. Figure 9 simplifies some WAN connectivity technology such as leased lines, circuit switching, packet switching and cell relay.

[5]

Option:	Description	Advantages	Disadvantages	Bandwidth range	Sample protocols used
<b>Leased line</b>	Point-to-Point connection between two computers or Local Area Networks (LANs)	Most secure	Expensive		PPP, HDLC, SDLC, HNAS
<b>Circuit switching</b>	A dedicated circuit path is created between end points. Best example is dialup connections	Less Expensive	Call Setup	28 - 144 kbit/s	PPP, ISDN
<b>Packet switching (Connection oriented)</b>	Devices transport packets via a shared single point-to-point or point-to-multipoint link across a carrier internetwork. Before information can be exchanged between two endpoints, they first establish a Virtual Circuit. Variable length packets are transmitted over Permanent Virtual Circuits (PVC) or Switched Virtual Circuits (SVC)		Shared media across link		X.25, Frame-Relay
<b>Packet switching (Connectionless)</b>	Devices transport packets via a shared single point-to-point or point-to-multipoint link across a carrier internetwork. Variable length packets are transmitted. Between endpoints no connection is build; endpoints can just offer packets to the network, addressed to any other endpoint and the network will try to deliver the packet. As an example: the Internet works this way.	Very robust and low overhead	Shared media across link		IPv4, IPv6
<b>Cell relay</b>	Similar to packet switching, but uses fixed length cells instead of variable length packets. Data is divided into fixed-length cells and then transported across virtual circuits	Before 2000 this was seen as the best option for simultaneous use of voice and data. With the much higher link speeds in modern networks, this advantage is effectively meaningless.	Overhead can be considerable		ATM

Figure 3.5.1 WAN Technology Connectivity Options [10]

A Virtual Private Network (VPN) which is a major topic of this thesis is a type of WAN technology. It connects different company or sites which are located at different geo-location and makes it like, the connected company or sites, as if they are connected locally.

### 3.6 Firewalls

A firewall is a device, hardware or software or both, that is designed to prevent unauthorized outside user from accessing a network or host. It is a network security that pre-vents inside users from sending sensitive information or accessing an unsecured net-work. It protects hosts by implementing boundaries or restricting IP network connectivity [4].

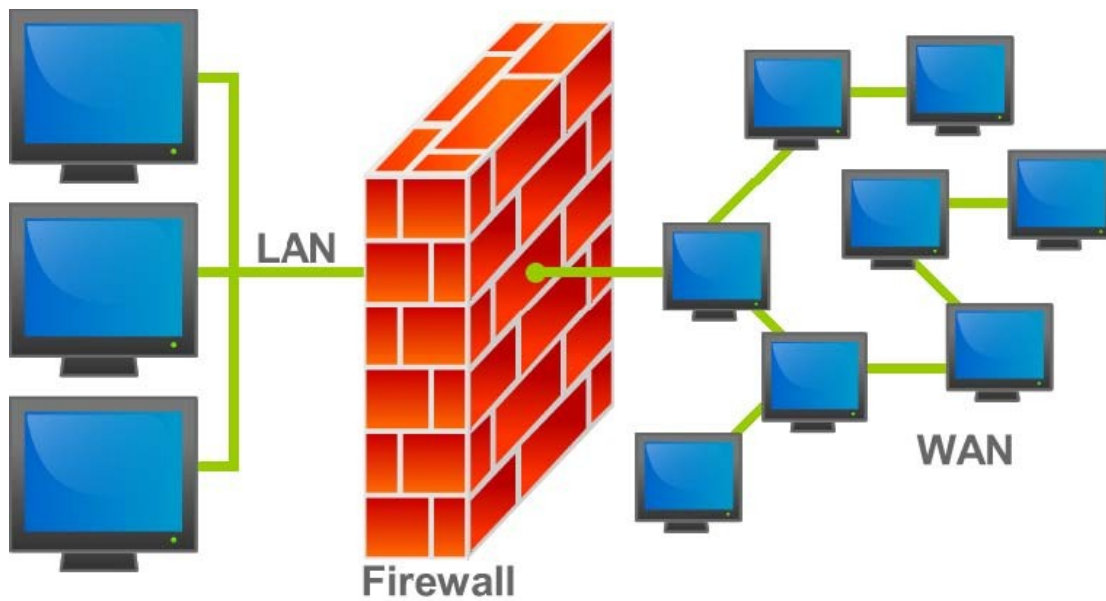


Figure 3.6.1 Firewall Location in the Network. Reprinted from Firewall [11].

A firewall needs a proper set of rules or proper security policy to prevent inside host or subnet vulnerability. To connect to the unsecure network a firewall implements a set of security policy and use proxy address. Firewalls can implement Network Address Translation (NAT), Port Address (PAT) or Virtual Private Network (VPN).

This project uses firewall or gateway appliances from two different vendors. Those are Cisco ASA 5505 and Juniper SRX240, they are connected and implemented using a VPN scenario to securely communicate over the public network.

## CHAPTER 4

### VIRTUAL PRIVATE NETWORKS (VPNS)

#### 4.1 Overview of VPNs

Virtual Private Network (VPN) is a generic term that is used to establish secure communication channel over public network infrastructure that is Internet or service provider network. The Internet domain network is sometimes known as the VPN backbone. It is important for transferring multiple data traffic over the public network for VPNs oriented communication or for non-VPN oriented communication [13].

VPN could refer to the network connectivity between two remote sites. If the VPN acronym is break down into its' individual letters, the letter V in a VPN stands for virtual and it refers to a logical connection between the two network devices. The letter P stands for private and it refer that the logical network that is created between two devices is private. The letter N is for network, of course a VPN is a WAN link network. For example, one user may be connected to the public network in corporate site 1 and another user may be connected to the public network in corporate site 2, a logical network or virtual network could be built between the two sites using the Internet as a transport medium. The word private refers to the communication between the two sites which is private [13].

However, if we had a VPN established between remote sites over the public network that is the Internet, what would prevent the data from an eavesdropper who is sniffing on the communication wire? To protect the data from malicious manipulation the VPN ingredients of confidentiality, authentication, data integrity and anti-replay comes to play. The eavesdropper cannot exploit the data since it is encrypted and he/she does not have the right key to exploit the data content [13].

#### 4.2 VPN Devices and Technologies

##### i. VPN Devices

In a corporate network or organization infrastructure a VPN terminator device erects in different area of the infrastructure network. The VPN devices that are erected in the customer and service provider can be clarified as follows [8].

- Customer (C) devices: Those devices belong to the customer network and they are not connected to the service provider infrastructure. Some of the C devices are routers and switches that reside within the customer network. The customer devices do not have any clue about the VPN network.
- Customer Edge (CE) devices: The CE devices are connected through the service provider network and they are located, as the name indicates, within the customer edge network. In a CE- based network the devices know about the VPN network, but in the Provider Edge (PE)-based network they do not know whether there is a VPN at all. Some examples of the CE devices that reside in this network are Customer Edge routers and Customer Edge switches.
- Service Provider (P) devices: The P devices are not connected directly to customer networks. The P devices do not know whether there is a VPN at all. Some examples of the P devices are routers and switches with in the perimeter of the provider network.
- Service Provider Edge (PE) devices: The PE devices are directly connected to the customer C network through the customer CE devices. Additionally, in the PE-based network VPNs the PE devices know about the VPN network. But in the CE-based VPNs the PE devices are not aware if there is a VPN network at all. Some examples of the devices are Provider Edge router, Provider Edge switch, and Provider Edge devices that have ability to route and switch.
- Network Access Servers (NAS) devices: NAS devices are points of access for components between modem devices network such as Public Switched Telephone Network (PSTN) and a packet switched network. A NAS device can act as a tunnel end in a remote access VPN.
- VPN gateways: A VPN concentrator is used as a VPN tunnel end in CE- based site-to-site VPN.
- There are many different kinds of commercially implemented VPNs. A VPN can be categorized into two primary broad categories: site-to-site and remote-access VPNs.

## **ii. VPN Technologies**

The VPN technologies implemented for connecting two peers over an unsecure network form a logical network connection. These logical network connections could be established at layer 2 or layer 3 of the OSI reference model. The VPN technologies formed could differ from layer to layer. For the layer 2 of the OSI model layer 2 VPNs are formed and for the layer 3 of the OSI model layer 3 VPNs are formed. A VPN connection made between sites using either



Layer 2 VPNs or Layer 3 VPNs ideally they are similar. The idea includes adding a header information to the front of the data segment content. [20]

### **iii. Layer 2 VPNs**

Layer 2 VPNs as the name indicates work at the layer 2 of the OSI reference model. They are point-to-point WAN links and perform connectivity between sites over a logical connection called a virtual circuit. A virtual circuit is a logical connection between two points in an internetwork from end to end, and can cover a large area of elements and multiple physical segments of a network. The two most common Layer 2 VPN technologies are Asynchronous Transfer Mode (ATM) and Frame Relay. ATM and Frame Relay network connection providers can give best site-to-site connectivity to a company by configuring a permanent virtual circuit (PVC) across a shared network infrastructure. They also offer great Quality of Service (QoS) characteristics, especially for delay-sensitive services such as voice [20].

### **iv. Layer 3 VPNs**

Communication between two peers is said to be Layer 3 VPN if the header information is for the layer 3 of the OSI reference model. Layer 3 VPNs could be either a point-to-point WAN link connection to connect two sites such as GRE and IPsec, or could perform connection any-to-any connectivity to multiple sites such as MPLS VPNs [20].

IPsec VPNs is a major concern that should be dealt with if the VPN technology is implemented to throughput a secure data communication between VPN peers. In this project IPsec VPN of the Layer 3 VPNs technology is implemented to connect two disparate sites and communicate securely over the public Internet [20].

## **4.3 Remote-access VPN**

A remote-access VPN provides access, resources or services, to a telecommuter or a remote user who is securely connected to the remote site or corporate network. They provide that functionality by running client software on the users or telecommuters to create secure communication to the corporate VPN concentrator. Users or telecommuters access the services or resources as if they were in the LAN of the corporate network [9].

In the early days, company users that need to have remote connectivity to access the company service were implementing dial-in networks and ISDN or Public Switched Telephone Network (PSTN) which is expensive. But by implementing a Virtual Private Network to dial-up to ISP is cost-effective [9].



Remote-access VPNs can be either IPsec VPNs or SSL VPNs. A remote-access VPN provides transparent functionality to the end-user or telecommuter who is remotely accessing the corporate services or resources. A remote-access VPN could be a clientless VPN or client-based VPN. A Clientless VPN uses a web browsers based VPN to securely create a remote-access tunnel. The client-based VPN implements client software which needs to be installed in the host Operating System (OS) to create a remote-access tunnel [9].

Large business organizations with multiple IT departments may setup and deploy their own remote-access VPN to give service to their resources. The remote-access VPNs are beneficial for the telecommuters. But for organization with thousands of employees and with many branch offices, implementing a remote-access VPN is not a wise decision. However, in such organizations' situation site-to-site VPNs are effective alternative solution.

#### 4.4 Site-to-site VPN

A site-to-site VPN is a VPN implementation where companies may have two or more sites that need to securely connect and communicate with each other. Site-to-site VPNs are primarily deployed to secure data between two remote sites in a corporate organization, or between a corporate organization and an individual user who is a telecommuter. Site-to-site VPNs are more common practice on the WAN connection over the public network infrastructure that is the Internet than over the private LANs networks. However, nowadays many corporate organizations are hiding data information between multiple sites of the private LAN networks to protect data communication. A LAN to LAN VPNs also provide a cheaper connectivity cost and high availability over the dedicated leased private links. They can provide network redundancy, if there is a failure in private net-works. [9]

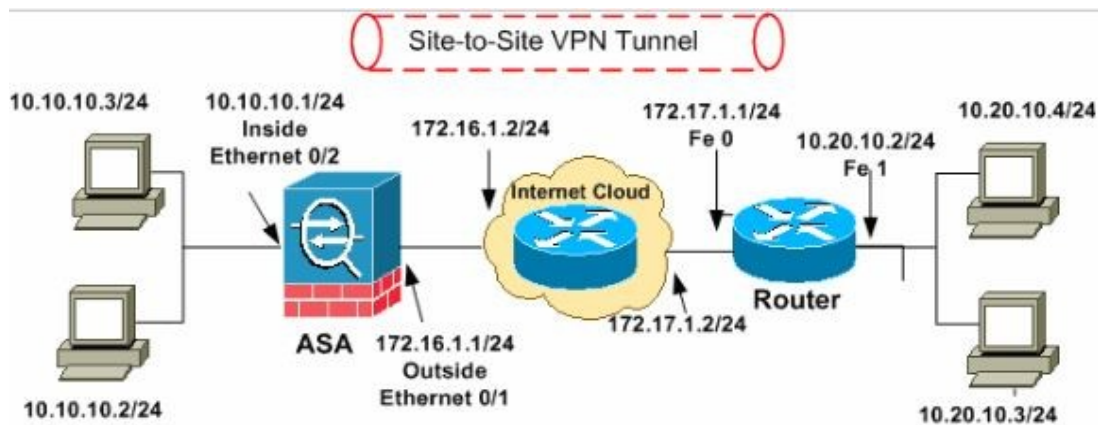


Figure 4.4.1 Site-to-Site VPN network diagram

#### 4.5 Remote-access VPN

A remote-access VPN allows individual users to establish secure connections with a remote computer network. Those users can access the secure resources on that network as if they were directly plugged in to the network's servers. An example of a company that needs a remote access VPN is a large firm with hundreds of salespeople in the field. Another name for

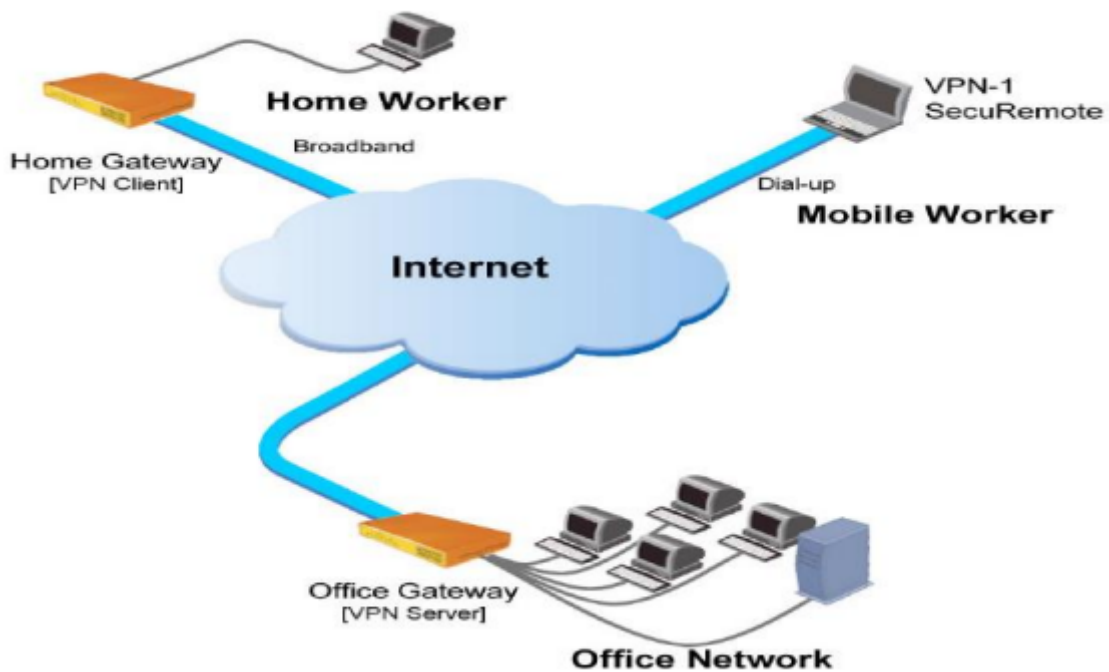


Figure 4.5.1 Remote Access VPN

This type of VPN is virtual private dial-up network (VPDN), acknowledging that in its earliest form, a remote-access VPN required dialing in to a server using an analog telephone system.

There are two components required in a remote-access VPN. The first is a network access server (NAS), also called a media gateway or a remote-access server. The other required component of remote-access VPNs is client software. In other words, employees who want to use the VPN from their computers require software on those computers that can establish and maintain a connection to the VPN. Most operating systems today have built-in software that can connect to remote-access VPNs, though some VPNs might require users to install a specific application instead. The client software sets up the tunneled connection to a NAS, which the user indicates by its Internet address. The software also manages the encryption required to keep the connection secure.

Large corporations or businesses with knowledgeable IT staff typically purchase, deploy and maintain their own remote-access VPNs. Businesses can also choose to outsource their remote access VPN services through an enterprise service provider (ESP). A remote-access VPN is great for individual employees.

## **CHAPTER 5**

# Design and Implementation of VPN

## 5.1 VPN Design proposal

The main office has an Email server and File server .Branches from different remote areas can easily communicate with each other and clients. The administrator of the branch sales office needs to configure a virtual private network (VPN) connection between the branch sales office and the corporate office to enable the remote connections.

Completing planning worksheets for VPN connection from the branch office to remote sales employees. The administrator of the Head office create VPN design and IP planning worksheets to help configure virtual private network (VPN) between the branch sales office and the corporate office.

Here we designed both Site-to-Site and Remote-Access VPNs over City bank ltd. For secure connectivity.

### Network requirement:

- All the offices should be interconnected with each other using VPN technology.
- The users at all the location should be able to access the email, Google and file server.
- Users at all the locations should have access to internet, and should not be routed through the VPN network.
- Appliances like routers to setup the network.
- Identify additional requirements like public ip addresses, internet connections etc.
- Identify the IP network schema for all the locations.
- Identify the methodology to route internet traffic separately and not through the
- User must know whether the IP address assigned to the other VPN device is static or dynamic. If the other VPN device has a dynamic IP address.
- Remote Branch Offices must know the shared key (passphrase) for the tunnel. The same shared key must be used by each device.

## 5.2 Site-to-Site VPN Design:

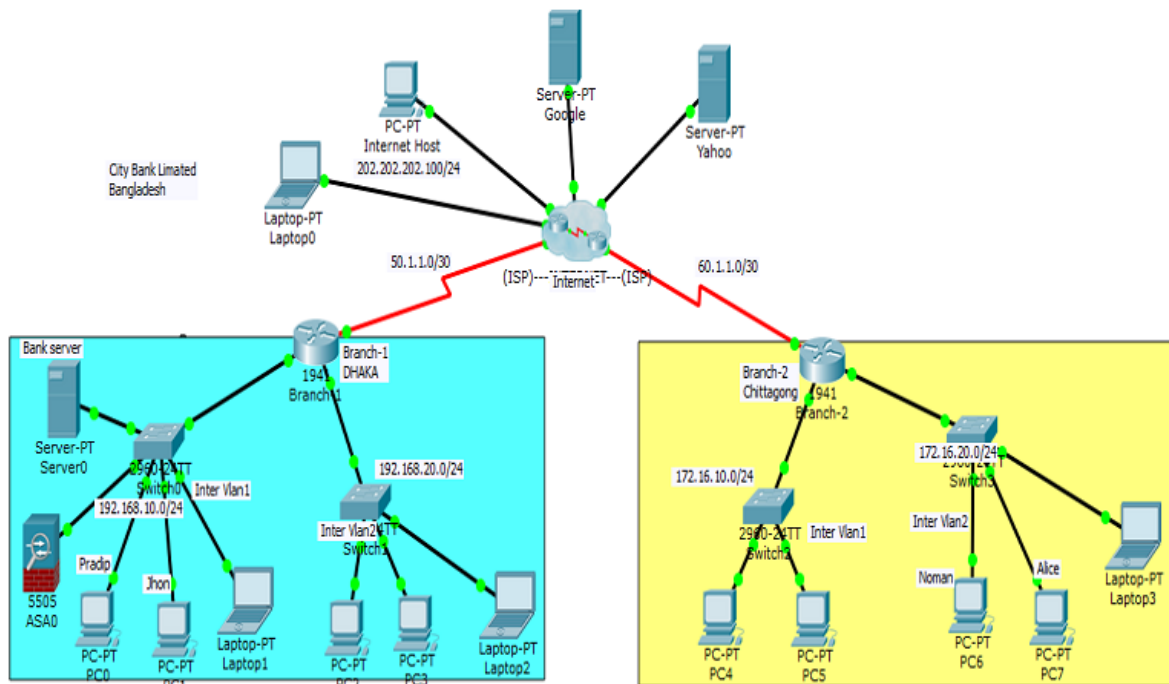


Figure 5.2.1 site-to-site VPN

**Procedure:**

A Branch employee X wants to communicate with Y.

- **Stage 1:** X establishes a TCP handshake with the VPN server and send First data packet
  - Second packet send VPN server to the VPN client program running on Y’s laptop
  - Third packet: ack from client to VPN server
  
- **Stage 2:** authentication
  - Client sends encrypted password and username to access VPN Server.However, VPN server CANNOT authenticate.
  - So, VPN server forwards the password to the AAA server (through a separate TCP session)
  - The AAA server checks the password
  - The AAA server sends “YES” message to VPN server;in addition, AAA server will tell the VPN server that X has permission to access the real server.
  - VPN server tells the client through the first TCP session that X is authenticated

### 5.3 Remote-Access VPN Design:

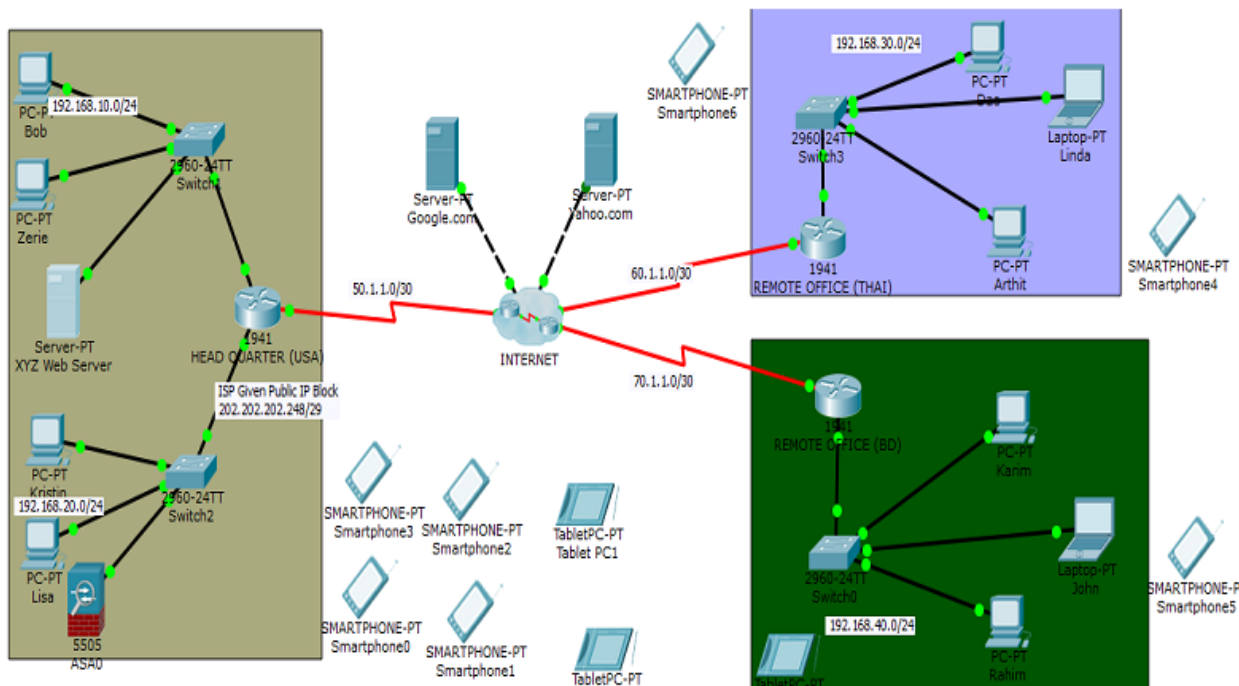


Figure 5.3.1 Remote access VPN design

#### Procedure:

If the organization has branches throughout the world with growing numbers of individuals working remotely, telecommuting or traveling the bank needs to offer network connectivity to their data resources for users, regardless of the user's location. Employees, contractors, or partners may need to access the network when traveling or working from home or from other off-site locations. Then remote-access connectivity should support:

- User authentication—The AnyConnect client requires all remote-access users to authenticate before negotiating a secure connection. Both centralized authentication and local authentication options are supported.
- The remote access VPN is configured to provide different access policies depending on assigned user roles. User can easily access to internet but to enter data server user need to login with password and strong authentication.
- Strong encryption for data privacy—The Advanced Encryption Standard (AES) cipher with a key length of 256 bits is used for encrypting user data. Additional ciphers are also supported.

- The Secure Hash Standard 1 (SHA-1) cryptographic hash function with a 160-bit message digest is used to ensure that data has not been modified during transit.
- The Cisco ASA firewall supports between and the active and standby units of a resilient firewall pair in the event of a hardware failure.

## **CHAPTER 6**

### **CONCLUSION**

A VPN data transmission goes through the public network and anyone eavesdropping the communication can intercept and modify the data. To mitigate this problem, it is important to consider the data integrity algorithm. This encryption algorithm adds a hash to the payload so that to verify the integrity of the original payload. If the transmitted hash matches the received hash, then the data is safe and has not been intercepted. But, if there is no match, then it has been intercepted and modified. Data integrity is verifying the content of the message whether it is misused or tampered during the communication between two peers. Data integrity is making sure that the communication is accurate between both ends

Anti-reply protection checks that each packet is unique and is not replayed. A reply attack is a form of network attack in which a valid VPN traffic is maliciously repeated or delayed. For example, an unwanted user might capture a VPN traffic with the intent to maliciously reply the packet and fake one of the VPN peers that he/she is a legitimate peer. To mitigate such problems, VPNs implement anti-rely protection mechanism



## REFERENCES

- [1]. Leased Line vs VPN - Which Technology Is Right For YOUR Business, Access Date and Time: 10-02-19, <https://www.hso.co.uk/leased-lines/leased-lines/leased-line-vs-vpn>
- [2]. Leased Lines Dedicated lines to your business, Access Date and Time: 10-02-19 <https://caelum-comms.co.uk/leased-lines/>
- [3]. MohdMuntjir, Mohd Rahul, "An Analysis of Internet of Things (IoT): Novel Architectures, Modern Applications, Security Aspects and Future Scope with Latest Case Studies" International Journal of Engineering Research & Technology (IJERT) <http://www.ijert.org> ISSN: 2278-0181 IJERTV6IS060238 (This work is licensed under a Creative Commons Attribution 4.0 International License.) Published by : [www.ijert.org](http://www.ijert.org) Vol. 6 Issue 06, June – 2017
- [4]. About Recommended Partitioning Scheme, Available at: [www.centos.org/docs/5/html/5.2/Installation\\_Guide/s2-diskpartrecommen-ppc.html](http://www.centos.org/docs/5/html/5.2/Installation_Guide/s2-diskpartrecommen-ppc.html), last accessed on 04April 2018, 4.00pm.
- [5]. About internship, Available at: <http://ashleydotson.blogspot.sg/2009/08/in-review-this-internship-has-been.html>, last access on 04April 2018, 10.20am
- [6]. Get Concept about File and directory details, Available at <http://www.bitpapers.com/2012/12/linux-working-with-files.html> last access on 04April 2018, 11.20pm
- [7]. Get Concept about Web server, Available at [http://www.webopedia.com/TERM/W/Web\\_server.html](http://www.webopedia.com/TERM/W/Web_server.html) last access on 04April 2018, 10.30am
- [8]. Get Concept about DNS server, Available at [http://compnetworking.about.com/od/dns\\_domainnamesystem/f/dns\\_servers.htm](http://compnetworking.about.com/od/dns_domainnamesystem/f/dns_servers.htm), last access , On04April 2018, 11:00am
- [9]. Get Concept about Mail Server, [https://www.centos.org/docs/5/html/Deployment\\_Guide-en-US/ch-email.html](https://www.centos.org/docs/5/html/Deployment_Guide-en-US/ch-email.html), last access on 04April 2018, 11:00am
- [10]. Get Concept about MikroTik Router,, <https://en.wikipedia.org/wiki/MikroTik> 04 April 2018, 11:00am
- [11]. Get Concept about RouterOS,, <http://www.revolv.com/main/index.php?s=MikroTik> 04April 2018, 11:00am.
- [12]. Get Concept about Release history, <http://www.revolv.com/main/index.php?s=MikroTik> 04April 2018, 11:00am.
- [13]. Get Concept about Router Board, <https://en.wikipedia.org/wiki/MikroTik> 04April 2018, 11:00am
- [14]. "VPN Installation for remote sites" <http://www.vpnazure.net>.
- [15]. "Performance of Virtual Private" Network <http://www.techrepublic.com>.
- [16]. Eurescom: P1107 – IP Virtual Private Networks, PIR 3.3: Interworking of Security Technologies, February 2002.
- [17]. Venkateswaran, R., "Virtual Private Networks", IEEE Potentials Magazine, February/March 2001.
- [18]. Aboba, B. and G. Zorn, "Implementation of PPTP/L2TP Compulsory Tunneling via RADIUS", April 2000.
- [19]. Microsoft White Paper, "Microsoft Privacy Protected Network Access: <http://www.microsoft.com>
- [20]. Virtual Private Networking and Intranet Security", May 1999.
- [21]. Brown, S., "Implementing Virtual Private Networks", McGraw Hill, 1999.
- [22]. Ferguson & Huston. (1998, April). What is a VPN? Retrieved September 19, 2002, from <http://www.employees.org/~ferguson/vpn.pdf>

## VIRTUAL PRIVATE NETWORK (VPN)

### ORIGINALITY REPORT

<b>29%</b> NDEX	<b>20%</b> INTERNET SOURCES	<b>3%</b> PUBLICATIONS	<b>13%</b> STUDENT PAPERS
--------------------	--------------------------------	---------------------------	------------------------------

### PRIMARY SOURCES

<b>1</b>	<b>www.theseus.fi</b> Internet Source	<b>16%</b>
<b>2</b>	<b>media.proquest.com</b> Internet Source	<b>9%</b>
<b>3</b>	<b>www.masud.net</b> Internet Source	<b>5%</b>
<b>4</b>	<b>www.gpcet.ac.in</b> Internet Source	<b>2%</b>
<b>5</b>	<b>masror.com</b> Internet Source	<b>1%</b>
<b>6</b>	<b>virtualstudysolutions.blogspot.com</b> Internet Source	<b>1%</b>
<b>7</b>	<b>www.ijircce.com</b> Internet Source	<b>1%</b>
<b>8</b>	<b>Submitted to St. Patrick's College</b> Student Paper	<b>1%</b>
<b>9</b>	<b>Submitted to University of Dundee</b> Student Paper	<b>&lt;1%</b>
<b>10</b>	<b>www.it-bari.net</b> Internet Source	<b>&lt;1%</b>
<b>11</b>	<b>Submitted to South University</b> Student Paper	<b>&lt;1%</b>
<b>12</b>	<b>Submitted to London School of Science &amp; Technology</b> Student Paper	<b>&lt;1%</b>

Exclude quotes Off  
Exclude bibliography Off

Exclude matches Off