HND PROJECT

ST PATRICK'S COLLEGE
LONDON

SCHOOL OF TECHNOLOGY

Student Name:

Student ID:

Project Title: Creating a Virtual Private Network Link (VPN) between two Local Area Networks (LAN)

Pathway: HND-Network Engineering and Telecommunications (NETS)

PRE

Acknowledgements

I would like to express my gratitude to my project instructor Mr. Tanveer Ahmad which gave me the golden opportunity to do this wonderful project on the security threats to wireless networks. The professor had helped me in conducting the research work, through which I have acquired so many much knowledge and information. I am really thankful to the professor for giving me this chance.
I would also like to thank my parents and my family who helped me a lot in finalizing this project within the limited time frame. I would like to show appreciation to Mr Alan to Mr Malcolm Thomson, head of Network Technology and his associate team, to all the administration team, to all my teachers. At the end to all my class mates: Toco, Simon, Amici, Mitterand. These people have supported me during my 2 years study of Networking Telecommunication. Because of their support, I have reached some acknowledges concerning IT.

Table of Contents

Chapter 1: Introduction to the project 3

1. Introduction: 3

1.2 Objectives: 4

1.3 Problem description 4

1.4 Solution 6

1.5 Resources 11

1.6 Special Conditions/ Constraints 11

1.7 Proposal 6

Chapter 2: Literature Review 12

2.1 Introduction 12

2.2 Domain Based Literature Review 12

2.3 Technological Based Literature Review 14

3. 1 Introduction: 21

3.2Functional and non-functional requirements 21

3.2.1 Functional requirements 21

3.2.2 Nonfunctional requirements 22

3.2 Discuss the Analysis with Evidence 22

6.1 Brief Description: 27

6.2 Gantt Chart: 27

6.3 Network Security Solution Diagram: .....**Error! Bookmark not defined.**

ABSTRACT

Demand for virtual private networks (VPN) are on the increase as enterprises opt for secure cost effective data networking solutions with specific quality of service (QoS) guarantees. The advantages of the Internet Protocol (IP) have made it the primary network layer protocol of choice for the future as well. Nevertheless, the concept of service differentiation and how to specify and guarantee it in IP VPN are rather difficult and often fuzzy. We propose a class of service (CoS) classification with an associated QoS parameter set for IP virtual private networks in the wide area. We study various scenarios and, in each case, we derive the conditions under which appropriate QoS can be guaranteed for each CoS by policing the aggregate arrival rates of each class from each VPN access interface into the IP network, thereby eliminating the difficulties associated with accurately estimating the end-to-end traffic profiles. In addition to simplifying the specifications, our proposal enables the users to exploit fully the potential of service differentiation in connectionless networks

VPNs have gone from obscurity to being a common method of linking private networks together across the Internet. Although VPNs initially became popular because they free companies from the expense of connecting networks with dedicated leased lines, part of the reason that VPNs have become so accepted is that they tend to be very reliable. Even so, VPN connections do occasionally experience problems. Here are several techniques you can use to troubleshoot VPN connections.

Chapter 1: Introduction to the project

Introduction:

VPNs have gone from obscurity to being a common method of linking private networks together across the Internet. Although VPNs initially became popular because they free companies from the expense of connecting networks with dedicated leased lines, part of the reason that VPNs have become so accepted is that they tend to be very reliable. Even so, VPN connections do occasionally experience problems. Here are several techniques you can use to troubleshoot VPN connections.

As a consultant of B S L C (Badiepa Solution Limited Company) I have been given the task to propose a Point-to-Point link for the company's new office. The office consist of two departments (sales, and IT) located in Manchester.

.1 Aim of project

The aim of this project is to design and develop a remote-access VPN uses a public telecommunication infrastructure like the Internet to provide remote users secure access to their organization's network. A VPN client on the remote user's computer or mobile device connects to a VPN gateway on the organization's network, which typically requires the device to authenticate its identity, then creates a network link back to the device that allows it to reach internal network resources (e.g., file servers, printers, intranets) as though it was on that network locally. A remote-access VPN usually relies on either IPsec or SSL to secure the connection, although SSL VPNs are often focused on supplying secure access to a single application rather than to the whole internal network. Some VPNs provide Layer

2access to the target network; these require a tunneling protocol like PPTP or L2TP running across the base IPsec connection. The successful design and development of such a model will be beneficial to those organization that need to use wireless network for the transfer of data and thus could be commercially implemented.

.2 Objectives:

The objective of this project is to provide iBasis with a scalable, redundant, secure and manageable means for remote users, such as their International sales force, to access corporate resources. This dial-up solution already exists today which is comprised of a Cisco AS5300 utilizing two T-1/PRI circuits and a Cisco Secure Access Control Server (ACS) authentication server. To leverage the accessibility of the Internet and provide a more global access solution, iBasis has expressed the desire to reap the benefits of utilizing a Virtual Private Network (VPN) solution. Implementing a VPN solution provides an alternate means for conventional dial-up connectivity to corporate resources. This will enable remote users to access local Internet Service Provider (ISP's) via xDSL or cable modems to reduce cost and possibly increase throughput. The VPN solution must be able to support their existing client base of fifty users and future growth of 100% each year. IBasis has expressed the desire, in the future, to complement the security of the Cisco Secure authentication server by utilizing token password technology to create dynamic passwords.

Supporting the user community and setting expectations with the remote users is a common challenge for IT departments. To speed adaptation of this new implementation for their users, iBasis also requires development of supporting documentation not only for their IT staff but also for their user community. An interactive Computer Based Training (CBT) and a step-by-step user manual will be created as part of this project. REALTECH also recommends a user feedback process. This critical portion of the project will enable IT to receive immediate user feedback and to use that knowledge to better understand the needs of their user community

1.3 Problem description

There are four types of problems that tend to occur with VPN connections. These include:

- The VPN connection being rejected.
- The acceptance of an unauthorized connection.
- The inability to reach locations that lie beyond the VPN server.
- The inability to establish a tunnel.

- The VPN connection is rejected

having a VPN client's connection rejected is perhaps the most common VPN problem. Part of the reason this problem is so common is that there are a lot of issues that can cause a connection to be rejected. If your VPN server is rejecting client connections, the first thing you need to do is to check to make sure the Routing and Remote Access service is running. You can check this by opening the server's Control Panel and clicking on the Administrative Tools icon, followed by the Services icon. Once you've verified that the necessary services are running, try pinging the VPN server by IP address from the VPN client. You should ping by IP address initially so that you can verify that basic TCP/IP connectivity exists. If the ping is successful, then ping the server again, but this time ping by the server's fully qualified

The problem could also be related to other routing issues. For example, if a user is dealing directly in to the VPN server, it's usually best to configure a static route between the client and the server. You can configure a static route by going to the Dial In tab of the user's properties sheet in Active Directory Users and Computers, and selecting the Apply A Static Route check box. This will cause Windows to display the Static Routes dialog box. Click the Add Route button and then enter the destination IP address and network mask in the space provided. The metric should be left at 1.

If you're using a DHCP server to assign IP addresses to clients, there are a couple of other problems that could cause users not to be able to go beyond the VPN server. One such problem is that of duplicate IP addresses. If the DHCP server assigns the user an IP address that is already in use elsewhere on the network, Windows will detect the conflict and prevent the user from accessing the rest of the network. Another common problem is the user not receiving an address at all. Most of the time, if the DHCP server can't assign the user an IP address, the connection won't make it this far. However, there are situations in which an address assignment fails, so Windows automatically assigns the user an address from the 169.254.x.x range. If the client is assigned an address in this range, but this address range isn't present in the system's routing tables, the user will be unable to navigate the network beyond the VPN server.

Difficulty establishing a tunnel

if everything seems to be working well, but you can't seem to establish a tunnel between the client and the server, there are two main possibilities of what could be causing the problem. The first possibility is that one or more of the routers involved is performing IP packet filtering. IP packet filtering could prevent IP tunnel traffic. I recommend checking the client, the server, and any machines in between for IP packet filters. You can do this by clicking the advanced button on each machine's TCP/IP Properties

sheet, selecting the Options tab from the Advanced TCP/IP Settings Properties sheet, selecting TCP/IP Filtering, and clicking the Properties button.

The other possibility is that a proxy server is standing between the client and the VPN server. A proxy server performs NAT translation on all traffic flowing between the client and the Internet. This means that packets appear to be coming from the proxy server rather than from the client itself. In some cases, this interaction could prevent a tunnel from being established, especially if the VPN server is expecting the client to have a specific IP address. You must also keep in mind that a lot of older or low-end proxy servers (or NAT firewalls) don't support the L2TP, IPSec, or PPTP protocols that are often used for VPN connections.

This project aims at designing such a model which would be able to provide higher levels of security to Virtual Private Networks.

1.4 Proposal

Through this project, I aim to create and develop a Virtual Private Network model that will increase the defense of Virtual Private Networks of Badiepa Solution Limited Company against various threats and attacks to their data.

1.5 Solution

Virtual Private Networks (VPNs) extends a protected network and resources to remote users over a public network such as the Internet. Careful consideration and planning is required to select the appropriate technology and components that will provide a balance of security and usability. The following sections summarize information from the Rapid Assessment and related research as well as the resulting recommendation for the solution.

The design for the iBasis' VPN Solution is based on determining the following:

- Identifying VPN technology that will best fit the requirements stated above
- Determining the necessary network elements needed to implement the solution
- Placement of the network elements to ensure security and full functionality

1.6 Design Overview

During the discovery process I have identified the following requirements:

- The solution is based on the Cisco product line to complement Badiepa Solution Limited Company of being a Cisco Powered Network
- Access must be achieved using VPN technology
- The solution utilizes the existing network elements and related software
- The traveling sales force and remote users are located worldwide
- User authentication is required to increase security in case of theft of the actual VPN client equipment
- Access to internal defined resources
- The solution must be manageable and minimize support requirements

The design includes utilizing the existing Cisco 7120-4T1 VPN router and the addition of an Integrated Service Module (ISM) to handle VPN processes which also provides a complimentary, unrestricted license for the Cisco VPN Client software.

After further discussions with iBasis, it has been decided that the 7120 specifications of 50+ Mbps throughput and 175 Kpps (with ISM, 90 Mbps throughput and 2000 simultaneous users) is sufficient for their current. Even though the 7140 provide a higher throughput and redundant power supply, the time it would take to receive the new router is unacceptable to iBasis. The time of completion of the VPN solution is a key factor as iBasis has many employees overseas with the immediate need for an alternative method to accessing corporate resources. Currently, iBasis is incurring the costs of International users dialing into the AS5300 access server.

1.6 VPN Technologies Summary

The technologies associated with VPN solutions include tunneling protocols, encryption standards and authentication methods.

1.6.1Tunnelling

Tunneling protocols are used to encapsulate either layer 2 or layer 3 protocols into another protocol to be transported over a network like the Internet. The virtual communication path that is developed using this protocol are referred to as “tunnels”. Using this technology, a company does not require the use of private leased lines for Wide Area communication, but instead create “tunnels” across public networks. Common tunneling protocols include the Internet Protocol Security (IPSec), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) and Layer 2 Forwarding (L2F).

1.6.2 Encryption

Cryptography, from the word “kryptos” meaning hidden, uses encryption algorithms to provide information security. The process of encrypting, converting data into a unreadable form, or decrypting, which is the opposite process, is called a “cipher”. Encryption methods include the Data Encryption Standard (DES), RC4, International Data Encryption Algorithm (IDEA) and Blowfish.

Encryption uses algorithms that are based upon keys to encrypt and decrypt information. Key algorithms can either be public-key (asymmetric) or secret-key (symmetric). Public-key algorithms use a different key for encryption and decryption whereas secret-key algorithms use the same key for encryption and decryption. Public-key algorithms or ciphers use a public key to encrypt data. This key can be known to anyone. The decryption of information requires a different key, the private or secret key. Only if the private or secret key is known can a user decrypt information created from the public key? Secret-key algorithms have the ability to encrypt a single bit of plain text at time (stream cipher) or can encrypt a number of bits of plain text at a time (block cipher). Examples of secret-key encryption algorithms are DES, Blowfish, IDEA and RC4

1.6.3 Authentication

Authentication is a method to challenge the device or person wanting access to resources. The most common and least secure authentication method utilizes a user name and password that will be required before allowing access. Internet businesses that require a more stringent authentication process can make use of digital certificates issued and verified by a Certificate Authority (CA).
Certificate Authorities (CA) revolves around the premise of issuing digital certificates to verify the identity of two parties and they are in fact whom they claim to be. This provides for the authenticity and data integrity of the information communicated. Digital certificates are primarily used when implementing public-key cryptography. Utilizing a public-key algorithm generates a key-pair, one is private and the other is public. The public key, only used for encryption, is passed within a digital certificate to persons wishing to communicate with the person holding the other half of the key-pair, the private key.

1.7 VPN Technology Comparison and Analysis

1.7.1 Tunneling

Point-to-Point Tunneling Protocol (PPTP), an extension of the Point-to-Point Protocol (PPP), encapsulates the local traffic into PPP and then into Generic Routing Encapsulation (GRE) packets to be sent through an IP network. Microsoft has an implementation of PPTP that uses Challenge-Handshake Authentication Protocol (MS-CHAPv1) for authentication and Microsoft's Point-to-Point Encryption (MPPE) for encryption (40/128-bit RC4). Microsoft's PPTP implementation lacked maturity in the areas of authentication and encryption. Instead of using a strong key-exchange algorithm like Diffie-Hellman or Internet Key Exchange (IKE), user passwords were used for keys in hash algorithms. The weaknesses of MS-CHAPv1 supposedly are fixed with MS-CHAPv2 which is available in version 1.3 of Dial-Up Networking (DUN).

Layer 2 Tunneling Protocol (L2TP) is another tunneling protocol, which tunnels PPP traffic. L2TP combines the features found in Layer 2 Forwarding (L2F) and PPTP. Authentication methods include CHAP, PAP (Password Authentication Protocol) and MS-CHAP.

IPSec is not a tunneling protocol but does provide for data confidentiality, integrity, and authentication of transmitted data. Tunneling protocols are used between two communication endpoints by encapsulating or hiding one protocol into another. Making the original protocol unnoticeable during transmission. IPSec performs the same function by encrypting the original information and making it undecipherable during transmission. Authentication methods ensure only the communication endpoints will be able to decrypt this information.

1.7.2 Encryption Methods

- Given time and resources, encryption algorithms are possible to decipher. The main objective is to make the process as difficult as possible.
- Data Encryption Standard (DES) is a block cipher that uses a 64-bit block size. This means that information can be encrypted in blocks of 64-bits.
- Triple-DES (3DES) is an extension of regular DES but uses a 128-bit public-key.
- Blowfish is a block cipher which uses a 64-bit block size but can also use variable length keys up to 448-bits.
- International Data Encryption Algorithm (IDEA) is a block cipher using a 128-bit key.
- RC4, a stream cipher that uses a variable–bit key (40/128).
- Microsoft's Point-to-Point Encryption (MPPE) and Cisco Encryption Technology (CET) are both encryption solutions, however they lack some key features necessary to fulfill iBasis requirements

1.7.3 Advantages and Disadvantages of VPN

A VPN is an inexpensive effective way of building a private network. The use of the Internet as the main communications channel between sites is a cost effective alternative to expensive leased private lines. The costs to a corporation include the network authentication hardware and software used to authenticate users and any additional mechanisms such as authentication tokens or other secure devices. The relative ease, speed, and flexibility of VPN provisioning in comparison to leased lines makes VPNs an ideal choice for corporations who require flexibility. For example, a company can adjust the number of sites in the VPN according to changing requirements.

There are several potential disadvantages with VPN use. The lack of Quality of Service (QoS) management over the Internet can cause packet loss and other performance issues. Adverse network conditions that occur outside of the private network is beyond the control of the VPN administrator. For this reason, many large corporations pay for the use of trusted VPNs that use a private network to guarantee QoS. Vendor interoperability is another potential disadvantage as VPN technologies from one vendor may not be compatible with VPN technologies from another vendor. Neither of these disadvantages have prevented the widespread acceptance and deployment of VPN technology

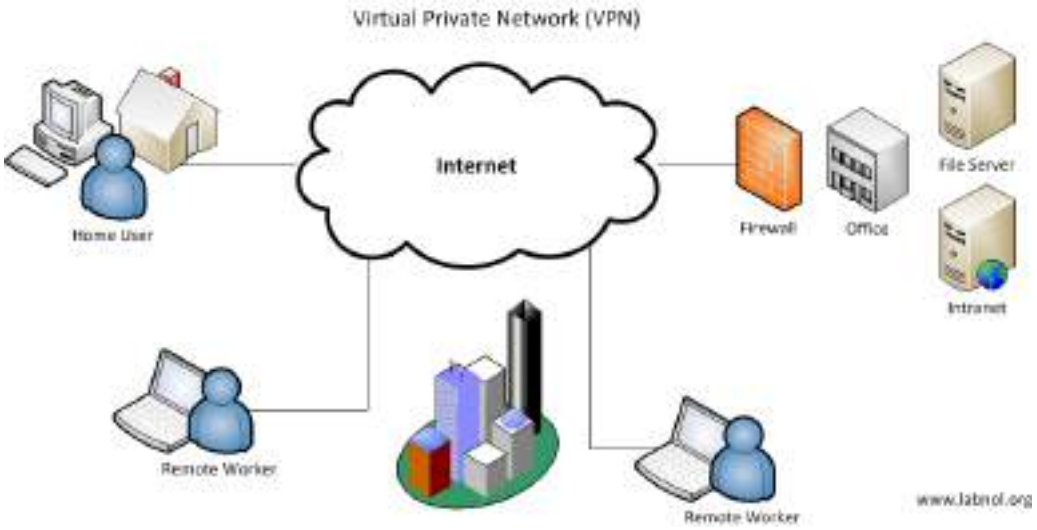
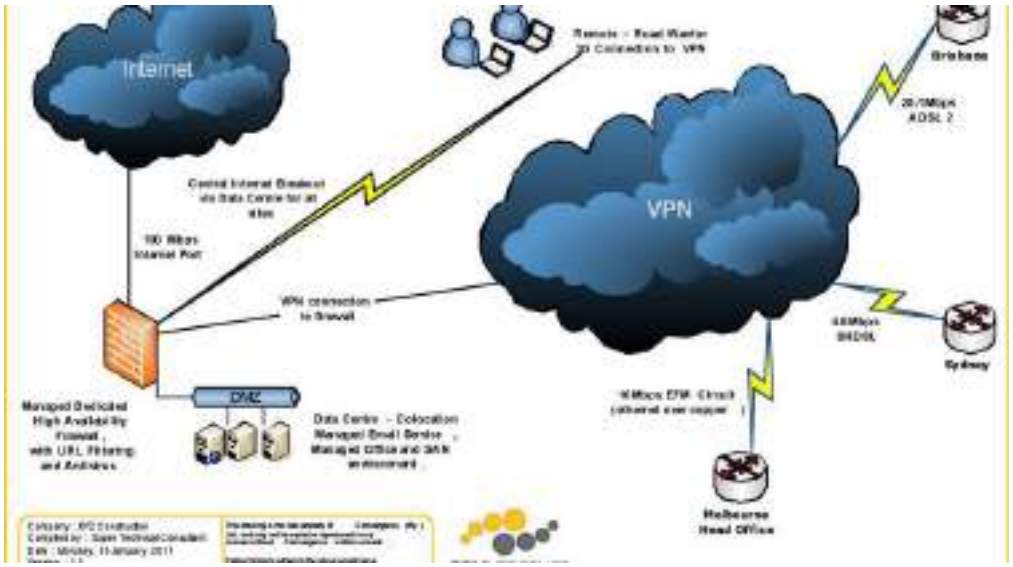


Figure: Virtual Private Network: Posted on June 29, 2014 by **Motiur Rahman**

The full meaning of VPN is virtual private network, which is used for security and privacy of personal computer, laptop etc. during internet use. Generally this VPN is use by internet user to change their ip or getting private browsing.



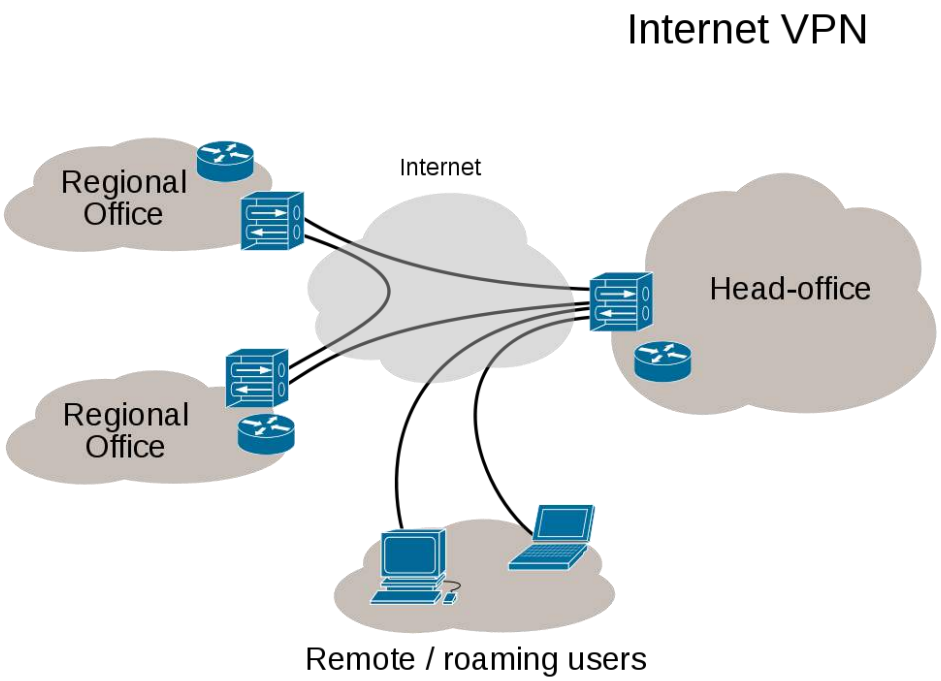
1.8 Resources

The following resources are rewired for the development of the model:

I. Secured wireless access points
II. Application gateways
III. Control servers
IV. Application servers
V. Authentication servers

1.9 Special Conditions/ Constraints

Security mechanisms:



VPNs cannot make online connections completely anonymous, but they can usually increase privacy and security. To prevent disclosure of private information, VPNs typically allow only authenticated remote access and make use of encryption techniques.

VPNs provide security by the use of tunneling protocols and often through procedures such as encryption. The VPN security model provides:

- Confidentiality such that even if the network traffic is sniffed at the packet level (see network sniffer and Deep packet inspection), an attacker would only see encrypted data
- Sender authentication to prevent unauthorized users from accessing the VPN
- Message integrity to detect any instances of tampering with transmitted messages

Secure VPN protocols include the following:

- Internet Protocol Security (IPsec) as initially developed by the Internet Engineering Task Force (IETF) for IPv6, which was required in all standards-compliant implementations of IPv6 before RFC 6434 made it only a recommendation. This standards-based security protocol is also widely used with IPv4 and the Layer 2 Tunneling Protocol. Its design meets most security goals: authentication, integrity, and confidentiality. IPsec uses encryption, encapsulating an IP packet inside an IPsec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.

Transport Layer Security (SSL/TLS) can tunnel an entire network's traffic (as it does in the Open VPN project and Soft Ether VPN project) or secure an individual connection. A number of vendors provide remote-access VPN capabilities through SSL. An SSL VPN can connect from locations where IPsec runs into trouble with Network Address Translation and firewall rules.

Chapter 2: Literature Review

2.1 Introduction

A large number of existing literary articles were reviewed so as to conduct a background study in the domain being reviewed. The existing models and methods that are currently being used to ensure the security of the Virtual Private networks have been studied in details so as to understand the ground level technology which is being used (Bera, Ghosh and Dasgupta, 2010). The details of all such background studies have been mentioned in the following section.

2.2 Domain Based Literature Review

- **Datagram Transport Layer Security (DTLS) – used in Cisco AnyConnect VPN and in Open Connect VPN to solve the issues SSL/TLS has with tunneling over UDP.**

- Microsoft Point-to-Point Encryption (MPPE) works with the Point-to-Point Tunneling Protocol and in several compatible implementations on other platforms.
- Microsoft Secure Socket Tunneling Protocol (SSTP) tunnels Point-to-Point Protocol (PPP) or Layer 2 Tunneling Protocol traffic through an SSL 3.0 channel. (SSTP was introduced in Windows Server 2008 and in Windows Vista Service Pack 1.)
- Multi Path Virtual Private Network (MPVPN). Regular Systems Development Company owns the registered trademark "MPVPN".
- Secure Shell (SSH) VPN – Open SSH offers VPN tunneling (distinct from port forwarding) to secure remote connections to a network or to inter-network links. Open SSH server provides a limited number of concurrent tunnels. The VPN feature itself does not support personal authentication.

1. Authentication

Tunnel endpoints must be authenticated before secure VPN tunnels can be established. User-created remote-access VPNs may use passwords, biometrics, two-factor authentication or other cryptographic methods. Network-to- tunnels often use passwords or digital certificates. They permanently store the key to allow the tunnel to establish automatically, without intervention from the user.

2. Routing:

Tunneling protocols can operate in a point-to-point network topology that would theoretically not be considered a VPN, because a VPN by definition is expected to support arbitrary and changing sets of network nodes. But since most router implementations support a software-defined tunnel interface, customer-provisioned VPNs often are simply defined tunnels running conventional routing protocols.

3. Provider-provisioned VPN building-blocks

Depending on whether a provider-provisioned VPN (PPVPN) operates in layer 2 or layer 3, the building blocks described below may be L2 only, L3 only, or combine them both. Multiprotocol label switching (MPLS) functionality blurs the L2-L3 identity.

RFC 4026 generalized the following terms to cover L2 and L3 VPNs, but they were introduced in RFC 2547. More information on the devices below can also be found in Lewis, Cisco Press.

Customer (C) devices
A device that is within a customer's network and not directly connected to the service provider's network. C devices are not aware of the VPN.

4. Customer Edge device (CE)
A device at the edge of the customer's network which provides access to the PPVPN. Sometimes it's just a demarcation point between provider and customer responsibility. Other providers allow customers to configure it.

Provider edge device (PE)
A PE is a device, or set of devices, at the edge of the provider network which connects to customer networks through CE devices and presents the provider's view of the customer site. PEs are aware of the VPNs that connect through them, and maintain VPN state.

Provider device (P)
A P device operates inside the provider's core network and does not directly interface to any customer endpoint. It might, for example, provide routing for many provider-operated tunnels that belong to different customers' PPVPNs. While the P device is a key part of implementing PPVPNs, it is not itself VPN-aware and does not maintain VPN state. Its principal role is allowing the service provider to scale its PPVPN offerings, for example, by acting as an aggregation point for multiple PEs. P-to-P connections, in such a role, often are high-capacity optical links between major locations of providers.

5. User-visible PPVPN service
This section deals with the types of VPN considered in the IETF.

OSI Layer 2 services

Virtual LAN
A Layer 2 technique that allow for the coexistence of multiple LAN broadcast domains, interconnected via trunks using the IEEE 802.1Q trucking protocol. Other trucking protocols have been used but have become obsolete, including Inter-Switch Link (ISL), IEEE 802.10 (originally a security protocol but a subset was introduced for trucking), and ATM LAN Emulation (LANE).

Virtual private LAN service (VPLS)
Developed by IEEE, VLANs allow multiple tagged LANs to share common trunking. VLANs frequently comprise only customer-owned facilities. Whereas VPLS as described in the above section (OSI Layer 1 services) supports emulation of both point-to-point and point-to-multipoint topologies, the method discussed here extends Layer 2 technologies such as 802.1d and 802.1q LAN trunking to run over transports such as Metro Ethernet.

2.3 Technological Based Literature Review

As used in this context, a VPLS is a Layer 2 PPVPN, rather than a private line, emulating the full functionality of a traditional local area network (LAN). From a user standpoint, a VPLS makes it possible to interconnect several LAN segments over a packet-switched, or optical, provider core; a core transparent to the user, making the remote LAN segments behave as one single LAN.

In a VPLS, the provider network emulates a learning bridge, which optionally may include VLAN service.

Pseudo wire (PW)
PW is similar to VPLS, but it can provide different L2 protocols at both ends. Typically, its interface is a WAN protocol such as Asynchronous Transfer Mode or Frame Relay. In contrast, when aiming to provide the appearance of a LAN contiguous between two or more locations, the Virtual Private LAN service or IPLS would be appropriate.

Ethernet over IP tunneling
Ether IP (RFC 3378) is an Ethernet over IP tunneling protocol specification. EtherIP has only packet encapsulation mechanism. It has no confidentiality nor message integrity protection. Ether IP was introduced in the FreeBSD network stack and the Soft Ether VPN server program.

IP-only LAN-like service (IPLS)
A subset of VPLS, the CE devices must have L3 capabilities; the IPLS presents packets rather than frames. It may support IPv4 or IPv6.

OSI Layer 3 PPVPN architectures

This section discusses the main architectures for PPVPNs, one where the PE disambiguates duplicate addresses in a single routing instance, and the other, virtual router, in which the PE contains a virtual router instance per VPN. The former approach, and its variants, have gained the most attention.

One of the challenges of PPVPNs involves different customers using the same address space, especially the IPv4 private address space. The provider must be able to disambiguate overlapping addresses in the multiple customers' PPVPNs**.**

Signal-Hiding Techniques**:**

.**BGP/MPLS PPVPN**

In the method defined by RFC 2547, BGP extensions advertise routes in the IPv4 VPN address family, which are of the form of 12-byte strings, beginning with an 8-byte Route Distinguisher (RD) and ending with a 4-byte IPv4 address. RDs disambiguate otherwise duplicate addresses in the same PE.

PEs understand the topology of each VPN, which are interconnected with MPLS tunnels, either directly or via P routers. In MPLS terminology, the P routers are Label Switch Routers without awareness of VPNs.

Virtual router PPVPN

The Virtual Router architecture, as opposed to BGP/MPLS techniques, requires no modification to existing routing protocols such as BGP. By the provisioning of logically independent routing domains, the customer operating a VPN is completely responsible for the address space. In the various MPLS tunnels, the different PPVPNs are disambiguated by their label, but do not need routing distinguishers.

Unencrypted Tunnels:

Some virtual networks may not use encryption to protect the privacy of data. While VPNs often provide security, an unencrypted overlay network does not neatly fit within the secure or trusted categorization. For example, a tunnel set up between two hosts that used Generic Routing Encapsulation (GRE) would in fact be a virtual private network, but neither secure nor trusted.

Native plaintext tunneling protocols include Layer 2 Tunneling Protocol (L2TP) when it is set up without IPsec and Point-to-Point Tunneling Protocol (PPTP) or Microsoft Point-to-Point Encryption (MPPE).

Trusted delivery networks

Trusted VPNs do not use cryptographic tunnelling, and instead rely on the security of a single provider's network to protect the traffic.

- Multi-Protocol Label Switching (MPLS) often overlays VPNs, often with quality-of-service control over a trusted delivery network.
- Layer 2 Tunneling Protocol (L2TP) which is a standards-based replacement, and a compromise taking the good features from each, for two proprietary VPN protocols: Cisco's Layer 2 Forwarding (L2F) (obsolete as of 2009) and Microsoft's Point-to-Point Tunneling Protocol (PPTP).

From the security standpoint, VPNs either trust the underlying delivery network, or must enforce security with mechanisms in the VPN itself. Unless the trusted delivery network runs among physically secure sites only, both trusted and secure models need an authentication mechanism for users to gain access to the VPN.

VPNs in mobile environments

Mobile VPNs are used in a setting where an endpoint of the VPN is not fixed to a single IP address, but instead roams across various networks such as data networks from cellular carriers or between multiple Wi-Fi access points. Mobile VPNs have been widely used in public safety, where they give law enforcement officers access to mission-critical applications, such as computer-assisted dispatch and

criminal databases, while they travel between different subnets of a mobile network. They are also used in field service management and by healthcare organizations, among other industries.

Increasingly, mobile VPNs are being adopted by mobile professionals who need reliable connections. They are used for roaming seamlessly across networks and in and out of wireless coverage areas without losing application sessions or dropping the secure VPN session. A conventional VPN cannot survive such events because the network tunnel is disrupted, causing applications to disconnect, time out, or fail, or even cause the computing device itself to crash.

Instead of logically tying the endpoint of the network tunnel to the physical IP address, each tunnel is bound to a permanently associated IP address at the device. The mobile VPN software handles the necessary network authentication and maintains the network sessions in a manner transparent to the application and the user. The Host Identity Protocol (HIP), under study by the Internet Engineering Task Force, is designed to support mobility of hosts by separating the role of IP addresses for host identification from their locator functionality in an IP network. With HIP a mobile host maintains its logical connections established via the host identity identifier while associating with different IP addresses when roaming between access networks.

VPN on Routers

With the increasing use of VPNs, many have started deploying VPN connectivity on routers for additional security and encryption of data transmission by using various cryptographic techniques. Setting up VPN services on a router will allow any connected device(s) to use the VPN network while it is enabled. This also makes it easy to set up VPNs on devices that do not have native VPN clients such as Smart-TVs, Gaming Consoles etc. Provisioning VPN on the routers will also help in cost savings and network scalability.

Many router manufacturers like Cisco Linksys, Asus and Netgear supply their routers with built-in VPN clients. Since these routers do not support all the major VPN protocols, such as Open VPN, many tend to flash their routers with alternative open source firmware such as DD-WRT, Open WRT and Tomato which support multiple VPN protocols such as PPTP and Open VPN.

Limitations:

Not every router compatible with open source firmware which depends on the built-in flash memory and processor. Firmware like DD-WRT require a minimum of 2 MiB flash memory and Broadcom chipsets. Setting up VPN services on a router requires a deeper knowledge of network security and careful installation. Minor misconfiguration of VPN connections can leave the network vulnerable. Performance will vary depending on the ISP and their reliability.

Networking limitations

one major limitation of traditional VPNs is that they are point-to-point, and do not tend to support or connect broadcast domains. Therefore communication, software, and networking, which are based on layer 2 and broadcast packets, such as NetBIOS used in Windows networking, may not be fully supported or work exactly as they would on a real LAN. Variants on VPN, such as Virtual Private LAN Service (VPLS), and layer 2 tunneling protocols, are designed to overcome this limitation.

A VPN, as its name suggests, is just a virtual version of a secure, physical network—a web of computers linked together to share files and other resources. But VPNs connect to the outside world over the Internet, and they can serve to secure general Internet traffic in addition to corporate assets

Implementation Star Methodology:

The following section describes the Virtual Private Network's Implementation Methodology that will facilitate tracking of milestones for this project, the ease of timeline creation and simplification to implementation procedures

Star Topology Diagram

In Star topology, all the components of network are connected to the central device named "hub". Which may be a hub, a router or a switch. In the Star Topology all the workstations are linked to central device with a point-to-point connection. So every computer is indirectly related to every other node by the help of "hub".
All the data on the Star Topology passes done the central device before reaching the planned destination. Hub performs a connexion to connect different nodes present in Star Network, and at the same time it accomplishes and controls whole of the network. Depending on which central device is used, "hub" can act as repeater or signal booster. Central device can also communicate with other hubs of different network. Unshielded Twisted Pair (UTP) Ethernet cable is used to connect workstations to central node.

- **Advantages of Star Topology:**

Star Topology gives better performance if you compare it to Bus Topology. Signals don't necessarily

get transmitted to all the workstations. A sent signal can reach the envisioned destination after passing through no more than 3-4 devices and 2-3 links. Performance of the network is reliant on the volume of central hub.

- Not difficult to connect new nodes or devices. In Star Topology new nodes can be added easily without affecting rest of the network. Likewise components can also be removed easily.

- Centralized management. It helps in monitoring the network. Let-down of one node or link doesn't affect the rest of network. At the same time, it's easy to detect the failure and troubleshoot it.

- **Disadvantages of Star Topology:**

There is too much dependence on central device has its own drawbacks. If it fails whole network goes down.

- The importance of using of hub, a router or a switch as central device rises the general cost of the network.

- Performance and as well number of nodes which can be added in such topology is depended on capacity of central device.

Pre-Implementation

The steps within this stage will follow immediately after the delivery and acceptance of this Scope of Work.

Procurement of the necessary hardware and software are based on the recommended solution list found in Recommended VPN Network Elements and Software. Ancillary materials such as cables and hubs are listed as part of iBasis' responsibilities.

The recommended solution uses 168-bit encryption in the Cisco 7120 router, registration for higher encryption IOS software must be done during the software purchasing process.

Plan development and acceptance

I will provide Badiepa Solution Limited Company with two deliverables to ensure the recommended solution will be thoroughly tested and customized to iBasis needs. The deliverables are as follows:

Test Plan

I will be developing a test plan to verify the functionality of the proposed VPN solution. iBasis will review and validate the test plan to address possible issues that were not foreseen by REALTECH. A VPN test plan is comprised of network system tests and user system testing. The test plan includes the following:

- IP connectivity from network systems to user systems
- VPN client connectivity to VPN router
- VPN authentication functions
- VPN users' system ability to browse Network Neighborhood
- VPN client NT domain login
- VPN session termination on timeout

User feedback plan

Badiepa Solution Limited Company's staff will identify six test users who will use the VPN solution. The six test users should be selected to ensure a complete test of this solution. After the six test users install and configured the VPN Client software, they will be asked to fill out a feedback questionnaire. The feedback questionnaire and the collection and distribution method will be developed in conjunction with BSLC to maximize the effectiveness of this process.

Sample system configuration

During the Implementation stage, sample system configurations and preparations will be made on the following network elements:

Cisco Catalyst 6509

Reserve a switch port on both internal and external VLANs in the Catalyst 6509 for the placement of the Cisco 7100 router. The port assignments are to be made by iBasis IT staff. These ports are then manually configured for setting of 100Mb full duplex with port fast enable.

Cisco 7120 Router

Configure both external and internal Fast Ethernet interfaces on the router with an IP addresses (assigned by iBasis) and descriptions of the interfaces. The router is then configured for client initiated VPN access. This includes the creation of the internal VPN IP address pool, the ISAKMP transform map, the IPSec encryption algorithm and the client dynamic map with extended authentication. The IP network address range is to be provided by iBasis IT staff and should be an entire class C network. X-auth uses TACACS+ to authenticate users wanting access. These TACACS+ authentication requests will be processed by a Cisco Secure Server, which will perform a search through the NT domain SAM databases for request validation. Routing for the internal interfaces will be handled by OSPF that directs

the VPN traffic through the internal network. Routing for the external interface will be performed by a static route, which will be pointing to the HSRP address of the external routers.

Cisco VPN Client 1.1 security policy

REALTECH will generate a VPN client security policy from a pre-installed VPN Security Policy Editor. This security policy will serve as a standard policy for all VPN clients. The security policy editor will be configured as follows:

- Add new connection policy
- Configure Secure Gateway Address
- Configure client's identity
- Setup pre-share key
- Configure authentication proposal
- Configure key exchange proposal
- Configure SA lifetimes to allow for session timeout
- Configure encryption and authentication methods

After configuration, the VPN policy will be saved to a file and the file will be transferred and loaded into other VPN clients.

Review drafts and 'sign off'

This is the final stage of the documentation process before distributing it to the test users. iBasis will review the document and provide comments/feedback to REALTECH. After considering the comments and implementing any changes, the document will be distributed to the test users during the implementation stage of the project. Their comments and feedback will be incorporated into the user manual. After final changes to the documentation has been made, REALTECH and iBasis will 'sign-off' on the document and have it ready for distribution.

Creation of CBT:

A CBT will be created to provide IT users with VPN client training. The organization's Training Department, with the input of Badiepa Solution Limited Company engineers, will work closely with IT to customize the CBT. After the user manual is created, BSLC's Training Department will create a project plan based on the resources needed to complete this task.

In order to develop the security model, a prototype methodology has been chosen. Using this methodology, a working prototype of the model is designed so as to check the functional efficiency of the design, before the actual system is build. The prototypes undergo various changes in different stages of the development, and the finalized designed is implemented as a working system.

During the prototype is built, the following activities are performed:

i. Requirement Gathering
ii. Feasibility Study
iii. System Analysis
iv. Software Design
v. Coding and Testing
vi. Integration and Implementation

Chapter 3. Analysis and design:

3. 1 Introduction:

Analysis and Design is considered as one of the most important part of conducting a technical project, as the ideas that are generated from the exhaustive survey of the existing literary works are found to be of immense help while developing the designs of a model that could serve the purpose of the project. In this project, the wide range of literary works that have been reviewed have been influential in the process of designing the VPN models that could reduce the vulnerabilities of the wireless networks to various threats and security attacks that are constantly being made by intruders. Needless to say the implementation of such a model would be helpful in hindering thee malicious activities attempted by the intruders (Wan and Alagar, 2014).

The system which has been designed so as to reduce the vulnerabilities of wireless network systems has been discussed in the following sections.

3.2 Functional and non-functional requirements

3.2.1 Functional requirements

The functional requirements of the system that is being designed so as to reduce the vulnerabilities of a wireless network towards the various threats and attacks have been discussed in the following section:

1. Performance management: the system being designed should be able to monitor the performance of the system (Wang, Guo and Zhan, 2010).

2. Configuration Management: the designed system should be able to perform configuration management of the network.

3. Management of the accounts or the usage of the network.

3.2.2 Nonfunctional requirements

The nonfunctional requirements of the system have been discussed in the following section:

1. Fault management: The system being designed should be able to detect the various issues or problems that the wireless network experiences. The designed system should also be able to fix such defects and prepare reports of such incidents, besides maintaining logs for each of the defects that have been detected (West phall and Mueller, 2010).

2. Security Management: is yet another nonfunctional requirement for the system being designed. The system administrator should be able to make changes to the security settings of the system such that the resources of the network function according to the security guidelines implemented by the business organizations (Williams, 2012).

3. The system being designed should be able to provide the users with the authority to access the various nodes if the system.

4. The security manages should be able to identify those resources which are crucial to the proper functioning of the wireless network using the designed system. The determination of the resources which are essential for the system would help the managers to assign the accessibility of the users to these resources (Zhang and Chen, 2012).

3.2 Discuss the Analysis with Evidence

Considering the various functional requirements and the non-functional requirements of the system to be developed, various security models have been designed which essentially meet the requirements (Zhang and Chen, 2012).

Managing the performance of the various access nodes so as to ensure the security of the entire wireless network is one of the core functionalities that has to be provide by such models. The activities related to the performance monitoring of the network include the measurement of the normal levels of data requests or access requirements being requested by the users of the network. Monitoring the effective user response times or the measurement of line utilization helps in the detection of abnormal wireless behavior (Zic et al. 2012).

Configuration management functionality is associated with the maintenance of the network inventory and the proper configuration of the wireless network system. The information being saved by this

process would be helpful in the detection of the various problems that might arise due to the issue in interoperability of the systems (Aksu et al. 2012).

The management of the accounts in order to measure the amount of data or information which is being used by the users of the system and the total billable amount for such purposes is yet another functional requirement for the system being designed. The proper management of the accounts ensures the fact that all the resources of the network are functioning to their fullest capacity and no rouge access point is operating within the secured network (Araujo *et al.* 2012).

Thus, according to the findings reported by experts conducting researches in this domain, any network security system must incorporate the above mentioned functionalities.

While conducting the literature review, we came accords certain materials which indicated that cloud services could also be used so as to secure the wireless networks. Thus, it has been decided that the storage of data generated by the business organization, controlling the access to the data and keeping the backup of data would be performed using Cloud based services, SAS services to be more specific.

Design of the project

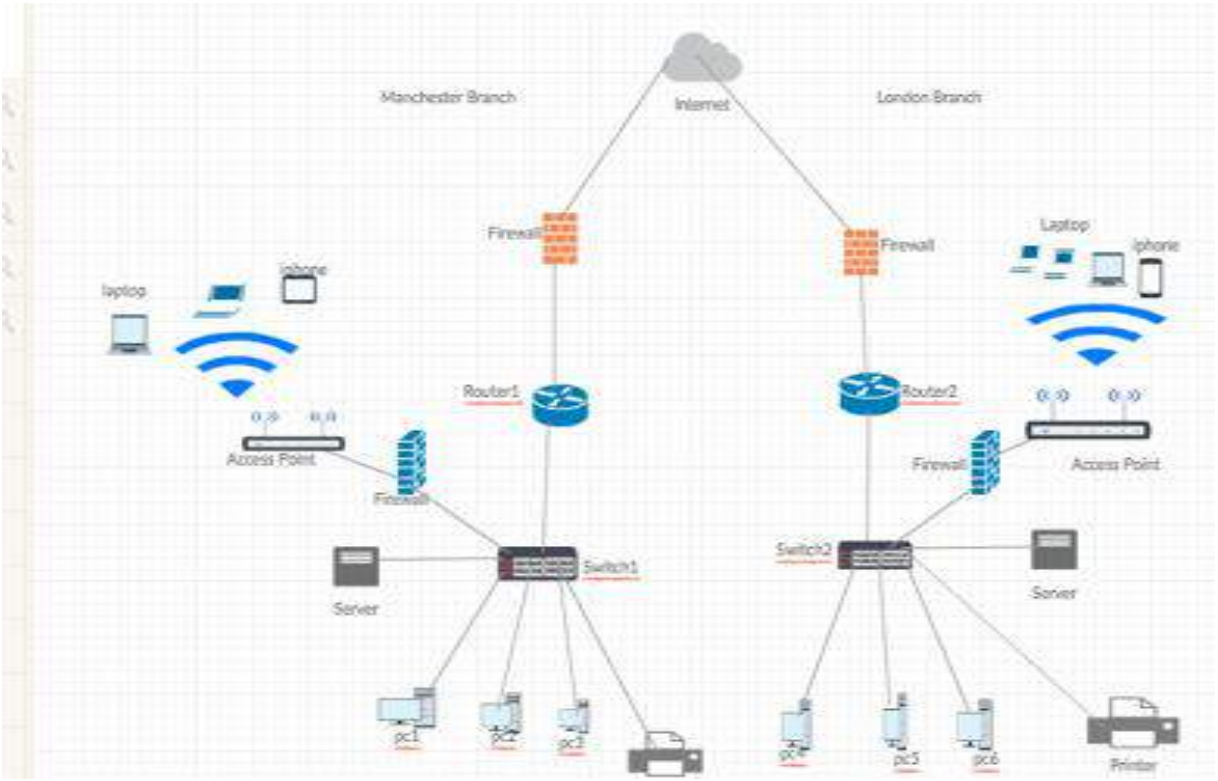


Figure: Network diagram

The network security model that will be used to provide security to the Virtual Private networks has been depicted in the above figure. As depicted, the applications servers would not have the access to any sensitive data, thus providing security against hacking. The entire network is protected by a fire wall that would limit the access of the outsiders to the data being stored and transported across the network. The access points will be secured by double authentication to as to ensure that only legitimate users are able to gain access to the network.

Chapter 4. Development and implementation

Stage II is the implementation. This stage incorporates the installation and configuration of the equipment in addition to the distribution of the client software to the six test users. After the equipment configuration, testing will be conducted according to the test plan developed in Stage I. The questionnaires will be collected after the testing for review. By the end of this stage, both the user manual and CBT will be completed and ready for distribution.

Hardware configuration

The necessary hardware will be installed onto the production network with minimal impact to iBasis' network. This includes the mounting of the Cisco equipment, inserting the new ISM module and connecting the router on the external and internal Fast Ethernet networks (parallel to the existing PIX firewall).

System configuration

All systems will be configured according to the sample configuration document from the Pre-implementation. The following are the systems that need to be configured:

- Cisco Catalyst 6509
- Cisco 7120 Router
- Cisco Secure Server
- User laptop configurations

Testing

A test of the client initiated VPN solution will be performed according to the test plan developed during the Pre-implementation. The test will be performed in the presence of a BSLC' staff for validation. The I will check off the validity of the test as it is done. A signature will be obtained from the iBasis test personnel after all tests in the test plan have been passed.

Post-documentation

I will submit documentation to iBasis upon completion of this project. I will receive two hard copies that contain the following:

- ❖ Summary of project goals and work performed
- ❖ Logical diagram(s) of the VPN network solution
- ❖ Inventory of installed hardware components including serial, part numbers and warranty contracts
- ❖ Hard and soft copies of the modified switch and router configurations
- ❖ Snapshots and descriptions of VPN client configurations
- ❖ Descriptions of modified server configurations
- ❖ Descriptions of laptop configurations
- ❖ Customer concurrence testing checklist and sign-off

Implement rollout support

Badiepa Solution Limited Company's engineering staff remains on-site monitoring network performance and responding to any issues raised by BSLC's staff. In general, standard post-rollout support includes a BSLC engineer to be on-site for at least 2 days (4 hours each day) after rollout and will be responsible for resolving network connectivity issues and escalating problems.

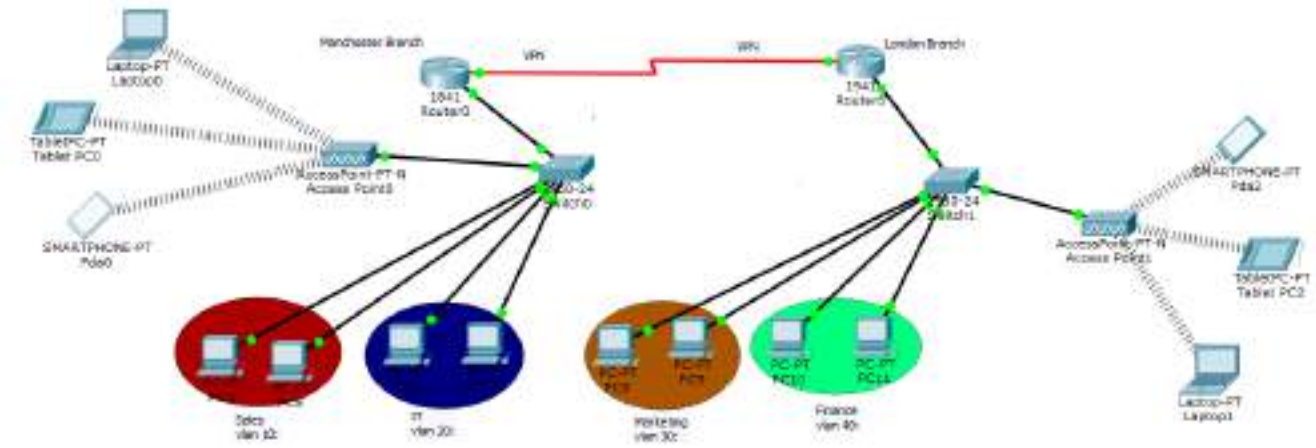


Figure: working model of the project in packet tracer

Since WEP encryptions alone cannot guarantee the security of the networks or the other information that are being transmitted across the network, yet placing a large number of hurdles that the intruders have to overcome in order to gain access to the information have been effective in many other security models(Ferng, Nurhakim and Horng, 2013). Thus the very same policy has been adopted in this case.

A two way authentication security system has been used in order to secure the system form the malicious activities of the intruders or the attackers. A secured application gateway ensures that only authorized users are able to gain access to the node of the wireless security system, whereas authentication from the user's side ensures that the person making requests for accessing the wireless network is a valid user (Fong, Parr and Morrow, 2010). The second authentication procedure has been implemented with the use of a secure ID and password system. The users have to validate themselves to the designed security system by the proper use of these two pieces of information (Gheorghe, Lo Cigno and Montresor, 2010).

Chapter 5. Testing the evaluating the project

The system being designed will be subjected to the following testing procedures in order to make sure that the security levels of the VPN system has indeed been enhanced (Hashim, Munasinghe and Jamalipour, 2010):

1. Threat modeling: The various components of the entire system are considered in order to evaluate their individual vulnerabilities to security risks (Jung and Peradilla, 2011).

2. Penetration testing: The configuration of the entire network security system is reviewed in order to ensure that a maximum security level exists in the network, a test process known as the network penetration process. The various applications that run on the wireless network are also tested for similar reasons, a process known as the application penetration test (Kaseva, Hämäläinen and Hännikäinen, 2011).

3. **The various cookies** and other such information that are continuously being stored at the devices which are connected to the wireless network need to be tested regularly in order to test the effective security of the system(Kim, Ikhlef and Schober, 2012).

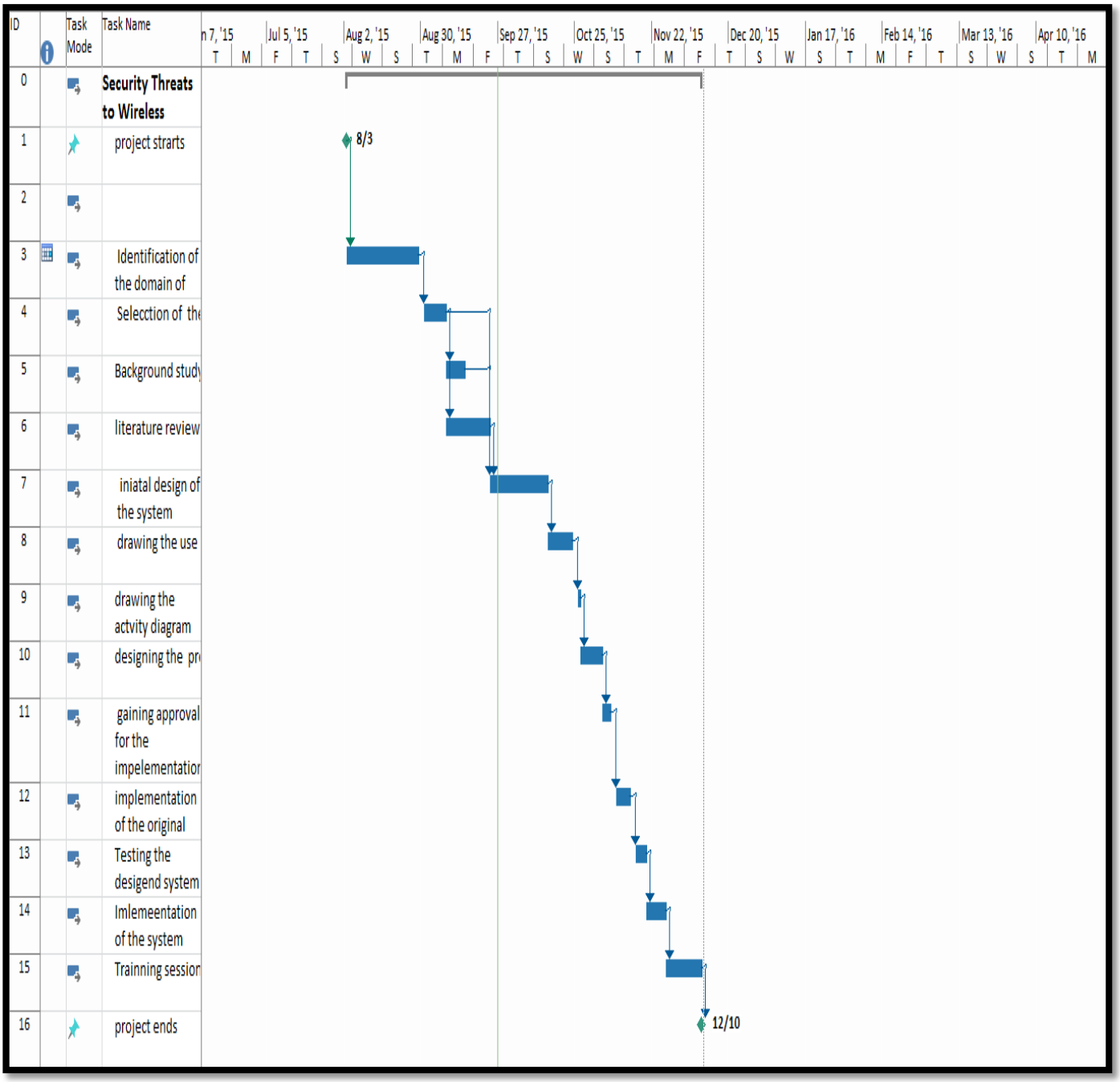
Chapter 6.

6.1 Brief Description:

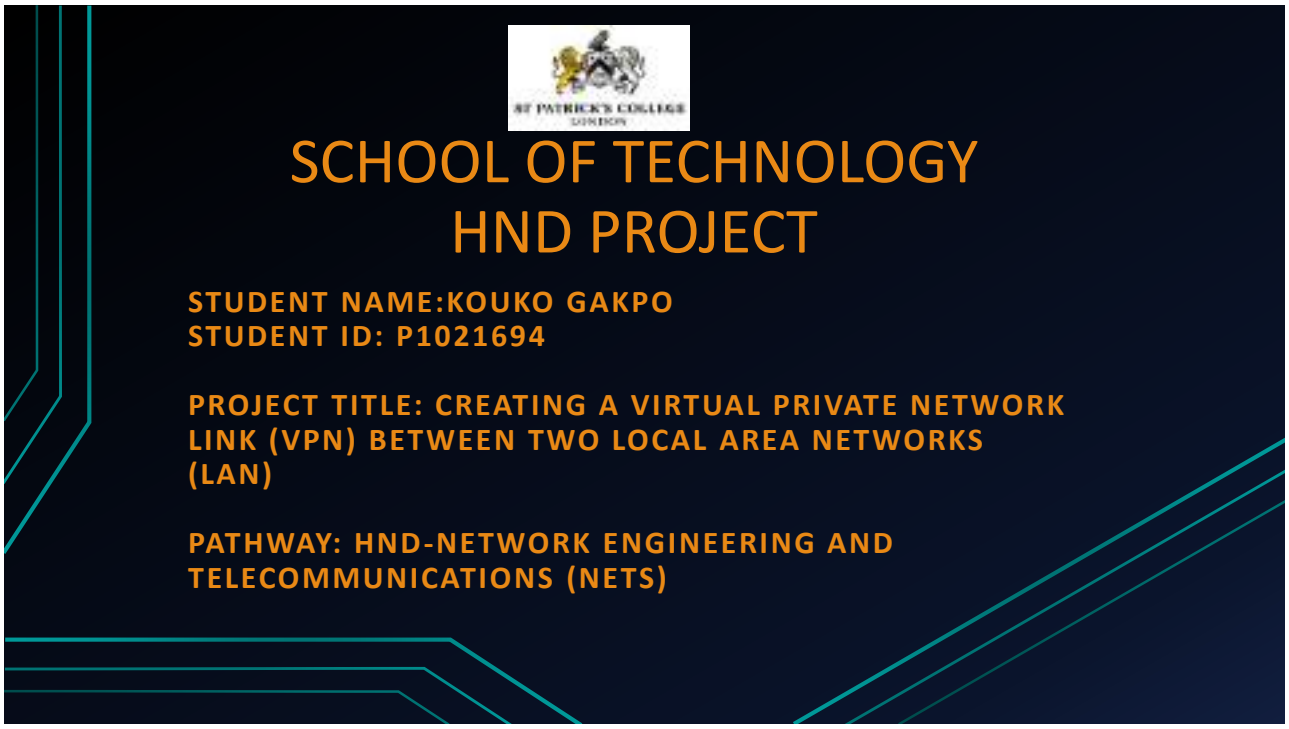
In this section of the project, the schedule according to which the project will progress has been discussed.

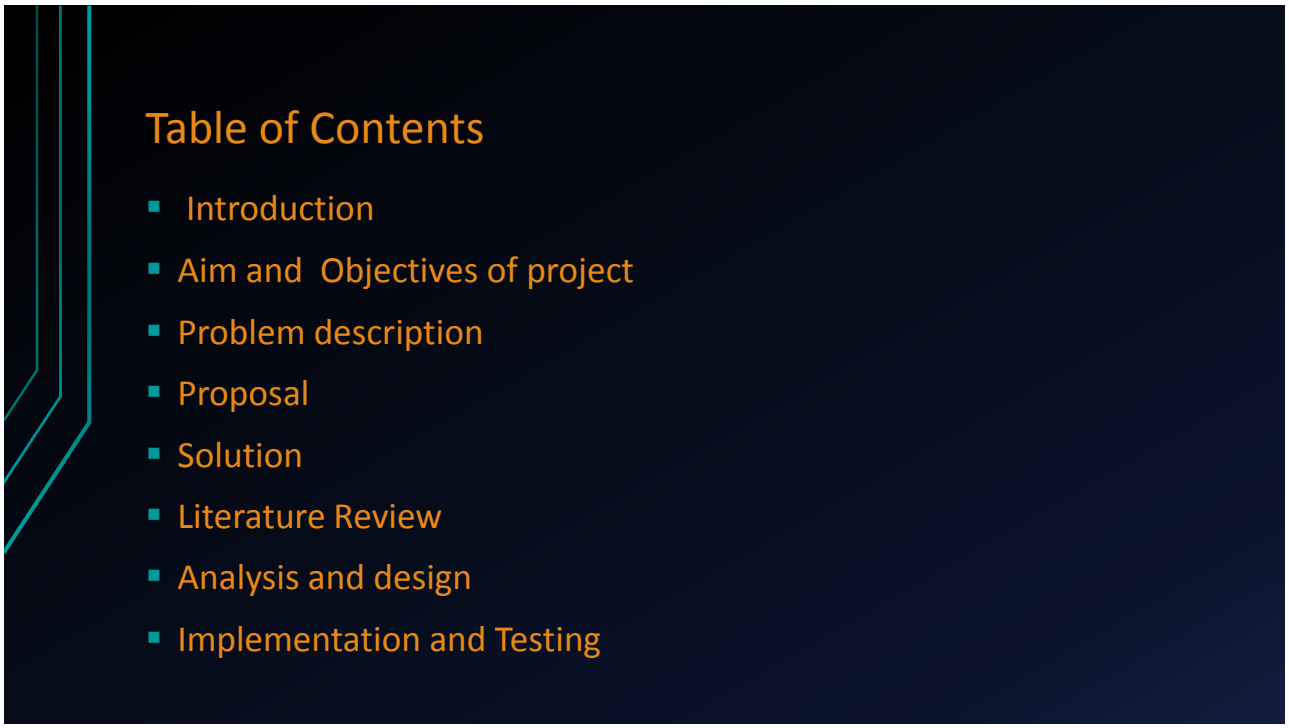
6.2 Gantt Chart:

The project is proceeding according to the following schedule:


ID
Task Mode
Task Name
n 7, '15
Jul 5, '15
Aug 2, '15
Aug 30, '15
Sep 27, '15
Oct 25, '15
Nov 22, '15
Dec 20, '15
Jan 17, '16
Feb 14, '16
Mar 13, '16
Apr 10, '16
T M F T S W S T M F T S W S T M F T S W S T M F T S W S T M
0 Security Threats to Wireless
1 project strarts
8/3
2
3 Identification of the domain of
4 Selecction of the
5 Background study
6 literature review
7 iniatal design of the system
8 drawing the use
9 drawing the actvity diagram
10 designing the pr
11 gaining approval for the impelementatior
12 implementation of the original
13 Testing the desigend system
14 Imlemeentation of the system
15 Trainning session
16 project ends
12/10

Presentation du project in Power Point





Problem description

To establish the safest method of data exchange communication between London and Manchester offices.

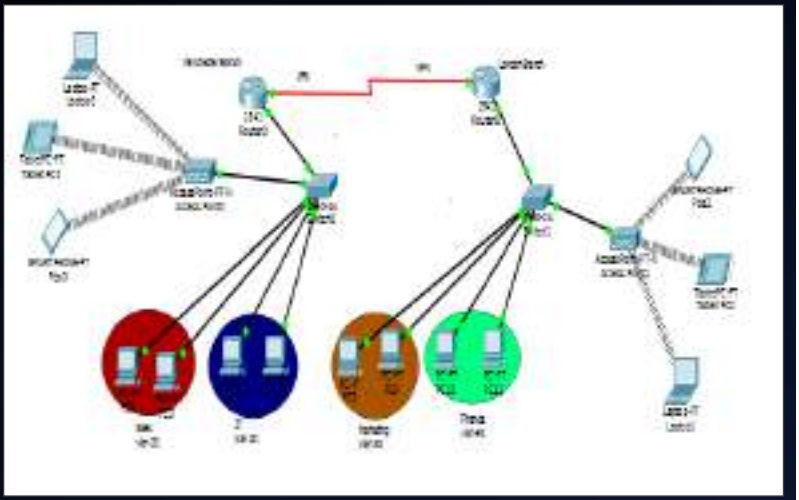
Proposal

Virtual Private Network

Virtual Private Network (VPN) is a very secure point-to-point networking technology that provides secure remote access to a public or private networks. VPN uses TCP/IP tunneling protocol for secured transmission of data.

SOLUTION

model of the project worked in packet tracer.



Literature Review

A large number of existing literary articles were reviewed so as to conduct a background study in the domain being reviewed. The existing models and methods that are currently being used to ensure the (Virtual Private Network) VPN has been studied in details so as to understand the ground level technology which is being used.

The following topics will be reviewed

- Layer 2 Tunneling protocol
- IP security
- Transport Layer Security

Analysis and design

Analysis and Design is considered as one of the most important part of conducting a technical project, as the ideas that are generated from the exhaustive survey of the existing literary works are found to be of immense help while developing the designs of a model that could serve the purpose of the project. In this project, the wide range of literary works that have been reviewed and also have been influential in the process of designing the VPN

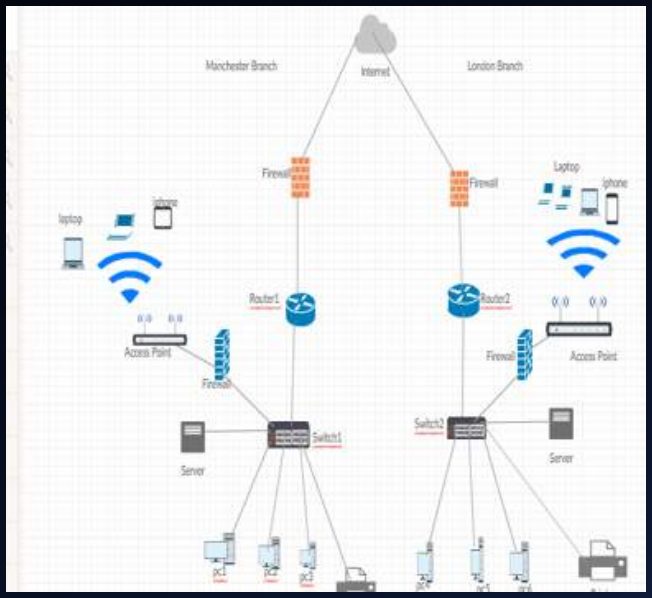
Implementation and Testing

The system being designed will be subjected to the following testing procedures

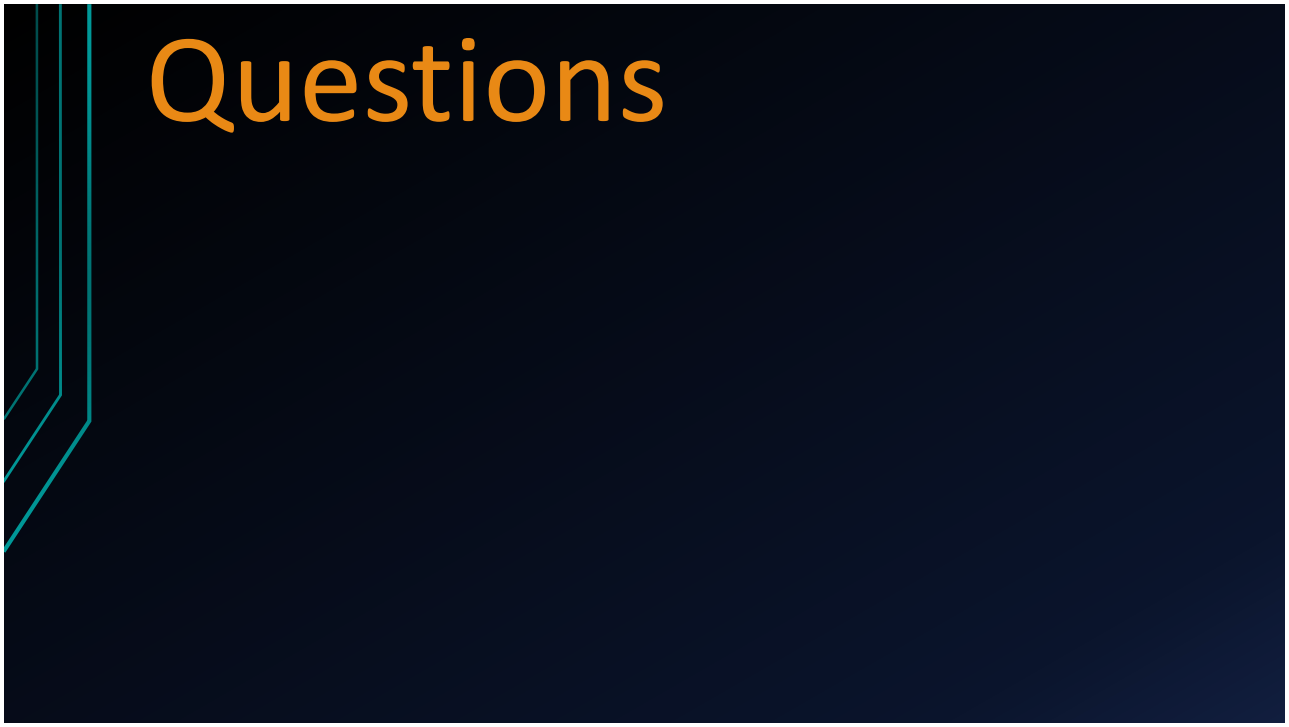
- Authentication: to ensure user authentication
- Point-to-point encryption: To ensure that information is not compromised or accessed by third parties.
- IP security: To ensure that incoming and outgoing data is encrypted

NETWORK IMPLEMENTATION DIAGRAM FOR THE PROPOSED SOLUTION

Wide Area Network with VPN point-to-point link



Thank You



Chapter 7. Limitations and Features Work

Limitations:

During my project studies in the college, problems (no enough time to concentrate on my project, I have to drop my children to school and picked them after school, I have to work at night) were added and I was overwhelmed after. This plague was caused by an attitude or an erroneous perception of workload. The first cause of my overflow feeling was too much to do. The 2 years that I have spent at Saint Patrick's college gave me a good education and good knowledge in the field of technology. I know now what Network Telecommunication means. This project that I gave myself was not reached the grade I was focused when I entered at the college, I do not have enough time to finish it on time. I can't use correctly Packet Tracer after trying with my friends and also with my own researches. Because of the lack of time, this unit cannot be finished in the college on time because there is too much things to learn which I did not achieve during my 2 years studies. At the end of my researches, I met the lecturer Alan who game me more attention regarding how to configure packet tracer. I have to complete this topic in my one year top up in University.

Features Works:

Since the project is not finished at the College, I am obliged to go to the University for a superior grade in the interest of having a deposed thorough regarding the use of packet tracer plot that I didn't finish because of the limit of time that was given to me at the college. One year on top of the 2 years I spent at college would allow me to have a good base and better knowledge on Network Telecommunication and it will open for me the way to return the better current life with an important intellectual baggage that would give me access to a good job in the future, because my objectivity would be to work in a large bank square like Barclays Bank Plc. To achieve this goal, I have to work harder at the University in all the units which would be presented to me.

Closeout meeting

The closeout meeting concludes phase I of the VPN solution project. The purpose of the meeting is to go over the closeout summary of the project and present the post-documentation to Badiepa Solution Limited Company' engineers

8. Conclusion

To give this organization the necessary versatility to support future unknown, possible multi-vendor customer premise equipment, I recommends IPSec. IPSec will provide the organization with the capability to support three essential components of a secured VPN connection: packet authentication, encryption and tunneling.

The encryption protocol to be selected depends on the level of security required and the laws governing the export and import of this technology. The sensitivity of information being transported will decide whether strong encryption (128-bit) will be used. Security must also be weighed against performance. Security should not be increased to a point where the performance of the secure transmission is substantially degraded.

A key factor in defining the solution are the International iBasis offices and their need to create a VPN back to the United States. Even though the United States has relaxed its regulations of exporting 128-bit encryption technology, Badiepa Solution Limited Company is extremely concerned with the laws governing this in other countries. Because of this, it has been decided to implement the minimal bit size key used for encryption/decryption. The use of the Cisco product line and IPSec currently only allows for DES and 3DES encryption methods.

9. Resources/ Reference list

Aksu, A., Krishnamurthy, P., Tipper, D. and Ercetin, O. (2012). On Security and Reliability Using Cooperative Transmissions in Sensor Networks. *Mobile Networks and Applications*, 17(4), pp.526-542.Araujo, A., Blesa, J., Romero, E. and Villanueva, D. (2012). Security in cognitive wireless sensor networks. Challenges and open problems. *EURASIP J Wirel Commun Netw*, 2012(1), p.48.

Bera, P., Ghosh, S. and Dasgupta, P. (2010). Policy Based Security Analysis in Enterprise Networks: A Formal Approach. *IEEE Transactions on Network and Service Management*, 7(4), pp.231-243.

Bloch, M., Debbah, M., Liang, Y., Oohama, Y. and Thangaraj, A. (2012). Special issue on physical-layer security. *Journal of Communications and Networks*, 14(4), pp.349-351.

Chan, A. and Castelluccia, C. (2011). A security framework for privacy-preserving data aggregation in wireless sensor networks. *ACM Trans. Sen. Netw.*, 7(4), pp.1-45.

Eghbal, M. and Abouei, J. (2014). Security Enhancement in Free-Space Optics Using Acousto-Optic Deflectors. Journal of Optical Communications and Networking, 6(8), p.684.

Farash, M. (2014). Security analysis and enhancements of an improved authentication for session initiation protocol with provable security. Peer-to-Peer Networking and Applications.

Ferng, H., Nurhakim, J. and Horng, S. (2013). Key management protocol with end-to-end data security and key revocation for a multi-BS wireless sensor network. *Wireless Netw*, 20(4), pp.625-637.

Fong, C., Parr, G. and Morrow, P. (2010). Security Schemes for a Mobile Agent Based Network and System Management Framework. J Netw Syst Manage, 19(2), pp.230-256.

Gheorghe, G., Lo Cigno, R. and Montresor, A. (2010). Security and privacy issues in P2P streaming systems: A survey. Peer-to-Peer Networking and Applications, 4(2), pp.75-91.

Gutierrez, P. (2011). A Simplified Internet Routing Architecture. *Mobile Networks and Applications*, 16(4), pp.433-445.

Harris, A., Jones, D., Horbatuck, K. and Sierra, A. (2012). A Novel Wavelength Hopping Passive Optical Network (WH-PON) for Provision of Enhanced Physical Security. Journal of Optical Communications and Networking, 4(3), p.289.

Hashim, F., Munasinghe, K. and Jamalipour, A. (2010). Biologically Inspired Anomaly Detection and Security Control Frameworks for Complex Heterogeneous Networks. IEEE Transactions on Network and Service Management, 7(4), pp.268-281.

Janssen, R. (2010). VDI and security. Network Security, 2010(3), pp.8-11.

Jung, Y. and Peradilla, M. (2011). Tunnel gateway satisfying mobility and security requirements of mobile and IP-based networks. Journal of Communications and Networks, 13(6), pp.583-590.

Kaseva, V., HÃ¤mÃ¤lÃ¤inen, T. and HÃ¤nnikÃ¤inen, M. (2011). A Wireless Sensor Network for Hospital Security: From User Requirements to Pilot Deployment. EURASIP J Wirel Commun Netw, 2011(1), p.920141.

Kim, J., Ikhlef, A. and Schober, R. (2012). Combined relay selection and cooperative beamforming for physical layer security. Journal of Communications and Networks, 14(4), pp.364-373.

KoÅ‚odziej, J., Jaatun, M., Khan, S. and Koeppen, M. (2013). Security-Aware and Data Intensive Low-Cost Mobile, Editorial. Mobile Networks and Applications, 18(5), pp.591-593.

Malekzadeh, M., Abdul Ghani, A. and Subramaniam, S. (2011). Design and Implementation of a Lightweight Security Model to Prevent IEEE 802.11 Wireless DoS Attacks. EURASIP J Wirel Commun Netw, 2011(1), p.105675.

Nogueira, M., Silva, H., Santos, A. and Pujolle, G. (2012). A Security Management Architecture for Supporting Routing Services on WANETs. IEEE Transactions on Network and Service Management, 9(2), pp.156-168.

Physical-layer security. (2011). Journal of Communications and Networks, 13(5), pp.545-545.

Polito, S., Zaghloul, S., Chamania, M. and Jukan, A. (2011). Inter-Domain Path Provisioning with Security Features: Architecture and Signaling Performance. IEEE Transactions on Network and Service Management, 8(3), pp.219-233.

Rass, S. (2012). On Game-Theoretic Network Security Provisioning. *J Netw Syst Manage*, 21(1), pp.47-64.

Rass, S., Wiegele, A. and Schartner, P. (2010). Building a Quantum Network: How to Optimize Security and Expenses. J Netw Syst Manage, 18(3), pp.283-299.

Reaz, A., Roy, R. and Atiquzzaman, M. (2013). P-SIGMA: security aware paging in end-to-end mobility management scheme. Wireless Netw, 19(8), pp.2049-2065.

Rowan, T. (2010). Negotiating Wi-Fi security. *Network Security*, 2010(2), pp.8-12.

Saleh, M. and Liang Dong, (2013). Real-Time Scheduling with Security Enhancement for Packet Switched Networks. IEEE Transactions on Network and Service Management, 10(3), pp.271-285.

Saleh, M. and Liang Dong, (2013). Real-Time Scheduling with Security Enhancement for Packet Switched Networks. IEEE Transactions on Network and Service Management, 10(3), pp.271-285.

Schonwalder, J. and Marinov, V. (2011). On the Impact of Security Protocols on the Performance of SNMP. IEEE Transactions on Network and Service Management, 8(1), pp.52-64.

Shon, T., Koo, B., Park, J. and Chang, H. (2010). Novel Approaches to Enhance Mobile WiMAX Security. EURASIP J Wirel Commun Netw, 2010(1), p.926275.

Smith, G. (2010). Countering datacenter security pressures. *Network Security*, 2010(8), pp.15-17.

Sourour, M., Adel, B. and Tarek, A. (2010). Network Security Alerts Management Architecture for Signature-Based Intrusions Detection Systems within a NAT Environment. *J Netw Syst Manage*, 19(4), pp.472-495.

Stiller, B., De Turck, F., Morariu, C. and Waldburger, M. (2010). Report on the 4th International Conference on Autonomous Infrastructures, Management, and Security (AIMS 2010) and the International Summer School on Network and Service Management (ISSNSM 2010). *J Netw Syst Manage*, 19(1), pp.130-136.

Stiller, B., De Turck, F., Morariu, C. and Waldburger, M. (2010). Report on the 4th International Conference on Autonomous Infrastructures, Management, and Security (AIMS 2010) and the International Summer School on Network and Service Management (ISSNSM 2010). J Netw Syst Manage, 19(1), pp.130-136.

Twitter told to tighten security. (2010). Network Security, 2010(7), p.20.

Venkatasubramanian, K. and Gupta, S. (2010). Physiological value-based efficient usable security solutions for body sensor networks. ACM Trans. Sen. Netw., 6(4), pp.1-36.

Wan, K. and Alagar, V. (2014). Context-Aware Security Solutions for Cyber-Physical Systems. Mobile

Networks and Applications, 19(2), pp.212-226.

Wang, L., Guo, Y. and Zhan, Y. (2010). Security Topology Control Method for Wireless Sensor Networks with Node-Failure Tolerance Based on Self-Regeneration. EURASIP J Wirel Commun Netw, 2010(1), p.201416.

Wang, L., Guo, Y. and Zhan, Y. (2010). Security Topology Control Method for Wireless Sensor Networks with Node-Failure Tolerance Based on Self-Regeneration. EURASIP J Wirel Commun Netw, 2010(1), p.201416.

Westphall, C. and Mueller, P. (2010). Management of Security and Security for Management Systems. J Netw Syst Manage, 18(3), pp.241-243.

Williams, K. (2012). Digital Fabrication. Nexus Netw J, 14(3), pp.407-408.

Zhang, F. and Chen, H. (2012). Security-Preserving Live Migration of Virtual Machines in the Cloud. *J* Netw Syst Manage, 21(4), pp.562-587.

Zhang, Y. and Chen, J. (2012). Wide-area SCADA system with distributed security framework. Journal of Communications and Networks, 14(6), pp.597-605.

Zic, J., de Groot, M., Liu, D., Jang, J. and Wang, C. (2012). Hardware Security Device Facilitated Trusted Energy Services. Mobile Networks and Applications, 17(4), pp.564-577.

POST

Virtual Private Network – A Study

Name of the student:

Id of the student:

Title of the project: Creation of Virtual Private Network Link (VPN)

between two Local Area Networks (LAN)

Pathway: HND-Network Engineering and Telecommunications (NETS)

Acknowledgements

I have done an excellent project on security threats to wireless networks. I am very much thankful to my coordinator of the project Mr. Tanveer Ahmad, who provided me this golden opportunity to work. I have got a lot of help and support from Professor Ahmad while doing the project as I got a lot of knowledge and insights from him. Therefore, I am always grateful to him for giving me a chance. I also thank my parents and all the rest of my family members who gave an excellent support in completing the project within thee given deadline. I also like to appreciate all those people belonging to my work field, from Mr. Alan to Mr. Malcolm Thomson, the head of Network Technology. I thank Mr. Thomson's team members along with the teachers and the team looking after the administration. I would finally like to appreciate all my class mates: Simon, Amici, Toco and Mitterand. All the four people whose name I have mentioned here have given me an extensive support at the time when I was studying

Networking Telecommunication for two years. They have helped me to reach some milestones related to IT.

ABSTRACT

In the current scenario, companies often look for secure, cost effective data communication solutions. Their demand for such kind of solutions with guaranteed services. Due to this reason, the companies look for Virtual Private Networks (VPN). The Internet Protocol (IP) has made VPN the ultimate choice for the future. It has been seen that the level of service differentiation to implement it in IP VPN is not an easy task. A proposal for class of service (COS) classification has been taken into consideration with the association of QOS parameter set. It is done to establish VPN in a wide area. Various scenarios will be studied where appropriate QOS are targeted to be met under each COS. It is done for doing streamlined communication for each VPN access interface. This interface is aimed to connect with the IP network. If the end to end traffic profiles can be estimated, then the difficulties in the network can be healed. To reduce the complexity of the specifications, the proposal aims the users to make themselves involved in wireless networks.

VPNs have become the ultimate choice nowadays regarding connecting the interlinked private networks on the internet. VPNs are very reliable in nature. They reduce the expense of connecting the systems through leased lines. In the case of VPN connection, the dedicated leased lines are not required. Due to this reason, VPNs have become very reliable. The VPN connections often face issues. The given statements are some of the techniques how issues can be dealt with:

Table of Contents

Chapter 1: Project Introduction 44

Introduction 44

1. Project Aim 44

2. Objectives 45

1.3 Description of the Problem 46

1.4 Proposal 48

1.5 Solution 48

1.6 Overview of the design 48

1.6 Summary of VPN Technologies 49

1.6.1 Tunnelling 49

1.6.2 Encryption 50

1.7 Analysis and comparison of VPN technology 50

1.7.1 Tunneling 50

1.7.2 Methods of Encryption 51

1.7.3 VPN's Advantages and Disadvantages 52

1.8 Resources 53

1.9 Special Conditions / Constraints 53

Chapter 2: Literature Review 55

2.1 Introduction 55

2.2 Literature Review based on Domain 55

2.3 Literature Review based on Technology 58

Signal Hiding Methods: The various types of signal hiding include the following:.....59
Unencrypted Tunnels 60
Entrusted networks for delivery 60
Use of VPNs in mobile surroundings.....61
Use of VPN on Routers 61
Implementation of the Star Methodology 63
Development and Plan acknowledgment 65
Configuration of Sample Structure.....65
Formation of CBT 67
Chapter 3. Design and Analysis 68
3.1 Introduction 68
3.2 Efficient and non-efficient needs 68
Deploy rollout maintenance 73
Chapter 6. 74
6.1 Short Description.....74
6.2 Gantt Chart 75
Project Presentation in Power Point 75
8. Conclusion.....80
References 82

Chapter 1: Project Introduction

Introduction

It has been seen that VPNs have undergone through some problems while linking the private networks on the internet. It is noticed that VPN does not require the dedicated leased lines which are very expensive. Therefore, VPN makes the companies free from the additional costs incurred in the leased lines. Thus, VPN has proved that it is much more reliable in its usage (Abramson and Sinha 2012). The problems which VPN face are infrequent. Some of the troubleshooting procedures are mentioned below.

The BSLC (Badiepa Solution Limited Company) has appointed me as the consultant to a new project and has assigned me a task to make a proposal for the creation of a Point to Point link. The link has been aimed at the company's new office (Aggarwal *et al*. 2014). There are two departments of the office located in Manchestor. The departments are Sales and IT respectively.

1. Project Aim

The project has the aim to develop and design a VPN of remote access. It is a public communication set up where the users can access the network of the organization from a remote place with an optimum level of security. In generally the VPN client of a remote user’s computer connects to the organization's VPN gateway. During the connection, the device looks for its authenticity in the network. After the

authentication takes place, the network link gets created so that the remote users can access the internal networks of the organization (Asati *et al*. 2014). They can access the file servers, intranets and printers as well as local user can do. The remote access VPN requires security which it gets from the SSL or IPsec. SSL or Secure Socket Layers are used for the single application. The concept is not preferred for the entire internal network. The VPNs which provide Layer to Access to the system require protocol other than IP. Those rules are termed as PPTP or L2TP. These are tunneling protocols which run across the IP connections (Baum and Voit 2014). This kind of model is required to be designed for such organizations who prefer wirlesless network for transferring data.

2. Objectives

The project objectives include providing IBasis technology for the users. The IBasis technology should be secure, manageable, scalable and redundant. An example is the International Sales Force, who are dedicated to access the corporate resources. It is a dial up solution still existing today. It is built on a Cisco Secure Access Control Server (ACS) authentication server and a Cisco AS5300 utilizing two T-1/PRI circuits. IBasis has aimed to provide more accessibility of internet throughout the globe. It is developed for better utilization of the benefits of the VPN solution. If a VPN solution is implemented, then it becomes an alternative for the dial up connections for the corporate resources (Border *et al*. 2015). The technology eventually helps the users sitting at a remote location to access the local Internet Service Providers (ISP). The get connected to the network through the use of cable modem or xDSL. In the procedure, they eventually notice a reduction in cost and increase in the throughput. It should be ensured that the VPN solution will be able to support its client at the fullest extent meeting their desires. They should be able to provide support to their each customer of atleast fifty users. They should ensure that each year's future growth is 100%. IBasis has planned for the creation of dynamic passwords. They have planned to do this work by proper utilization of token password technology initiated by Cisco Secure Authentication Server (Unnimadhavan *et al*. 2016). Thus, it will be done to complement the security structure of Cisco.

The IT departments often face challenges regarding support to the user communities and setting the expectation for the remote users. IBasis also looks for supportive technical documentation for fast adaptation for their users and IT staffs. For support, the project aims to develop a user manual which will guide the user through every step. The project also initiates an interactive Computer Based Training (CBT) for fast adaptability for the users and IT staffs. A user feedback process is also required to carry on the project. REALTECH also has the recommendation for such process (Bragg *et al*. 2013). It is a very crucial part of the project as it will help to identify the exact needs of the users community.

1.3 Description of the Problem

The most common problems that are detected are in generally of four types. They are:

- The VPN connection gets rejected.
- The connection without authorization gets accepted.
- Certain locations which lie beyond the VPN server are not reached.
- A tunnel can not be established.

It is a massive probem if the VPN connection gets rejected. This kind of problem is very much standard. There may be another kind of issues which can also create problems resulting to the rejection of the VPN. If it has been noticed that the VPN connections have turned down for some unknown reasons, the Router and Remote Access Service should be primarily checked whether they are properly functioning (Bragg *et al*. 2015). The functionalities can be verified by going to the Control Panel of the server and clicking the Administrative Tools icon. After clicking the Administrative Tools, the Services icon should be clicked. As the service gets verified, it is required to keep on pinging the VPN server by IP address from the VPN client in a continuous manner. The pinging procedure is needed to be done initially to check the existence of the basic TCP / IP (Brahim *et al*. 2012). If the pinging gets successful, then the server is required to be pinged again.

The issue can be related to other problems detected while routing. For an instance, if any user is dealing without any medium in the VPN server, it's recommended to create a path of static nature between the server and the client (Brakerski and Vaikuntanathan 2014). The procedure for configuring a static route is mentioned below.

- Go to the Dial-In Tab of the properties sheet of the user in Computers and Active Directory Users.
- Select the Apply A Static Route check box.

The procedure will lead to displaying the Static Routes Dialogue Box on the Windows screen.

- Click the Add Route button and enter the network mask and destination IP address in the given space. Please make sure to leave the metric space at 1.

If the user is using the DHCP server for assignment of the IP addresses to the clients, particular problems can occur which can make the user not able to go beyond VPN server. A problem that can occur is about IP conflict. An IP conflict is nothing but all about duplicate IP addresses. The DHCP server if assigns an IP address to a user which already exists in the network, then the Windows automatically detects the conflict. It eventually blocks the user from accessing the system. Other problems may be that a user is not getting an IP address to access the network (Chen *et al*. 2014). It is the prime responsibility of the DHCP server for assigning an IP address to the user. If the server is not able to perform the assignment task, then connections will not take place by any means. There is a procedure in case of issues in assigning IP addresses where the users are provided IP address from 169.254.x.x range. In such process, Windows perform the assignment task automatically (Cai *et al*. 2014). If the IP address does not belong to the range of the system's routing tables, then the user will not be able to access the network.

Difficulties in establishment of a tunnel

If all the functionalities take place as per the standards, but a tunnel is not established between the client and server, it denotes that there may be two main possibilities causing the problem. The first possibility may be like that; IP packet filtering is done by one or more routers. It can hamper the traffic in the IP tunnel. Therefore, it is highly recommended to check the client, the server and all the other machines that lie between IP packet filters (Xiang *et al*. 2014). The difficulties can be recovered by following the procedures.

- Click the Advanced button on each Machine’s TCP / IP Properties sheet.
- Select the Options tab from the Advanced TCP / IP Settings Properties sheet.
- Select the TCP / IP filtering.
- Click the Properties button.

The second possibility can be the existence of proxy server in between the main server and the client. The proxy server is responsible for translating the NAT on all the traffic between the network and its client. It, therefore, implies that the packet has been transmitted from the proxy server. The package does not come with the customer's machine. In some cases, the tunnel can go in a complete deadlock stage. This kind of situation can occur especially if the VPN server asks for an IP address from its client

(Das *et al*. 2016). It should always be remembered that L2TP, IPSec, PPTP protocols used in the VPN networks are often not supported by the NAT firewalls or the low-end proxy servers.

The following project has been developed to initiate a higher level of security in the VPN networks.

1.4 Proposal

This project has been designed to create a model that is based on Virtual Private Network, which will enhance the defense structure of the Badiepa Solution Limited Company. The defense system will protect the company from severe threats and attacks (Dimitri *et al*. 2016). Those threats and attacks which can destroy or hamper their valuable data.

1.5 Solution

The remote users who access network are protected by the Virtual Private Networks (VPN). To have a balance in the security structure, the user must be careful in opting the appropriate technologies (Dutta and Kwok 2013). They always require a proper planning for its usability. The sections mentioned below gives us a summary of the Rapid Assessment and its related research. The summarization can also be done on the recommendation of the solution.

The determinants of the IBasis VPN Solution are given below:

- Identification of the VPN technologies that are the best fit for the requirements.
- Determination of the necessary network elements that are required for the implementation of the solution.
- Placing the network elements so that they can be fully active in functionality and security (Dutta *et al*. 2014).

1.6 Overview of the design

The below-mentioned requirements have been identified during the discovery process.

- The solution is aimed to complement Badiepa Solution Limited Company. The solution is based on the Cisco product line.
- Usage of VPN technology can lead the user to access the network

- The proper utilization of the system and its associated software can be done by the solution.
- The remote users and the sales force who are traveling are located throughout the world.
- In the case to avoid theft of the actual VPN client, the technology of user authentication is required (Figueira *et al*. 2013).
- Internally defined resources are needed to be accessed.
- The solution must be in that structure so that it can be properly managed. The solution will also aim for minimization of support requirements.

The design which has been produced consists of utilization of the existing Cisco 7120-4T1 VPN router. The addition of an Integrated Service Module (ISM) also leads to an unrestricted, complimentary license for Cisco VPN client software.

A rigorous discussion has been done with the IBasis. The decision taken was that 7120 specifications of 50+ Mbps throughput and 175 Kbps are proper for the current. (in ISM there are 2000 parallel users and 90 Mbps throughput). It has been seen that 7140 specifications can provide better performance (Goldwasser *et al*. 2013). It can also provide a better redundant supply of power. But the thing is that the time it will take to receive the new router is not acceptable to IBasis. IBasis has many employees who reside overseas. They can have an urgent need for accessing the corporate resources. In such cases, the time for completion of the VPN solution is a critical factor (Gong *et al.* 2013). In the current era, IBasis is incurring the costs of the international users. They are dialing into AS5300 access server.

1.6 Summary of VPN Technologies

The main technologies that are associated with VPN solutions are mentioned here. They are encryption standards, authentication methods, and methods of tunneling.

1.6.1 Tunnelling

The above mentioned protocol encapsulates the layer 2 or layers three protocols into the other protocols. It is used to be transported over the internet. A virtual communication path is developed using this protocol. This kind of protocol is mentioned as "tunnels." By the help of this type of technology, a company does not require the expensive leased line structure in its Wide Area Communication. As an alternative, they create “tunnels” across public networks. There are some standard protocols of tunneling

(Gorbunov *et al*. 2015). The Internet Protocol Security or IPSec, Layer 2 Tunneling Protocol or L2TP, Point to Point Tunneling or PPTP are some of the examples of tunneling.

1.6.2 Encryption

The word “cryptography” comes from the word “kryptos”, that implies hidden. The concept uses the algorithms to ensure the security of information. Cipher is a process where encryption and decryption, both can be done. Encryption is a process of converting data into an unreadable form. The method of encryption consists of Data Encryption Standard (DES), RC4, Blowfish and International Data Encryption Algorithm (IDEA).

Encryption is the techniques which use algorithms. These algorithms are based on keys to encrypt and decrypt information. The main algorithms are of two types, symmetric and asymmetric. The symmetric algorithms based on the secret key and the asymmetric algorithms based on the public key (Hasan 2014). The secret key algorithm uses the same key for encryption and decryption whereas the public key algorithm uses a different key for decryption and encryption. Cipher programs use a public key to encrypt data. The public key known to any person or user. In the case of decrypting the information, some other key is required, which is the private key. The user can only decrypt the information if he has the knowledge of the private key. The single bit of plain text encrypted by the Secret-Key algorithms. The algorithm can also encode some bits of plain text at one time. The first case is termed as Stream Cipher whereas the second instance termed as the block cipher (Gong *et al*. 2013). DES, IDEA, RC4, and DES are the examples of the secret key algorithms.

1.7 Analysis and comparison of VPN technology

1.7.1 Tunneling

The Point to Point Protocol (PPP) has an extension Point to Point Tunneling Protocol (PPTP). It encapsulates the local traffic into PPP. The Generic Routing Encapsulation (GRE) packets are then required to sent through the IP network. Microsoft has recently implemented a PPTP that uses a protocol. The protocol termed as Challenge Handshake Authentication Protocol (MS-CHAPv1). It utilized for the purpose of authentication. Another usage is for Microsoft's Point to Point Encryption (MPPE). The implemented PPTP of Microsoft did not reach the stage of maturity regarding authentication and encryption. The password of users is often used for hash algorithms. This kind of algorithms used as an alternative to storing key change algorithm like Diffie-Hellman or Internet Key Exchange (IKE). Certain weaknesses are required to fixed. The weaknesses are of MS-CHAPv1 that is

needed to set with MS-CHAPv2 (Hasan 2014). The corrected version is available in Dial Up Networking (DUN)'s version 1.3.

Another tunneling protocol that tunnels the PPP traffic is the L2TP or Layer 2 Tunneling Protocol. The features in Layer 2 Forwarding or L2F and PPTP combined in L2TP. The methods of authentication include MS-CHAP, PAP (Password Authentication Protocol) and CHAP.

IPSec provides data confidentiality, integrity, and authentication of transmitted data. It is therefore not a tunneling protocol. This kind of rules used in case of communication between two end points. It is done by hiding one protocol into other. The encapsulation process is applied to protect the original contract during the transmission (Hines *et al*. 2015). IPSec used for encrypting the original information. It also makes the data undecipherable during transmission. The methods of authentication can only do the decryption of information at the both endpointsuthentication.

1.7.2 Methods of Encryption

- The algorithms for encryption are entirely possible for deciphering in the given resources and time. It aims to make the overall process much difficult.
- The usage of Data Encryption Standard (DES) is a 64-bit block size. It is a block cipher. It implies that information can take under encryption in blocks of 64 bits.
- A regular DES's extension is Triple-DES (3DES) that uses 128-bit public-key.
- Blowfish is a kind of block cipher. It uses a 64-bit block size. It can also use a variable keys of length which can be up to 448 bits (Kamite *et al*. 2014).
- Another kind of block cipher is the International Data Encryption Algorithm (IDEA). It uses the 128 bit key.
- RC4 is also a kind of stream cipher. It uses a variable-bit key (40/128).
- The encryption solutions are Cisco Encryption Technology (CET) and Microsoft's Point to Point Encryption (MPPE). There are some fewer features which are required to meet the requirements of IBasis.

1.7.3 VPN's Advantages and Disadvantages

To build an inexpensive private network, VPN is an ultimate choice. To avoid the usage of leased private lines which is very much costly, opting the usage of internet is a wise decision due to its cost effectiveness. There are several costs for a company to incur for implementation of the network. One is the hardware cost and the other is for the software used to authenticate the users. The additional cost required for mechanisms such as authentication tokens or other devices prepared for security. The VPN connections have more flexibility, speed and its easy for implementation. Due to this reason, it has become an ideal option for a corporation which looks for less cost efficient network structure (Khanna *et al*. 2015). For an instance, it can be said that an organization can adjust the number of sites as per the varying requirements.

Their usage of VPN also has several disadvantages. There may be packet loss and performance issues due to lack of Quality of Service (QOS) in the communication through the internet. If any adverse network effects occur outside of the private network, then the VPN administrator is not able to do anything. As a result, the big corporate houses always pay a high amount for trusted VPNs to ensure Quality of Service. In VPN connections, Vendor Interoperability is again a disadvantage. It is due to the reason that VPN technologies adopted from one vendor may not be compatible with VPN technologies of another supplier (Klein *et al*. 2012). These advantages were not able to reduce the acceptance and deployment of VPN technology.

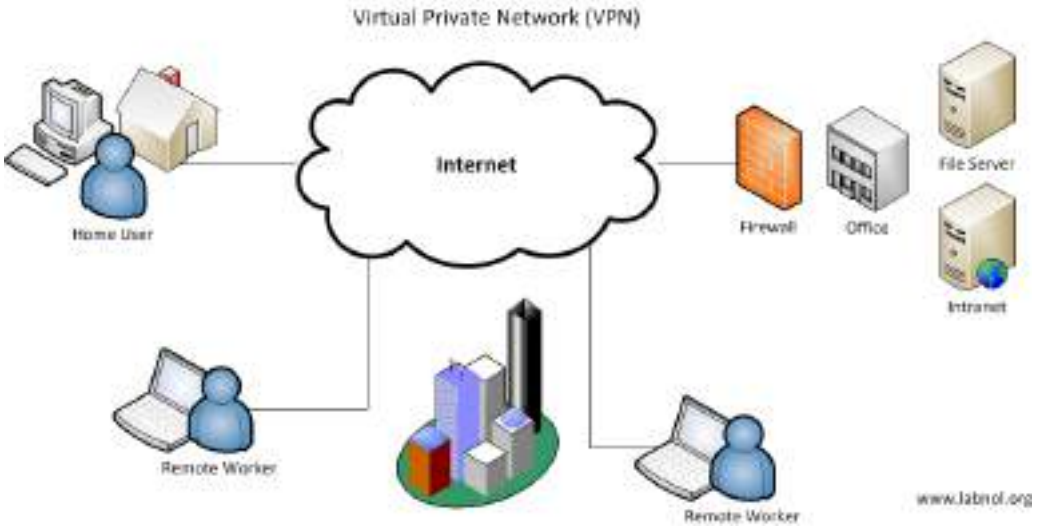
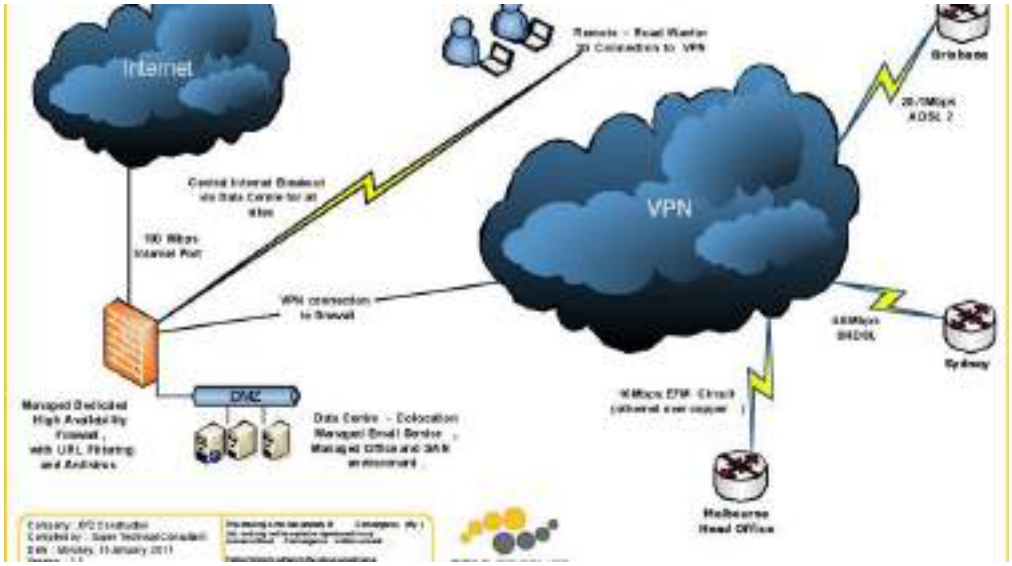


Figure: Virtual Private Network: Posted on June 29, 2014, by **Motiur Rahman**

The concrete meaning of VPN is, therefore, Virtual Private Network. The system used for security and privacy of personal computer and laptops during usage of internet (Kompella 2012). In generally, the internet user access VPN to change their IP.



1.8 Resources

The development of the model based on the rewiring of the following resources.

I. Access points which are secured wireless

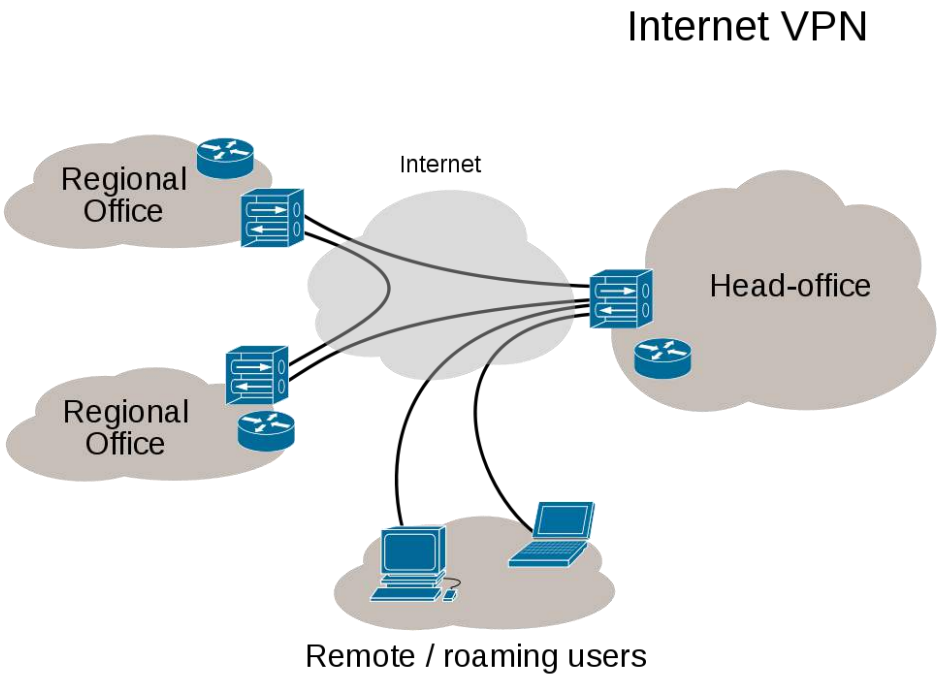
II. Gateways of Application

III. Control Servers

IV. Authentication Servers (Kothari and Fernando 2012)

1.9 Special Conditions / Constraints

Mechanisms of security:



VPNs are not able to make the online connections to be completely anonymous. They can enhance the level of privacy and safety. VPNs in generally allow authenticated remote access. It also provides the usage of encryption techniques.

VPNs ensure the security by usage of tunneling protocols (Koushik *et al*. 2014). They often provide that security through encryption procedures. The security model of VPN provides:

- Confidentiality in the case of network traffic sniffed at the level of the packet. If the system gets attacked, then the attacker can notice the data encrypted.
- Authentication of the sender regarding prevention from the unauthorized access to VPN.
- The integrity of the message for detecting the instances of tampering along with the transmitted messages (Kshirsagar and Thomas 2012).

The VPN-based protocols include the following:

- The Internet Engineering Task Force (IETF) initially developed the Internet Protocol or IPSec for IPv6. It required in all standards-compliant implementations. The implementations are of IPv6 before RFC6434 has made a recommendation to it. The

protocol mainly used for IPv4 and Tunneling protocol of Layer 2. The design of the protocol meets the requirements given below:

Confidentiality, authentication, and integrity. IPSec mainly used for encryption purpose; it aimed for encapsulation of the IP packet inside the other one. The reverse process, therefore, decryption happens at the tunnel end. The IP packet gets encapsulated and becomes forwarded to its destination.

The SSL or TLS or Transport Layer Security can tunnel the traffic from the network entirely. Such kind of tunneling is done in the case of Open VPN project as well as Soft Ether VPN project. This type of VPN connections is provided by the vendors. The Transport Layer Security or SSL VPN has the capability to connect the networks. It always complies with the rules of firewall and the translation of Network Address (Le Roux *et al*. 2013). The VPN also connects through SSL in the case of the trouble in IPSec.

Chapter 2: Literature Review

2.1 Introduction

To check the background, a large number of articles have reviewed. The models and methods regarding VPNs have studied in an extensive manner for understanding the technology (Liu *et al*. 2014)). The details are given below.

2.2 Literature Review based on Domain

- **Datagram Transport Layer Security (DTLS) – It used in Cisco. The Open Connect VPN and AnyConnect VPN required for resolution of the issues. It's the tunneling through the UDP of SSL/TLS.**
- The Point to Point Tunneling Protocol functions with Microsoft Point to Point Encryption (MPPE) in several compatible implementations on other platforms.

- The SSTP or Microsoft Secure Socket Tunneling Protocol has a tunneling contact with Layer 2 tunneling protocol through an SSL 3.0 channel. It tunnels with Point to Point protocol. (SSTP came in notice in Windows Server 2008 and Windows Vista Pack 1.)
- Multi Path Virtual Private Network (MPVPN) – Its owned by the traditional system development companies (Liyanage and Gurtov 2013).
- Secure Shell (SSH) VPN – The SSH, which are open, provides the tunneling of VPN, which can connect the inter-network links. It provides a limited numbered channels of concurrency. This kind of architecture does not support the personal authentication.

1. Authentication

As the VPNs established, it must be made sure that the authentication of the tunnel endpoints has been done. The remote access VPNs created for access user use various methods including cryptography, biometrics, passwords or two-factor authentication. The tunnel connections often employ the digital certificates or passwords. Here the user's intervention is not at all required (Liyanage *et al*. 2016). The establishment of tunnel happens automatically by keeping the key in the store.

2. Routing

In the point to point network topology, the tunneling protocol can be active. But in such case, it can not be treated as the VPN. It can say due to that reason as VPN supports the arbitrary nodes along with the mobile networks. The software-defined interface of the tunnel is mostly compatible with the implemented routers (McDysan 2013). The conventional protocols of routing are in generally followed by the customized VPNs.

3. VPN building blocks of provider provision

By operation in the Layer 3 or Layer, 2 of the supplier provisioned VPN (PPVPN), it can state that the blocks that have been built are either of L2 or L3 or may be the combined structure of the two. Mostly the combined structure is denoted by the Multiprotocol label switching (MPLS) (Mullick *et al*. 2013).

RFC4026 frequently follows the L3 and L2 VPNs. In generally they have taken place in RFC2547. Lewis and Cisco Press also provides this kind of information on the device.

4. Customer (C) devices

This type of device not attached to the service provider's network but with the client's system. This device does not have the knowledge of the VPN.

Edge Device of the Customer (CE)

This kind of device lays at the edge of the client's network. It typically supports the client to access to the PPVPN. In some instances, it becomes a point of demarcation in between the responsibility of the customer and the service provider (Pati *et al*. 2014). The rest of the service providers provides the power for configuration to the customers.

Edge Device of the Provider (PE)

This kind of devices usually connects the customer networks and gives the view of the provider for the client site. It lays at the edge of the network of the supplier. PEs in generally maintain the state of the VPN. They are usually aware of the VPNs that typically connect to them.

Device of the Provider (P)

There is no such direct interface to any endpoint of the customer with the P device. It operates in the core network of the provider. In some cases for an instance, provider run tunnels that belong to PPVPNs of different customers might provide routing. For the implementation of PPVPNs, P device is the key part. The device does not implement VPN state. The device is is also unaware of the VPN. The principal role of the device is to allow the service provider to scale its PPVPN offerings. For an example, it represents itself as the multiple PE device's points of aggregation (Sahai and Waters 2014). In between the primary locations of the providers, P to P connections are treated as often high capacity optical links.

5. PPVPN Service of User Visibility

The section particularly deals with the VPN types. The models considered in the IETF.

OSI Layer 2 Services.

Virtual LAN

It is a kind of Layer 2 technique that allows the coexistence of the broadcast domains of multiple LAN; it's interconnected by the trunks through the usage of IEEE802. The protocols of trucking types have become obsolete. The old rules include Link of Inter-Switch (ISL), IEEE 802.0. The IEEE 802.0 is originally protocol made for security. But its basically a subset which has introduced for trucking purpose (Sajassi *et al*. 2014). Other kinds of old rules are the Emulation of ATM LAN (LANE).

Private LAN Service of Virtuality (VPLS)

This type of LAN service developed by the IEEE. To share common trunking, the VLANs also allow the multiple tagged LANs. The VLANs comprise the facilities that are owned by the customer. In the OSI Layer 1 services, the VPLS typically supports the emulation of both points to point topologies. The VPLS also supports the emulation of topologies of a point to multipoint nature. The discussed methods usually make an extension of Layer 2 technologies. Those techniques categorized as 802.1q and 802.1d (Salaam *et al*. 2014). This kind of trunking of LAN done over the transports. An example is the Metro Ethernet.

2.3 Literature Review based on Technology

The VPLS is ordinarily a PPVPN of Layer 2 which uses the context. It is not a private line. It has the full functionality of the Local Area Network (LAN) of tradition. It can say from the standpoint of a user that, VPLS can make the interconnection between several LAN segments. It can make the interlinks over an optical, provider core or packet switched segments. The base made of transparency to the user (Shokhor and Shigapov 2013). It can make the LAN segments of small area act like a single LAN.

In the VPLS system, the emulation of a bridge of learning is done by the provider network. It optionally includes the service of VLAN.

Pseudo Wire

The Pseudo Wire or PW is quite same to the VPLS. The Pseudo Wire has the potential to provide different L2 protocols in the ends of both sides. Normally, the interface of such PW is the WAN protocol. The example of such protocol is the Frame Relay or the Asynchronous Mode of Transfer. The Virtual Private LAN service or the IPLS should be made appropriate for aiming to provide the LAN appearance (Si *et al*. 2014). The LAN will be therefore contiguous between two or more locations.

IP tunneling based Ethernet

An example for an Ethernet which relies on IP tunneling protocol specification is the Ether IP (RFC 3378). The mechanism for packet encapsulation has involved in EtherIP. The EtherIP has no protection for message integrity. It also lacks confidentiality. The Soft Ether program of VPN and the network stack of Free BSD has introduced the Ether IP.

IP-only LAN-like service (IPLS)

The L3 capabilities are already present in the CE devices. The IPLS are nothing but the subset of VPLS. The IPLS service in generally provides packets (Simon *et al*. 2015). They don't provide any frames. The IPLS typically supports the IPV6 or the IPV4.

PPVPN architectures of OSI Layer 3

The segment in generally discusses the central structures of the PPVPNs. In this part, the PE makes a disambiguation for a duplicate address in a single routing service. In another case, the PE does have a virtual router in every VPN. In the standard approach, its variants, have got the maximum attention.

The PPVPN frequently involves many challenges. Such challenges include different customers who are using the address space in common. Such joint space includes the IPv4 address space. The provider should have the ability for disambiguating the addresses of overlapping nature (Stokes *et al*. 2014). Those overlapping addresses will be in the PPVPNs of the multiple customers.

Signal Hiding Methods: The various types of signal hiding include the following:

1. **MPLS/BGP PPVPN-** RFC 2547 defines this method in which the BGP extensions broadcast the routes present in address group of IPv4 VPN, that are comprises of 12-byte string, which begins from a Route Distinguisher (RD) of 8-byte while ends with an address of 4 byte IPv4. The main purposes of RDs are to authorize the duplicate addresses in the same PE.

The purpose of PEs is to investigate the topology of every VPN, which gets interconnected with the tunnels known as MPLS, in a direct way or with the help of P routers (Sundarrajan *et al*. 2014). The MPLS consists of Label Switch Routers and P routers beyond VPNs consciousness.

2. **PPVPN Virtual Router-** As hostile to BGP/MPLS methods, the Virtual Router architecture do not need any modification in the pre-existing protocols of routing such as BGP. With the help of logically autonomous routing domains, a VPN that the consumer acts is wholly responsible for the space of

address. There are several MPLS-tunnels, which comprises of various PPVPNs that are authorized by their label, and they do not need any distinguisher for routing.

Unencrypted Tunnels

Few virtual networks are present which are not using the method of encryption to protect and to bring privacy to their data (Van Der Merwe *et al*. 2014). The VPNs provides security by with the help of an unencrypted network overlay, which not suitable for the trusted or secured arrangements. For example, using Generic Routing Encapsulation (GRE) for performing a tunnel set up between two hosts may comprise of a virtual private network, which is not secure and trustworthy.

The method of resident plaintext protocols for tunneling which consists of Layer 2 Tunneling Protocol (L2TP) while performing the construction without including the Microsoft Point-to-Point Encryption (MPPE) or Point-to-Point Tunneling Protocol (PPTP) and IPsec.

Entrusted networks for delivery

The entrusted VPNs are not using the method of cryptographic tunneling and instead of that, they depend on the individual provider's network for protecting the traffic.

- Layer 2 Tunneling Protocol (L2TP), known as a principles-oriented substitution, and which involves in captivating the appropriate characteristics from each of the two healing VPN protocols namely as Cisco’s Layer 2 Forwarding (L2F) (which becomes obsolete after 2009) and the Microsoft’s Point-to-Point Tunneling Protocol (PPTP) (Wijnands *et al*. 2015).
- The VPNs are overlaid by the Multi-Protocol Label Switching (MPLS) which consists of quality-of-service control upon a reliable delivery network.

From the security point of view, VPNs either need to enforce the security within the VPN mechanism or trusts the major delivery system. If the trusted delivery systems do not run on the physically secure sites only then both the safe and trusted techniques, require a mechanism for authentication for the users to obtain the right to use the VPN.

Use of VPNs in mobile surroundings

Mobile VPNs are set up in such a way that the endpoint of the VPN is not configured to an individual IP address though they move crosswise in different networks comprises of networking data between multiple Wi-Fi access points and also from cellular carriers. The mobile VPNs are used for bringing the public security, in which they offer law prosecution officers the approach to the serious mission operations, including the criminal databases and computer-assisted dispatch during their travel between various subnets present in the mobile network (Van Der Merwe *et al*. 2014). Mobile VPNs also plays a crucial role in the field of service management and are also used by healthcare organizations and other industries.

Recently, the mobile professionals are also adopting the use of mobile VPNs, as they require some stable connections. The uses of mobile VPNs are increasing as they help the users to roam in a seamless manner through the overall networks available. During the incoming and outgoing from any wireless exposure, mobile VPNs are used which helps in continuation of the application session without any losing or reducing of the secure VPN session. A conservative Virtual Private Network is unable to stay alive on these types of events since the overall tunnel of the network is disturbed, which results in a time out, disconnection, failure of applications, or even results in damage to the computing devices.

As an alternative to logically connecting the physical IP address with the endpoint of the network, each tunnel of the system is connected with a fixed IP address within the appliance. The purpose of software in mobile VPN is to maintain the sessions of the network in a transparent manner between the user and the application and also to handle the basic network authentication (Stokes *et al*. 2014). From the learning by the Internet Engineering Work Force, it is evident that the Host Identity Protocol (HIP) is prepared for supporting the flexibility of host by differentiating the work of IP address to identify the host from their performance locator available in the network of IP. With the help of HIP, a host of a mobile can maintain their rational connection, which is recognized through the host identification identifier during the connection with various IP addresses while meandering among the right to use the network protocols.

Use of VPN on Routers

The use of VPN is increasing day by day, and many people are focusing on the implementation of VPN connectivity o their routers for bringing some extra security and for encryption of data communication by different types of cryptographic methods. After fixing the Virtual Private Network services within a router, it will enable the attached device(s) to employ the Virtual Private Network when it gets on. This

technique provides ease in setting up of the Virtual Private Networks on the devices, which does not contain any local Virtual Private Network clients including Gaming Consoles, Smart Televisions, and so on (Simon *et al*. 2015). Implementing the VPNs on the routers also allows in bringing network scalability and enhances the cost savings.

There are many router manufacturers such as Netgear, Asus, and Cisco Linksys those who are supplying routers with inbuilt Virtual Private Network clients. Since the routers are not supporting all the relevant Virtual Private Network protocols including Open Virtual Private Network, many of these manufacturers provide their router with substitute open source firmware, which comprises of Tomato, Open WRT, and DD-WRT, and they support a multiple numbers of VPN protocols including the Open VPN and PPTP.

Limitations: Not all the routers are well matched with open source firmware. They depend on inbuilt flash memory and processor. Firmware such as DD-WRT requires Broadcom chipsets and a minimum of 2MB flash memory. Setting up of VPN services on any router it is necessary to have an in-depth information of network safety and proper fixing. Small disarrangement of any Virtual Private Network connection can make the network vulnerable (Si *et al*. 2014). The performance depends on the ISP of the VPN connections and their reliability.

Networking Limitations

One of the key drawbacks of conventional VPN is that they do not allow connecting or supporting the transmitting domains and are point-to-point in nature. Hence, the communication and software networking, which are dependable on broadcast packets and layer two, including the NetBIOS that the Windows networking uses. These factors do not entirely support or work accordingly since they would be on a real Local Area Networkv (Shokhor and Shigapov 2013). Modifications to Virtual Private Network including the layer two tunneling protocols and Virtual Private LAN are prepared for overcoming these sort of limitations.

A VPN is usually a virtual version of a safe, secure form of physical network, which comprises of a web of computers that are connected for sharing the files and various resources. VPNs also connect itself with the outside world with the help of Internet and which in turn allows securing the normal Internet traffic in accumulation of corporate assets.

Implementation of the Star Methodology

The section is going to discuss the VPN's Implementation Technique, which allows to track the landmark for this particular project, enhances the easiness of literary creation and generalization of the deployment processes.

Figure: Diagram of Star Topology

In the case of Star topology, all the different networking components are linked with an intermediate device known as "hub." It might be a switch, a hub, and even a router. Every workstations are connected to intermediate device by the help of point-to-point attachment in the star topology. For this reason, every computer is not directly attached to each and every node with the help of "hub".

All the data present the star topology goes through the central-device before getting to the actual destination (Salaam *et al*. 2013). The centre serves as a connection for connecting the various points available in the Star Network and also controls and manages the overall networking structure. "Hub" acts as an indication booster or repeater taking the help of central device it is using. The intermediate devices also get the opportunity to communicate with the other available hubs of different networks. For connecting the workstations to the central node, it is necessary to use Unshielded Twisted Pair (UTP) Ethernet cable.

Benefits of Star Topology

- Bus Topology is not providing a better performance as that of Star topology. The signals do not gets transmitted necessarily through all the workstations. A sent signal reaches the actual destination after going through 2-3 links and 3-4 devices. The basic performance of the network totally depends upon the volume of the central hub (Sahai and Waters 2014).
- In a star topology, there is no difficulty while connecting the current devices or nodes. Without affecting the overall network, the new nodes can be added quickly. In the same way, the components can also be removed in a straightforward manner.
- The use of centralized management in star topology helps in network monitoring. The inactiveness of any single link or point does not influence the overall networking structure. It is quite easy for troubleshooting and detecting the breakdown at a particular moment.

Demerits of Star Topology

- Very much dependency is there in the mid-device, which is one of the drawbacks of a star topology. If it becomes inactive, then the overall network gets a failure.
- The using of a switch, a router, or a hub as an intermediate device enhances the regular price of the network structure (Sajassi *et al*. 2014).
- The presentation and the number of nodes that are integrated into these types of topologies are very dependent upon the capability of the fundamental device.

Pre-Implementation

Different steps that are available in this pre-implementation phase will start soon after the acceptance and delivery of this particular project.

Acquisition of the hardware and requiring software are dependent on the suggested solution series present in the suggested Virtual Private Network Software and Elements. Additional components including the hubs and cables are enlisted as the duties of iBasis (Pati *et al.* 2014).

The resolution, which is recommended, implements the 168-bit encryption present in the Cisco 7120 router and the listing needed for good encryption IOS software need to be completed while the process of purchasing the software.

Development and Plan acknowledgment

I am going to give the Badiepa Solution Limited Company two separate output for ensuring the suggested solution which is repeatedly experienced and customized to fulfill iBasis's needs. The deliverables for the Badiepa Solution Limited Company includes:

1. **Test Plan-** I am going to develop a test plan for verifying the functionality of the suggested VPN solution. iBasis is going to validate and review the test plan for addressing the expected problems which were not seen before by REALTECH (Mullick *et al*. 2013). Virtual Private Network test structure typically consists of user structure testing and network structure testing. The overall test arrangement comprises of:

- The IP connectivity from the network systems to the user systems
- Functions of VPN authorization
- Connectivity between VPN client and VPN router
- VPN users' system ability for browsing Network Neighborhood
- Virtual Private Network Client NT login domain
- Virtual Private Network Session expiry on timeout

2. **User response plan-** The Badiepa Solution Limited Company's employee is going to find six test users those who are going to use the VPN solution. The six test users are necessary to be present for ensuring the entire test of this result (McDyson 2013). With the completion of the six criteria, the user installs and configures the Virtual Private Network Client software and then they are asked to fill up a response questionnaire. The total response questionnaire, the distribution and collection techniques will be developed to maintain a partnership with BSLC for maximizing the overall efficiency of this system.

Configuration of Sample Structure

While the implementation process, the sample structure arrangement, and settings is to be done depending on the following fundamentals:

1. **Cisco-Catalyst 6509-** It is necessary to reverse a switch-port on both the external and internal Virtual Local Area Networks present within the Catalyst 6509 for replacing the Cisco 7100 router. The tasks of the port are needed to be done by the iBasis IT staffs (Liyanage *et al*. 2016). These ports are ultimately configured manually by setting up of 100 Mb full duplex also to fast port permit.

2. Cisco 7120 Router- The configuration of both the internal and external Fast Ethernet need to be interfaced with IP addresses (as given by iBasis) on the router and overall description regarding the interfaces need to be there. The configuration of the router is done for client commenced VPN access. It comprises of the ISAKMP transform map, the client dynamic map with full authentication, the formation of the internal VPN IP address pool, and the IPSec encryption algorithm. The iBasis IT staffs need to provide the network address range, and it shall comprise of a total class C network. The Xauth for authenticating the access required by the user uses TACACS+. A Cisco Safe Server is going to handle these TACACS+ authentication requirements (Liyanage and Gurtov 2013). The Cisco Safe Server is going to perform an investigation with the help of NT domain SAM databases for the justification of request. The routing for the internal interfaces will be handled by the OSPF, which insists the VPN traffic throughout the internal network. A static route is going to perform the routing for the external interfaces. It is going to point to the HSRP address present in the exterior routers.

3. **Cisco Virtual Private Network Client 1.1 security policy-** The REALTECH is going to produce a Virtual Private Network client security policy from a pre-existing Virtual Private Network Security Policy Editor. This security policy is going to serve as a standard procedure for every Virtual Private Network clients (Liu *et al*. 2014). The configuration of safety policy editor comprises of the following:

- Addition of new policy for connection
- Configuration of Safe Gateway Address
- Configuration of customer's identification
- Configuration of pre-shared key
- Configuration of authentication request
- Shape of key exchange request
- Shape of key exchange request
- Configuration of SA lifetimes for permitting for timeout session

- ❖ Configuration of encryption techniques and authentication

Completing the overall setup, the Virtual Private Network policy is going to save safely in a file and the file is going to be conveyed and uploaded into the other Virtual Private Network clients (Le Roux *et al*. 2013).

4. **'Sign off' and Inspecting drafts-** The inspecting drafts and 'sign off' is the ultimate phase of the procedure of documentation before the allocation to the test users. The document is going to be reviewed by iBasis and accordingly they will offer feedbacks/comments to REALTECH. Later on, the consideration of the comments and implementation of any diversity, the documents is going to be circulated among the test users at the time of deployment of the project. The feedbacks and comments of iBasis are going to be included in the user handbook (Koushik *et al*. 2014). At the end of the documentation, the final changes are made, both the REALTECH and iBasis are going to 'sign-off' based on the available manuscript and make it prepared for delivery.

Formation of CBT

CBT is going to be developed for providing VPN client training to the IT users. The training department of the organization also to engineers of Badiepa Solution Limited Company is going to perform intimately with the help of IT for customizing the CBT. Later on, the user handbook is formed, and then the BSLC's Training Department will be creating an active planning of the project depending on the sources that are required for the completion of the task.

For developing the security model, it was necessary to choose a prototype methodology. With the help of that method, a working prototype of the particular model has been designed for checking the functional effectiveness and efficiency of conception, before setting up the actual system (Kothari and Fernando 2012). The working prototype undergoes several changes during the various developmental stages, and ultimately the finalized model is deployed with the final operational system.

While the designing of this prototype model the following tasks are done:

i. Congregation of requirements

ii. Probability Lessons

iii. System Study

iv. Design of Software

v. Testing and Coding

vi. Addition as well as Execution

Chapter 3. Design and Analysis

3.1 Introduction

Design and analysis play a crucial role in conducting any technological project since the overall ideas produced from some comprehensive survey of the pre-existing fictional works are considered to be of enormous support to develop the model designing that could necessarily serve the project purpose. The extensive ranges of fictional works that have been analyzed in this project were significant in the process of constructing the VPN models (Klein *et al*. 2012). This VPN model in turn reduce the vulnerabilities of the wireless networks comprising of security attacks and several threats that are always made by the intruders. There is no need to say that the deployment of such a model would be beneficial in hampering the hostile tasks that are done by the invaders.

The discussion regarding the designed prototype is present in the following section which tries to reduce the susceptibilities of the wireless network structures.

3.2 Efficient and non-efficient needs

3.2.1 Efficient needs

The economic needs of the systems that are prepared by reducing the sensitivity of the wireless networks of several attacks and threats are mentioned in this section:

1. Management of Conduct: The available system need to check the efficiency of the scheme (Khanna *et al*. 2012).

2. Composition Management: The available system need to work properly while doing composition management of the network.

3. Network usage management and account management: The available system needs to concentrate on the management of account and the management of the usage of the network.

3.2.2 Non-efficient needs

The non-efficient needs of the overall system are discussed in the below unit:

1. Wrong administration- The available system need to identify each and every problem that are going to occur while experiencing the wireless networks. The proposed system is required to solve the problems by fixing those challenges and need to organize reports regarding those circumstances (Kamite *et al*. 2014). The proposed system also needs to keep records of the defects that were identified.

2. Protective administration- the Protective management is also a non-efficient need for designed system. The structural administrator needs to bring changes in the warm settings of the system in such a way that the network resources perform well on the deployed security guidelines by the production institution.

3. With the help of designed system, the security management needs to recognize those resources which are essential for the good performance of the wireless network. Determination of resources plays a crucial role in helping the management team to allocate the convenience of user resources.

4. The designed system needs to provide the customers with the power to connect several nodes present in the system (Hines *et al*. 2015).

3.2 Discussion regarding the Investigation with Confirmation

Different types of security models are prepared which fundamentally fulfill the needs of the systems by considering the different efficient and non-effective needs.

The various security models need to provide the core functionalities which includes performance management of the different access nodes for ensuring the protection of the overall wireless network. The tasks that are connected with the overall performance controlling of the network which consists of the dimensions of the average levels of access needs or data requirements that the network user is requested (Hasan 2014). The measurement of the line operation or controlling the active user response times which allows the recognition of different wireless performance.

The functionality of composition management is related to the safeguarding of the overall inventory of network with exact configuration of the wireless network structure. The saved information of this process would be beneficial in the discovery of several issues, which might occur because of the problem of interoperability of the structure (Gorbunov *et al*. 2014).

The accounts administration is necessary for measuring the amount of information or data that the user of the system uses. It is also a need for keeping the records of the total billable amount required for such

reasons. Appropriate administration of the account assures the fact that all the network resources are working effectively as a whole, and no uneven access point is in used within the secured network.

Hence, by the findings described by experienced researchers doing research in this particular field, it is quite evident that the safety structures need to apply the previous performance (Gong *et al*. 2013).

During the conduction of the literature review, we came to several resources, which illustrated that the use of cloud services could be beneficial in securing the wireless connections. Hence, it is fixed that the formation of data storage by the business association, maintaining the backup of data and calculating the data access would ultimately execute by the Cloud-oriented service provider such as SAS.

Project Designing

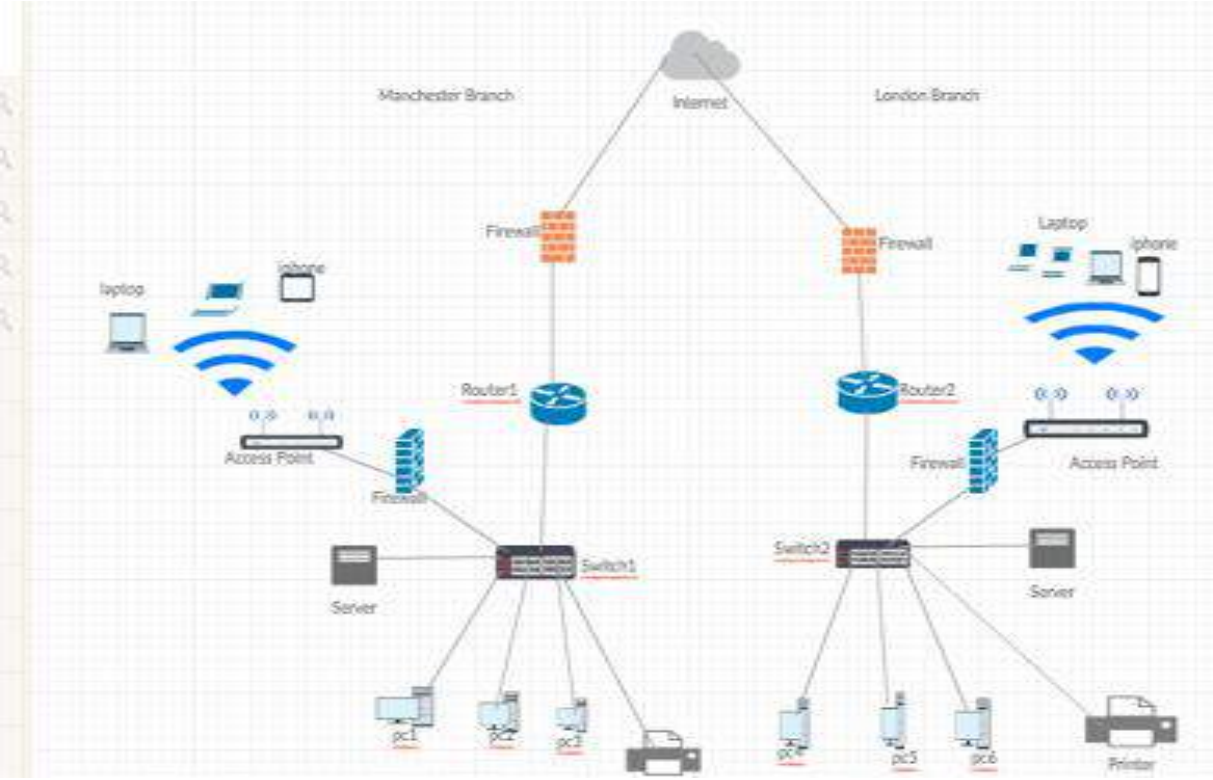


Figure: Network related diagram

In the above illustration, a free designing of the network security model is done which would offer protection to the Virtual Private Networks. It was stated earlier that the application servers would not be given the advantage of accessing any sensitive data, and which in turn would allow protection against the hacking. The overall network is confined with the help of a firewall, which would not the outside access to the data that are being gathered and transported through the network (Goldwasser *et al*. 2013).

Double authentication would be implemented for securing the access points to make sure only the authorized users could get the network access.

Chapter 4: Implementation and Development

The second stage comprises of implementation. This particular stage deals with the configuration and installation of the apparatus in integration to the allocation of software for clients to the users of six tests. After the completion of the apparatus arrangement, a testing session will be organized on the trial plan prepared in the first stage. Different types of questionnaires are going to be collected after the completion of screening for review (Figueira *et al*. 2013). At the end of this point, the CBT, as well as the user manual, will be totally finished and need to be prepared for distribution.

Configuration of Hardware

The essential hardware materials will be installed on the construction network with minimal effect on the system of iBasis. The necessary hardware configuration comprises of escalating of the Cisco apparatus, connecting the router to both the internal and external Fast Ethernet networks (which is in a parallel position to the pre-existing PIX firewall) and insertion of latest ISM module.

Structure arrangement

With the help of the sample configuration document present in the Pre-implementation, all the systems are going to be configured. The system that requires settings are as follows:

- Cisco Secure Server
- Cisco 7120 Router
- Cisco Catalyst 6509
- Configurations of user laptop

Testing

Based on the developed test plan during the pre-implementation, a test will be performed for the client initiated VPN solution. For the validation purpose, the test will be carried out under the guidance of BSLC's staffs. Then I will check the validity of the trial after its completion (Dutta and Kwok 2013). Finally, the personnel of iBasis test will give a signature after the completion of all the tests present in the test plan.

Post-certification

After the conclusion of this project, I am going to submit the certification to iBasis. Then I am going to obtain two paper, which will contain the following:

- Synopsis of the project targets and job completed
- VPN network solution related logical diagram(s)
- Stock of installed hardware components comprising of warranty contracts, part numbers, and serials
- Both soft copies and hard copies of router configurations and customized switches
- Descriptions and Snapshots of VPN client structure
- Details of laptop structures
- Details of customized server configurations
- User concurrency testing inventory and sign-off (Dimitri *et al*. 2013)

Deploy rollout maintenance

The engineering staffs of Badiepa Solution Limited Company belong to on-site controlling network presentation and answering to any problems, which is raised by the workers of BSLC. A standard post-rollout maintenance comprises of BSLC engineer for at least two years (4 hours per day) as an on-site after rollout and is going to be dependable to resolve network connectivity related problems and any other increasing problems.

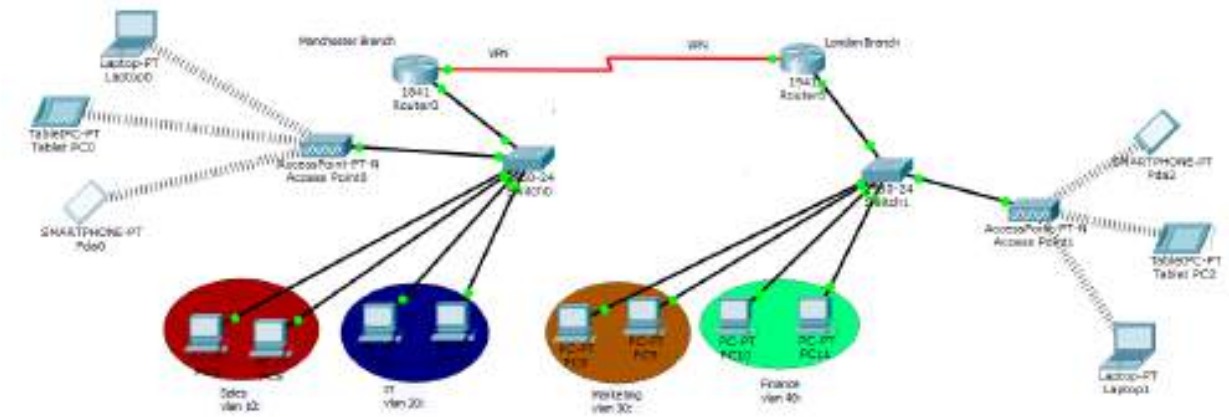


Figure: Operational model of the project present in packet tracer

As WEP encryption separately unable to guarantee the network's security or the different types of information that are transferred through the network (Das *et al*. 2016). For this reason only, the intruders need to cross a large number of hurdles for gaining the access towards the information, which is quite useful in different security models. Hence, the same technique has been taken in this particular case. A dual way of authentication security structure has been developed for securing the structure from any hateful behavior of the attackers or invaders. The purpose of the secured application gateway is to allow the authorized users with the access to the nodes present in the wireless security structures. On the other hand, the validation from the side of user assures that the person involved in making requests for promoting the use of the wireless network is a legitimate user (Chen *et al*. 2014). The next part of the authentication procedure is deployed by using a password system and secured ID. With the proper use of these two pieces of information, the users need to validate themselves in the well-designed security system.

Chapter 5. Testing of the Project Evaluation

The designed system needs to be subjected to the below-mentioned testing procedures for gaining surety about the enhanced security levels of the VPN system. They are as follows:

1. Risk Designing: Different types of components available in the overall system are taken into account for estimating their different susceptibility to protection threat.

2. Saturation Testing: The overall network security system is reviewed for ensuring the highest level of safety present in the network, which is termed as saturation network process (Cai *et al*. 2014). The different types of applications that runs on the wireless networks are known as the application penetration test.

3. The various kinds of cookies and information are being stocked on the available devices which are directly connected to the wireless network require being tested in an orderly manner for testing the efficiency of system security.

Chapter 6.

6.1 Short Description

This section comprises of a brief description regarding the schedule that is related to the project progression.

6.2 Gantt Chart

The overall project is going to proceed in the following manner:

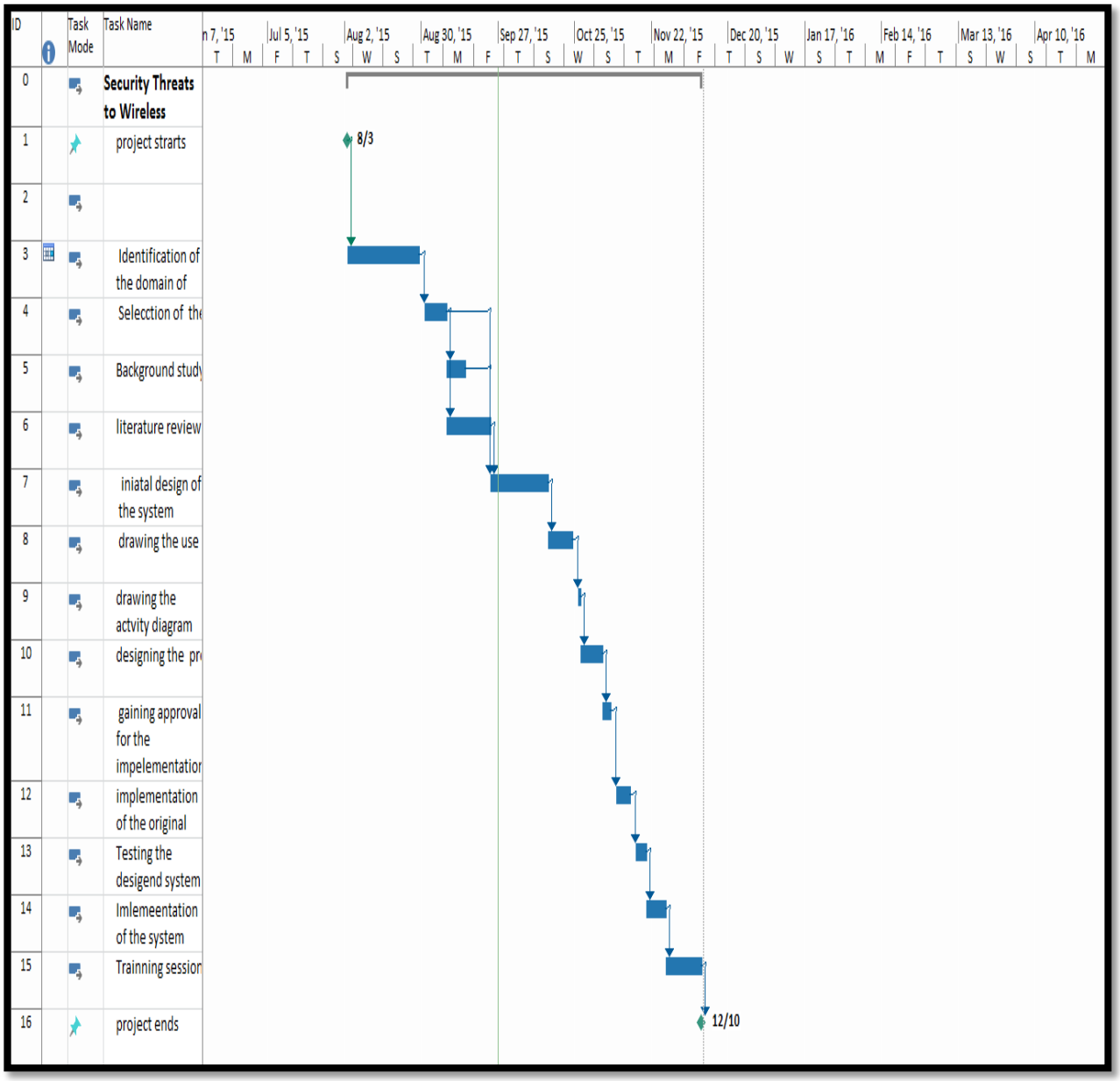


Figure: Gantt chart Representation

Project Presentation in Power Point

SCHOOL OF TECHNOLOGY
HND PROJECT

Student Name:KOUKO GAKPO
Student ID: P1021694

Project Title: Creation of a Virtual Private Network Link (VPN) between two local area networks (lan)

Pathway: HND-Network Engineering and Telecommunications (NETS)

TABLE OF CONTENTS

- Introduction
- Aim and Objectives of project
- Description of the problem
- Proposal
- Solution
- Literature Review
- Investigation and designing
- Deployment and Testing

DESCRIPTION OF THE OVERALL PROBLEM

- For establishing the most secured way of data exchange communication between London and Manchester offices

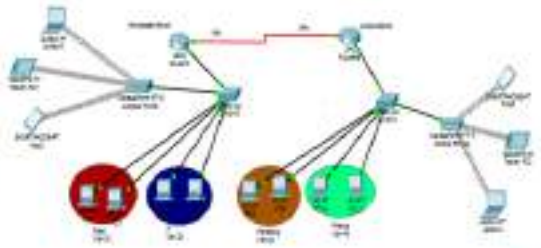
PROPOSAL

Virtual Private Network

Virtual Private Network (VPN) is a very safety point-to-point networking technology which provides safe and secure remote access to any private or public networks. The VPN are using TCP/IP tunneling protocol for having a secured transmission of the available data.

SOLUTION

- **Model of the project work in packet tracer**



LITERATURE REVIEW

A plenty of existing literary articles were checked for conducting a overall study in the domain. The pre-existing methods and structures that are presently being used for ensuring the (Virtual Private Network) VPN which has been studied in depth for understanding the ground level technology that has been used.

The topics that were checked includes:

- Layer 2 Tunneling protocol
- IP security
- Transport Layer Security

INVESTIGATION AND DESIGNING

- Investigation and Designing is regarded as one of the vital section for organizing a technical project, as the thought that are prepared from the exhaustive survey of the pre-existing literary tasks are established to be of immense support during the development of the model designing which could be suitable for the project. In this particular project, a variety of literary works have been checked and also have been significant in the designing process of VPN

DEPLOYMENT AND TESTING

The designed system is subjected to the various testing procedures including the following:

- Validation: for ensuring the user validation
- Point-to-point encryption: For ensuring that information will not be shared or accessed by any third-parties
- IP address protection: For making sure that incoming and outgoing of data is encrypted in a proper manner

NETWORK DEPLOYMENT DIAGRAM FOR THE SUGGESTED SOLUTION

- Wide Area Network with VPN point-to-point link

Chapter 7. Features Works and Constraints

Features Works

As this project is not completed at the college, I am compelled to visit the University for a remarkable Grade in the significance of having a remote on the usage of packet tracer plot I was unable to finish as the time given to me at the college was not sufficient (Brakerski and Vaikuntanathan 2014). After the completion of 2 years at this college, I can grasp a sound knowledge, and I have prepared a good base on the Network Telecommunication topic. This knowledge, in turn, will brush up my mind with valuable knowledge regarding the Network Telecommunication and with the help of this important intellectual baggage I can able to get a good job in future. Since my objective is to work with the large bank square like Barclays Bank Plc. and hence, this study will open up better opportunities for me

(Brahim *et al*. 2012). For achieving this goal, I need to work very hard at the University in all the units that the professor will present to me.

Limitations

While I was doing my project in the college, there was some personal problem occurred and I was submerged later on. The problem was I did not have enough time to focus on the given project, I need to drop my children at school and pick them up after the school, and I have to work at night. This situation occurred due to plenty of workloads and for an attitude. The primary reason for my overflow feeling was much more to work on. While staying at Saint Patrick's College for the two long years, I have excellent knowledge and education in the technological field. Right now I am well concerned about the study of Network Telecommunication (Bragg *et al*. 2015). The project, which I gave on my own, was not sufficient to reach my expected grade. The stipulated time for the completion of the project was not enough. I was unable to use the Packet Tracer in a correct manner after practicing with my friend and even with my researches. Due to the lack of time, this project cannot be finished in college within time since I need to learn many things to complete this project, which I have not studied during my two years course in college. After the completion of my research activities, I met with lecturer Mr. Alan, who have helped me a lot in focusing on the configuration of packet tracer. I need to finish this project topic within one year in University.

End meeting

The end meeting achieves the phase 1 of the VPN project solution. The primary requirement of this meeting is to make an ending summary of the overall plan, and a post-documentation is presented to the engineers of Badiepa Solution Limited Company.

8. Conclusion

The organization often requires the necessary versatility to support the unknown future. The equipment that needed is usually of multivendor type. Here IPSec is recommended by I. The IPsec can provide the organization with three components which are essential (Unnimadhavan *et al.* 2016). They are essential in the VPN connections of security which comprises of tunneling, encryption, and authentication of packets.

The selected protocols of encryption based on the security level that is required. The laws imposed by the government for import and export of the technology also determines the selected protocol. The 128-

bit strong encryption either used or not will decided by the sensitivity of the information for transportation. There can be a measurement of performance for the security level. The standard of security should not increase to a point where the security transmission's performance can degrade in a substantial manner (Border *et al*. 2015).

There is an essential factor which defines the solution in the creation of VPN back again in the United States. Such factors are the International iBasis offices. The United States government initiated relaxations in the regulations of exporting its 128-bit encryption technology. In such cases, Badiepa Solution Limited Company always keeps their eye with the laws governing in other countries. Due to this reason, implementation of minimal bit size key used for encryption and decryption has been decided (Baum and Voit 2012). The 3DES and DES methods of encryption are allowed to the usage of IPSec and the product line of Cisco.

References

Abramson, S. and Sinha, R., Avaya Inc., 2012. *Social network virtual private network*. U.S. Patent 8,332,476.

Aggarwal, R., Kamite, Y., Fang, L., Rekhter, Y. and Kodeboniya, C., 2014. Multicast in Virtual Private LAN Service (VPLS). *Internet Request for Comments*, *vol. RFC*, *7117*.

Asati, R., Khalid, M., Cherukuri, S., Durazzo, K.A. and Murthy, S., Cisco Technology, Inc., 2014. *Integrating service insertion architecture and virtual private network*. U.S. Patent 8,650,618.

Baum, R.T. and Voit, E.A., Verizon Communications Inc., 2012. *Methods, apparatus and data structures for preserving address and service level information in a virtual private network*. U.S. Patent 8,243,627.

Border, J., Dillon, D. and Pardee, P., Hughes Network Systems, Llc, 2015.*Method and system for communicating over a segmented virtual private network (VPN)*. U.S. Patent 8,976,798.

Unnimadhavan, S., Bandlamudi, V.K., Adhya, T.K., Vadivelu, J. and Viswanathan, A., ARUBA NETWORKS INC., 2016. *DISTRIBUTED VIRTUAL PRIVATE NETWORK*. U.S. Patent 20,160,036,700.

Bragg, N.L., Allan, D., Smith, P.A. and Ungehagen, P., Rockstar Consortium Us Lp, 2013. *Resilient provider link state bridging (PLSB) virtual private LAN service (VPLS) interworking*. U.S. Patent 8,565,244.

Bragg, N.L., Allan, D., Smith, P.A. and Ungehagen, P., Rpx Clearinghouse Llc, 2015. *Resilient provider link state bridging (PLSB) virtual private LAN service (VPLS) interworking*. U.S. Patent 9,100,316.

Brahim, H.O., Allan, D. and Mohan, D., Rockstar Bideo LP, 2012. *Method and apparatus for interworking VPLS and ethernet networks*. U.S. Patent 8,144,715.

Brakerski, Z. and Vaikuntanathan, V., 2014. Efficient fully homomorphic encryption from (standard) LWE. *SIAM Journal on Computing*, *43*(2), pp.831-871.

Chen, M., Liu, Z., Paul, M., JOUNAY, F., Kamite, Y., Kunze, R., Key, R. and Jin, L., 2014. Extension to LDP-VPLS for Ethernet Broadcast and Multicast.

Chen, R., Cai, D., Liu, Z., Salam, S. and Jin, L., 2014. Redundancy Mechanism for Inter-domain VPLS Service.

Chen, Z., Thangavelu, A., Xiang, D. and Yanjun, Y.A.N.G., Sonicwall, Inc., 2014. *Virtual private network dead peer detection*. U.S. Patent Application 14/150,537.

Das, S.K., Samantray, A.K. and Patra, S.K., 2016. Hybrid crosstalk aware Q-factor analysis for selection of optical virtual private network connection.*International Journal of Electronics*, *103*(1), pp.113-129.

Dimitri, P., Belotti, S., Ceccarelli, D., Tochio, Y., Fedyk, D. and Zhang, F., 2013. Applicability Statement for Layer 1 Virtual Private Network (L1VPN) Enhanced Mode.

Dutta, P. and Kwok, P., 2013. MAC Flush Loop Detection in VPLS.

Dutta, P., Balus, F., Stokes, O., Calvignac, G. and Fedyk, D., 2014. *LDP Extensions for Optimized MAC Address Withdrawal in a Hierarchical Virtual Private LAN Service (H-VPLS)* (No. RFC 7361).

Figueira, N.R., Liaw, F. and Gitlin, R.D., Brixham Solutions Ltd., 2013.*Mapping PBT and PBB-TE traffic to VPLS and other services*. U.S. Patent 8,619,784.

Figueira, N.R., Liaw, F. and Gitlin, R.D., Brixham Solutions Ltd., 2013.*Mapping pbt and pbb-te traffic to vpls and other services*. U.S. Patent Application 14/050,067.

Ghosh, K., Juniper Networks, Inc., 2013. *Forwarding multicast packets in a VPLS router on the basis of MAC addresses*. U.S. Patent 8,576,844.

Gong, L.H., Liu, Y. and Zhou, N.R., 2013. Novel quantum virtual private network scheme for PON via quantum secure direct communication.*International Journal of Theoretical Physics*, *52*(9), pp.3260-3268.

Gorbunov, S., Vaikuntanathan, V. and Wee, H., 2015. Attribute-based encryption for circuits. *Journal of the ACM (JACM)*, *62*(6), p.45.

Hasan, S., Juniper Networks, Inc., 2014. *Handling switchover of multi-homed connections in VPLS networks*. U.S. Patent 8,780,699.

Hasan, S.S., Juniper Networks, Inc., 2014. *Extending VPLS support for CE lag multi-homing*. U.S. Patent 8,705,526.

Hines, M., Malas, D., Miles, J. and Ratterree, G., Level 3 Communications, Llc, 2015. *System and method for providing network services over shared virtual private network (VPN)*. U.S. Patent 9,077,587.

Kamite, Y., Fang, L., Rekhter, Y. and Aggarwal, R., 2014. Multicast in Virtual Private LAN Service (VPLS).

Khanna, S., Medikonda, R. and Dillon, G.D., Tellabs Operations, Inc., 2015.*Method and apparatus for media distribution using VPLS in a ring topology*. U.S. Patent 9,083,551.

Klein, D., Pries, R., Scharf, M., Soellner, M. and Menth, M., 2012, June. Modeling and evaluation of address resolution scalability in VPLS. In*Communications (ICC), 2012 IEEE International Conference on* (pp. 2741-2746). IEEE.

Kompella, K., Juniper Networks, Inc., 2012. *Inter-autonomous system (AS) virtual private local area network service (VPLS)*. U.S. Patent 8,125,926.

Kothari, B. and Fernando, R., Juniper Networks, Inc., 2012. *Virtual private local area network service (VPLS) flush mechanism for BGP-based VPLS networks*. U.S. Patent 8,170,033.

Koushik, A.K., Mediratta, R. and Nadeau, T., 2014. Virtual Private LAN Service (VPLS) Management Information Base.

Kshirsagar, S. and Thomas, C.N., Juniper Networks, Inc., 2012. *Application-specific network-layer virtual private network connections*. U.S. Patent 8,095,786.

Le Roux, J.L., Decraene, B. and Transy, E., 2013. *System for securing the access to a destination in a virtual private network*. U.S. Patent 8,379,511.

Liu, Z., Jin, L., Chen, R., Cai, D. and Salam, S., 2014. *Redundancy Mechanism for Inter-domain VPLS Service* (No. RFC 7309).

Liyanage, M. and Gurtov, A., 2013, April. A scalable and secure VPLS architecture for provider provisioned networks. In *Wireless Communications and Networking Conference (WCNC), 2013 IEEE* (pp. 1115-1120). IEEE.

Liyanage, M., Gurtov, A. and Ylianttila, M., 2016. Improving the Tunnel Management Performance of Secure VPLS Architectures with SDN. In *Proc. of IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, USA. IEEE*.

McDysan, D.E., Verizon Business Global Llc, 2013. *System, method and apparatus that isolate virtual private network (VPN) and best effort traffic to resist denial of service attacks*. U.S. Patent 8,543,734.

Mullick, A., Nanjundaswamy, S. and Soni, A., Citrix Systems, Inc., 2013.*Method and appliance for authenticating, by an appliance, a client to access a virtual private network connection, based on an attribute of a client-side certificate*. U.S. Patent 8,413,229.

Pati, M., Salam, S., Patel, K. and Sajassi, A., Cisco Technology, Inc., 2014.*Managing active edge devices in VPLS using BGP signaling*. U.S. Patent 8,743,886.

Sahai, A. and Waters, B., 2014, May. How to use indistinguishability obfuscation: deniable encryption, and more. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing* (pp. 475-484). ACM.

Sajassi, A., Matsushima, S., Salam, S. and Martini, L., 2014. Inter-Chassis Communication Protocol for Layer 2 Virtual Private Network (L2VPN) Provider Edge (PE) Redundancy.

Salam, S.M., Sajassi, A. and Henderson, S., Cisco Technology, Inc., 2013.*Connectivity fault management (CFM) auto-provisioning using virtual private LAN service (VPLS) auto-discovery*. U.S. Patent 8,385,353.

Shokhor, S. and Shigapov, A., F5 Networks, Inc., 2013. *System and method for dynamic policy based access over a virtual private network*. U.S. Patent 8,560,709.

Si, X., Cui, T. and Wang, Q., Oracle International Corporation, 2014. *System and method for allowing virtual private network users to obtain presence status and/or location of others on demand*. U.S. Patent 8,804,928.

Simon, F., Hanika, J. and Dachsbacher, C., 2015, May. Rich-VPLs for Improving the Versatility of Many-Light Methods. In *Computer Graphics Forum* (Vol. 34, No. 2, pp. 575-584).

Stokes, O., Balus, F., Fedyk, D. and Dutta, P., 2014. LDP Extensions for Optimized MAC Address Withdrawal in a Hierarchical Virtual Private LAN Service (H-VPLS).

Sundarrajan, P., He, J., Soni, A., Nanjundaswamy, S. and Kumar, A., Citrix Systems, Inc., 2014. *System and method for establishing a virtual private network*. U.S. Patent 8,726,006.

Van Der Merwe, J., Gerber, A. and Ramakrishnan, K., At&T Intellectual Property I, LP, 2014. *Methods and apparatus to communicatively couple virtual private networks to virtual machines within distributive computing networks*. U.S. Patent 8,705,513.

Wijnands, I., Boers, A., Cai, Y. and Rosen, E., 2015. Multicast Virtual Private Network (MVPN): Using Bidirectional P-Tunnels.