Efficient Usage of Hardware & Software to accommodate New Technology and Establishment of Virtual Private Network

Prepared By:

Akbor Aziz Susom

ID: 2009-2-55-020

Department of Electronics and Communication Engineering

East West University

Supervised By:

Dr. M. Mofazzal Hossain

Professor

Department of Electronics and Communications Engineering

East West University

East West University

Declaration

This report is on the basis of my internship program and its enhancement of studies throughout my project work is submitted to follow the terms and conditions of the department of Electronics and Communications Engineering. This report is the requirement for the successive competition of B. Sc. Engineering in Electronics and Communications Engineering.

I state that the report along with its analysis, research, experimental results and solution that have been demonstrated in this report papers, is my own work with the masterly guidance and fruitful assistance of my supervisor for the finalization of my report successfully.

Signature:

02.09.2014

Akbor Aziz Susom

ID: 2009-2-55-020

Department of Electronics and Communication

Engineering, East West University.

Signature of Supervisor:

02.09.2014

Dr. M. Mofazzal Hossain

Professor,

Department of Electronics & Communications

Engineering, East West University.

Signature of Chairperson:

Gmandal 2/9/14

Dr. Gurudas Mandal

Associate Professor,

Department of Electronics & Communications

Engineering, East West University.

Acknowledgement

Incipiently, I would like to express my profound gratitude and deep regards to Dr. M. Mofazzal Hossain for his guidance and invariable support throughout the project effort. I have successfully accomplished the goal of the project due to his tireless and patient monitoring during the time of my project. I am extremely grateful to him as he gives me the opportunities and exposure that I never would have had if he had not worked with me.

In addition, I take this opportunity to express my deepest appreciation to all the staff of the Robi Axiata Ltd in the division of IT who provided me the ideas and perception of the IT related activities and the issues of networking through the implementation. This practical experience in the corporate environment let me to amass my concepts and knowledge for succeeding my project work .I am also so pleased to all the faculty members of ECE department for their guidance and support for the successive completion of my graduation degree. Similarly, I would like to acknowledge with much appreciation the crucial role of the Lab instructor of networking Lab, who gave the permission to use all required equipment and the necessary materials to complete the task.

Moreover, I would like to thank to all my friends, batch-mates for their companion and lifting me up in any type of situation for their inspirative presence beside me. I would like to pay my homage to my parents who se encouragement and prayer are always with me and moving with me like a shadow of mine which will protect me in any emergency situation. The name without whom my thanksgiving is incomplete is the Almightily Allah, who allowed me to live in this beautiful world.

Thank you all for your great support to me.

Abstract

Nowadays there are lots of efforts are taken for the sake of implementation and establishment to IT & Networking based technology by different concern groups. Here I have shown some practical significance of the VPN network that can be used to secure all types of networking communications. As we can implement this networking facilities through the software and hardware basis , so its implementation can enables us to secure communication not only for any specific Zone but for the remote access of long distance communication also. Based on my project work, I have proposed to establish this networking system in all over the country regarding the security purposes of the Governmental issues, multi-national companies even in the arena of our everyday's communication. Finally, the facilities and the implementation method of these networking issues have been demonstrated to give the overall ideas of this network.

Table of Content

Chapter: 1

Introduction

1.1 Overture to the IT development Division

In the division of the IT development sector where all the activities are related with the innovation and the progression of the IT. It involves not only the activities with the software and hardware implementation and innovation but having lots of technical issues related with the activities of the networking. In the section of the software development where all needed and essential software are implemented precisely as it follow the cloning process and the process Robi calls it Imaging that means to create a disk that is like a software or windows . This software and windows are used by all the users of the robi as well as to maintain their privacy and security, this works need to be implemented successfully. The need for better quality control of the software development process has given rise to the discipline of software engineering, which aims to apply the systematic approach exemplified in the engineering paradigm to the process of software development.

Moreover, Hardware related activities are so sophisticated as it has a different structure, performance and technical issues that should be done accurately. In this sector, all the parts of the computer like Motherboard, Ram, CD-Rom, Hard-drive, Cooling fan, Graphics-Card, Key-board, LCD, Caching, Drivers, need to be known with its operation and structural knowledge. Here, hardware engineers work in multidisciplinary teams and have a deep understanding for adjacent expertise and embedded disciplines. They have a holistic approach to projects meaning faster and better development.

Networking practice is so high in Robi so as to implement some big project with lots of technical and sophisticated accomplishment involving here. Information and communication are two of the most important strategic issues for the success of every enterprise. While today we use a substantial number of computers and communication tools. While managers today are able to use the newest applications, many departments still do not communicate and much needed information cannot be readily accessed. To overcome these obstacles in an effective usage of information technology, computer networks are necessary. At the same time they are the means to converge the two areas; the unnecessary distinction between tools to process and store information and tools to collect and transport information can disappear. Computer networks can manage to put down the barriers between information held on several (not only computer) systems. Only with the help of computer networks can a borderless communication and information environment be built. Computer networks allow the user to access remote programs and remote databases either of the same organization or from other enterprises or public sources. Computer networks provide communication possibilities faster than other facilities. Because of these optimal information and communication possibilities, computer networks may increase the organizational learning rate, which many authors declare as the only fundamental advantage in competition. So as to elaboration of my ideas, I decided to enhance my knowledge and to enact act my ideas through the successive result of my networking by dint of establishing Virtual private Network throughout my project works.

Chapter: 2

Different spheres of IT related activities

2.1 Computer Configuration

Computer configuration is termed complete when all the major functional parts which include hardware and software parts of it get assembled. Proper assembling plays a major role in the performance of the computer. The performance and productivity of a computer completely depends on how smart is your choice of accessories. Before you start using your PC, first you must configure it with all the basic set ups. Basics setups needed for assembling a PC includes the main memory, hard disk drive, card reader, CPU, CD drive, monitor, modem, and definitely a windows operating system. You can always choose your own specifications for your computer configuration. There are many different types of microprocessors available but a computer savvy person will choose the one which works real fast. Other hardware accessories like monitor, keyboard, mouse and speakers should also be configured wisely for better performance.

In case you need to install a new device, game, software or a program you have to configure the system by adding various jumpers for hardware and parameters for software. This feature guides the system to recognize what type of printer or video adapter or any other additional device is connected to the system. In present times highly advanced technology has made computer configuration smooth and easy as almost everything gets configured automatically. Thanks to Plug-and-play technology for this benefit. At times you may need to configure only the hardware or the software but for a start up model you have to configure both. A proper computer configuration needs a lot of research. One cannot just buy whatever is available; there are many processors which are extremely slow but still sold by the dealers to clear stock. One should be aware of what he/she is actually taking home might affect the performance of the system. Low cost of microprocessors has lead to auto configuration. USB is one fine example of it. Configure well to get excellent performance.

- Bios Updating
- Cloning Process
- Bios Security Configuration
- Computer Properties
- Required Software Installation
- Attachment with Domain

2.1.1 Bios Updating

Occasionally, a computer will need to have its BIOS updated. This is especially true of older machines. As new devices and standards arise, the BIOS needs to change in order to understand the new hardware. Since the BIOS are stored in some form of ROM, changing it is a bit harder than upgrading most other types of software.

To change the BIOS itself, you'll probably need a special program from the computer or BIOS manufacturer. Look at the BIOS revision and date information displayed on system startup or check with your computer manufacturer to find out what type of BIOS you have. Then go to the BIOS manufacturer's Web site to see if an upgrade is available. Download the upgrade and the utility program needed to install it. Sometimes the utility and update are combined in a single file to download. Copy the program, along with the BIOS update, onto a floppy disk. Restart your computer with the floppy disk in the drive, and the program erases the old BIOS and writes the new one. You can find a BIOS Wizard that will check your BIOS at BIOS Upgrades.

2.1.2 Disk cloning

Is the process of copying the contents of one computer hard disk to another disk or to an "image" file. This may be done straight from one disk to another, but more often, the contents of the first disk are written to an image file as an intermediate step, then the second disk is loaded with the contents of the image. Typically, this is done for archiving purposes, to restore lost or damaged data, or to move wanted data into a new disk, though other reasons also exist.

Unlike standard copying functions, disk cloning involves copying hidden and in-use files, and thus presents special challenges, as those types of files are typically not available for copying. Additional complications arise when the process is used for networked computers, as the network must be able to distinguish between different computers. Post-cloning operations may be necessary to address these and other issues.

2.1.3 Bios Security Configuration

The security section of the BIOS is used to keep unauthorized people from making any changes to the BIOS. Because settings in the BIOS are so critical to proper PC operation, many offices IT staff chooses to lock out all non-IT personnel by using a password that only IT personnel know.

- **Security Option**: This feature lets you password-protect the BIOS to prevent unauthorized users from making changes. It can also be set to require a password for the

PC to boot up. The options available are Setup or System; this setting controls the options for the parameters below.

- **Set Supervisor Password**: If you choose to select a Supervisor Password, a password will be required to enter the BIOS after you choose setup, as described above. If you choose SYSTEM as described above, then a password will be required for cold-booting, too.

- **Set User Password**: A different password assigned to users is required to boot the PC, and if a Supervisor Password has also been selected, permits the user to only adjust the date and time in the BIOS.

2.1.4 Computer Properties

The process for viewing your computer's properties is relatively the same for Windows XP, Windows Vista, and Windows 7. Find a My Computer or Computer icon (sometimes on your desktop or in your Start menu) and right click it. Then, go to Properties to open a new window. In Windows Vista and Windows 7, additional information is found in the System section. Next to System type, you may find a note about either a 32-bit Operating System or a 64-bit Operating System. It is important to know what version is installed on your computer for software compatibility reasons. Many software applications can run in either a 32-bit or 64-bit version of Windows, but there are some programs that are written specifically for use on 64-bit versions only. Knowing what type of operating system can help determine if a certain software application will run on your computer.

The Device Manager is a Control Panel applet in Microsoft Windows operating systems. It allows users to view and control the hardware attached to the computer.

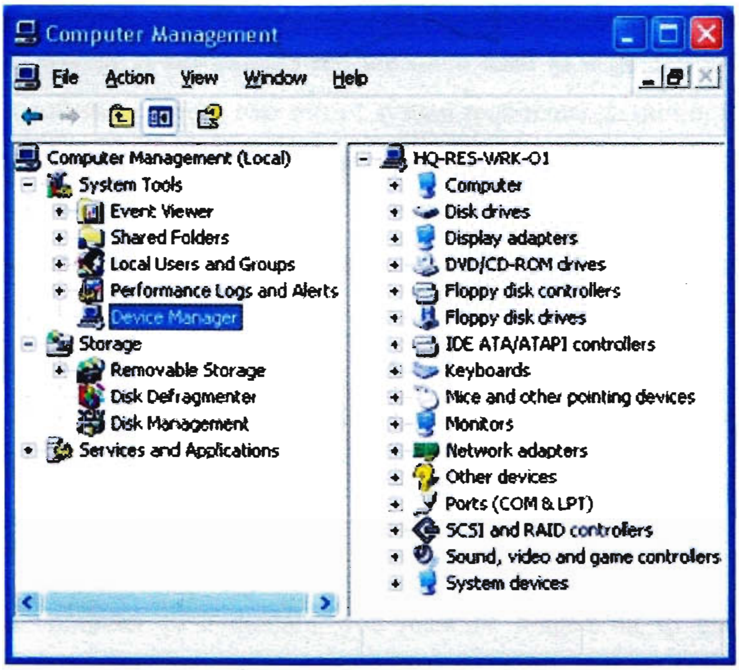


Figure: 2.1.4 (a) Device Manager

When a piece of hardware is not working, the offending hardware is highlighted for the user to deal with. The list of hardware can be sorted by various criteria.

For each device, users can:

- Supply device drivers
- Enable or disable devices
- Tell Windows to ignore malfunctioning devices
- View other technical properties

Device Manager was introduced with Windows 95 and later added to Windows 2000. In NT-based versions, it is included as a Microsoft Management Console snap-in.

- **Required Software Installation**

  To be used efficiently, all computer software needs certain hardware components or other software resources to be present on a computer.[1] These prerequisites are known as (computer) **system requirements** and are often used as a guideline as opposed to an absolute rule. Most software defines two sets of system requirements: minimum and recommended. With increasing demand for higher processing power and resources in newer versions of software, system requirements tend to increase over time. Industry analysts suggest that this trend plays a bigger part in driving upgrades to existing computer systems than technological advancements. A second meaning of the term of System requirements is a generalization of this first definition, giving the requirements to be met in the design of a system or sub-system. Typically an organization starts with a set of Business requirements and then derives the System requirements from there.

- **Attachment with Domain**

  To join a computer to a domain, you must be logged on to the computer with the local Administrator account or, if you are logged on to the computer with a user account that does not have local computer administrative credentials, you must provide the credentials for the local Administrator account during the process of joining the computer to the domain. In addition, you must have a user account in the domain to which you want to join the computer. During the process of joining the computer to the domain, you will be prompted for your domain account credentials (user name and password).

2.2 Bit Locker Drive Encryption & Decryption

Windows Bit Locker Drive Encryption is a new security feature that provides better data protection for your computer, by encrypting all data stored on the Windows operating system volume. (In this version of Windows, a volume consists of one or more partitions on one or more hard disks. Bit Locker works with simple volumes, where one volume is one partition. A volume usually has a drive letter assigned, such as

A Trusted Platform Module (TPM) is a microchip that is built into a computer. It is used to store cryptographic information, such as encryption keys. Information stored on the TPM can be more secure from external software attacks and physical theft.

Bit Locker uses the TPM to help protect the Windows operating system and user data and helps to ensure that a computer is not tampered with, even if it is left unattended, lost, or stolen.

Bit Locker can also be used without a TPM. To use Bit Locker on a computer without a TPM, you must change the default behavior of the Bit Locker setup wizard by using Group Policy, or configure Bit Locker by using a script. When Bit Locker is used without a TPM, the required encryption keys are stored on a USB flash drive that must be presented to unlock the data stored on a volume.

Your data is protected by encrypting the entire Windows operating system volume.

If the computer is equipped with a compatible TPM, Bit Locker uses the TPM to lock the encryption keys that protect the data. As a result, the keys cannot be accessed until the TPM has verified the state of the computer. Encrypting the entire volume protects all of the data, including the operating system itself, the Windows registry, temporary files, and the hibernation file. Because the keys needed to decrypt data remain locked by the TPM, an attacker cannot read the data just by removing your hard disk and installing it in another computer.

During the startup process, the TPM releases the key that unlocks the encrypted partition only after comparing a hash of important operating system configuration values with a snapshot taken earlier. This verifies the integrity of the Windows startup process. The key is not released if the TPM detects that your Windows installation has been tampered with.

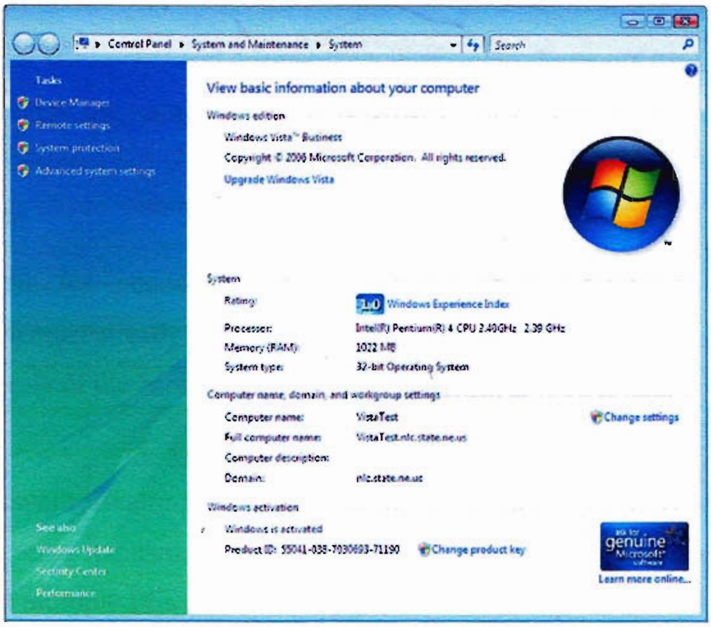
By default, the Bit Locker setup wizard is configured to work seamlessly with the TPM. An administrator can use Group Policy or a script to enable additional features and options.

For enhanced security, you can combine the use of a TPM with either a PIN entered by the user or a startup key stored on a USB flash drive.

On computers without a compatible TPM, Bit Locker can provide encryption, but not the added security of locking keys with the TPM. In this case, the user is required to create a startup key that is stored on a USB flash drive.

Bit Locker can be turned off in two ways: by disabling Bit Locker or by decrypting the volume. When you disable Bit Locker, your hard drive is still encrypted but your computer uses a plain text decryption key. That is stored on the hard drive to read the information. When you decrypt the volume, everything on your hard drive is decrypted.

Disabling Bit Locker Drive Encryption is a temporary method for removing Bit Locker protection without decrypting the drive Windows is installed on. Disable Bit Locker if you need to update the computer's basic input/output system (BIOS) or startup files. This precaution will help prevent Bit Locker from locking the drive and can help avoid the potentially lengthy decryption process.



View basic information about your computer

Windows edition

Windows Vista™ Business

Copyright © 2006 Microsoft Corporation. All rights reserved.

System

Rating: 1.0 Windows Experience Index

Processor: Intel(R) Pentium(R) 4 CPU 2.40GHz 2.39 GHz

Memory (RAM): 1022 MB

System type: 32-bit Operating System

Computer name, domain, and workgroup settings

Computer name: VistaTest

Full computer name: VistaTest.nlc.state.ne.us

Computer description:

Domain: nlc.state.ne.us

Windows activation

Windows is activated

Product ID: 55041-035-7030693-71190

Figure: 2.2 (a) Windows Properties

Enable Bit Locker again when the update is complete and you have restarted the computer. When it is disabled, Bit Locker uses a plain text key that it stores on the computer to read your files. Even though the hard drive is encrypted, the information on the drive is not secure. When you re-enable Bit Locker, the plain text key is removed and Bit locker once again secures the volume by using the Trusted Platform Module (TPM) or a password (if enabled by Group Policy settings).

Decrypting the volume means that Bit Locker protection is removed from the computer and the drive is decrypted, which can be time-consuming. When you decrypt the volume, all of the information stored on that computer is decrypted. If you decide to turn Bit Locker back on, it will either use the TPM on that computer or it will require you to set up another password. You might want to decrypt a volume before moving it to a new computer and then turn on Bit Locker on the new computer to encrypt the volume again.

To turn off or temporarily disable Bit Locker

1. Open Bit locker Drive Encryption by clicking the **Start** button, clicking **Control Panel,** clicking **Security**, and then clicking **Bit locker Drive Encryption**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

2. Do one of the following:

    - To temporarily disable Bit Locker, click **Turn off Bit Locker**, and then click **Disable Bit Locker Drive Encryption**.
    - To turn off Bit Locker and decrypt the volume, click **Turn off Bit Locker**, and then click **Decrypt the volume**.

2.3 Wi-Fi Salvation

The easiest solution for connecting the PC to wireless Internet is the wireless solution. To use the Wi-Fi, you must already have an internet router/modem (allowing transmission of information) these boxes play the role of the "sender".

These types of equipment usually offer a throughput of 54 Mbps (802.11g), with a range of about 100 meters, but there are other standards. Adequate for surfing and chatting, but a bit limited for download. It is possible to connect multiple PCs to a router, but with a necessarily limited flow with multiple users.

NIC: Network Interface Card

2.3.1 Equipment Needed

To receive the signal from the box, it is necessary that the PC has a network card (normally most PCs have, even being old enough).

You can still check:

Windows:

1. Click on "Start"
2. Right click My Computer (or Computer in Vista) and click on "properties"
3. Click on the tab "hardware"
4. Click on "Device Manager"
5. Click on the + sign in front of NIC
6. The name and brand of the card appear if the pc has a network card.

After verifying that your pc does have a network card, you need a "receiver" connected to the PC to receive information from the router/modem.
Note: The notebooks are usually already equipped with a Wi-Fi receiver.

2.3.2 The USB WI-FI Key

This is the simplest solution, and very inexpensive, you can buy them in supermarkets and on the Internet. Latest keys can provide a throughput of 300 Mbps maximum (802.11n). Must purchase a key corresponding to the standard of your router (802.11g is the current standard and most common).

2.3.3 Wi-Fi card

The Wi-Fi card is another solution, it is more difficult to install because it generally fits into a port on the motherboard (typically PCI). To get there, we must open the computer case and recognize the corresponding port on the motherboard of the computer.
The card may offer a maximum throughput of 300Mbps (802.11n) with a longer range than the USB key, so it's more comfortable. But this is only useful if your box has 802.11n (300 Mbps).

2.3.4 Setting Network

Once your purchase made, it must set the wireless network.
To prepare all this, you will need:

- The NIC
- The installation cd of the Wi-Fi Card/USB Key
- The security key (WEP or WPA) on your Internet box, usually located on your box to the back or bottom, in the manual box, or you can find the code in the settings box Internet via Internet.
- The SSID (network name of your box) available on the manual or via the internet within the parameters of the internet box.

Chapter: 3

Introduction to VPN Network

3.1 What is VPN?

VPN (Virtual Private Network) is a generic term used to describe a communication network that uses any combination of technologies to secure a connection tunneled through an otherwise unsecured or untrusted network1. Instead of using a dedicated connection, such as leased line, a "virtual" connection is made between geographically dispersed users and networks over a shared or public network, like the Internet. Data is transmitted as if it were passing through private connections. VPN transmits data by means of tunneling. Before a packet is transmitted, it is encapsulated (wrapped) in a new packet, with a new header. This header provides routing information so that it can traverse a shared or public network, before it reaches its tunnel endpoint. This logical path that the encapsulated packets travel through is called a tunnel. When each packet reaches the tunnel endpoint, it is "decapsulated" and forwarded to its final destination. Both tunnel endpoints need to support the same tunneling protocol. Tunneling protocols are operated at either the OSI (Open System Interconnection) layer two (data-link layer), or layer three (network layer). The most commonly used tunneling protocols are IPSec, L2TP, PPTP and SSL. A packet with a private non-routable IP address can be sent inside a packet with globally unique IP address, thereby extending a private network over the Internet.

3.2 VPN Security

VPN Security uses encryption to provide data confidentiality. Once connected, the VPN makes use of the tunneling mechanism described above to encapsulate encrypted data into a secure tunnel, with openly read headers that can cross a public network. Packets passed over a public network in this way are unreadable without proper decryption keys, thus ensuring that data is not disclosed or changed in any way during transmission. VPN can also provide a data integrity check. This is typically performed using a message digest to ensure that the data has not been tampered with during transmission. By default, VPN does not provide or enforce strong user authentication. Users can enter a simple username and password to gain access to an internal private network from home or via other insecure networks. Nevertheless, VPN does support add-on authentication mechanisms, such as smart cards, tokens and RADIUS.

3.3 Insecure Storage of Authentication Credentials by VPN Clients

Many VPN client programs offer to store some or all of the authentication credentials (e.g. username and password), and for some clients, this is the default setting. While this makes the VPN easier to use it also introduces security risks, especially if the credentials are not well protected.

The common client issues that have been seen are:

- Storing the username unencrypted in a file or the registry. Anyone with access to the client computer can obtain the username. If the VPN is using IKE Aggressive Mode, then knowledge of the username allows an offline cracking attack against the password.

- Storing the password in a scrambled form. This is often referred to as "encryption", but it is really obfuscation rather than encryption because there is no unique key needed to decrypt it. If the obfuscation algorithm becomes known, then it is a simple matter to obtain the password if you have access to the client computer

- Storing the plain-text password in memory. If storing an obfuscated version of the password in a file or registry is not bad enough, many clients decrypt this when they start up, and store a plaintext version of the password in memory. In this case, anyone with access to the client computer can obtain the password by starting the VPN client and then dumping the process memory with a tool such as pm dump, or crashing the computer to get a dump of physical memory. Figure 1 shows an example memory dump from a VPN client with the clear-text password *W0ntGu355Th15* highlighted. Notice that the last two characters of the password are repeated in the memory dump. This is repeatable behavior for this VPN client, and may give some insight into the obfuscation mechanism.
- Weak registry or file permissions for stored credentials. It is a bad idea to cache credentials at all, but this is made worse if they are stored in a file or registry entry that is readable by everybody. This allows these details to be obtained from guest or anonymous network connections as well as via physical access to the client system.

Three common faults were found in the way that VPN servers respond to the first packet from the client:

1. Some VPN servers only respond to the client if the username is valid, they do not respond at all to invalid usernames;
2. Some VPN servers will respond with a notification message, e.g. no-proposal chosen, if the username is incorrect.
3. Some VPN servers respond to both valid and invalid usernames, but the hash payload for invalid usernames is calculated using a null password, and it is simple for the client to determine this.

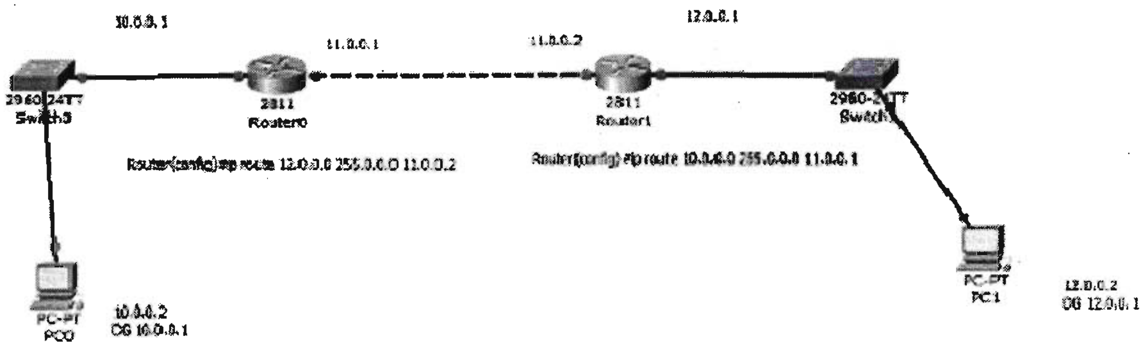
   In all three cases, the response to an invalid username is different to that for a valid username, and this allows the client to determine if a given username is valid or not. The correct way for the VPN server to respond to an invalid username is for it to respond using a random password for the hash payload. This is simple to implement, and does not allow the client to determine if a username is valid or not. It is therefore surprising that so many VPN implementations get this wrong. An example of this issue is shown below. In this example, like-scan is used to demonstrate that the VPN server responds to valid usernames normally, but to invalid usernames with a notify message. This shows that, for this VPN server, the username fred is valid, but the username jim is not valid.

Chapter: 4

VPN Development

4.1 Establishment VPN Network through Packet Tracer

first of all you need to study Well the concepts of IPSec , VPN types , CRYPTOLOGY before you read this document Its just show you how to type the right commands on both router sides using packet tracer 5.3 We will have the following topology



```
Router(config)#ip route 12.0.0.0 255.0.0.0 11.0.0.2
Router(config)#ip route 10.0.0.0 255.0.0.0 11.0.0.1
```

Addressing Table

Device Default	Interface	IP Address	Subnet Mask	Gateway
R1	Fa0/0	10.0.0.1	255.255.255.0	N/A
	Fa0/1	11.0.0.1	255.255.255.0	N/A
R2	Fa0/0	12.0.0.1	255.255.255.0	N/A
	Fa0/1	11.0.0.2	255.255.255.0	N/A
PC0	N/A	10.0.0.2	255.255.255.0	10.0.0.1
PC1	N/A	12.0.0.2	255.255.255.0	12.0.0.1

ISAKMP Phase 1 Policy Parameters

Parameters		R1	R2
Key distribution method	Manual or ISAKMP	ISAKMP	ISAKMP
Encryption algorithm	DES, 3DES, or AES	AES	AES
Hash algorithm	MD5 or SHA-1	SHA-1	SHA-1

Authentication method	Pre-shared keys or RSA	pre-share	pre-share
Key exchange	DH Group 1, 2, or 5	DH 2	DH 2
IKE SA Lifetime	86400 seconds or less	86400	86400
ISAKMP Key		Cisco	cisco

IPsec Phase 2 Policy Parameters

Parameters	R1	R2
Transform Set	VPN-SET	VPN-SET
Peer Hostname	R1	R2
Peer IP Address	10.0.0.1	12.0.0.1
Network to be encrypted	10.0.0.0/24	12.0.0.0/24
Crypto Map name	VPN-MAP	VPN-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp

Objectives

Part 1: Enable Security Features

Part 2: Configure IPSec Parameters on R1

Part 3: Configure IPSec Parameters on R2

Part 4: Verify the IPSec VPN

Scenario

In this activity, you will configure two routers to support a site-to-site IPsec VPN for traffic flowing from their respective LANs. The IPsec VPN traffic will pass through another router that has no knowledge of the VPN. IPsec provides secure transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (peers), such as Cisco routers.

Part 1: Enable Security Features

Step 1: Activate securityk9 module.

The Security Technology Package license must be enabled to complete this activity.

Notice you will set static route between the two routers while on real live both will connected through ISP's

a. Issue the show version command in the user EXEC or privileged EXEC mode to verify that the Security

Technology Package license is activated.

```
----------------------------------------------------------------------
Technology        Technology-package          Technology-package
                  Current     Type             Next  reboot
----------------------------------------------------------------------
ipbase            ipbasek9          Permanent        ipbasek9
Security          None              None             None
uc                None              None             None
Data              None              None             None

Configuration register is 0x2102
```

b. If not, activate the securityk9 module for the next boot of the router, accept the license, save the

```
Configuration and reboot.
R1(config)# license boot module c2900 technology-package
securityk9
R1(config)# end
R1# copy running-config startup-config
R1# reload
```

c. After the reloading is completed, issue the show version again to verify the Security Technology Package license activation.

```
Technology Package License Information for Module:'c2900'
----------------------------------------------------------------------------------
Technology              Technology-package                 Technology-package
                        Current       Type                 Next          reboot
----------------------------------------------------------------------------------
Ipbase                  ipbasek9      Permanent            ipbasek9
Security                securityk9    Evaluation           securityk9
uc                      None          None                 None
Data                    None          None                 None
```

Part 2: Configure IPSec Parameters on R1

Step 1: Test connectivity.

Ping from PC-A to PC-C.

Step 2: Identify interesting traffic on R1.

Configure ACL 110 to identify the traffic from the LAN on R1 to the LAN on R3 as interesting. This interesting traffic will trigger the IPsec VPN to be implemented whenever there is traffic between R1 to R3 LANs. All other traffic sourced from the LANs will not be encrypted. Remember that due to the implicit deny any, there is no need to add the statement to the list.

```
R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255
```

Step 3: Configure the ISAKMP Phase 1 properties on R1.

Configure the crypto ISAKMP policy 10 properties on R1 along with the shared crypto key cisco. Refer to the ISAKMP Phase 1 table for the specific parameters to configure. Default values do not have to be configured therefore only the encryption, key exchange method, and DH method must be configured.

```
Router(config)#crypto isakmp enable
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#encryption aes
Router(config-isakmp)#hash sha
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#crypto isakmp key 0 address 11.0.0.1
```

Step 4: Configure the ISAKMP Phase 2 properties on RI.

Create the transform-set VPN-SET to use esp-3des and esp-sha-hmac. Then create the crypto map VPNM AP that binds all of the Phase 2 parameters together. Use sequence number 10 and identify it as an ipseci sakmp map.

```
R1(config)# crypto ipsec transform-set VPN-SET esp-3des
esp-sha-hniac
Ri(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to R3
R1(config—crypt.o—map)# set peer 10.2.2.2
```

```
R1(config-crypto-rnap) # set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1 (con fig-crypt.o-map) #exit
```

Step 5: Configure the crypto map on the outgoing interface.

Finally, bind the VPN-MAP crypto map to the outgoing Serial 0/0/0 interface. Note: This is not graded.

```
R1(config)# interface .50/0/0
R1(config-if)# crypto map VPN-MAM
```

Part 3: Configure IPsec Parameters on R2

Step I: Configure router R3 to support a site-to-site VPN with RI.

Now configure reciprocating parameters on R3. Configure ACL 110 identifying the traffic from the LAN on R3 to the LAN on *RI* as interesting.

```
R2(onfig)# access—list 110 permit ip 192.168.3.0 0.0.0.255
           192.168.1.0 0. 0. 0 .255
```

Step 2: Configure the ISAKMP Phase *I* properties on R3.

Configure the crypto ISAKMP policy 10 properties on R3 along with the shared crypto key cisco.

```
R3(config)# crypto isakmp policy 10
R3(config—isakrnp)# encryption aes
R3 (config-isakrnp) 4 authentication pre-share
R3(config-isakmp)# group 2
R3 (config—isakrnp) 4 exit
R3(config)# crypto isakmp key cisco address 10.1.1.2
```

Step 3: Configure the ISAKMP Phase 2 properties on *RI.*

Like you did on RI, create the transform-set VPN-SET to use esp-3des and esp-sha-hmac. Then create the crypto map VPN-MAP that binds all of the Phase 2 parameters together. Use sequence number 10 and identify it as an ipsec-isakmp map.

```
R2(config)# crypto ipsec transform-set VPN-SET esp-3des
esp-sha-hmac
R2(config)# crypto map VPN-MAP 10 ipsec-isakmp
R2 (config-crypt.o-map)# description VPN connection to Ri
```

```
R2 (config—crypt.o—map)# set peer 10.1.1.2
R2 (config-crypto-map)* set transform-set VPN-SET
R2 (config-crypto-map)# match address 110
R2 (config—crypto—map) 4 exit
```

Step 4: Configure the crypto map on the outgoing interface.

Finally, bind the VPN-MAP crypto map to the outgoing Serial 010/1 interface. Note: This is not graded.

```
R3(config)4 interface SO/Oil
R3(config-if)# crypto map VPN-MAP
```

Part 4: Verify the IPsec VPN

Step 1: Verify the tunnel prior to interesting traffic.

Issue the show crypto ipsec sa command on RI. Notice that the number of packets encapsulated encrypted, decapsulated and decrypted are all set to 0.

```
R1# show crypto ipsec sa
interface: SerialO
Crypto map tag: VPN—MAP, local addr 10.1.1.2
protected vrf: (none)
local ident (addr/mask/prot/port) :
(192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port) :
(192.168.3.0/255.255.255.0/0/0)
current peer 10.2.2.2 port 500
PERMIT, flagsoriginisacl,)
Ipkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
tpkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
Ipkts compressed: 0, pkts decompressed: 0
pkts not compressed: 0, *pkts compr. failed: 0
Ipkts not decompressed: 0, #pkts decompress failed: 0
Isend errors 0, Irecv errors 0
local crypto endpt.: 10.1.1.2, remote crypto endpt.
:10.2.2.2
path mtu 1500, ip mtu 1500, ip mtu idb SerialO/0/0
current outbound api: OxO(0)
<output omitted>
```

Step 2: Create interesting traffic.

Ping PC-C from PC-A.

Step 3: Verify the tunnel after interesting traffic.

On RI, re-issue the show crypto ipsec sa command. Now notice that the number of packets is more than 0 indicating that the IPsec VPN tunnel is working.

```
R1#. show crypto ipsec sa
ntertace: Serial0/0/0
Crypto map tag: VPI4—MAP, local addr 10.1.1.2
protected vrf: (none)
local ident (addr/maskJprot/port):
(192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
current peer 10.2.2.2 port 500
PERMIT, flags(origin_is_acl,)
Ipkts encaps: 3, *pkts encrypt: 3, 41pkts digest: 0
Ipkts decaps: 3, *pkts decrypt: 3, #pkts verify: 0
tpkts compressed: 0, 4pkts decompressed: 0
Ipkts not compressed: 0, #pkts compr. failed: 0
Ipkts not decompressed: 0, 41pkts decompress failed: 0
Isend errors 1, Irecv errors 0
local crypto endpt..: 10.1.1.2, remote crypto endpt.
:10.2.2.2
path mtu 1500, ip mtu 1500, ip mtu idb SerialO/OfO
current outbound spi: 0x0A496941(172583233)
<output omitted>
```

Step 4: Create uninteresting traffic.

Ping PC-B from **PC-A.**

Step **5: Verify the tunnel.**

On RI re-issue the show crypto ipsec sa command. Finally, notice that the number of packets has not changed verifying that uninteresting traffic is not encrypted.

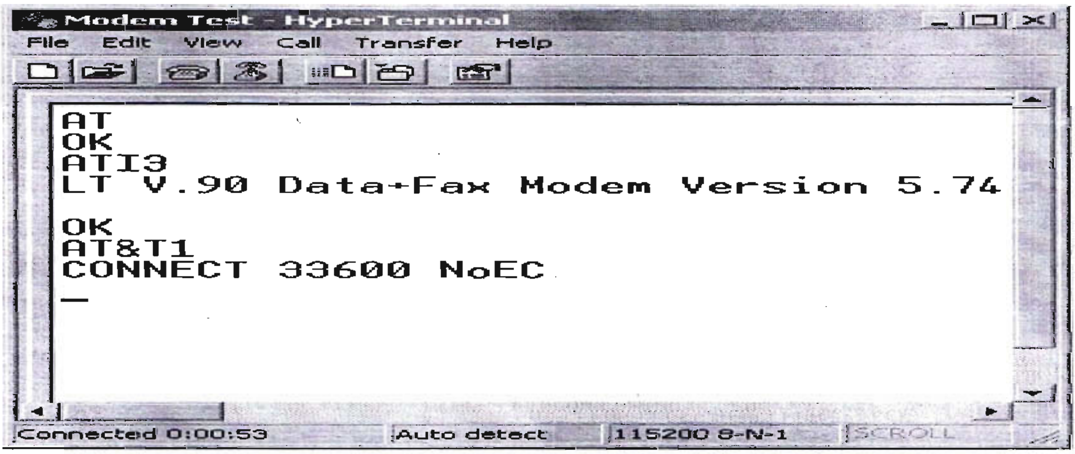
4.2Practical Connection of routers setting up VPN network

4.2.1 Usage of HyperTerminal Software:

he HyperTerminal tool, included with Windows 2000, allows you to communicate directly with your system's modem. Through HyperTerminal, you can reset the modem or issue configuration and diagnostic commands. These capabilities can help you determine whether or not the modem and computer are communicating correctly.

Starting HyperTerminal and setting up a new connection Before you can use HyperTerminal to troubleshoot your modem, you must create a connection to the port the modem is using. To do so, follow these steps:

1. Click Start | Programs | Accessories | Communications | HyperTerminal.
2. Once HyperTerminal opens, it will automatically prompt you to create a new connection if none exist. If no connection(s) exists, you can click File | New Connection to create a new one.
3. Specify a name for the connection, choose an icon, and click OK.
4. In the Connect To dialog box, choose the COM port being used by your modem (usually COM1 or COM2) from the Connect Using drop-down list and click OK.
5. In the port property sheet that appears, choose a port speed (bits per second) that matches the device. (For a modem, choose its maximum speed.)
6. Then, choose communications parameters that match the device. For most devices, you can typically use 8 data bits, no parity (set to none), one stop bit, and hardware flow control. When you click OK, HyperTerminal will immediately open a connection to the port. You'll then be ready to troubleshoot. Using AT commands When using a modem, you can type *AT* and press [Enter] in the
7. HyperTerminal connection to test communications. You should receive an OK message if your settings are correct and the modem is working, as shown in **Figure A**.



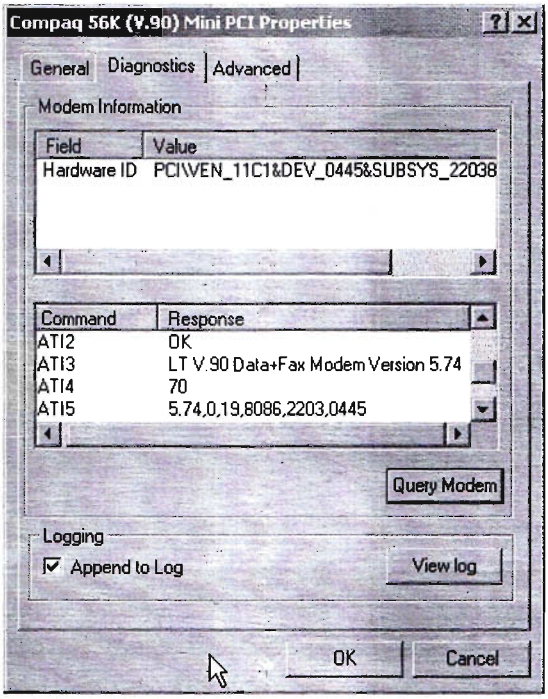
```
AT
OK
ATI3
LT V.90 Data+Fax Modem Version 5.74

OK
AT&T1
CONNECT 33600 NoEC
_
```

Figure: 4.2.1. (a) , Hyper Terminal

If you don't see the AT text appears when you type, choose File | Properties, click the Settings tab, and then click ASCII Setup. Select Echo Type Characters Locally and click OK twice. Once you know the modem is at least communicating with the computer, you can use an AT command to perform further diagnostic testing or change configuration settings. Refer to your modem's manual for configuration and diagnostic commands.

Other troubleshooting methods

There are a few other ways to perform diagnostics on a modem and issue special configuration commands. For diagnostics, open the Control Panel and then open the Phone and Modem Options object. Click the Modems tab, select the modem, and click Properties. Use the Diagnostics tab (**Figure B**) to query the modem and view the modem log when troubleshooting communications problems.



Field	Value
Hardware ID	PCI\VEN_11C1&DEV_0445&SUBSYS_22038

Command	Response
ATI2	OK
ATI3	LT V.90 Data+Fax Modem Version 5.74
ATI4	70
ATI5	5.74,0,19,8086,2203,0445

☑ Append to Log

Figure : 4.2.1(b) Mini PCI properties

Clicking the Query Modem button will send the same AT commands to the modem that we entered manually using HyperTerminal. If you need to include a special initialization command for the modem, click the advanced tab and enter the modem commands in the Extra Initialization Commands field. This will cause Windows to use the initialization commands for all sessions in which the modem is used.

Once the routers are connected with the computers then u have to turn on the power of the routers. After that, routers will be initialized and command page will be shown on the computer to run the program based on the VPN Network establishment.

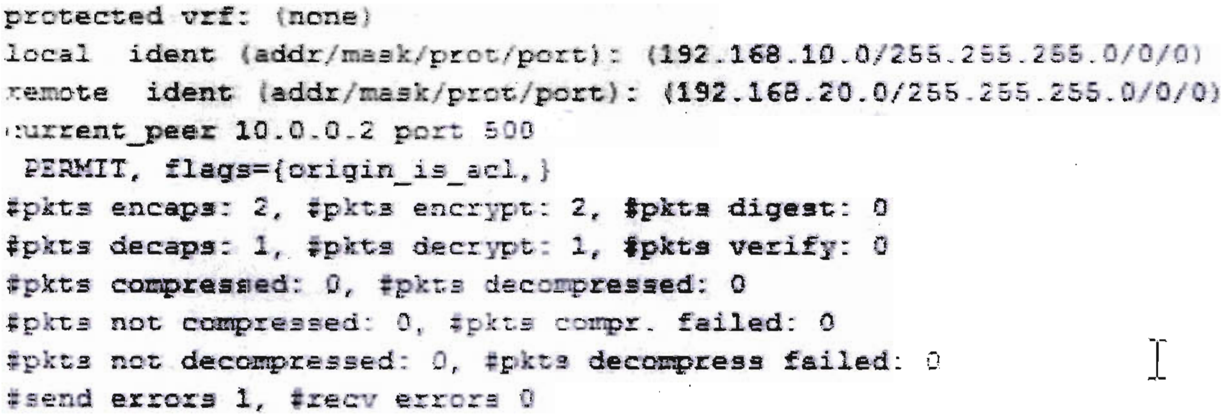
Two ways configuration of the routers first to configure the terminal then to configure the router for the sake of enacting of VPN network that is similar to the configuration command of VPN through the packet tracer.

4.2.2 Verification of the establishment of VPN network:

To verify the proper network of virtual private network, we are to check it to give the command of the command windows or to send the packets to observe that whether it's being encrypted or not. Depending on the packets sent to the destination from the source, we are to check, how many packets are encrypted, how many packets are digested also the result of decrypted message and verification will be shown.

To check the source and destination of the sending packets are to give the command: **show crypto isakmp sa** To check the overall results of encrypted and decrypted message, we are to give the command like: **show crypto IPSec sa**

The result will be shown like:



```
protected vrf: (none)
local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
remote  ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
current_peer 10.0.0.2 port 500
 PERMIT, flags={origin_is_acl,}
#pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 0
#pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0
```

4.3 Remote Access Based on Software basis VPN

In this case, the most significant aspect of virtual private network is to connect the users under the VPN network by means of using some software based VPN. Here, some companies establish their their VPN network and depending on this network, they are to use some soft ware's which enables the users to be connected through the VPN network wherever they stay. In the case of Remote user, where communication is very rare, VPN can enable you to communicate.

As it has been mentioned previously how to create the VPN network to configure the routers, here to show some software that is used for the remote users to be connected for the sake of secure communications.

Using Software purposed of VPN Network

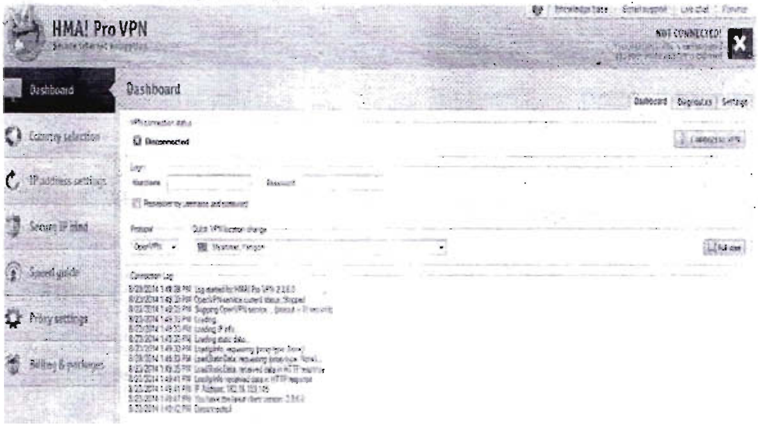


Figure:4.3(a) Software based VPN connection for remote users.

- Using some software that helps your IP to be connected with the VPN server. Anyone achieving this IP, sometimes it can be achieved randomly can connect through the VPN network in any place of the world same technology implemented for the VPN server where users from any place are given the user id and password based on country location that is like the connection of VPN device. Only difference for the software based VPN is to patch & upgrade to the operating system while it has always been implemented in the case of hardware based VPN.
- The remote users need to use telephone or any transparent facilities to communicate which is so costly as well s not so secured where using VPN supported soft ware's you may easily elaborate your communications that is also so secured.
-

Chapter: 5

Types of VPN product

VPNs can be broadly categorized as follows:

1. A firewall-based VPN is one that is equipped with both firewall and VPN capabilities. This type of VPN makes use of the security mechanisms in firewalls to restrict access to an internal network. The features it provides include address translation, user authentication, real time alarms and extensive logging.

2. A hardware-based VPN offers high network throughput, better performance and more reliability, since there is no processor overhead. However, it is also more expensive.

3. A software-based VPN provides the most flexibility in how traffic is managed. This type is suitable when VPN endpoints are not controlled by the same party, and where different firewalls and routers are used. It can be used with hardware encryption accelerators to enhance performance.

4. An SSL VPN3 allows users to connect to VPN devices using a web browser. The SSL (Secure Sockets Layer) protocol or TLS (Transport Layer Security) protocol is used to encrypt traffic between the web browser and the SSL VPN device. One advantage of using SSL VPNs is ease of use, because all standard web browsers support the SSL protocol, therefore users do not need to do any software installation or configuration.

5.1 COMMON VPN TUNNELING TECHNOLOGIES

The following tunneling technologies are commonly used in VPN:

5.1.1 IPSEC (INTERNET PROTOCOL SECURITY)

IPSec was developed by IETF (the Internet Engineering Task Force) for secure transfer of information at the OSI layer three across a public unprotected IP network, such as the Internet. IPSec enables a system to select and negotiate the required security protocols, algorithm(s) and secret keys to be used for the services requested. IPSec provides basic authentication, data integrity and encryption services to protect unauthorized viewing and modification of data. It makes use of two security protocols, AH (Authentication header) and

ESP (Encapsulated Security Payload), for required services. However, IPSec is limited to only sending IP packets.

5.1.2 Security Protocols for Traffic Security

IPSec makes use of the AH and ESP protocols to provide security services:

1. AH (Authentication Header) protocol provides source authentication, and integrity of IP packets, but it does not have encryption. An AH header added to the IP packet contains a hash of the data, a sequence number etc., and information that can be used to verify the sender, ensure data integrity and prevent replay attacks.

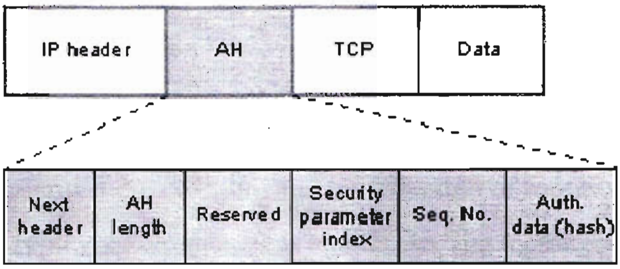


Figure: 5.2.2(a) Authentication Header

2. ESP (Encapsulated Security Payload) protocol provides data confidentiality, in addition to source authentication and integrity. ESP uses symmetric encryption algorithms, such as 3DES, to provide data privacy. The algorithm needs to be the same on both communicating peers. ESP can also support encryption-only or authentication-only configurations. However, research in 2007 showed that any RFC-compliant implementations of IPSec that make use of encryption-only ESP can be broken.

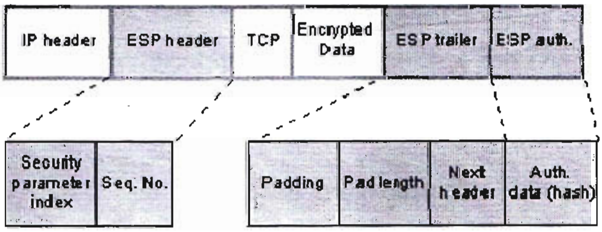


Figure: 5.2.2(b) ESP (Encapsulated Security Payload)

Chapter: 6

Risks & Limitations of VPN

6.1 Hacking Attacks

A client machine may become a target of attack, or a staging point for an attack, from within the connecting network. An intruder could exploit bugs or mis-configuration in a client machine, or use other types of hacking tools to launch an attack. These can include VPN hijacking or man-in-the-middle attacks:

1. VPN hijacking is the unauthorized take-over of an established VPN connection from a remote client, and impersonating that client on the connecting network.

2. Man-in-the-middle attacks affect traffic being sent between communicating parties, and can include interception, insertion, deletion, and modification of messages, reflecting messages back at the sender, replaying old messages and redirecting messages.

Here is a growing concern as to how secure MPLS IP VPNs really are and how they can be protected from Internet attacks. Fortunately, the answer is pretty straight forward and doesn't require a lot of technical analysis to see why.

In pure MPLS IP VPN environments without Internet access, where the network is used to connect different sites, the core network and customer address space is concealed 100%. This means that no information is revealed to third parties or the Internet. With no information revealed, hackers are unable to obtain access to critical information such as router IP addresses in order to perform Denial of Service (DoS) attacks and bring down the network.

In addition, service providers prevent their routers from being reachable via the Internet by using well-known techniques such as packet filtering, applying access control lists (ACLs) to limit access only to the ports of the routing protocol (e.g. BGP) from specific areas within their network.

In an environment where Internet access is provided to the customer via the MPLS link; ISP's use similar mechanisms to lock down their Customer Edge routers that provide access to the Internet. In addition, the routing protocols used by the ISP have built-in mechanisms that are usually enabled and increase the security level even more. A few examples are the configuration of the MD5 authentication for routing protocols (BGP, OSPF e.t.c), configuration of maximum number of routes accepted per Virtual Routing and Forwarding instance (VRF) and a few more.

6.2 USER AUTHENTICATION

By default VPN does not provide / enforce strong user authentication. A VPN connection should only be established by an authenticated user. If the authentication is not strong enough to restrict unauthorized access, an unauthorized party could access the connected network and its resources. Most VPN implementations provide limited authentication methods. For example, PAP, used in PPTP, transports both user name and password in clear text. A third party could capture this information and use it to gain subsequent access to the network

His authentication of virtual private network (VPN) clients by the VPN server is a vital security concern. Authentication takes place at two levels:

- **Computer-level authentication:** When Internet Protocol security (IPSec) is used for a Layer Two Tunneling Protocol (L2TP) over IPSec (L2TP/IPSec) VPN connection, computer-level authentication is performed through the exchange of computer certificates or a pre shared key during the establishment of the IPSec security association.

- **User-level authentication:** before data can be sent over the Point-to-Point Tunneling Protocol (PPTP) or L2TP tunnel, the remote access client or demand-dial router that requests the VPN connection must be authenticated. User-level authentication occurs through the use of a Point-to-Point Protocol (PPP) authentication method.

His is an authentication error from the Cisco VPN client. Either the username and/or password entered were incorrect or the VPN client was not able to launch the XAuth (user authentication) process. You may also see this with the 413 error "The necessary VPN sub-system is not available. You cannot connect to the remote VPN server.

You may need to work with your network administrator or help desk to make sure your account is ok (not locked) and you're using the correct credentials. If you're using tokens, make sure the token key is synchronized. In some cases, if you're connected and then get disconnect with this error, uninstalling and re-installing the VPN client may help. Sometimes a firewall or anti-virus policy mismatch needs to be checked.

6.3 CLIENT SIDE RISKS

The VPN client machines of, say, home users may be connected to the Internet via a standard broadband connection while at the same time holding a VPN connection to a private network, using split tunneling. This may pose a risk to the private network being connected to. A client machine may also be shared with other parties who are not fully aware of the security implications. In addition, a laptop used by a mobile user may be connected to the Internet, a wireless LAN at a hotel, airport or on other foreign networks. However, the security protection in most of these public connection points is inadequate for VPN access. If the VPN client machine is compromised, either before or during the connection, this poses a risk to the connecting network.

A connecting network can be compromised if the client side is infected with a virus. If a virus or spyware infects a client machine, there is chance that the password for the VPN connection might be leaked to an attacker. In the case of an intranet or extranet VPN connection, if one network is infected by a virus or worm, that virus / worm can be spread quickly to other networks if anti-virus protection systems are ineffective

6.4 Incorrect Network Access Rights

You can configure a server that allows remote users to access resources on your private network over dial-up or virtual private network (VPN) connections. This type of server is called a remote access/VPN server. Remote access/VPN servers can also provide network address translation (NAT). With NAT, the computers on your private network can share a single connection to the Internet. With VPN and NAT, your VPN clients can determine the IP addresses of the computers on your private network, but other computers on the Internet cannot.

This topic explains the basic steps for configuring a remote access/VPN server using Manage Your Server, the Configure Your Server Wizard, and the Routing and Remote Access Server Setup Wizard. After you finish configuring a basic remote access/VPN server, you can complete additional configuration tasks, depending on how you want to use the remote access/VPN server.

Before you configure your server as a remote access/VPN server, you should verify whether or not:

- The operating system is configured correctly. In the Windows Server 2003 family, remote access/VPN depends on the appropriate configuration of the operating system and its services. If you have a new installation of a product in the Windows Server 2003 family, you can use the default service settings. No further action is necessary. If you upgraded to a product in the Windows Server 2003 family or you want to confirm that your services are configured correctly for best performance and security, verify your service settings by comparing them to the table in Default settings for services.

- Your server is correctly configured for optimal security for your network needs. Because your remote access/VPN server will connect your private network, the Internet, and your remote clients, you must make sure the server is secure. The security of your private network depends on the security of your remote access/VPN server. For more information, see Security information for remote access.

- This computer has two network interfaces, one that connects to the Internet and one that connects to the private network. The connection to the Internet must be a dedicated connection with enough bandwidth that VPN users can connect to your private network and users on your private network can connect to the Internet. The connection to computers on your private network must be made through a hardware device, such as a network adapter.

- All needed network protocols have been installed for your network interfaces. For more information, see Network interfaces.

- Windows Firewall is disabled on the server that you want to configure for remote access/VPN. You will configure the Basic Firewall feature of Routing and Remote Access during setup, which will serve in place of Windows Firewall.

- Internet Connection Sharing is disabled on the server that you want to configure for remote access/VPN. Internet Connection Sharing is not compatible with Routing and Remote Access. Internet Connection Sharing and Network Bridge are not included in Windows Server 2003, Web Edition; Windows Server 2003, Datacenter Edition; and the Itanium-based versions of the original release of the Windows Server 2003 operating systems.

- The Security Configuration Wizard is installed and enabled. For information about the Security Configuration wizard, see Security Configuration Wizard Overview.

Chapter: 7

Security Considerations

7.1 General VPN Security Considerations

Interoperability is also a concern. For example, IPSec compliant software from two different vendors may not always be able to work together.

The following is general security advice for VPN deployment:

1. VPN connections can be strengthened by the use of firewalls.

2. An IDS / IPS (Intrusion Detection / Prevention System) is recommended in order to monitor attacks more effectively.

3. Anti-virus software should be installed on remote clients and network servers to prevent the spread of any virus / worm if either end is infected.

4. Unsecured or unmanaged systems with simple or no authentication should not be allowed to make VPN connections to the internal network.

5. Logging and auditing functions should be provided to record network connections, especially any unauthorized attempts at access. The log should be reviewed regularly.

6. Training should be given to network/security administrators and supporting staff, as well as to remote users, to ensure that they follow security best practices and policies during the implementation and ongoing use of the VPN.

7. Security policies and guidelines on the appropriate use of VPN and network support should be distributed to responsible parties to control and govern their use of the VPN.

8. Placing the VPN entry point in a Demilitarized Zone (DMZ) is recommended in order to protect the internal network.

9. It is advisable not to use split tunneling to access the Internet or any other insecure network simultaneously during a VPN connection. If split tunneling is used, a firewall and IDS should be used to detect and prevent any potential attack coming from insecure networks
10. Unnecessary access to internal networks should be restricted and controlled.

7.2 EXTRANET VPN SECURITY CONSIDERATIONS

The following are additional security considerations for extranet VPN deployment:

1. Strong user authentication mechanisms should be enforced.

2. The VPN entry point should be placed inside a DMZ to prevent partners from accessing the internal network.

3. Access rights should be granted on an as-needed basis. Only necessary resources should be available to external partners. Owners of these resources should review access permissions regularly.

The following are general security considerations for VPN users:

1. Strong authentication is required when users are connecting dynamically from disparate, untrusted networks, for example:
   - By means of certificates and/or smart cards, or tokens: A smart card is used to store a user profile, encryption keys and algorithms. A PIN number is usually required to invoke the smart card. A token card provides a one-time password. When the user authenticates correctly on the token by entering the correct PIN number, the card will display a one-time pass code that will allow access to the network.
   - By means of add-on authentication system, like TACACS+, RADIUS. This kind of central authentication system contains a profile of all VPN users, controlling the access to the private network.
2. Personal firewalls should be installed and configured properly on client VPN machines to block unauthorized access to the client, ensuring it is safe from attack. Many of the more recent remote access VPN clients include personal firewalls. Some may also include other configuration checks, such as the client not being able to connect to the network if anti-virus software is not running, or if virus signatures are out of date.

3. The client machine should have anti-virus software installed, with up-to-date signatures, to detect and prevent virus infections.

4. The user should remain aware of the physical security of the machine, in particular when authentication information is stored on the machine.

5. All users should be educated on good Internet security practices. Access from home should be considered an insecure channel, as traffic is routed over the Internet.

Chapter: 8

8.1 Results and Discussion

In the light of the above discussion and experimental issues on the basis of my internship program and project, it can be cited that the overall result of my project based on the VPN establishment to create a new concept for the sake of networking security is successful. In this project, I have proved that VPN configuration is not only restricted for the large transparent company for its cost saving policy and scalability facilities but it can be successfully implemented in the place where you want a secure communication also. In the reflection of this project proves that VPN network can be used to secure our communication in our daily life that can help to prevent the cyber crime.

At the initial moment of my internship program, I have discovered the advantages and accomplishment of the VPN Network as soon as my project work helps me to establish this network successfully. We know that VPN Network ensures the encrypted communication where lots of protocols are used for the process of encryption and authentication for the sake of creating secure network. Through the experiment of Packet tracer and the Real routers Based experiment shows the result that data is being encrypted and authenticated while communication begins through the VPN network.

In the case of usage the routers connection when I along with my supervisor has faced some hindrance to establish the network, but finally we have succeeded the creation of secured network of VPN. So on the basis of my experimental and structural result of my project, it can be demonstrated that VPN network can be a tough one to establish, but with its proper utilization, it can be used widely for any kind of secured, secret, encrypted and authenticated communication so easily. I have shown the virtual private network theoretically for the reason to establish the network , then I have ensured the network creating through the basis on the software using Packet Tracer as well as through the utilization of the real routers to create the VPN tunnel between the routers for VPN network.

8.2. Conclusion

The completion of my project work base on the VPN network come to end as a great achievement because of its creation of different spheres of usage s of this network. Through my internship program the ideas and knowledge, I gathered both theoretically and practically that is the main issue of my successive completion of my project works. Though the concept of VPN networking is not so new but its proper initialization and establishments is very rare especially to consider our country .Nowadays, every time we rouge internet and read newspapers, there are lots of news related with the cyber crime. Here it is obvious from this experimental base projects, VPN network can easily solve this treat to sane our communication to ensure that secure communication happens.

To consider last five years, the using of VPN network is tremendously increasing day by day because of its significance. Throughout my project works, it has been proved that some new thoughts & ideas can be implemented through the VPN network in the case of its elaboration and significance of VPN by dint of extensive utilizations. Nowadays our top security level of activities of Government is based on Computer Database, where cyber crime can exist at anytime that can be controlled spontaneously through the VPN network. Furthermore, it can also be said that through the experiment of the software based VPN can connect the remote users to communicate under the VPN network.

It has also been demonstrated that VPN uses some protocols and algorithm that is highly strong for the process of encryption, decryption, and authentication for showing some hash value that is actually encrypted vale of the data. So, it can also break the VOIP restriction to enables the users using some application, servers, and a browser that is not verified by the VOIP. Finally, to conclude the finalization of this internship program and project, it can be mentioned that internship program helped me to enrich my concepts and ideas while project works help me to implement.

8.3. Reference

1. https://courses.cs.ut.ee/MTAT.08.004/2014_spring/uploads/Main/37_1
2. http://en.kioskea.net/faq/5772-hardware-connect-the-pc-to-wireless-internet-wi-fi
3. http://windows.microsoft.com/en-us/windows-xp/help/networking/install-wireless-network-adapter
4. written by Rahul Banarlee-" Networking Technologies-An Engineering Perspective" , Prentice Hall in India
5. K George And D. Panagiotis,A Review of Energy Efficiency in Telecommunication Network,"Telfor journal,vol.2 No.1,2010
6. M. Dachyar,N. Monasisca,Customer Satisfaction Index Telecommunication Industry in Indonesia,World Academy of Science, Enginnering and Technology 69,2012
7. http://h30434.www3.hp.com/t5/Wireless-Internet-Home-Networking/Solution-for-issues-connecting-wifi-or-wireless-using-Ralink/td-p/2248179
8. http://www.tomshardware.com/answers/id-1976880/wifi-adapter-slow.html
9. http://pi4.informatik.uni-mannheim.de/pi4.data/content/courses/1996-ss/rn96/CN-Title/form/motivate.htm
10. http://en.wikipedia.org/wiki/Network
11. http://en.wikipedia.org/wiki/Computer_network
12. http://www.ictglobal.com/
13. http://www.top10bestvpn.com/
14. https://strongvpn.com/locations.html
15. http://www.goldenfrog.com/vyprvpn/features/vpn-server-locations
16. http://www.slickvpn.com/locations.html
17. http://www.hotspotshield.com/
18. http://searchenterprisewan.techtarget.com/definition/virtual-private-network