Journal of Engineering and Development, Vol. 13, No. 4, Des (2009) **ISSN 1813-7822**

Virtual Privet Networks using Cisco Routers

Haider Tarish Haider
Asst. Lect.
hth.1977@yahoo.com

Deia Halboot Mohussen
Asst. Lect.
deia_mohussen@yahoo.com

Al-Mustansiriya University
Engineering College
Computer and Software Dep.

Abstract

Virtual private Network (VPN), is a technology that provides a secure communications mechanism for data and control information transmitted between networks. It can be used over existing network such as data across public network. This is often less expensive than the alternatives such as dedicated private telecommunications lines between organization or branch offices,

VPN uses many protocols that work together in various combinations to provide protection for communications. IPSec is flexible enough to meet many needs, because this it's works in network layer. But there are other protocols such as (PPP, PPTP,L2TP, ….) that provide a better solution, Cisco, the largest manufacturer of IP routers, offers VPN-IPSec implementation in its routers.

The purpose of this paper is to present and explain the steps necessary to configure tunnel mode IPSec between two Cisco routers. In order to provide a thorough understanding of the configuration.

الخلاصـــــة

ان الشبكات الوهمية (VPN)، هي تكنولوجيا تضمن نقل المعلومات بصورة امنية وسرية بين الشبكات، ويمكن استخدامها ضمن الشبكات العامة ومنها شبكة الانترنت وهذا يضمن الكلفة القلية في حال استخدام الشبكات العامة لكون انشاء شبكة خاصة لنقل المعلومات تكون مكلفة جدا، وقد زاد استخدام هذا النوع من الحلول في الشركات والمؤسسات التي تحوي عدة فروع حيث يتم ربط الفروع ببعضها بشبكات وهمية سرية (VPN) ضمن الشبكات العامة (الانترنت) وذلك لنقل المعلومات بسرية عالية وبكلفة قليلة. ان هذه الشبكات الوهمية (VPN) تستخدم عدة تقنيات وبرتوكولات لتزيد من قوة النقل الامن للمعلومات لكن من اهمها واقواها هو برتوكول (IPSec) لكونه يتعامل مع الطبقة الثالثة طبقة الشبكة (Network Layer). شركة سيسكو اكبر منتج للموجهات قد ضمنت منتجاتها هذه القابلية لانشاء الشبكات الوهمية (VPN) باستخدام برتوكول (IPSec).

سوف يتناول بحثنا هذا تصميم وانشاء وفحص شبكة وهمية بين موقعين وذلك لنقل المعلومات ضمن الشبكة العامة (الانترنت) بسرية عالية باستخدام موجهات سيسكو (Cisco Routers).

1. Introduction

With the growth and versatility of the internet, security has become a primary focus of companies large and small. Organizations often need to transfer proprietary data between geographically separated branch offices. Where as leased lines provide a secure way of doing this, they are not economically feasible for small or mid-sized businesses. A secure way to communicate over the pre-existing infrastructure of the internet is the only viable solution for such cost conscious businesses [1].

Security can be built in different layers of the OSI model. Link-layer security for example offers great protection but is only feasible for a private network not separated by large geographic distances. On the world wide web of the internet, security must be implemented on higher layers. One solution is presented by the various security offerings at the application layer. However, these technologies are cumbersome and inefficient since each application must implement its own application specific security architecture. The solution lies in offering security on the layer that is common to the vast infrastructure of the internet which is the network layer. Since the expansive architecture of the internet primarily shares the same protocol, the Internet Protocol, to interconnect nodes and hosts at the network layer, it is most desirable that a security solution be implemented uniformly at this layer. IPSec offers exactly such a solution to VPN [2].

2. Type of VPNs

There are several types of VPNs depending on the functional requirements, so that for each method of construction a type of VPN is available. The process of selection should include consideration of what problem is being solved, risk analysis of the security provided by a particular implementation, issues of scale in growing the site of the VPN, and the complexity involved in both implementing the VPN, as well as, ongoing maintenance and troubleshooting , as shown in Figure (1) [3].

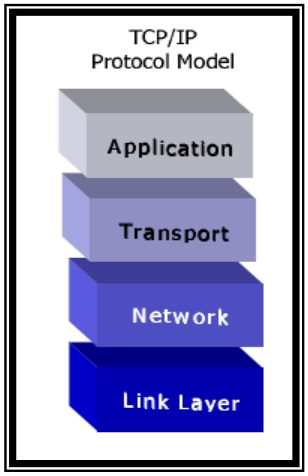

Figure (1) TCP/IP protocol mode

2-1 Data Link Layer VPNs

With data link layer VPNs, two private networks are connected on Layer 2 of the OSI model using a protocol such as Frame Relay or ATM. Although these mechanisms provide a suitable way of creating VPNs, they are often expensive, because they require dedicated Layer 2 pathways to be created. Frame Relay and ATM protocols inherently do not provide encryption mechanisms. They only allow traffic to be segregated based on which Layer 2 connection it belongs to. Therefore, if you need further security, it is important to have some sort of encryption mechanism in place [3].

2-2 Network Layer VPNs

The network layer in the TCP/IP protocol suite consist of the IP routing system – how reach ability information is conveyed from one point in the network to another.

Most VPNs use the concept of tunneling to create a private network that extends across the Internet. Conceptually, it's as if a secure tunnel has been built between two end devices (routers, firewall, or VPN device). Data can be directed into one end of the tunnel and it travels securely to the other end. These end devices, or tunnel interfaces, are typically the perimeter router firewalls for the LANs being connected.

Technically, no tunnel exists and the process doesn't resemble a tunnel, but the term "tunneling" somewhat describes the end result of traffic being able to pass through a non-secure environment without concerns about eavesdropping, data hijacking, or data manipulation. *Tunneling* is a process of encapsulating an entire data packet as the payload within a second packet, which is understood by the network and both end points. Depending on the protocols used, the new payload the original packet can be encrypted. Figure (2) is a common graphical representation of Layer 3 tunneling technology. The tunneling process requires three different protocols [3 - 5].

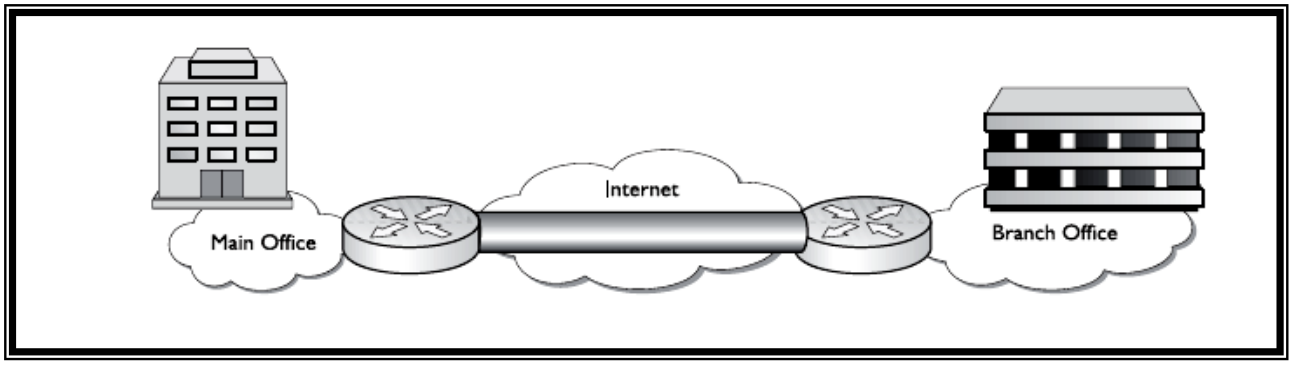

Figure (2) layer 3 tunneling technology

2-3 Transport and Application Layer VPNs

While VPNs can certainly be implemented at the transport and application layers of the protocol stack, it is not very common. The most prevalent method of providing virtualization at these layers is to use encryption services at either layer. For example, encrypted e-mail transactions, or perhaps authenticated DNS (Domain Name System) zone transfers between different administrative name servers, as described in DNSSec (Domain Name System Security). There is some interesting, and perhaps extremely significant, work being done in the IETF to define a Transport Layer Security protocol (TLS), which would provide privacy and data integrity between two communicating applications. The TLS protocol, once finalized and deployed, would allow applications to communicate in a fashion that is designed to prevent eavesdropping, tampering, or message forgery. It is unknown at the time of this writing, however, how long it may be before this work is finalized, or if it will be embraced by the networking community as a whole once the protocol specification is completed. The significance of a "standard" transport layer security protocol, however, is that once implemented, it could provide a highly granular method for the virtualizing communications in TCP/IP networks, thus making VPN's a pervasive commodity, and native to all desktop computing platforms [6].

3. Network VPN Protocols

3-1 IPSEC

IPSec stands for Internet Protocol Security. It is a suite of protocols developed by the Internet Engineering Task Force (IETF) to allow for the implementation of security features in data traversing over the IP protocol. It accomplishes these using three main features as part of the suite of protocols [3, 5]:

1) A key exchange feature known as Internet Key Exchange (IKE),
2) An authentication-only feature known as Authentication Header (AH), and
3) A combined authentication and encryption feature known as Encapsulating Security Payload (ESP).

3-1-1 Internet Key Exchange (IKE)

The Internet Key Exchange (IKE) protocol is a key management protocol standard which is used in conjunction with the IPSec standard, The purpose of the (IKE) protocol is to negotiate, create, and manage security associations, Security Association (SA) is a generic term of asset of values that define the IPsec features and protections applied to a connection, that can also be manually created, using values agreed upon in advance by both parties, but these SAs cannot updated, this method does not scale for real – life large – scale VPNs. IKE is a hybrid protocol which implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.) IKE automatically negotiates IPSec security associations (SAs) and enables IPSec secure communications without costly manual preconfiguration. [3, 5]
Specifically, IKE provides these benefits [3]:

- Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers.
- Allows you to specify a lifetime for the IPSec security association.
- Allows encryption keys to change during IPSec sessions.
- Allows IPSec to provide anti-replay services.

- Permits Certification Authority (CA) support for a manageable, scalable IPSec implementation.
- Allows dynamic authentication of peers.

3-1-2 Authentication Header (AH)

AH is one of the IPsec security protocols that provides integrity protection for packet headers and data, as well as user authentication. It can optionally provide replay protection and access protection. AH cannot encrypt any portion of packet. The initial version of IPSec, Encapsulation Security Payload (ESP) protocol, could provide only encryption, not authentication, so AH and ESP were often used together to provide both confidentiality and integrity protection for communications. Because authentication capabilities were added to ESP in the second version of IPSec, AH become less significant; in fact, some IP version software no longer support AH. However, AH is still of value because AH can authenticate portion of packets that ESP cannot [3].

AH have two modes: transport and tunnel. In tunnel mode, AH creates a new IP header for each packet as shown in figure.(3); in transport mod, AH does not create a new IP header as shown in figure.(4). In IPSec architectures that use a gateway, the true source or destination IP address for packets must be altered to the gateway's IP address. Because transport mode can not alter the original IP header or create a new IP header, transport mode is generally used in host– to host architectures [3, 6].

New IP Header	***AH header***	***Original IP header***	***transport and application protocol headers and data***
Authenticated (integrity protection)			

Figure (3) AH tunnel mode packet

IP Header	***AH header***	***transport and application protocol headers and data***
Authenticated (integrity protection)		

Figure (4) AH transport mode packet

3-1-3 Encapsulating Security Payload (ESP)

ESP is the second core IPsec security protocol. In the initial version of IPSec, ESP provided only encryption for packet payload data. Integrity protection was provided by the AH protocol if needed, in the second version of IPSec, ESP become more flexible. It can perform authentication to provide integrity protection, although not for outermost IP header. Also, ESPs encryption can be disabled through the null ESP encryption algorithm , therefore, in all but the oldest IPSec Implementations, ESP can be used to provide only encryption and integrity protection; or only integrity protection [3, 4].

a ESP Modes

ESP has two modes: transport and tunnel. In tunnel mode, ESP creates a new IP header for each packet. The new IP header lists the endpoint of the ESP tunnel (such as two IPSec gateways) as the source and destination of the packet. Because of this, tunnel mode can be used with all three VPN architecture models as shown in figure (5) [6] .

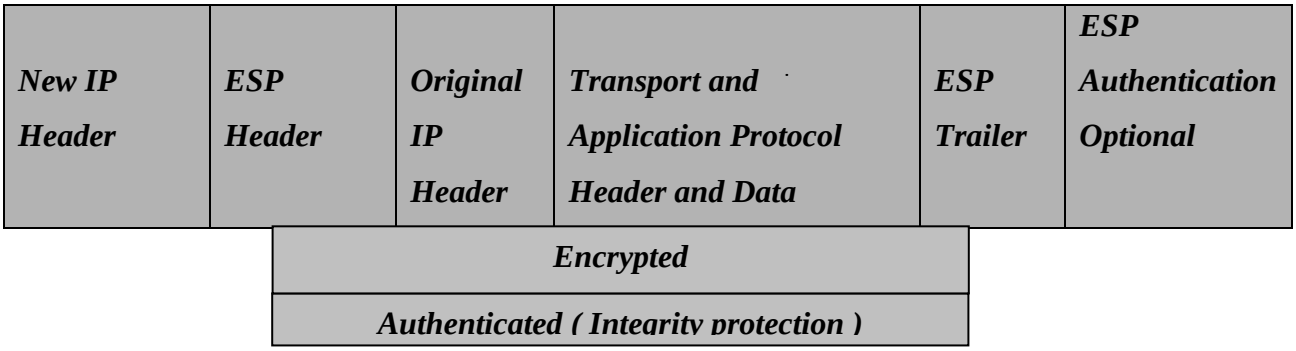

Figure (5) tunnel mode packet

In Transport mode, ESP uses the original IP header instead of creating a new one. ESP can only encrypt and/or protect the integrity of packet payloads and certain ESP components, but not IP header. As with AH, ESP transport mode is generally used only in host to host architecture as shown in figure (6). Also, transport mode is incompatible with NAT [3, 6].

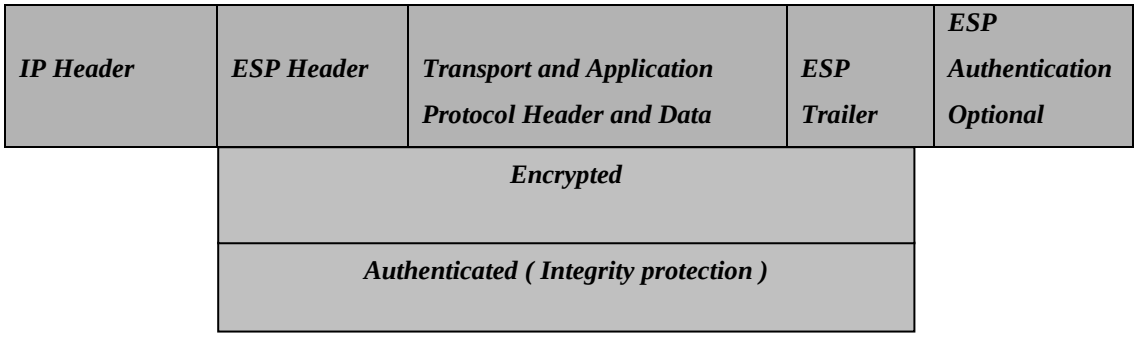

Figure (6) ESP Transport Mode Packet

4. Data Link Layer VPN Protocols

Data link layer VPN protocols function below the network layer in the TCP/IP model. This means that various network protocols such as IP, IPX, and Net BEUI, dually be used with a data link layer VPN. Most VPN protocols (including IPsec) only support IP, so data link layer VPN protocols may provide a viable option for protecting networks running non – IP protocols. The most commonly used data link layer VPN protocols are as follows: [4].

4-1 Point to Point Tunneling Protocol (PPTP) Version 2

PPTP provides a protected tunnel between a PPTP enable client and a PPTP – enabled server. Each system that may use PPTP needs to have PPTP client software installed and configured appropriately. The original version of PPTP contained serious

security flaws. PPTP version 2 addressed many of these issues, but researchers have identified weakness with it as well [5].

4-2 Layer 2 Tunneling Protocol (L2TP)

Like PPTP, L2TP protocol communication between a L2TP enabled client and an L2TP – enabled server, and it require L2TP client software to be installed and configured on each user system. L2TP often uses IPsec to provide encryption and key management[7].

5. Models for VPN Architecture

5-1 Gateway to Gateway

It connects two networks by deploying a gateway to each network and establishing a VPN connection between the two gateways. Connections between hosts on the two networks are then passed through the VPN connection, which provide protection for them. No protection is provided between each host and its local gateway. The gateway to gateway is most often used when connecting two secured network, such as branch office and headquarter, over an internet this is often replaces more costly private WAN circuits. Gateway to gateway VPN are typically transparent to users and do not involve installing or configuring any software on client or servers [7].

5-2 Host to Gateway

It connect hosts on various networks without hosts on the organization's network by deploying a gateway to organization's network and permitting external hosts to establish individual VPN connections to that gateway communications are protected between the host and the gateway, but not between the gateway and the destination hosts within the organization. The host to gateway model is most often used when connecting hosts on unsecured networks to resources on secured networks, such as linking traveling employees to headquarter over the internet. Host to gateway VPNs are typically not transparent to users because each user must authenticate before using the VPN and each host must have VPN client software installed and configured [6 , 7].

5-3 Host to Host

It connects hosts to single target host by deploying VPN software to each host and configuring the target host to receive VPN connections from the other hosts. This is the only VPN model that provides protection for data throughout its transit.

It is most often used when a small number of users need to use or administer a remote system that requires the use of insecure protocol and can be updated to provide VPN services. The host to host model is resource intensive to implement and maintain because it requires configuration on each host involved, including the target [7].

6. Proposal System

6-1 Introduction

The proposed system will use Cisco Router 2600 series to build secure tunnel between two or more locations using the traditional WAN (Internet). The goal is to build and test the proposed system for transferring information between these locations in secure tunnel. Also the test will explain how to make sure that the connection is active for data transformation.

6-2 Cisco Router

Cisco is unrivaled world wide leader networking for the Internet. Cisco products make it simple for people to access and transfer information without regard to differences in time, place, or platform. Cisco provides end to end networking solution that customers can use to build an efficient, unified information infrastructure [8].

The Internetwork Operating System (IOS) is what runs Cisco router and also Cisco switches, and it allows you to configure the devices as well. The Cisco IOS was created to divider network services and enable network applications that runs on most Cisco routers, These are some of the important things the Cisco IOS software is responsible for :

1. Carrying network protocols and functions.
2. Connecting high speed traffic between devices.
3. Adding security to control access and stop unauthorized network use.
4. Providing scalability in case of network growth and redundancy.
5. Supplying network reliability for connecting to network resources.

In this system any Cisco router supports IPSec protocol and VPN that can be used. Cisco 2621xm series is the selected type it is a Modular Multi-services Router Family the most widely deployed Cisco 2600 series. It is a ccost – effective solutions to meet to days and tomorrow's branch office needs for [8]:

1. Multi-services voice / data integration.
2. Virtual private network (VPN) access with firewall options.
3. Analog and digital dial access services.
4. Routing with bandwidth management.
5. Inter – VLAN routing.
6. Delivery of high speed business class DSL access.
7. Cost effective T1 / E1 ATM access [8].

6-3 Practical System Implementation

The system explains all implement of secure tunnels of VPN Network between two locations. Each location has a private Network connected to the Internet via a router (2600 series), as shown in Figure (7).

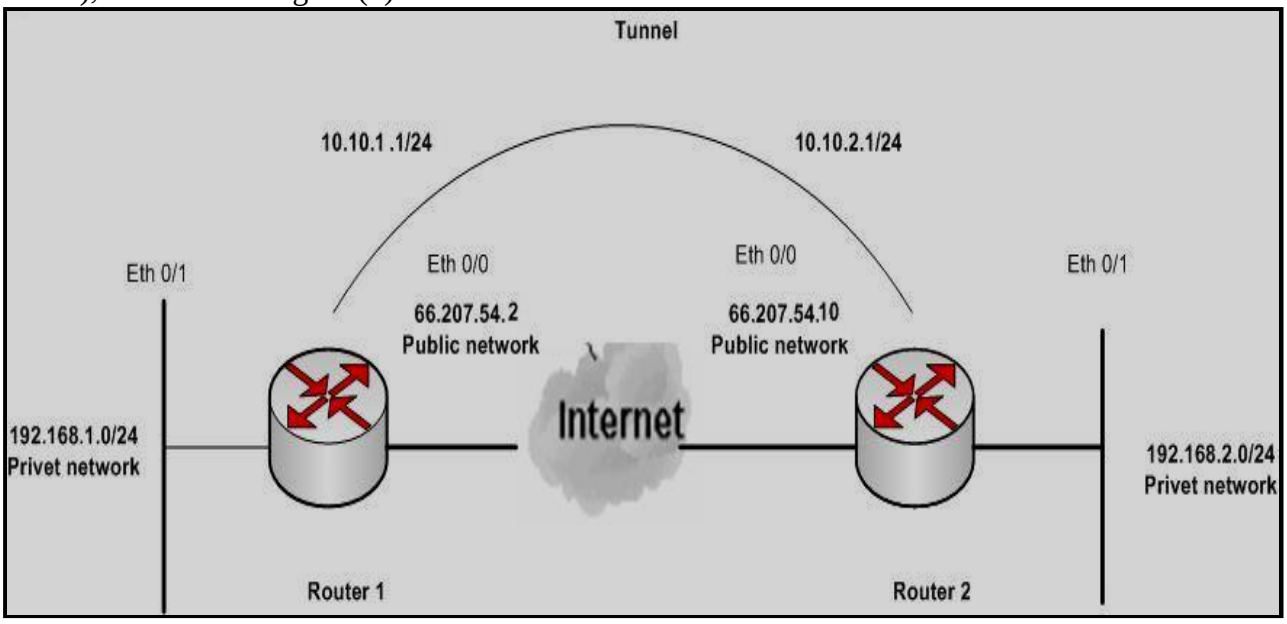

Figure (7) secure tunnel f VPN

6-3-1 System Requirements

a. Two Routers (Cisco 2621xm series).
b. Traditional network (Internet) in two locations.
c. Computers (at least two) connected to network.

6-3-2 Information of Router 1

a. Interface Fast Ethernet 0/0.
b. Interface Fast Ethernet 0/1.

6-3-3 Configuration of Router 1

a. **Management** :

Let host name of router 1, Router 1
Enable password, Cisco
Enable secret, Cisco

a. Interface:

Interface fast Ethernet 0/0
IP address 66.207.54.2
Subnet mask 255.255.255.0
IP nat out side

Interface fast Ethernet 0/1
IP address 192.168.1.0
Subnet mask 255.255.255.0
IP nat inside

b. DHCP :

IP DHCP pool VPN
Network: 192.168.1.0
Default Router : 192.168.1.1
DNS 216.147.131.33 216.147.131.34

c. Tunneling

Interface Tunnel 1
IP address 10 . 10 . 1 . 1 255 . 255 . 255 .0
Tunnel source fast Eth 0 / 0
Tunnel destination 66 . 207 . 54 . 10
Set the encryption key cisco
Encryption 3des

d. Access List

Access list 101
Permit IP host 66 . 207 . 54 . 2

Permit IP host 66 . 207 . 54 . 10

e. Routing

IP Route 192 . 168 . 1 . 0 Subnet mask 255 . 255 . 255 . 0 Tunnel 1

6-3-4 Information of Router 2

a. Interface fast Ethernet 0/0

b. Interface fast Ethernet 0/1

6-3-5 Configuration of Router 2

f. Management :

Let host name of router 2, Router 2

Enable password, Cisco

Enable secret, Cisco

g. Interface :

Interface fast Ethernet 0/0
IP address 66.207.54.10
Subnet mask 255.255.255.0
IP nat out side

Interface fast Ethernet 0/1
IP address 192.168.2.0
Subnet mask 255.255.255.0
IP nat inside

h. DHCP :

IP DHCP pool
Network : 192.168.2.0
Default Router : 192.168.2.1
DNS 216.147.131.333 216.147.131.34

i. Tunneling

Interface Tunnel 1
IP address 10 . 10 . 2 . 1 255 . 255 . 2 55 .0
Tunnel source fast Eth 0 / 0
Tunnel destination 66 . 207 . 54 . 10
Set the encryption key cisco
Encryption 3des

j. Access List

Access list 101

Permit IP host 66 . 207 . 54 . 10
Permit IP host 66 . 207 . 54 . 2

k. **Routing**

IP Route 192 . 168 . 1 . 0 255 . 255 . 255 . 0 Tunnel 1

6-3-6 The Results

The result can be taken by using two command Prompt instruction that be used to test the system:

a. ***ipconfig:*** that can be used to explain the network configuration to be taken from the router, containing the IP address, subnet mask and default gateway,

b. ping: is the instruction that sends a series of packets over a network or the Internet to a specific computer or URL in order to generate a response from that computer or URL. The other side responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

For each side the test is started by taken the ***ipconfig (network information)*** to check if the computer takes the correct network setting from the router. The second step is to test the connectivity of each device by using the ***ping*** instruction for each IP in the system to check step by step the connection until reaching the other side. Then repeat the procedure from the other side to make sure the connection is active from both side.

i) The result of Router 1

Step 1 :

a. ipconfig
b. Pinging 192 . 168 . 1. 1
c. Pinging 66 . 207 . 54 . 2

From Figure(8), first step appears the result of ***ipconfi***g instruction, IP address, subnet mask, and default gateway that is taken from router 1, that is mean we are connect to router 1, and Dynamic Host Configuration protocol **(DHCP)** work right, also the second instruction ***(ping)*** showing the reply of ping to the fist IP address **(192.168.1.1 for inside interface of router 1)** also for the second IP address **(66.207.54.2 for outside interface of router 1)**

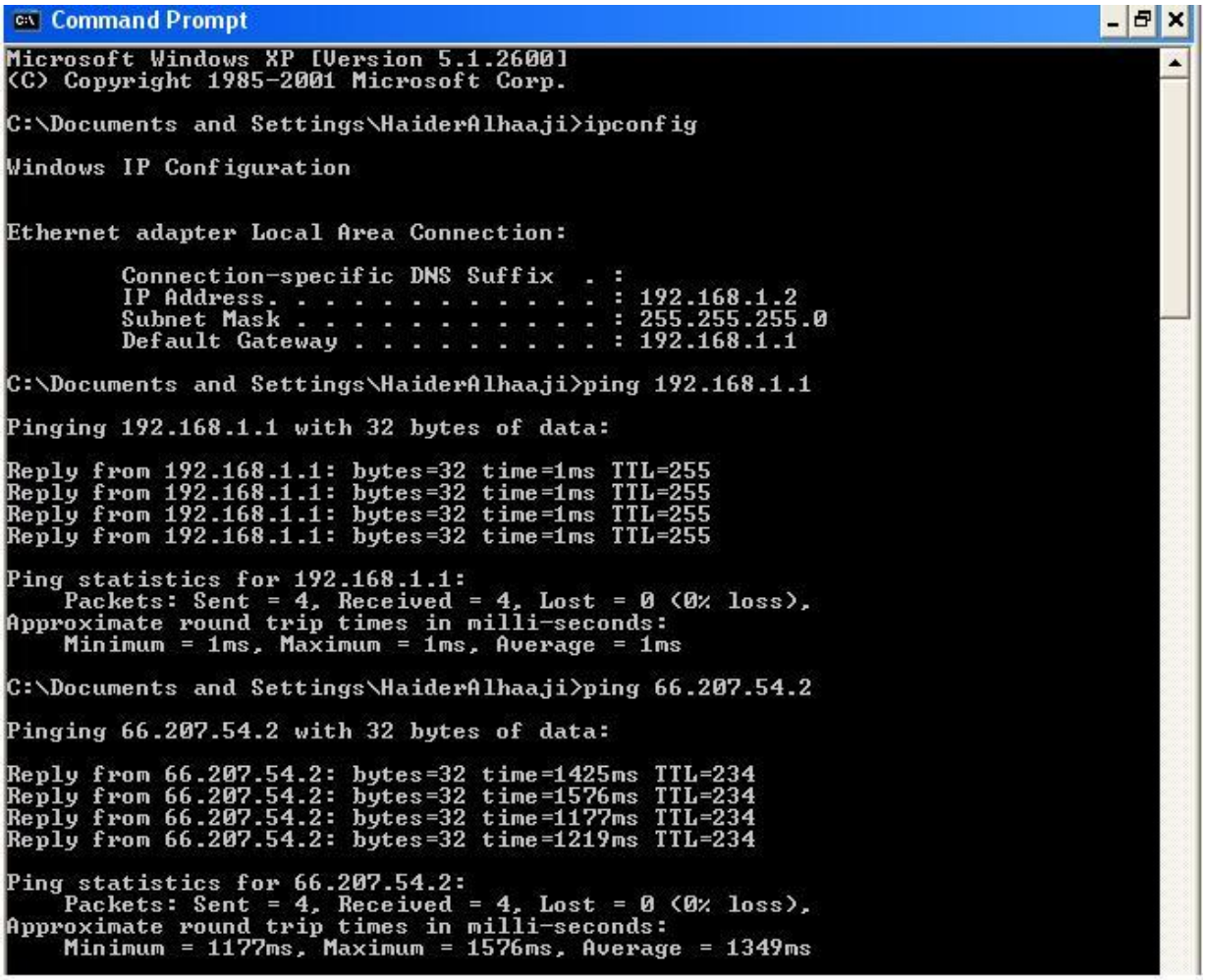

Figure (8) result 1 of rout

Step 2 :

a. Pinging 10 . 10 . 1. 1
b.Pinging 10 . 10 . 2 . 1
c.pinging 66 . 207 . 54 . 10

There is a reply from **10 . 10 . 1 . 1** (tunnel ip address of router 1), reply from **10 . 10 . 2 . 1** (tunnel ip address of router 2) and reply from **66 . 207 . 54. 10 (outside interface of router2)** as shown in Figure (9).

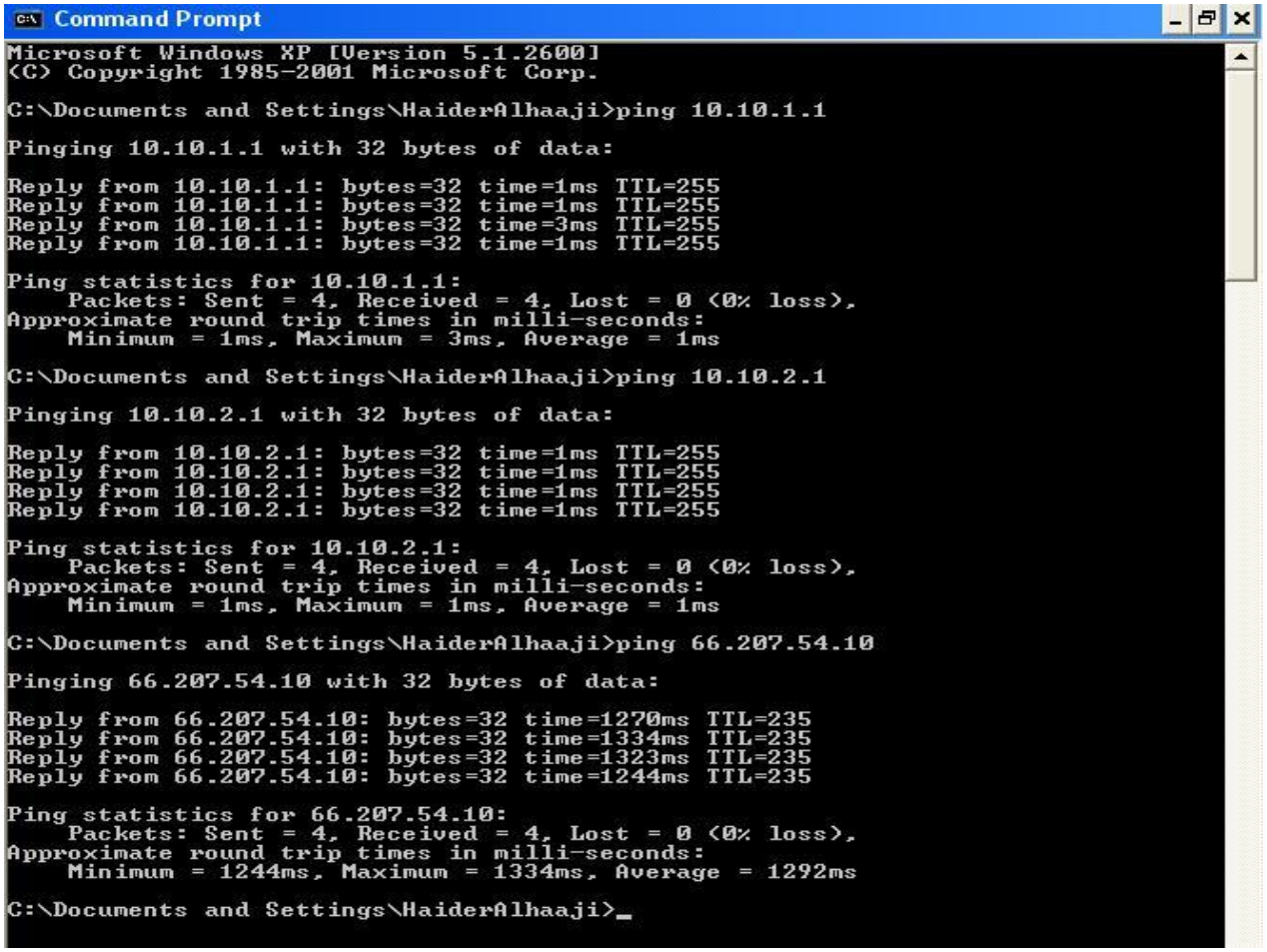

Figure (9)result 2 of router 1

Step 3 : Pinging 192 . 168 . 2. 1

According to the received replies, the link is active, because each packet send from router 1 will be received from router 2 this means the link active and the information will be transferred between Routers via the created VPN tunnel, as shown in Figure (10).

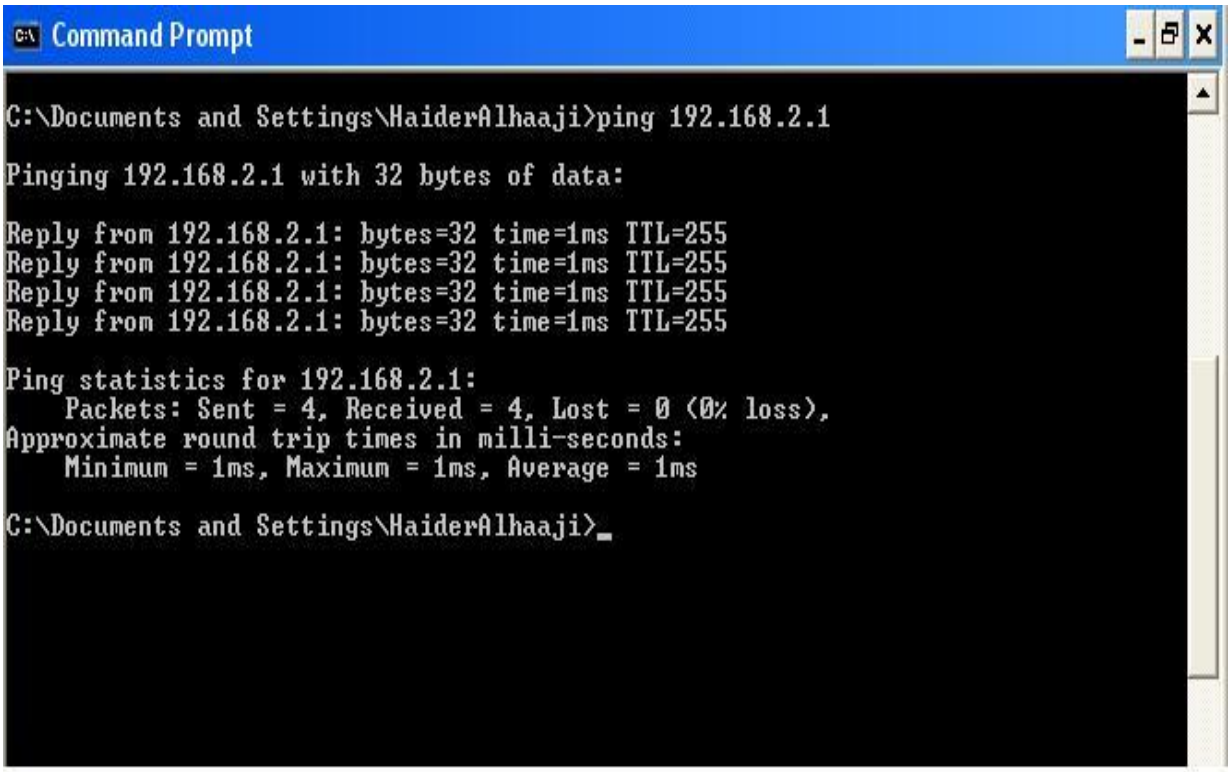

Figure (10) result 3 of router 1

ii) Result of Router 2

The same procedure will be used for router 2 to make sure that the link is active from the second side

Step 1 :

a. Pinging 192 . 168 . 2. 1

b. Pinging 66 . 207 . 54 . 10

As shown in Figure (11) ***ipconfi***g instruction, show IP address, subnet mask, and default gateway that is taken from router 2. Also ***(ping)*** showing the reply of the first IP address **(192.168.2.1 for inside interface of router 2)** also for the second IP address **(66.207.54.10 for outside interface of router 2)**

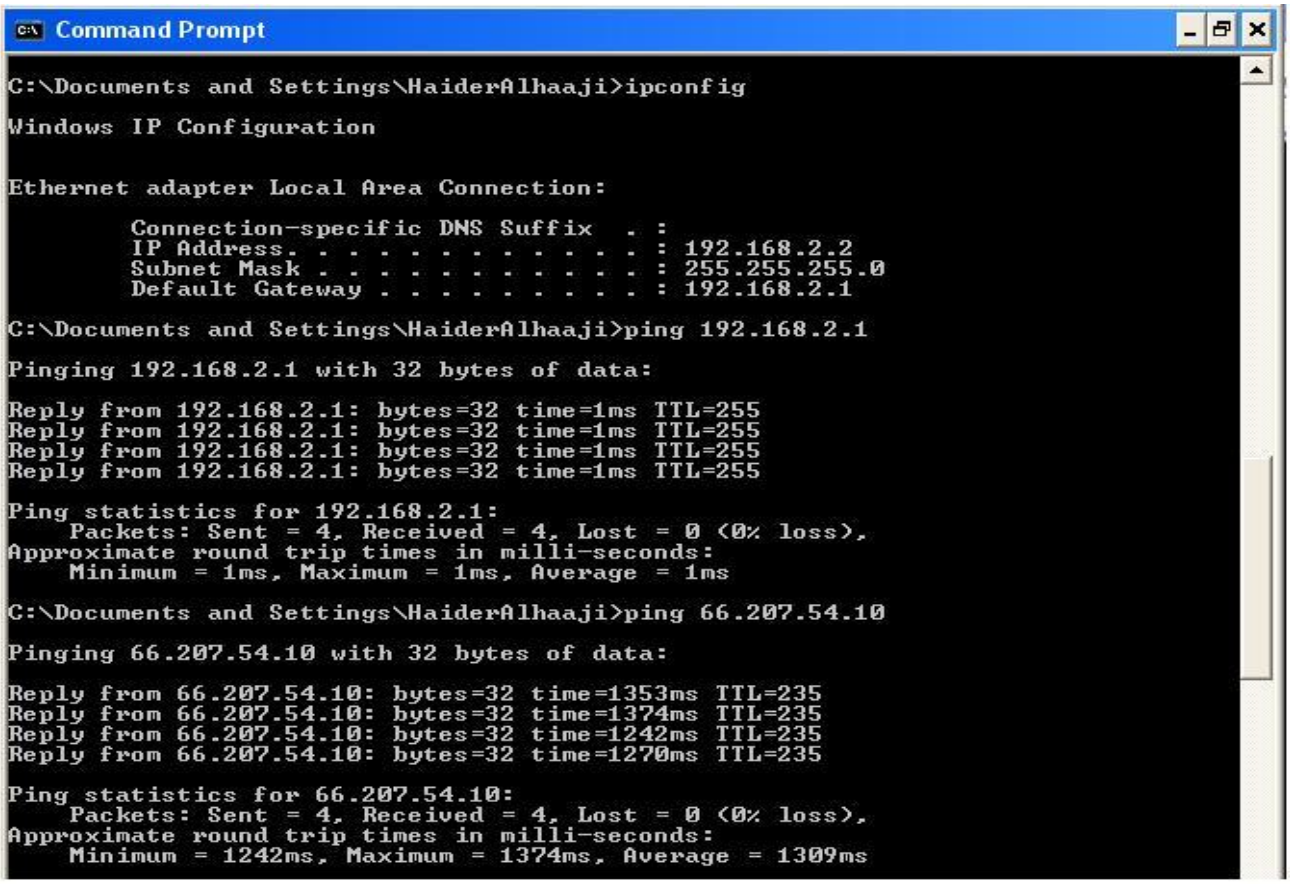

Figure (11) result 1 of router 2

Step 2 :

a. Pinging 10 . 10 . 2. 1
b. Pinging 10 . 10 . 1 . 1
c. pinging 66 . 207 . 54 . 2

There is a reply from 10 . 10 . 2 . 1 **(tunnel IP address of router 2)**
There is a reply from 10 . 10 . 1 . 1 **(tunnel IP address of router 1)**
There is a reply from 66 . 207 . 54. 2 **(outside interface of router1)**

According to the received replies, the link is active, as shown in Figure (12).

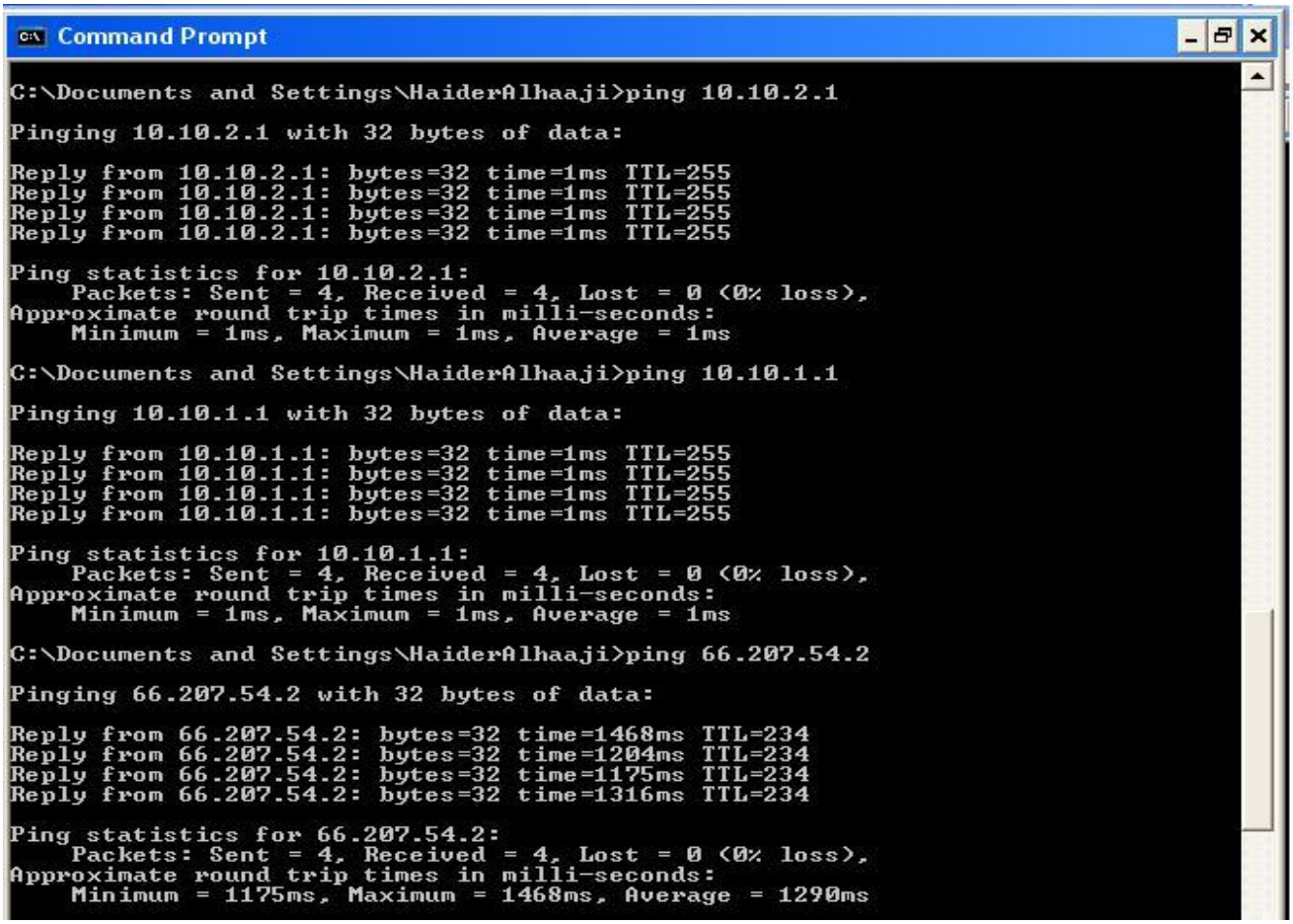

Figure (12) result 2 of router 2

Step 3 :

Pinging 192 . 168 . 1. 1

Finally the result from Router2 shows that the link is active and the packets that send are received from Router1 according to these results as shown in Figure (13). The VPN tunnel is initiated and it is active for data communication.

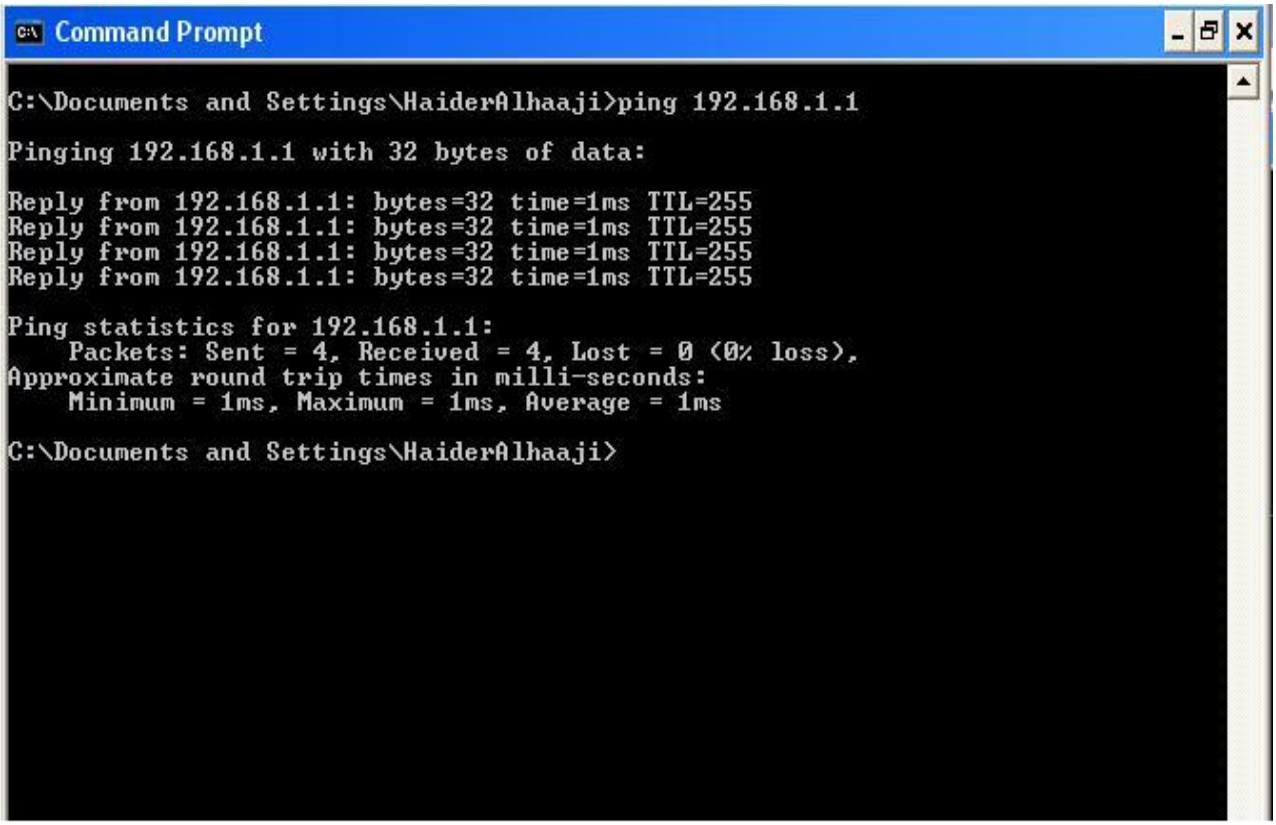

Figure (13) result 3 of router 2

7. Conclusion

In this paper, the explanation of the method of configuring tunnel-mode IPSec on Cisco routers was done to create a VPN over an insecure network (i.e. internet) for the purposes of providing secure communications between two sites. at a small scale, IPSec can be configured using manual key management. When the number of interconnected sites is large, an automated key management protocol, IKE, is more feasible. In both cases, Cisco routers offer a comprehensive solution for configuring IPSec to allow businesses to securely share data over the pre-existing internet infrastructure, thus providing an economical and cost-effective alternative to leased lines.

8. References

1. Fouzan M. ***"configuration of Tunnel mode IPSec VPN using cisco Routers"*** SANS institute, GIAC Practical, November, 2003.
2. Paul F. ***" What is a VPN – Part I",*** The Internet Protocol Journal – Volume 1, No.1, Aug. 2007 cisco press.
3. Robert E. Larson and Lance C. ***"Cisco Certified security Professional certification"*** ,McGraw-Hill ,2003.
4. Millie I. ***"Implementing Site-to-Site IPSec VPN using cisco Routers"*** .SANS institute, GIAC Practical , 2002.
5. Rawl F. and Geoff H. ***"What is a VPN "*** .Published April 1998 Revision 1. Cisco press.
6. Vitaly O. and Mike S. ***"Cisco PIX Firewall"*** .Syngress publishing, 2002,
7. Todd L. ***"Securing Cisco IOS Networks"*** SYBEX Publisher, 2003.
8. ***" Cisco 2006 series Modular Access Routers "*** Data Sheet of 2600 router from URL *http://www.cisco.com/en/US/prod/collateral/routers/ps259/product_data_sheet0900aecd800fa5be.html*