Packet Transfer Through TCP/IP

وضاح صبري ابراهيم* علياء هاشم محمد**

Abstract

Internet has penetrated the international border in different parts of the globe and has become exceptionally quickly to the most effective means to transfer detailed information and interactive on various critical aspects of the activities of individuals and human societies.

The village has become the electronic world now is the best evidence of the transfer of information, communications and networking among human societies place limits without permission or passport to enter or transit. Despite this, the users of this network of people who have no knowledge of the protocols for this information transfer network.

Through this research to look at how the transfer of information within the network and offer Packet Transfer Through TCP/IP Reference Model.

لقد اخترق الانترنيت الحدود الدولية في مختلف أنحاء الكرة الأرضية وتحولت بسرعة استثنائية إلى الوسيلة الأكثر فاعلية في نقل المعلومات التفصيلية والتفاعلية حول مختلف الجوانب الحيوية من نشاطات الإفراد والمجتمعات البشرية.

ولعل القرية الالكترونية التي أصبح عليها العالم ألان لهو خير دليل على عملية نقل المعلومات والرسائل والتواصل بين المجتمعات البشرية بدون حدود للمكان أو إذن للمرور أو جواز للدخول، ورغم هذا فان الأشخاص المستخدمين لهذه الشبكة ليس لديهم أي معرفه بالبروتوكولات الخاصة بهذه الشبكة لنقل المعلومات.

من خلال هذا البحث سنتطرق فيه إلى كيفية تناقل المعلومات داخل الشبكة وذلك بعرض نقل رزمة من خلال النموذج المرجعي TCP/IP.

* مدرس مساعد/ الجامعة المستنصرية/كلية الادارة والاقتصاد/ قسم الاحصاء

** مدرس مساعد/ الجامعة المستنصرية/كلية الادارة والاقتصاد/ قسم الاحصاء

1. Introduction

TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

It was initially successful because it delivered a few basic services that everyone needs (file transfer, electronic mail, remote logon) across a very large number of client and server systems. Several computers in a small department can use TCP/IP (along with other protocols) on a single LAN. The IP component provides routing from the department to the enterprise network, then to regional networks, and finally to the global Internet [Gilb95].

2. Network Hardware

Broadly speaking, there are two types of transmission technology:

1. Broadcast Network, have a single communication channel that is shared by all the machines on the network short message (packets) sent by any machine are received by all the others. An address field within the packet specifies for whom it is intended, upon receiving a packet, a machine checks the address field if the packet is intended for itself, it processes the packet, if the packet is intended for some other machine, it is just ignored.

It is also possible to address a packet to all destinations using a special code in the address field. Some broadcast systems support transmission to a subset of the machines, something known as multicasting. With this type one bit in the address field can be used to indicate multicasting and the remaining address bits can hold a group number. Each machine can subscribe to any or all of the groups.

2. Point- to- Point Networks consist of many connections between individual pairs of machines. To go from the source to the destination a packet may have to first visit one or more intermediate machines [Tane96].

3. Protocol Hierarchies

To reduce their design complexity, most networks are organized as series of layers or levels, each one built upon the one below it. The number of layers, the name of each layer, the contents of each layer, and the

function of each layer differ from network to network. However, in all networks, the purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented.

Layer N on one machine carries on a conversation with layer N on another machine. The rules and conventions used in this conversation are collectively known as the layer N protocol. Basically, a protocol is an agreement between the communicating parties on how communication is to proceed.

A five-layer network is illustrated in figure (1.1) the entities comprising the corresponding layers on different machines are called peers, in other words, it is the peers that communicate using the protocol.

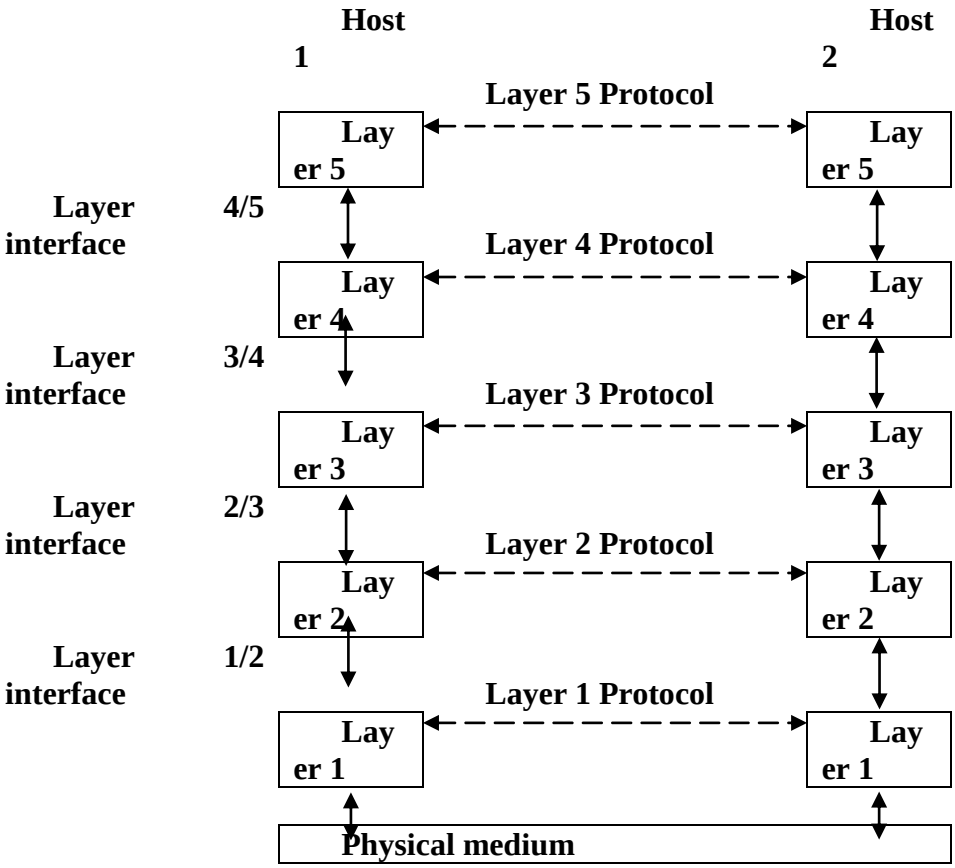


Figure (1.1) Layers, Protocols, and Interfaces

In reality, no data are directly transferred from layer N on one machine to layer N on another machine. Instead, each layer passes data and control information to the layer immediately below it, until the lowest layer is reached. Below layer 1 is the physical medium through which actual communication occurs.

Between each pair of adjacent layers there is an interface. The interface defines which primitive operations and services the lower layer offers to the upper one, a set of layers and protocols is called a network architecture. Neither the details of the implementation nor the specification of the interfaces are part of the architecture because these are hidden away inside the machines and not visible from the outside[Tane96].

3.1 Interfaces And Services [Tane96]

The user service provided by a layer are specified by a set of service primitives, associated with each service primitive is a define set of parameters [Hals96]. The function of each layer is to provide services to the layer above it. The action elements in each layer are often called entities. Entities in the same layer on different machines are called peer entities. The entities in layer N implement a service used by layer N+1 in this case layer N is called the service provider and layer N+1 is called the service user. Layer N may use the services of layer N-1 in order to provide its service it may offer several classes of service.

Services are available at SAPs (Service Access Points). The layer n SAPs are the places where layer N+1 can access the services offered. Each SAP has an address that uniquely identifiers it.

In order for two layers to exchange information, there has be an agreed upon set of rules about the interface. At a typical interface, the layer N+1 entity passes an IDU (Interface Data Unit) to the layer N entity through the SAP . the IDU consists of an SDU (Service Data Unit) and some control information. The SDU is the information passed across the network to the peer entity and then up to layer N+1. the control information is needed to help the lower layer do its job but is not part of the data itself.

In order to transfer the SDU, the layer N entity may have to fragment it into several pieces, each of which is given a header and sent as a separate PDU (Protocol Data Unit) such as a packet. The PDU headers are used by the peer entity to carry out their peer protocol. They identify which PDUs contain data and which contain control information, provide sequence numbers and counts, and so on.

3.2 Connection-Oriented And Connectionless Services [Tane96]

Layers can offer two different types of service to the layers above them: Connection- Oriented And Connectionless, Connection-oriented service is modeled after the telephone system, to use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection. The essential aspect of a connection is that it acts like a tube: the sender pushes objects (bits) in at one end, and the receiver takes them out in the same order at the other end.

In contrast, connectionless service is modeled after the postal system. Each message (letter) carries the full destination address, and each one is routed through the system independent of all the others, normally, when two messages are sent to the same destination, the first one sent will be the first one to arrive. However, it is possible that the first one sent can be delayed so that the second one arrives first. With a connection-oriented service this is impossible.

4. The Transmission Control Protocol

Transport protocols Provide reliability, which is fundamental for many applications. TCP service is obtained by having both the sender and receiver create end points, called sockets, Each socket has a socket number (address) consisting of the IP address of the host and a 16-bit number local to that host, called a port. To obtain TCP service, a connection must be explicitly established between a socket on the sending machine and a socket on the receiving machine.

A socket may be used for multiple connections at same time. In other words, two or more connections may terminate at same socket. Connections are identified by the socket identifiers at both ends, that is, (socket1, socket2). No virtual circuit numbers or other identifiers are used.

Port numbers below 256 are called well-known ports and are reserved for standards services. For example, any process wishing to establish a connection to a host to transfer a file using FTP can connect to the destination host's port 21 to contact its FTP daemon.

All TCP connections are full-duplex and point-to-point. When an application passes data to TCP, TCP may send it immediately or buffer it (in order to collect a large amount to send at once), at its discretion. However, sometimes, the application really wants the data to be sent immediately [Come99].

4.1 The TCP Protocol [Tane96]

Every byte on a TCP connection has its own 32-bit sequence number. For a host blasting away at full speed on a 10-Mbps LAN. The sending and receiving TCP entities exchange data in the form of segments. A segments consists of a fixed 20-byte header. The TCP software decides how big segments should be. It can accumulate data from several writes into one segment or split data from one write over multiple segments. Two limits restrict the segment size. First, each segment, including the TCP header, must fit in the 65,535 byte IP payload. Second, each network has a Maximum transfer unit (MTU), and each segment must fit in the MTU. The MTU is generally a few thousand through a sequence of networks without being fragmented and then hits one whose MTU is smaller than the segment, the router at the boundary fragments the segment into two or more smaller segments.

The basic protocol used by TCP entities is the sliding window protocol, when a sender transmits a segment, it also starts a timer. When the segment (with data if any exists, otherwise without data) bearing an acknowledgement number equal to the next sequence number it expects to receive. If the sender's timer goes off before the acknowledgement is received, the sender transmits the segment again.

4.2 The Service TCP Provides To Applications [Come99]

The service offered by TCP has seven major features:

Connection Orientation: TCP provides connection- oriented service in which an application must first request a connection to a destination, and then use the connection to transfer data.

Point-To-Point Communication: Each TCP has exactly two endpoints.

Complete Reliability: TCP guarantees that the data sent across a connection will be delivered exactly as sent, with no data missing or out of order.

Full Duplex Communication: A TCP connection allows data to flow in either direction, and allows either application program to send data at any time. TCP can buffer outgoing and incoming data in both directions, making it possible for an application to send data and then to continue computation while the data is being transferred.

Stream Interface: We say that TCP provides a stream interface in which an application sends a continuous sequence of octets across a connection. That is, TCP does not provide a notation of records, and does

not guarantee that data will be delivered to the receiving application in the same size pieces that it was transferred by the sending application.

Reliable Connection Startup: TCP requires that when two application create a connection, both must agree to the new connection; duplicate packets used in previous connections will not appear to be valid responses or otherwise interfere with the new connection.

Careful Connection Shutdown: An application program can open a connection, send arbitrary amounts of data, and then request that the connection be shut down. TCP guarantees to deliver all the data reliably before closing the connection.

5. The IP Protocol

When IP was first developed in 1970, the Internet world was very different. The Internet used for research and education. The success of the Internet has been so great that IP is embedded into the operation of many businesses and homes [Doyl01]. IP packets are the bundles of data that form the foundation for the TCP/IP protocol suite[Ches02.]The IP standard specifies that each host is assigned a unique 32-bit number known as the host's Internet Protocol address, which is often abbreviated IP address, or Internet address. Each packet sent across an internet contains the 32-bit IP address of the sender (source) as well as intended recipient (destination). Thus, to transmit information across a TCP/IP internet, a computer must know the IP address of the remote computer to which the information is being sent [Come99].

6. TCP/IP Layers Encapsulation

The research depends on this model. As we know the networks is a group of many devices connect to each other by way of connection subsequently will appear for us the known division for (OSI) organization for connection process which pass through 7 layers and every layer has it's own certain work to be add headers on the send data and abridgement till five layers in protocol TCP/IP figure (1.2) show that[Nooh05].

OSI	TCP/IP
Application	Applications SMTP, POP, HTTP FTP Telnet DNS
Presentation	
Session	
Transport	Transport TCP UDP
Network	Internet IP , ICMP, IGMP,ARB,RARP
Data link	Network Interface
Physical	Physical + Data Link

Figure (1.2) TCP/IP model with Reference to OSI model.

The operation of tuning send message begin in application layers and it's job treat with message itself and convert from text to data possible to send through network for example. the programs of chat possible convert the written text to ASCII code and then to set of binary codes or bit put in the matrix to prepare and send via socket which bind the transport layer with network layer or internet layer, figure (1.3) shows the socket work.

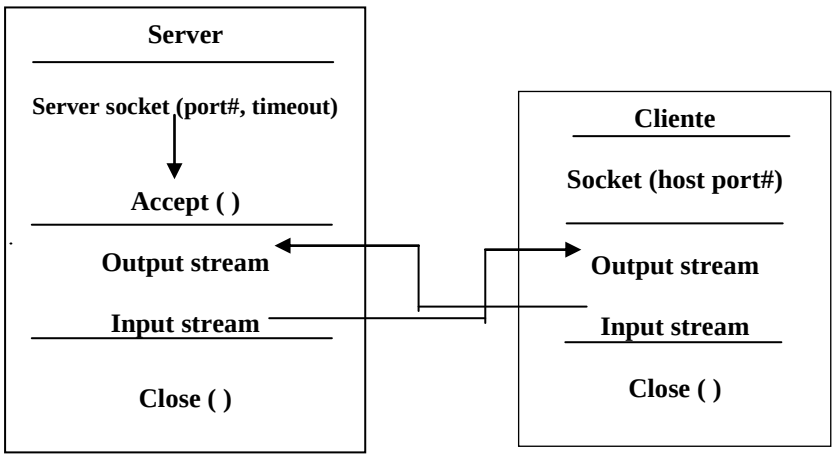


Figure (1.3) Nature of the socket work

Here the certain No. of the port bound to the transport layer with destination IP in network layer and the other side server in the other end will agree for clients demand and the socket work is limited in the server to bind the port No. with socket option which all ready be selected and now the beginning of *listen* to the port which was selected and in this stage it possible to make some condition to access in the conversation like destination in Authentication or such thing or agreement directly.

In the sample of OSI the upper layers was divided to three layers

I. Application :

To deal with program itself or which is called user interface.

II. Presentation:

Represent data as explained above by converting them to ASCII or using ways of compressing the data or coding.

III. Session:

In this operation connection between two devices will begin define them to each other (Conversation opening).

In the protocol TCP/IP there is Application layer which does the work of the first 3 layers in the OSI, in the session layer defining and conversation opening is made by many ways such as:-

1. Make primary connection in the server via IP and the selected port after naming the connection operation either via UDP or TCP.

2. The definition itself and the work of authentication if it will be required by the server.

3. Accept or refuse the conversation and it's done by sending acceptance to open conversation or refuse.

4. Begning of the conversation and the server will do the listening operation to the special port of program.

When the acceptance will be got for opening conversation and the beginning connection operation the cline will down load the message in the second layer which is the transport layer ,and in this layer select the nature of connection either via connection oriented protocol TCP or via connectionless UDP protocol, in the first protocol to side will be selected:- the sender &receiver(connection port) but in the UDP it possible that receiver end would be all the devices and that mean any on who listen via this port can receive this message and can do multicasting and that is done. Put broadcast IP or the multicast IP with the port No. in the socket.

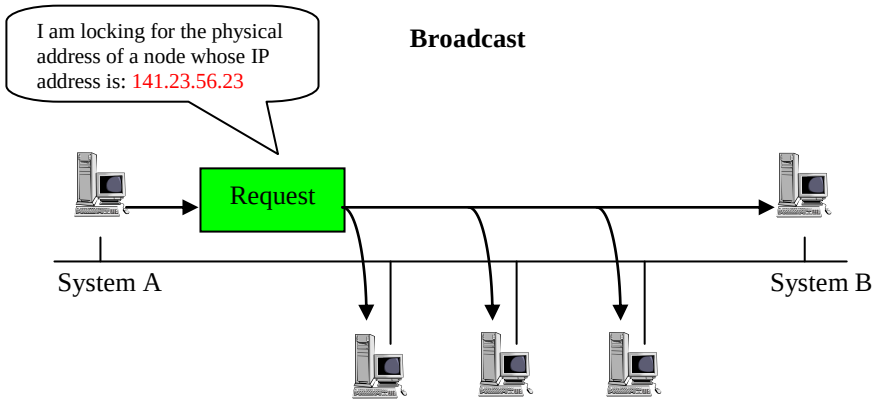
And for the sending the message through the network via TCP is used network stream and he's responsible dealing with the means of

communication and sending the message to the concerned part by a form stream data or with the use himself socket.

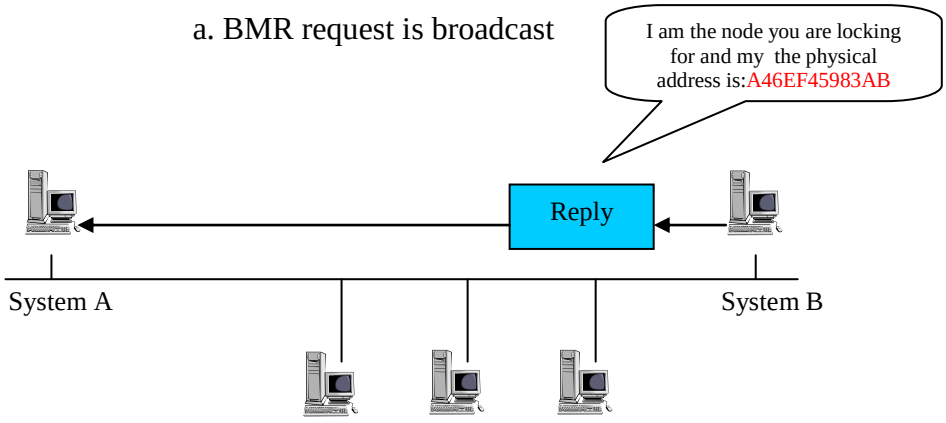
And after a rubbing it submits to network layer do completes the entitlement of the message and putting the address of recipient and the future on it and delivers to the lower layer so that it completes it's sending via physical

It carries out the message by the same classes but on an on the contrary where it receives the network card the bits to convert to data link then to network then to transport and then to application and from it a change from binary to ASCII to text.

By sending BMR Broadcast Message Request to the network to ask the owner of address IP who is wanted to send for. If he found him the selected device will send ICMP message telling his special address of MAC address and after receiving the message will save this address in his special MAC table so as to us it in the next times like as in the figure (1.4).



a. BMR request is broadcast



b. Send MAC address

And after this step the type of internet encapsulation or Ethernet encapsulation will be selected and that will be done in data link layer figure (1.5) .

Figure (1.4) Explain the broadcast

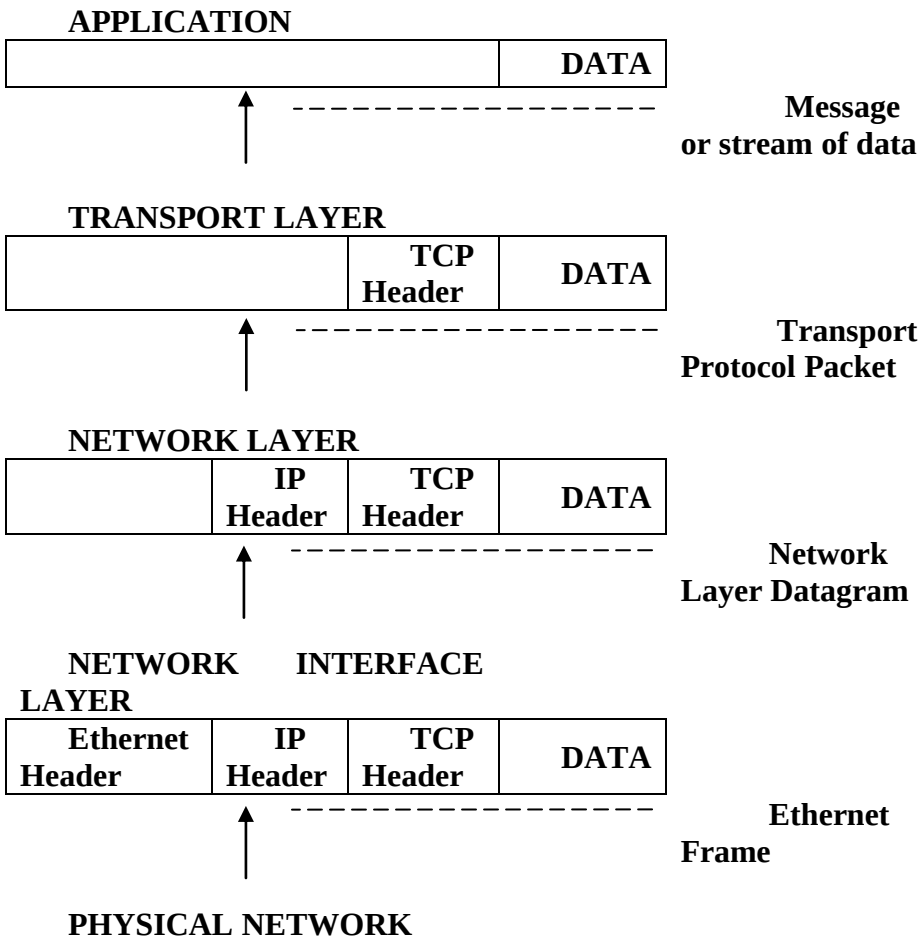


Figure 1.5 Explain of the layers work

And at the end the packet format like as in the figure (1.6).

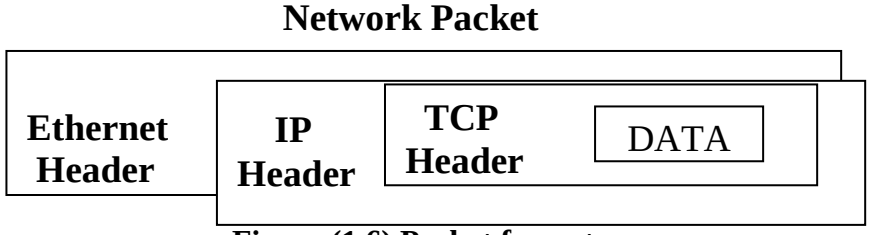


Figure (1.6) Packet format

5. Conclusions

1- TCP/IP is open standard; All of the documents describing the TCP/IP standard are available on the Internet for anyone to download and implement for free. There are no trade secrets or hidden implementation details limiting who may implement it.

2- TCP/IP is independent of any particular transmitting medium; TCP/IP will work over Ethernet, parallel port cables, or any other mechanism that allows two or more computers to exchange signals.

3- The model does not distinguish clearly between serves, interface and protocol, and Engineering design qualities of a good materiel Lin is a distinction between the specification and the specification on the ground.

4- The model TCP/IP form did not distinguish between the physical layer and the data link layer and until that it did not mention them clearly despite that they different totally.

The physical layer is interested in transmission via copper wires, optical or wireless communications, but the data link layer is defined beginning and ending of each framework and delivered from one party to another according to the degree of the required credibility

5- There are many of the other protocols in the model TCP/IP its designer in an exceptional and to special purposes and most probably way their designing takes place from some of the graduation students in the universities and when they become ready the university or the students themselves carry out their distribution for free get by network with the operating system

6. References

[Ches02] **Cheswick, W., "Firewalls and Internet Security", Addison Wesley professional computing series,2000**

[Come99] **Comer, D. E., "Computer network And Internets", Second Edition, Department of Computer Sciences, purdue University, Prentice- Hall, Inc., 1999.**

[Doyl01] **Doyle, J., "Routing TCP/IP volume II" ,Cisco Systems. Inc, 2001.**

[Gilb95] **Gilbert, H., "Introduction to TCP/IP", copyright 1995 PcLT. WWW.Yale.edu/Pult/comm/TCP/IP.HTM**

[Hals96] **Halsall, F., "Data Communications, Computer Networks and open system", Fourth Edition, Addision- wesley publishing company Inc., 1996.**

[Nooh05] **Nooh, A., "Development of Packet Filtering and Overload NAT Firewall Simulation" M. Sc Thesis, Iraqi Commission for Computers And Informatics, 2005.**

[Tane96] **Tanenbaum, A., "Computer Networks", International Edition Third Edition, Prentice- Hall, Inc., 1996 .**