Significance of TCP/IP Model

Divya Shree
Assistant Professor (Resource Person),
Department of computer science and engineering, UIET, MDU, Rohtak

Abstract: TCP/IP (Transmission Control Protocol/Internet Protocol) is a set of protocols independent of the physical medium used to transmit data, but most data transmission for Internet communication begins and ends with Ethernet frames. The Ethernet can use either a bus or star topology. A bus topology attaches all devices in sequence on a single cable. In a star topology all devices are wired directly to a central hub. 10Base-T uses a combination called a star-shaped bus topology because while the attached devices can share all data coming in on the cable, the actual wiring is in a star shape. The access method used by the Ethernet is called Carrier Sense Multiple Access with Collision Detect (CSMA/CD). This is a contention protocol, meaning it is a set of rules to follow when there is competition for shared resources.

Keywords: TCP/IP, Model, Hub, Ethernet, Transmission.

Introduction

All Ethernet interfaces have a unique 48-bit address that is supplied by the manufacturer. It is called the Ethernet address (also known as the MAC address, for Media Access Control). Ethernet-enabled Z-World boards store this value in Flash Memory (EEPROM) that is programmed at the factory.

A Realtek RTL8019 10Base-T interface chip provides a 10 Mbps Ethernet connection. This chip is used on many Ethernet-enabled Z-World boards. The corresponding port can be connected directly to an Ethernet network. By using hubs and routers, a network can include a large number of computers. A network might include all the computers in a particular building. A local network can be connected to the Internet by means of a gateway. The gateway is a computer that is connected both to the local network and to the Internet. Data that must be sent out over the Internet are sent to the local network interface of the gateway, and then the gateway sends them on to the Internet for routing to some other computer in the world. Data coming in from the Internet are directed to the gateway, which then sends them to the correct recipient on the local network.

Ethernet cables are similar to U.S. telephone plug cables, except they have eight connectors. For our purposes, there are two types of cables—crossover and straight-through. In most instances, the straight-through cables are used. It is necessary to use a crossover cable when two computers are connected directly without a hub (for example, if you want to connect your PC’s Ethernet directly to the Rabbit Semiconductor TCP/IP Development Board.) Some hubs have one input that can accept either a straight-through or crossover cable depending on the position of a switch. In this case make sure that the switch position and cable type agree.

TCP/IP Protocol Stack

TCP/IP is the protocol suite upon which all Internet communication is based. Different vendors have developed other networking protocols, but even most network operating systems with their own protocols, such as Netware, support TCP/IP. It has become the de facto standard. Protocols are sometimes referred to as protocol stacks or protocol suites. A protocol stack is an appropriate term because it indicates the layered approach used to design the networking software.

Each host or router in the internet must run a protocol stack. The details of the underlying physical connections are hidden by the software. The sending software at each layer communicates with the corresponding layer at the receiving side through information stored in headers. Each layer adds its header to the front of the message from the next higher layer. The header is removed by the corresponding layer on the receiving side.

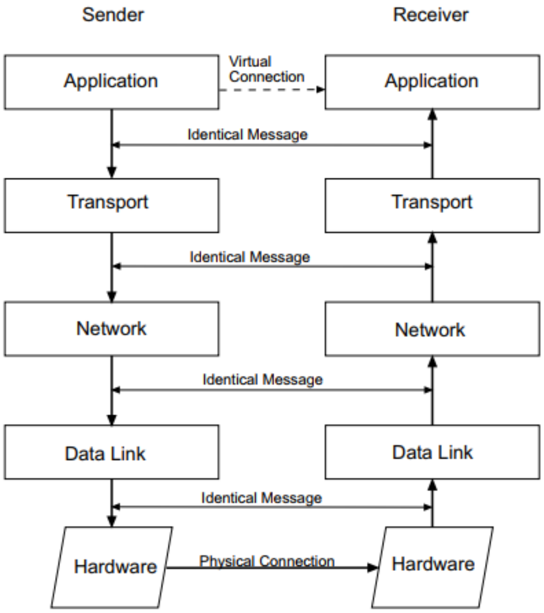


Figure : Flow of data between two computers using TCP/IP stacks.

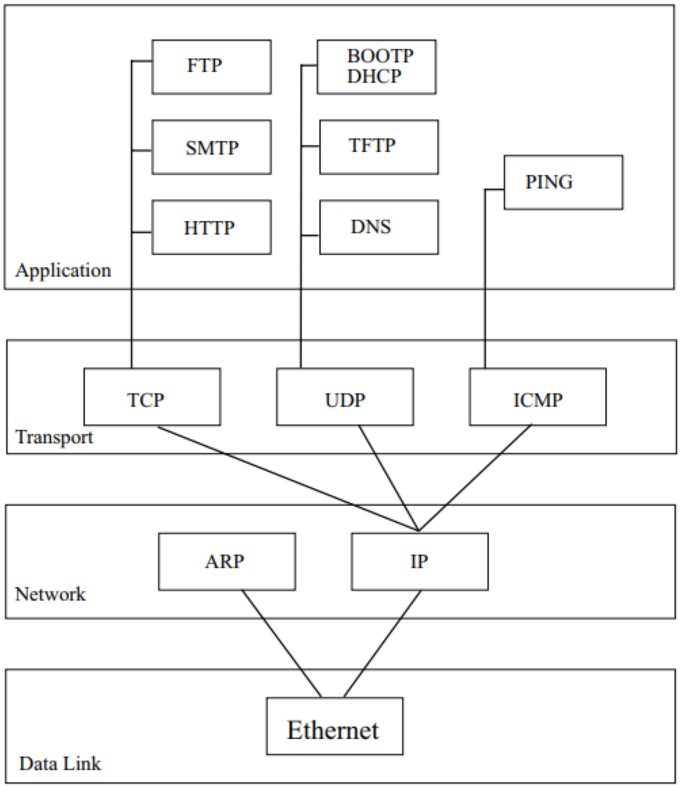


Figure : TCP/IP Protocol Flow

IP

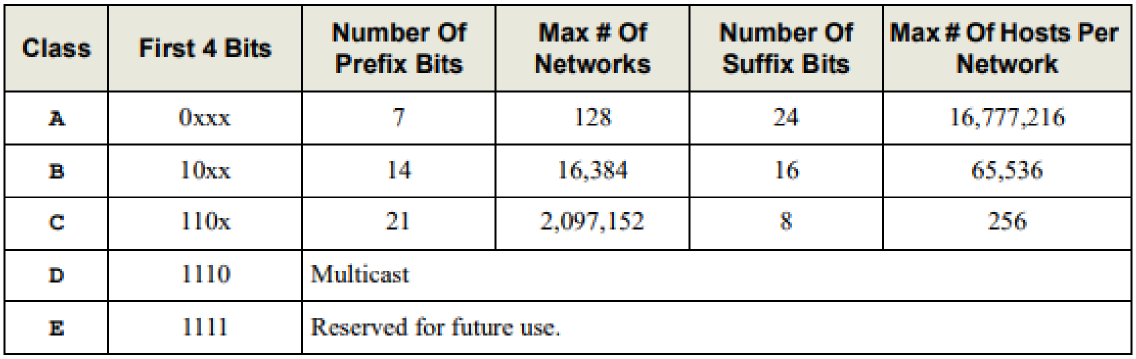
IP provides communication between hosts on different kinds of networks (i.e., different data-link implementations such as Ethenet and Token Ring). It is a connectionless, unreliable packet delivery service. Connectionless means that there is no handshaking, each packet is independent of any other packet. It is unreliable because there is no guarantee that a packet gets delivered; higherlevel protocols must deal with that.

IP Address

IP defines an addressing scheme that is independent of the underlying physical address (e.g, 48-bit MAC address). IP specifies a unique 32-bit number for each host on a network. This number is known as the Internet Protocol Address, the IP Address or the Internet Address. These terms are interchangeable. Each packet sent across the internet contains the IP address of the source of the packet and the IP address of its destination. For routing efficiency, the IP address is considered in two parts: the prefix which identifies the physical network, and the suffix which identifies a computer on the network. A unique prefix is needed for each network in an internet. For the global Internet, network numbers are obtained from Internet Service Providers (ISPs). ISPs coordinate with a central organization called the Internet Assigned Number Authority (IANA).

IP Address Classes

The first four bits of an IP address determine the class of the network. The class specifies how many of the remaining bits belong to the prefix (aka Network ID) and to the suffix (aka Host ID). The first three classes, A, B and C, are the primary network classes.



Class	First 4 Bits	Number Of Prefix Bits	Max # Of Networks	Number Of Suffix Bits	Max # Of Hosts Per Network
A	0xxx	7	128	24	16,777,216
B	10xx	14	16,384	16	65,536
C	110x	21	2,097,152	8	256
D	1110	Multicast			
E	1111	Reserved for future use.			

When interacting with mere humans, software uses dotted decimal notation; each 8 bits is treated as an unsigned binary integer separated by periods. IP reserves host address 0 to denote a network. 140.211.0.0 denotes the network that was assigned the class B prefix 140.211.

Netmasks

Netmasks are used to identify which part of the address is the Network ID and which part is the Host ID. This is done by a logical bitwise-AND of the IP address and the netmask. For class A networks the netmask is always 255.0.0.0; for class B networks it is 255.255.0.0 and for class C networks the netmask is 255.255.255.0.

Subnet Address

All hosts are required to support subnet addressing. While the IP address classes are the convention, IP addresses are typically subnetted to smaller address sets that do not match the class system. The suffix bits are divided into a subnet ID and a host ID. This makes sense for class A and B networks, since no one attaches as many hosts to these networks as is allowed. Whether to subnet and how many bits to use for the subnet ID is determined by the local network administrator of each network. If subnetting is used, then the netmask will have to reflect this fact. On a class B network with subnetting, the netmask would not be 255.255.0.0. The bits of the Host ID that were used for the subnet would need to be set in the netmask.

IP Routing

Each IP datagram travels from its source to its destination by means of routers. All hosts and routers on an internet contain IP protocol software and use a routing table to determine where to send a packet next. The destination IP address in the IP header contains the ultimate destination of the IP datagram, but it might go through several other IP addresses (routers) before reaching that destination.

Routing table entries are created when TCP/IP initializes. The entries can be updated manually by a network administrator or automatically by employing a routing protocol such as Routing Information Protocol (RIP). Routing table entries provide needed information to each local host regarding how to communicate with remote networks and hosts. When IP receives a packet from a higher-level protocol, like TCP or UDP, the routing table is searched for the route that is the closest match to the destination IP address.

ARP

The Address Resolution Protocol is used to translate virtual addresses to physical ones. The network hardware does not understand the software-maintained IP addresses. IP uses ARP to translate the 32-bit IP address to a physical address that matches the addressing scheme of the underlying hardware (for Ethernet, the 48-bit MAC address).

TCP/IP can use any of the three. ARP employs the third strategy, message exchange. ARP defines a request and a response. A request message is placed in a hardware frame (e.g., an Ethernet frame), and broadcast to all computers on the network. Only the computer whose IP address matches the request sends a response.

The Transport Layer

There are two primary transport layer protocols: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). They provide end-to-end communication services for applications.

TCP is a connection-oriented transport service; it provides end-to-end reliability, resequencing, and flow control. TCP enables two hosts to establish a connection and exchange streams of data, which are treated in bytes. The delivery of data in the proper order is guaranteed. TCP can detect errors or lost data and can trigger retransmission until the data is received, complete and without errors.

Sequence Number - This 32-bit number contains either the sequence number of the first byte of data in this particular segment or the Initial Sequence Number (ISN) that identifies the first byte of data that will be sent for this particular connection. The ISN is sent during the connection setup phase by setting the SYN control bit. An ISN is chosen by both client and server. The first byte of data sent by either side will be identified by the sequence number ISN + 1 because the SYN control bit consumes a sequence number. The following figure illustrates the three-way handshake.

Internet Control Message Protocol is a set of messages that communicate errors and other conditions that require attention. ICMP messages, delivered in IP datagrams, are usually acted on by either IP, TCP or UDP. Some ICMP messages are returned to application protocols. A common use of ICMP is “pinging” a host. The Ping command (Packet INternet Groper) is a utility that determines whether a specific IP address is accessible. It sends an ICMP echo request and waits for a reply. Ping can be used to transmit a series of packets to measure average roundtrip times and packet loss percentages.

The Application Layer

There are many applications available in the TCP/IP suite of protocols. Some of the most useful ones are for sending mail (SMTP), transferring files (FTP), and displaying web pages (HTTP). These applications are discussed in detail in the TCP/IP User's Manual. Another important application layer protocol is the Domain Name System (DNS). Domain names are significant because they guide users to where they want to go on the Internet.

The Domain Name System is a distributed database of domain name and IP address bindings. A domain name is simply an alphanumeric character string separated into segments by periods. It represents a specific and unique place in the "domain name space." DNS makes it possible for us to use identifiers such as zworld.com to refer to an IP address on the Internet. Name servers contain information on some segment of the DNS and make that information available to clients who are called resolvers.

References

1. A two-part article, Introduction to TCP/IP, in Embedded Systems Programming discusses issues related to programming embedded systems. http://www.embedded.com/internet/9912/9912ia1.htm

2. Ethereal is a good, free program for viewing network traffic. It works under various Unix operating systems and under Windows. http://www.ethereal.com

3. Computer Networks and Internets, Douglas E. Comer. Published by Prentice Hall. ISBN 0- 13-239070-1. This book gives an excellent high-level description of networks and their interfaces.

4. TCP/IP Illustrated, Volume 1 The Protocols, W. Richard Stevens. Published by AddisonWesley. ISBN 0-20-163346-9. This book gives many useful low-level details about TCP/IP, UDP and ICMP.