KEY ELEMENTS

OF

COMPUTER NETWORK

Authors:

Mr. Chetan N. Rathod [M.C.A., M.Phil.]

VIVEKANAND COLLEGE FOR ADVANCED COMPUTER & INFORMATION SCIENCE, SURAT

Mr. Sagar V.Fegade [M.C.A.]

M.L.PARMAR COLLEGE OF COMPUTER SCIENCE & I.T, SURAT

Ms. Bhumika K. Charnanand [M.C.A., M.Phil.]

PRABHU B.C.A. COLLEGE, UMRA, SURAT

Unit - 4

Basic of TCP/IP Model

4.1 Introduction to TCP/IP Model
4.2 Network Access Layer – MAC Address
4.3 Internet Layer – IP Address, IP Subnetting
4.4 Transport Layer - TCP, UDP, Port number
4.5 Application Layer

4.1 INTRODUCTION TO TCP/IP MODEL

As discussed earlier, you are familiar with computer networks, transmission media as well, as seven layers of OSI model. Network is nothing but group of two or more computer systems sharing services and interacting in some way. But for this interaction you need some physical pathway (transmission media). This transmission media connects the systems, and a set of rules determines how they communicate. These rules are known as protocol. A network protocol is software installed on machine that determines the agreed-upon set of rules for two or more machines to communicate with each other.

Common protocols in the Microsoft family include the following.

- NetBEUI
- NWLink
- DLC (Data Link Control)
- TCP/IP (Transmission Control Protocol / Internet Protocol)

In order to understand how to configure the functions of network devices, you must have a solid understanding of the protocols and their functions. The most common protocol used; in data networks today is the TCP / IP protocol stack. TCP/IP is used to interconnect devices in corporate networks as well as being the protocol of the Internet. The TCP/IP suite of protocols was developed as part. of the research done by the Defense Advance Research Projects Agency (DARPA). Later TCP/IP was included with the Berkeley Software Distribution (BSD) UNIX. TCP/IP is an industry standard suite of protocols designed to be routable, robust, and functionally efficient.

The Internet protocols can be used to communicate across any set of Interconnected networks. They are equally well suited for both LAN and WAN communication the Internet protocol suite includes not only Layers 3 and 4 specifications, but also specifications for such common applications as e-mail, remote login, terminal emulation, and file transfer. The TCP/IP protocol stacks maps closely to the OSI reference model in the lower layer. All standard Physical and data-link protocols are supported.

INSTALLING TCP/IP AS A PROTOCOL ON YOUR MACHINE OR NETWORK PROVIDES THE FOLLOWING ADVANTAGES :

1. AN INDUSTRY-STANDARD PROTOCOL

Because TCP/IP is not maintained or written by one company, it is not subject to as many compatibility issues. The Internet community as whole decides whether a particular change or implementation is worthwhile. This slows down the implementation of new features and characteristics compared to how quickly one directed company might make changes, but it does guarantee that changes are well thought out, that they provide functionality with most other implementations of TCP/IP.

2. AS SET OF UTILITIES FOR CONNECTING DISSIMILAR OPERATING SYSTEMS

Many connectivity utilities have been written for the TCP/IP suite, including the Pile Transfer Protocol (FTP) and Terminal Emulation Protocol (Telnet). Because these utilities use the windows Sockets API, connectivity from one machine to another is not dependent on the network operating system used on either machine.

3. A SCALABLE CROSS-PLATFORM CLIENT-SERVER ARCHITECTURE

4. ACCESS TO THE INTERNET

TCP/IP is the de facto protocol of the Internet and allows access to a wealth of information that can be found at thousands of locations around the world. To connect to the Internet, a valid IP address is required. Because IP address have become more and more scare, and as security issues surrounding access to the Internet have been raised, many creative alternatives have been established to allow connections to the internet.

Now you understand the benefits of installing TCP/IP, you are ready to team about how the TCP/IP protocol suite maps to a four -layer model.

OSI	TCP/IP
Application	Application
Presentation	
Session	Application
Transport	Transport
Networking	internet
Data Link	Network interface

PHYSICAL

TCP/IP maps to four layer architectural model. This model is called the Internet protocol suite and is broken into the network interface, Internet, Transport, and Application layers. Each of these layers corresponds to one or more layers of the OSI model. The Network Interface layer corresponds^\o the Physical and Date Link layers. The Internet layer corresponds to Network layer. The transport layer corresponds to the transport and application layer corresponds to the Session, Presentation, and Application layer.

PURPOSE OF LAYERS (TCP/IP MODEL)

The Network Interface layer is responsible for communicating directly with the network. The Internet layer is primarily concerned with the routing and delivery of packets through the Internet protocol (IP). All protocols in transport layer must use IP to send data.

The transport layer maps to the Transport Layer of OSI model and is responsible for providing communication between machines for applications.

The Application layer of the Internet Protocol Suite is responsible for all the activities that occur in the session, presentation an application layer of the OSI model. Numerous protocols have been written for use in this layer, including HTTP, Simple Network Management Protocol SNMP File Transfer Protocol (FTP) etc.

4.2 Network Access Layer – MAC Address

In a TCP/IP environment, end stations communicate seamlessly with servers or other end stations. This communication occurs because each node using the TCP/IP protocol suite has a unique 32-bit logical IP address. These addresses are called as Network classes. Each IP diagram includes a source IP address and destination IP address that identify the source and desolation network and host.

There are currently A, B, C, D and E classes of addresses. The unique address given to a machine is derived from the class A, B, or C addresses. Class D addresses are used for combining machines into one functional group, and class E addresses are considered experimental and are not currently available. For now, the most important concept to understand is that each machine requires a unique address and that IP is responsible for maintaining, utilizing, and manipulating it to provide communication between two machines. The whole concept behind uniquely identifying machines, is to be able to send data to one machine and one machine only, even in the event that the IP stack has to broadcast at the physical layer.

TERM	DEFINITION
Default Mask Class A	The mask used for class A network when no subnetting The value is 255.0.0.0
Default Class B Mask	Mask The mask used for class B network when no subnetting is used. The value is 255.255.0.0
Default Class C Mask	The mask used for class A network when no subnetting is used. The value is 255.255.255.0

When IP was first developed, there were no classes of addresses, because it was assumed that 254 networks would be more than enough for an Internet of academic and research computers. As the number of networks grew, the IP addresses were broken into classes as illustrated in the figure given below

8 Bits	8 Bits	8 Bits	8 Bits	8 Bits
Class B:	Network	Host	Host	Host
Class C:	Network	Network	Host	Host
Class D:	Network	Network	Network	Host
Class E:	Multicast Research			

Class A address has only 8 network bits (1 byte) and 24 bits (3 bytes) in the host field. Therefore, few Class A networks, each consisting of many hosts, exist. There are more Class B and Class C networks, each with fewer hosts. This scheme allows addresses to be assigned based on the size of network. This address design was based on assumption that there would be many more small networks than large networks in the world. Characteristics of Class A, B and C addresses

CLASS A ADDRESS	CLASS B ADDRESS	CLASS C ADDRESS
The first bit is 0.	The first two bits are 10	The first three bits are 110.
Range of network numbers: 1.0.0.0 to 126.0.0.0	Range of network numbers: 128.0.0.0 to 191 .255.0.0	Range of network numbers: 92.0.0.0 to 223 .255.255.0
Number of possible networks: 127 (through 126 are usable127 is reserved)	Number of possible networks 116,384	Number of possible networks 2,097,152
Number of possible values host portion: 16777,216 (the number of usable hosts is two less than the total number possible because the host portion must be nonzero and cannot be all 1s.)	The number of possible values in the Host portion: 65,536 (the number of usable hosts is two less than the total number possible because the host portion must be nonzero and cannot be all 1s.)	The number of possible in the values in the host portion: 256 (the number of usable hosts is two less than the total number possible because the host portion must be nonzero and cannot be all 1 s.)

Class D and Class E addressee are also defines. Class D addresses include the range of networks numbers: 224.0.0.0 to 239.255.255.255.Class E addresses start at 240.0.0.0 and are used for experimental purposes.

When installing the TCP/IP protocol, you have, the choice of installing and using several different services that work in conjunction with it. You may want or need to install the following services.

- **Internet Information Server (IIS)**

The Internet Information Server provides you the ability to share information to any type of computer that can use the TCP/IP protocol. IIS 3 includes FTP and WWW servers

- **Dynamic Host Configuration Protocol (DHCP)**

Provides automatic configuration remote hosts, making management of a TCP/IP environment easy.

- **Windows Internet Name Service**

Without the ability to find another computer on the network, you would never be able to communicate .The WINS server provides a centralized method of name management that is both flexible and dynamic in Microsoft only network.

- **Domain Name Server**

When the WINS server provides the capability to find the NETBIOS names, the DNS server will work with host names to enable you to integrate your systems into the Internet or to resolve hosts on the Internet.

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

The configuration of Microsoft TCP/IP involves knowing the correct values for several fields for each TCP/IP host and entering them manually. At the minimum, the host IP address and the subnet mask need to be configured. In most cases, other parameter such as WINS and DHCP server addresses also need to be configured on each host. DHCP relives the need for manual configuration and provides a method of configuring and reconfiguring all the TCP/IP related parameters. It is critical that the correct TCP/IP address is configured on each host.

The use of Microsoft's DHCP server greatly reduces the administrative overhead of managing TCP/IP client computers by eliminating the needs to manually configure clients. The DHCP server also allows for greater flexibility and mobility of clients on a TGP/IP network without administrator intervention. If used correctly DHCP can eliminate nearly all the problems associated with TCP/IP. The administrator enters the valid IP addresses or ranges of IP addresses (called a scope) in the DHCP server database, which then assigns the IP addresses to the DHCP client hosts.

DOMAIN NAME SYSTEM

The Domain Name System is one way to resolve hostnames in IP addresses in a TCP/IP environment. In non-Microsoft environment, hostnames are typically resolved through HOST files or DNS. In a Microsoft environment, WINS and broadcasts are also used to resolve hostnames on the Internet.

In it's early days, the Internet was a small network established by the Department of Defence for research purposes. This network linked computers at several government agencies with a few universities. The host names of the computers in this network were registered in a single HOSTS file located on a centrally administered server. Each site that heeded to resolve hostnames downloaded ^his file. Few computers were being added to this network, so the HOSTS file was not updated too often and the different sites only had to download this file periodically to update their own copies. As the number of hosts on the Internet grew, it becomes more and more difficult to manage all the names through a central HOSTS file.

DNS was introduced in 1984 as a way to resolve hostnames without relying on due central HOSTS file. With DNS, the hostnames reside in a database that can be distributed among multiple servers, decreasing the load on any one server and also allowing more than one point of administration for this naming system. DNS allows more types of registration than the simple hostname-to-TCP/IP address mapping used in HOSTS files and allows room for future-defined types. Because the database is distributed, it can support a much larger database that can store in single HOSTS file.

Structure of DNS

Some hostname systems, like NetBIOS names, use a flat database. With a flat database, all names exist at the same level, so there cannot be any duplicate names. These names are like Social Security numbers: every participant in the Social Security program must have a unique number, so it must be an identification system to distinguish all the individuals in the security. DNS names are located in hierarchical paths, like a directory structure. In a network using DNS, you can have more than one server with the same name, as long as each is located in a different path.

DNS Domains

The Internet Network Information Center Controls the top-level domains. These have names such as "com", "edu", ‘Gov’, "org" etc.

NAME	TYPE OF ORGANIZATION
COM	Commercial organizations
Edu	Educational institutions
Org	Non-profit organizations
Net	Networks
Gov	Non-military government organizations
Num	Phone numbers

The DNS database is stored in a file called zones. It is possible, even desirable, to break the DNS database into a number of zones. Breaking the DNS database into zones was part of the original

4.3 INTERNET LAYER – IP ADDRESS, IP SUBNETTING

IP ADDRESS

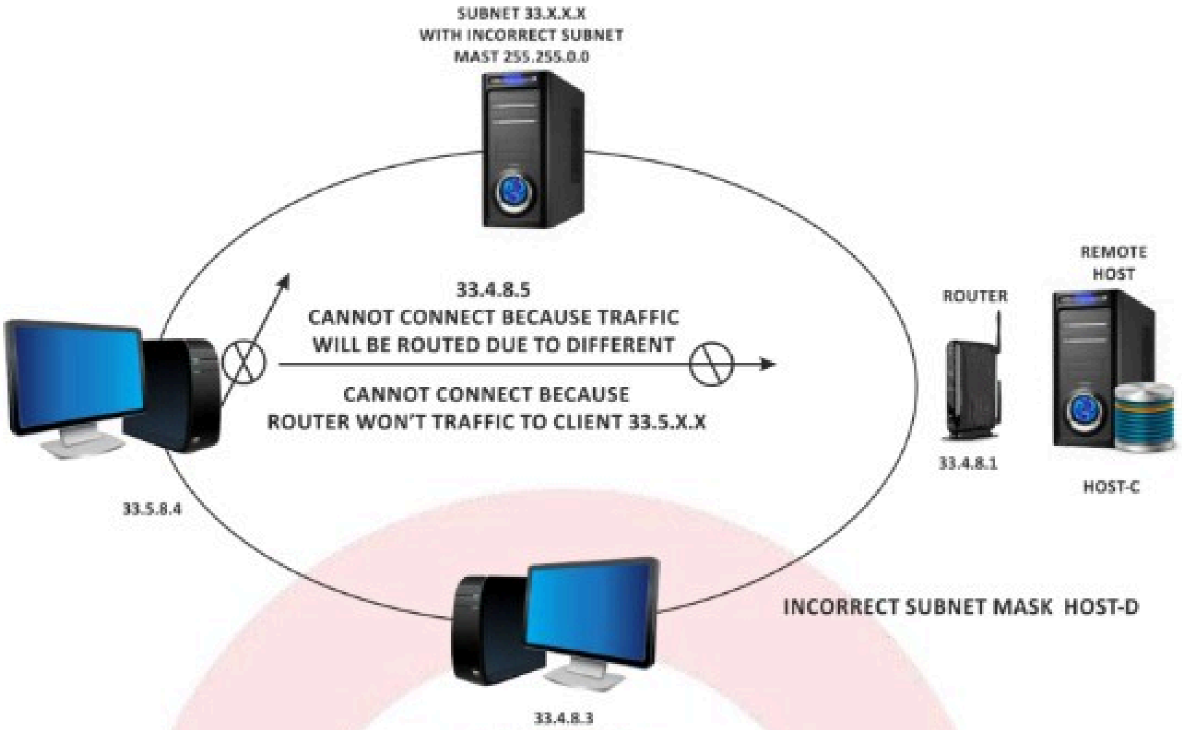
A TCP/IP address has two or possibly three components that uniquely identify the computer the address assigned to. At the very least, the IP address specifies the network address and host address of the computer. Also, if you are subnetting (using part of the host address to specify a subnet address), the third part of the address specifies the subnet address of the host.

If the incorrect host (143.168.3.9) sends a message to a local client (133.168.3.20 the TCP/IP configuration of the pending host indicates this is a remote address because it doesn't IP match the network address of the -host initiating the communication. The packet will not reach the local client, because the address 133.168.3.20 is interrupted as remote address.

If a local client the incorrect host (143.168.3.9), the message never reaches its intended destination. The message is either routed (if the local client sends the it to what should have been the address, 133.168.3.9). If the message is routed, the routed, the client for whom it was intended cannot receive the message because it is on the same segment of the network as the local client. If the message is not routed, the message still does not reach the incorrect client because the IP address for the destination host (133.168.3.9) does not match the address as configured on the incorrect client (143.168.3.9).

Following figure gives an example of an incorrect IP address. In this case a class A address is used, 33.x.x.x. The subnet mask (255.255.0.0) indicates the second octet is also being used to create subnets. In this cases even though the client has the same network address as the other clients, on the same subnet, the client has a different number because the address was typed incorrectly. This time the incorrect address specifies the Wrong subnet ID. The client 33,5.8.4 is on subnet 5, but the other clients on this subnet have the address 33.4.x.x. In this case, if the client 33.5.3.4 tries to contact other clients on the same subnet, the message is pouted because the subnet ID does not match the subnet number of the source host. If the client 33.5.8.4 tries to send a message to a remote host the message grouted but the message is not returned to the client because the router doesn't handle subnet 5, only subnet 4.

If a local client tries to send a message to 33.5.8.4, the message does not reach the client. If the local client uses the address as configured, the message is routed, which is not the correct solution because the destination host is local. If the local client sends the message to what should have been the IP address, 33.5.8.4 does not receive the message because the IP address is not configured correctly. The last component of an IP address that can cause communication problems in the host address.

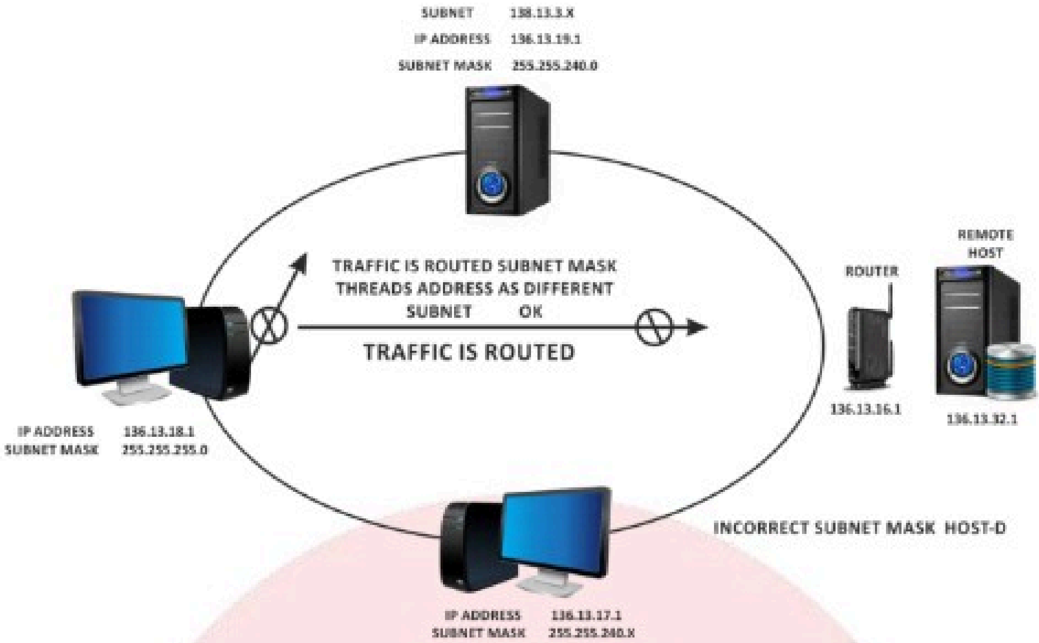

SUBNET 33.X.X.X
WITH INCORRECT SUBNET
MAST 255.255.0.0
REMOTE
HOST
ROUTER
33.4.8.5
CANNOT CONNECT BECAUSE TRAFFIC
WILL BE ROUTED DUE TO DIFFERENT
CANNOT CONNECT BECAUSE
ROUTER WON'T TRAFFIC TO CLIENT 33.5.X.X
33.4.8.1
HOST-C
33.5.8.4
INCORRECT SUBNET MASK HOST-D
33.4.8.3

4.1 INCORRECT SUBNET MASK

IP SUBNETTING

The subnet mask specifies which portion of the IP address specifies the network address and which portion of the address specifies the host address. Also, the subnet mask can be used to take part of what would have been the host address and use it to further divide the network into subnet. If the subnet mask is not configured correctly, yours client may not be able to communication at all, or you may see partial communication problems.

The following figure shows a subnet on a TCI/IP network. It uses a Class B network address of 130.13.x.x. The third octet is used in this case for subnetting, however, so all the clients in the figure should be on subnet 4, as indicated by the common address 138.13,3.x. Unfortunately, the subnet mask entered for one client is 255.255.0.0. When this client tries to communicate with other hosts on the same subnet, it should be able to contact them because the subnet mask indicates they are on the same subnet, which is correct. If the client tries to contact a host on another subnet such as 138.13.3.x, however the client fails.

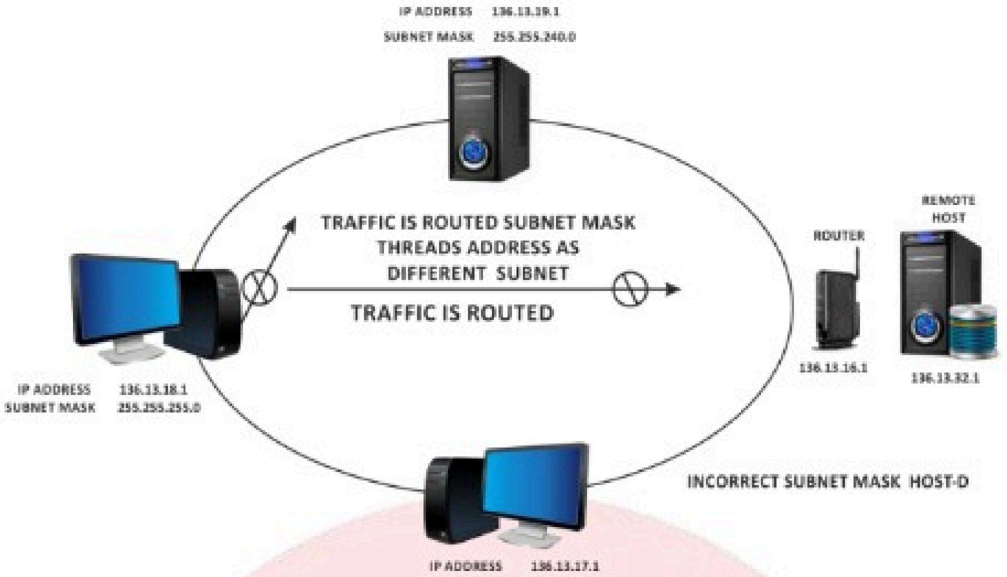

SUBNET 138.13.3.X
IP ADDRESS 136.13.19.1
SUBNET MASK 255.255.240.0
TRAFFIC IS ROUTED SUBNET MASK
THREADS ADDRESS AS DIFFERENT
SUBNET OK
TRAFFIC IS ROUTED
REMOTE HOST
ROUTER
136.13.16.1
136.13.32.1
IP ADDRESS 136.13.18.1
SUBNET MASK 255.255.255.0
INCORRECT SUBNET MASK HOST-D
IP ADDRESS 136.13.17.1
SUBNET MASK 255.255.240.X

4.2 IP SUBNETTING

In this case, the subnet mask still interprets the destination host to be on the same subnet and the message is never routed. Because the destination host is on another subnet, the message never reaches the intended destination.

The subnet mask is used to determine whether the host is local or remote, so the client with the incorrect subnet mask can receive incoming messages. When the client tries to return communications, however, the message is not routed if the source host is on the same network but on a different subnet. So in actuality, the client really can establish communications with only one side of the conversation. Contact with hosts outside the local network still works because those contacts are routed.

The following figure shows a subnet mask that masks too many bits. In this case, the subnet mask, is 255:255.255.0. The network designers had Intended the subnet mask to be 255.255.240.0, however, with 4 bits of the third octet used for the subnet and 4 bits as part of the host address. If the incorrect client tries to send a message to a local host and third octet is the same, the message is not routed and therefore reaches the local client, if the local client has an address that differs in the last 4 bits<of the third octet, however, the message is routed and never reaches its destination. If the incorrect client tries to send a message to another client on another subnet, the message is routed because the third octet is different.


IP ADDRESS 136.13.19.1
SUBNET MASK 255.255.240.0
TRAFFIC IS ROUTED SUBNET MASK THREADS ADDRESS AS DIFFERENT SUBNET
TRAFFIC IS ROUTED
REMOTE HOST
ROUTER
136.13.16.1
136.13.32.1
IP ADDRESS 136.13.18.1
SUBNET MASK 255.255.255.0
INCORRECT SUBNET MASK HOST-D
IP ADDRESS 136.13.17.1

4.3 IP SUBNETTING

4.4 TRANSPORT LAYER - TCP, UDP, PORT NUMBER

TRANSPORT LAYER PROTOCOLS

The transport layer is represented by two protocols:

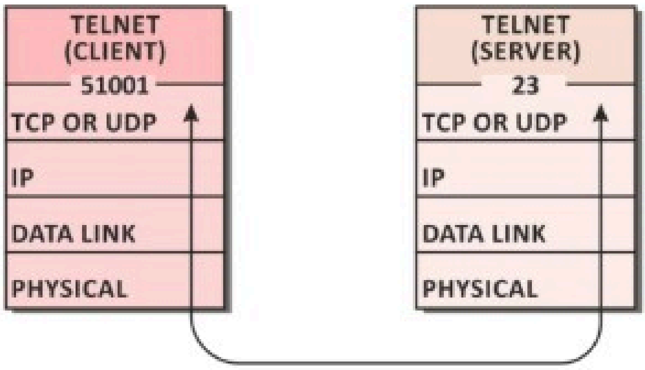
TCP and UDP

The IP protocol in the network layer delivers a datagram from a source host to the destination host.

Nowadays, the operating system supports multiuser and multiprocessing environments; an executing program is called a process. When a host sends a message to other host means that source process is sending a process to a destination process. The transport layer protocols define some connections to individual ports known as protocol ports.

An IP protocol is a host-to-host protocol used to deliver a packet from source host to the destination host while transport layer protocols are port-to-port protocols that work on the top of the IP protocols to deliver the packet from the originating port to the IP services, and from IP services to the destination port.

Each port is defined by a positive integer address, and it is of 16 bits.



4.4 TCP AND UDP

TCP

- TCP stands for Transmission Control Protocol.
- It provides full transport layer services to applications.
- It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

FEATURES OF TCP PROTOCOL

Stream data transfer: TCP protocol transfers the data in the form of contiguous stream of bytes. TCP group the bytes in the form of TCP segments and then passed it to the IP layer for transmission to the destination. TCP itself segments the data and forward to the IP.

RELIABILITY: TCP assigns a sequence number to each byte transmitted and expects a positive acknowledgement from the receiving TCP. If ACK is not received within a timeout interval, then the data is retransmitted to the destination.

The receiving TCP uses the sequence number to reassemble the segments if they arrive out of order or to eliminate the duplicate segments.

FLOW CONTROL: When receiving TCP sends an acknowledgement back to the sender indicating the number the bytes it can receive without overflowing its internal buffer. The number of bytes is sent in ACK in the form of the highest sequence number that it can receive without any problem. This mechanism is also referred to as a window mechanism.

MULTIPLEXING: Multiplexing is a process of accepting the data from different applications and forwarding to the different applications on different computers. At the receiving end, the data is forwarded to the correct application. This process is known as demultiplexing. TCP transmits the packet to the correct application by using the logical channels known as ports.

LOGICAL CONNECTIONS: The combination of sockets, sequence numbers, and window sizes, is called a logical connection. Each connection is identified by the pair of sockets used by sending and receiving processes.

FULL DUPLEX: TCP provides Full Duplex service, i.e., the data flow in both the directions at the same time. To achieve Full Duplex service, each TCP should have sending and receiving buffers so that the segments can flow in both the directions. TCP is a connection-oriented protocol. Suppose the process A wants to send and receive the data from process B. The following steps occur:

Establish a connection between two TCPs.

Data is exchanged in both the directions.

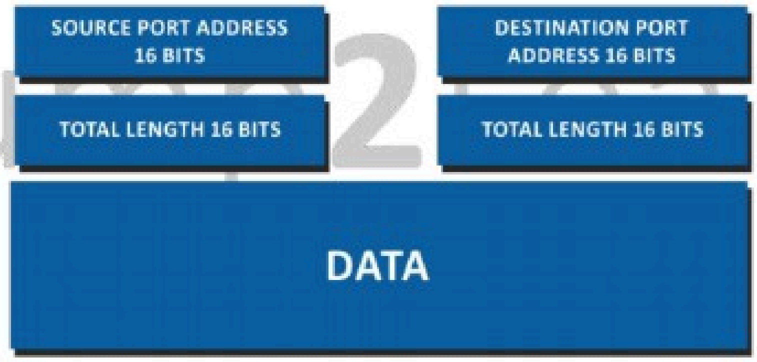
The Connection is terminated.

UDP

- UDP stands for User Datagram Protocol.
- UDP is a simple protocol and it provides no sequenced transport functionality.
- UDP is a connectionless protocol.
- This type of protocol is used when reliability and security are less important than speed and size.
- UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
- The packet produced by the UDP protocol is known as a user datagram.

USER DATAGRAM FORMAT

The user datagram has a 16-byte header which is shown below:



4.5 USER DATA FORMAT

Where,

SOURCE PORT ADDRESS: It defines the address of the application process that has delivered a message. The source port address is of 16 bits address.

DESTINATION PORT ADDRESS: It defines the address of the application process that will receive the message. The destination port address is of a 16-bit address.

TOTAL LENGTH: It defines the total length of the user datagram in bytes. It is a 16-bit field.

CHECKSUM: The checksum is a 16-bit field which is used in error detection.

DISADVANTAGES OF UDP PROTOCOL

- UDP provides basic functions needed for the end-to-end delivery of a transmission.
- It does not provide any sequencing or reordering functions and does not specify the damaged packet when reporting an error.
- UDP can discover that an error has occurred, but it does not specify which packet has been lost as it does not contain an ID or sequencing number of a particular data segment.

PORT NUMBER:

- At the data link layer we need a MAC address, at the network layer we need an IP address to choose on host among millions. A datagram in the network layer needs a destination IP address for delivery and source IP address for the destination's reply
- At the transport layer a transport layer address called a **port number** is required to choose among multiple processes running on the destination host
- The destination port number is required for delivery and the source port number is needed for the reply.
- In the internet model, the port numbers are 16 bit integers between 0 and 65,535.
- The Client program defines itself with a port number which is chosen randomly. This number is called as ephemeral port number.
- The server process should also define itself with a port number but this port number cannot be chosen randomly
- The internet uses universal port number for server and these numbers are called as well known port numbers.
- Every client process knows the well-known port numbers of the corresponding server process.

- For example, a day time client process can use an temporary port number 43000 for identifying itself, the day time server process must use the well-known port number 15.

4.5 APPLICATION LAYER

The application layer in the OSI model is the closest layer to the end user which means that the application layer and end user can interact directly with the software application. The application layer programs are based on client and servers.

THE APPLICATION LAYER INCLUDES THE FOLLOWING FUNCTIONS:

IDENTIFYING COMMUNICATION PARTNERS: The application layer identifies the availability of communication partners for an application with data to transmit.

DETERMINING RESOURCE AVAILABILITY: The application layer determines whether sufficient network resources are available for the requested communication.

SYNCHRONIZING COMMUNICATION: All the communications occur between the applications requires cooperation which is managed by an application layer.

SERVICES OF APPLICATION LAYERS

NETWORK VIRTUAL TERMINAL: An application layer allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal, which in turn, talks to the host. The remote host thinks that it is communicating with one of its own terminals, so it allows the user to log on.

FILE TRANSFER, ACCESS, AND MANAGEMENT (FTAM): An application allows a user to access files in a remote computer, to retrieve files from a computer and to manage files in a remote computer. FTAM defines a hierarchical virtual file in terms of file structure, file attributes and the kind of operations performed on the files and their attributes.

ADDRESSING: To obtain communication between client and server, there is a need for addressing. When a client made a request to the server, the request contains the server address and its own address. The server response to the client request, the request contains the destination address, i.e., client address. To achieve this kind of addressing, DNS is used.

MAIL SERVICES: An application layer provides Email forwarding and storage.

DIRECTORY SERVICES: An application contains a distributed database that provides access for global information about various objects and services.

AUTHENTICATION: It authenticates the sender or receiver's message or both.

NETWORK APPLICATION ARCHITECTURE

Application architecture is different from the network architecture. The network architecture is fixed and provides a set of services to applications. The application architecture, on the other hand, is designed by the application developer and defines how the application should be structured over the various end systems.

APPLICATION ARCHITECTURE IS OF TWO TYPES:

Client-server architecture: An application program running on the local machine sends a request to another application program is known as a client, and a program that serves a request is known as a server. For example, when a web server receives a request from the client host, it responds to the request to the client host.

CHARACTERISTICS OF CLIENT-SERVER ARCHITECTURE:

In Client-server architecture, clients do not directly communicate with each other. For example, in a web application, two browsers do not directly communicate with each other.

A server is fixed, well-known address known as IP address because the server is always on while the client can always contact the server by sending a packet to the sender's IP address.

DISADVANTAGE OF CLIENT-SERVER ARCHITECTURE: It is a single-server based architecture which is incapable of holding all the requests from the clients. For example, a social networking site can become overwhelmed when there is only one server exists.

P2P (PEER-TO-PEER) ARCHITECTURE: It has no dedicated server in a data center. The peers are the computers which are not owned by the service provider. Most of the peers reside in the homes, offices, schools, and universities. The peers communicate with each other without passing the information through a dedicated server, this architecture is known as peer-to-peer architecture. The applications based on P2P architecture includes file sharing and internet telephony.