UNIT 2 OSI AND TCP/IP MODELS

Structure **Page Nos**

2.0 INTRODUCTION

In order for a computer to send information to another computer, and for that computer to receive and understand the information, there has to exist a set of rules or standards for this communication process. These standards ensure that varying devices and products can communicate with each other over any network. This set of standards is called a network reference model. There are a variety of networked models currently being implemented. However, in this unit, the focus will be on the OSI and TCP/IP models.

2.1 OBJECTIVES

After going through this unit, you should be able to know:

- The seven layers of OSI reference model
- Understand each layer of OSI model
- Functions of each layer of OSI model
- Understanding of TCP/IP model and its four Layers
- Detail Description of protocol used in each layer
- Similarities of OSI and TCP/IP

2.2 OSI REFERNCE MODEL

In 1983, the International Standards Organization (ISO) developed a model called Open Systems Interconnection (OSI) which is a standard reference model for

communication between two end users in a network. The model is used in developing products and understanding networks. It is a prescription of characterizing and standardizing the functions of a communications system in terms of abstraction layers. Similar communication functions are grouped into logical layers. A layer serves the layer above it and is served by the layer below it.

2.2.1 Layers in the OSI Model

OSI divides Telecommunications into Seven Layers as shown below in the Figure 1 given below. Each layer is responsible for a particular aspect of data communication. For example, one layer may be responsible for establishing connections between devices, while another layer may be responsible for error checking during transfer.

The layers of the OSI model are divided into two groups: the upper layers and lower layers. The upper layers (Host layers) focus on user applications and how files are represented on the computers prior to transport. The lower layers (Media Layers) concentrate on how the communication across a network actually occurs. Each layer has a set of functions that are to be performed by a specific protocol(s). The OSI reference model has a protocol suit for all of its layers.

In computing, a protocol is a convention or standard that controls or enables the connection, communication, and data transfer between two computing endpoints. In its simplest form, a protocol can be defined as the rules governing the syntax, semantics, and synchronization of communication.

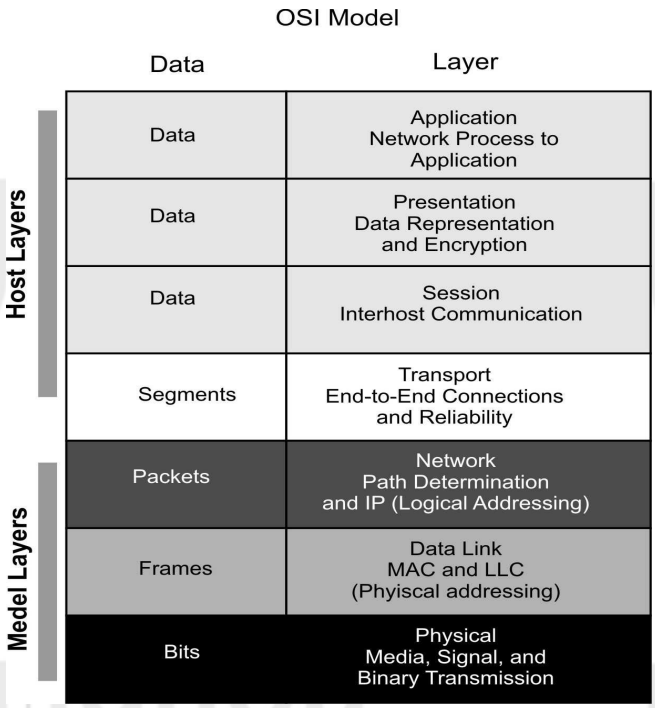

Figure 1: The OSI Model

2.2.2 Layer 1: The Physical Layer

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

- **Data encoding:** modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization.
- **Transmission technique:** determines whether the encoded bits will be transmitted by baseband (digital) or broadband (analog) signaling.
- **Physical medium transmission:** transmits bits as electrical or optical signals appropriate for the physical medium, and determines: What physical medium options can be used? And How many volts/db should be used to represent a given signal state, using a given physical medium?

2.2.3 Layer 2: The data-link layer

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:

- **Frame Traffic Control:** tells the transmitting node to "stop" when no frame buffers are available.
- **Frame Sequencing:** transmits/receives frames sequentially.
- **Frame Acknowledgment:** provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.
- **Frame Delimiting:** creates and recognizes frame boundaries.
- **Link Establishment and Termination:** establishes and terminates the logical link between two nodes.
- **Frame Error Checking:** checks received frames for integrity.
- **Media access management:** determines when the node "has the right" to use the physical medium.

Data Link Sub layers

The Data Link Layer is described in more detail with Media Access Control (MAC) and Logical Link Control (LLC) sub layers; where LLC is consider as upper data link layer and MAC as lower data link layer as shown below in the Figure 2.

- Logical Link Control (LLC): The LLC is concerned with managing traffic (flow and error control) over the physical medium and may also assign sequence numbers to frames and track acknowledgements. LLC is defined in the IEEE 802.2 specification and supports both connectionless and connection-oriented services used by higher-layer protocols.
- Media Access Control (MAC): The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it.

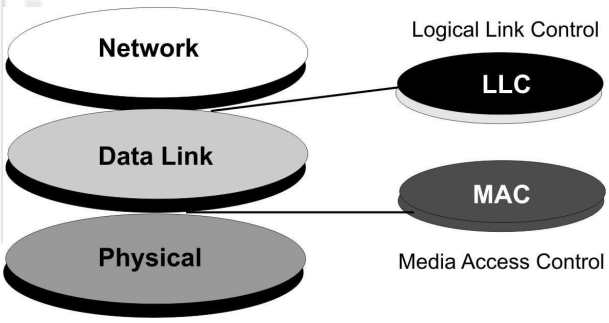

Figure 2: Data Link Sub-Layers

2.2.4 Layer 3: The Network Layer

The network layer provides the functional and procedural means of transferring variable length data sequences from a source host on one network to a destination host on a different network. The network layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors. Routers operate at this layer, sending data throughout the extended network and making the Internet possible.

Functions of the network layer include:

- Connection setup
- Addressing
- Routing
- Security
- Quality of Service
- Fragmentation

The Network Layer identifies computers on a network. Two types of packets are used at the Network layer; Data packets and Route update packets. Data packets are used to transport user data through the Internet work. Protocols used to support data traffic are called routed protocols. Route update packets are used to update neighboring routers about the network connected to all routers within the internet work. Protocols that send route updates are called routing protocols. This layer is concerned with two functions Routing and Fragmentation / Reassembly:

Routing: It is the process of selecting the best paths in a network along which to send data on physical traffic as shown in Figure 3.

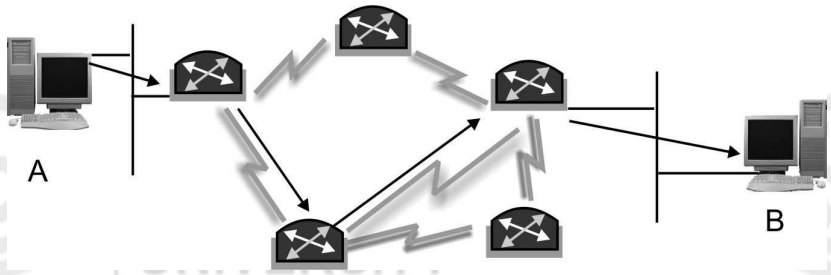

Figure 3: Routing at Network Layer

Fragmentation / Reassembly: if the network layer determines that a next router's maximum transmission unit (MTU) size is less than the current frame size, a router can fragment a frame for transmission and re-assembly at the destination station.

2.2.5 Layer 4: The Transport Layer

The transport layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The transport layer controls the reliability of a given link through flow control, segmentation/de-segmentation, and error control. This layer manages the end-to-end control (for example, determining whether all packets have arrived). It ensures complete data transfer. The Basic Transport Layer Services are:

- **Resource Utilization (multiplexing):** Multiple applications run on the same machine but use different ports.
- **Connection Management (establishing & terminating):** The second major task of Transport Layer is establishing connection between sender & the receiver before data transmission starts & terminating the connection once the data transmission is finished
- **Flow Control (Buffering / Windowing):** Once the connection has occurred and transfer is in progress, congestion of the data flow can occur at a destination for a variety of reasons. Possible options include:
    - The destination can become overwhelmed if multiple devices are trying to send it data at the same time.
    - The destination can become overwhelmed if the source is sending faster than it can physically receive.

The Transport Layer is responsible for providing flow control to alleviate the issue of congestion in the data transfer. Two main methods for flow control include:

Buffering: Buffering is a form of data flow control regulated by the Transport Layer as depicted in Figure 4. It is responsible for ensuring that sufficient buffers (Temporary Memory) are available at the destination for the processing of data and that the data is transmitted at a rate that does not exceed what the buffer can handle.

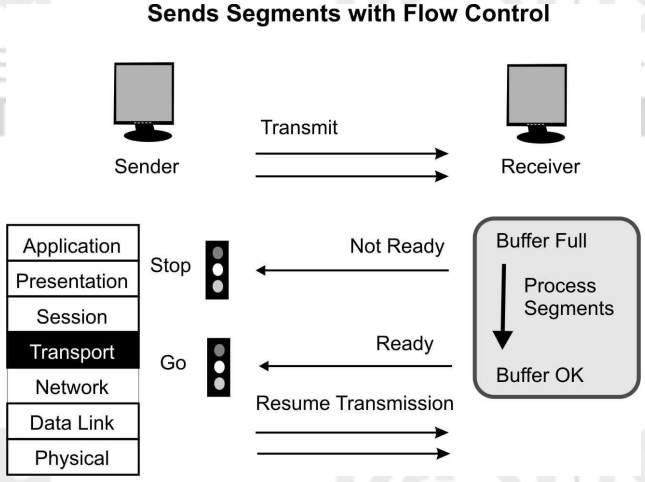

Figure 4: Buffering at Work

Windowing: Windowing is a flow control scheme in which the source computer will monitor and make adjustments to the amount of information sent based on successful, reliable receipt of data segments by the destination computer as shown in Figure 5. The size of the data transmission, called the "window size", is negotiated at the time of connection establishment, which is determined by the amount of memory or buffer that is available.

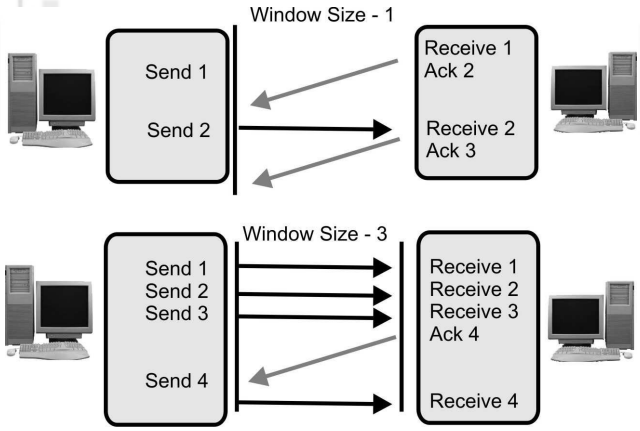

Figure 5: Flow Control & Reliability through Windowing

Reliable Transport (positive acknowledgment): Transport layer provides reliable transport of data by sending positive acknowledgements back to the sender once the data has reached the receiving side, if the data is lost or is corrupted, a negative acknowledgement is sent.

2.2.6 Layer 5: The Session Layer

The session Layer establishes, manages, and terminates sessions (different from connections) between applications as they interact on different hosts on a network. Its main job is to coordinate the service requests and responses between different hosts for applications.
The session established between hosts can be Simplex, half duplex and full duplex:

- **Simplex:** Simplex transmission is like a one-way street where traffic moves in only one direction. Simplex mode is a one-way-only transmission, which means that data can flow only in one direction from the sending device to the receiving device.
- **Half Duplex:** Half Duplex is like the center lane on some three-lane roads. It is a single lane in which traffic can move in one direction or the other, but not in both directions at the same time. Half-duplex mode limits data transmission because each device must take turns using the line. Therefore, data can flow from A to B and from B to A, but not at the same time.
- **Full Duplex:** is like a major highway with two lanes of traffic, each lane accommodating traffic going in opposite directions. Full-duplex mode accommodates two-way simultaneous transmission, which means that both sides can send and receive at the same time. In full-duplex mode, data can flow from A to B and B to A at the same time.

Note: Full-duplex transmission is, in fact, two simplex connections: One connection has traffic flowing in only one direction; the other connection has traffic flowing in the opposite direction of the first connection.

2.2.7 Layer 6: The Presentation Layer

The presentation layer transforms data into the form that the application accepts. This layer formats and encrypts data to be sent across a network. This layer, usually part of an operating system, that converts incoming and outgoing data from one presentation format to another (for example, from a text stream into a popup window with the newly arrived text). This layer is sometimes called the syntax layer. The Presentation Layer is responsible for the following services:

- **Data representation:** The presentation layer of the OSI model at the receiving computer is also responsible for the conversion of "the external format" with

which data is received from the sending computer to one accepted by the other layers in the host computer. Data formats include postscript, ASCII, or BINARY such as EBCDIC (fully Extended Binary Coded Decimal Interchange Code).

- **Data security:** Some types of encryption (and decryption) are performed at the presentation layer. This ensures the security of the data as it travels down the protocol stack.
- **Data compression:** Compression (and decompression) may be done at the presentation layer to improve the throughput of data.

2.2.8 Layer 7: The Application Layer

The application layer is closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a communicating component.

The Application Layer is the highest layer in the protocol stack and the layer responsible for introducing data into the OSI stack. The functions of Application Layer are:

- Resource sharing and device redirection
- Remote file access
- Remote printer access
- Network management
- Directory services
- Electronic messaging (such as mail) etc

2.3 TCP/IP MODEL

The TCP/IP Model is a specification for computer network protocols created in the 1970s by DARPA, an agency of the United States Department of Defense. It laid the foundation for ARPANET, which was the world's first wide area network and a predecessor of the Internet.

2.3.1 Layers in the TCP/IP Model

TCP/IP is generally described as having four 'layers' or five if we include the bottom physical layer. The layers near the top are logically closer to the user application, while those near the bottom are logically closer to the physical transmission of the data.

2.3.2 TCP/IP Application Layer

TCP/IP application layer protocols provide services to the application software running on a computer. The application Layer identifies the application running on the computer through Port Numbers.

The various protocols that are used at the Application Layer are:

- **Telnet**: Terminal Emulation, Telnet is a program that runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. Port Number :23

- **FTP**: File Transfer Protocol, the protocol used for exchanging files over the Internet. FTP is most commonly used to download a file from a server using the Internet or to upload a file to a server. Port Number : 20(data port) ,21(control port)
- **HTTP**: Hyper Text Transfer Protocol is the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when we enter a URL in the browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. Port Number :80
- **NFS**: Network File System, a client/server application that allows all network users to access shared files stored on computers of different types. Users can manipulate shared files as if they were stored locally on the user's own hard disk. Port Number :2049
- **SMTP**: Simple Mail Transfer Protocol, a protocol for sending e-mail messages between servers. In addition, SMTP is generally used to send messages from a mail client to a mail server. Port Number :25
- **POP3**: Post Office Protocol, a protocol used to retrieve e-mail from a mail server. Most e-mail applications (sometimes called an e-mail client) use the POP, although some can use the newer IMAP (Internet Message Access Protocol)as a replacement for POP3 Port Number :110
- **TFTP**: Trivial File Transfer Protocol, a simple form of the File Transfer Protocol (FTP). TFTP provides no security features. It is often used by servers to boot diskless workstations, X-terminals, and routers. Port Number :69
- **DNS**: Domain Name System (or Service or Server), an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. Port Number :53
- **DHCP**: Dynamic Host Configuration Protocol, a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. Port Number : 67(Server),68(Client)
- **BOOTP**: Bootstrap Protocol (BOOTP) is utilized by diskless workstations to gather configuration information from a network server. This enables the workstation to boot without requiring a hard or floppy disk drive. Port Number : 67(Server),68(Client)
- **SNMP**: Simple Network Management Protocol, a set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. Port Number :161

2.3.3 TCP/IP Transport Layer

The protocol layer just below the Application layer is the *host-to-host layer (Transport layer)*. It is responsible for end-to-end data integrity. Transport Layer identifies the segments through *Socket address* (Combination of Port Number & I.P. address).

The two most important protocols employed at this layer are the

- *Transmission Control Protocol (*TCP*):* TCP provides *reliable, full-duplex connections* and *reliable service* by ensuring that data is retransmitted when transmission results in an error (end-to-end error detection and correction). Also, TCP enables hosts to maintain multiple, simultaneous connections.
- *User Datagram Protocol (UDP):* When error correction is not required, UDP provides *unreliable datagram service* (connectionless) that enhances network throughput at the host-to-host transport layer. It's used primarily for *broadcasting* messages over a network.

2.3.4 TCP/IP Internet Layer

The best known TCP/IP protocol at the internetwork layer is the *Internet Protocol (*IP*),* which provides the basic packet delivery service for all TCP/IP networks node addresses, the IP implements a system of logical host addresses called IP addresses.

The IP addresses are used by the internetwork and higher layers to identify devices and to perform internetwork routing. IP is used by all protocols in the layers above and below it to deliver data, which means all TCP/IP data flows through IP when it is sent and received, regardless of its final destination.

The basic protocols used at the Internet Layer are:

- I.P. (Internet Protocol): It is a protocol used at the internet layer of TCP/IP model by which data is encapsulated and is sent from one computer to another on the Internet.
- ARP (Address Resolution Protocol): It is used to map the known I.P. addresses into Physical address.
- RARP(Reverse Address Resolution Protocol): It is used to map Physical address into I.P. address
- I.C.M.P.(Internet Control Message Protocol): It is used to send error & control Messages in the network
- I.G.M.P. (Internet Group Management Protocol): It is a protocol which is used to form multicast groups in a network to receive multicast messages.

2.3.5 TCP/IP Network Access Layer

The *network access layer* is the lowest layer in the TCP/IP model. This layer contains the protocols that the computer uses to deliver data to the other computers and devices that are attached to the network. The protocols at this layer perform three distinct functions:

- They define how to use the network to transmit a *frame*, which is the data unit passed across the physical connection.
- They exchange data between the computer and the physical network.
- They deliver data between two devices on the same network using the physical address.

The network access layer includes a large number of protocols. For instance, the network access layer includes all the variations of Ethernet protocols and other LAN standards. This layer also includes the popular WAN standards, such as the Point-to-Point Protocol (PPP) and Frame Relay.

2.4 COMPARISON OF OSI AND TCP/IP MODELS

As it can be seen from the previous pages, there are a number of comparisons, which can be drawn between the two models as shown below in the Figure 6. This section will therefore be focusing on highlighting the similarities and differences between the OSI and TCP/IP models.

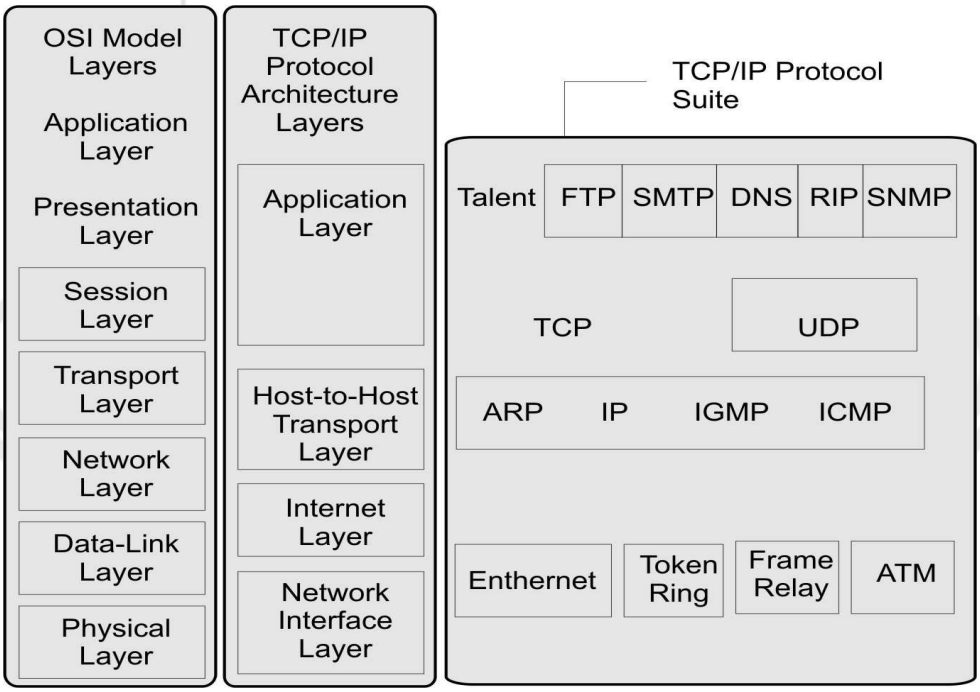

Figure 6: OSI Vs TCP/IP

Similarities

The main similarities between the OSI and TCP/IP models include the following:

- They share similar architecture. - Both of the models share a similar architecture. This can be illustrated by the fact that both of them are constructed with layers.
- They share a common application layer.- Both of the models share a common "application layer". However in practice this layer includes different services depending upon each model.
- Both models have comparable transport and network layers.- This can be illustrated by the fact that whatever functions are performed between the presentation and network layer of the OSI model similar functions are performed at the Transport layer of the TCP/IP model.
- Both models assume that packets are switched.- Basically this means that individual packets may take differing paths in order to reach the same destination.

Differences

The main differences between the two models are as follows:

- TCP/IP Protocols are considered to be standards around which the internet has developed. The OSI model however is a "generic, protocol- independent standard."
- TCP/IP combines the presentation and Chapter layer issues into its application layer.
- TCP/IP combines the OSI data link and physical layers into the network access layer.
- TCP/IP appears to be a simpler model and this is mainly due to the fact that it has fewer layers.
- TCP/IP is considered to be a more credible model- This is mainly due to the fact because TCP/IP protocols are the standards around which the internet was developed therefore it mainly gains creditability due to this reason. Where as in contrast networks are not usually built around the OSI model as it is merely used as a guidance tool.

☞ **Check Your Progress 1**

1. How transport layer of OSI model provide flow control to improve the issue of congestion in the data transfer?

   ……

   ……

   ……

   ……

2. Write the main similarities between the TCP/IP and OSI reference models.

   ……

   ……

   ……

2.5 TCP/IP PROTOCOLS

Transmission Control Protocol (TCP)/Internet Protocol (IP) is a set of protocols developed to allow computers of all sizes from different vendors, running different operating systems, to communicate or to share resources across a network. A packet switching network research project was started by the USA Government in the late 1960s in 1990s, became the most widely used form of computer networking. This project centered on ARPANET. ARPANET is best-known TCP/IP network. TCP/IP is the principal UNIX networking protocol and was designed to provide a reliable end-to-end byte stream over an unreliable internetwork. TCP is a connection-oriented protocol while IP is a connectionless protocol. TCP supplies logic to give a reliable connection-oriented protocol above IP. It provides a virtual-circuit that two processes can use to communicate. IP provides a connectionless and unreliable delivery system and transfer each datagram independently in the network. UDP is a connectionless and unreliable protocol running over IP. It adds a checksum to IP for the contents of the datagram and pass members. In this section, we are going to discuss all the protocols of TCP/IP in brief.

2.5.1 Application Layer Protocols

The Application layer provides applications the ability to access the services of the other layers and defines the protocols that applications use to exchange data. There are many Application layer protocols and new protocols are always being developed. The major functions of Application Layer are:

- Transfer of file that make up of Web pages
- Interactive file transfer(FTP)
- Transfer of mail messages and attachments
- Logging on remotely to networks hosts
- Resolving host name of an IP address
- Exchanging routing information on an IP internetwork.
- Collecting and exchanging network management information.

The Most common Application Layer Protocols are:

- Telnet (Network Terminal Protocol)
- FTP (File Transfer Protocol)
- SMTP(Simple Mail Transfer Protocol)
- DNS(Domain Name Server)
- RIP(Routing Information Protocol)
- SNMP(Simple Network Management Protocol)

Network Terminal Protocol

The purpose of the Telnet protocol is to provide a fairly general, bi-directional, eight-bit byte-oriented communications facility. Its primary goal is to allow a standard method of interfacing terminal devices and terminal-oriented processes to each other.

Telnet not only allows the user to log in to a remote host, it allows that user to execute commands on that host. Thus, an individual in Los Angeles can Telnet to a machine in New York and begin running programs on the New York machine just as though the user were actually in New York.

File Transfer Protocol

FTP (File Transfer Protocol) is the simplest and most secure way to exchange files over the Internet. Whether you know it or not, you most likely use FTP all the time. The most common use for FTP is to *download* files from the Internet. When *downloading* a file from the Internet you're actually *transferring* the file to your computer from another computer over the Internet. This is why the \T (transfer) is in FTP. You may not know where the computer is that the file is coming from but you most likely know its URL or Internet address.

An FTP address looks a lot like an HTTP, or Website, address except it uses the prefix *ftp://* instead of *http://*.

Example Website address:	http://www.ignou.ac.in
Example FTP site address:	ftp://www.ignou.ac.in

Simple Mail Transfer Protocol

SMTP is a relatively simple, text-based protocol, in which one or more recipients of a message are specified (and in most cases verified to exist) along with the message text and possibly other encoded objects. The message is then transferred to a remote server using a procedure of queries and responses between the client and server. Either an end-user's email client, a.k.a. MUA (Mail User Agent), or a relaying server's MTA (Mail Transport Agents) can act as an SMTP client.

An email client knows the outgoing mail SMTP server from its configuration. A relaying server typically determines which SMTP server to connect to by looking up the MX (Mail eXchange) DNS record for each recipient's domain name (the part of the email address to the right of the at (@) sign). Conformant MTAs (not all) fall back to a simple A record in the case of no MX. (Relaying servers can also be configured to use a smart host.)

The SMTP client initiates a TCP connection to server's port 25 (unless overridden by configuration). It is quite easy to test an SMTP server using the telnet program. SMTP is a "push" protocol that does not allow one to "pull" messages from a remote server on demand. To do this a mail client must use POP3 or IMAP. Another SMTP server can trigger a delivery in SMTP using ETRN.

HyperText Transfer Protocol

Hypertext Transfer Protocol (HTTP) is a communications protocol for the transfer of information on the intranet and the World Wide Web. Its original purpose was to provide a way to publish and retrieve hypertext pages over the Internet.

HTTP is a request/response standard between a client and a server. A client is the end-user; the server is the web site. The client making an HTTP request - using a web browser, spider, or other end-user tool - is referred to as the user agent. The responding server - which stores or creates resources such as HTML files and images - is called the origin server. In between the user agent and origin server may be several intermediaries, such as proxies, gateways, and tunnels. HTTP is not constrained to using TCP/IP and its supporting layers, although this is its most popular application on the Internet. Indeed HTTP can be "implemented on top of any other protocol on the Internet, or on other networks. HTTP only presumes a reliable transport; any protocol that provides such guarantees can be used."

Typically, an HTTP client initiates a request. It establishes a Transmission Control Protocol (TCP) connection to a particular port on a host (port 80 by default; see List of TCP and UDP port numbers). An HTTP server listening on that port waits for the client to send a request message. Upon receiving the request, the server sends back a status line, such as "HTTP/1.1 200 OK", and a message of its own, the body of which is perhaps the requested file, an error message, or some other information.

The reason that HTTP uses TCP and not UDP is because much data must be sent for a webpage, and TCP provides transmission control, presents the data in order, and provides error correction.

Domain Name Server

The most basic task of DNS is to translate hostnames to IP addresses. In very simple terms, it can be compared to a phone book. DNS also has other important uses.

Above all, DNS makes it possible to assign Internet names to organizations (or concerns they represent) independent of the physical routing hierarchy represented by the numerical IP address. Because of this, hyperlinks and Internet contact information

can remain the same, whatever the current IP routing arrangements may be, and can take a human-readable form (such as "example.com"), which is easier to remember than the IP address 208.77.188.166. People take advantage of this when they recite meaningful URLs and e-mail addresses without caring how the machine will actually locate them.

The Domain Name System distributes the responsibility for assigning domain names and mapping them to IP networks by allowing an authoritative name server for each domain to keep track of its own changes, avoiding the need for a central register to be continually consulted and updated.

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network. Using SNMP, you can monitor network performance, audit network usage, detect network faults or inappropriate access, and in some cases configure remote devices. SNMP is designed to be deployed on the largest possible number of network devices, to have minimal impact on the managed nodes, to have minimal transport requirements, and to continue working when most other network applications fail.

Network File System

NFS stands for Network File System, a file system developed by Sun Microsystems, Inc. It is a client/server system that allows users to access files across a network and treats them as if they resided in a local file directory. For example, if you were using a computer linked to a second computer via NFS, you could access files on the second computer as if they resided in a directory on the first computer. This is accomplished through the processes of exporting (the process by which an NFS server provides remote clients with access to its files) and mounting (the process by which file systems are made available to the operating system and the user).

The NFS protocol is designed to be independent of the computer, operating system, network architecture, and transport protocol. This means that systems using the NFS service may be manufactured by different vendors, use different operating systems, and be connected to networks with different architectures. These differences are transparent to the NFS application, and thus, the user.

2.5.2 Transport Layer Protocols

In the TCP/IP model, the transport layer is responsible for delivering data to the appropriate application process on the host computers. This involves multiplexing of data from different application processes, i.e. forming a *segment* by adding source and destination port numbers in the header of each transport layer data packet. Together with the source and destination IP address (from the internet layer), the port numbers constitutes a network socket, i.e. an identification address of the process-to-process communication.

The major functions of Transport Layer are:

- It sets up and maintains a Chapter connection between two devices.
- It can provide for the reliable or unreliable delivery of data across the connection.
- It can implement flow control through ready/not ready signals or Windowing to ensure that the sender do not overwhelm the receiver with too many segments.

- It multiplexes the connections, allowing multiple applications to simultaneously send and receive data through port or socket numbers

The Most common Transport Layer Protocols are:

- T.C.P (Transmission Control Protocol)
- U.D.P (User Datagram Protocol)

Transmission Control Protocol

TCP is a Reliable (guarantees that the data sent across the connection will be delivered exactly as sent, without missing or duplicate data), Connection oriented (An application requests a connection, and then uses it for data transfer) protocol on the transport layer that provides in-order delivery of data and also use buffering and windowing to implement flow control.

User Datagram Protocol

The UDP is an unreliable connectionless protocol of the transport layer. UDP is *unreliable*, means that UDP does not provide mechanisms for error detection and error correction between the source and the destination. Because of this, UDP utilized bandwidth more efficiently than TCP. *Connectionless*, means that a network node can communicate with another network node using UDP without first negotiating any kind of handshaking or creating a connection. Because of this, UDP is very efficient for protocols that send very small amounts of data at irregular intervals.

2.5.3 Internet Layer Protocols

The TCP/IP internet-layer functionality includes transmitting data to and from the TCP/IP network interface layer, routing data to the correct network and station on the destination network, and handling packet errors and fragmentation.

Internet Protocol

The Internet Protocol is the building block of the Internet. IP is a **connectionless protocol**, means it does not exchange control information (handshake) to provide end-to-end control of communications flow. It relies on other layers to provide this function if it is required. IP also relies on other layers to provide error detection and correction. Because of this IP is sometimes referred to as an **unreliable protocol** because it contains no error detection and recovery code. IP can be relied upon to accurately deliver your data to the connected network, but it doesn't check whether that data was correctly received.

Its functions include:

- Defining the datagram, which is the basic unit of transmission in the Internet
- Defining the Internet addressing scheme
- Moving data between the Network Access Layer and the Host-to-Host Transport Layer
- Routing datagrams to remote hosts
- Performing fragmentation and re-assembly of datagrams

Address Resolution Protocol (ARP)

The address resolution protocol is a protocol used by the Internet Protocol (IP), specifically IPv4 (IP version 4), to map IP network addresses to the hardware addresses used by a data link protocol as depicted in figure 7. It is used when IPv4 is used over Ethernet. ARP works on Ethernet networks as follows. Ethernet network

adapters are produced with a physical address embedded in the hardware called the Media Access Control (MAC) address.

Manufacturers take care to ensure these 6-byte (48-bit) addresses are unique, and Ethernet relies on these unique identifiers for message delivery. When any device wishes to send data to another target device over Ethernet, it must first determine the MAC address of that target given its IP address These IP-to-MAC address mappings are derived from an **ARP cache** maintained on each device.

If the given IP address does not appear in a device's cache, that device cannot direct messages to that target until it obtains a new mapping. To do this, the initiating device first sends an *ARP request broadcast message* on the local subnet. The host with the given IP address sends an *ARP reply* in response to the broadcast, allowing the initiating device to update its cache and proceed to deliver messages directly to the target.

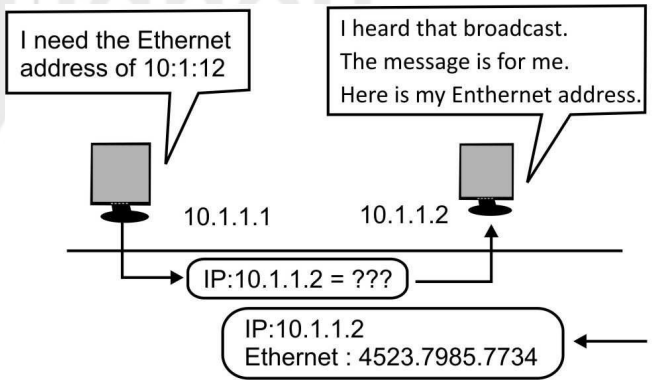

Figure 7: Working of ARP

Reverse Address Resolution Protocol (RARP)

Reverse Address Resolution Protocol, a TCP/IP protocol that permits a physical address, such as an Ethernet address, to be translated into an IP address. Hosts such as diskless workstations often only know their hardware interface addresses, or MAC address, when booted but not their IP addresses. They must discover their IP addresses from an external source, usually a RARP server.

To obtain the I.P. address, diskless workstations broadcast their MAC address in the whole network, when the RARP server receives the request it responds the workstation with a unique I.P. address.

Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (ICMP) is a protocol tightly integrated with IP. ICMP messages, delivered in IP packets, are used for sending *error & control messages* i.e. information about the status of the network itself. Since ICMP uses IP, ICMP packet delivery is unreliable, so hosts can't count on receiving ICMP packets for any network problem. Some of ICMP's functions are to:

- **Announce network errors,** such as a host or entire portion of the network being unreachable, due to some type of failure. A TCP or UDP packet directed at a port number with no receiver attached is also reported via ICMP.
- **Announce network congestion.** When a router begins buffering too many packets, due to an inability to transmit them as fast as they are being received, it will generate ICMP *Source Quench* messages. Directed at the sender, these messages should cause the rate of packet transmission to be slowed. Of course,

generating too many Source Quench messages would cause even more network congestion, so they are used sparingly.

- **Assist Troubleshooting.** ICMP supports an *Echo* function, which just sends a packet on a round--trip between two hosts. Ping, a common network management tool, is based on this feature. Ping will transmit a series of packets, measuring average round--trip times and computing loss percentages.

- **Announce Timeouts.** If an IP packet's TTL (Time To Live) field drops to zero, the router discarding the packet will often generate an ICMP packet announcing this fact. TraceRoute is a tool which maps network routes by sending packets with small TTL values and watching the ICMP timeout announcements.

☞ **Check Your Progress 2**

1. How does the HTTP protocol transfer the information on the World Wide Web?

   ……

   ……

   ……

   ……

2. Explain the working of Address Resolution Protocol (ARP).

   ……

   ……

   ……

   ……

2.6 SUMMARY

This unit began with an introduction to OSI reference model. It gave detailed information about various layers and functions of each layer of OSI reference model. The unit covers on understanding of how does the communication happen in a network. It also covered TCP/IP model. Comparison was made between OSI and TCP/IP models along with similarities and differences. Some of useful protocols of each layer of TCP/IP were described.

2.7 REFERENCES/FURTHER READINGS

1. *Computer Networks*, A. S. *Tanenbaum* 4th Edition, Practice Hall of India, New Delhi. 2003.
2. *Introduction to Data Communication & Networking,* 3rd Edition, Behrouz Forouzan, Tata McGraw Hill.
3. *Computer Networking*, J.F. Kurose & K.W. Ross, A Top Down Approach Featuring the Internet, Pearson Edition, 2003.
4. *Communications Networks*, Leon Garcia, and Widjaja, Tata McGraw Hill, 2000.
5. *www.wikipedia.org*
6. *Data and Computer Communications,* Willian Stallings, 6th Edition, Pearson Education, New Delhi.

7. Larry L. Peterson, *Computer Networks*: A Systems Approach, 3rd Edition (The Morgan Kaufmann Series in Networking).

2.8 SOLUTIONS/ANSWERS

☞ Check Your Progress 1

1. The Transport Layer is responsible for providing flow control to alleviate the issue of congestion in the data transfer. Two main methods for flow control include:

   Buffering: Buffering is a form of data flow control regulated by the Transport Layer as depicted in Figure 8. It is responsible for ensuring that sufficient buffers (Temporary Memory) are available at the destination for the processing of data and that the data is transmitted at a rate that does not exceed what the buffer can handle.

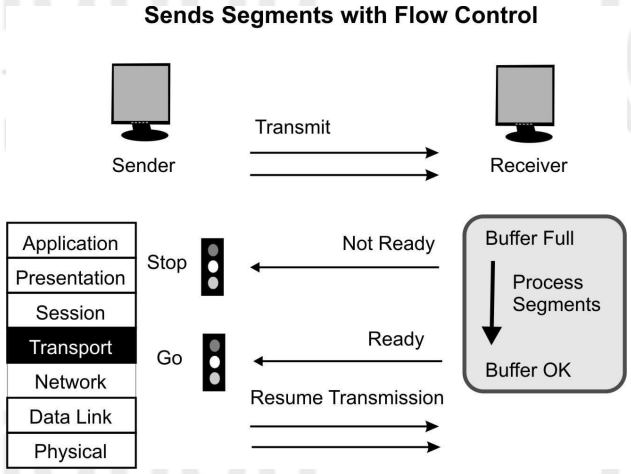

Figure 8: Buffering at Work

Windowing: Windowing is a flow control scheme in which the source computer will monitor and make adjustments to the amount of information sent based on successful, reliable receipt of data segments by the destination computer as shown in Figure 9. The size of the data transmission, called the "window size", is negotiated at the time of connection establishment, which is determined by the amount of memory or buffer that is available.

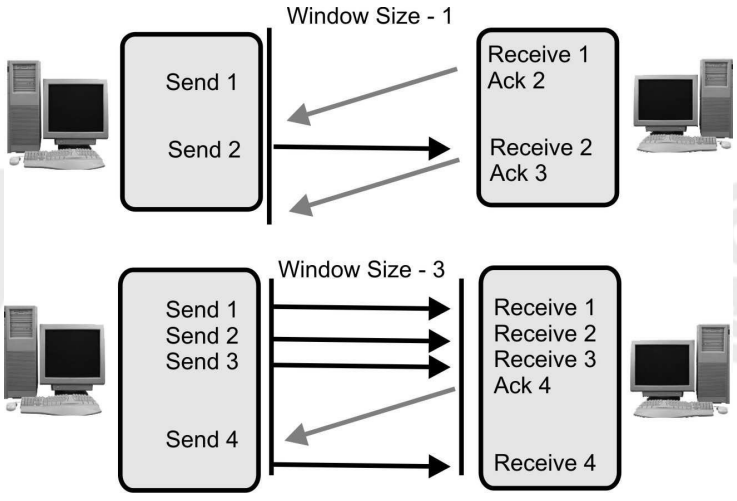

Figure 9: Flow Control & Reliability through Windowing

2. The main similarities between the OSI and TCP/IP models include the following:

- They share similar architecture. - Both of the models share a similar architecture. This can be illustrated by the fact that both of them are constructed with layers.
- They share a common application layer.- Both of the models share a common "application layer". However in practice this layer includes different services depending upon each model.
- Both models have comparable transport and network layers.- This can be illustrated by the fact that whatever functions are performed between the presentation and network layer of the OSI model similar functions are performed at the Transport layer of the TCP/IP model.
- Both models assume that packets are switched.- Basically this means that individual packets may take differing paths in order to reach the same destination.

☞ Check Your Progress 2

1. Hypertext Transfer Protocol (HTTP) is a communications protocol for the transfer of information on the intranet and the World Wide Web. Its original purpose was to provide a way to publish and retrieve hypertext pages over the Internet.

   HTTP is a request/response standard between a client and a server. A client is the end-user, the server is the web site. The client making an HTTP request - using a web browser, spider, or other end-user tool - is referred to as the user agent. The responding server - which stores or creates resources such as HTML files and images - is called the origin server. In between the user agent and origin server may be several intermediaries, such as proxies, gateways, and tunnels. HTTP is not constrained to using TCP/IP and its supporting layers, although this is its most popular application on the Internet. Indeed HTTP can be "implemented on top of any other protocol on the Internet, or on other networks. HTTP only presumes a reliable transport; any protocol that provides such guarantees can be used."

   Typically, an HTTP client initiates a request. It establishes a Transmission Control Protocol (TCP) connection to a particular port on a host (port 80 by default; see List of TCP and UDP port numbers). An HTTP server listening on that port waits for the client to send a request message. Upon receiving the request, the server sends back a status line, such as "HTTP/1.1 200 OK", and a message of its own, the body of which is perhaps the requested file, an error message, or some other information.

2. The address resolution protocol is a protocol used by the Internet Protocol (IP), specifically IPv4 (IP version 4), to map IP network addresses to the hardware addresses used by a data link protocol. It is used when IPv4 is used over Ethernet. ARP works on Ethernet networks as follows. Ethernet network adapters are produced with a physical address embedded in the hardware called the Media Access Control (MAC) address.

   Manufacturers take care to ensure these 6-byte (48-bit) addresses are unique, and Ethernet relies on these unique identifiers for message delivery. When any device wishes to send data to another target device over Ethernet, it must first determine the MAC address of that target given its IP address These IP-to-MAC address mappings are derived from an **ARP cache** maintained on each device.

If the given IP address does not appear in a device's cache, that device cannot direct messages to that target until it obtains a new mapping. To do this, the initiating device first sends an *ARP request broadcast message* on the local subnet. The host with the given IP address sends an *ARP reply* in response to the broadcast, allowing the initiating device to update its cache and proceed to deliver messages directly to the target.