PDHonline Course E175 (8 PDH)

Introduction to Computer Networking

Instructor: Dale W. Callahan, Ph.D., P.E. and Lea B. Callahan, P.E.

2020

PDH Online | PDH Center

5272 Meadow Estates Drive
Fairfax, VA 22030-6658
Phone: 703-988-0088
www.PDHonline.com

An Approved Continuing Education Provider

Introduction to Computer Networking

Dale Callahan, Ph.D., P.E.

MODULE 5: Protocols in Networking

5.1 Review

As explained in module 2, a protocol is a set of rules that enables communication between two computers or a group of computers. Data transfer or communication is in the form of lower level entities termed as bits, which is simply a series of 1's and 0's. A protocol allows a computer to make sense out of a series of incoming bits from another computer. A protocol is analogous to the exchange of welcome messages during a telephone conversation. Whenever a call is initiated, both sides exchange "HELLO" messages and then conversation begins. The call is terminated when both sides say "BYE".

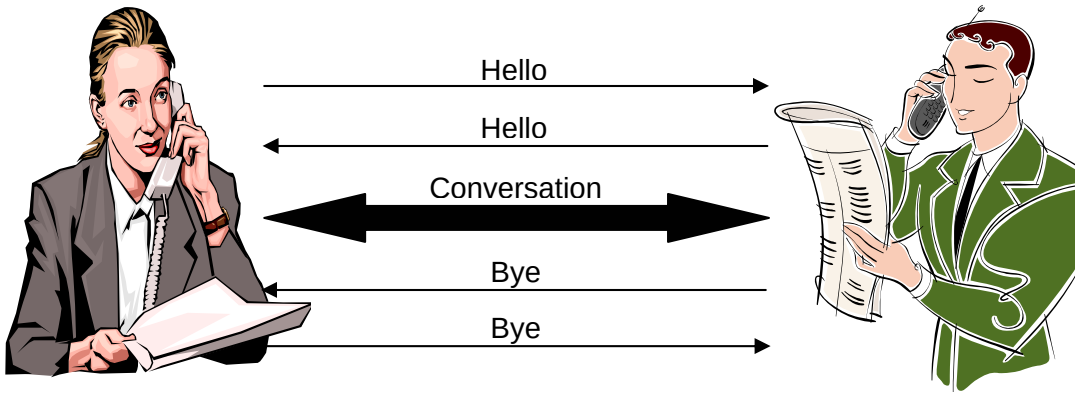


Figure 24. Analogy of phone conversation similar to a protocol

The transfer of data over a network is a complex process and hence is communicated in specific steps. Many protocols exist, which can result in interoperability problems, as two devices cannot communicate if they do not follow the same set of rules. The OSI model was developed in order to define and standardize the rules for communication and to encourage interoperability among devices from various vendors. The OSI model defines a protocol stack using the 7 layers such that each layer has its own set of rules for guiding data. These protocols are used in a top down (Layer 7 to Layer 1) manner during transmission and in bottom up (Layer 1 to Layer 7) manner during data reception. Most protocols are simply software – usually contained on the NIC or the memory of a computer.

This module will explain the Internet Protocol suite used for transferring multimedia over the Internet. These protocols help in reliable and continuous flow of data for real time services such as a telephone conversation.

5.2 Internet Protocols

The Internet Protocol suite is a set of protocols (ever growing set) that can be used for LAN and WAN communications. The Internet Protocol defines how communication must take place at lower layers such as the Layer 3 and Layer 4 using the well-known protocols such as TCP and IP. The suite also specifies communication at the application layer using Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP) etc.

Figure 25 shows the various protocols at different layers in the OSI model. Each of the acronyms mentioned in the figure will be explained in this module.

OSI Model	Internet Protocol Suite
Application Layer (7)	HTTP, FTP, SNMP, SMTP
Presentation Layer (6)	XDR
Sessions Layer (5)	RPC, SSH
Transport Layer (4)	TCP, UDP, RTP
Network Layer (3)	Routing Protocols, IP , ICMP, X.25, ARP
Data Link Layer (2)	Ethernet, Token Ring, PPP, Frame Relay, FDDI, ISDN, ATM, 802.11 Wi-Fi
Physical Layer (1)	Unspecified (Wire, Radio, Fiber optic)

Figure 25. Internet Protocol Suite at various layers in the OSI model

5.2.1 Physical Layer Protocols – Layer 1

The physical layer is responsible for the transmission of the bit stream over a physical medium. It is concerned with the characteristic of the interface between devices and the transmission medium. It also defines the type (wires, fiber optic links or radio links) of transmission medium. The physical layer contains data in the form of bits (1's and 0's) and specifies the type of encoding required of data transmission. The Internet Protocol does not specify any transmission medium and may vary based on the need or the configuration of the network.

5.2.2 Data link Layer Protocols – Layer 2

The data link layer ensures that the physical layer is reliable and supports end-to-end delivery. It is responsible for framing of the bits, physical addressing, flow control, and error control. The important protocols at this layer are Ethernet, Token Ring, Point-to-Point Protocol (PPP), Frame Relay, FDDI, Integrated Services Digital Network (ISDN), ATM, and Wireless Fidelity (WiFi or 802.11). Ethernet and Token Ring have been covered under Chapter 3 - LAN's.

a) Point to Point Protocol

Point-to-Point Protocol (PPP) is used to establish a direct connection between two nodes. The physical link is typically a telephone line, but data transfer is controlled and managed by the PPP. PPP is typical used for dial up or leased telephone lines. The protocol was developed to overcome the shortcomings of the Serial Line Internet Protocol (SLIP) that worked only in tandem with the Internet Protocol. PPP works with several network layer protocols such as IP, Internetwork Packet eXchange (IPX), and AppleTalk [6].

Figure 26. Point-to-point Physical Link [6]

A PPP connection between two nodes may have several states in which it may operate. The states are:

Idle State: Idle state indicates that the link is not in use. The end nodes are not trying to connect to each other.

Establishing State: The connection enters the establishing state, when one of the end nodes tries to connect to the other node. Both end devices agree upon certain conditions and move to the authenticating state. If certain parameters cannot be negotiated, the connection is terminated.

Authenticating State: Two nodes may enter in this state by exchanging certain security keys, which will authenticate the two nodes and establish the connection. If the authentication is unsuccessful, then the devices move to the terminating state. If authentication sharing is disabled, the two nodes may not enter this state and directly move to the Networking state.

Networking State: Both devices exchange data packets and control packets and stay in this stage until one of the end nodes tries to terminate the session.

Terminating State: The connection is terminated and the link is closed. The connection enters the Idle state.

b) Frame Relay

Frame Relay is a protocol that provides a low cost and high-speed backbone for transmitting information from a user device to a bridge or a router. It is used for internetworking of LANs and is a virtual circuit technology that uses virtual circuit identifiers to define the Data Terminal Equipment (DTE) connected to the network. Frame Relay provides both permanent and switched connections. In permanent connections, a dedicated point-to-point connection is established while switched connections are set up on a call-by-call basis. The devices that connect users to the network are called DTE while the network host is considered as the Data Communication Equipments (DCE) [6].

i) Permanent Virtual Circuit Connection

In a Permanent Virtual Circuit (PVC) connection, the two DTEs are connected permanently using a virtual connection and both the DTEs have a Data Link Connection Identifier (DLCI) assigned to them. These DLCIs are permanent and assigned by the network provider. Data transfer in PVC type connections between the two devices take place using these DLCI instead of physical addresses. In Figure 27, DTE 1 connects with DTE 4 using DLCI 26 while DTE 4 Communicates using DLCI 34 [6].

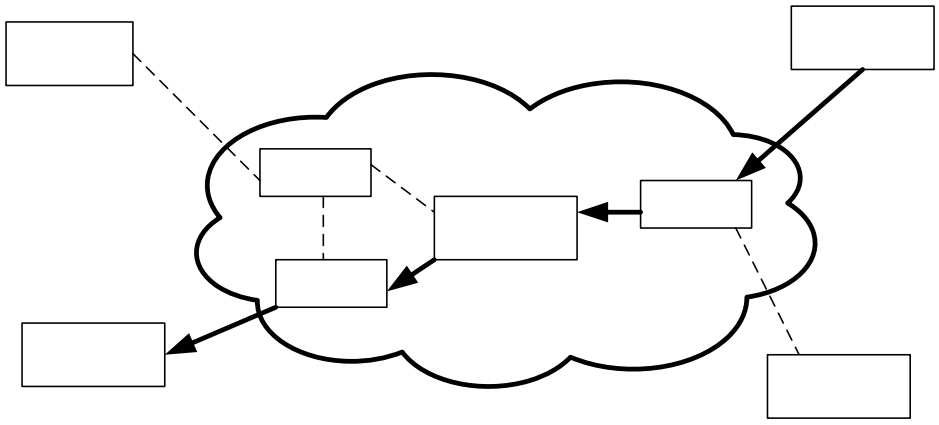


Figure 27. Permanent Virtual Connection in Frame Relay [6]

ii) Switched Virtual Circuit Connection

In Switched Virtual Connections, a virtual circuit connection has to be established each time a DTE needs to communicate with another DTE. Frame Relay operates at the physical and data link layers and hence requires the support of another protocol (e.g. IP) to make this connection using network layer addresses. The connection mechanism

depends on the networking protocol. In this case, DLCIs are assigned by the Frame Relay and are temporary to the connection [6].

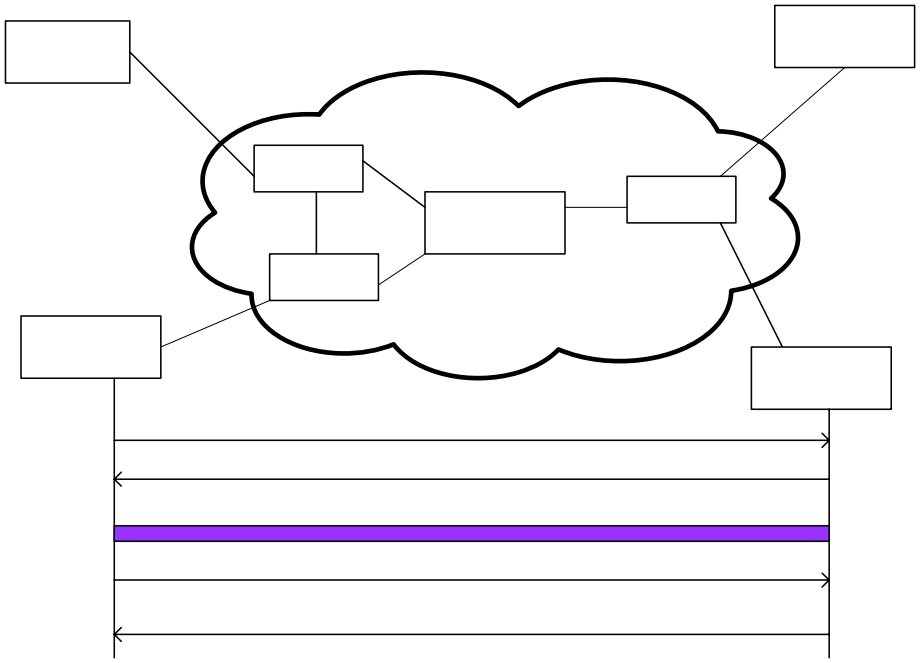


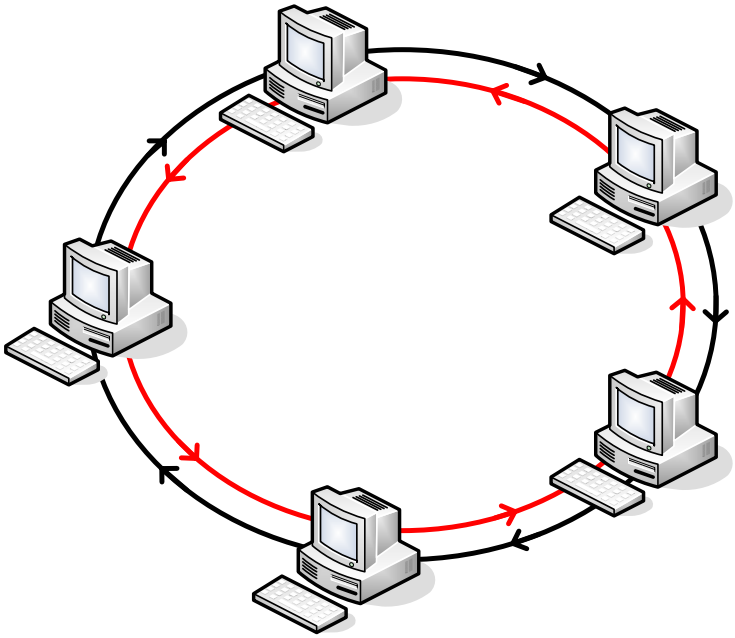
Figure 28. Switched Virtual Connection in Frame Relay [6]

DTE

c) Fiber Distributed Data Interface

FDDI is a high-speed 100-Mbps token ring type protocol using fiber optic as the transmission medium. It is typically used as a backbone for slower LANs or as a MAN. FDDI II is an enhanced version of FDDI that provides both packet-switched and circuit-switched data.

DTE



While FDDI is similar to Token Ring, FDDI uses two rings so that traffic on each ring flows in different directions. The outer ring is called the primary ring and is responsible for handling the flow of data between devices. The inner ring is a secondary ring and is used as a back up when the primary ring fails. If one of the transmitting stations fails, then the dual rings wrap themselves into a single ring topology without affecting the performance of the network. The two rings help to provide robustness and reliability to the network. FDDI allows distances up to 2 km (1.24 miles) between stations using multimode fiber. The distance increases if single mode fiber is used instead of multimode fiber.

In FDDI, a token travels around the ring and is captured by a station that needs to transmit data. A station can continue to send data frames until all the data is transmitted or until the Token Holding Timer (THT) expires. The transmitted frames are checked at each station for errors and destination address and then retransmitted to the next station. When the destination station recognizes its IP address on the frame, it retrieves the data on the frame and sets the error indicator and the address recognized indicator. The destination packet alters the frame and sends it back to the source destination, which recognizes its address in the source address field. This process of removing its own frame is termed as stripping [7].

If a station grabs a token and fails to transmit a frame, a Null Void frame that contains a destination MAC address of all zeros and source MAC address of its own is transmitted.

d) Integrated Services Digital Network

Integrated Services Digital Network (ISDN) is a circuit switched network system that enables digital transmission of voice and data over copper wires. ISDN specifies a set of protocols for establishing and terminating circuit switched connection, and for providing fully integrated

advanced digital user services. In order to achieve fully integrated digital service, the analog local loops between the end office and the customer needs to be replaced by digital subscriber loops [6].

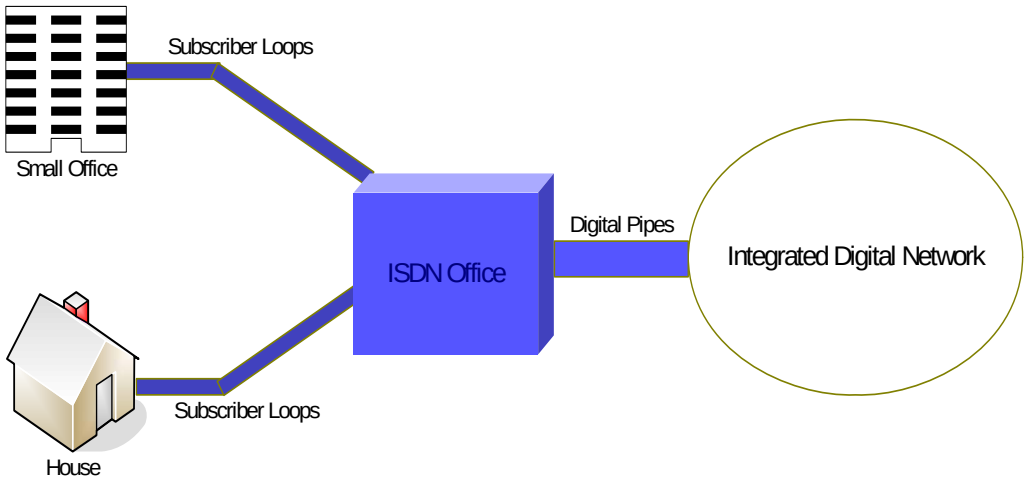


Figure 30. Integrated Services Digital Network [6]

The digital pipes that connect the customer to the ISDN office consist of various sizes in order to allow flexibility and to meet the specific requirements of the customers. ISDN consists of two types of channels and both channels support different data rates. They are B (data) channel and D (control and signaling) channel and are used in combination to provide ISDN services.

ISDN contains subscriber loops of two types:

i) Basic Rate Interface (BRI)

The BRI comprises of two B channels of 64 Kilobits per second (Kbps) each and one D channel of 16 Kbps. Thus the total size of the pipe is 2B + D = 144 Kbps. In addition, BRI also requires 48 Kbps of overhead. Hence, BRI requires a pipe of a total of 144 + 48 = 192 Kbps. The BRI is used to meet the demands of residential and small office customers.

ii) Primary Rate Interface (PRI)

In North America, PRI consists of 23 B channels of 64 Kbps each and one 64 Kbps D channel with 8 Kbps of overhead. PRI provide speeds of up to 1.544 Mbps. The number of B channels varies based on the country. Europe specifies 30 B and one 64 Kbps D channel as its PRI providing speeds of 2.048 Mbps.

Data is transmitted over the data channels (B channel) and signaling and control is achieved over the D channel. On call set up, a bidirectional 64 Kbps channel is assigned

for the voice or data transmission. This channel is released on call termination. The number of calls possible over the interface is equal the number of available data channels.

ISDN is not used much in the United States. The advent of DSL, Frame Relay, and ATM technologies has made ISDN mostly obsolete.

e) Asynchronous Transfer Mode

Asynchronous Transfer Mode (ATM) was developed to meet the higher bandwidth requirements of the applications. The older networks were unable to support a mixture of various types of network traffic. ATM was capable of handling different types of traffic such as voice, video and data, which provided more efficient and economical service.

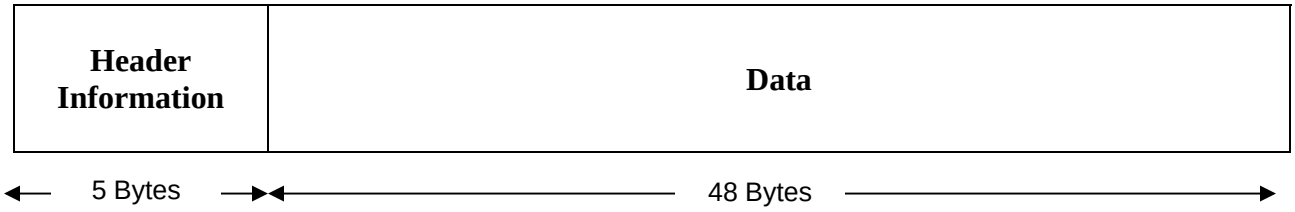


Figure 31. Packet Structure in ATM

ATM carries traffic in a stream of fixed-size packet of 53 bytes. An ATM packet comprises of 5 bytes of header information and 48 bytes of payload. The fixed size of an ATM packet improved the switching and multiplexing speeds considerably, which reduced congestion problems as the delay time was reduced. ATM is a connection oriented technology and requires both the sender and receiver to negotiate upon certain conditions before connection is established

ATM uses Virtual Channels (VC) to establish connection between two devices. It allows various connections to uses the same link on a demand basis and guarantees quality of service (QoS) by limiting the number of VCs. The header of an ATM packet is of two forms; one is used at the User Node Interface (UNI) and other from Network to Node Interface (NNI). The addressing field in ATM is divided into two subfields called Virtual Channel Identifier (VCI) and Virtual Path Identifier (VPI). The use of such an addressing scheme helps in assigning a VPI to sessions that share the same path so that they can be switched together [8].

f) 802.11 Wi-Fi

802.11 is a protocol developed by the IEEE for Wireless LAN technology. It specifies a wireless air-interface between a client and the base station. It can operate in two modes: Ad-Hoc mode and Infrastructure mode. In Ad-Hoc mode, the devices communicate with each other directly without the use of a central device - such a Hub or Access Point. In Infrastructure mode, the devices communicate through a central station called an Access Point.

802.11 currently has 3 variations of the technology in terms of the speed and radio frequency. They are the 802.11a, 802.11b and 802.11g.

802.11a: provides speeds up to 54Mbps in the five Gigahertz (GHz) band.
802.11b: provides speeds up to 11Mbps in the 2.4 GHz band.
802.11g: combination of the 802.11a and 802.11b standard and provides speeds between 11Mbps – 54 Mbps while operating in the 2.4 and 5 GHz band.

5.2.3 Network Layer Protocols – Layer 3

The network layer performs addressing by transporting each packet from the source node to the destination node. The network layer is responsible for delivery of packets between two networks as the data link layer is capable of routing data locally. The important protocols that provide such functionality are routing protocols, Internet Protocol, X.25, and Address Resolution Protocol.

a) Routing Protocols

A protocol that contains sufficient information about the source/destination address in order to allow packets to be exchanged between two hosts successfully is called a routing protocol. Routing protocols are classified as Interior Gateway Protocols and Exterior Gateway Protocols.

i) Interior Gateway Protocol

An Interior Gateway Protocol (IGP) is used to exchange routing information within a single autonomous network. The two commonly used IGPs are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

Routing Information Protocol (RIP)

RIP is a commonly used protocol that maintains router information within an autonomous network. If a network employs RIP as its IGP, then a gateway host is required to send its entire routing table to its nearest neighbor every 30 seconds. Similarly, the neighbors exchange their routing tables such that all the hosts have knowledge about the possible routes within the network. The exchange of routing information helps a router to determine the next step in routing a packet towards its destination.

RIP was designed for use in small networks and may put significant load on a large network since each router sends routing tables every 30 seconds [9].

Open Shortest Path First (OSPF)

OSPF is suited to larger autonomous networks. OSPF multicasts its routing table to its neighbors only when it detects a change in the network and only the changed portion in the routing table is sent to the neighbors. Thus, all the hosts maintain the same routing table within the network without constant updates that bog down the network.

OSPF uses the link state algorithm, which combines network information associated with the links such that links can be prioritized during data transmission. OSPF has built in

support for Variable Length Subnet Masking (VLSM), which allows the flexibility of dividing a network into smaller networks [9].

ii) Exterior Gateway Protocols

Exterior Gateway Protocols (EGP) are used to exchange routing information between hosts in two different autonomous systems. Border Gateway Protocol (BGP) is an example of an EGP.

Border Gateway Protocol (BGP)

BGP is used between the Internet Service Providers (ISPs). It is the main routing protocol employed on the Internet due to its robustness and scalability. In BGP, hosts communicate using the Transmission Control Protocol (TCP) and only the changed portion of the routing table is sent to the neighbors. Internal BGP does not send routing updates periodically and only the optimal path towards a destination network is transmitted to the neighbors [10].

BGP communicates with autonomous networks using the Internal BGP (IBGP). Hence the routers within an autonomous network need to maintain two routing tables: one for IGP and one of IBGP. The next-hop information from BGP is carried into IBGP. If IBGP does not have a route to reach the next hop, then the route will be discarded. These routes are established by the IGP.

b) Internet Protocol

IP developed to interconnect several networks. Its primary function is to route datagrams over the Internet and to provide addressing information of the source and destination nodes. It is also responsible for fragmentation of packets into smaller packets, since all networks cannot support large sized packets.

IP addresses are 32 bits long. Out of the 32 bits variable portions of the bits are used to specify the network address and the remaining bits are used to specify the host address. The networks are divided in to three classes, A, B, and C based on size. Class A is the largest network and can support up to 16,777,216 hosts (24 host bits). Class B is the second largest network with 65,536 hosts (16 host bits) and class C has 256 hosts (8 host bits).

The size of datagram is initially set to a convenient value but is fragmented as it passes through other networks that have limitations in packet lengths. The fragmented datagrams then travel independently taking separate paths and are assembled at the destination. If any one of the datagrams is lost, then the remaining datagrams are discarded and the source node retransmits the original datagram again. During fragmentation, most of the header is copied on to each datagram including the source/destination address but the length, offset, and the identifier for the last datagram fields are changed. These changed fields allow the original datagram to be reconstructed at the destination. The IP header also contains a Time-To-Live (TTL) field, which

is set by the source node, which is decremented by one every time it passes through a router. The packet is discarded when the TTL count reaches zero. The use of TTL field allows a packet to exist within a network for a limited amount of time thus avoiding congestion [8].

c) X.25 Network Layer Standard

X.25 is a network layer standard that provides an interface between a DTE and DCE. The DTE is basically an external computer while the DCE is a node inside the network.

The header structure of X.25 is 3 bytes long and contains fields for virtual channels. Apart from the 3 bytes it also contains an address field for the source and destination addresses. These addresses are used to set up a virtual circuit for a new session in the network. The virtual channel number does not help in setting up the virtual circuit but they simply specify the virtual channel to be used once the connection is established.

In order to set up the connection, a call-request packet is sent by the caller. The DCE receives this packet, sets up a path towards the destination and forwards the packet to the destination. Once the callee accepts the call, a call-accept packet is sent to the caller and the session is established. If a virtual circuit cannot be set up as then a clear-request packet is sent which contains the reason so as to why the session could not be established [8].

d) Internet Control Message Protocol

Internet Control Message Protocol (ICMP) communicates error messages during network operation. ICMPs are considered as a part of the IP layer and operate behind the application layer to indicate any problem in the connection or data transfer. ICMP is encapsulated within the IP datagram and contains the ICMP header and the ICMP message. The functions of ICMP are:

i) Report network problems:

Any network errors such as a host or some portions of a network that is unreachable due to some link failure are reported by ICMP error messages. A TCP or UDP packet directed towards a host that is not present in the network is reported using ICMP [11].

ii) TTL expiration announcement:

As discussed earlier, an IP packet contains a TTL field that is set to an integer value, which is decremented by one as the packet traverses a router. When this TTL field becomes zero, an ICMP message is generated and sent to the source computer indicating the time exceeded. TraceRoute (or tracert) is a utility that uses these TTL expiration messages to determine the path or intermediate routers traversed by an IP packet towards its destination. TraceRoute is an important tool for debugging network related problems [11].

iii) Source Quench Message:

Some times the sender sends data at higher speeds than the router can process. As a result the buffer space in the router is full and the router starts discarding the packets. The router sends an ICMP Source Quench message to indicate the dropping of packets by the router. The sender can thus reduce its data rate to match the rate of the router [11].

iv) Parameter problem:

An ICMP parameter problem message is sent to the source host in order to indicate some local or remote implementation error when the IP header is invalid or when an IP header option is missing [11].

e) Address Resolution Protocol

Address Resolution Protocol (ARP) maps the IP address of a computer to the hardware address used by the data link layer. The Internet Protocol uses ARP, which lies between the network layer and the data link layer in the OSI stack. The process of ARPing uses a client server model in which the server responds with the required address when a request is received.

As explained in module 4, the NIC has a unique 6 byte address stored in its memory. This address is called as the MAC address, which is used by the Ethernet to identify systems in a network. This address is attached with every packet that goes out of a system and is scanned in order to accept a packet in to the system.

The ARP protocol consists of 2 messages: ARP request and ARP reply. The ARP request contains the IP address of the requestor and IP address of the computer whose MAC address is desired. The ARP packet is broadcasted and the destination computer accepts the packet by looking at its IP address. The other computers simply reject the ARP request packet. The destination computer then sends an ARP reply packet that contains its IP address and MAC address to the requestor.

5.2.4 Transport Layer Protocols – Layer 4

The transport layer makes sure that the transmitted data is delivered to the destination node. It is responsible for end-to-end delivery of the entire message in contrast with the network layer that treats each packet of the message as a different message. The important transport layer protocols are TCP, UDP, and Real-time Transport Protocol (RTP).

a) Transmission Control Protocol (TCP)

The main feature of TCP is multiplexing and sequencing. In TCP, the complete address of source or the destination is called as the socket address. The socket address is a combination the IP address and the port number. Port numbers in TCP are 16 bits long. The IP address is divided into two parts: the network address and the host address. Thus TCP and IP work together as TCP provides the port addresses while IP provides the source and destination addresses. There may be

several packets destined for the same IP address, but they may belong to different sessions on the same computer. These packets will contain the same source and destination address, which is provided by the network layer. It is TCP that distinguishes which packet belongs to which session. Each session runs on a different port number, so the packets belonging to the same session have the same port number. Thus, TCP performs multiplexing and de-multiplexing by using port numbers [8].

The size of a TCP header is 20 bytes and it contains specific fields to handle fragmentation. A large message may be fragmented into several smaller datagrams due to the limitation of the network. TCP numbers each of these datagrams such that they can be reassembled in order when they are received at the destination. TCP performs error detection using a 16 bit check sum to verify the integrity of the received packet. TCP is a reliable protocol and supports retransmission of data that has been lost or discarded due to congestion.

b) User Datagram Protocol (UDP)

UDP is used in transport layer and was developed by the US Department of Defense in order to provide best-effort datagram delivery between two hosts. UDP is an unreliable protocol since it does not guarantee delivery of the datagram to the destination. The source computer does not need to establish a connection with the destination computer. Its header simply contains the source and destination port numbers and uses the support of the network layer in order to obtain the IP addresses of both the hosts.

At the destination, the transport layer receives the packets from the network layer. Each packet is verified for data integrity using the checksum field within the UDP header. The packets are discarded if an error is found in the received packet. Since UDP does not support retransmissions, the source computer remains unaware of the packets that were discarded or dropped during delivery.

UDP is used in delay-sensitive situations such as real time data transfer and streaming video. UDP packets are not processed at each node; hence the delay is reduced significantly. UDP is a connectionless protocol; hence every packet takes a different route towards the destination. These packets are finally arranged in sequence at the destination host [8].

c) Real-Time Transport Protocol (RTP)

Real-Time Transport Protocol manages transmission of real-time multimedia over the Internet. RTP was developed to support video conferencing between users in different locations around the globe.

RTP works in combination with the Real-Time Control Protocol (RTCP) in order to manage the transport of multimedia across large networks. RTCP allows the receiver to detect any packet losses during transmission and both protocols work transparent to the lower layer protocols. RTP works over UDP.

RTP does not ensure timely delivery of packets or deliver packets in sequence. It includes sequence numbers that allow the receiver to reconstruct the message. RTCP works with RTP to monitor the Quality of Service (QoS) and provides support for controlling a multimedia session.

5.2.5 Session Layer Protocols - Layer 5

The session layer establishes, maintains, and synchronizes communication between two computers. The session layer also provides some enhanced services such as file transfer between two computers, supports dialogue control by allowing the data traffic to be half duplex or full duplex, and supports synchronization (which is significant during large file transfers over the Internet). The session layer adds markers in the data stream such that even if the transfer is interrupted, the download can be resumed from the last checkpoint and not from the beginning.

Some of the important session layer protocols are Remote Procedure Call (RPC) and Secure SHell (SSH).

a) Remote Procedure Call (RPC)

RPC is designed to allow a computer to make a subroutine call on to a remote machine. RPC is designed to support network programming and uses a Client/Server model to provide service. The client side implements small software that initiates remote procedure calls to services supported by the server.

A remote procedure call is similar to the local procedure call where parameters are passed to a subroutine. The main program then passes the control to the subroutine and regains control after the task is accomplished. RPC uses a request-reply to implement this feature. The client sends a request message that contains the parameters required by the remote procedure. The server executes the procedure and sends a reply message that contains the results of the procedure. The client extracts the results from the reply packet and resumes execution of its task.

A process listens for a request message over a specified port on the server side. The server receiving the message extracts the parameters, sends the reply, and waits for the next connection attempt from clients [12].

b) Secure SHell (SSH)

SSH allows users to log into host systems remotely. As the name suggests, SSH provides encryption, preventing eavesdropping on the data transfer. It is safer than traditional remote login tools such as *rlogin* and *telnet* – which do not encrypt passwords between the client and server [13].

SSH provides security by verifying its connection to the same server during subsequent sessions. The server authenticates the client using a username and password that is transmitted in an

encrypted format by the client. SSH uses 128 bit encryption during the data transfer between the client and server making it next to impossible for intruders to intercept and interpret the data.

A large number of clients and servers can use the SSH protocol. The server uses a digital certificate to verify its identity and since each packet in the transfer is encrypted using a key know only to the client and server.

5.2.6 Presentation Layer Protocols – Layer 6

The presentation layer processes requests from the application layer and uses the services of the session layer. It is responsible for the formatting and syntax of the data exchanged between two hosts. The presentation layer changes data such as string or numbers in to bit streams in order to be transmitted. The presentation layer at the receiving end converts this bit format into a format that is supported by the receiving computer. The presentation layer is also responsible for data compression that helps in conserving network bandwidth.

One of the important Presentation layer protocols is eXternal Data Representation (XDR).

a) eXternal Data Representation (XDR)

XDR is a standard for description and encoding of data. It is used to transfer data between two computers that contain different architectures. The process of converting from local representation to XDR format is termed as encoding while conversion from XDR format to local representation is called as decoding. It is independent of the transport layer and is implemented in a format that portable between different operating systems.

XDR defines the following data types: Boolean, char, short, int, long, float, double, enumeration, structure, string etc [14].

5.2.7 Application Layer Protocols – Layer 7

The application layer provides an interface for a user to access network based services. Most networking software we use in day-to-day operations are applications – thus they interface with the application layer. All email, web browsers, and ftp programs are based on the application layer.

The application layer issues request to the presentation layer. Some of the supported applications are mail services such as email forwarding and storage and directory services. Some of the important application layer protocols are HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Network Management Protocol (SNMP), and Simple Mail Transfer Protocol (SMTP).

a) HyperText Transfer Protocol (HTTP)

HTTP is a standard for transmitting web pages over the Internet. HTTP operates usually over port 80. An HTTP transaction comprises of a request response cycle in which the client sends a HTTP request message to the server. The server replies back with an HTTP response. HTTP messages are readable with the simplest request message being 'GET url'. The server responds by sending the web page of the Uniform Resource Locater (URL) contained in the request message.

The request message consists of a request line, headers, and an optional body. The response message consists of a status line, headers, and an optional body. In addition to the GET request, the client can send HEAD and POST messages. POST messages are sent when a large amount of data is to be sent to the server. A web form requires a user to send data that can be sent with a POST message. A POST message contains a header followed by a blank line and then data. The header also contains a Content-Length field that allows the server to determine the amount of data transmitted [15].

b) File Transfer Protocol (FTP)

FTP is used to exchange files between computers over the Internet. FTP uses TCP/IP protocols and is similar to HTTP.

There are several FTP software packages available currently such as Cute FTP and a freeware called as CORE FTP. FTP software can be either command line based or has graphical user interface to uploading or downloading data files. An FTP server listens on port number 21 for connection requests. The port number can be changed but the client needs to make sure that it connects to the same port on which the server is listening for FTP connections.

FTP uses separate connections for control and data, which allows the flexibility to decide the desired QoS. The client always initiates the connection and both of the client and the server can send data after the connection is established. A graphical FTP interface requires to user to specify the server name and the user name and password to establish the connection. A command line FTP requires the server name or IP followed by the port number. Shown below is a typical FTP request.

Ftp www.myftpserver.com 21

The server then prompts the user for a user name and password. Once this information is verified, the authentication is complete and the two hosts can exchange files between each other use the PUT and GET commands.

c) Simple Mail Transfer Protocol (SMTP)

SMTP is a standard for transferring email over the Internet. SMTP is a text-based protocol that uses email addresses of the recipients to transfer the message. SMTP uses port number 25 to establish connection with the client.

SMTP does not have the capability to queue up messages at the receiving end. Hence, it is used with either the IMAP or POP3 protocol, which allows a user to download messages periodically from the server. A users SMTP process opens a TCP connection to an SMTP server over port 25. When the TCP connection is established, a request/response dialogue is exchanged where in the mail addresses of the sender and receiver is sent to the server. The server verifies these addresses and the email message are sent to the receiver [16].

d) Simple Network Management Protocol (SNMP)

SNMP is used for monitoring devices attached to the network. The SNMP architecture consists of a network agent and a network manager. The network manager is typically a client that issues request to the agents for management of the network and receives traps from the agents. SNMP exchanges messages to support management operations. They are:

1. GET REQUEST: used to retrieve management information from the SNMP agent.
2. GET RESPONSE: fetches the response from the SNMP agent.
3. SET: used to make any changed to the managed sub system.
4. TRAP: sent by the agent to report any event or changes in the state of the agent.

SNMP uses UDP port number 161 for the agent and 162 for the manager [17].