CHAPTER 1

Network Software:

It normally handles following things:

- Errors
- Flow in the channel
- Defining the path
- User applications

Computer Network:

Network is the collection of computers, software and hardware that are all connected to each other to help their users work together. A network connects computers by means of cabling systems, specialized software and devices that manage data traffic. A network enables users to share files and resources, such as printers as well as send messages electronically to each other. Computer network falls under two types:

i. Client/Server Network
ii. Peer to peer Network

Client/Server Network:

Each client is assigned an account name and password that is verified by an authentication service. The authentication service guards access to the network. With the centralization of user accounts, security, and access control, server based networks simplify the administration of large networks.

The concentration of network resources such as files, printers and applications on servers also make it easier to back-up and maintain the data. Resource can be located on specialized, dedicated servers for easier access.

Advantages:

- Easier to administer when the network is large.
- All data can be backed up on one central location.
- Provides better security.

Disadvantages:

- Require expensive, more powerful hardware for the server machine.
- Has a single point of failure. User data is unavailable when the server is down.
- Requires expensive specialized network administrative and operational software.
- Requires a professional administrator.

Peer-to-Peer Network:

Network computers act as equal partners, or peers. Each computer can take on the client function or the server function. Computer A may request for a file from computer B, which then sends the file to Computer A. Computer A acts like the client and Computer B acts like the server. At a later time, Computer A and B may reverse roles.

Individual users control their own resources. The users may decide to share certain files with other users. The users may also require passwords before they allow others to access their resources. Since individual users make these decisions, there is no central point of control or administration in the network. When a computer acts as a server, the user of that machine may experience reduced performance as the machine serves the requests made by the other systems.

Advantages:

- Less expensive to implement.

- Doesn’t require additional specialized network administration software.
- Doesn’t require a dedicated network administrator.

Disadvantages:

- Less secure.
- Doesn’t scale well to large networks and administration becomes unmanageable.
- Each must be trained to perform administrative tasks.
- All machines sharing resources negatively impact the performance.

Active Networks:

Active networks can be at least as secured as legacy networks. Data and algorithm in active network are mutable and fluid.

Benefits:

- Faster hardware, more fully utilized
- Enables more flexible network
- Decouples protocol from transport
- Minimizes global agreement overhead
- Enables on-the-fly experimentation
- Enables faster development of new services
- Adaptive monitoring and predictive control
- Devices become network-aware and smart
- Reduces protocol deployment time from years to months

Protocol:
Protocol defines the format and the order of message exchanged between two or more entities, as well as the action taken on the transaction and/or received of message or other events.

Q. Why do you think network software is in layer form?
To reduce the design complexity, most network software are organized as a stack of layers; each one built upon the one below it. The number of layer, the name of each layer, contents of each layer and the function of each layer differs. The purpose of each layer is to offer certain services to the higher levels, shielding those layers from the details of how the offered services are actually implemented. Layer concept is actually a familiar one and used throughout computer science where it is variously known as information hiding, abstract data types, data encapsulation and object oriented programming.
Other factors are:

- Independent implementation
- Reduced complexity
- Standardized interface
- Modular engineering
- Accelerate evolution
- Simplified teaching and learning

Types of Network:

- Intranet (within a single organization) ex: within ACEM
- Extranet (between two or more organizations) ex: between ACEM and Pulchowk
- Internet (worldwide connections)
- Multiprocessors
- PAN (Personal Area Network) ex: bluetooth, infrared

- LAN (Local Area Network) ex: within one room or building or organization
- MAN (Metropolitan Area Network) ex: cable T.V.
- WAN (Wide Area Network)

Network Topologies:

Network topology is the arrangement of the various elements (links, nodes, etc.) of a computer or biological network. Essentially, it is the topological structure of a network, and may be depicted physically or logically.

Physical topology refers to the placement of the network's various components, including device location and cable installation.

Logical topology shows how data flows within a network, regardless of its physical design.

Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ between two networks, yet their topologies may be identical.

Physical Topologies:

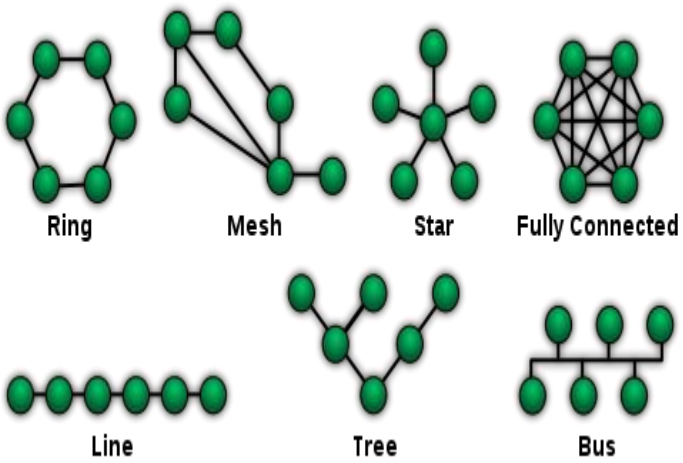
1. Ring Topology:
    - Each computer is connected to the network in a closed loop/ring.
    - A signal is passed along the ring in one direction from device to device until it reaches destination.
    - Primary disadvantage is that failure in one machine will cause entire network to fail.

2. Bus Topology:
    - Multipoint connection (more than two devices share single link).
    - Every machine is connected to single cable.
    - Ease of installations.
    - Less cabling.
    - If cable breaks in any condition, entire network will breakdown.

3. Star Topology:
    - Each machine is connected to the central hub.
    - If one link fails, only that link is affected.
    - But if hub goes down, whole system is affected.

4. Mesh Topology:
    - Every device has point-to-point link to every other devices.
    - If one link becomes unusable, it doesn’t incapacitate the entire system.
    - More amount of cabling and i/o ports are required.

5. Tree Topology:
    - Central root node is connected to one or more nodes that are one level lower in hierarchy.
6. Hybrid Topology:
    - Connection of different types of topologies.
    - Can form any structure as per need.



OSI model and TCP/IP model:

Differences:

OSI model	TCP/IP model
It is seven-layered.	It is four-layered.
Layers were first developed than protocol.	Protocol was first developed than layers.
Network layer provides both connectionless and connection-oriented services.	Internet layer provides connectionless service.
Transport layer provides only connection-oriented service.	Transport layer provides both connection-oriented and connectionless service.
It works in hierarchical form.	It also works in hierarchical form.

Layers of OSI model:

Layer 7: Application Layer

It defines interface to user processes for communication and data transfer in network. It provides standardized services such as virtual terminal, file and job transfer and operations.

Layer 6: Presentation Layer

It masks the differences of data formats between dissimilar systems and specifies architecture-independent data transfer format. It encodes and decodes data, encrypts and decrypts data, compresses and decompresses data.

Layer 5: Session Layer

It manages user sessions and dialogues, controls establishment and termination of logic links between users. It reports upper layer errors.

Layer 4: Transport Layer

It manages end-to-end message delivery in network, and provides reliable and sequential packet delivery through error recovery and flow control mechanisms. It provides connection oriented packet delivery.

Layer 3: Network Layer

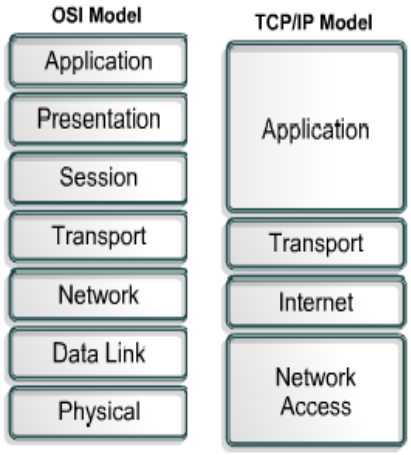
It determines how data are transferred between network devices, routes packets according to unique network device addresses and provides flow and congestion control to prevent network resource depletion.

Layer 2: Data Link Layer

It defines procedures for operating the communication links. It transfer frames. It detects and corrects packets transmit errors.

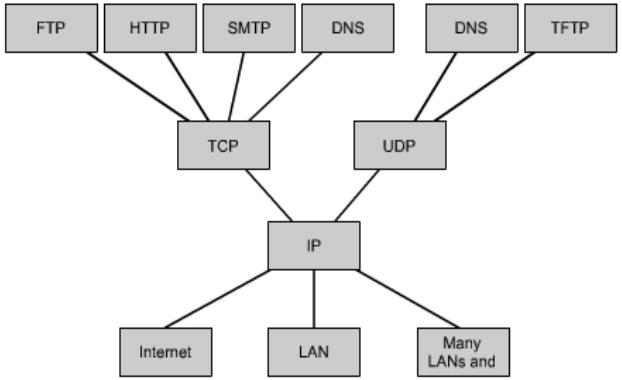
Layer 1: Physical Layer

It defines physical means of sending data over network devices. It acts as an interface between network medium and devices. It defines optical, electrical and mechanical characteristics.



TCP/IP

The four layers of the TCP/IP model are the application layer, transport layer, Internet layer, and network access layer. Some of the layers in the TCP/IP model have the same name as layers in the OSI model.



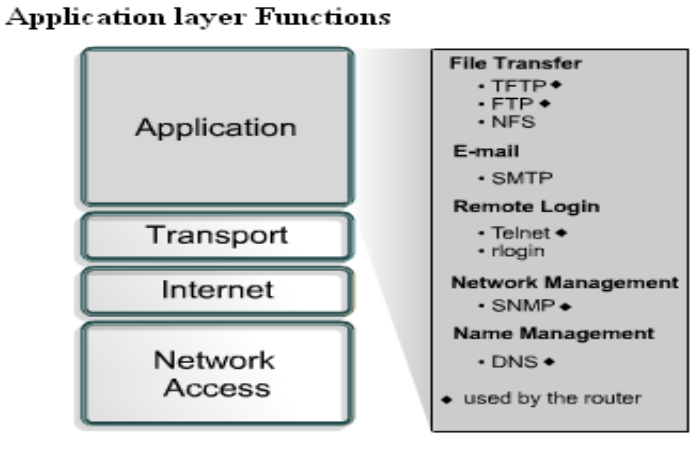
Common TCP/IP Protocols in different Layers

Application Layer

The session, presentation, and application layers of the OSI model are bundled into the application layer of the TCP/IP model. This means that representation, encoding, and dialog control are all handled in the TCP/IP application layer. This design ensures that the TCP/IP model provides maximum flexibility at the application layer for software developers.

The TCP/IP protocols that support file transfer, e-mail, and remote login are probably the most familiar to users of the Internet. These protocols include the following applications:

- DNS
- FTP
- HTTP
- SMTP



- SNMP
- Telnet

DNS

The Internet is built on a hierarchical addressing scheme. This scheme allows for routing to be based on classes of addresses rather than based on individual addresses. The problem this creates for the user is associating the correct address with the Internet site. It is very easy to forget an IP address to a particular site because there is nothing to associate the contents of the site with the address. Imagine the difficulty of remembering the IP addresses of tens, hundreds, or even thousands of Internet sites.

A domain naming system was developed in order to associate the contents of the site with the address of that site. The Domain Name System (DNS) is a system used on the Internet for translating names of domains and their publicly advertised network nodes into IP addresses. A domain is a group of computers that are associated by their geographical location or their business type. A domain name is a string of characters, number, or both. Usually a name or abbreviation that represents the numeric address of an Internet site will make up the domain name. There are more than 200 top-level domains on the Internet, examples of which include the following:

.us – United States

.uk – United Kingdom

.np – Nepal

There are also generic names, which examples include the following:

.edu – educational sites

.com – commercial sites

.gov – government sites

.org – non-profit sites

.net – network service

FTP and TFTP

FTP is a reliable, connection-oriented service that uses TCP to transfer files between systems that support FTP. The main purpose of FTP is to transfer files from one computer to another by copying and moving files from servers to clients, and from clients to servers. When files are copied from a server, FTP first establishes a control connection between the client and the server. Then a second connection is established, which is a link between the computers through which the data is transferred. Data transfer can occur in ASCII mode or in binary mode. These modes determine the encoding used for data file, which in the OSI model is a presentation layer task. After the file transfer has ended, the data connection terminates automatically. When the entire session of copying and moving files is complete, the command link is closed when the user logs off and ends the session.

TFTP is a connectionless service that uses User Datagram Protocol (UDP). TFTP is used on the router to transfer configuration files and Cisco IOS images and to transfer files between systems that support TFTP. TFTP is designed to be small and easy to implement. Therefore, it lacks most of the features of FTP. TFTP can read or write files to or from a remote server but it cannot list directories and currently has no provisions for

user authentication. It is useful in some LANs because it operates faster than FTP and in a stable environment it works reliably.

HTTP

Hypertext Transfer Protocol (HTTP) works with the World Wide Web, which is the fastest growing and most used part of the Internet. One of the main reasons for the extraordinary growth of the Web is the ease with which it allows access to information. A Web browser is a client-server application, which means that it requires both a client and a server component in order to function. A Web browser presents data in multimedia formats on Web pages that use text, graphics, sound, and video. The Web pages are created with a format language called Hypertext Markup Language (HTML). HTML directs a Web browser on a particular Web page to produce the appearance of the page in a specific manner. In addition, HTML specifies locations for the placement of text, files, and objects that are to be transferred from the Web server to the Web browser.

Hyperlinks make the World Wide Web easy to navigate. A hyperlink is an object, word, phrase, or picture, on a Web page. When that hyperlink is clicked, it directs the browser to a new Web page. The Web page contains, often hidden within its HTML description, an address location known as a Uniform Resource Locator (URL).

In the URL http://www.cisco.com/edu/, the "http://" tells the browser which protocol to use. The second part, "www", is the hostname or name of a specific machine with a specific IP address. The last part, /edu/ identifies the specific folder location on the server that contains the default web page.

URL

http://	www.	cisco.com	/edu/
Identifies to the browser what protocol should be used.	Identifies the hostname or name of a specific machine.	Represents the domain entity of the website.	Identifies the folder where the Web page is located on the server. Also, since no name is specified, the browser will load the default page identified by the server.

A Web browser usually opens to a starting or "home" page. The URL of the home page has already been stored in the configuration area of the Web browser and can be changed at any time. From the starting page, click on one of the Web page hyperlinks, or type a URL in the address bar of the browser. The Web browser examines the protocol to determine if it needs to open another program, and then determines the IP address of the Web server using DNS. Then the transport layer, network layer, data link layer, and physical layer work together to initiate a session with the Web server. The data that is transferred to the HTTP server contains the folder name of the Web page location. The data can also contain a specific file name for an HTML page. If no name is given, then the default name as specified in the configuration on the server is used.

The server responds to the request by sending to the Web client all of the text, audio, video, and graphic files specified in the HTML instructions. The client browser reassembles all the files to create a view of the Web page, and then terminates the session. If another page that is located on the same or a different server is clicked, the whole process begins again.

TELNET

Telnet client software provides the ability to login to a remote Internet host that is running a Telnet server application and then to execute commands from the command line. A Telnet client is referred to as a local host. Telnet server, which uses special software called a daemon, is referred to as a remote host.

To make a connection from a Telnet client, the connection option must be selected. A dialog box typically prompts for a host name and terminal type. The host name is the IP address or DNS name of the remote

computer. The terminal type describes the type of terminal emulation that the Telnet client should perform. The Telnet operation uses none of the processing power from the transmitting computer. Instead, it transmits the keystrokes to the remote host and sends the resulting screen output back to the local monitor. All processing and storage take place on the remote computer.

Telnet works at the application layer of the TCP/IP model. Therefore, Telnet works at the top three layers of the OSI model. The application layer deals with commands. The presentation layer handles formatting, usually ASCII. The session layer transmits. In the TCP/IP model, all of these functions are considered to be part of the application layer.

SMTP

Email servers communicate with each other using the Simple Mail Transfer Protocol (SMTP) to send and receive mail. The SMTP protocol transports email messages in ASCII format using TCP.

When a mail server receives a message destined for a local client, it stores that message and waits for the client to collect the mail. There are several ways for mail clients to collect their mail. They can use programs that access the mail server files directly or collect their mail using one of many network protocols. The most popular mail client protocols are POP3 and IMAP4, which both use TCP to transport data. Even though mail clients use these special protocols to collect mail, they almost always use SMTP to send mail. Since two different protocols, and possibly two different servers, are used to send and receive mail, it is possible that mail clients can perform one task and not the other. Therefore, it is usually a good idea to troubleshoot e-mail sending problems separately from e-mail receiving problems.

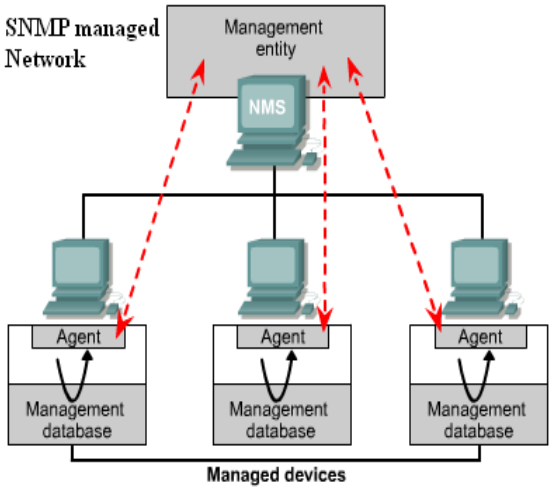
When checking the configuration of a mail client, verify that the SMTP and POP or IMAP settings are correctly configured. A good way to test if a mail server is reachable is to Telnet to the SMTP port (25) or to the POP3 port (110). The following command format is used at the Windows command line to test the ability to reach the SMTP service on the mail server at IP address 192.168.10.5:

C:\>telnet 192.168.10.5 25

The SMTP protocol does not offer much in the way of security and does not require any authentication. Administrators often do not allow hosts that are not part of their network to use their SMTP server to send or relay mail. This is to prevent unauthorized users from using their servers as mail relays.

SNMP

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. SNMP uses UDP as its transport layer protocol.



An SNMP managed network consists of the three key components: **Network management**

system (NMS) – NMS executes applications that monitor and control managed devices. The bulk of the processing and memory resources required for network management are provided by NMS. One or more NMSs must exist on any managed network.

Managed devices – Managed devices are network nodes that contain an SNMP agent and that reside on a managed network. Managed devices collect and store management information and make this information available to NMSs using SNMP. Managed devices, sometimes called network elements, can be routers, access servers, switches, and bridges, hubs, computer hosts, or printers.

Agents – Agents are network-management software modules that reside in managed devices. An agent has local knowledge of management information and translates that information into a form compatible with SNMP.

Transport Layer

The primary duties of the transport layer are to transport and regulate the flow of information from a source to a destination, reliably and accurately. End-to-end control and reliability are provided by sliding windows, sequencing numbers, and acknowledgments.

To understand reliability and flow control, think of someone who studies a foreign language for one year and then visits the country where that language is used. In conversation, words must be repeated for reliability. People must also speak slowly so that the conversation is understood, which relates to flow control.

The transport layer establishes a logical connection between two endpoints of a network. Protocols in the transport layer segment and reassemble data sent by upper-layer applications into the same transport layer data stream. This transport layer data stream provides end-to-end transport services.

The two primary duties of the transport layer are to provide flow control and reliability. The transport layer defines end-to-end connectivity between host applications.

Some basic transport services are as follows:

- Segmentation of upper-layer application data
- Establishment of end-to-end operations
- Transportation of segments from one end host to another
- Flow control provided by sliding windows
- Reliability provided by sequence numbers and acknowledgments

Protocols used in Transport layer are: TCP and UDP.

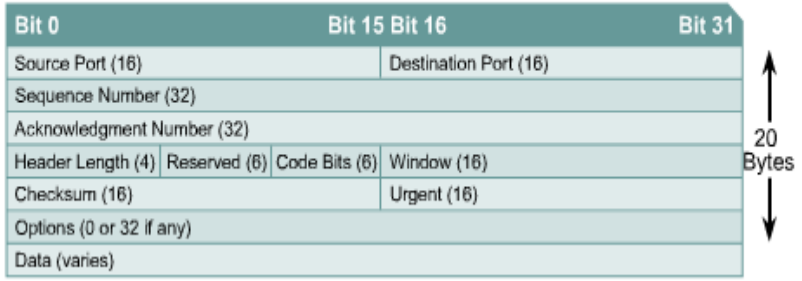
TCP

TCP is a connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack. In a connection-oriented environment, a connection is established between both ends before the transfer of information can begin. TCP breaks messages into segments, reassembles them at the destination, and resends anything that is not received. TCP supplies a virtual circuit between end-user applications.

The following application layer protocols use TCP:

FTP, HTTP, SMTP and Telnet

TCP Segment Format



Source port – Number of the port that sends data

Destination port – Number of the port that receives data

Sequence number – Number used to ensure the data arrives in the correct order

Acknowledgment number – Next expected TCP octet

HLEN – Number of 32-bit words in the header

Reserved – Set to zero

Code bits – Control functions, such as setup and termination of a session

Window – Number of octets that the sender will accept

Checksum – Calculated checksum of the header and data fields

Urgent pointer – Indicates the end of the urgent data

Option – One option currently defined, maximum TCP segment size

Data – Upper-layer protocol data

UDP

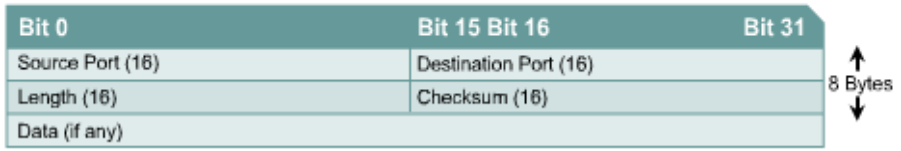
UDP is the connectionless transport protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagram without guaranteed delivery. It relies on higher-layer protocols to handle errors and retransmit data.

UDP does not use windows or ACKs. Reliability is provided by application layer protocols. UDP is designed for applications that do not need to put sequences of segments together.

The following application layer protocols use UDP:

TFTP, SNMP, DHCP, DNS

UDP Segment Format



Source port – Number of the port that sends data

Destination port – Number of the port that receives data

Length – Number of bytes in header and data

Checksum – Calculated checksum of the header and data fields

Data – Upper-layer protocol data

TCP/UDP Port Numbers

Both TCP and UDP use port numbers to pass information to the upper layers. Port numbers are used to keep track of different conversations that cross the network at the same time.

Application software developers agree to use well-known port numbers that are issued by the Internet Assigned Numbers Authority (IANA). Any conversation bound for the FTP application uses the standard port numbers 20 and 21. Port 20 is used for the data portion and Port 21 is used for control. Conversations that do not involve an application with a well-known port number are assigned port numbers randomly from within a specific range above 1023. Some ports are reserved in both TCP and UDP. However, applications might not be written to support them. Port numbers have the following assigned ranges:

Numbers below 1024 are considered well-known ports numbers.

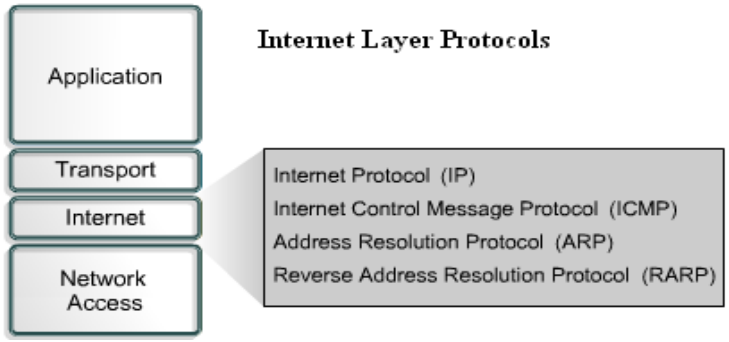
Numbers above 1024 are dynamically-assigned ports numbers.

Registered port numbers are for vendor-specific applications. Most of these are above 1024. End systems use port numbers to select the proper application. The source host dynamically assigns source port numbers. These numbers are always greater than 1023.

Internet Layers

The purpose of the Internet layer is to select the best path through the network for packets to travel. The main protocol that functions at this layer is IP. Best path determination and packet switching occur at this layer.

The following protocols operate at the TCP/IP Internet layer:



- IP provides connectionless, best-effort delivery routing of packets. IP is not concerned with the content of the packets but looks for a path to the destination.
- Internet Control Message Protocol (ICMP) provides control and messaging capabilities.
- Address Resolution Protocol (ARP) determines the data link layer address, or MAC address, for known IP addresses.
- Reverse Address Resolution Protocol (RARP) determines the IP address for a known MAC address.

IP performs the following operations:

- Defines a packet and an addressing scheme
- Transfers data between the Internet layer and network access layer
- Routes packets to remote hosts

IP is sometimes referred to as an unreliable protocol. This does not mean that IP will not accurately deliver data across a network. IP is unreliable because it does not perform error checking and correction. That function is handled by upper layer protocols from the transport or application layers.

ICMP

The internet protocol is connectionless-mode protocol, and as such, it has no error reporting and error-correcting mechanisms. It relies on a module called the Internet control message protocol (ICMP) to;

a. Reports errors on the processing of a datagram
b. Provide for some administrative and status messages.

ICMP sends messages and reports errors to the source host regarding the delivery of a packet. ICMP notifies the host if a destination is unreachable. ICMP is also responsible for managing and creating a time-exceeded message in the event that the lifetime of the datagram expires. ICMP also performs certain editing functions to determine if the IP header is in error or otherwise unintelligible.

The error and status reporting services of ICMP are summarized as below.

- Source Quench: This service is a form of flow and congestion control invoked by a route. When traffics become congested at the router, Router sends source quench message to a sending host to lower its transmission rate.
- Redirect: When preferred route is detected, gateway sends this message to host to send its traffics to another gateway. When route becomes congested, this message redirects the traffics to alternate route.
- Destination Unreachable: If a gateway encounters problems reaching the destination network specified in the IP destination address, this message is invoked if there is no route available such as when a line goes down.
- The time exceeded on the datagram lifetime: This service is executed by a gateway in the event the time-to live (TTL) field in the IP datagram has expired (value is zero) and gateway has discarded the datagram.
- Parameter unintelligible: when destination host or gateway encounters problem processing any part of an IP datagram and can't process datagram, destination host or gateway executed this message.
- Echo and echo reply: The echo can be sent to any IP address such as gateway. The gateway must return a reply to the originator indicating the state of the network or internet. If a problem exists, no reply is returned.
- Timestamp and timestamp reply: Used by gateways and hosts to determine the delay incurred in the delivering the data/traffic.
- Information request and reply: This service is used for a host to determine the identification of the network to which it is attached.
- Address mask request and reply: The use of an address mask allows the host part of IP address to be divided to subnetwork address and the host address. This service is used by a host to obtain a subnet mask used on the host's network.

IP Datagram:

Different s field used in IP (Version 4) datagram are depicted in fig below:

Version (4)	HLEN (4)	Types of services	Datagram Length (16)

		(8)		
Identifier (16)			Flags (3)	Fragment Offset (13)
TTL (8)		Protocol (8)	Header Checksum (16)	
Source IP address (32)				
Destination IP address				
Options or Padding not always				
Data (variable)				

* number in bracket indicates bits used in that field.

Version: Identifies the version of IP in use. Current version is IPV4.

HLEN: Header length is set to a value to indicate the length of datagram header. Most IP datagram doesn't contain options, so HLEN mostly indicates where the data begins in datagram. Typical IP datagram has 20 bytes header.

Types of services: Identifies different types of services included in IP datagram such as delay, throughput, precedence etc. IP datagram can be real-time or non-real-time as per type of services

Datagram Length: Indicates total length (Data + Header) of the IP datagram. Maximum length if IP datagram is 2^{16}=65535 bytes but in general not more than 1500 bytes.

Identifiers / Flags / Fragment Offset: Identifier (also called Fragment ID) indicates all fragments that belong together. Flags indicate that other fragments to follow. All fragments except last is indicated as 1 and last flag is 0.Fragment offset is used to tell the receiving host how to reassemble the packets.

Time-to-Live (TTL): TTL is used to measure the time a datagram has been in internet. Each Gateway in internet checks this field and discards packet if TTL is 0.

Protocol: this field is used to indicate upper layer protocols (Transport layer) that are to receive the datagram at the destination host. Either TCP or UDP receive the IP datagram at destination.

Header Checksum: Used o detect bit error at the receiving datagram.

Source/Destination address: IP datagram used two 32-bits addresses called source IP address and Destination IP address.

Options: The option field is not used in every datagram. His field is used sometimes for network management and diagnostics.

Data: Data field contains the user data. IP stipulates that the combination of header and Data can't exceed 65535 bytes. Data length varies from protocol to protocol used in network access layer.

IP datagram Fragmentation:

Not all network access layer protocols can carry packets of the same size. Some protocols can carry big packets and other protocols can carry small packets. For example, Ethernet packets can carry no more than 1500 bytes of data, whereas packets for many wide area network are not more than 576 bytes. The maximum amount of the data that the network access layer (TCP/IP model) protocol can carry is called Maximum Transfer Unit (MTU). Because each IP datagram is encapsulated within the network

access layer packet for transport between routers, the MTU of the network access protocol places a hard limit on the size of an IP datagram. The main problems here are that each of the links along the route between sender and receiver can use different network access protocols, and each of these protocols can have different MTUs.

When the size of IP datagram is large than the MTU of Network access layer protocols, this IP datagram need to be fragmented into two or more fragments. These fragments need to be reassembled before they reach to the destination transport layer. Reassembling is done with fragment ID and Fragment Offset. Indeed, both TCP and UDP are expecting to receive complete unfragmented segments from the Internet layer.

The designers of IPV4 felt that the fragmenting, reassembling and possibly again fragmenting and reassembling datagram into the routers would introduce significant complication into the protocol and put a damper on router performance. Fragmentation and reassembly add extra burden at sending routers and receiving hosts. So fragmentation should be minimized as far as possible. This is often done by limiting the TCP /UDP segments to a relatively small size i.e. less than 576 bytes (all network access layer protocols supported by IP are supposed to have MTUs at least 576 bytes. Fragmentation can be entirely eliminated by using an MSS (maximum segment size) of 536 bytes, 20 bytes for TCP header and 20 bytes for IP header.

Fragmentation is supported by only IPV4 not by IPV6.

Features of IP:

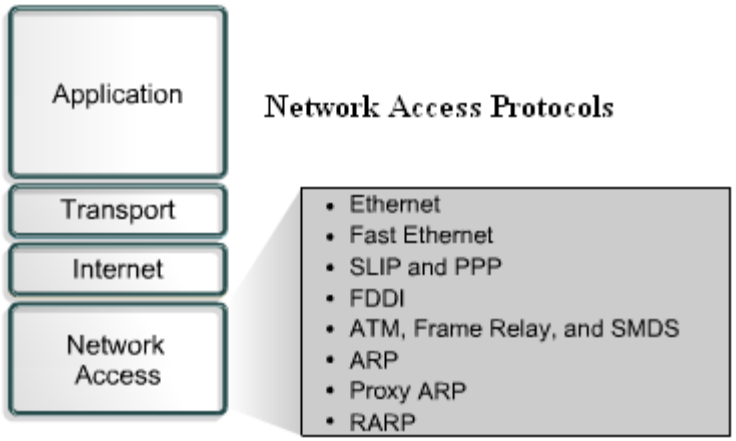
- *It is connectionless service:* So without prior call setup, it permits to exchange traffics between two host computers.
- *Datagram could be lost*: As IP is connectionless; it is possible that datagrams could be lost between two end user's stations.
- *IP hides underlying subnetwork from the end user:* In this context, it creates a virtual network for the end user. This aspect of IP is quite attractive, because it allows different types of networks to attach to an IP gateway. As a reason IP is reasonably simple to install and, because of its connectionless design, it is quite accommodating.
- *IP is unreliable, best effort and datagram type protocol:* It has no reliability mechanisms. It has no error recovery procedures for the underlying subnetworks.
- *IP has no flow control mechanisms:* The user datagram may lost, duplicated or even arrive at out of order. It is not the job of IP to deal with most of these problems. It is not the job of IP to deal with most of these problems, as most of the problems are passed to the next upper layer, TCP.
- *IPV4 supports fragmentation:* Fragmentation refers to an operation where in a protocol data unit (PDU) is divided or segmented into smaller units.

Network Access Layer

TCP/IP network access layer is also called the host-to-network layer. The network access layer allows an IP packet to make a physical link to the network media. It includes the LAN and WAN technology details and all the details contained in the OSI physical and data link layers.

Drivers for software applications, modem cards, and other devices operate at the network access layer. The network access layer defines the procedures used to interface with the network hardware and access the transmission medium. Modem protocol standards such as Serial Line Internet Protocol (SLIP) and Point-to-Point Protocol (PPP) provide network access through a modem connection. Many protocols are required to

determine the hardware, software, and transmission-medium specifications at this layer. This can lead to confusion for users. Most of the recognizable protocols operate at the transport and Internet layers of the TCP/IP model.



ARP and RARP work at both Internet and network access layers.

Network access layer protocols also map IP addresses to physical hardware addresses and encapsulate IP packets into frames. The network access layer defines the physical media connection based on the hardware type and network interface.

Here is an example of a network access layer configuration that involves a Windows system set up with a third party NIC. The NIC would automatically be detected by some versions of Windows and then the proper drivers would be installed. In an older version of Windows, the user would have to specify the network card driver. The card manufacturer supplies these drivers on disks or CD-ROMs.

The Internet:

The internet is a global system of interconnected computer network that uses the standard internet protocol suit (often called TCP/IP) to serve billions of users worldwide. It is a network of networks that consists of millions of private, public, academic, business and government networks of local to global scope that are linked by a broad array of electronic, wireless and optical network technologies.

MPLS (MultiProtocol Label Switching):

Cisco IOS MPLS enables enterprises and service providers to build next-generation intelligent networks. MPLS encapsulates packets with an additional header containing “label” information. The labels are used to switch the packets through the MPLS network. MPLS can be integrated seamlessly over any existing infrastructure, such as IP, Frame Relay, ATM (Asynchronous Transfer Mode), or Ethernet. MPLS is independent of access technologies.

MPLS technology is critical to scalable VPNs (Virtual Private Networks) and end-to-end QoS (Quality of Service). MPLS enables efficient use of existing networks to meet future growth and rapid fault correction of link and node failure. The technology also helps deliver highly scalable, and end-to-end IP services with simpler configuration, management, and provisioning for both Internet providers and subscribers.

VOIP:

Voice over IP (**VoIP**, abbreviation of **voice over Internet Protocol**) is a methodology and broad range of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms commonly associated with VoIP are *IP telephony*, *Internet telephony*, *voice over broadband* (VoBB), *broadband telephony*, *IP communications*, and *broadband phone service*.

Internet telephony refers to communications services—voice, fax, SMS, and/or voice-messaging applications—that are transported via an IP network, rather than the public switched telephone network (PSTN). The steps involved in originating a VoIP telephone call are signaling and media channel setup, digitization of the analog voice signal, encoding, packetization, and transmission as Internet Protocol (IP) packets over a packet-switched network. On the receiving side, similar steps (usually in the reverse order) such as reception of the IP packets, decoding of the packets and digital-to-analog conversion reproduce the original voice stream. Even though IP telephony and VoIP are used interchangeably, IP telephony refers to all use of IP protocols for voice communication by digital telephony systems, while VoIP is one technology used by IP telephony to transport phone calls.