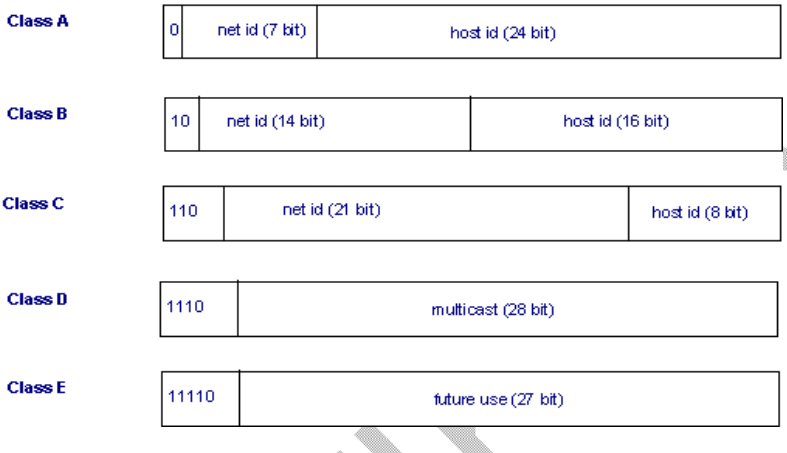
Unit-4

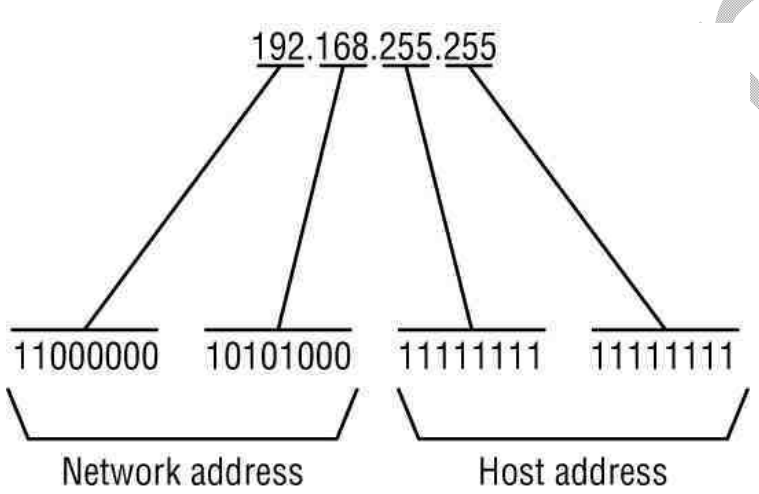
IP addressing

IP address class and network and host addressing: -

- The physical layer address (NIC address) that identify individual device.
- An IP address that identifies the connection of a host to its network.
- Each internet IP address consists of four bytes (32 bits).
- That defines three fields. [1] Class type [2] Net-id [3] Host-id.
- There are five types of classes are available for addressing.
- The different classes are design to cover the needs of different types of organizations.

	Range for first byte
Class A	0 - 127
Class B	128 - 191
Class C	192 - 223
Class D	224 - 239
Class E	240 - 255

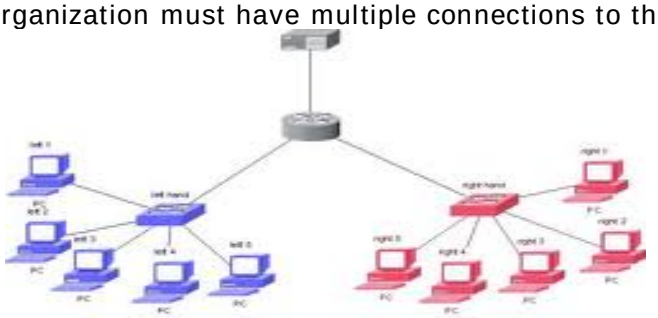




- An internet address defines the node's connections to its network.
- Any device connected to more than one network must have more than one internet address.
- A device has a different address for each network connected to it.

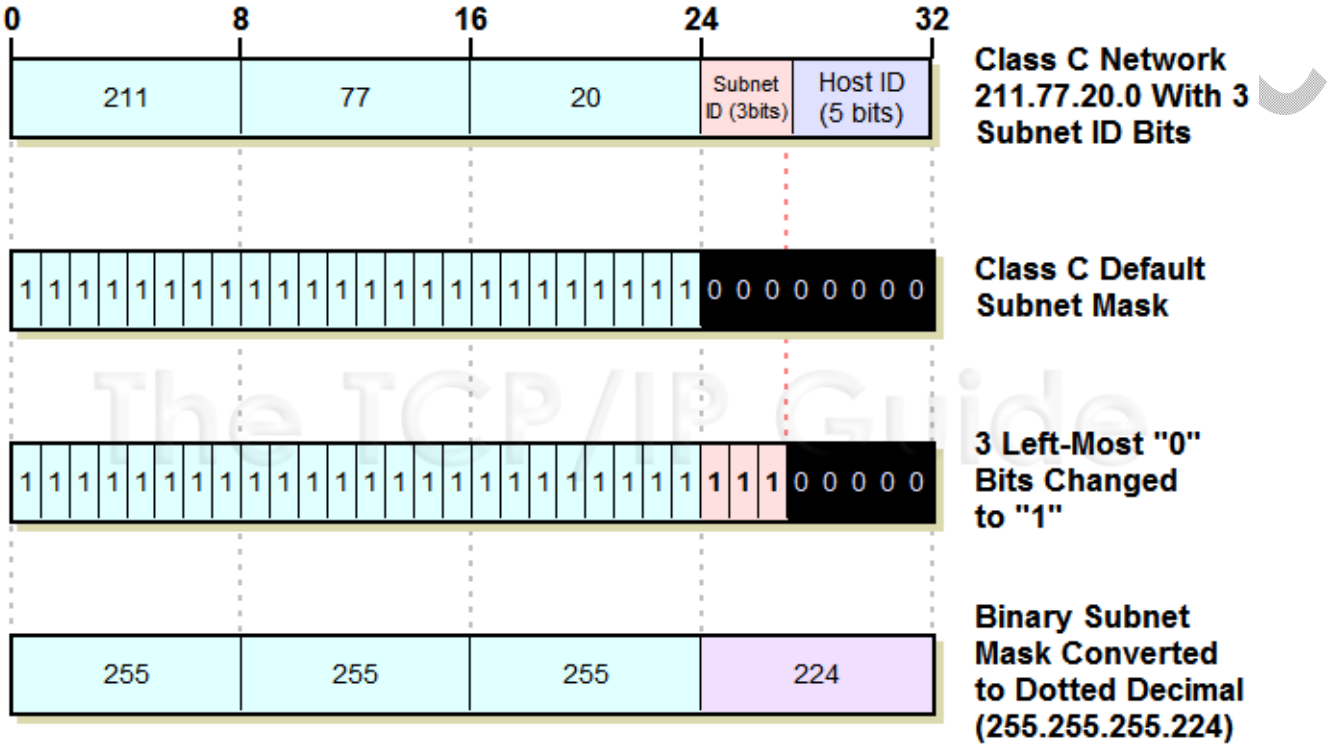
Subnet: -

- A subnet is short form of sub-network.
- A subnet is separate part of network.
- A subnet may represent all the machines at one geographic location in one building or on the same LAN.
- The network divided into small manageable segments it is called subnet.
- Subnet allows it to be connected to the internet with a single shared network address.
- Without subnets, an organization must have multiple connections to the internet.

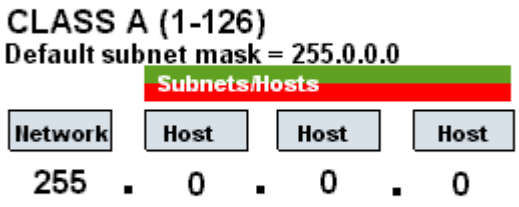


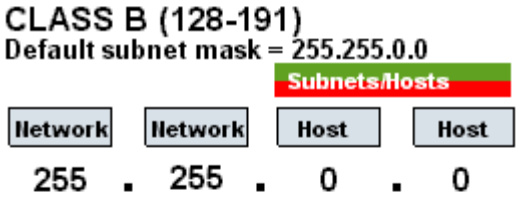
Subnet mask: -

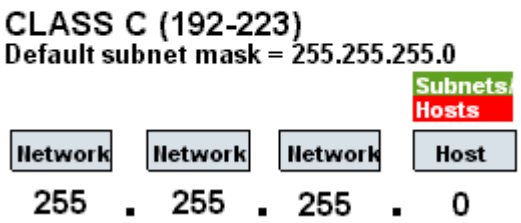
- An IP address has two components, the network address and the host address.
- A subnet mask separates the IP address into the network and host address.
- A mask used to determine what subnet an IP address belongs.
- For example, consider the IP address 150.215.017.009.
- This is the part of class B network.
- The first two numbers are represents the network address and last two numbers represents the host address.
- Sub netting enables the network administrator to further divide the host part of the address into two or more subnets.
- In this case, a part of the host address is reserved to identify the particular subnet.

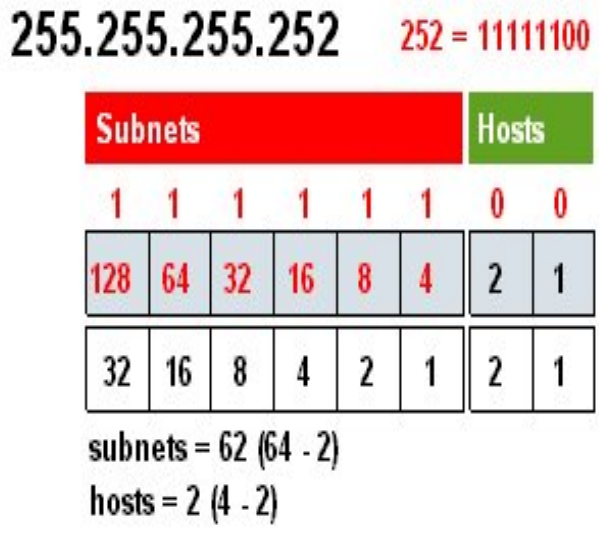


From Computer Desktop Encyclopedia
© 2003 The Computer Language Co. Inc.



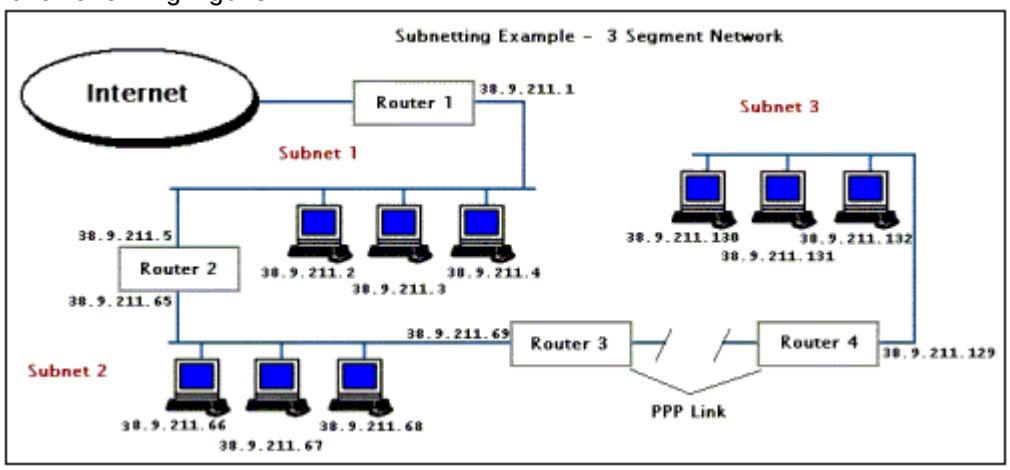






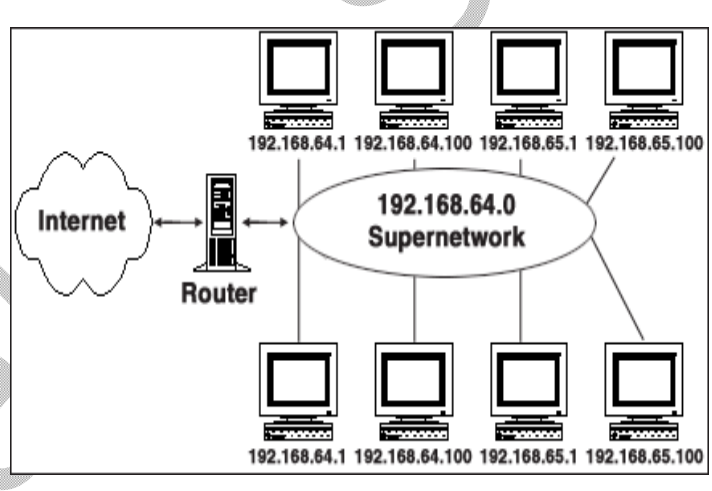
Sub netting: -

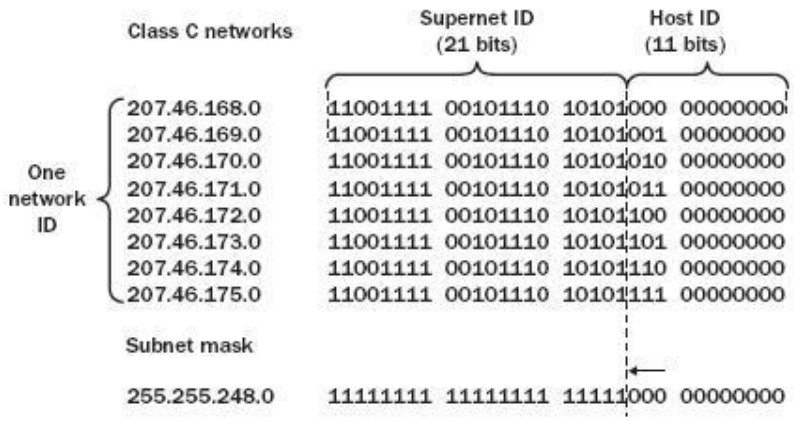
- An IP address is 32 bit long. One portion of the address indicates a network id, and other portion indicates the host id.
- To reach a host on the internet, we must first reach the network using the first portion of address.
- Then we must reach the host using second portion of the address.
- The organization has one network with many host then we use the sub netting.
- The sub netting is division of a network into smaller network called sub network.
- Consider the following figure.



Supper netting: -

- Supper netting is also called classless inter-domain routing (CIDR).
- CIDR is a way to aggregate multiple internet address of the same class.
- The original internet protocol (IP) defines OP addresses in four major classes of address structure.
- Using super netting, the network address 192.168.2.0/24 and adjacent address 192.168.3.0/24 can be merged into 192.168.2.0/23.
- The 23 at the end of address says that the first 23 bits are network part of the address.
- Remaining nine bits for specific host address.
- Super netting is most often used to combine class C network.



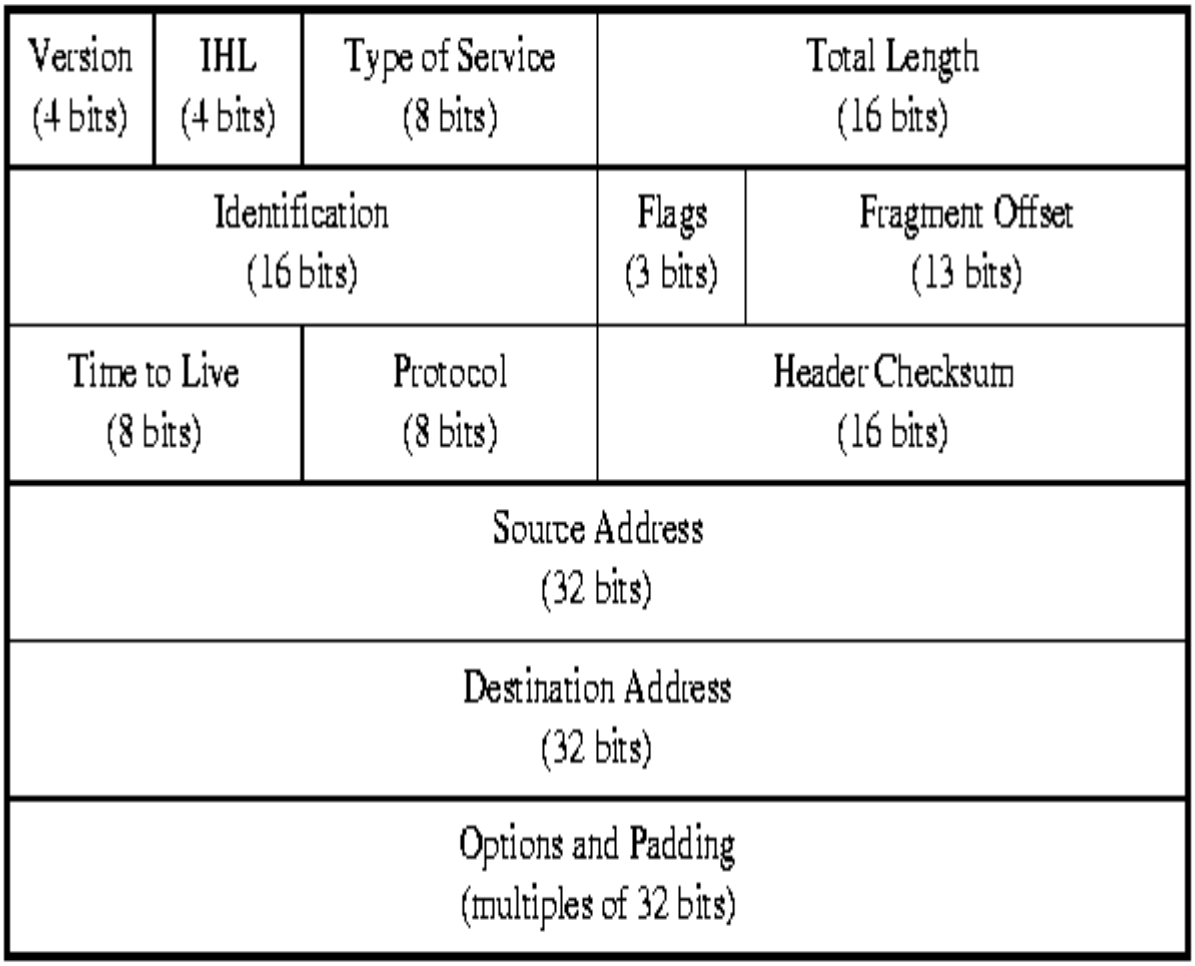


TCP / IP protocol suite

Network layer protocols: - IP, ARP, RARP, ICMP, IGMP

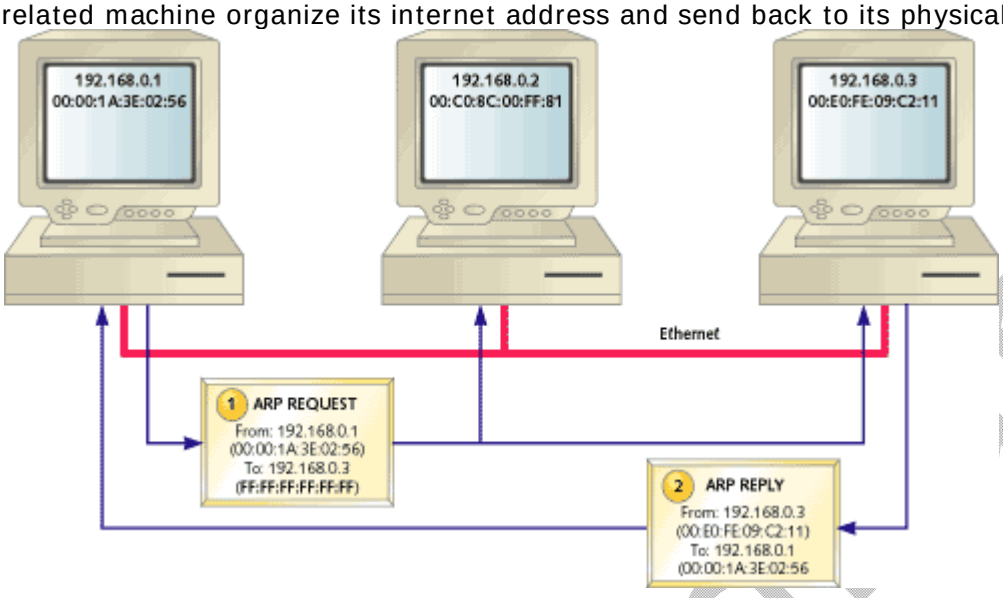
IP protocol: -

- IP transports data in packet called datagram. IP is connectionless protocol.
- Datagram may travel from different route.
- IP does not keep the track of the routs and does not provide the facility to reordering.
- A datagram is a variable length packet of 65,536 bytes.
- IP datagram consist of two parts: header and data.
- The header can be from 20-60 bytes.
- **Version:** The first field defines the version of IP.
- **Header length:** The HLEN field defines the length of header.
- **Service type:** The service type field defines how the datagram should be handled. It includes bit that defines the priority of the datagram.
- **Total length:** The total length field defines the total length of the IP datagram.
- **Identification:** The identification field is used in fragmentation. Each fragment is identified with sequence number in this field.
- **Flags:** The bits in the flags field deal with fragmentation. The datagram can or can not be fragmented.
- **Fragmentation offset:** The fragmentation offset is pointer that shows the offset of data.
- **Time to live:** The time to live field defines the number of hops on network.
- **Protocol:** The protocol field defines which upper-layer protocol data are used in datagram.
- **Header checksum:** This is a 16 bit field used to check the integrity of the header.
- **Source address:** The source address field is 4 byte (32 bits) internet address of source machine.
- **Destination address:** The destination address is 4 byte (32 bit) internet address of destination machine.
- **Options:** The option field provides more functionality to the IP datagram.



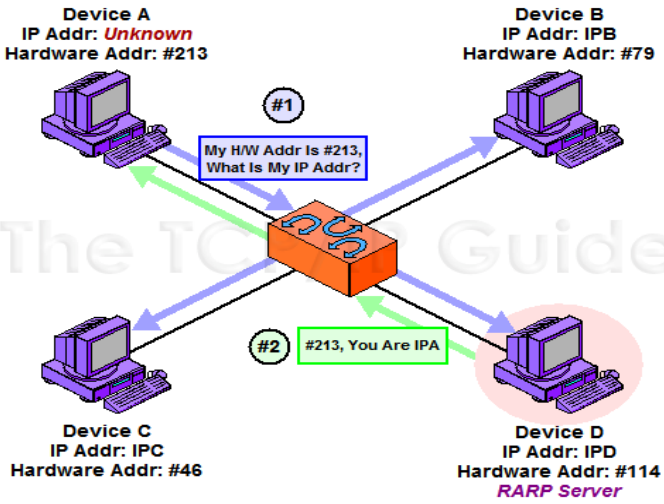
Address resolution protocol (ARP): -

- The ARP associates an IP address with the physical address.
- On a network, such as LAN, each device on a link identified by physical address.
- ARP used to find the physical address of the node when the internet address is known.
- An ARP query packet that includes the IP addresses and broadcast it over network.
- Every host on network receives the packet and process on it.
- But only related machine organize its internet address and send back to its physical address.



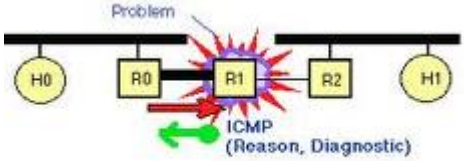
Reverse address resolution protocol (RARP): -

- The RARP allows a host to discover its internet address by using its physical address.
- This technique is used with diskless computer which are connected to the LAN.
- RARP works same as ARP.
- If the host want to retrieve its internet address, the machine broadcasts its RARP query packet that contains its physical address to every host on network.
- A server on the network process on that packet and provides the host's internet address.



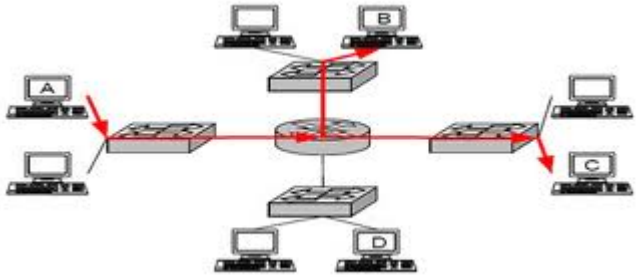
Internet control message protocol (ICMP): -

- The ICMP is mechanism used by hosts to send notification of problems back to the sender.
- ICMP allows informing a sender if datagram is undeliverable.
- ICMP uses echo test/replay to test weather a destination is reachable and responding.
- It also handles both control and error message.
- ICMP is not responsible to solve that error.
- A datagram contain the address of original source and destination. For this reason the ICMP can send messages only to source.



Internet group message protocol (IGMP): -

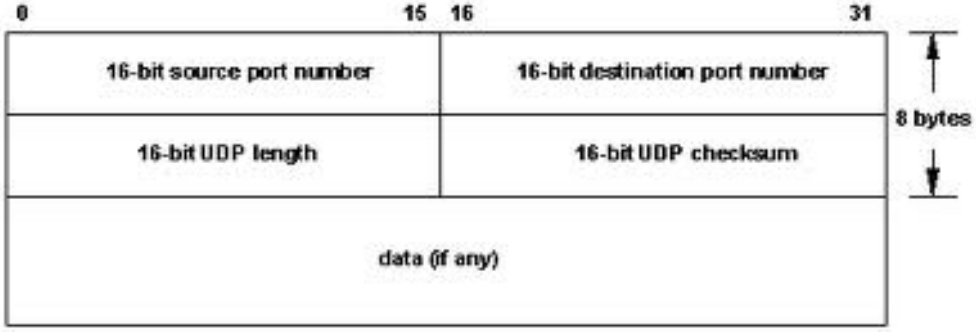
- The IP protocol can be communicate in two ways. [1] Uni-casting [2] Multi-casting.
- Uni-casting is the communication between one sender and one receiver.
- It is one-to-one communication.
- But some time we need to send the same message to a large number of receivers at the same time.
- This is called multi-casting.
- It is one-to many communications.
- For example: stock market, online travel booking, video and audio conferencing.
- IP address supports to the multi-casting.
- The IGMP has been design to help a multi-cast router to identify the hosts on LAN that are members of a multi-cast group.



Transport layer protocols: - UDP, TCP

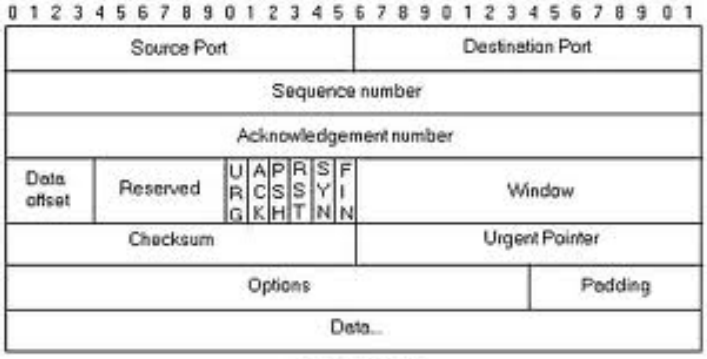
User datagram protocol (UDP): -

- The user datagram protocol is the simple and TCP/IP transport layer protocol.
- It is an end-to-end protocol and port-to-port protocol.
- The packet produce by the UDP is called a datagram.
- Port is buffer for storing a data for use by a particular process.
- UDP provides only the basic functions for end-to-end delivery.
- **Source port address:** The source port address is the address of the application program that has created the message.
- **Destination port address:** The destination port address is the address of the application program that will receive the message.
- **Total length:** The total length field defines the total length of the user datagram.
- **Checksum:** The checksum is a 16 bit field used in error detection.



Transmission control protocol (TCP): -

- TCP is connection oriented, reliable protocol.
- It is transport layer port-to-port protocol.



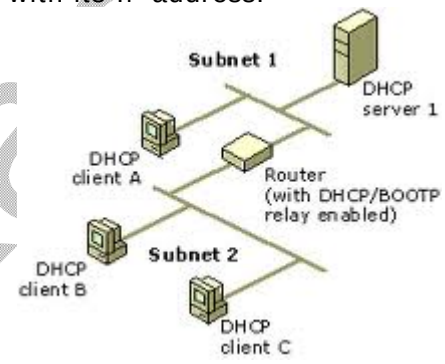
TCP Header

- TCP generates the virtual circuit between sender and receiver for data transmission.
- TCP divides long transmission into smaller data units called segments.
- Each segment includes sequence number.
- Port is buffer for storing a data for use by a particular process.
- **Source port address:** The source port address defines the application program in source computer.
- **Destination port address:** The destination port address defines the application program in the destination computer.
- **Sequence number:** A data stream is divided into TCP segments. The sequence number field shows the position of the data in the data stream.
- **Acknowledgement number:** The 32 bit acknowledgement number is used to acknowledge the receipt of data from the other communicating device.
- **Data offset (HLEN):** The four bit HLEN field indicates size of the TCP header.
- **Reserved:** A six bit field reserved for future use.
- **Control:** A six bit control fields is consists of urgent pointer (URG), acknowledgement number (ACK), push (PSH), reset (RST), synchronization (SYN), and finish (FIN).
- **Window size:** The window is a 16 bit field that defines the size of sliding window.
- **Checksum:** the checksum is a 16 bit field used in error detection.
- **Urgent pointer:** Its value is valid only if the URG bit in the control field is set. In this case, the sender informing that there are urgent data in the data portion of segment.
- **Option and padding:** This field of TCP header defines the optional field. They are used to provide the additional information to the receiver.

Application layer protocols: - BOOTP, DHCP, DNS, Telnet, FTP, TFTP, SMTP, SNMP

Bootstrap protocol (BOOTP): -

- The BOOTP is a client-server protocol.
- BOOTP is a static configuration protocol.
- It is design to provide the information like: IP address, subnet mask, IP address of router, and IP address of server for diskless computers.
- This protocol is used when diskless computer is boot first time from network.
- The BOOTP protocol privies the physical and internet address to the machine.
- When the client requests its IP address, the BOOTP server searches a table that matches the physical address of the client with its IP address.

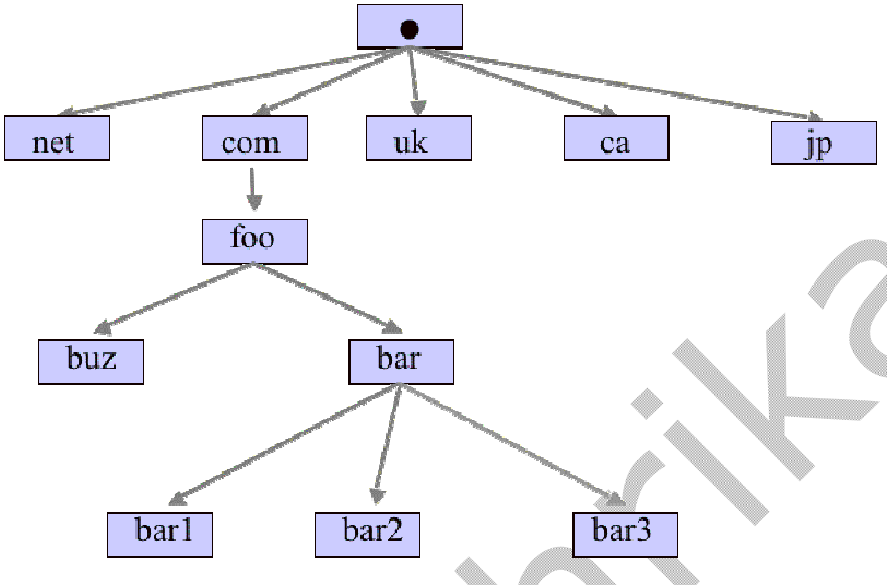


Dynamic configuration protocol (DHCP): -

- The DHCP has been designed to provide dynamic configuration.
- DHCP is the extension of BOOTP.
- The host machine running BOOTP client can request a static configuration from a DHCP server.
- DHCP is needed when a host moves from one network to another network.
- DHCP also needed when the client is removed or added to the network.
- DHCP provides temporary IP addresses for a limited period of time.

Domain name system (DNS): -

- To identify an entity, TCP/IP protocols use the IP address, which uniquely identifies the connection of host to the internet.
- Peoples are uses the names instead of IP address.
- Therefore, we need a system that can map a name to the address.
- DNS is protocol that can be used in different platforms.
- In the internet, the domain name space is divided into sections. [1] Generic domain [2] Country domain.
- **Generic domain:** The generic domains define registered hosts according to their behaviour. Each node in the tree defines a domain.

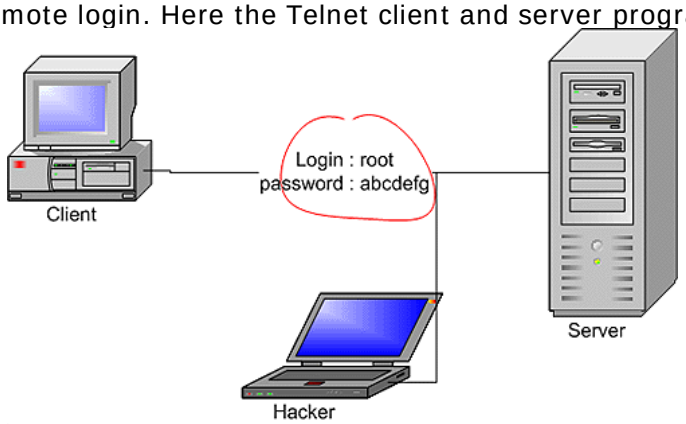


Label	Description
com	Commercial organization
edu	Educational institutions
gov	Government institutions
int	International organization
mil	Military groups
net	Network support centre
org	Non-profit organization

- **Country domain:** The country domain section uses two character country domains. For example India ‘in’, United States ‘us’, France ‘fr’.

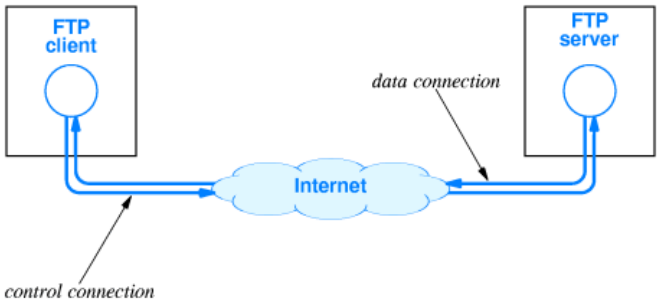
Terminal network (Telnet): -

- The main task of Telnet is to provide the services for users.
- For example, users want to be able to run different application program at a remote site and create results that can be transfer to the local machine.
- The Telnet is a client-server application program.
- **Local login:** When a user logs into a local system, it is called local login.
- **Remote login:** When user wants to access an application program located on a remote machine, he or she perform remote login. Here the Telnet client and server program come into use.



File transfer protocol (FTP): -

- FTP is mechanism provided by TCP/IP for copying a file from one host to another.
- FTP establishes two connections between the hosts.
- One connection is used to data transfer, another for control information.
- Separation of data transfer and control makes FTP more efficient.
- In FTP the client has three components. [1] User interface [2] Control process [3] Data transfer process.
- The server has two components. [1] Control process [2] Data transfer process.
- The connection is made between the control process of client and server.
- The data connection is made between the data transfer process of client and server.

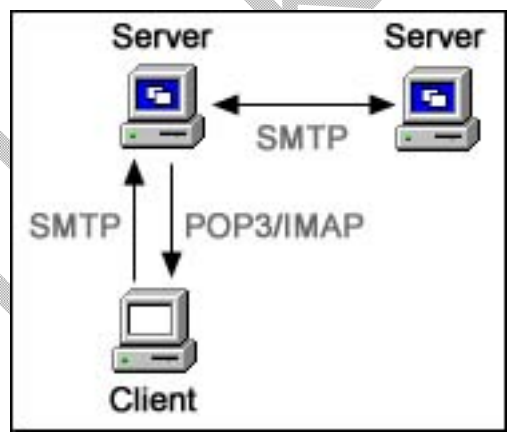


Trivial file transfer protocol (TFTP): -

- There are some situations when we need to simply copy a file without the need for all of the functionalities of the FTP.
- That time we just need a protocol that quickly copies the files.
- TFTP is designed for these types of file transfer.
- The software package can fit into read-only memory of a diskless machine.
- TFTP can read or write a file for the client.
- Reading means copying a file from sever site to client site.
- Writing means copying a file from client site to server site.

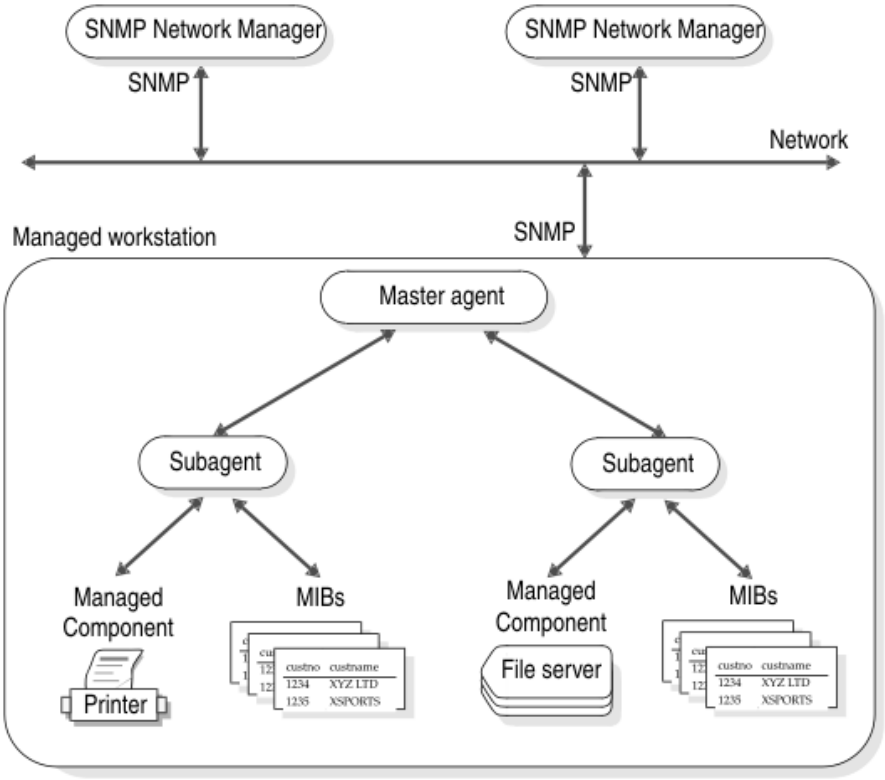
Simple mail transfer protocol (SMTP): -

- One of the most popular network services is e-mail.
- The TCP/IP protocol that supports e-mail on internet is called SMTP.
- SMTP provides for mail exchange between users.
- SMTP can provides the following:
  1. Sending a single message to one or more recipients.
  2. Sending messages that include text, voice, video, or graphics.
  3. Sending message to users on networks outside the internet.



Simple network management protocol (SNMP): -

- The SNMP is a framework for managing devices in an internet using TCP/IP protocols.
- It provides the set of fundamental operations for monitoring an internet.
- SNMP uses the concept of manager and agent.
- A manager, usually a host, controls and monitors as a set of agents.
- SNMP is an application-level protocol a few manager stations control a set of agents.
- The protocol is designed at the application level so that it can monitor the devices.
- It can be used in internet which is made of different LANs and WANs connected by routers or gateways made by different manufacturers.



Just remember: -

- **56K modem: -** A modem technology is using two different data rates: one for uploading and one for download from the internet.
- **Acknowledgement (ACK): -** A response sent by the receiver to indicate the successful receipt and acceptance of data.
- **Active hub:** - A hub that repeats or regenerates a signal. It functions same as the repeater.
- **Address resolution protocol (ARP): -** ARP is a protocol for obtaining the physical address of a node when internet address is known.
- **Advance research project agency (ARPA): -** The government agency that founded ARPANET.
- **ARPANET:** - The packet switching network that was founded by ARPA.
- **Amplitude modulation (AM): -** An anlog-to-analog conversion method in which the carrier signal's amplitude varies with the amplitude of modulating signals.
- **Angel of incidence: -** In optics, the angel formed by light ray approaching the interface between two media and the line perpendicular to the interface.
- **Angel of reflection:** - In optics, the angel formed by reflected light ray at the interface between two media and the line perpendicular to the interface.
- **Angel of refraction:** - In optics, the formed by a refracted light ray at the interface between to media and the line perpendicular to the interface.
- **Asymmetric digital subscriber line (ADSL):** - A communication technology in which the downstream data rate is higher than the upstream rate.
- **Asynchronous balanced mode (ABM):** - In HDLC, a communication mode in which all stations are equal.
- **Asynchronous transfer mode (ATM):** - A wide area network protocol featuring high data rate and equal-sized packets (cells); ATM is suitable for transferring text, audio, and video data.
- **Asynchronous time division multiplexing:** - Time division multiplexing in which link time is allocated dynamically according to the activity of the link.
- **Attenuation:** - The loss of signal's energy due to the resistance of the medium.
- **Bandwidth:** - The difference between the highest and the lowest frequencies of a composite signal. It also measures the information carrying capacity of a line or a network.
- **Backbone: -** The major transmission path in a network.
- **Baseband: -** Referring to a technology in which a signal is transmitted directly onto a channel without modulation carrier.
- **Binary synchronous communication (BSC): -** A popular character oriented data link protocol.
- **Bit oriented protocol: -** A protocol in which a frame is seen as a bit return.
- **Bit rate:** - The number of bits transmitted per second.
- **Blocked asynchronous transmission (BLAST):** - A more powerful version of XMODEM, featuring full-duplex transmission and sliding window flow control.
- **Bootstrap protocol (BOOTP):** - The protocol that provides configuration information from a table (file).
- **Bridge:** - A network device operating at the first two layer of the OSI model with filtering and forwarding capabilities.
- **Broadband: -** Referring to a technology in which a signal shares the bandwidth of a medium.
- **ISDN:** - ISDN with a high data rate based upon cell relay delivery.
- **Broadcasting: -** Transmission of message to all nodes in a network.
- **Brouter (Bridge/Router): -** A device that functions as both a bridge and a router.
- **Carrier sense multiple access (CSMA):** - A contention access method in which each station listen to the line before transmitting data.
- **Carrier sense multiple access with collision detection (CSMA/CD): -** CSMA with retransmission when collision is detected.
- **Character oriented protocol: -** A protocol in which the frame or packet is interpreted as a series of character.
- **Circuit switching:** - A switching technology that establishes an electrical connection between stations using dedicated path.
- **Cladding: -** Glass or plastic surrounding the core of an optical fiber; the optical density of the cladding must be less than that of the core.
- **Coaxial cable:** - A transmission medium consisting of a conduction core, insulating material, and a second conducting sheath.
- **Collision: -** The event that occurs when two transmitter send at the same time on a channel designed for only one transmission at a time; data will be destroyed.
- **Common gateway interface (CGI):** - A standard for communication between HTTP servers and executable programs. CGI is used in creating dynamic documents.
- **Congestion:** - Excessive network or internetwork traffic causing a general degradation of service.
- **Cognation control: -** A method to manage network and internetwork traffic to improve throughput.

- **Country domain: -** A sub-domain in the domain name system that uses two characters to identify a country as the last suffix.
- **Critical angel:** - In refraction, the value of angel of incidence that produces a 90-degree angel of refraction.
- **Crosstalk: -** The noise on a line caused by signals travelling along another line.
- **Cross-point:** - The junction of an input and an output on a crossbar switch.
- **Datagram:** - In packet switching, an independent data unit.
- **Demodulation: -** The process of separating the carrier signal from the information bearing signal.
- **Demodulator:** - A device that perform demodulation.
- **De-multiplexer (DEMUX): -** A device that separates a multiplexed signal into its original components.
- **Digital data service (DDS): -** A digital version of an analog leased line with a rate of 64 Kbps.
- **Digital subscriber line (DSL): -** A technology using existing telecommunication networks to accomplish high-speed delivery of data, voice, video, and multimedia.
- **Distortion:** - Any change in signal due to noise, attenuation, or other influence.
- **Domain name system (DNS):** - A TCP/IP application service that converts user-friendly name to IP address.
- **Dynamic host configuration protocol (DHCP): -** An extension of BOOTP that dynamically assigns configuration information.
- **Electromagnetic spectrum: -** A frequency range occupied by electromagnetic energy.
- **Error:** - A mistake in data transmission.
- **Error control:** - The detection and handling of error in data transmission.
- **Error correction:** - The process of correcting bits that have been changed during transmission.
- **Error detection:** - The process of determining whether or not some bit has been changed during transmission.
- **Error handling: -** The methods used to detect or correct error.
- **Error recovery: -** The ability of a system to resume normal activity after errors is detected.
- **Ethernet: -** A local area network using CSMA/CD access method.
- **Fiber distributed data interface (FDDI): -** A high speed (100 Mbps) LAN, defined by ANSI, using fiber optics, dual ring technology, and the token passing access method. Today an FDDI network is also used in MAN.
- **Fiber optic cable:** - A high bandwidth transmission medium that carries data signals in the form of pulses of light.
- **File transfer protocol (FTP): -** In TCP/IP, an application layer protocol that transfer files between two sites.
- **Flag:** - In HDLC, a field that alerts the receiver to the beginning or ending of a frame.
- **Flow control:** - A technique to control the rate of flow of frame (packet or message).
- **Frame: -** A group of bits representing a block of data.
- **Frequency:** - The number of cycle per second of a periodic signal.
- **Frequency division multiplexing (FDM):** - The combining of analog signals into a single signal.
- **Frequency modulation (FM): -** An analog-to-analog modulation method in which the carrier signal's frequency varies with amplitude of the modulating signal.
- **Full-duplex mode: -** A transmission mode in which communication can be two way simultaneously.
- **Gateway: -** A device used to connect two separate networks that use different communication protocols.
- **Generic domain: -** A sub-domain in the domain name system (DNS) that use generic suffix.
- **Guided media:** - Transmission media with physical link.
- **Half duplex mode:** - Transmission mode in which communication can be two way but not at same time.
- **High bit rate digital subscriber line (HDSL): -** A DSL based technology that uses 2B1Q encoding to lessen the effect of attenuation.
- **High level data link protocol (HDLC): -** A bit oriented data link protocol defined by the ISO.
- **Hub: -** A centre device in star topology that provides a common connection among the node.
- **Hyper text transfer protocol (HTTP): -** An application service for retrieving a web page document.
- **Integrated digital network (IDN): -** The integration of communication functions using digital technology in a telecommunication network.
- **Integrated services digital network (ISDN): -** An ITU-T standard for an end-to-end global digital communication system providing fully integrated digital service.
- **Internet: -** A collection of networks connected by internetworking devices such as router or gateways. Or a global internet that uses the TCP/IP protocol.
- **Internet control message protocol (ICMP): -** A protocol in the TCP/IP protocol suit that handles error and control message.

- **Internet group message protocol (IGMP):** - A protocol in the TCP/IP protocol suite that handles multicasting.
- **Internetworking devices: -** An electronic device such as routers and gateways that connect networks together to from the internet.
- **Internetworking (Internet) protocol (IP): -** The network layer protocol in the TCP/IP protocol suites governing connectionless transmission across packet-switching network.
- **IP datagram: -** The internetworking protocol data unit.