Network protocols are sets of rules for exchanging information. This exchange usually occurs much like a dialog between two computers. The exchange often begins with the client sending a signal to the server, providing key information about what kind of data is being requested. Network protocols made the modernization of the Internet possible. Such protocols allow computers to communicate with other computers without users having to know what is happening in the background.

*Significance : *Without a set of rules, computers would not have the capability of "talking" to each other across the Internet. Certain protocols help computers identify themselves on the Internet.*

*How Exchange Begins ? *The data exchange between computers on the Internet begins when the client introduces itself to the remote server it wants data from.*

*After the Handshake : *Some exchanges between computers are in short bursts (such as HTTP) while others can stream for long periods of time (as in instant messaging). The server may send a bundle of data and then close the connection, or it may continue to interact with the client computer until the client decides to end the conversation.*

*When Rules Aren't Followed ? *Network protocols were created to allow computers to communicate in an organized manner without any room for misinterpretation. Clients that do not follow the rules oftentimes are disconnected by the server, or vice versa, depending on what the protocol specifications state.*

1.1 Historical Development

Historical development of Internet

- 1950-1960 : electronic computer was become in 1950's. USA creates the Advanced Research Projects Agency (ARPA).
- 1960-1970 : ARPA contracts out work to BBN. BBN is called upon to build the first switch. ARPNET created - BBN creates the first switched network by linking four different nodes in California and Utah
- 1970-1980 : BBN creates the first program devoted to email. ARPA officially changes its name to DARPA Defense Advanced Research Projects Agency. Kahn and Cerf refer to the system as the Internet for the first time. Ethernet is developed by Dr. Robert M. Metcalfe.
- 1980-1990 : The National Science Foundation releases CSNET 56 to allow computers to network without being connected to the government networks. TCP/IP becomes the standard for internet protocol. Domain Name System introduced. No of host breaks 100000.
- 1990-2000 : U.S green-light for commercial enterprise to take place on the Internet. First internet ordering system created by Pizza Hut. First internet bank opened: First Virtual. Internet Service Providers begin appearing such as Sprint and MCI. Nokia releases first cell phone with internet access. A wireless technology called 802.11b, more commonly referred to as Wi-Fi, is standardized.
- 2000-2010 : Blackberry releases first internet cell phone in the United States. The spread of P2P file sharing across the Internet. Web 2.0 rises in popularity. 2005- Estonia offers Internet Voting nationally for local elections. 2005-Youtube launches. 2006- There are an estimated 92 million websites online. 2008 – NASA successfully tests the first deep space communications network modeled on the Internet. 2010- Facebook announces in February that it has 400 million active users.

Historical development of Network Protocols

- The Internet base protocols and systems were mainly devised in the 1970s and 1980s.
- The DNS was introduced in 1984, several years before commercial traffic was able to be part of the Internet.
- SMTP, or the Simple Message Transfer Protocol, is the basic standard for email, and again exists since the 1980s
- pre 1972 is FTP, or the file transfer protocol

Historical development of IPng (IPv6)

- Basic protocol (RFC 2460) published in 1998
- Basic socket API (RFC 2553) and DHCPv6 (RFC 3315) published in 2003.
- Mobile IPv6 (RFC 3775) published in 2004
- Flow label specifications (RFC 3697) added 2004
- Address architecture (RFC 4291) stable, minor revision in 2006
- Node requirements (RFC 4294) published 2006

1.2 OSI Model

layers: each layer implements a service

- via its own internal-layer actions
- relying on services provided by layer below

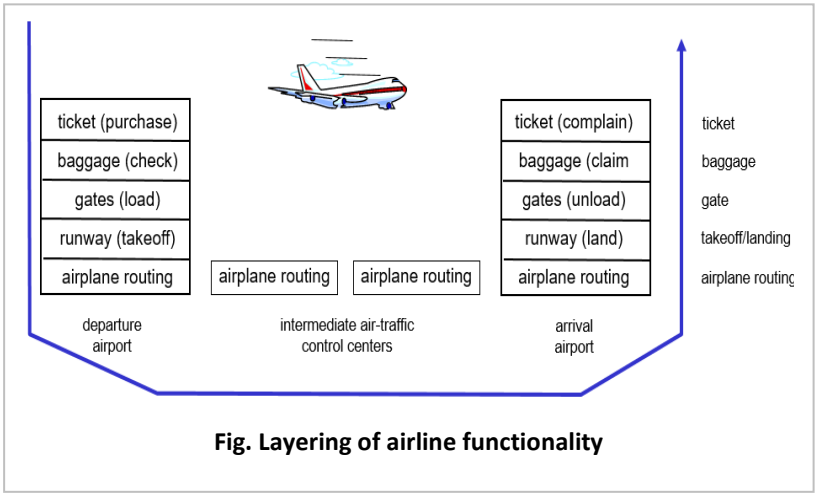

Fig. Layering of airline functionality

ISO-OSI Model:

There are many users who use computer network and are located all over the world. To ensure national and worldwide data communication ISO (ISO stands for International Organization of Standardization.) developed this model. This is called a model for open system interconnection (OSI) and is normally called as OSI model. OSI model architecture consists of seven layers. It defines seven layers or levels in a complete communication system.

Feature of OSI Model :

1. Big picture of communication over network is understandable through this OSI model.
2. We see how hardware and software work together.
3. We can understand new technologies as they are developed.
4. Troubleshooting is easier by separate networks.
5. Can be used to compare basic functional relationships on different networks.

Protocol Data Unit (PDU) : In telecommunications, the term **protocol data unit** (**PDU**) has the following meanings:

- Information that is delivered as a unit among peer entities of a network and that may contain control information, such as address information, or user data, also known as a service data unit (SDU).
- In a layered system, a unit of data which is specified in a protocol of a given layer and which consists of protocol-control information and possibly user data of that layer. For example: Bridge PDU or iSCSI PDU

Protocol Control Information : In telecommunication, the term **protocol-control information** or PCI has the following meanings:

1. The queries and replies among communications equipment to determine the respective capabilities of each end of the communications link.
2. For layered systems, information exchanged between entities of a given layer, via the service provided by the next lower layer, to coordinate their joint operation.

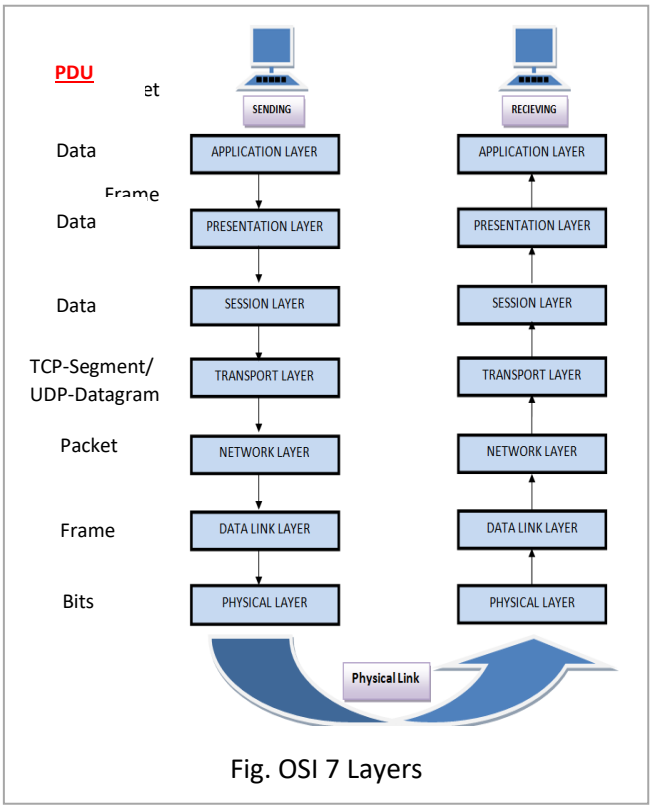

Fig. OSI 7 Layers

OSI Layers are

1.PHYSICAL LAYER

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

- *Data encoding*: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:
  - What signal state represents a binary 1
  - How the receiving station knows when a "bit-time" starts
  - How the receiving station defines a frame
  - Physical medium attachment, accommodating various possibilities in the medium:
  - Will an external transceiver (MAU) be used to connect to the medium?
  - How many pins do the connectors have and what is each pin used for?

- *Transmission technique*: determines whether the encoded bits will be transmitted by baseband (digital) or broadband (analog) signaling.
- *Physical medium transmission:* transmits bits as electrical or optical signals appropriate for the physical medium, and determines:
  - What physical medium options can be used
  - How many volts/db should be used to represent a given signal state, using a given physical medium

2.DATA LINK LAYER

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

- *Link establishment and termination:* establishes and terminates the logical link between two nodes.
- *Frame traffic control*: tells the transmitting node to "back-off" when no frame buffers are available.
- *Frame sequencing*: transmits/receives frames sequentially.
- *Frame acknowledgment*: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.
- *Frame delimiting*: creates and recognizes frame boundaries.
- *Frame error checking*: checks received frames for integrity.
- *Media access management*: determines when the node "has the right" to use the physical medium.

3.NETWORK LAYER

The network layer controls the operation of the subnet, routing : deciding which physical path the data should take based on network conditions, priority of service. Handles packet routing via logical addressing and switching functions. It provides:

- *Routing*: routes frames among networks.
- *Subnet* traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
- *Frame fragmentation*: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
- *Logical-physical address mapping*: translates logical addresses, or names, into physical addresses

4.TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers. provides quality of service (QoS) functions and ensures the complete delivery of the data. The integrity of the data is guaranteed at this layer via error correction and similar functions. The transport layer provides:

- *Message segmentation:* accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
- *Message acknowledgment:* provides reliable end-to-end message delivery with acknowledgments.
- *Message traffic control:* tells the transmitting station to "back-off" when no message buffers are available.
- *Session multiplexing:* multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

5.SESSION LAYER

Handles authentication and authorization functions. It also manages the connection between the two communicating devices, establishing a connection, maintaining the connection, and ultimately terminating it. The session layer allows session establishment between processes running on different stations. It provides:

- *Session establishment, maintenance and termination:* allows two application processes on different machines to establish, use and terminate a connection, called a session.
- *Session support:* performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

6.PRESENTATION LAYER

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:

- *Character code translation*: for example, ASCII to EBCDIC.
- *Data conversion*: bit order, CR-CR/LF, integer-floating point, and so on.

- *Data compression*: reduces the number of bits that need to be transmitted on the network.
- *Data encryption*: encrypt data for security purposes. For example, password encryption.

7.APPLICATION LAYER

The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

- Resource sharing and device redirection
- Remote file access, printer access
- Inter-process communication
- Network management
- Directory services
- Electronic messaging (such as mail)
- Network virtual terminals

OSI Reference Model Example

A web browser serves as a good practical illustration of the OSI model and the TCP/IP protocol suite:

• The web browser serves as the user interface for accessing a website. The browser itself does not function at the Application layer. Instead, the web browser invokes the Hyper Text Transfer Protocol (HTTP) to interface with the remote web server, which is why http:// precedes every web address.

• The Internet can provide data in a wide variety of formats, a function of the Presentation layer. Common formats on the Internet include HTML, XML, PHP, GIF, and JPEG. Any encryption or compression mechanisms used on a website are also considered a Presentation layer function.

• The Session layer is responsible for establishing, maintaining, and terminating the session between devices, and determining whether the communication is half-duplex or full-duplex. However, the TCP/IP stack generally does not include session-layer protocols, and is reliant on lower-layer protocols to perform these functions.

• HTTP utilizes the TCP Transport layer protocol to ensure the reliable delivery of data. TCP establishes and maintains a connection from the client to the web server, and packages the higher-layer data into segments. A sequence number is assigned to each segment so that data can be reassembled upon arrival.

• The best path to route the data between the client and the web server is determined by IP, a Network layer protocol. IP is also responsible for the assigned logical addresses on the client and server, and for encapsulating segments into packets.

• Data cannot be sent directly to a logical address. As packets travel from network to network, IP addresses are translated to hardware addresses, which are a function of the Data-Link layer. The packets are encapsulated into frames to be placed onto the physical medium.

• The data is finally transferred onto the network medium at the Physical layer, in the form of raw bits. Signaling and encoding mechanisms are defined at this layer, as is the hardware that forms the physical connection between the client and the web server

1.3 Internet IP/TCP/UDP

Relation between TCP and IP

If by "payload" you're referring to the data that comes after an IP header, then TCP is the "payload" of an IP packet when receiving data, since it's an upper level protocol.

TCP is connection oriented, while IP is a connection-less protocol. IP stands for a logical address, which works as packet address. The source packet has destination address for its destination. Tcp works with this logical address and helps the packets to reach their destinations, and provides acknowledgement when packet reached to its destination.

- Transmission Control Protocol (TCP)

It provides reliable communication between two hosts. *E.g. World Wide Web(HTTP), E-mail (SMTP TCP), File Transfer Protocol (FTP), Secure Shell (SSH).* ***Example*** *:***Email:** ***Reason:*** suppose if some packet(words/statement) is missing we cannot understand the content. It should be reliable.

The transmission Control Protocol (TCP) is one of the most important protocols of Internet Protocols suite. It is most widely used protocol for data transmission in communication network such as internet.

Features

- TCP is reliable protocol i.e. the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has bright clue about whether the data packet is reached the destination or it needs to resend it.
- TCP ensures that the data reaches intended destination in the same order it was sent.
- TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.
- TCP provides error-checking and recovery mechanism.
- TCP provides end-to-end communication.
- TCP provides flow control and quality of service.

- TCP operates in Client/Server point-to-point mode.
- TCP provides full duplex server, i.e. it can perform roles of both receiver and sender.

- **User Datagram Protocol (UDP)**

It provides unreliable communication between two hosts. *E.g. Domain Name System (DNS), Streaming media applications such as movies, Online multiplayer games, Voice over IP (VoIP), Trivial File Transfer Protocol (TFTP).* **Example : Video streaming: Reason:** Suppose if some packet(frame/sequence) is missing we can understand the content. Because video is collection of frames. For 1 second video, there should be 25 frames(image). Even though we can understand some frames are missing due to our imagination skills.

UDP is simplest Transport Layer communication protocol available of the TCP/IP protocol suite. It involves minimum amount of communication mechanism. UDP is said to be an unreliable transport protocol but it uses IP services which provides best effort delivery mechanism.

In UDP, the receiver does not generate an acknowledgement of packet received and in turn, the sender does not wait for any acknowledgement of packet sent. This shortcoming makes this protocol unreliable as well as easier on processing.

Features of UDP

- UDP is used when acknowledgement of data does not hold any significance.
- UDP is good protocol for data flowing in one direction.
- UDP is simple and suitable for query based communications.
- UDP is not connection oriented.
- UDP does not provide congestion control mechanism.
- UDP does not guarantee ordered delivery of data.
- UDP is stateless.
- UDP is suitable protocol for streaming applications such as VoIP, multimedia streaming.

How TCP Works

TCP stands for Transmission Control Protocol. It's the most commonly used protocol on the Internet.

When you load a web page, your computer sends TCP packets to the web server's address, asking it to send the web page to you. The web server responds by sending a stream of TCP packets, which your web browser stitches together to form the web page and display it to you. When you click a link, sign in, post a comment, or do anything else, your web browser sends TCP packets to the server and the server sends TCP packets back. TCP isn't just one way communication — the remote system sends packets back to acknowledge it's received your packets.

TCP guarantees the recipient will receive the packets in order by numbering them. The recipient sends messages back to the sender saying it received the messages. If the sender doesn't get a correct response, it will resend the packets to ensure the recipient received them. Packets are also checked for errors. TCP is all about this reliability — packets sent with TCP are tracked so no data is lost or corrupted in transit. This is why file downloads don't become corrupted even if there are network hiccups. Of course, if the recipient is completely offline, your computer will give up and you'll see an error message saying it can't communicate with the remote host.

How UDP Works

UDP stands for User Datagram Protocol — a datagram is the same thing as a packet of information. The UDP protocol works similarly to TCP, but it throws all the error-checking stuff out. All the back-and-forth communication and deliverability guarantees slow things down.

When using UDP, packets are just sent to the recipient. The sender won't wait to make sure the recipient received the packet — it will just continue sending the next packets. If you're the recipient and you miss some UDP packets, too bad — you can't ask for those packets again. There's no guarantee you're getting all the packets and there's no way to ask for a packet again if you miss it, but losing all this overhead means the computers can communicate more quickly.

UDP is used when speed is desirable and error correction isn't necessary. For example, UDP is frequently used for live broadcasts and online games.

For example UDP Use,

let's say you're watching a ***live video stream****. Live streams are often broadcast using UDP instead of TCP. The server just sends a constant stream of UDP packets to computers watching. If you lose your connection for a few seconds, the video will freeze for a moment and then jump to the current bit of the broadcast, skipping the bits you missed. If you experience minor packet-loss, the video or audio may be distorted for a moment as the video continues to play without the missing data.*

This works similarly in ***online games*** *— if you miss some UDP packets, player characters may appear to teleport across the map as you receive the newer UDP packets. There's no point in requesting the old packets if you missed them, as the game is continuing without you. All that matters is what's happening right now on the game server — not what happened a few seconds ago. Ditching TCP's error correction helps speed up the game connection and reduce latency.*

Difference between TCP and UDP

TCP	UDP
Reliable	Unreliable
Connection Oriented	Connectionless

Segment retransmission and flow control through windowing	No windowing and Retransmission
Segment Sequencing	No Sequencing
Acknowledge Sequencing	No Acknowledge
E.g. Client Server Application	e.g. Video Streaming, DNS

1.4 IPv4 Addressing Review

An Internet address uniquely identifies a node on the Internet. Internet address may also refer to the name or IP of a Web site (URL). The term Internet address can also represent someone's e-mail address.

In classless addressing variable-length blocks are assigned that belong to no class. In this architecture, the entire address space (232 addresses) is divided into blocks of different sizes.

Classful is based on the default Class A,B or C networks of 32 bit size.

All devices in the same routing domain must use the same subnet mask. Since routers running a classful routing protocol do not include subnet mask information with routing updates, the router assumes either its own subnet mask, or defaults to the classful subnet mask.

Classless on the other hand, allows the use of variable length subnet masks, or Variable-Length Subnet Masking (VLSM), because subnet mask information is included with routing updates. You can have a mixture of different subnet masks in the same routing domain: - 10.1.0.0/19, 10.2.0.0/20, 172.16.8.0/21, 172.16.16.0/24

Classful addressing:

- In the classful addressing system all the IP addresses that are available are divided into the five classes A,B,C,D and E, in which class A,B and C address are frequently used because class D is for Multicast and is rarely used and class E is reserved and is not currently used.
- Each of the IP address belongs to a particular class that's why they are classful addresses.
- Earlier this addressing system did not have any name, but when classless addressing system came into existence then it is named as Classful addressing system.
- The main disadvantage of classful addressing is that it limited the flexibility and number of addresses that can be assigned to any device.
- One of the major disadvantage of classful addressing is that it does not send subnet information but it will send the complete network address. The router will supply its own subnet mask based on its locally configured subnets. As long as you have the same subnet mask and the network is contiguous, you can use subnets of a classful network address.

Host *IP* address - The Host ID portion of an IP address, is the portion of the address used to identify hosts (any device requiring a Network Interface Card, such as a PC or networked printer) on the network. *e.g. ip add 192.168.100.2 and subnet mask 255.255.255.0 now 192.168.100.X is network id which is used to identify from which network u belongs to and x is host id which is unique for every node on network*

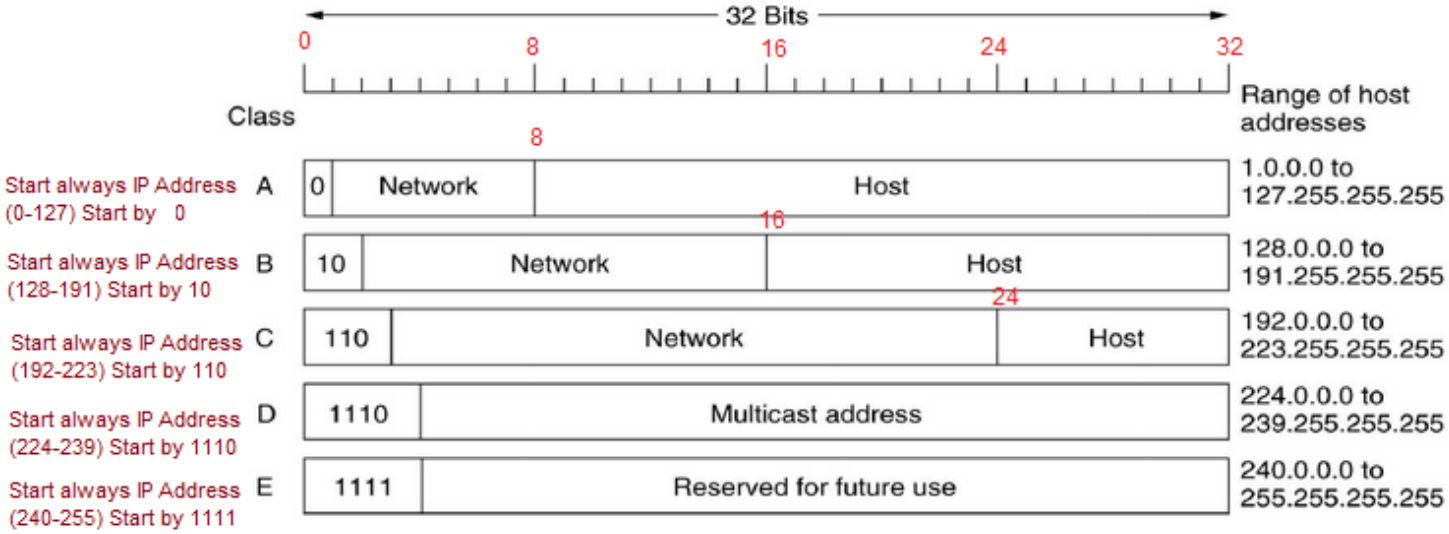

Table 43: IP Address Classes and Class Characteristics and Uses

IP Address Class	Fraction of Total IP Address Space	n = Number Of Network ID Bits	p = Number Of Host ID Bits	IP Range	Intended Use
Class A	1/2	8	24	0-127	Unicast addressing for very large organizations with hundreds of thousands or millions of hosts to connect to the Internet.
Class B	1/4	16	16	128-191	Unicast addressing for medium-to-large organizations with many hundreds to thousands of hosts to connect to the Internet.

Class C	1/8	24	8	192-223	Unicast addressing for smaller organizations with no more than about 250 hosts to connect to the Internet.
Class D	1/16	n/a	n/a	224-239	IP multicasting.
Class E	1/16	n/a	n/a	240-255	Reserved for "experimental use".

Class	Starting Bits (fixed to m bits)	Example	Max Networks 2^{n-m}	Max Hosts 2^{p}-2	Default subnet mask
A	0 (m=1)	125.168.3.5 = 01111101.10101000.0000011.00000101	2^{8-1} = 126	2^{24}-2= 16,777,214	255.0.0.0
B	10 (m=2)	155.168.3.5 = 10011011.10101000.0000011.00000101	2^{16-2} = 16,384	2^{16}-2=65,534	255.255.0.0
C	110 (m=3)	192.168.3.5 = 1100000.10101000.0000011.00000101	2^{24-3} = 2,097,152	2^{8}-2=254	255.255.255.0
D	1110				
E	1111				

Private IP Address

- A private IP address is an IP address that's reserved for internal use behind a router or other Network Address Translation (NAT) device, apart from the public.
- Private IP addresses are in contrast to public IP addresses, which are public and cannot be used within a home or business network.
- Sometimes a private IP address is also referred to as a *local IP address*.
- The Internet Assigned Numbers Authority (IANA) reserves the following IP address blocks for use as private IP addresses:
  i. **10.0.0.0 to 10.255.255.255**, allows over 16 million addresses
  ii. **172.16.0.0 to 172.31.255.255**, allows over 1 million addresses
  iii. **192.168.0.0 to 192.168.255.255**, allows over 65,000 addresses

RFC1918 name	IP address range	host id	mask bits	number of addresses	*classful* description	largest CIDR block (subnet mask)
24-bit block	10.0.0.0 - 10.255.255.255 11111111.x.x.x	24 bits	8 bits	16,777,216	single class A network	10.0.0.0/8 (255.0.0.0)
20-bit block	172.16.0.0 - 172.31.255.255 11111111.1111xxxx.x.x	20 bits	12 bits	1,048,576	16 contiguous class B networks	172.16.0.0/12 (255.240.0.0)
16-bit block	192.168.0.0 - 192.168.255.255 11111111.11111111.x.x	16 bits	16 bits	65,536	256 contiguous class C networks	192.168.0.0/16 (255.255.0.0)

Reserved IP Address

- Another set of IP addresses that are restricted even further are called *reserved* IP addresses.
- These are similar to private IP addresses in the sense that they can't be used for communicating on the greater internet, but they're even more restrictive than that.
- The most famous reserved IP is 127.0.0.1. This address is called the loopback address and is used to test the network adapter or integrated chip. No traffic addressed to 127.0.0.1 is sent over the local network or public internet.
- Technically, the entire range from **127.0.0.0 to 127.255.255.255** is reserved for loopback purposes but you'll almost never see anything but 127.0.0.1 used in the real world.
- The range from **0.0.0.0 to 0.255.255.255** are also reserved but don't do anything at all.