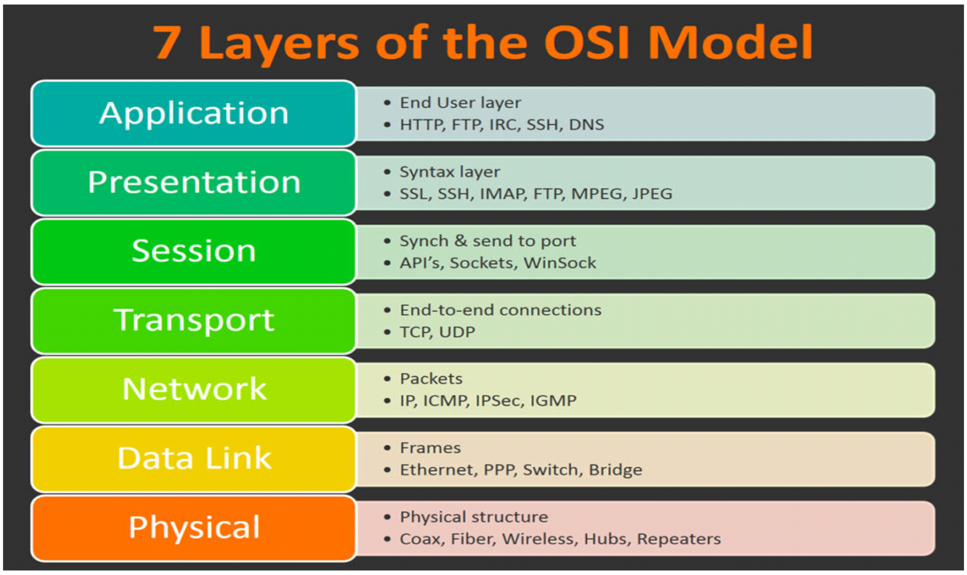
OSI (open system Interconnection) MODEL:

In the year 1974 ISO (International Organization of Standardization) defined 7 layer architecture of a computer network. Each layer has a specific functionality. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.



7 Layers of the OSI Model

Application	• End User layer • HTTP, FTP, IRC, SSH, DNS
Presentation	• Syntax layer • SSL, SSH, IMAP, FTP, MPEG, JPEG
Session	• Synch & send to port • API's, Sockets, WinSock
Transport	• End-to-end connections • TCP, UDP
Network	• Packets • IP, ICMP, IPSec, IGMP
Data Link	• Frames • Ethernet, PPP, Switch, Bridge
Physical	• Physical structure • Coax, Fiber, Wireless, Hubs, Repeaters

Physical layer

This is the lowest layer, which is responsible for actual physical connection between the devices. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer.

Hub, Repeater, Modem, Cables are Physical Layer devices.

Data Link layer (node to node delivery)

The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error free from one node to another. When a packet arrives in a network, it is the responsibility of Data Link Layer to transmit it to the Host using its MAC address.

Switch & Bridge are Data Link Layer devices.

Network Layer (host to host delivery)

Network layer works for the transmission of data from one host to the other host located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP address are placed in the header by network layer.

Network layer is implemented by networking devices such as routers.

Transport Layer (process to process delivery)

Transport layer provides services to application layer and takes services from network layer. It is also responsibility of Transport Layer to provide acknowledgement of successful data transmission.

At the sender's end the transmission layer receives formatted data and adds source and destination port numbers. At the receiver's end the transport layer reads the port number. It also does the function of sequencing and rearranging the segmented data.

Transport layer is operated by the Operating System.

Session Layer

This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.

Presentation Layer

The data from the application layer is extracted here and manipulated as per the required format to transmit over the network. It also takes care of encryption and decryption of data.

Application Layer

This is the top most layer. This is implemented using the network applications like Browsers, Skype Messenger etc.

Network Architecture

It is a framework for the specification of a network's physical components and their functional organization and configuration, its operational principles and procedures, as well as communication protocols used.

There are two main network architectures

Client-server architecture:

In this architecture the structure divided between the providers of a resource or service, called servers, and service requesters, called clients. The client sends a request, and the server returns a response.

Since servers are usually accessed over a network they would need to be run for long periods without interruption. Also the servers would need better hardware to take care of number of users and total bandwidth consumed.

The server will be given more administrative powers than the clients to equip it to provide requisite service and takes care of security of the network.

For example: when a customer accesses the online banking service of a bank, the web browser acts as a client that requests data from bank’s web server.

Peer- To – Peer architecture:

In a P2P network, the "peers" are computer systems which are connected to each other via the Internet. Files can be shared directly between systems on the network without the need of a central server. All the computers connected to each other have equal status in the network. Also normally the computers connected in peer-to-peer fashion are having comparable hardware.

For example, the computers connected in a school laboratory.

WWW

1. WWW (World Wide Web), is a collection of interlinked hypertext documents accessed using Internet.
2. These documents can be viewed using web browser. These documents can contain text, pictures, audio and video.
3. English scientist Tim Berners Lee invented WWW in 1989. The first web browser also was written by him in 1990.
4. first web browser was www and later renamed as nexus
5. Multiple web documents or web pages related to each other are collected in one place and such collection is called web site.
6. Web sites are stored on a special computer that works 24x7 to respond to the request to view the web pages. Such special computers \are called web servers.

URL

1. Every type of resource (text, audio, and video) on www (World Wide Web) has global address that identifies these resources uniquely.
2. This global address is called URL (uniform resource locator).
3. When you search Google, for example, the search results will display the URL of the resources that match your search query. The title in search results is simply a hyperlink to the URL of the resource.

Parts of url:

2 parts: protocol identifier and resource location separated by colon followed by two forward slash (://)

Example:

ftp://www.webopedia.com/stuff.exe

File transfer protocol is used to download executable file.

http://www.webopedia.com/index.html

Web page access using http.

In given examples www.webopedia.com is the domain name which is used to access the website.

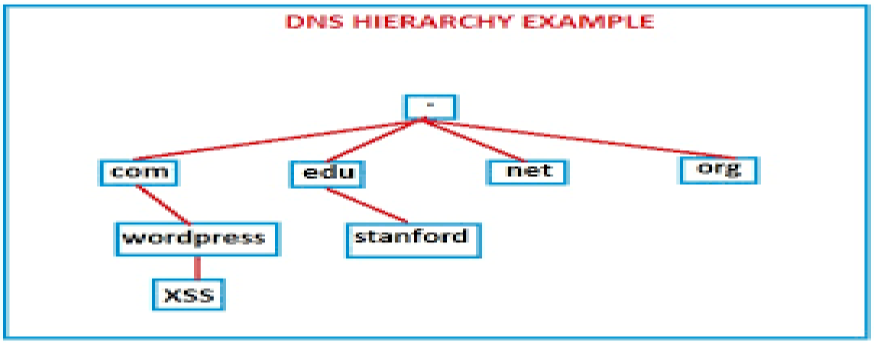
DNS SERVER:

1. Each device connected to internet is having a IP address which is used to identify it uniquely. But human being can’t remember it so a domain name is assigned.
2. DNS server translate domain name to IP address for communicating purpose.

Domain name of Google : https://www.google.com
IP address: 172.217.14.228

Domain name consists of top level domain and sub-domains under it.
In Google domain name: com is top-level domain.
Google is sub-domain under com.

Domain name assignment is hierarchical in nature or organized as inverted tree with root at the top.
Total 128 levels are possible.



Generic domain
Com –commercial organization
Gov- govt organization
Edu -educational organizations
Mil- military
Net- networking organization
Country specific domain
In- India
Ch- China

Us- US
Ca- Canada
Nz-   Newzeland
Pk-Pakistan
Jp- Japan

HTTP:

1. It is a **Application layer protocol** which is used to access information from www because every resource on www is in the form of html pages.
2. It uses TCP/IP protocol. (one TCP connection)
3. It is **request-response protocol** which uses **client and server model.**
4. Web browser acts as **client** and computer hosting a particular website will be **server**.
5. When we submit query it goes link **http request** and response comes as **http response**.
6. It is a **stateless protocol** because it doesn't require http server to retain any previous information about http client.

Diagram from notebook.

Different methods are used in http request packet:

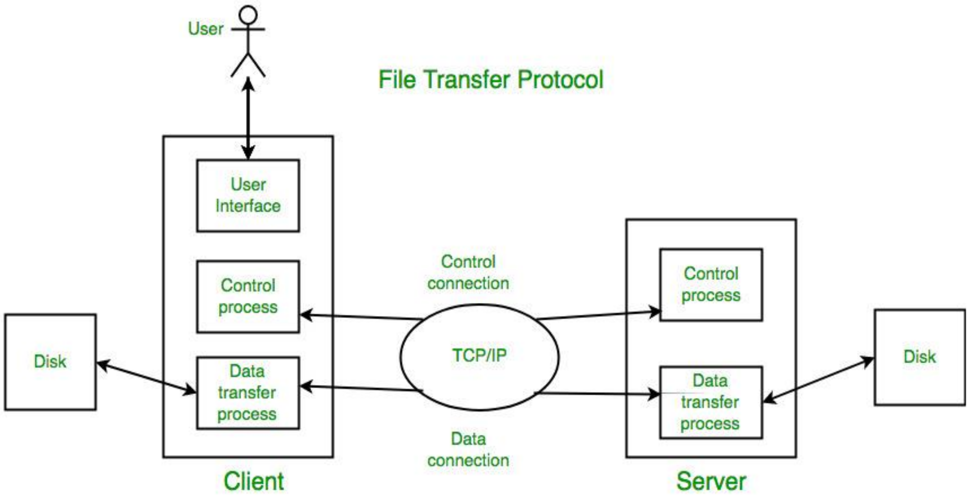
a) **Get method:** to get resource or output for particular query as message body of hhtp response packet. Here query goes as part of url.
b) **Head:** to get only header information of document of response of particular query.
c) **Post:** to submit information on to server. Here information is submitted as aprt of http request packet. So this method provides security.

HTTPS:
All working is like HTTP
Here 's' stands for secure, means information between browser and webserver is encrypted using transport layer security or using secure socket layer(SSL).

HTTPS=HTTP+Security using SSL

File Transfer Protocol (FTP):

1. It is a **appliaction layer protocol** used for downloading and uploading file from server connected through internet.
2. It uses **Client-server architecture.**
3. Here **2 TCP connections** are created one for data and other for control information.
4. Client and server both should run FTP software.
5. **Authentication** is done here using username and password.
6. It is **stateful protocol**.



Remote login:

1. Remote login refers to the ability to access a computer, such as a home computer or an office network computer, from a remote location.
2. This allows employees to work offsite, such as at home or in another location, while still having access to a distant computer or network, such as the office network.
3. Remote access can be set up using a local area network (LAN), wide area network (WAN).
4. To establish a remote connection, both the local machine and the remote computer/server must have remote-access software.

TELNET:

Telnet is protocol which helps a user to perform remote login. Through Telnet, an administrator or another user can access someone else's computer remotely.

On the Web, HTTP and FTP protocols allow you to request specific files from remote computers, but not to actually be logged on as a user of that computer.

With Telnet, you log on as a regular user to remote site computer.

Working of Telnet:

1. User login and invokes a telenet program.
2. Telnet client starts and make tcp/ip connection with telenet server on destination system.
3. Once connection is created, client accepts character from keyboard and passes to server and vice-versa.
4. Connection can be terminated by logoff or logout on the system prompt.

Telnet sends all messages in clear text and has no specific security mechanisms. Thus, in many applications and services, Telnet has been replaced by Secure Shell (SSH).

SSH:

1. SSH, also known as Secure Shell or Secure Socket Shell, is a network protocol that gives users a secure way to access a computer over an unsecured network.

2. Secure Shell provides strong **authentication and encrypted data communications** between two computers connecting over an open network such as the internet.

3. SSH is widely used by network administrators for managing systems and applications remotely, allowing them to log into another computer over a network, execute commands and move files from one computer to another.

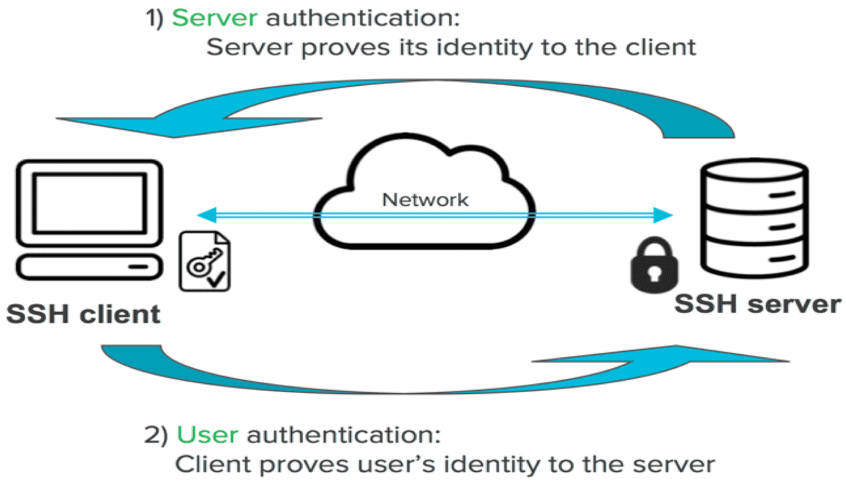
4. It uses **client-server model.**

5. It uses **public key cryptography.**

6. **Two public key pairs** for each connection: one for client and other for server.

7. SSH clients and servers can use a number of encryption methods, the mostly widely used being Advanced Encryption Standard (AES) and Blowfish.

8. It was designed to replace insecure terminal emulation using telenet, and it has replaced FTP also.


1) Server authentication:
Server proves its identity to the client
Network
SSH client
SSH server
2) User authentication:
Client proves user's identity to the server

SCP (secure copy protocol):

1. Secure copy (SCP) is a **file transfer protocol,** which helps in transferring computer files securely from a local host to a remote host. It works on the **Secure Shell (SSH)** protocol technique.

2. The SCP protocol is a file transfer network protocol, which supports encryption and authentication features.

3. It allows **client and server** to communicate using single TCP connection.

NFC:

1. It is a Short distance wireless technology to communicate using radio waves (within 4 cm).
2. NFC tags are used like QR code.

It works in 3 modes.

3. **Peer to peer**:
   2 mobiles are connected to share files and data.

4. **Reader/writer mode:**
   It reads NFC tag using electromagnetic induction method.
   It is up gradation of RFID tags.

5. **Card emulation mode:**
   Smart phone and payment terminal.
   Mobile phone acts like card or passive device that responds to signal given by payment machine.

6.

7. **Applications:**
   Information sharing
   Payment
   Information read using smart poster and business card having NFC tag.

VOIP

1. Digitized, compressed and fragmented and sent through IP.
2. Used for voice traffic (telephone calls and faxes)
3. It uses packet-switching
4. Session initiation protocol, is used for initiation, modification and termination of telephone calls.
5. It provides video conferencing, so that single person can communicate with multiple persons at a time.

Secure communication:

Only authorized persons are allowed to access information not third party.
Two schemes are used:

1. **Encoding :**
   Representing info to be shared using different code symbols. No key.

2. **Encryption:**
   Conversion of information from one format to other using algorithm and key.

Error Checking:

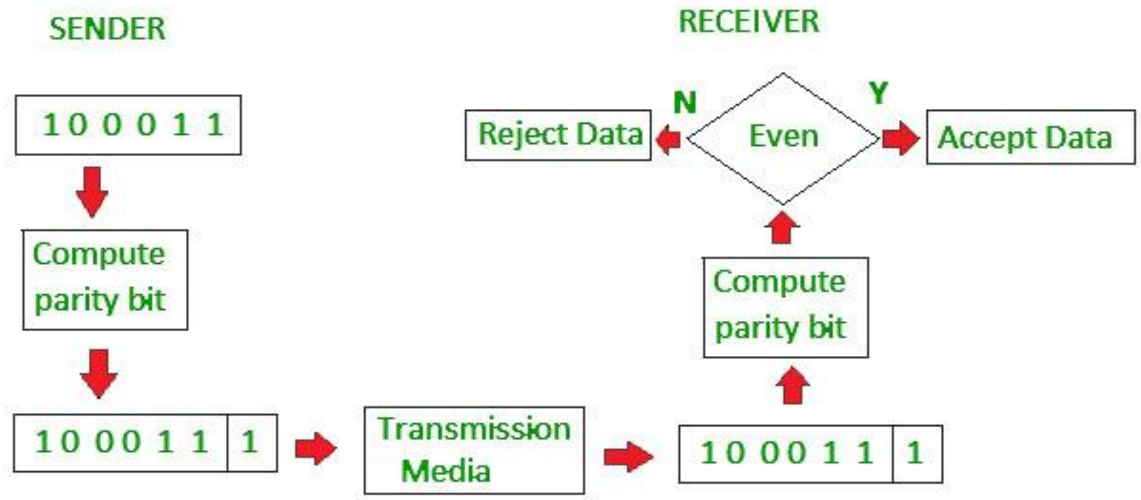
Error
A condition when the receiver's information does not matches with the sender's information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0.

Error-detecting codes which are additional data added to a given digital message to help us detect if any error has occurred during transmission of the message.

Some popular techniques for error detection are:

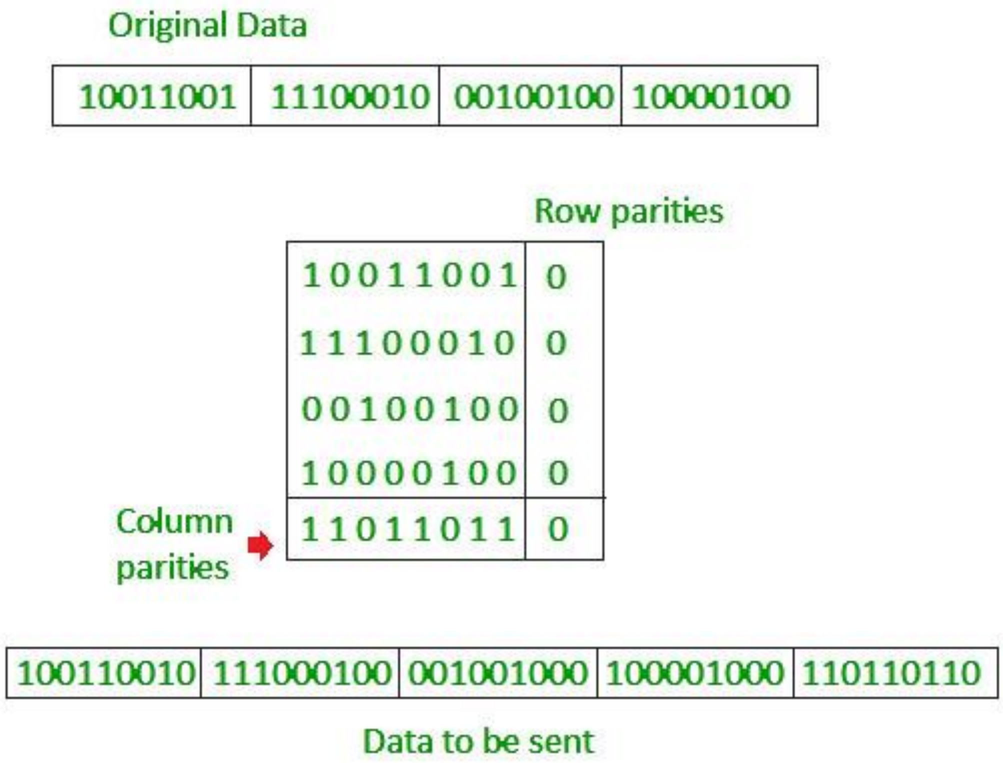
1. Simple Parity check
2.Two-dimensional Parity check
3. Checksum

Simple parity check:
If even parity is used, Sender calculates parity bit as 1 if no 1's in data are odd and as 0 if no. of 1's in data is even and appends that parity bit. This information will go through transmission medium then receiver check for even parity.



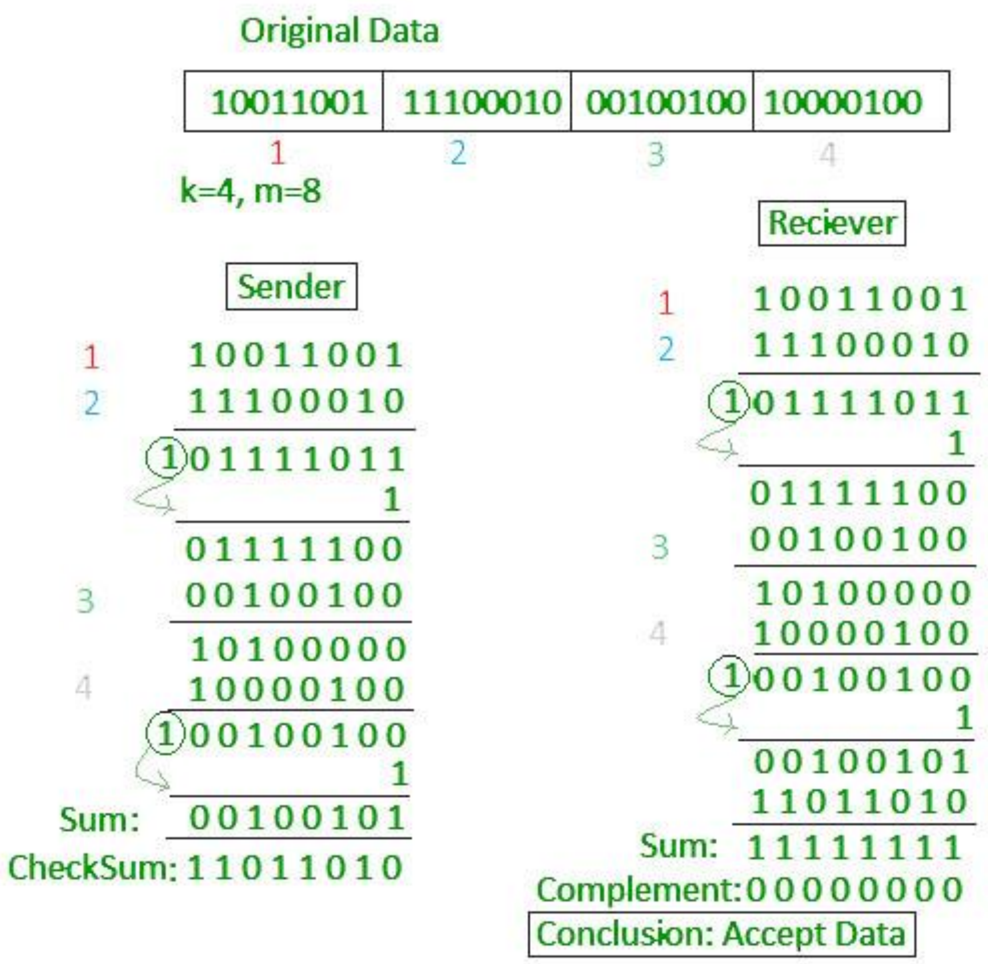
Two dimensional parity checks:

Here data is divided into equal size fragments and arranged in from of rows and columns then parity bits are calculated row-wise and column-wise and appended to data to transfer.



Checksum:

Here also data is divided into fixed size fragments and performed binary addition to calculate sum after adding all fragments, result value is complemented, this value is called checksum. It is added as error detecting code in data to be transferred.



Collision in wired and wireless system:

CSMA/CD: used in wired networks
CSMA/CA: used in wireless networks

EMAIL WORKING
SMTP
POP
IMAP

Read from notebook.