What are computer networks?

⇨ A computer network or data network is a telecommunications network which allows computers to exchange data. In computer networks, networked computing devices exchange data with each other using a data link. The connections between nodes are established using either cable media or wireless media. The best-known computer network is the Internet.

There are many types of computer networks, including the following:
i) **local-area networks (LANs):** The computers are geographically close together (that is, in the same building).

ii) **wide-area networks (WANs):** The computers are farther apart and are connected by telephone lines or radio waves.

iii) **campus-area networks (CANs):** The computers are within a limited geographic area, such as a campus or military base.

iv) **metropolitan-area networks MANs):** A data network designed for a town or city.

v) **home-area networks (HANs):** A network contained within a user's home that connects a person's digital devices.

Needs of Computer Networks :

Here are some of the ways a computer network can help wer business:

- **File sharing:** Have we ever needed to access a file stored on another computer? A network makes it easy for everyone to access the same file and prevents people from accidentally creating different versions.
- **Printer sharing:** If we use a computer, chances are we also use a printer. With a network, several computers can share the same printer. Although we might need a more expensive printer to handle the added workload, it's still cheaper to use a network printer than to connect a separate printer to every computer in wer office.
- **Communication and collaboration:** It's hard for people to work together if no one knows what anyone else is doing. A network allows employees to share files, view other people's work, and exchange ideas more efficiently. In a larger office, we can use e-mail and instant messaging tools to communicate quickly and to store messages for future reference.
- **Organization:** A variety of scheduling software is available that makes it possible to arrange meetings without constantly checking everyone's schedules. This software usually includes other helpful features, such as shared address books and to-do lists.
- **Remote access:** Having our own network allows greater mobility while maintaining the same level of productivity. With remote access in place, users are able to access the same files, data, and messages even when they're not in the office. This access can even be given to mobile handheld devices.
- **Data protection:** We should know by now that it's vital to back up our computer data regularly. A network makes it easier to back up all of our company's data on an offsite server, a set of tapes, CDs, or other backup systems. (Of course, another aspect of data

protection is data *security*. In our article, What Is a Firewall? we can read more about how a network can protect the data it transmits.)

Network Topology:

A Network Topology is the arrangement with which computer systems or network devices are connected to each other. Topologies may define both physical and logical aspect of the network. Both logical and physical topologies could be same or different in a same network.

Point-to-Point:

Point-to-point networks contains exactly two hosts such as computer, switches or routers, servers connected back to back using a single piece of cable. Often, the receiving end of one host is connected to sending end of the other and vice-versa.

If the hosts are connected point-to-point logically, then may have multiple intermediate devices. But the end hosts are unaware of underlying network and see each other as if they are connected directly.

Bus Topology:

In case of Bus topology, all devices share single communication line or cable.Bus topology may have problem while multiple hosts sending data at the same time. Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue. It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning.

Both ends of the shared channel have line terminator. The data is sent in only one direction and as soon as it reaches the extreme end, the terminator removes the data from the line.

Star Topology

All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and hub. The hub device can be any of the following:

- Layer-1 device such as hub or repeater
- Layer-2 device such as switch or bridge
- Layer-3 device such as router or gateway

As in Bus topology, hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails. Every communication between hosts, takes place through only the hub.Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.

Ring Topology

In ring topology, each host machine connects to exactly two other machines, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. To connect one more host in the existing structure, the administrator may need only one more extra cable.

Failure of any host results in failure of the whole ring.Thus, every connection in the ring is a point of failure. There are methods which employ one more backup ring.

Mesh Topology

In this type of topology, a host is connected to one or multiple hosts.This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only.

Hosts in Mesh topology also work as relay for other hosts which do not have direct point-to-point links. Mesh technology comes into two types:

- **Full Mesh**: All hosts have a point-to-point connection to every other host in the network. Thus for every new host n(n-1)/2 connections are required. It provides the most reliable network structure among all network topologies.
- **Partially Mesh**: Not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrarily fashion. This topology exists where we need to provide reliability to some hosts out of all.

Tree Topology

Also known as Hierarchical Topology, this is the most common form of network topology in use presently.This topology imitates as extended Star topology and inherits properties of bus topology.

This topology divides the network in to multiple levels/layers of network. Mainly in LANs, a network is bifurcated into three types of network devices. The lowermost is access-layer where computers are attached. The middle layer is known as distribution layer, which works as mediator between upper layer and lower layer. The highest layer is known as core layer, and is central point of the network, i.e. root of the tree from which all nodes fork.

All neighboring hosts have point-to-point connection between them.Similar to the Bus topology, if the root goes down, then the entire network suffers even.though it is not the single point of failure. Every connection serves as point of failure, failing of which divides the network into unreachable segment.

Daisy Chain

This topology connects all the hosts in a linear fashion. Similar to Ring topology, all hosts are connected to two hosts only, except the end hosts.Means, if the end hosts in daisy chain are connected then it represents Ring topology.

Each link in daisy chain topology represents single point of failure. Every link failure splits the network into two segments.Every intermediate host works as relay for its immediate hosts.

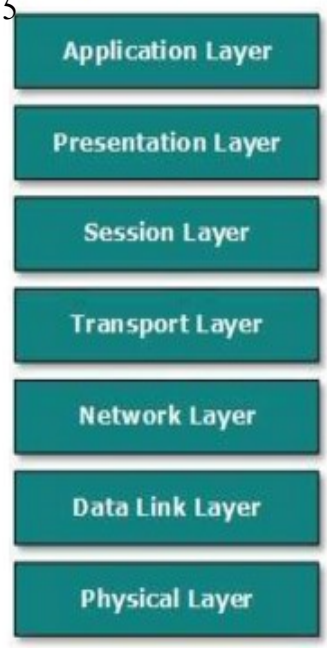
Hybrid Topology

A network structure whose design contains more than one topology is said to be hybrid topology. Hybrid topology inherits merits and demerits of all the incorporating topologies.

The above picture represents an arbitrarily hybrid topology. The combining topologies may contain attributes of Star, Ring, Bus, and Daisy-chain topologies. Most WANs are connected by means of Dual-Ring topology and networks connected to them are mostly Star topology networks. Internet is the best example of largest Hybrid topology.

OSI Model :

Open System Interconnect is an open standard for all communication systems. OSI model is established by International Standard Organization (ISO). This model has seven layers:



- **Application Layer**: This layer is responsible for providing interface to the application user. This layer encompasses protocols which directly interact with the user.
- **Presentation Layer**: This layer defines how data in the native format of remote host should be presented in the native format of host.
- **Session Layer**: This layer maintains sessions between remote hosts. For example, once user/password authentication is done, the remote host maintains this session for a while and does not ask for authentication again in that time span.
- **Transport Layer**: This layer is responsible for end-to-end delivery between hosts.
- **Network Layer**: This layer is responsible for address assignment and uniquely addressing hosts in a network.
- **Data Link Layer**: This layer is responsible for reading and writing data from and onto the line. Link errors are detected at this layer.
- **Physical Layer**: This layer defines the hardware, cabling wiring, power output, pulse rate etc.

Internet Model

Internet uses TCP/IP protocol suite, also known as Internet suite. This defines Internet Model which contains four layered architecture. OSI Model is general communication model but Internet Model is what the internet uses for all its communication. The internet is independent of its underlying network architecture so is its Model. This model has the following layers:

- **Application Layer**: This layer defines the protocol which enables user to interact with the network.For example, FTP, HTTP etc.
- **Transport Layer**: This layer defines how data should flow between hosts. Major protocol at this

layer is Transmission Control Protocol (TCP). This layer ensures data delivered between hosts is in-order and is responsible for end-to-end delivery.

- **Internet Layer**: Internet Protocol (IP) works on this layer. This layer facilitates host addressing and recognition. This layer defines routing.
- **Link Layer**: This layer provides mechanism of sending and receiving actual data.Unlike its OSI Model counterpart, this layer is independent of underlying network architecture and hardware.

Differences between OSI Reference Model and TCP/IP Reference Model:

Following are some major differences between OSI Reference Model and TCP/IP Reference Model, with diagrammatic comparison below.

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	5. TCP/IP model is, in a way implementation of the OSI model.
6. Network layer of OSI model provides both connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.
7. OSI model has a problem of fitting the protocols into the model.	7. TCP/IP model does not fit any protocol

8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.
9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	9. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
10. It has 7 layers	10. It has 4 layers

FDDI:

Fiber Distributed Data Interface (**FDDI**) is a standard for data transmission in a local area network. It uses optical fiber as its standard underlying physical medium, although it was also later specified to use copper cable, in which case it may be called **CDDI** (Copper Distributed Data Interface), standardized as **TP-PMD** (Twisted-Pair Physical Medium-Dependent), also referred to as TP-DDI (Twisted-Pair Distributed Data Interface).

FDDI provides a 100 Mbit/s optical standard for data transmission in local area network that can extend in range up to 200 kilometers (120 mi). Although FDDI logical topology is a ring-based token network, it did not use the IEEE 802.5 token ring protocol as its basis; instead, its protocol was derived from the IEEE 802.4 token bus *timed token* protocol. In addition to covering large geographical areas, FDDI local area networks can support thousands of users. FDDI offers both a Dual-Attached Station (DAS), counter-rotating token ring topology and a Single-Attached Station (SAS), token bus passing ring topology.

ATM:

Asynchronous transfer mode (ATM) is a switching technique used by telecommunication networks that uses asynchronous time-division multiplexing to encode data into small, fixed-sized cells. This is different from Ethernet or Internet, which use variable packet sizes for data or frames. ATM is the core protocol used over the synchronous optical network (SONET) backbone of the integrated digital services network (ISDN).

Token ring :

Token ring local area network (LAN) technology is a communications protocol for local area networks. It uses a special three-byte frame called a "token" that travels around a logical "ring" of workstations or servers. This token passing is a channel access method providing fair access for all stations, and eliminating the collisions of contention-based access methods.

Introduced by IBM in 1984, it was then standardized with protocol **IEEE 802.5** and was fairly successful, particularly in corporate environments, but gradually eclipsed by the later versions of Ethernet.

Introduction to FTP:

File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections.

FTP is a client-server protocol that relies on two communications channels between client and server: a command channel for controlling the conversation and a data channel for transmitting file content. Clients initiate conversations with servers by requesting to download a file. Using FTP, a client can upload, download, delete, rename, move and copy files on a server. A user typically needs to log on to the FTP server, although some servers make some or all of their content available without login, also known as anonymous FTP.

or

FTP stands for "file transfer protocol." FTP powers one of the fundamental Internet functions and is the prescribed method for the transfer of files between computers. It is also the easiest and most secure way to exchange files over the Internet.

Basic Terminologies in FTP

FTP Server

Ftp Server is basically a computer or server machine that receives requests form the clients and transfer requests. FTP server generally uses FTP commands to communicate with the clients.

FTP Client

The FTP client is the client side software that is designed and responsible for the transmission of files back and forth between the server and the client over the network. The FTP client software has to be installed at the client side computer and can be only used with a live internet connection.

The FTP client is the actual computer that initiates the transfer process by sending request to the server machine i.e. the FTP server. Once the FTP server receives the request it verifies it and the FTP client is indicated with a positive acknowledgment. Once the acknowledgment is received, the FTP client can download or upload from or to the server. File transfers are as easy as drag and drop operation from one pane to the other or it can also be done by highlighting a file and pressing one of the navigation arrows located inbetween the panes.

FTP client software include additional features like multiple file transfer the auto re get or resuming feature, queuing and scheduling feature, Search and synchronization facility. A scripting utility is also available for advanced users.

Anonymous FTP

An anonymous FTP means that a FTP client can get connected to the server with little or no qualification or verification. To be more precise there will be no prompting of username and password for an anonymous FTP. Many of the sites featuring freely downloadable data uses this option to enable the clients to download form their site.

Nowadays most of the FTP hosts provides that provides FTP services also provide additional facilities to use anonymous FTP access as well. In order to do so the client has to enter either “anonymous” or “ftp” when the FTP server or host is prompting for an username. Under this understanding, users do not need a description or account on the host. Though users are prompted for their email in place of password no actual verification process takes place.

In case of modern FTP clients, the clients typically hide the anonymous login process from the user. These clients send a dummy data as the password when it is prompted. This happens because the user’s email id is not known to the application. Here are some of the FTP user agents and their dummy specifications as passwords for anonymous login.

FTP host

An FTP host is a service that hosts or that contains a FTP site. Hence instead of using the FTP server one can logon to the FTP site and perform the uploading and downloading operations

inside this hosted area. The process of hosting can cost a bit depending on the memory and the limitations.

FTP Site
FTP site is a collection of files that can be hosted using a FTP host. The hosted data can be accessed using a username and a password. Many of the stored data are available only on the hosted servers. The other data may be located in the server owned by the creator of the data.

FTP Proxy
The FTP proxy is much similar to a gate keeper. All the requests send to the FTP server goes through the proxy first and then the request gets redirected to the server.

FTP SERVER :

An FTP server is a software.html application running the File Transfer Protocol (FTP), which is the protocol for exchanging files over the Internet.

FTP Authentication :

FTP Authentication feature page to configure the authentication methods that FTP clients can use to gain access to your content. You can sort this list by name, status, or type by clicking the appropriate column heading. By using the Group by drop-down list, you can also group authentication features by type or status.
By default, no authentication methods are enabled. Enable an authentication method if you want to allow FTP users to access your content. There are two types of authentication methods: Built-In and Custom.

- Built-In authentication methods are integral parts of the FTP server. These authentication methods can be enabled or disabled, but cannot be removed from the FTP server.
- Custom authentication methods are implemented through an installable component. These authentication methods can be enabled or disabled, and they can be added to or removed from the FTP server.

GUI based ftp client:

An FTP client is a software program with a GUI (graphical user interface) that provides various options to help manage the process of transferring files.

Overview of internet security:

Internet security is a branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole. Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information leading to a high risk of intrusionor fraud, such as phishing. Different methods have been used to protect the transfer of data, including encryption and from-the-ground-up engineering.

Firewall

A firewall is a network security system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of

both. Network firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Understanding the need for information security.

There is a rising, and probably essential, need, for all companies no matter what size they are, to understand information security.

The mix of company change/growth and the external threat landscape needs managers at all levels to take on a proactive information security methods that will protect your company from Internet threats.

And that means initiatives are required to be taken to provide more secure technology solutions.

These initiatives should include information security strategies and plans that apply security requirements and address known identified risks.

And what all that means is, and being as concise as possible, having recommendations and implementing changes to company policies, standards, procedures and communications to

But wait, I hear you saying what was that you were saying about taking on “proactive information security methods?” I will come on to Internet security management/countermeasures in a later blog.

I hope that you find the concepts that I have described so far relatively easy to understand.

Internet security management support.

Easy to understand or not, one of the major challenges facing senior management when it comes to Internet security management is finding someone to support the concepts and can implement your information security strategies.

And even if you can find someone, can you afford them?

Take my domain industry, automotive distribution. Most dealers, unless they belong to a large multi franchise, multi branch chain of dealers suffice with an I.T. supervisor, and that person probably also doubles up in another capacity in the accounts department.

Can this person realistically be expected to also take on Internet security management concepts, implement them and also keep up to date with the ever changing external threat landscape? I think not.

The Dealer Principal could turn to external consultants to provide advice and guidance and consultancy. But have you tried to hire any type of consultant for any length of time recently? The vast majority are simply too expensive for most dealers and almost all small to medium sized businesses.

JavaScript :
JavaScript is a high-level, dynamic, untyped, and interpreted programming language. It has been standardized in the ECMAScript language specification. Alongside HTML and CSS, JavaScript is one of the three core technologies of World Wide Web content production; the majority of websites employ it, and all modern Web browsers support it without the need for plug-

ins. JavaScript is prototype-based with first-class functions, making it a multi-paradigm language, supporting object-oriented, imperative, and functional programming styles. It has an API for working with text, arrays, dates and regular expressions, but does not include any I/O, such as networking, storage, or graphics facilities, relying for these upon the host environment in which it is embedded.
JavaScript is also used in environments that are not Web-based, such as PDF documents, site-specific browsers, and desktop widgets. Newer and faster JavaScript virtual machines (VMs) and platforms built upon them have also increased the popularity of JavaScript for server-side Web applications. On the client side, developers have traditionally implemented JavaScript as an interpreted language, but more recent browsers perform just-in-time compilation. Programmers also use JavaScript in video-game development, in crafting desktop and mobile applications, and in server-side network programming with run-time environments such as Node.js.

JavaScript provides different data types :

JavaScript provides different **data types** to hold different types of values. There are two types of data types in JavaScript.

1. Primitive data type
2. Non-primitive (reference) data type

JavaScript is a **dynamic type language**, means you don't need to specify type of the variable because it is dynamically used by JavaScript engine. You need to use **var** here to specify the data type. It can hold any type of values such as numbers, strings etc. For example:

```
1.  var a=40;//holding number
2.  var b="Rahul";//holding string
```

JavaScript primitive data types:

There are five types of primitive data types in JavaScript. They are as follows:

Data Type	Description
String	represents sequence of characters e.g. "hello"
Number	represents numeric values e.g. 100
Boolean	represents boolean value either false or true
Undefined	represents undefined value
Null	represents null i.e. no value at all

JavaScript non-primitive data types :

The non-primitive data types are as follows:

Data Type	Description
Object	represents instance through which we can access members
Array	represents group of similar values
RegExp	represents regular expression

PHP:

PHP is a server-side scripting language designed primarily for web development but also used as a general-purpose programming language. Originally created by Rasmus Lerdorf in 1994, the PHP reference implementation is now produced by The PHP Development Team. PHP originally stood for *Personal Home Page*, but it now stands for the recursive acronym *PHP: Hypertext Preprocessor*.

PHP code may be embedded into HTML code, or it can be used in combination with various web template systems, web content management systems and web frameworks. PHP code is usually processed by a PHP interpreter implemented as a module in the web server or as a Common Gateway Interface (CGI) executable. The web server combines the results of the interpreted and executed PHP code, which may be any type of data, including images, with the generated web page. PHP code may also be executed with a command-line interface (CLI) and can be used to implement standalone graphical applications.[8]

The standard PHP interpreter, powered by the Zend Engine, is free software released under the PHP License. PHP has been widely ported and can be deployed on most web servers on almost every operating system and platform, free of charge.

The PHP language evolved without a written formal specification or standard until 2014, leaving the canonical PHP interpreter as a *de facto* standard. Since 2014 work has gone on to create a formal PHP specification.

Basic programming principles:

Object Oriented Programming, or OOP, refers to the method of programming that invokes the use of classes to organize the data and structure of an application. With PHP, OOP started to become feasible with the release of PHP 4, but really came into its own with PHP 5. Now, as the world awaits the release of PHP 6 we await another great leap in the evolution of PHP OOP.

While a large number of programmers shun the use of OOP as a programming paradigm, many more are seeing the advantages of OOP every day. Objects are here to stay - and if you don't like them yet, give it a chance: there comes a time in every developers career when he makes the evolutionary step up to OOP.