Web Design & Internet Development – Introductory Concepts

Jahangir Alam
University Women's Polytechnic
AMU Aligarh (India) - 202002

Computer Network and Networking

- A set of autonomous computers connected together to share resources (Data, Information, Hardware, and Software). By autonomous we mean that no computer can be forcibly start/ stop by any other computer on the network.
- Another definition is – A group of computers and other devices connected together is called a network and the concept of connected computers sharing information and resources, is called networking. Each device on the network is referred to as node.
- We can not only share the information on a network but can also control the way it is shared. For example a company's financial statement is a vital document and can not be shared with everyone. It must be shared with some confidential personnel.

Why Networks???

Networks are all about:

- Sharing Resources
- Preserving Information
- Protecting Information

Sharing Resources on Networks

- Resource sharing means sharing H/W and S/W.
- Hardware Resource Sharing: Networked Computers can share:
  - Printers, Fax Modem, Scanners, Hard Disks, Floppy Disks, CD-ROMS, Tape Backup Units, Plotters, Any device that can be attached to the Network.
- Software Resource Sharing:
  - Software resources can be used more effectively over networks. With stand alone computers the software used on the computers must be present on each computer's hard disk, whether or not that computer is used at that moment for the task the software performs.
  - For a large number of stand alone computers S/W cost can become more than expectations. It is also difficult and time consuming to install and configure the S/W individually on each computer.

- With a network we can install and configure the software on one computer (server) and can share it with other computers on the network. We can also control the access to that S/W.
- Not all S/W will use a network even if one is installed on the server. Different S/W packages have different restrictions on how the software can legally be used on a network. We must check the S/W documentation to check what features the S/W provides in a networked environment.

Preserving Information

- Besides, information and resource sharing a network allows information to be backed up to a central location.
- Important information can be lost by mistake or accidentally when a stand alone computer has no backup means.
- It is also difficult to maintain regular backups on a number of stand alone computers.
- In a networked environment when we take backup at a central location from all computers, we have one place

Protecting Information

- With stand alone computer, access to the computer means access to the information on that computer.
- Networks provide an additional layer of security by means of passwords.
- We can give each network user a different account name and password, allowing the network server to distinguish among those who need access to have it and protecting the information from tampering by those who do not.

Roles for a Computer on a Network

- A Computer can have one of the following three roles to play on a network:
  - Client: A Computer which uses but don't provide Networking Resources. They are also known as nodes or workstations (only when they run UNIX or its flavour)
  - Server: A computer which provides network resources.
  - Peer: A computer which provides as well as uses resources.
- Often the role of a computer on a Network can also be determined by the Operating System it is using:
  - Clients run client operating system such as MS-DOS, OS/2 etc.

- Peers run peer operating system such as Win 95/ Win 98/ Win NT workstation/ Win 2000 Professional/ Win XP (Professional and Home Editions)/ Win Vista (Home & Professional Editions) etc.
- Servers run Network Operating Systems such as Unix/ Linux/ HP-UX/ AIX/ Novell Netware/ Solaries/ Win NT/ Win 2000 Server/ Win 2000 Advanced Server/ Win 2000 Data Centre Server etc.

- Note that simply by looking at the Operating System we can't decide whether a computer on a Network is a Client or a Peer or a Server as almost all server operating systems can also be used as client OS.
- So a straight forward method to identify the role of a computer on a network is to identify its use on the network

Classification of Networks

Traditionally networks are classified as:

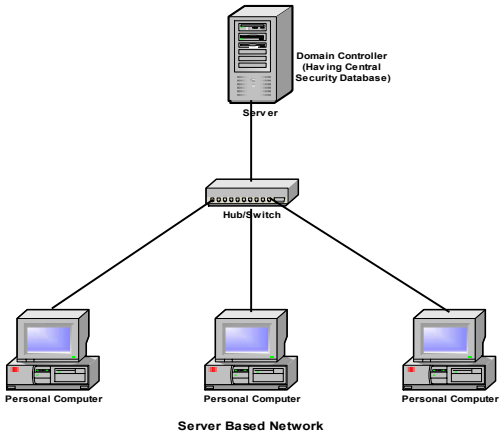
- LAN (Local Area Network) is a numbers of computers connected to each other by a cable or otherwise in a single location usually in a building or in a University campus.
- MAN (Metropolitan Area Network) is a numbers of computers connected to each other within a city.
- WAN (Wide Are Network) are the set of connecting links between LANs and WANs.

Based on the roles of the computers attached to them networks can be classified as:

- Server Based or Client/ Server Networks.
- Peer-to-Peer Networks.
- Hybrid Networks.

Server Based Networks

- Are identified by the presence of server (s) on the network.
- Server provides security and administration of the network.
- Client/ Server networks divide processing tasks between client and server. Clients (referred to as front ends) request services such as file storage and printing, and servers (referred to as back ends) deliver them.
- Server computers are typically more powerful than client computers or are optimized to function as servers.
- Windows NT/ 200X based networks are organized into domains.



Server Based Network

- A domain is a logical grouping of network computers that share a central directory database.
- A directory database contains user accounts and security information for the domain. In a domain the directory resides on the computers that are configured as domain controllers.
- A domain controller is a server that manages all security related user/ domain interactions and centralizes administration.

Advantages of Server Based Networks

- Strong central security.
- Centralized storage and backup.
- Ability to share resources.
- Optimized dedicated server which are faster than peers when sharing resources.
- Easy manageability of large number of users.

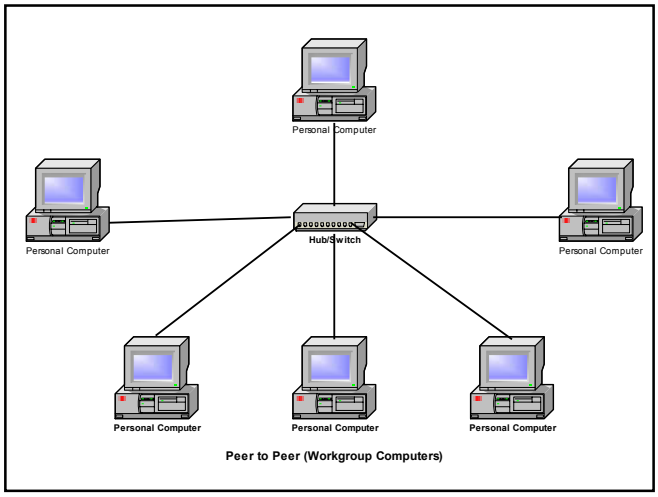
Disadvantages of Server Based Networks

- Expensive dedicated servers.
- Expensive Network Operating System and Client Licenses.
- A dedicated network administrator.

Peer Networks

- There are no servers on a peer network.
- Are defined by no central control over the network.
- Users simply share resources.
- Peer networks are organized into workgroups.
- A workgroup is a logical grouping of networked computers that share resources (and strictly not the security information).
- Each Windows (server or client flavour) computer in the workgroup maintains a local security database which contains a list of user accounts and resource security information for that computer.
- As each computer in the workgroup maintains a local security database, the administration of user accounts and resource security is decentralized.

- A user must have a user account on each computer that the user needs to access.
- Any changes to the user account information such as changing a password or adding new accounts must be made on each computer.
- As already discussed, access to individual resources can be controlled if the user who share the resource requires a password to access.
- Since there is no central security trust users will have to know the individual passwords for each resource we wish to access. This can be quite inconvenient.
- Peers are also not optimized to share resources. When a number of users are accessing the resources on a peer, they notice significantly degraded performance.



Advantages of Peer Based Networks

- No extra investment on server.
- Easy Setup.
- No network administrator required.
- Ability of users to control the share of resources.
- Convenient for limited number of computers in close proximity.

Disadvantages of Peer Based Networks

- Additional load on computers because of resource sharing.
- Inability of handling large networks.
- Lack of central organization which can make data hard to find.
- Requirement that users themselves administer the network.
- Weak and insecure security.

- They generally have licensing limitations that prevent more than a small number of users from simultaneously accessing resources.

Hybrid Networks

- Hybrid computers have all types of computers operating on them and generally have active domains and workgroups.
- It means that while most shared resources are located on servers, users still have access to any resources being shared by the peers in their workgroup.
- It also means that network users don't have to logon to the domain controller to access workgroup resources being shared by peers.
- If users log on to the network with proper username and password they are eligible to enjoy "all shared" resources either they lie with the domain controllers or with the peers.
- If users don't log on the network with proper username and password they are eligible to enjoy the resources contributed by the peers.

Advantages of Hybrid Networks

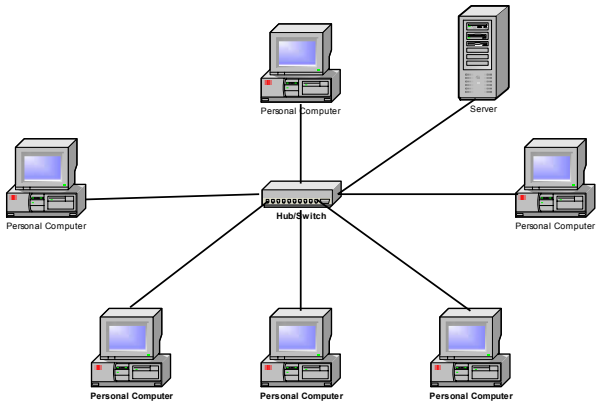
- All advantages of Server based networks.
- All advantages of Peer Networks.

Disadvantages of Hybrid Networks

- All disadvantages of Server Based and Peer Networks.

Topics to be Covered

- What is Internet.
- Protocols, ISO OSI Model, DOD Model etc.
- Getting Connected to Internet
- Types of Internet Accounts
- Configuring Windows for Internet – Modems etc.



Hybrid Network (Some Users Can't Access the Domain Resources)

What is Internet?

- Internet is a global network of networks.
- When large networks are built, interconnecting small networks, one should have as the main goal – interoperability.
- By interoperability we mean the ability of Hardware and Software of multiple machines from multiple vendors to communicate and operate together meaningfully.
- This is achieved to a great extent by a World Wide Computer Network known as Internet.
- Internet is also defined as a collection of packet switched networks operating on a protocol (a term we shall discuss shortly) known as TCP/IP.

- Internet is basically a shared network of government agencies, educational institutions, private organizations, and individuals from over a hundred nations. No one owns the Internet and anyone can have access to it. Its user are increasing in number everyday and every hour.
- The US has begun to put its weight behind the development of the National Information Infrastructure (better known as information superhighway).
- The stated goals are to connect networks through "superhighways" with data rates higher than several Gbps.

Intranet and Intraware

- A local area network (LAN) that uses internet like services is called an Intranet. In other ways we can say that any LAN operating on TCP/IP is an Intranet.
- Intraware is a Network Operating System from Novell to incorporate Internet on Novell's LAN. Novell LANs used IPX/ SPX protocols but with the release of Intraware Novell LANs had the support for TCP/IP.

Evolution of Internet

- The US Department of Defense (DOD) was an early supporter of the much of the research into advanced computing and networking.
- In 1960s the US Military relied on Computer Technology. So, the advances in that area were of critical importance. A network that could be shutdown by the malfunction of a single computer or node was highly undesirable and so the military wanted to develop a network that could remain in service even if one or many of computers on the network didn't work.
- Around 1960 the ARPA (Advanced Research Project Agency) – a part of the DOD, setup the first steps for what the world today knows as Internet. The goal of agency was to design a computer network with following features:
  1. The network should be able to run even if many of the computers or the connections between them fail.
  2. To accommodate the many different types of computers coming into the market, the DOD wanted dissimilar computers to be able to exchange the information smoothly.
  3. It had to be a Network of Networks.

  4. Only one computer on the network had to be connected directly to this network and every other computer on that network would be on this network.
- The above goals were implemented as ARPANET (Advanced Research Project Agency Network) and are still part of today's Internet. Soon after the inception of ARPANET, military computers and educational institutions were given access to this Network.
- In the 1980s it was opened for commercial use.

Network Protocols

- Protocols means a set of rules and regulations based on which two devices communicate.
- A simple example of a protocol from the kingdom of human communication is the different ways of greeting people.
- Should you bow, shake hands or hug to the person you are greeting? It depends on where you are and whom you are greeting. If you make a mistake, you could be understood.
- Although in the data communication world protocols are more complex and precise, the same idea holds.
- For example, a protocol may define the shape of a packet that will be transmitted across the network, as well as all the fields within the packet and how they should be interpreted.
- Obviously both the sender and receiver must agree on the exact way the packet should be formatted in order for communication to occur.
- Clearly, to communicate smoothly the devices must have at least one protocol as common protocol.

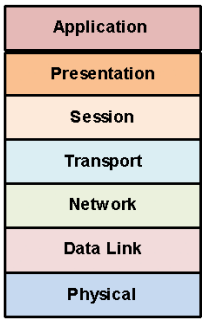
- A protocol suit is a group of protocols that evolved together, whether created by the same company as IPX/ SPX or used in the same environment such as the Internet. Following are some examples of Protocols Suits:
  - **NetWare IPX/SPX** – Novell's proprietary protocol suit.
  - **TCP/IP** – The nonproprietary protocols suit that make the Internet.
  - **AppleTalk** – Apple Computer's proprietary protocols which began with the Macintosh.
  - **DNA** – Digital Equipment Corporation's proprietary protocol suit which has evolved from a mainframe-centric environment to OSI compliance. DECnet is an implementation of DNA.
  - **SNA** – IBM's proprietary protocol suit, based on the System Network Architecture (SNA) model, the grandfather of data communications technology and inspiration for the OSI model.

Question????

- What is your opinion about protocols? Are they Hardware or Software?

The ISO – OSI Model (A Brief Overview)

- International Standards Organization (Estd. 1947) is a multinational body dedicated to worldwide agreement on International Standards.
- An ISO standards that covers all aspects of network communications is the Open System Interconnection (OSI) model.
- An Open System is a model that allows any two different systems to communicate regardless of their underlying architectures.
- The purpose of OSI model is to open communication between different systems without requiring changes to the logic of underlying hardware and software.
- The OSI model is not a protocol. It is a model for understanding and designing a network architecture that is flexible, robust and interoperable.



ISO - OSI Model

A famous mnemonic to help people remember the OSI layers from top is:

"All People Seem To Need Data Processing"

NOTE:

- Refer to A.S Tanenbaum for an in depth understanding of the functions of OSI Layers.
- ISO OSI is just a framework for designing networks. No protocols suit has ever been developed around this framework till date. However, the existing protocols suit may roughly be fitted into this framework.
- In the next section we shall discuss the TCP/IP or Internet protocols suit in detail. We will roughly fit this suit into ISO OSI framework and will briefly discuss the several protocols available at different layers.
- Then we will study the Internet Application Layer Protocols in detal.

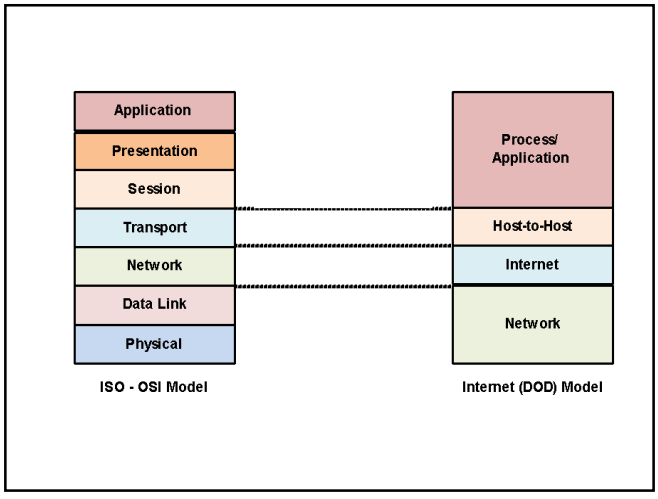
- It is a layered framework for design of network systems that allows communication across all types of computer systems.
- It consists of seven separate but related layers each of which defines a segment of the process of moving information across a network.
- Understanding the fundamentals of OSI model provides a solid basis for exploration of data communication.

Question: We've just studied that OSI is not a protocol, then what Protocols are and how do they differ from network models?

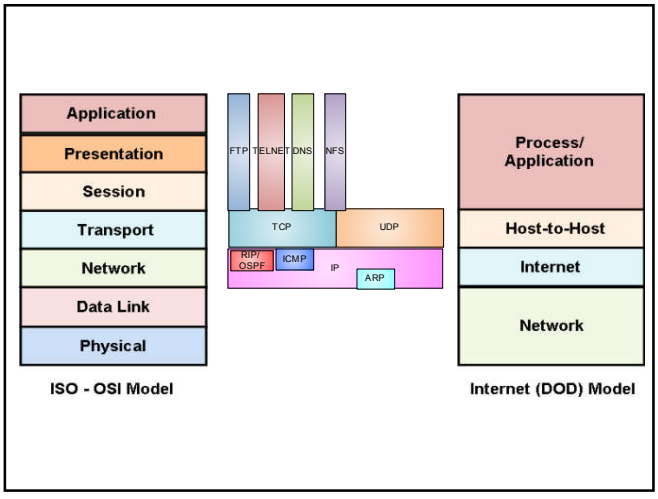
Internet Protocols (TCP/IP Protocols Suit)

- The Internet Protocol suit was developed along with its name sake – the Internet.
- The protocols that make up the Internet protocols suit, the best known being TCP/IP (Transmission Control Protocol/ Internet Protocol), have become de facto standards because of the success of Internet. The entire protocols suit is referred to as TCP/IP.
- The Internet Protocol suit is unique in that it is made up of nonproprietary protocols. This means that they do not belong to any one company and the technology is available to anyone who wishes to use it.
- As a result the Internet Protocol Suit is supported by the widest variety of vendors.

- The suit was developed about ten years before the OSI model was defined and can therefore be roughly mapped into it.
- The suit was defined according to its own model, known as the Internet or DOD model.
- The DOD model layers (shown in the figure on next page) and the OSI model layers they correspond to are as follows:
  - The Network Access Layer corresponds to the physical and data link layers.
  - The Internet Layer corresponds to the OSI network layer. Protocols at this layer are concerned with transporting packets through the internetwork. The main Internet Layer Protocol is IP.
  - The host-to-host layer corresponds roughly to the OSI transport layer. Protocols at this layer communicate with the peer processes in other hosts or networked devices. An example of a host-to-host protocol is TCP.



- The process/ application layer corresponds to the OSI session, presentation and application layers. Protocols at this layer provide application services on the network. Examples of protocols at this layer are Telnet, FTP, DNS etc.
- The Internet protocols do not cover the lower two layers of the OSI model. This is because the designers of TCP/ IP used existing physical and data link standards to make TCP/ IP hardware independent. As a result the protocols of Internet Suit are widely used to connect heterogeneous systems and are classified as Internet Middle Layer Protocols and Internet Upper Layer Protocols.
- The implementation of different layers of Internet Protocols Suit is shown in following figure.



Internet Middle-Layer Protocols
1.IP (Internet Protocol)

- As we know that protocols at the OSI model's network and transport layers are concerned with transporting packets across the inter-network. TCP/ IP uses two types of addresses for network
  - Hardware or Physical addresses are used by the physical and data link layers. Theses addresses are encoded into network card of each device on the network.
  - IP addresses provide logical addressing. They are the unique addresses assigned by the administrator according to certain guidelines. They are expressed in four part dotted decimal notation like 10.1.1.100.
- IP works at the network layer. The functions it handles and methods it uses are as follows:

- For addressing, IP uses logical Network Addresses
- For, switching purposes it uses the packet switching method.
- For route selection, it uses the dynamic routing method.
- For connection services IP provides error control.

- We shall discuss IP addressing in detail.

Address Resolution Protocol (ARP) and Reverse ARP (RARP)

- Associates an IP address with the physical address.
- On a typical local network such as LAN, each device on a link is identified by a physical address usually imprinted on the NIC.
- Physical addresses have local jurisdiction and can be changed easily. If NIC on a particular machine fails the physical address changes. The IP addresses on the other hand have universal jurisdiction and can't be changed.
- ARP is used to find the physical address of the node when its IP address is known.
- Anytime a host or a router needs to find the physical address of another host on its network, it formats an ARP query packet that has the target host's IP address and broadcasts it on the network.

- All host on the network receive the packet but only the target host recognizes its IP address and sends back its physical address.
- The Reverse ARP (RARP) allows a host to discover its IP address when it knows only its physical address.

ICMP (Internet Control Message Protocol)

- Is used with IP to augment error-handling and control procedures. It works at the network layer and is concerned with connection services.
- ICMP detects error conditions such as internetwork congestion and downed links and notifies IP and upper layer protocols so packets can be routed around problem areas.
- The famous ping command is actually an implementation of ICMP.

RIP and OSPF

- Routing information protocol (RIP) is a Network Layer Protocol.
- It periodically broadcasts routing tables across internetwork and learns the new routs. RIP causes bottlenecks in WANs and is thus being replaced by OSPF.
- OSPF (Open Shortest Path First) is another protocol that addresses the route discovery.
- It was developed to be more efficient and to create less overhead than RIP.

TCP (Transmission Control Protocol)

- It is Internet suit's main transport layer protocol.
- It provides reliable, full duplex, connection oriented transport services to upper layer protocols.
- TCP works in conjunction with IP to move packets through internetwork.

WHAT'S NEXT

- WE HAVE TO STUDY INTERNET UPPER LAYER PROTOCOLS IN DETAIL.