CHAPTER 2: INTERNETWORKING

Internetworking is the practice of connecting a computer network with other networks through the use of gateways that provide a common method of routing information packets between the networks. The resulting system of interconnected networks is called an **internetwork**, or simply an internet.

a) Evolution of Internetworking:

The internetworking is developed in various steps which took numbers of decades. Year by year quality of networks was improved and new technology was invented and used in the networks. Very first real network came into practice in nineteenth century. It was the telegraph that was used to send the messages. In technical terms, it is called the primitive form of message switching. Voice communication was introduced in 1876. This was the first step towards telecommunications. The different stages in which computer internetworking was developed are as below:

The networks that came prior to all other networks were developed in 60s and 70s. Those networks were the time sharing networks and used mainframe computer and centralized computing architecture. Those networks were of limited access up to 300 bits/sec which is very less as compare to today's network speed some of which are up to 10 Gb/sec.

After that in 1980s, Local Area Networks (LANs) came which were PC based computer networking systems that connects the computers and other devices in a small area such as office building, school, college or home. A Local Area network is very helpful to share the resources. Resources include hardware parts such as printers, hard disks, memory and even processor and also abstract part of computer like files, games, applications, softwares and even operating system.

The evolution of LANs helps in development of client-server computing in late 1980s and early 1990s that helps to improve the performance of the networks in which resource sharing was used. In previous networks if one computes shares a resource and at same time another needs the same resource then that computer faces the problem of deadlock. But in this type of networking, the solution of this problem came. Clients send request to server to use some resources and server receives the request, processes it and gives feedback to the corresponding client. Clients are given some authorities to do the tasks.

In mid of 1990s, the evolution of protocols (like TCP/IP) introduced internet that was the biggest change in internetworking. Internet is the network of networks in which two or more globally separated computers as well as networks are connected to from a larger network. Globally separated computers means that computers can be placed anywhere in the world.

b) Concepts

i). Internetworking Requirements

The overall requirements for an internetworking facility are as follows:

1. Provide a link between networks. At minimum, a physical and link control connection is needed.
2. Provide for the routing and delivery of data between processes on different networks.
3. Provide an accounting service that keeps track of the use of the various networks and routers and maintains status information.
4. Provide the services listed in such a way as not to require modifications to the networking architecture of any of the constituent networks. The internetworking facility must accommodate a number of differences among networks, including the following:

- Different addressing schemes
- Different maximum packet size
- Different network access mechanisms
- Different timeouts
- Error recovery
- Status reporting

- Routing techniques
- User access control
- Connection, connectionless

ii). Internetworking Devices

Network Interface Cards

The network interface card (NIC) provides the physical connection between the network and the computer workstation. Most NICs are internal, and they are included in the purchase of most computers. Network interface cards are a major factor in determining the speed and performance of a network. It is a good idea to use the fastest network card available for the type of workstation you are using.

The most common network interface connections are Ethernet cards and wireless adapters.

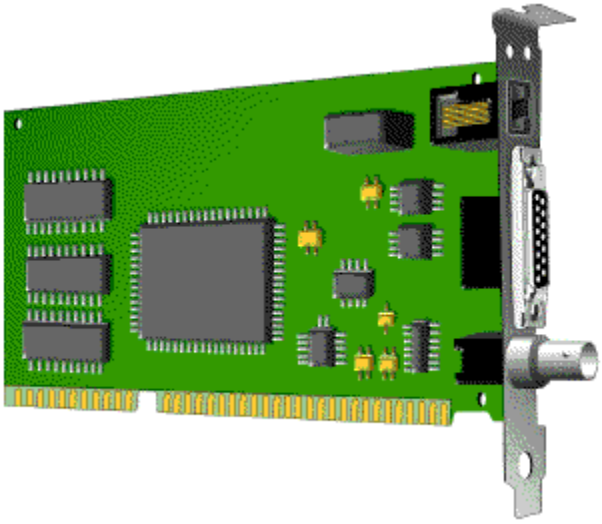


Fig. 1. Ethernet card.
From top to bottom:
RJ-45, AUI, and BNC connectors

Wireless Adapters

Wireless adapters are found in most portable devices, such as laptops, smart phones, and tablet devices. External wireless adapters can be purchased and installed on most computers having an open USB (Universal Serial Bus) port, or unused expansion slot.

Switches

An ethernet switch is a device that provides a central connection point for cables from workstations, servers, and peripherals. In a star topology, twisted-pair wire is run from each workstation to a central switch/hub. Most switches are active, that is they electrically amplify the signal as it moves from one device to another. The predecessor of the switch was the hub, which broadcasted all inbound packets out all ports of the device, creating huge amounts of unnecessary network traffic. Modern switches build a port map of all IP address which respond on each port, and only broadcasts on all ports when it doesn't have a packet's target IP address already in its port map. Switches are:

- Usually configured with 8, 12, or 24 RJ-45 ports
- Often used in a star or tree topology
- Available as "managed" or "unmanaged", with the later less expensive, but adequate for smaller networks
- direct replacements for hubs, immediately reducing network traffic in most networks
- Usually installed in a standardized metal rack that also may store network servers, bridges or routers.

Repeaters

Since a signal loses strength as it passes along a cable, it is often necessary to boost the signal with a device called a repeater. The repeater electrically amplifies the signal it receives and rebroadcasts it. Repeaters can be separate devices or they can be incorporated into a concentrator. They are used when the total length of your network cable exceeds the standards set for the type of cable being used.

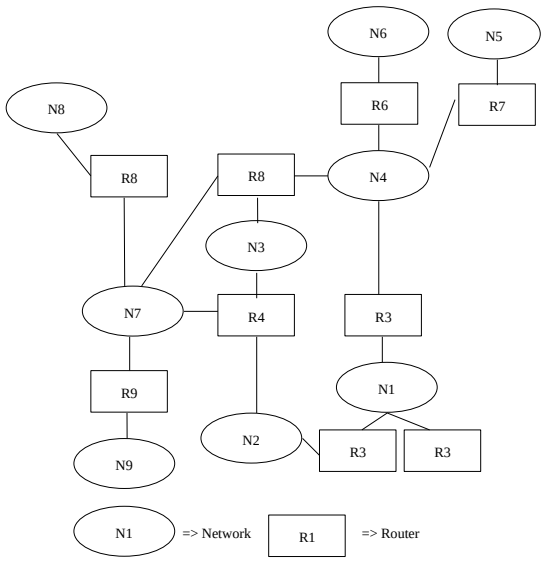
Bridges

A bridge is a device that allows you to segment a large network into two smaller, more efficient networks. If you are adding to an older wiring scheme and want the new network to be up-to-date, a bridge can connect the two.

A bridge monitors the information traffic on both sides of the network so that it can pass packets of information to the correct location. Most bridges can "listen" to the network and automatically figure out the address of each computer on both sides of the bridge. The bridge can inspect each message and, if necessary, broadcast it on the other side of the network.

Routers

Routers are the traffic directors of the global internet. All routers maintain complex routing tables which allow them to determine appropriate paths for packets destined for any address. Routers communicate with each other, and forward network packets out of or into a network.



Brouters

Brouters combines the best of both bridges and routers. When brouters receive packets that are routable, they will operate as a router by choosing the best path for the packet and forwarding it to its destination. However, when a nonroutable packet is received, the brouter functions as a bridge, forwarding the packet based on hardware address. To do this brouters maintain both bridging table, which contains hardware address, and a routing table, which contains network address.

Gateway

A gateway is a protocol converter which connects dissimilar systems and protocols. A router itself transfers, accepts, and relays packets only across network using similar protocols. A gateway on the other hand, can accept a packet formatted for one protocol (e.g. AppleTalk) and convert it to a packet formatted for another protocol (e.g. TCP/IP) before forwarding it. Gateways operate in all seven layers of OSI model.

A gateway is generally software installed within a router. The gateway understands the protocol used by each network linked into the router and is therefore able to translate from one to another.

Strengths and limitations of Gateway

Strength:

- Can connect completely different system.
- Dedicated to one task and perform that task well.

Limitation:

- More expensive than other devices.
- More difficult to install and configure.
- Greater processing requirements mean they are slower than other devices.

c) Common internet protocols

A protocol is a set of rules that governs the communications between computers on a network. These rules include guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling, and speed of data transfer.

Transmission control Protocol (TCP)

The TCP provides reliable transmission of data in an IP environment. TCP corresponds to the transport layer (Layer 4) of the OSI reference model. Among the services TCP provides are stream data transfer, reliability, efficient flow control, full-duplex operation, and multiplexing.

- Full-duplex means that TCP processes can both send and receive at the same time.
- Multiplexing means that numerous simultaneous upper-layer conversations can be multiplexed over a single connection.

TCP offers reliability by providing connection-oriented, end-to-end reliable packet delivery through an internetwork. It does this by sequencing bytes with a forwarding acknowledgment number that indicates to the destination the next byte the source expects to receive. Bytes not acknowledged within a specified time period are retransmitted. The reliability mechanism of TCP allows devices to deal with lost, delayed, duplicate, or misread packets. A time-out mechanism allows devices to detect lost packets and request retransmission.

Internet protocol (IP)

The Internet protocols are the world's most popular open-system protocol suite because they can be used to communicate across any set of interconnected networks and are equally well suited for LAN and WAN communications. The Internet protocols consist of a suite of communication protocols, of which the two best known are:

- Transmission Control Protocol (TCP)
- Internet Protocol (IP).

User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) is a connectionless transport-layer protocol (Layer 4) that belongs to the Internet protocol family. UDP is basically an interface between IP and upper-layer processes. UDP protocol ports distinguish multiple applications running on a single device from one another.

Unlike the TCP, UDP adds no reliability, flow-control, or error-recovery functions to IP. Because of UDP's simplicity, UDP headers contain fewer bytes and consume less network overhead than TCP. UDP is useful in situations where the reliability mechanisms of TCP are not necessary, such as in cases where a higher-layer protocol might provide error and flow control.UDP is the transport protocol for several well-known application-layer protocols, including Network File System (NFS), Simple Network Management Protocol (SNMP), Domain Name System (DNS), and Trivial File

Transfer Protocol (TFTP).

Hypertext Transfer Protocol (**HTTP**)

This is an application protocol for distributed, collaborative, hypermedia information systems.[1] HTTP is the foundation of data communication for the World Wide Web.

Hypertext is a multi-linear set of objects, building a network by using logical links (the so-called hyperlinks) between the nodes (e.g. text or words). HTTP is the protocol to exchange or transfer hypertext

File Transfer Protocol (**FTP**)

This is a standard network protocol used to transfer files from one host or to another host over a TCP-based network, such as the Internet.

FTP is built on a client-server architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves using a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it.

Post Office Protocol (**POP**)

In computing, the **Post Office Protocol** (**POP**) is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.

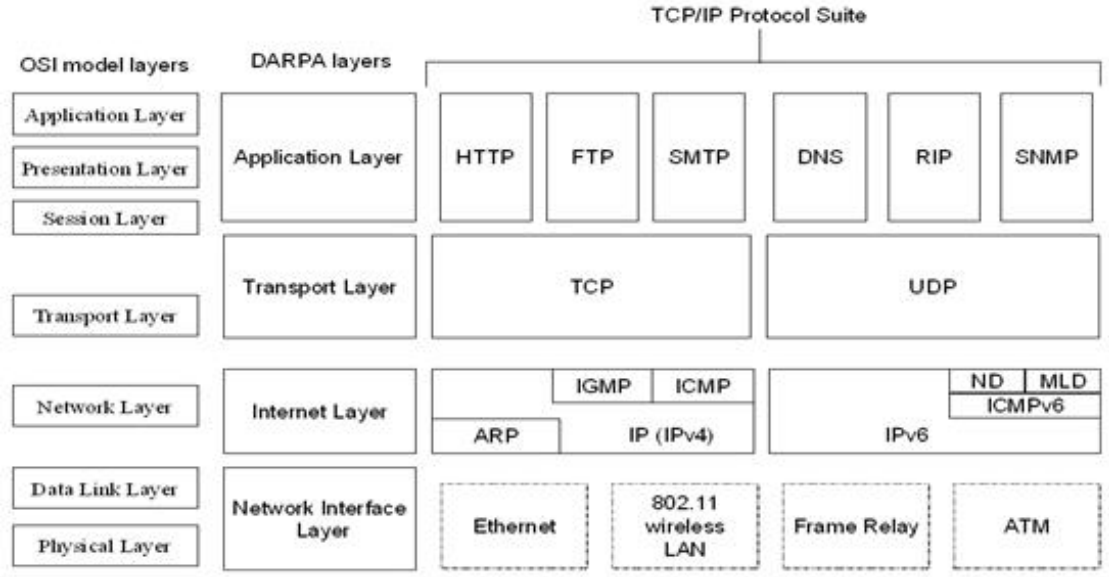
POP and IMAP (Internet Message Access Protocol) are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both. The POP protocol has been developed through several versions, with version 3 (POP3) being the current standard. Most webmail service providers such as Hotmail, Gmail and Yahoo! Mail also provide IMAP and POP3 service.

Simple Mail Transfer Protocol (**SMTP**) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

While electronic mail servers and other mail transfer agents use SMTP to send and receive mail messages, user-level client mail applications typically only use SMTP for sending messages to a mail server for relaying. For receiving messages, client applications usually use either the Post Office Protocol (POP) or the Internet Message Access Protocol (IMAP) or a proprietary system (such as Microsoft Exchange or Lotus Notes/Domino) to access their mail box accounts on a mail server.

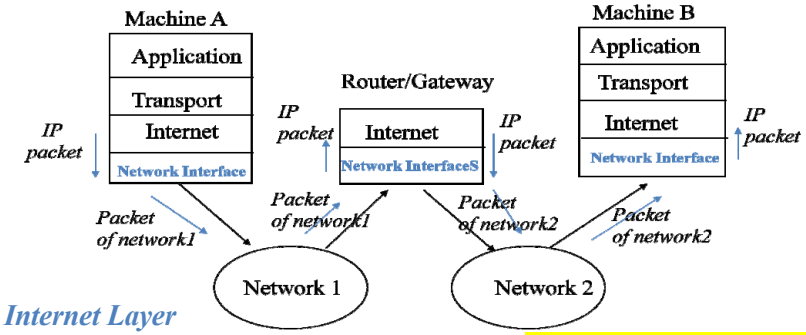
Internet message access protocol (**IMAP**) is one of the two most prevalent Internet standard protocols for e-mail retrieval, the other being the Post Office Protocol (POP).[1] Virtually all modern e-mail clients and mail servers support both protocols as a means of transferring e-mail messages from a server.

TCP/IP Architecture



Network Interface Layer

The Network Interface layer (also called the Network Access layer) sends TCP/IP packets on the network medium and receives TCP/IP packets off the network medium. TCP/IP was designed to be independent of the network access method, frame format, and medium. Therefore, you can use TCP/IP to communicate across differing network types that use LAN technologies—such as Ethernet and 802.11 wireless LAN—and WAN technologies—such as Frame Relay and Asynchronous Transfer Mode (ATM). By being independent of any specific network technology, TCP/IP can be adapted to new technologies.

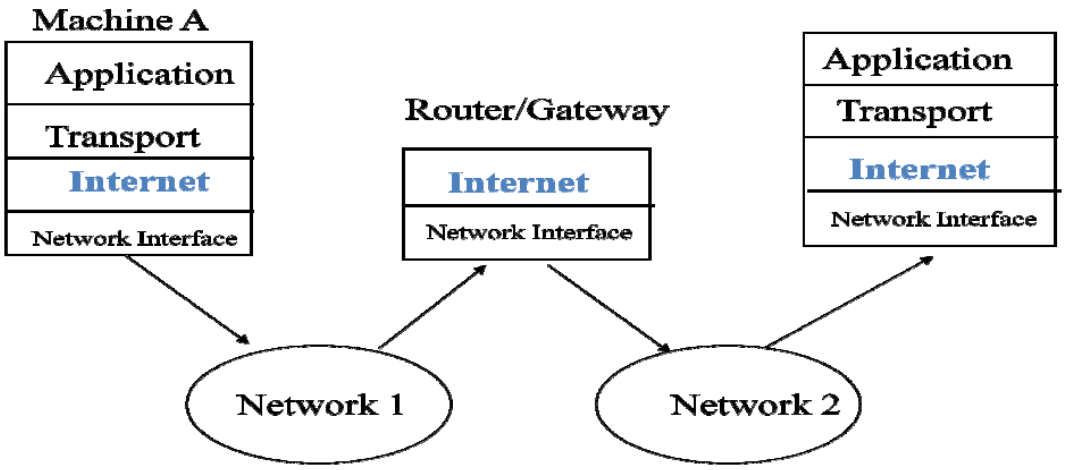


Internet Layer

The Internet layer responsibilities include addressing, packaging, and routing functions. The Internet layer is analogous to the Network layer of the OSI model.

The core protocols for the IPv4 Internet layer consist of the following:

- The Address Resolution Protocol (ARP) resolves the Internet layer address to a Network Interface layer address such as a hardware address.
- The Internet Protocol (IP) is a routable protocol that addresses, routes, fragments, and reassembles packets.
- The Internet Control Message Protocol (ICMP) reports errors and other information to help you diagnose unsuccessful packet delivery.
- The Internet Group Management Protocol (IGMP) manages IP multicast groups. The core protocols for the IPv6 Internet layer consist of the following:
- IPv6 is a routable protocol that addresses and routes packets.
- The Internet Control Message Protocol for IPv6 (ICMPv6) reports errors and other information to help you diagnose unsuccessful packet delivery.
- The Neighbour Discovery (ND) protocol manages the interactions between neighbouring IPv6 nodes.
- The Multicast Listener Discovery (MLD) protocol manages IPv6 multicast groups.



Transport Layer

The Transport layer (also known as the Host-to-Host Transport layer) provides the

Application layer with session and datagram communication services. The Transport layer encompasses the responsibilities of the OSI Transport layer. The core protocols of the Transport layer are TCP and UDP. TCP provides a one-to-one, connection-oriented, reliable communications service. TCP establishes connections, sequences and acknowledges packets sent, and recovers packets lost during transmission. In contrast to TCP, UDP provides a one-to-one or one-to-many, connectionless, unreliable communications service. UDP is used when the amount of data to be transferred is small (such as the data that would fit into a single packet), when an application developer does not want the overhead associated with TCP connections, or when the applications or upper-layer protocols provide reliable delivery.TCP and UDP operate over both IPv4 and IPv6 Internet layers.

Application Layer

The Application layer allows applications to access the services of the other layers, and it defines the protocols that applications use to exchange data. The Application layer contains many protocols, and more are always being developed.

The most widely known Application layer protocols help users exchange information:

- The Hypertext Transfer Protocol (HTTP) transfers files that make up pages on the World Wide Web.
- The File Transfer Protocol (FTP) transfers individual files, typically for an interactive user session.
- The Simple Mail Transfer Protocol (SMTP) transfers mail messages and attachments.

Additionally, the following Application layer protocols help you use and manage TCP/IP networks:

- The Domain Name System (DNS) protocol resolves a host name, such as www.microsoft.com, to an IP address and copies name information between DNS servers.
- The Routing Information Protocol (RIP) is a protocol that routers use to exchange routing information on an IP network.
- The Simple Network Management Protocol (SNMP) collects and exchanges network management information between a network management console and network devices such as routers, bridges, and servers.

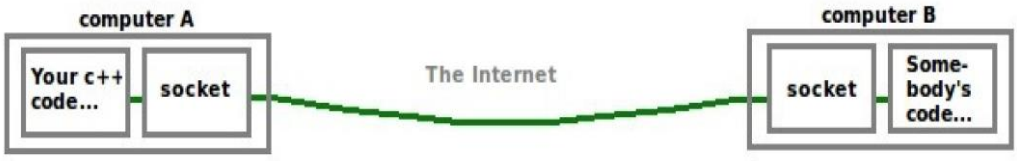
Windows Sockets and NetBIOS are examples of Application layer interfaces for TCP/IP applications.

d) Internetworking architecture

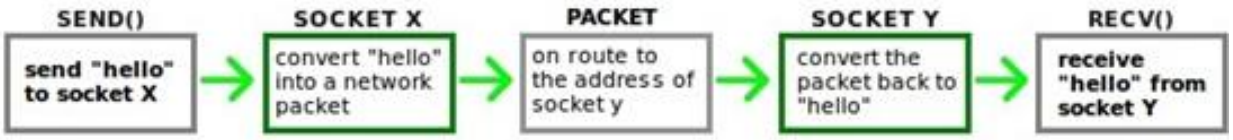
i). Sockets

Sockets are a protocol independent method of creating a connection between processes. Also Sockets are a mechanism for exchanging data between processes. These processes can either be on the same machine, or on different machines connected via a network. Once a socket connection is established, data can be sent in both directions until one of the endpoints closes the connection. Sockets can be either:

- *connection based* or *connectionless*: Is a connection established before communication or does each packet describe the destination?
- *packet based* or *streams based*: Are there message boundaries or is it one stream?
- *Reliable* or *unreliable*. Can messages be lost, duplicated,reordered, or corrupted?



Socket is a begin or endpoint in a tcp/ip network connection .
You can see a socket as the entrance or exit of a tunnel. A socket translates all incoming data in to "human readable text" or translates all outgoing data into networks packets.
The purpose of sockets is simplifying the network code of your c++ application. All the user has to



do is create a socket and connect it. Once your socket is connected the socket takes care of the networking part, and all you have to worry about now is sending data to, or receiving data from, the socket.
A socket can be a server or a client. Before a socket can be connected to another socket and "create a tunnel" you have to specify what type of socket it will be and where it should connect to.

How to communicate to a socket

Socket APIs

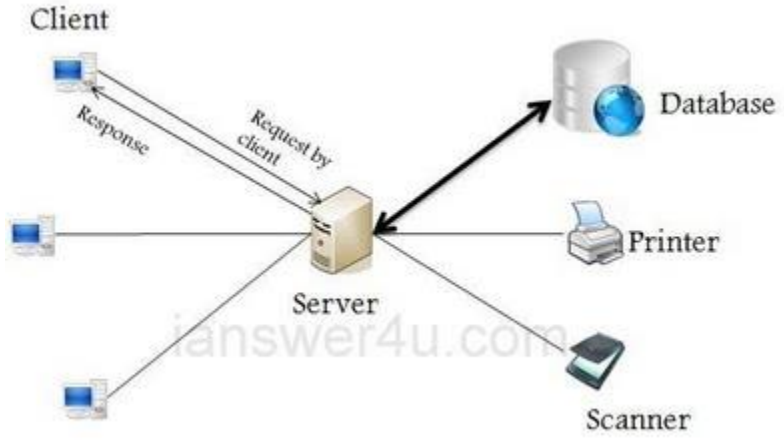
- *socket*: creates a socket of a given domain, type, protocol (buy a phone)
- *bind*: assigns a name to the socket (get a telephone number)
- *listen*: specifies the number of pending connections that can be queued for a server socket. (call waiting allowance)
- *accept*: server accepts a connection request from a client (answer phone)
- *connect*: client requests a connection request to a server (call)
- *send*, *sendto*: write to connection (speak)
- *recv*, *recvfrom*: read from connection (listen)
- *shutdown*: end the call

ii). Client Server Architectures

What is a Client Server Network?
The type of computing system in which one powerful workstation serves the requests of other systems, is an example of client server technology. A computer network is an interconnection of computers which share various resources.
What is computer server?
A computer server is the powerful computer, or the set of computers connected to each other, which provide services to other systems. They usually have database integrated in them, and are very powerful machines with very advanced configuration. They process the requests of client machines. Their role is to make management of network easy and uniform.
Features of Servers :-
1) They have large storage capacity.
2) They are able to provide information to many computers simultaneously, therefore have large RAM.
3) Its processor speed is high, as it may have to execute multi-tasking too.

What are clients in client-server model?
Clients are the individual components which are connected in a network. They have a basic configuration. Client sends a request/query to server and server responds accordingly. Please note that the client doesn't share any of its resources. They are subordinates to servers, and their access rights are defined by servers only. They have localized databases.

Client Server Diagram



Client Server Architecture

Components of Client Server

1) Clients or Workstations.
2) Servers.
3) Network Devices :- They connect the clients and servers, and at the same time ensure proper collision free routing of information.
4) Other components like scanner, printer, etc can also be connected to network architecture.

Server Types

Depending on the size and requirements of the network, servers can be classified as below:

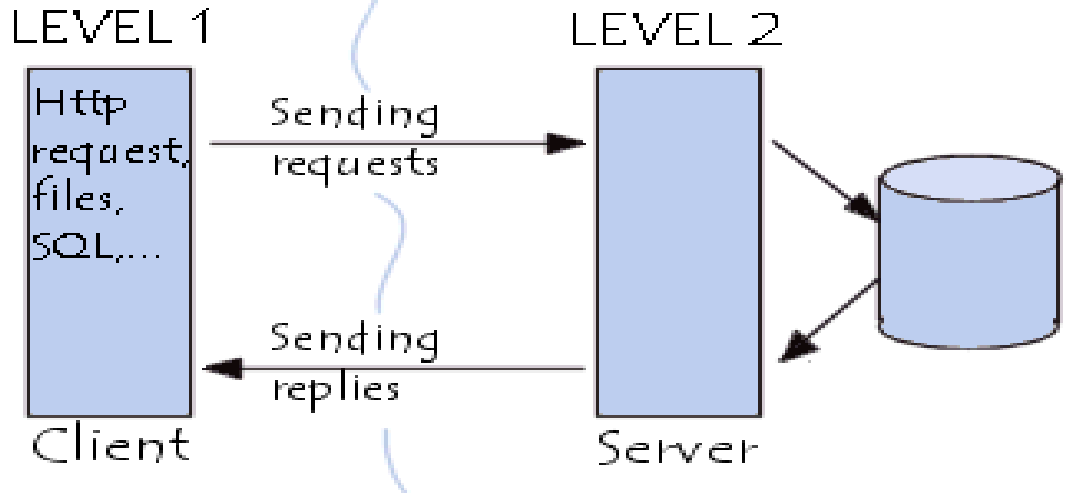
1. **File Server**
   A file server allows user to share files. It several LAN users need access to an application such as word processing, only one copy of the application software needs to reside on a file server. This copy can be shared among all the users. When a user requests to start an application, that application is downloaded into the users workstation.
2. **Database Server**
   The database server was developed to solve the problem of passing an entire file over the medium. The most common example of a database server is the SQL server. Structured Query Language (SQL) is standard database definition, access, and update language for relational database. An SQL server accepts a database request, accesses all necessary records locally, and then sends only the result back to the requester (not the whole database).
3. **Print Server**
   Print server allows anyone on the network to have access to a printing service.
4. **Disk Server**
   It is server with large storage. A portion of storage is given to each user to store their files/data. It is very useful in university where each student is given a user account with password and some storage space in disk server. Once the student completes the education the same space can be assigned to new student.
5. **Dedicated Vs Non-Dedicated Server**
   Many networks will let their user run standard programs while their computer is simultaneously functioning as a server to others. A computer that both runs standard programs and lets other user see its data at the same time is said to be "non-dedicated server". Non-dedicated servers can be clever way of setting up a small LAN without having to buy

any extra system. Dedicated server are specially assigned for network management and provided no general-purpose services.

6. Web Server
   Web server can refer to either the hardware (the computer) or the software (the computer application) that helps to deliver content that can be accessed through the Internet. E.g. of web servers are proxy servers, mail servers, application servers, etc.

The following are the examples of client/server architectures.

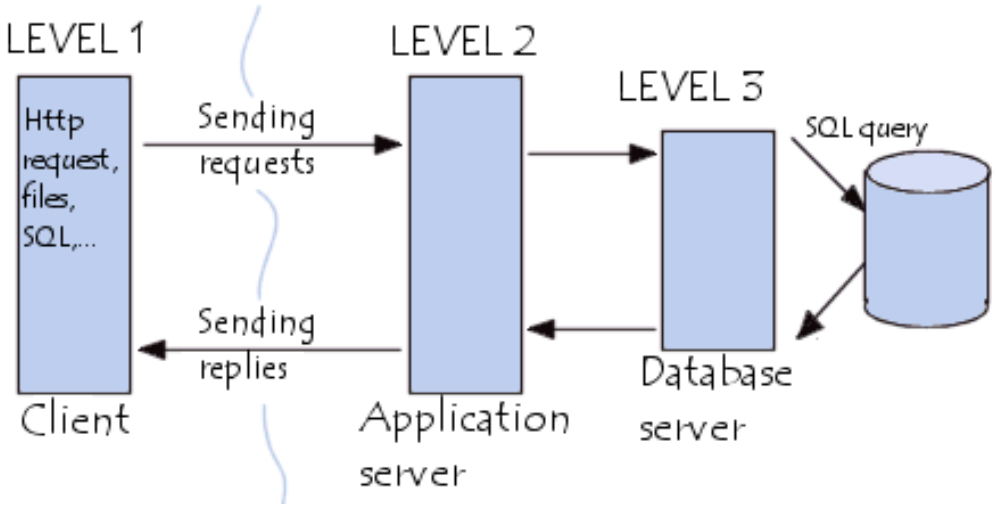
1) Two tier architectures In two tier client/server architectures, the user interface is placed at user's desktop environment and the database management system services are usually in a server that is a more powerful machine that provides services to the many clients. Information processing is split between the user system interface environment and the database management server environment. The database management server supports for stored procedures and triggers. Software vendors provide tools to simplify development of applications for the two tier client/server architecture.



2) Three tier architectures The three tier architecture is introduced to overcome the drawbacks of the two tier architecture. In the three tier architecture, a middleware is used between the user system interface client environment and the database management server environment. These middleware are implemented in a variety of ways such as transaction processing monitors, message servers or application servers. The middleware perform the function of queuing, application execution and database staging. In addition the middleware adds scheduling and prioritization for work in progress. The three tier client/server architecture is used to improve performance for large number of users and also improves flexibility when compared to the two tier approach. The drawback of three tier architectures is that the development environment is more difficult to use than the development of two tier applications.

i) Three tier with message server. In this architecture, messages are processed and prioritized asynchronously. Messages have headers that include priority information, address and identification number. The message server links to the relational DBMS and other data sources. Messaging systems are alternative for wireless infrastructures.

ii) Three tier with an application server This architecture allows the main body of an application to run on a shared host rather than in the user system interface client environment. The application server shares business logic, computations and a data retrieval engine. In this architecture applications are more scalable and installation costs are less on a single server than maintaining each on a desktop client.



Uses Client/server architectures are used in industry as well as in military. They provide a versatile architecture that allows insertion of new technology more readily than earlier software designs.

Comparing both types of architecture

- 2-tier architecture is therefore a client-server architecture where the server is versatile, i.e. it is capable of directly responding to all of the client's resource requests.
- In 3-tier architecture however, the server-level applications are remote from one another, i.e. each server is specialized with a certain task (for example: web server/database server). 3-tier architecture provides:
- A greater degree of flexibility
- Increased security, as security can be defined for each service, and at each level
- Increased performance, as tasks are shared between servers

How to make client:

The system calls for establishing a connection are somewhat different for the client and the server, but both involve the basic construct of a socket. The two processes each establish their own sockets.

The steps involved in establishing a socket on the client side are as follows:

1. Create a socket with the *socket()* system call.
2. Connect the socket to the address of the server using the *connect()* system call.
3. Send and receive data. There are a number of ways to do this, but the simplest is to use the *read()* and *write()* system calls.

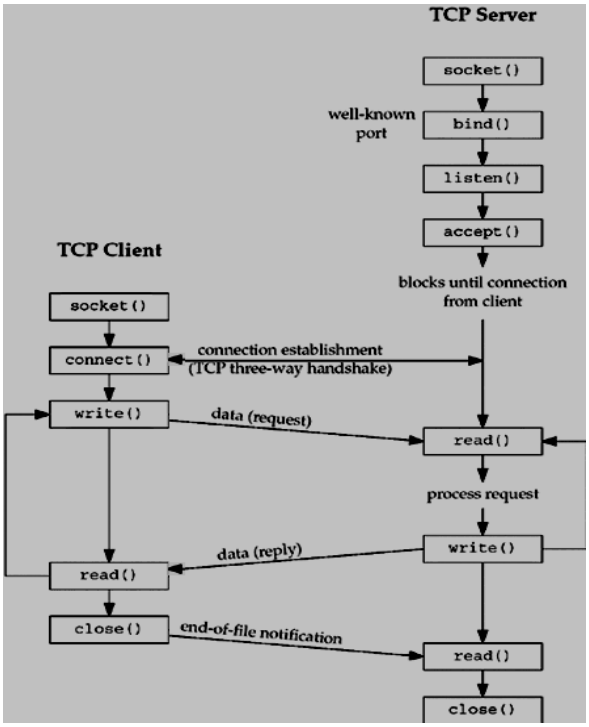
How to make a server:

The steps involved in establishing a socket on the server side are as follows:

1. Create a socket with the *socket()* system call.
2. Bind the socket to an address using the *bind()* system call. For a server socket on the Internet, an address consists of a port number on the host machine.
3. Listen for connections with the *listen()* system call.
4. Accept a connection with the *accept()* system call. This call typically blocks until a client connects with the server.
5. Send and receive data using the *read()* and *write()* system calls.

Client and Server Interaction:

Following is the diagram showing complete Client and Server interaction:


TCP Server
socket()
well-known port
bind()
listen()
accept()
blocks until connection from client
TCP Client
socket()
connect()
connection establishment (TCP three-way handshake)
write()
data (request)
read()
process request
write()
data (reply)
read()
close()
end-of-file notification
read()
close()

CHAPTER 3: INTERNET INFRASTRUCTURE

i). Intranet

This is an internal company network that uses Internet standards (HTML, HTTP & TCP/IP protocols) & software and is accessed only by authorized persons, especially members or employees of the organization.

Two levels of Security required:

Internal

It can be imposed by Public Key Security & Encryption Key.

External

Through Firewall.

Applications of Intranet

- Sharing of company policies/rules & regulations
- Access employee database
- Distribution of circulars/Office Orders
- Access product & customer data
- Sharing of information of common interest
- Launching of personal/departmental home pages
- Submission of reports
- Corporate telephone directories

Benefits of Intranet

- Intranet is an easy, economical and fast system of communication within the enterprise.
- It serves information automatically and thus, demand for information is more frequent and detailed.
- Intranet replaces grapevine as it permits inter employee communication with more transparency and free expression of views
- It improves productivity of the manager.
- Intranet helps in eliminating the latency of information in the enterprise and makes the flow of information need-driven than availability-driven.

Disadvantages

- *Management problem*

A company may not have person to update their Intranet on a routine basis

Fear of sharing information and the loss of control

Limited bandwidth for the business

- *Security problem*
  - Unauthorized access
  - Abuse of access
  - Denial of service
- *Productivity problem*
  - Information overload lowers productivity
  - True purpose of the Intranet is unknown to many employees/departments
  - Hidden or unknown complexity and costs

ii). Extranet?

Extranet is an Intranet for outside authorized users using same internet technology. It is an inter-organizational information system which enable outsiders to work together with company's employees. It is open to selected suppliers, customers & other business partners

Dealers/distributors have access to product files such as :-

- product specification,
- pictures,
- images, etc.

to answer the queries of the customer.

Components of extranets.

Some basic infrastructure components such as the internet including:-

- TCP/IP protocols,
- E-mail,
- Web-browsers,
- External business partners &
- Tele-commuting employees place order, check status & send E-mail.

Benefits of Extranet

- Improved quality.
- lower travel costs.
- lower administrative & other overhead costs.
- reduction in paperwork.
- delivery of accurate information on time.
- improved customer service.
- better communication.
- overall improvement in business effectiveness.

Disadvantages

- The suppliers & customer who don't have technical knowledge feel problem.
- Faceless contact.
- Information can be misused by other competitors.
- Fraud may be possible.
- Technical Employees are required.