




# **CST426 - CLIENT SERVER ARCHITECTURE**



## **Module – 4**

### **Client/ Server Systems Development**

- Services and Support- System administration, Availability, Reliability, Scalability, Observability, Agility, Serviceability. Software Distribution, Performance, Network management.
- Remote Systems Management- RDP, Telnet, SSH, Security.
- LAN and Network Management issues, Training, Connectivity, Communication interface technology, Interprocess communication, Wide area network technologies, Network Acquisition, PC-level processing unit, X-terminals, Server hardware.



# Services and Support


- System administration
- Availability
- Reliability
- Scalability
- Observability
- Agility
- Serviceability
- Software Distribution
- Performance
- Network management


# Systems Administration


- The principle of "do it right the first time" applies to the long-term success of your client/server application.
- It is important to ensure that **client/server hardware is specified and assembled according to organizational standards and tested prior to implementation.**
- **Software should be loaded by trained staff and tested** to ensure that it is installed according to standards and works as expected.
- The largest number of user problems are caused by incorrect installation and equipment that is faulty at installation.
- Most LAN administration problems can be prevented by **proper architecture supported by trained installers.**

# Availability

- Availability means **system uptime or the capability of the system to be available for processing information and doing its expected work whenever called on.**
- Minicomputer and mainframe data centers should provide at least 99.8-percent availability with today's technology.
- To achieve this level of availability, **a combination of technological and procedural steps are followed.**
- Most availability failure today is caused by **human error.**
- To minimize this, data centers implement **rigid procedures to manage change.**

- 
- Whether the change is hardware, network, system, or application software, **stringent procedures to request, validate, test, and implement the change are defined and adhered to.**
  - **Backout procedures are defined and tested** to ensure that if a failure occurs after implementation of the change, the data center can fall back to its previous status.
  - **Technological features** such as separate electrical power sources, backup diesel generator and battery power sources, redundant processors, and magnetic disk devices all are used to ensure that failure of a single component will not take down the data center.
  - Very critical systems **use fault-tolerant processors** to ensure 100 percent availability.

- 
- Data centers use **highly skilled professionals** in the central location.
  - They are expected to be able to recover the site quickly after any failure.
  - **Vendor service contracts** are used to guarantee that repair can be accomplished in one, four, or eight hours as necessary.
  - Client/server applications must be able to provide the appropriate level of availability demanded by the business need.

- 
- The provision of **highly qualified technical staff** at each site is sometimes physically and rarely economically feasible.
  - **Remote LAN management** is the only way to make effective use of scarce resources.
  - Remote management requires a central site connected through WAN services to each LAN.
  - Products such as **Openvison**, **Sun Connect**, **HP Openview**, IBM's **NetView** and **SystemView** can be integrated through industry-standard network management protocols to provide the desired level of availability for reasonable cost.




# Reliability

- All current technology minicomputer and mainframe operating systems provide basic services to support system reliability.
- **Reliability first requires availability factors to be resolved.**
- Reliability requires
  - applications to be protected from overwriting each other
  - **shared memory to be accessed only by authorized tasks.**
  - **Security** must be implemented to allow access to resources only by authorized users.
  - Database management software must ensure that either the entire set of updates requested by a unit-of-work be completed or that none be completed.
  - The software must automatically handle multiple user contention, provide **full recovery after failure** of in-flight updates
  - Provide utility functions **to recover a damaged magnetic disk.**


# Serviceability


- Most minicomputer and mainframe operating systems and hardware provide **diagnostic services that pinpoint the location of failures.**
- Transient errors are noted so that **preventive maintenance** can correct problems before they affect availability.
- The central location of the equipment allows **trained technicians to institute regular preventive maintenance programs.**
- For this reason, many organizations install their first servers in the glass room until they have more experience with remote LAN management.

- 
- Products based on standard protocols such as the **Simple Network Management Protocol (SNMP)** provide the **necessary feedback of event alerts** to support the remote systems management function.
  - It is necessary that the architecture design take into account the issues of standards and products to be serviceable.

# Software Distribution


- **The centralized minicomputer and mainframe environment shares executable software from a single library.**
- Software maintenance and enhancement are accomplished by changes to a single location.
- **In the distributed client/server model, executable software is resident on servers located throughout the organization.**
- Changes to system and application software must be replicated across the organization.
- This presents a tremendous complication in serviceability of these applications.

- 
- An additional complexity is incurred in the UNIX world **when several different hardware platforms are used.**
  - **The source level of the software is compatible across the various platforms, the executable binary form of the software is not compatible.**
  - The executable libraries must be created on a machine with the same physical hardware.
  - This causes serious problems for distribution of software throughout a large network of disparate computer platforms.
  - Testing should also be done on each platform before changes are distributed.
  - Most organizations have addressed this requirement by **installing one of each of the hardware platforms from the field in a central support location.**


- 
- **The solution to this problem is a properly designed client/server architecture supported by effective software management tools.**
  - This problem is solvable through design and planning.
  - There are special requirements in supporting distributed technology.
  - **Remote support personnel must be able to discover the hardware and software configuration of the remote technology so that they can determine which software versions to send and provide educated support for problems.**

# Performance

- In the centralized minicomputer and mainframe environment, **trained technical support personnel and operations staff monitor performance on an ongoing basis.**
- Sophisticated **monitoring tools**, such as Candle Corporation's **Omegamon MVS**, and analysis tools, such as **RMF** from IBM, **track the system's day-to-day performance.**
- IBM and Digital Equipment Corporation include features in their large computers' operating systems that provide considerable dynamic tuning capabilities.
- **If trends show performance degrading, systems managers can add hardware or make adjustments to improve performance before it affects the user community.**


- 
- Additional tools, such as **Crystal** from BBN and **TPNS** from IBM, are available **to simulate new applications** before they move into production.
  - This means that the organization learns in advance the resource requirements of new applications.
  - Changes can be made to the operating environment to ensure that performance will be acceptable.



- 
- In the client/server environment, neither UNIX, Windows NT, nor OS/2 yet provides these sophisticated performance-monitoring tools.
  - Certain tools, such as Network General's **Sniffer**, are available to **remotely monitor the LAN traffic**.
  - UNIX, Windows NT and OS/2 provide limited capabilities to define task priorities.
  - Many vendors are now marketing products to support this need.


# Network Management

- **Network management tools** such as those from **OpenVision**, IBM's **NetView**, AT&T's **UNMA**, and Digital Equipment Corporation's **EMA** products, provides a level of **remote monitoring that can track response time and network loading**.
- Products such as **ESRA** from Elegant Computing, are available to do **remote analysis of UNIX servers in order to monitor disk usage, error logs, and user profiles**.
- This product is used extensively to manage remote UNIX servers.

- 
- Other products, such as Microcoms **LANlord**, provide significant capabilities for **remote access to Windows and OS/2 PC LAN desktops**.
  - It is impossible to provide adequate support for distributed client/server applications without the capability to support the desktop and the server remotely.
  - During 1993, a number of major systems integrators implemented NOS to provide desktop support for Novell, LAN Manager, LAN Server, and NFS client/server environments.


# Remote Systems Management


- LAN administrators should be able to connect remotely to and then manage the workstation of any user who has a problem.
- **LANlord** from Microcom provides support for the **Windows 3.x desktop**.
- Microsoft's **Hermes** product will provide support for **Windows NT desktops** in late 1994.
- The products **DCAF** from IBM, **PolyMod2** from Memsoft and **Remote OS** from Menlo provide support for the **OS/2 environment**.
- DCAF requires an OS/2 workstation but can control a user DOS or Windows workstation.
- Network General provides **Distributed Sniffer**, which operates both locally and remotely.
- It provides excellent support to a LAN administrator with a graphical user interface (GUI) to display results.

- 
- Because **UNIX provides support for remote login**, all UNIX environments provide good tools for remote systems management.
  - **Sun Connect, IBM Netview 6000, HP Openview, and OpenVisors** products all provide good support dependent on the specific requirements of the distributed computing environment.
  - Each of these products **provides an accurate record of performance and traffic loading** at the point of analysis.
  - If these analyses are done regularly, LAN administrators can detect problems as they arise.


# Security


- In any application environment, managers must assess the security requirements.
- Users should find security to be invisible when they are authorized for a function and impenetrable when they are unauthorized.
- **Security of the server** should start by **placing physical barriers** around unauthorized access.
- Because users do not need physical access to the **database and application servers, both should be placed in a locked room.**
- Frequently the existing host computer room can be used to hold workgroup servers.


- 
- **Every user of a client/server application should be assigned a personal ID and password.**
  - The ID can be used to assign authority and track access.
  - Customized procedures can be built for each individual ID to manage backup, access times, and prompting.
  - The DCE-defined **Kerberos standard is preferred for UNIX servers.**

- 
- Physical network security standards are being defined by several groups including the IEEE.
  - **SNMP-2 is being enhanced to support greater security.**
  - Operating systems designed from the ground up with security in mind form a **trusted computing base (TCB)** that incorporates encryption of passwords, safeguards against bypassing the logon system and the capability to assign privileges to user groups.
  - NetWare 4.0 and Windows NT can also **log attempted security breaches and trigger alarms** that notify a network manager.




- 
- The new operating systems require that **each account specifically be granted rights for remote access** or encrypt passwords during remote access.
  - Effective security must be defined as part of the enterprise-wide architecture put in place as an organization moves to the client/server model.
  - **Effective administrative procedures for user definition, password maintenance, physical security, and application design must be instituted.**

- 
- When maximum security is required, **network and permanently stored data should be encrypted.**
  - The **data encryption standard (DES)** algorithm uses a personal key to make data unusable to anyone who lacks that key.
  - This **data is encrypted when it's stored and decrypted on retrieval.**
  - Only when the correct DES key is provided is the information meaningful.

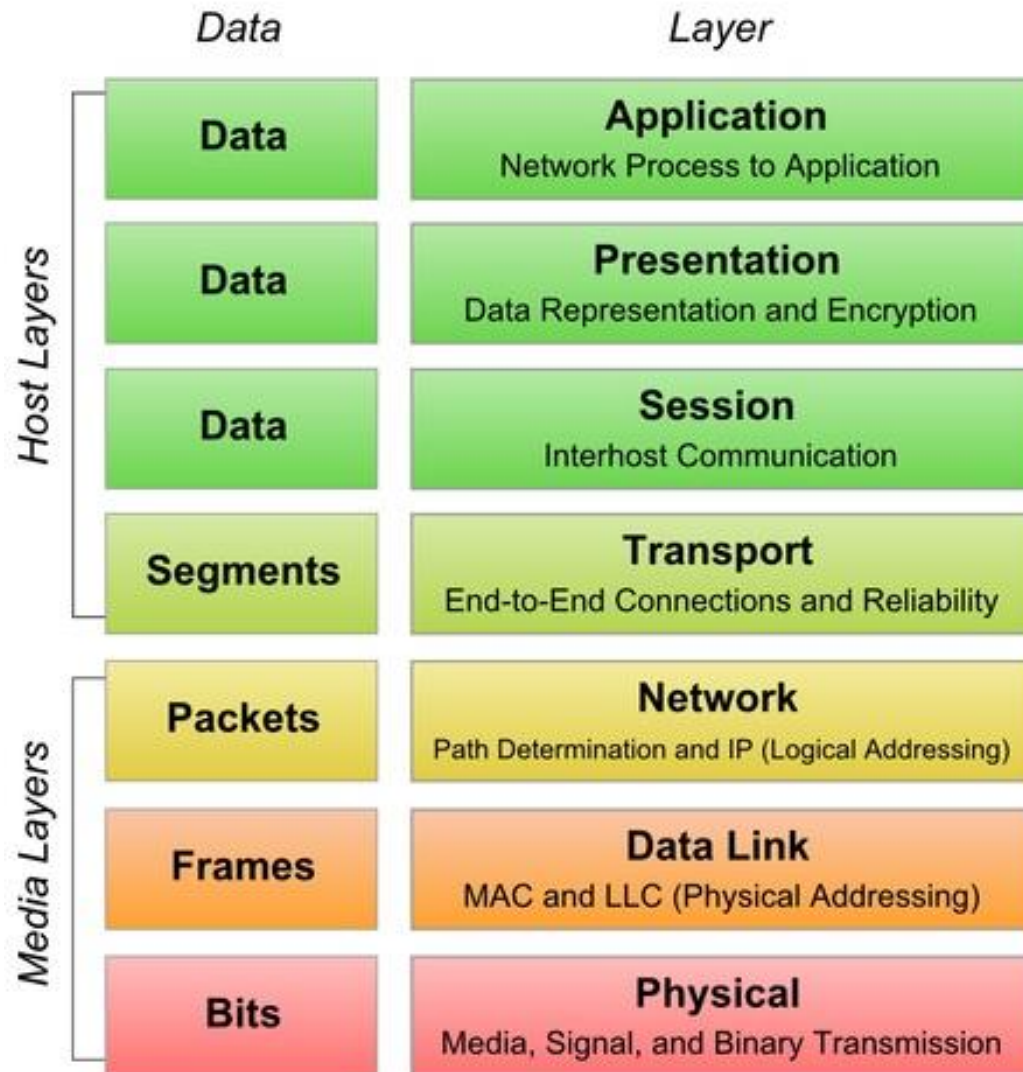
- 
- **Diskless workstations** can **prevent information from being copied to a floppy** and removed or from being left where someone might break into the workstation to access the hard disk.
  - No sensitive data should be stored on the client workstation or on an unprotected workgroup server.

# **Communications Interface Technology**

- **LAN Cabling**
- **Ethernet IEEE 802.3**
- **Token Ring IEEE 802.5**
- **Fiber Distributed Data Interface (FDDI)**
- **Copper Distributed Data Interface (CDDI)**
- **Ethernet versus Token Ring versus FDDI**
- **Asynchronous Transfer Mode (ATM)**
- **Hubs**
- **Internetworking Devices Bridges and Routers**
- **Transmission Control Protocol/Internet Protocol (TCP/IP)**
- **Internet Protocol**
- **Transport Protocols**
- **Telnet**
- **File Transfer Protocol (FTP)**
- **Simple Network Management Protocol (SNMP)**
- **Network File System (NFS)**
- **Simple Mail Transfer Protocol (SMTP)**
- **TCP/IP and Internetworks**
- **Vendor Products**


- 
- Connectivity and interoperability between the client workstation and the server are achieved through a combination of physical cables and devices, and software that implements communication protocols.

# OSI Model



# LAN Cabling

- A corporation's investment in cabling is significant.
- Implementation costs are too high, and maintenance is a nonbudgeted, nonexistent process.
- Studies have shown that over 65 percent of all LAN downtime occurs at the physical layer.
- Cabling standards include
  - RG-58 A/U coaxial cable (thin-wire 10Base2 Ethernet),
  - IBM Type 1 (shielded, twisted pair for Token Ring),
  - unshielded twisted pair (UTP for 10BaseT Ethernet or Token Ring)
  - Fiber Distributed Data Interface (FDDI for 10BaseT or Token Ring).

- 
- Wireless LAN technology is useful and cost-effective when the cost of cable installation is high.
  - In old buildings or locations where equipment is frequently moved, the cost of running cables may be excessive, so in these instances wireless technology is an attractive alternative.
  - NCR's WaveLAN provides low-speed wireless LAN support.
  - It also is subject to interference by other transmitters, such as remote control
  - electronics, antitheft equipment, and point-of-sale devices.




# Ethernet IEEE 802.3

- Ethernet is the most widely installed network topology today.
- It uses CSMA/CD (Carrier-Sense Multiple Access/Collision Detection) mechanism.
- Ethernet is a Bus shaped topology.
- Ethernet does not contain routing information.
- Ethernet networks have a **maximum throughput of 10 Mbps.**
- The first network interface cards (NICs) developed for Ethernet were much cheaper than corresponding NICs developed by IBM for Token Ring.
- **10BaseT Ethernet** is a standard that enables the implementation of the Ethernet protocol over telephone wires in a physical star configuration.
- Its robustness, ease of use, and low cost driven by hard competition have made 10BaseT the most popular standards-based network topology.


# Token Ring IEEE 802.5


- IBM uses the Token Ring LAN protocol as the standard for connectivity in its products.
- In an environment that is primarily IBM hardware and SNA connectivity, Token Ring is the preferred LAN topology option.
- IBM's Token Ring implementation is a modified ring configuration that provides a **high degree of reliability** since failure of a node does not affect any other node.
- In the token ring, the token passing mechanism is used.
- A token ring is a Star shaped topology.


- 
- IBM and Hewlett-Packard have established a single 100Mbps standard for both Token Ring and Ethernet networks called **100VG-AnyLAN**.
  - 100VG-AnyLAN is designed to operate over a variety of cabling, including unshielded twisted pair (Categories 3, 4, or 5), shielded twisted pair, and FDDI.
  - The entire LAN operates at the speed of the slowest NIC.
  - In token ring, flow of data is unidirectional as data is passed from one workstation to another only when the token is received by the workstation.
  - The token ring contains routing information.
  - Most of the vendors today, including IBM and SynOptics, support 16 Mbps over unshielded twisted-pair cabling (UTP).

## Fiber Distributed Data Interface (FDDI)

- The third prevalent access method for Local Area Networks is Fiber Distributed Data Interface (FDDI).
- FDDI provides support for **100 Mbps over optical fiber**, and offers improved fault tolerance by implementing **logical dual counter rotating rings**.
- FDDI can extend in range up to 200 kilometers.
- This is effectively running two LANs.
- The physical implementation of FDDI is in a star configuration.
- FDDI is derived from the **IEEE 802.4 token bus timed token protocol**.

- 
- It contains two token rings, a primary ring for data and token transmission and a secondary ring that provides backup if the primary ring fails.
  - The primary ring offers up to 100 megabits per second (Mbps) capacity, while the secondary ring can also be used to carry data, increasing capacity to 200 Mbps.
  - One ring will operate in a clockwise direction and the other in a counter clockwise direction.

- 
- In a token network, only the device with the token may transmit.
  - The use of a timed token ensures the maximum wait time for each device to be able to transmit.
  - By use of **dual homing hubs** (the capability to have workstations and hubs connected to other hubs for further fault tolerance), highly critical nodes such as servers or routers can be physically attached to the ring in two distinct locations.
  - **Station Management Technology (SMT)** is the portion of the standard that provides **ring configuration, fault isolation, and connection management**.
  - This is an important part of FDDI, because it delivers tools and facilities that are desperately needed in other access method technologies.

- 
- There are two primary applications for FDDI:
    1. as a **backbone technology for interconnecting multiple LANs**, and
    2. as a **high-speed medium to the desktop** where bandwidth requirements justify it.


# Copper Distributed Data Interface

- The original standards in the physical layer specified optical fiber support only.
- Many vendors, have developed technology that enables FDDI to run over copper wiring.
- Currently, there is an effort in the ANSI X3T9.5 committee to produce a standard for FDDI over Shielded Twisted Pair (IBM compliant cable), as well as Data grade unshielded twisted pair.
- Several vendors, including DEC, IBM, and SynOptics are shipping an implementation that supports STP and UTP.



# Asynchronous Transfer Mode (ATM)

- ATM has been chosen by CCITT as the basis for its **Broadband Integrated Services Digital Network (B-ISDN) services**.
- The integrated support for all types of traffic is provided by the implementation of multiple classes of service categorized as follows:
- **Constant Bit Rate (CBR)**: connection-oriented with a timing relationship between the source and destination, for applications such as 64 kbits voice or fixed bit rate video
- **Variable Bit Rate (VBR)**: connection-oriented with a timing relationship between the source and destination, such as variable bit rate video and audio
- **Bursty traffic**: having no end-to-end timing relationship, such as computer data and LAN-to-LAN.

- 
- Cell in ATM is a **53-byte packet of data**, the standard packet size used by Asynchronous Transfer Mode (ATM) communication technologies.
  - Cells are to ATM technologies what frames are to Ethernet networking.
  - ATM's capability to make the "computing anywhere" concept a reality is made possible because ATM eventually will be **implemented both in the LAN and in the WAN.**

ATM Cells

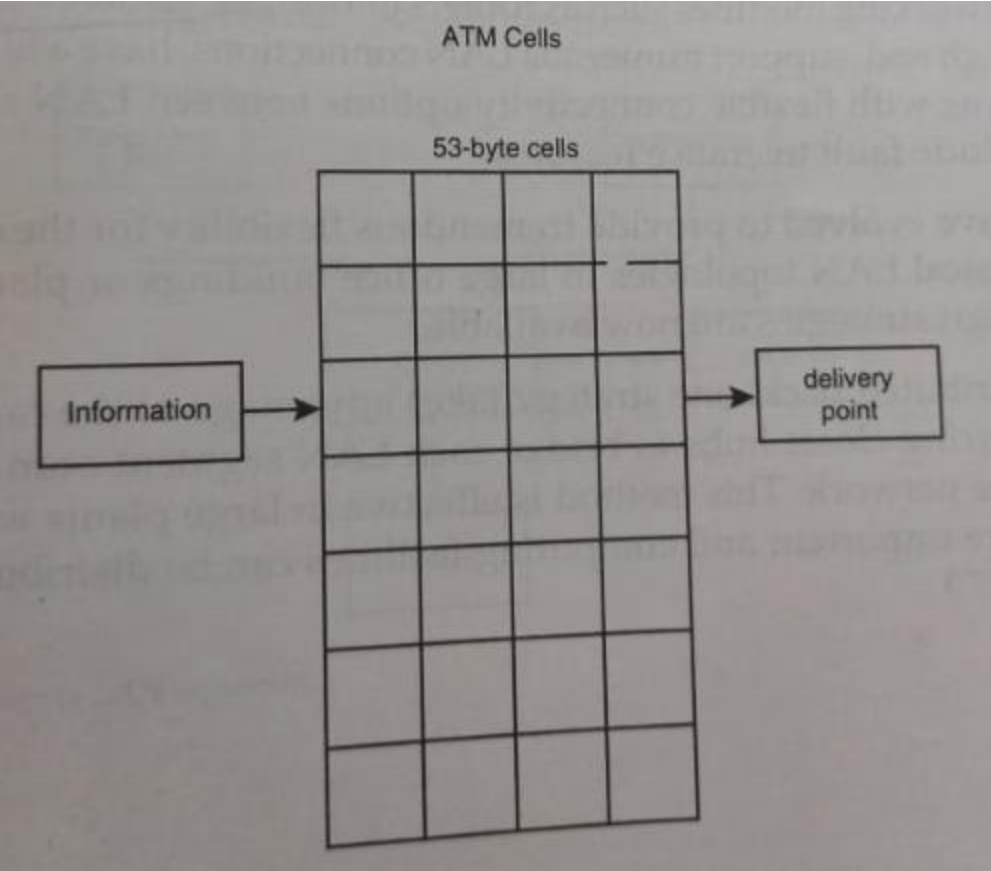
53-byte cells

Information → [Grid of 8 rows and 4 columns of 53-byte cells] → delivery point

ATM Cells


53-byte cells


Information → [Grid of 8 rows and 4 columns of 53-byte cells] → delivery point



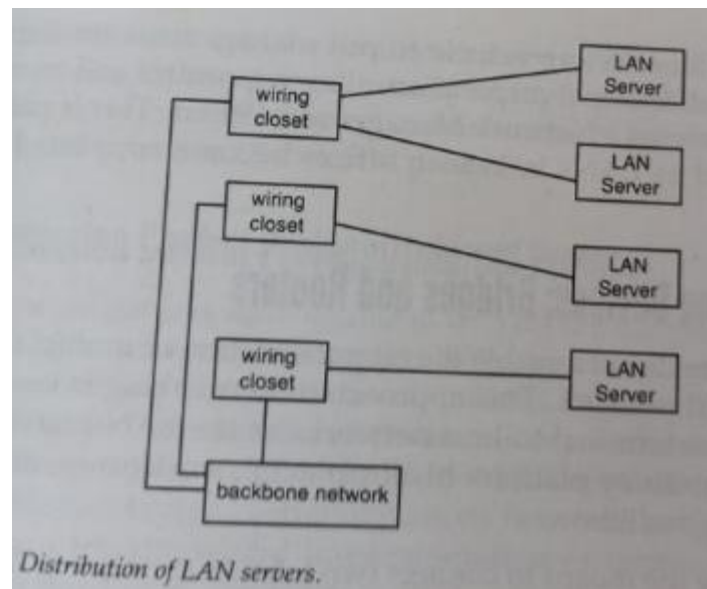
# Hubs

- One of the most important technologies in delivering LAN technology to mainstream information system architecture is the intelligent hub.
- Hubs provide integrated support for the different standard topologies (such as Ethernet, Token-Ring, and FDDI) over different types of cabling.
- By repeating or amplifying signals where necessary, they enable the use of high-quality UTP cabling in virtually every situation.

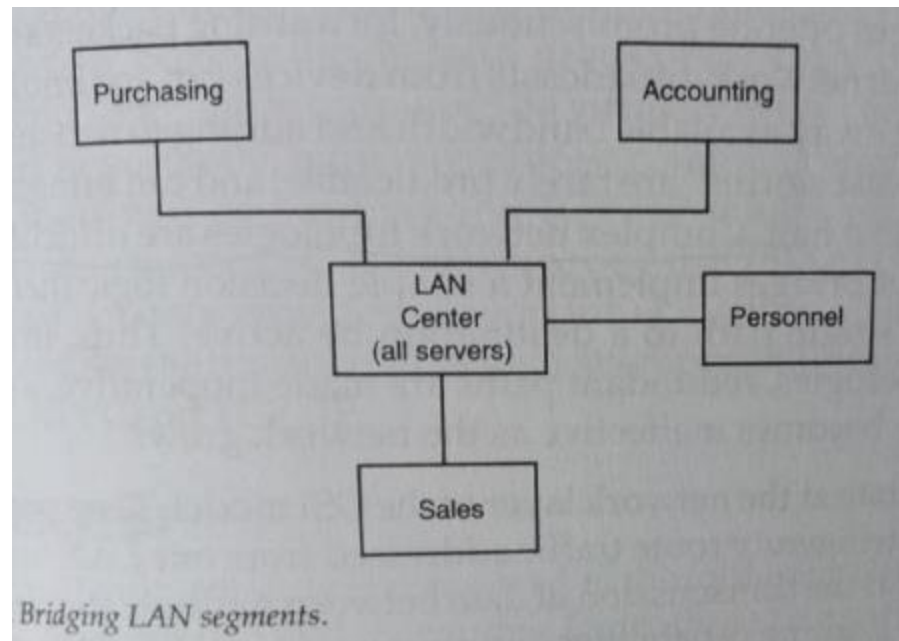
- 
- These intelligent hubs provide the necessary functionality to distribute a structured hardware and software system throughout networks, serve as network integration and control points, provide a single platform to support all LAN topologies, and deliver a foundation for managing all the components of the network.
  - There are three different types of hubs.
    - *Workgroup hubs*
    - *Wiring closet hubs*
    - *Network center hubs*

- 
- ***Workgroup hubs*** support one LAN segment and are packaged in a small footprint for small branch offices.
  - ***Wiring closet hubs*** support multiple LAN segments and topologies, include extensive management capabilities, and can house internetworking modules such as routers or bridges.
  - ***Network center hubs***, at the high end, support numerous LAN connections, have a high-speed backplane with flexible connectivity options between LAN segments, and include fault tolerance features.

- The **distributed backbone strategy** takes advantage of the capabilities of the wiring closet hubs to bridge each LAN segment onto a shared backbone network.
- This method is effective in large plants where distances are important and computing facilities can be distributed.




- Hubs also helps to put management intelligence throughout the LANs in a corporation, **allowing control and monitoring capabilities from a Network Management Center.**
- This is particularly important as LANs in branch offices become supported by a central group.






## **Internetworking Devices Bridges and Routers**

- Internetworking devices enable the interconnection of multiple LANs in an integrated network.
- This approach to networking is inevitable in the terminal-to-host networks as the LAN becomes the preferred connectivity platform to all personal, workgroup, or corporate computing facilities.

- 
- ***Bridges** provide the means to connect two LANs together, to extend the size of the LAN by dividing the traffic and enabling growth beyond the physical limitations of any one topology.*
  - Bridges **operate at the data link layer** of the OSI model, which makes them topology-specific.
  - Thus, **bridging can occur between identical topologies** only (Ethernet-to-Ethernet, Token Ring-to-Token Ring).
  - **Source-Route Transparent bridging**, a technology that enables bridging between Ethernet and Token-Ring LANs, is seldom used.
  - Limitations - In a large internetwork, broadcasts from devices can accumulate, effectively taking away available bandwidth and adding to network utilization.

- 
- **Routers** operate at the **network layer** of the **OSI model**.
  - They provide the means to **intelligently route traffic addressed from one LAN to another**.
  - They support the transmission of data between multiple standard LAN topologies.
  - Routing capabilities and strategies are inherent to each network protocol.
  - IP can be routed through the OSPF routing algorithm, which is different than the routing strategy for Novell's IPX/SPX protocol.
  - Intelligent routers can handle multiple protocols; most leading vendors carry products that can support mixes of Ethernet, Token Ring, FDDI, and from 8 to 10 different protocols.

# Transmission Control Protocol/Internet Protocol (TCP/IP)

- The TCP/IP protocol suite is now being used in many commercial applications.
- TCP/IP is specifically **designed to handle communications through "networks of interconnected networks."**
- It is the **de facto protocol for LAN-based Client/Server connectivity** and is supported on virtually every computing platform.
- More importantly, most interprocess communications and development tools embed support for TCP/IP where **multiplatform interoperability** is required.
- IBM provides support for TCP/IP on all its platforms and enables the transport of its own interoperability interfaces (such as CPIC, APPC) on TCP/IP.

# TCP/IP's Architecture

- The TCP/IP protocol suite is composed of the following components:
  - a network protocol (IP) and its routing logic,
  - three transport protocols (TCP, UDP, and ICMP), and
  - a series of session, presentation and application services.

## OSI Model

Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

Data Link Layer

Physical Layer

## TCP/IP Model

Application Layer

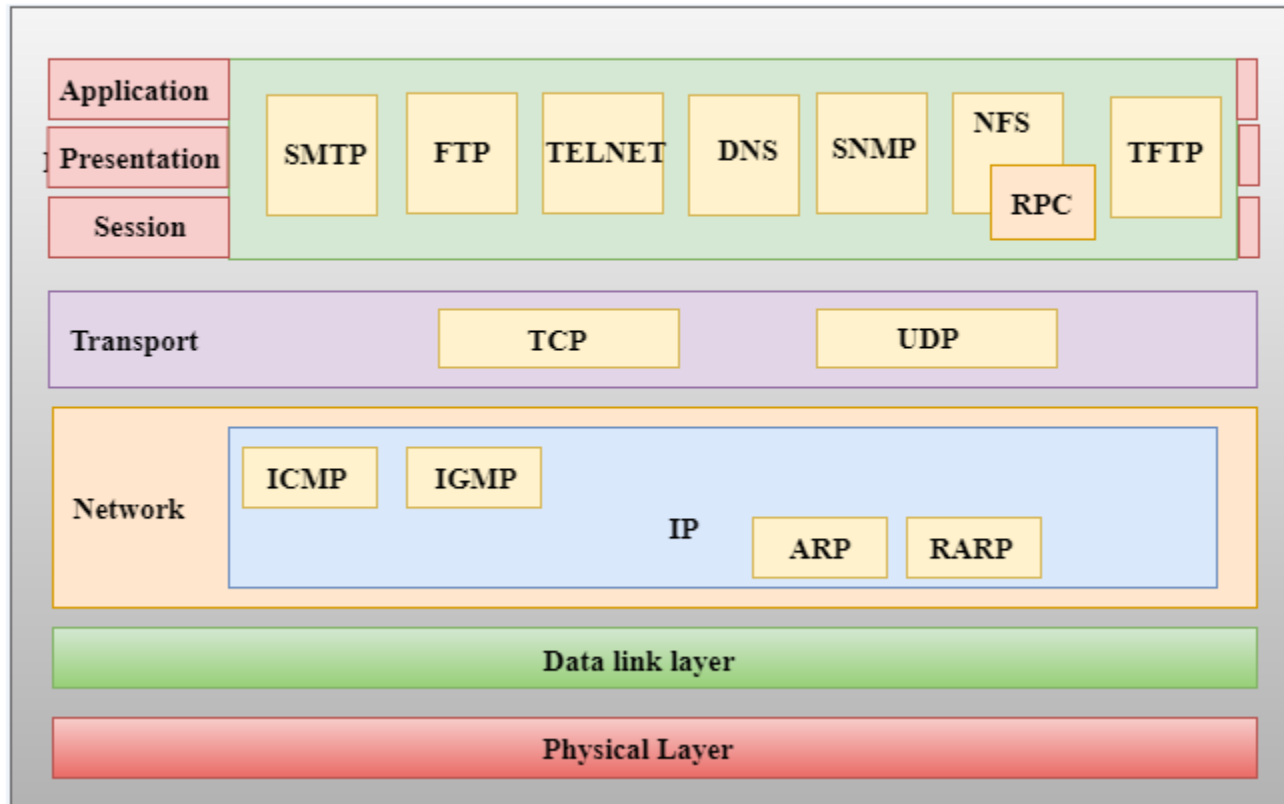
Transport Layer

Internet Layer

Network Access Layer



## Functions of TCP/IP layers:



# Internet Protocol

- IP represents the network layer and is equivalent to OSI's IP or X.25.
- A **unique network address is assigned to every system**, whether the system is connected to a LAN or a WAN.
- The system comes with its associated routing protocols and lower level functions such as network-to-physical **address resolution protocols (ARP)**.
- Commonly used **routing protocols** include RIP (Routing Information Protocol), OSPF, IGRP (Interior Gateway Routing Protocol), and Cisco's proprietary protocol.
- OSPF (**Open Shortest Path First**) has been adopted by the community to be the standards-based preferred protocol for large networks.



# Transport Protocols

- **TCP** provides Transport services over IP.
- It is **connection-oriented**, meaning it requires a session to be set up between two parties to provide its services.
- It ensures **end-to-end data transmission, error recovery, ordering of data, and flow control**.
- TCP provides the kind of communications that users and programs expect to have in locally connected sessions.
- **UDP** provides **connectionless transport services**, and is used in very specific applications that do not require end-to-end reliability such as that provided by TCP.

# Telnet

- Telnet is an application service that uses TCP.
- It provides **terminal emulation services and supports terminal-to-host connections** over an internetwork.
- It is composed of **two different portions: a client entity** that provides services to access hosts and a **server portion** that provides services to be accessed by clients.
- Even workstation operating systems such as OS/2 and Windows can provide telnet server support, thus **enabling a remote user to log onto the workstation using this method.**

# File Transfer Protocol (FTP)

- FTP uses TCP services to provide **file transfer services to applications**.
- FTP includes a **client and server portion**.
- Server FTP listens for a **session initiation request** from client FTP.
- Files may be transferred in either direction, and ASCII and binary file transfer is supported.
- FTP provides a simple means to perform **software distribution** to hosts, servers, and workstations.

# Simple Network Management Protocol (SNMP)

- SNMP provides intelligence and **services to effectively manage an internetwork**.
- It has been widely adopted by hub, bridge, and router manufacturers as the preferred technology to **monitor and manage their devices**.
- SNMP **uses UDP to support communications** between **agents** - intelligent software that runs in the devices - and the **manager**, which runs in the management workstation.
- Two basic forms of communications can occur:
  - **SNMP polling** (in which the manager periodically asks the agent to provide status and performance data) and
  - **trap generation** (in which the agent proactively notifies the manager that a change of status or an anomaly is occurring).

- **SNMP components –**

There are 3 components of SNMP:

- **SNMP Manager –**

It is a centralized system used to monitor network. It is also known as Network Management Station (NMS)

- **SNMP agent –**

It is a software management software module installed on a managed device. Managed devices can be network devices like PC, routers, switches, servers, etc.

- **Management Information Base –**

MIB consists of information on resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are essentially variables.

# Network File System (NFS)

- NFS enables a client to view, store, and update files on a remote computer as if they were locally stored.
- The NFS protocol enables the use of **IP** by servers **to share disk space and files** the same way a Novell or LAN Manager network server does.
- It is useful in environments in which servers are running different operating systems.
- However, it does not offer support for the same administration facilities that a NetWare environment typically provides.


# Simple Mail Transfer Protocol (SMTP)

- SMTP uses **TCP connections** to **transfer text-oriented electronic mail** among users on the same host or among hosts over the network.
- Developments are under way to adopt a standard to add multimedia capabilities (MIME) to SMTP.
- Its use is widespread on the Internet, where it enables any user to reach millions of users in universities, vendor organizations, standards bodies, and so on.
- Most electronic mail systems today provide some form of SMTP gateway to let users benefit from this overall connectivity.

# TCP/IP and Internetworks


- The interconnected LAN environment exhibits many of the same characteristics found in the environment for which TCP/IP was designed. In particular
- ***Routing:*** Internetworks need support for routing; routing is very efficient in TCP/IP environments with efficient protocols such as OSPF.
- ***Connections versus Connectionless:*** LAN activity includes both; the TCP/IP protocol suite efficiently supports both within an integrated framework.




- 
- ***Administrative Load Sensitivity:*** A LAN administrative support is usually limited; contrary to IBM's SNA, TCP/IP environments contain a tremendous amount of dynamic capabilities, in which **devices and networks are dynamically discovered, and routing tables are automatically maintained and synchronized.**
  - ***Networks of Networks:*** TCP/IP provides extreme flexibility as the administrative approach to the management of federations of networks. Taking advantage of its dynamic nature, it **enables very independent management of parts of a network.**

# Hardware/Network Acquisition


- Before selecting client hardware for end users, organizations should **define standards for classes of users.**
- This set of standards simplifies the selection of the appropriate client hardware for a user and allows buyers to arrange purchasing agreements to gain volume pricing discounts.
- There are a number **of issues to consider when selecting the client workstation, including processor type, coprocessor capability, internal bus structure, size of the base unit, and so on.**
- One of the most overlooked regarding client/server applications is the use of a GUI.

- 
- GUI applications require VGA or better screen drivers.
  - Screens, larger than the 15-inch PC standard, are required for users who normally display several active windows at one time; the more windows active on-screen, the larger the monitor viewing area requirements.
  - **The use of image, graphics, or full-motion video requires a large screen with very high resolution for regular usage.**
  - It is important to remember that productivity is dramatically affected by inability to easily read the screen all day.
  - Inappropriate resolution will lead to fatigue and inefficiency.

- 
- The enterprise on the desk requires that **adequate bandwidth be available to provide responsiveness** to the desktop user.
  - If **regular access to off LAN data** is required, a **router based internetworking** implementation will be required.
  - If only occasional off LAN access is required, bridges can be used.
  - Routers provide the additional advantage of support for multiprotocol internetworking.

# PC-Level Processing Units

- Client/server applications vary considerably in their client processing requirements and their I/O demands on the client processor and server.
- In general, **clients that support protected-mode addressing should be purchased.**
- This implies the use of 32-bit processors - with a 16-bit I/O bus if the I/O requirement is low.
- Low means the client isn't required to send and receive large amounts of data, such as images, which could be 100K bytes or larger, on a constant basis.

- 
- As multiwindowed and multimedia applications become prevalent during 1994, many applications will require the bandwidth only provided by a 32-bit I/O bus using VESA VL-bus or Intel PCI technology.
  - Windowed applications require considerable processing power to provide adequate response levels.
  - The introduction of application integration via DCE, OLE, and DOE significantly increases the processing requirements at the desktop.
  - The recommended minimum configuration for desktop processors has the processing capacity of a 33Mhz Intel 486SX.
  - By early 1995, the minimum requirement will be the processing capacity of a 50Mhz Intel 486DX or a 33Mhz Intel Pentium.


# X-Terminals


- X-terminals provide the **capability to perform only presentation services** at the workstation.
- Processing services are provided by another UNIX, Windows 3.x, NT, OS/2 2.x, or VMS server.
- Database, communications, and applications services are provided by the same or other servers in the network.
- The minimum memory configuration requirement for an X-terminal used in a client/server application is **4-8 Mbytes RAM**, depending on the number of open windows.

# Server Hardware

- Server requirements vary according to the complexity of the application and the distribution of work.
- Because servers are multiuser devices, the **number of active users is also a major sizing factor.**
- Servers that provide for 32-bit preemptive multitasking operating systems with storage protection are preferred in the multiuser environment.



- 
- Intel-based tower PCs and Symmetric Multi-Processors (SMPs) are commonly used for workgroup LANs with file and application service requirements.
  - Most PC vendors provide a 66Mhz Intel 486DX or Intel Pentium for this market in 1994.
  - SMP products are provided by vendors such as IBM, Compaq, and NetFrame.
  - Traditional UNIX vendors, such as Sun, HP, IBM, and Pyramid provide server hardware for applications requiring UNIX stability and capacity for database and application servers and large workgroup file services.

- 
- **The SMP products, in conjunction with RAID disk technology,** can be configured to provide mainframe level reliability for client/server applications.
  - It is critical that the server be architected as part of the systems management support strategy to achieve this reliability.