JOMO KENYATTA UNIVERSITY OF AGRICULTURE & TECHNOLOGY

SCHOOL OF OPEN, DISTANCE & eLEARNING

IN COLLABORATION WITH

INSTITUTE OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

DEPARTMENT OF COMPUTING

ICS 3205 COMPUTER NETWORKS AND DISTRIBUTED SYSTEMS

LAST REVISION ON November 5, 2013

P.O. Box 62000, 00200
Nairobi, Kenya

ICS 3205 COMPUTER NETWORKS AND DISTRIBUTED SYSTEMS

Course description

Introduction to computer networks.
Types of computer networks; cable and wireless networks.
Network design process.
Network configurations.
Networks systems administration.
Distributed systems.
Distributed algorithms; mutual exclusion, deadlocks, election algorithms.

Course aims

To equip learners with appropriate skills in network concepts, principles and distributed systems applications.

Learning outcomes

At the end of this unit, the learner should be to:

1. Describe network hardware and software.
2. Design and implement computer networks.
3. Apply networking technologies in a distributed environment.

Instruction methodology

- Lectures
- Practicals.

Learning Resources

Whiteboard, computers, internet, books and journals.

Course Journals

IEEE software Engineering.

Assessment information

The module will be assessed as follows;

- 40% Continuous Assessment Test.
- 60% examination.

References

1. Computer Networks by Tanenbaum A.S. Prentice Hall. 2006
2. Distributed algorithms and protocols. Raynall M. John Wiley. 2006.

Contents

1 Computer networks and distributed systems **xi**

1.1 Objective: . . . xi

1.1.1 Advantages of networking . . . xii

1.1.2 The Disadvantages (Costs) of Networking . . . xii

1.2 Fundamental Network Classifications . . . xii

1.3 Intranet and Internet Specifications . . . xiii

1.3.1 Client and Server computer role in networking . . . xv

1.3.2 Client/Server Networking . . . xv

1.4 Network topology . . . xvii

1.4.1 Bus . . . xvii

1.4.2 Star Topology . . . xvii

1.4.3 Ring . . . xix

1.4.4 Mesh . . . xix

1.4.5 Advantages and Disadvantages of Network Topologies . . . xxi

1.5 Hardware, Software and Networks Peripherals (device) . . . xxi

1.5.1 Network Interface Card (NIC) . . . xxi

- Preparing Data . . . xxii
- Sending and Controlling Data . . . xxii
- Compatibility . . . xxiii
- Performance . . . xxiii
- Repeaters . . . xxiii
- Hubs . . . xxiv
- Bridges . . . xxiv
- Routers . . . xxvi
- Switch . . . xxvi

2 Network Models **xxix**

2.1 Information Age xxix
2.1.1 Three Faces of Networking xxx
2.2 History of Information Systems xxxi
2.2.1 Multi-layer Network Models xxxi
2.2.2 7-Layer Model of OSI xxxi
2.2.3 Internet's 5-Layer Model xxxii
2.2.4 Comparison of Network Models xxxiii
2.2.5 Message Transmission Using Layers xxxiii
2.3 Protocols xxxiv
2.4 Important Points to Observe xxxiv
2.5 Standards xxxiv
2.5.1 Standardization Processes xxxv
2.5.2 Major Standards Bodies xxxv
2.6 Emerging Trends in Networking xxxvi
• Pervasive Networking xxxvi
• Integration of Voice, Video & Data xxxvii
• New Information Services xxxvii
• Implications for Management xxxvii

3 Network Design **xxxix**
3.1 Outline xxxix
3.2 Traditional Network Design xxxix
3.2.1 Inadequacy of Traditional Design xxxix
3.3 Building Block Network Design xl
3.3.1 Phases of Building Block Design xl
• Objective of Needs Analysis xli
• First Step in Needs Analysis xlii
• Next Step in Needs Analysis xlii
3.4 Design Process xlii
3.5 Application Systems xliii
3.6 Network Users xliii
3.6.1 Categorizing Network Needs xliv
3.6.2 Deliverables xliv
3.7 Technology Design xliv

3.7.1 Designing Clients and Servers . . . xlv
3.7.2 Designing Circuits and Devices . . . xlv
3.7.3 Estimating Circuit Traffic . . . xlvi
3.7.4 Capacity Overbuilding Dilemma . . . xlvi
3.7.5 Network Design Tools . . . xlvii
3.7.6 Simulation . . . xlvii
3.7.7 Deliverables . . . xlviii
3.7.8 Cost Assessment . . . xlviii
3.8 Request for Proposal (RFP) . . . xlix
3.8.1 Outline for Request for Proposals . . . xlix
3.8.2 Vendor Selection Process . . . l
3.8.3 Selling the Proposal to Management . . . l
3.8.4 Deliverables . . . li

4 Designing for Network Performance liii
4.1 Managed Networks . . . liii
4.2 Network Management Software . . . liv
• Network Management Standards . . . liv
4.3 Policy-Based Management . . . lv
4.4 Network Circuits . . . lv
4.5 Network Devices . . . lvi
4.5.1 Device Latency . . . lvi
4.5.2 Device Memory . . . lvi
4.5.3 Load Balancing . . . lvii
4.5.4 Minimizing Network Traffic . . . lvii
4.5.5 Content Caching . . . lviii
• Network with Content Engine . . . lviii
4.5.6 Content Delivery . . . lviii
• Benefits of Content Delivery . . . lix
4.5.7 Implications for Management . . . lix

5 Application Layer lxii
5.1 Outline . . . lxii
5.2 Application Layer - Introduction . . . lxii
5.2.1 Functions of Applications . . . lxii

5.3 Application Architectures lxiii
5.3.1 Host-Based Architectures lxiii
5.3.2 Problems with Host-based Arch lxiii
5.3.3 Problems with Client-Based Arch. lxiv
• Client-Server Architectures lxv
5.3.4 Client-Server Architectures lxv
• Advantages lxv
• Disadvantages lxv
• Multi-tier Architectures lxvi
• 3-tier Architecture lxvi
• N-tier Architecture 2 - 14 lxvii
• Multi-tier Architectures lxvii
•.1 Advantages lxvii
•.2 Disadvantages lxvii
• Fat vs. Thin Clients lxviii
• Thin-Client Example: Web Architecture lxviii
• Criteria for Choosing Architecture lxviii
• Choosing an Architecture lxix
5.3.5 Applications lxix
• World Wide Web lxx
• How the Web Works lxx
• HTTP Request Message lxxi
• HTTP Response Message lxxi
• Example of an HTTP Response lxxii
• HTML - Hypertext Markup Language lxxii
• Two-Tier E-mail Architecture lxxii
• File Transfer Protocol (FTP) lxxiii
• Telnet lxxiii
• Instant Messaging (IM) lxxiv
• How Instant Messaging Works lxxiv
• Webcasting lxxv
• Implications for Management lxxv

6 Physical Layer **lxxviii**

6.1 Outline lxxviii
6.2 Overview lxxviii
6.3 Types of Data Transmitted lxxix
6.4 Types of Transmission lxxix
6.4.1 Digital Transmission: Advantages lxxx
6.5 Circuit Configuration lxxx
6.6 Communications Media lxxxi
6.6.1 Twisted Pair (TP) Wires lxxxi
6.6.2 Fiber Optic Cable lxxxi
• Types of Optical Fiber lxxxii
6.7 Wireless Media lxxxii
6.8 Factors Used in Media Selection lxxxiii
6.9 Digital Transmission of Digital Data lxxxiii
6.9.1 Transmission Modes lxxxiv
• Signaling of Bits lxxxiv
• Signaling (Encoding) Techniques lxxxv
6.10 Analog Transmission of Digital Data lxxxv

7 Modulation **lxxxvii**
7.1 Modem - Modulator/demodulator lxxxvii
7.1.1 Digital Transmission of Analog Data lxxxviii
7.2 Distributed Deadlock lxxxviii
7.2.1 Deadlocks in distributed systems lxxxviii
7.2.2 Centralized deadlock detection lxxxix
7.2.3 Distributed deadlock detection xc
7.2.4 Distributed deadlock prevention xcii

8 Distributed Systems **xciv**
8.1 Outline xciv
8.2 What is Distributed? xciv
8.3 History of Distributed Computing xciv
8.4 Centralised System Characteristics xcv
8.5 Distributed System Characteristics xcv
8.6 Model of a Distributed System xcvi
8.6.1 Examples of Distributed Systems xcvi

8.7 Common Characteristics xcvii
8.7.1 Resource Access and Sharing xcviii
8.7.2 Openness xcviii
8.7.3 Concurrency xcviii
8.7.4 Scalability xcix
8.7.5 Fault Tolerance xcix
8.7.6 Transparency xcix
8.7.7 Access Transparency c
8.7.8 Location Transparency c
8.7.9 Migration Transparency c
8.7.10 Replication Transparency ci
8.7.11 Concurrency Transparency ci
8.7.12 Scalability Transparency ci
8.7.13 Performance Transparency ci
8.7.14 Failure Transparency cii
8.8 Dimensions Of Transparency cii

9 Metropolitan and Wide Area Networks civ
9.1 Introduction cv
9.1.1 Introduction (Cont.) cv
9.1.2 Services Used by MANs/WANs cv
9.1.3 Circuit Switched Services cvi
9.2 Basic Architecture of Circuit Switched Services cvi
9.2.1 Broadband ISDN cvi
• Circuit Switched Services cvii
• Ring Architecture cvii
9.2.2 Star Architecture cviii
• Packet Switching Concepts cviii
• Packet Routing Methods cix
• Ethernet/IP Packet Networks cix
• VPN Types cx
• MAN/WAN Design Practices cx
• Improving MAN/WAN Performance cxi
• Improving Device Performance cxi

- Improving Circuit Capacity cxi

9.2.3 Reducing Network Demand cxii

- Implications for Management cxii

10 Mutual Exclusion & Election Algorithms **cxiv**

10.1 Process Synchronization cxiv

10.2 Distributed Mutual Exclusion cxiv

10.2.1 Centralized algorithm cxiv

- Benefits cxv
- Problems cxv

10.2.2 Token Ring algorithm cxv

10.2.3 Ricart & Agrawala algorithm cxvi

10.2.4 Election Algorithms cxvii

10.2.5 Wireless Environments cxvii

10.2.6 Very Large Scale Networks cxviii

Solutions to Exercises cxx

LESSON 1

Computer networks and distributed systems

1.1. Objective:

To be acquainted with:

- The definitions of networking
- Network topology
- Network peripherals, hardware and software

Definition 1. Network

- A network can be defined as two or more computers connected together in such a way that they can share resources.
- The purpose of a network is to share resources.

A resource may be:

- A file
- A folder
- A printer
- A disk drive
- Or just about anything else that exists on a computer.

A network is simply a collection of computers or other hardware devices that are connected together, either physically or logically, using special hardware and software, to allow them to exchange information and cooperate. Networking is the term that describes the processes involved in designing, implementing, upgrading, managing and otherwise working with networks and network technologies.

1.1.1. Advantages of networking

- Connectivity and Communication
- Data Sharing
- Hardware Sharing
- Internet Access
- Internet Access Sharing
- Data Security and Management
- Performance Enhancement and Balancing
- Entertainment

1.1.2. The Disadvantages (Costs) of Networking

- Network Hardware, Software and Setup Costs
- Hardware and Software Management and Administration Costs
- Undesirable Sharing
- Illegal or Undesirable Behavior
- Data Security Concerns

1.2. Fundamental Network Classifications

Local Area Networks (LANs)

A local area network (LAN) is a computer network covering a small geographic area, like a home, office, or group of buildings

Wide Area Networks (WANs)

Wide Area Network (WAN) is a computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries). Or, less formally, a network that uses routers and public communications links The largest and most well-known example of a WAN is the Internet. WANs are used to connect LANs and other types of networks together, so that users

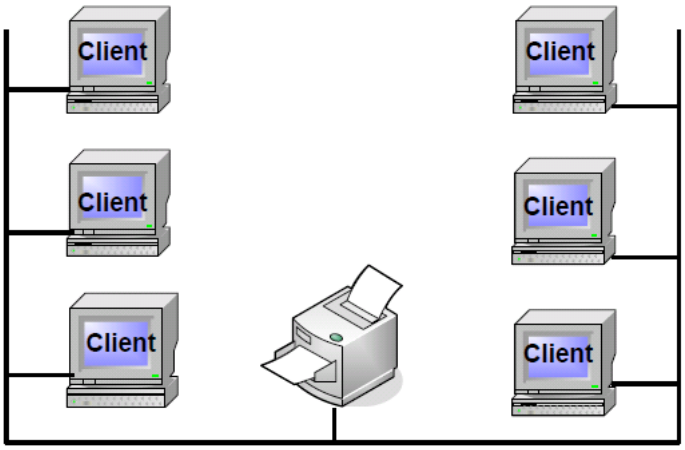


Figure 1.1: Local Area Networks

and computers in one location can communicate with users and computers in other locations

Metropolitan Area Network (MAN)

A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN). The term is applied to the interconnection of networks in a city into a single larger network (which may then also offer efficient connection to a wide area network). It is also used to mean the interconnection of several local area networks by bridging them with backbone lines. The latter usage is also sometimes referred to as a campus network.

1.3. Intranet and Internet Specifications

- **Intranet:** An intranet is a private network that is contained within an enterprise. It may consist of many interlinked local area networks and also use leased lines in the wide area network.

- An intranet uses TCP/IP, HTTP, and other Internet protocols and in general looks like a private version of the Internet. With tunneling, companies can send private messages through the public network, using the public network with special encryption/decryption and other security safeguards to connect one part of their intranet to another.

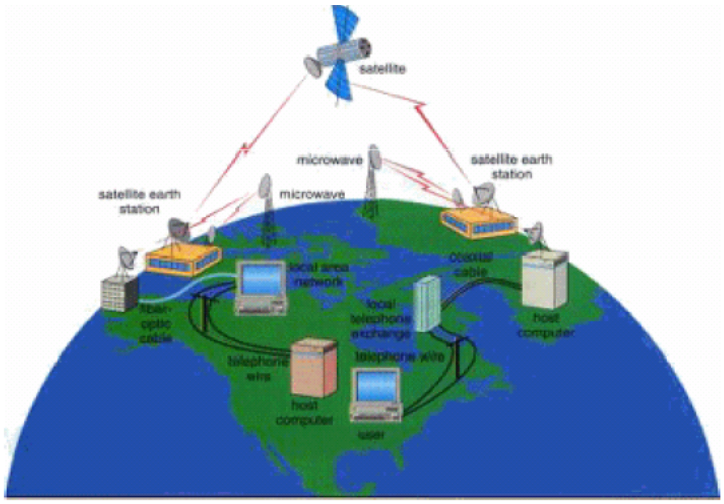


Figure 1.2: Wide Area Networks

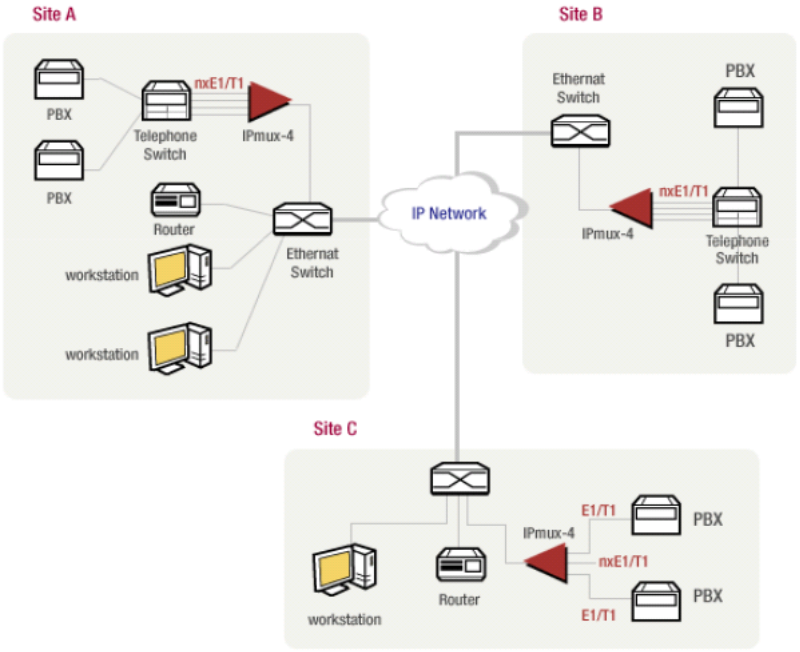


Figure 1.3: Metropolitan Area Network

- **Internet:** is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers).

1.3.1. Client and Server computer role in networking

- **Server** computer is a core component of the network, providing a link to the resources necessary to perform any task.
- A server computer provides a link to the resources necessary to perform any task.
- The link it provides could be to a resource existing on the server itself or a resource on a client computer.
- **Client** computers normally request and receive information over the network client. Client computers also depends primarily on the central server for processing activities.

1.3.2. Client/Server Networking

• In this design, a small number of computers are designated as centralized servers and given the task of providing services to a larger number of user machines called clients

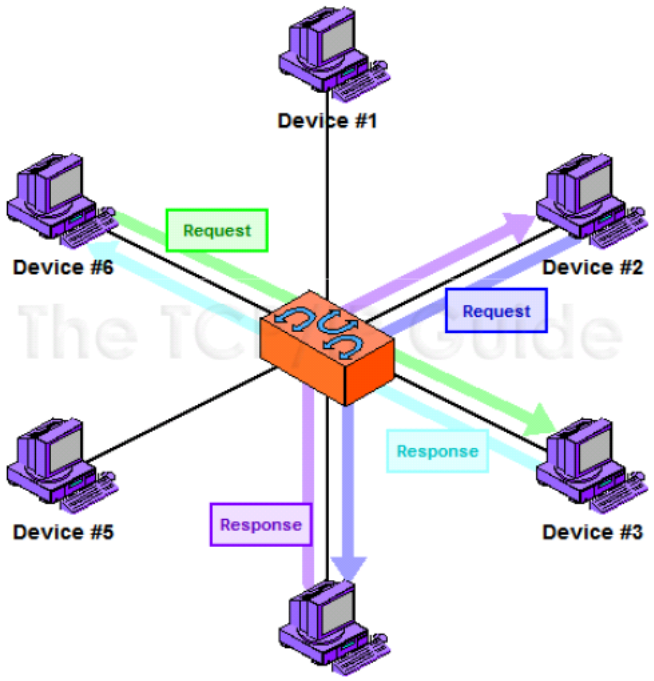
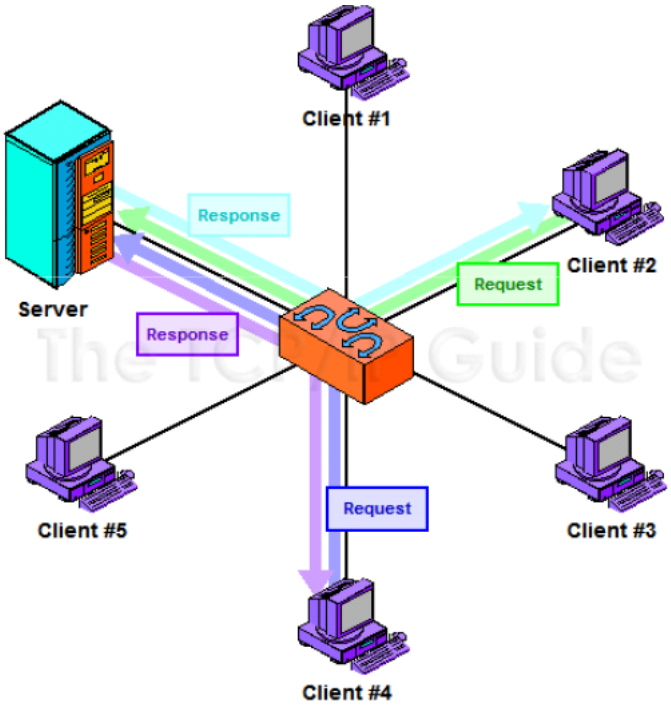


Figure 1.4: Peer-to peer network



1.4. Network topology

A topology is a way of "laying out" the network. Topologies can be either physical or logical.

1. *Physical topologies* describe how the cables are run.
2. *Logical topologies* describe how the network messages travel

- Bus (can be both logical and physical)
- Star (physical only)
- Ring (can be both logical and physical)
- Mesh (can be both logical and physical)

1.4.1. Bus

A bus is the simplest physical topology. It consists of a single cable that runs to every workstation This topology uses the least amount of cabling, but also covers the shortest amount of distance. Each computer shares the same data and address path. With a logical bus topology, messages pass through the trunk, and each workstation checks to see if the message is addressed to itself. If the address of the message matches the workstation's address, the network adapter copies the message to the card's on-board memory. It is difficult to add a workstation have to completely reroute the cable and possibly run two additional lengths of it. if any one of the cables breaks, the entire network is disrupted. Therefore, it is very expensive to maintain.

1.4.2. Star Topology

A physical star topology branches each network device off a central device called a hub, making it very easy to add a new workstation. Also, if any workstation goes down it does not affect the entire network. (But, as you might expect, if the central device goes down, the entire network goes down.)
Star topologies are easy to install. A cable is run from each workstation to the hub. The hub is placed in a central location in the office. Star topologies are more expensive to install than bus networks, because there are several more cables that need to be installed, plus the cost of the hubs that are needed.

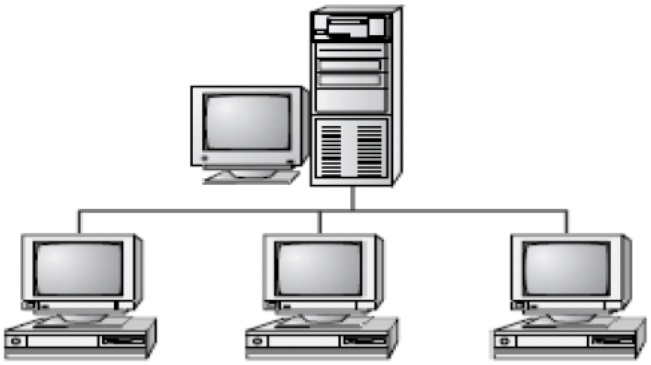


Figure 1.5: Bus Topology

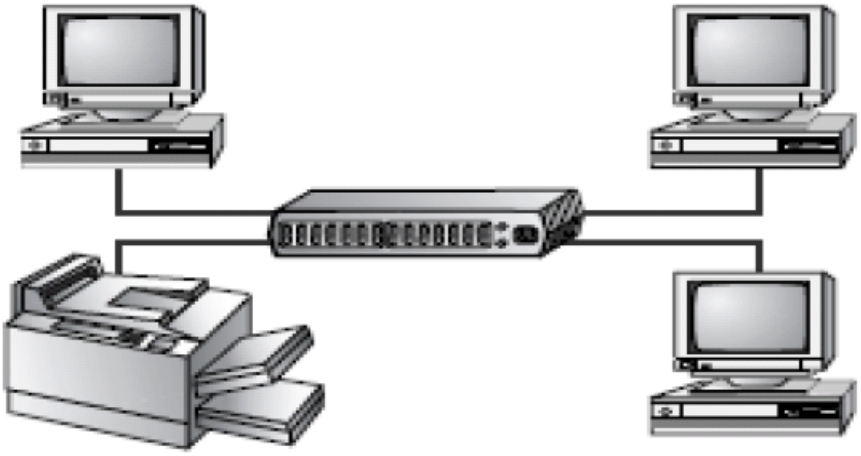


Figure 1.6: Star Topology

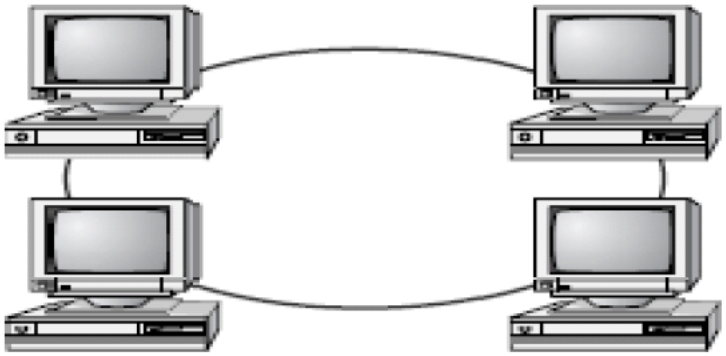


Figure 1.7: Ring Topology

1.4.3. Ring

Each computer connects to two other computers, joining them in a circle creating a unidirectional path where messages move workstation to workstation. Each entity participating in the ring reads a message, then regenerates it and hands it to its neighbor on a different network cable.
The ring makes it difficult to add new computers. Unlike a star topology network, the ring topology network will go down if one entity is removed from the ring. Physical ring topology systems don't exist much anymore, mainly because the hardware involved is fairly expensive and the fault tolerance is very low.

1.4.4. Mesh

The mesh topology is the simplest logical topology in terms of data flow, but it is the most complex in terms of physical design. In this physical topology, each device is connected to every other device This topology is rarely found in LANs, mainly because of the complexity of the cabling. If there are x computers, there will be
$(x \times (x-1)) \div 2$cables in the network. For example, if you have five computers in a mesh network, it will use $5 \times (5-1) \div 2$, which equals 10 cables. This complexity is compounded when you add another workstation. For example, your five-computer, 10-cable network will jump to 15 cables just by adding one more computer. Imagine how the person doing the cabling would feel if you told them you had to cable 50 computers in a mesh network - they'd have to come up with
$50 \times (50-1) \div 2 = 1225$ cables!
Because of its design, the physical mesh topology is very expensive to install and

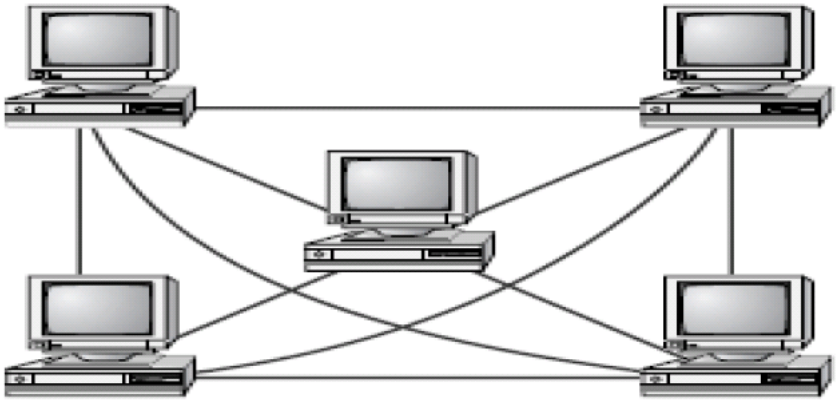


Figure 1.8: Mesh topology

maintain. Cables must be run from each device to every other device. The advantage you gain from it is its high fault tolerance. With a logical mesh topology, however, there will always be a way of getting the data from source to destination. It may not be able to take the direct route, but it can take an alternate, indirect route. It is for this reason that the mesh topology is still found in WANs to connect multiple sites across WAN links. It uses devices called routers to search multiple routes through the mesh and determine the best path. However, the mesh topology does become inefficient with five or more entities.

1.4.5. Advantages and Disadvantages of Network Topologies

Topology	Advantages	Disadvantages
Bus	Cheap. Easy to install.	Difficult to reconfigure. Break in bus disables entire network.
Star	Cheap. Easy to install. Easy to reconfigure. Fault tolerant.	More expensive than bus.
Ring	Efficient. Easy to install.	Reconfiguration difficult. Very expensive.
Mesh	Simplest. Most fault tolerant.	Reconfiguration extremely difficult. Extremely expensive. Very complex.

1.5. Hardware, Software and Networks Peripherals (device)

- Network Interface Card (NIC)
- Repeater
- Hub
- Bridge
- Routers
- Switch

1.5.1. Network Interface Card (NIC)

NIC provides the physical interface between computer and cabling. It prepares data, sends data, and controls the flow of data. It can also receive and translate data into bytes for the CPU to understand.

The following factors should be taken into consideration when choosing a NIC:

1. Preparing data
2. Sending and controlling data
3. Configuration
4. Drivers
5. Compatibility
6. Performance

- **Preparing Data**
  - In the computer, data moves along buses in parallel, as on a four-lane interstate highway. But on a network cable, data travels in a single stream, as on a one lane highway. This difference can cause problems transmitting and receiving data, because the paths traveled are not the same.
  - It is the NIC's job to translate the data from the computer into signals that can flow easily along the cable.
  - It does this by translating digital signals into electrical signals (and in the case of fiber-optic NICs, to optical signals).
- **Sending and Controlling Data**
  - For two computers to send and receive data, the cards must agree on several things. These include the following:
    - The maximum size of the data frames
    - The amount of data sent before giving confirmation
    - The time needed between transmissions
    - The amount of time needed to wait before sending confirmation
    - The amount of data a card can hold
    - The speed at which data transmits
  - In order to successfully send data on the network, you need to make sure the network cards are of the same type and they are connected to the same piece of cable.

- **Compatibility**
  - When choosing a NIC, use one that fits the bus type of your PC. If you have more than one type of bus in your PC (for example, a combination ISA/PCI), use an NIC that fits into the fastest type (the PCI, in this case).
  - This is especially important in servers, as the NIC can very quickly become a bottleneck if this guideline isn't followed.
- **Performance**
  - The most important goal of the network adapter card is to optimize network performance and minimize the amount of time needed to transfer data packets across the network.
  - There are several ways of doing this, including assigning a DMA channel, use of a shared memory adapter, and deciding to allow bus mastering.
- **Repeaters**
  - Repeaters are very simple devices. They allow a cabling system to extend beyond its maximum allowed length by amplifying the network voltages so they travel farther.
  - Repeaters are nothing more than amplifiers and, as such, are very inexpensive.
  - Repeaters can only be used to regenerate signals between similar network segments.
  - For example, we can extend an Ethernet 10Base2 network to 400 meters with a repeater. But can't connect an Ethernet and Token Ring network together with one.
  - The main disadvantage to repeaters is that they just amplify signals. These signals not only include the network signals, but any noise on the wire as well.
  - Eventually, if you use enough repeaters, you could possibly drown out the signal with the amplified noise. For this reason, repeaters are used only as a temporary fix.

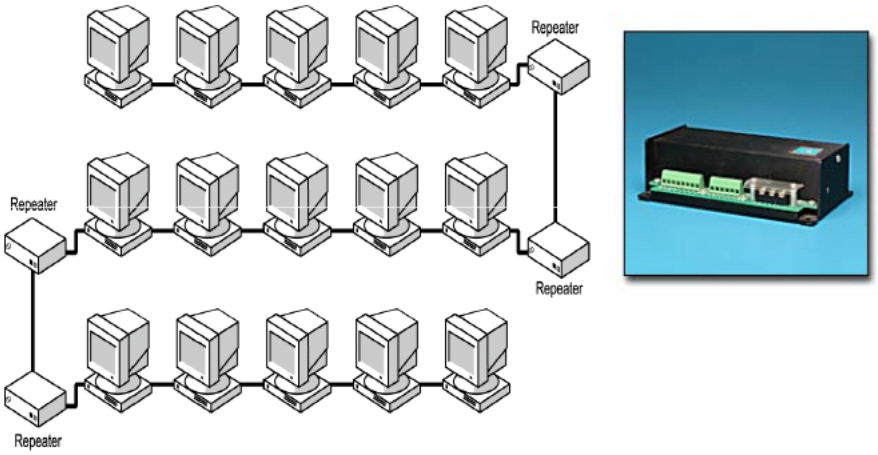


Figure 1.9: Repeaters

- **Hubs**
  - Hubs are devices used to link several computers together.
  - They repeat any signal that comes in on one port and copy it to the other ports (a process that is also called broadcasting).
  - There are two types of hubs: active and passive.
  - Passive hubs simply connect all ports together electrically and are usually not powered.
  - Active hubs use electronics to amplify and clean up the signal before it is broadcast to the other ports.
  - In the category of active hubs, there is also a class called “intelligent” hubs, which are hubs that can be remotely managed on the network.

- **Bridges**
  - They join similar topologies and are used to divide network segments.
  - For example, with 200 people on one Ethernet segment, the performance will be mediocre, because of the design of Ethernet and the number of workstations that are fighting to transmit. If you divide the segment into two seg-

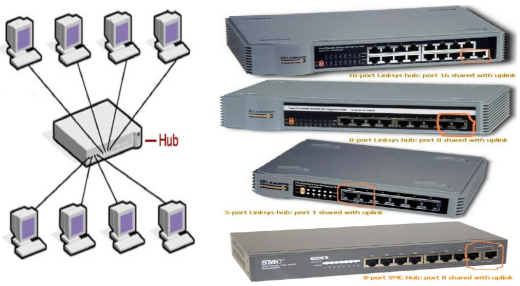


Figure 1.10: Hub

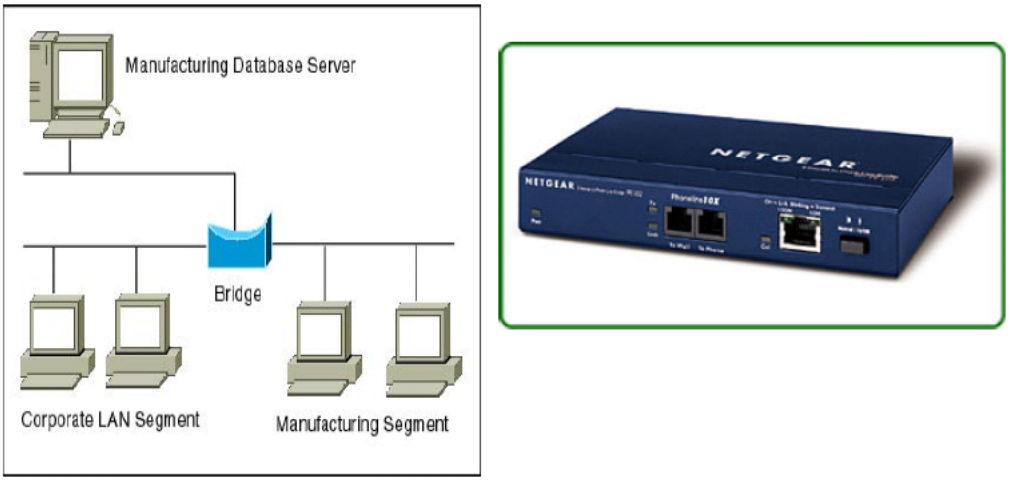


Figure 1.11: Bridges

ments of 100 workstations each, the traffic will be much lower on either side and performance will increase.

- If it is aware of the destination address, it is able to forward packets; otherwise a bridge will forward the packets to all segments. They are more intelligent than repeaters but are unable to move data across multiple networks simultaneously.
- Unlike repeaters, bridges can filter out noise.
- The main disadvantage to bridges is that they can't connect dissimilar network types or perform intelligent path selection. For that function, you would need a router.

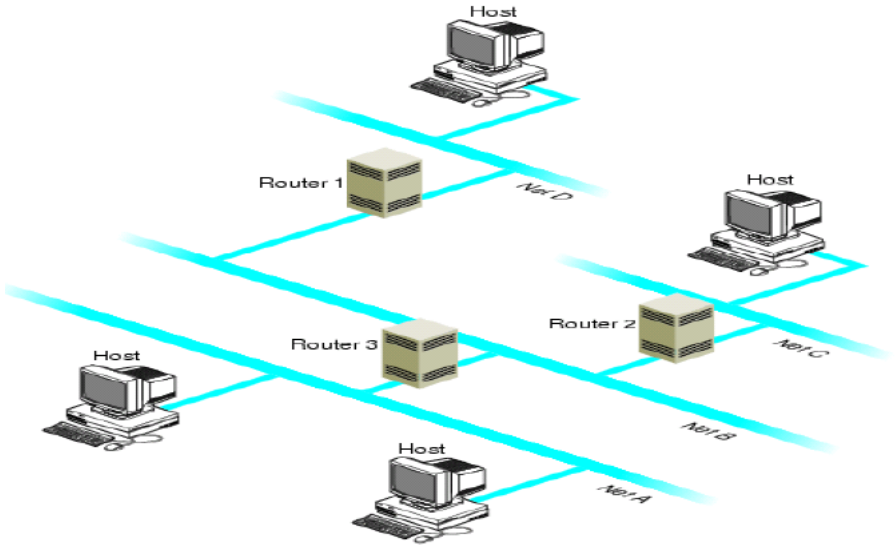


Figure 1.12: Router

- **Routers**
  - Routers are highly intelligent devices that connect multiple network types and determine the best path for sending data.
  - The advantage of using a router over a bridge is that routers can determine the best path that data can take to get to its destination.
  - Like bridges, they can segment large networks and can filter out noise.
  - However, they are slower than bridges because they are more intelligent devices; as such, they analyze every packet, causing packet-forwarding delays. Because of this intelligence, they are also more expensive.
  - Routers are normally used to connect one LAN to another.
  - Typically, when a WAN is set up, there will be at least two routers used.

- **Switch**
  - A network switch is a computer networking device that connects network segments.

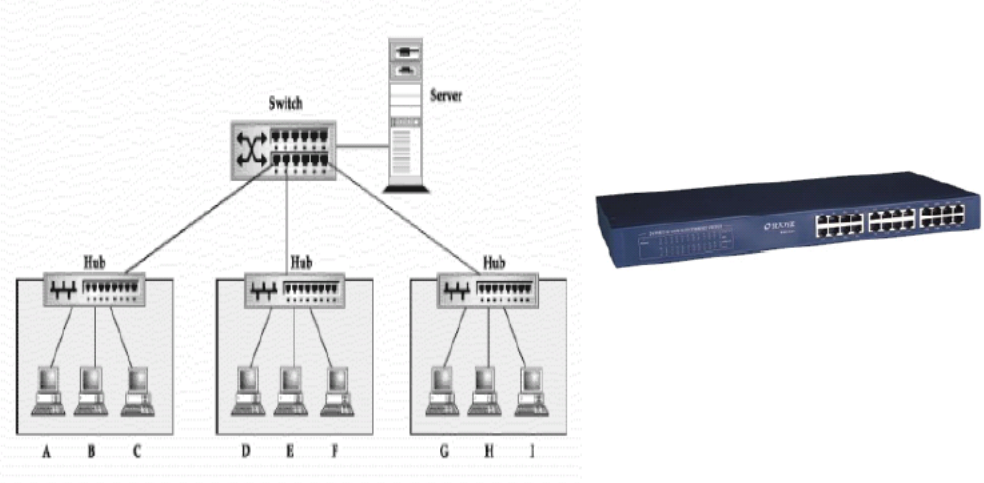


Figure 1.13: Switch

- Low-end network switches appear nearly identical to network hubs, but a switch contains more "intelligence" (and a slightly higher price tag) than a network hub.
- Network switches are capable of inspecting data packets as they are received, determining the source and destination device of that packet, and forwarding it appropriately.
- By delivering each message only to the connected device it was intended for, a network switch conserves network bandwidth and offers generally better performance than a hub.
- A vital difference between a hub and a switch is that all the nodes connected to a hub share the bandwidth among themselves, while a device connected to a switch port has the full bandwidth all to itself.
- For example, if 10 nodes are communicating using a hub on a 10-Mbps network, then each node may only get a portion of the 10 Mbps if other nodes on the hub want to communicate as well.
- But with a switch, each node could possibly communicate at the full 10 Mbps.

Revision Questions

EXERCISE 1. ✍ Connect 2 buildings 3 storey high with a distance of 500m between each building.

• Each floor is occupied by the Finance Department, Administration Department and Computing Department.

• Your report should have the following items. Anything extra is encouraged.

a. Introduction

b. Network Diagrams

c. Devices that will be used.

Example ✎. Define the term protocol.

Solution: Set of rules established for users to exchange information. □

EXERCISE 2. ✍ Define the term deterministic.

EXERCISE 3. ✍ What is the difference between a hub and a switch?

LESSON 2

Network Models

Network Models - OSI model, Internet model, Layers

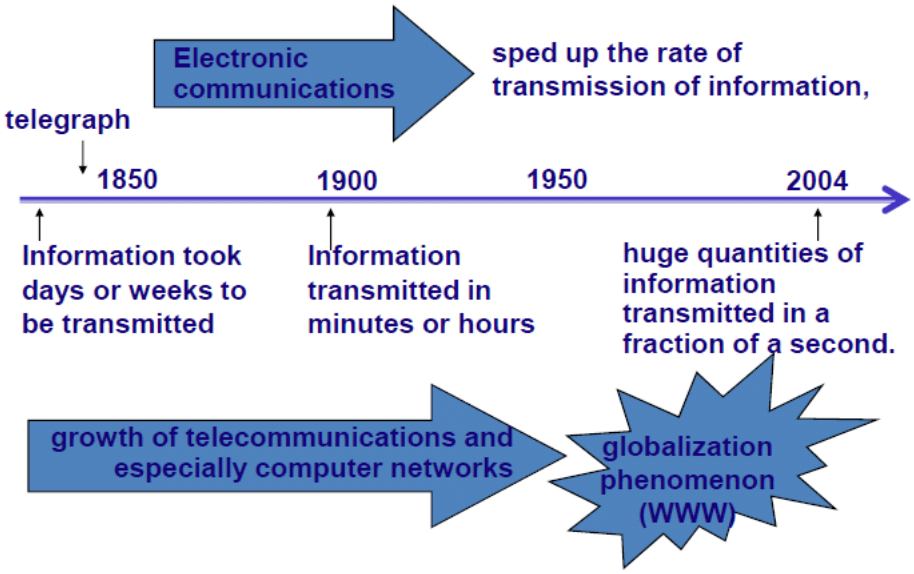
Network Standards - Standards making, common standards

Future Trends - Pervasive networking, integration of voice, video, and data, new information services

2.1. Information Age

- First Industrial Revolution
  - Introduction of machinery
  - New organizational methods
  - Changed the way people worked
- Second Industrial Revolution
  - Information Age
  - Introduction of computers
  - Introduction of networking and data communication
  - Changed the way people worked again
    - Faster communication Collapsing Information lag
    - Brought people together Globalization

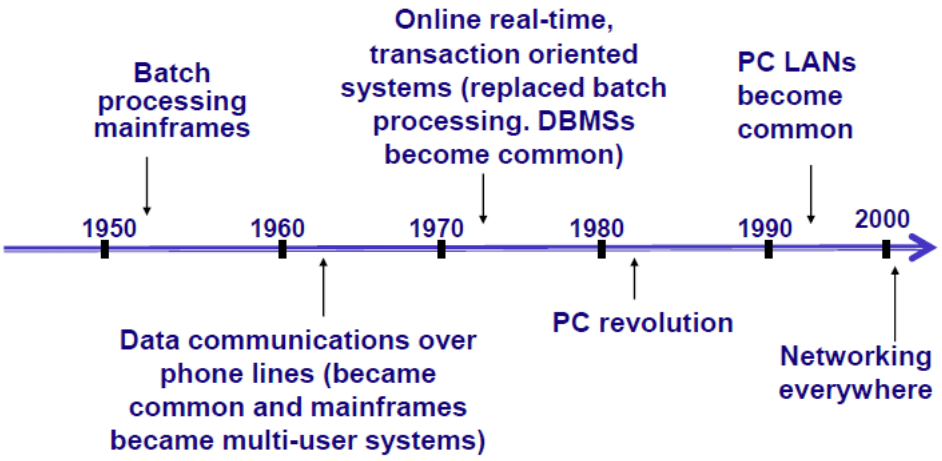
Collapsing Information Lag



2.1.1. Three Faces of Networking

1. Fundamental concepts of networking
    - How data moves from one computer to another over a network
    - Theories of how network operate
2. Technologies in use today
    - How theories are implemented, specific products
    - How do they work, their use, applications
3. Management of networking technologies
    - Security
    - Network Design
    - Managing the network

2.2. History of Information Systems



2.2.1. Multi-layer Network Models

- The two most important such network models: OSI and Internet
- Open Systems Interconnection Model
  - Created by International Standards Organization (ISO) as a framework for computer network standards in 1984
  - Based on 7 layers
- Internet Model
  - Created by DARPA originally in early 70's
  - Developed to solve to the problem of internetworking
  - Based on 5 layers
  - Based on Transmission Control Protocol/ Internet Protocol (TCP/IP) suite

2.2.2. 7-Layer Model of OSI

- Application Layer
  - set of utilities used by application programs
- Presentation Layer

  - formats data for presentation to the user
  - provides data interfaces, data compression and translation between different data formats

- Session Layer
  - initiates, maintains and terminates each logical session between sender and receiver

- Transport Layer
  - deals with end-to-end issues such as segmenting the message for network transport, and maintaining the logical connections between sender and receiver

- Network Layer
  - responsible for making routing decisions

- Data Link Layer
  - deals with message delineation, error control and network medium access control

- Physical Layer
  - defines how individual bits are formatted to be transmitted through the network

2.2.3. Internet's 5-Layer Model

- Application Layer
  - used by application program

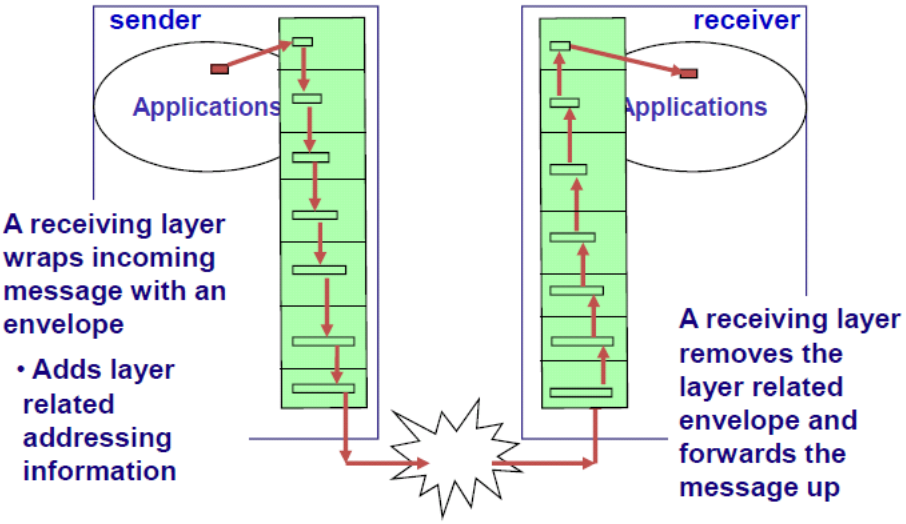
- Transport Layer
  - responsible for establishing end-to-end connections, translates domain names into numeric addresses and segments messages

- Network Layer - same as in OSI model
- Data Link Layer - same as in OSI model
- Physical Layer - same as in OSI model

2.2.4. Comparison of Network Models

OSI Model	Internet Model	Groups of Layers
7. Application Layer	5. Application Layer	*Application Layer*
6. Presentation Layer		
5. Session Layer		
4. Transport Layer	4. Transport Layer	*Internetwork Layer*
3. Network Layer	3. Network Layer	
2. Data Link Layer	2. Data Link Layer	*Hardware Layer*
1. Physical Layer	1. Physical Layer	

2.2.5. Message Transmission Using Layers



2.3. Protocols

- Used by Network model layers
- Sets of rules to define how to communicate at each layer and how to interface with adjacent layers

2.4. Important Points to Observe

- Many different software packages (protocols) and many different packets (at different layers)
  - Easy to develop new software
  - Simple to change the software at any level
- Matching layers communicate at different computers
  - Accomplished by standards
  - e.g., Physical layer at the sending computer must be the same in the receiving computer
- Somewhat inefficient
  - Involves many software and packets
  - –Packet overhead (slower transmission, processing time)

2.5. Standards

- Importance
  - Provide a “fixed” way for hardware and/or software systems (different companies) to communicate
  - Help promote competition and decrease the price
- Types of Standards
  - Formal standards
    - Developed by an industry or government standards-making body

  - De-facto standards
    * Emerge in the marketplace and widely used
    * Lack official backing by a standards-making body

2.5.1. Standardization Processes

- Specification
  - Developing the nomenclature and identifying the problems to be addressed
- Identification of choices
  - Identifying solutions to the problems and choose the "optimum" solution
- Acceptance
  - Defining the solution, getting it recognized by industry so that a uniform solution is accepted

2.5.2. Major Standards Bodies

1. ISO (International Organization for Standardization)
   - Technical recommendations for data communication interfaces
   - Composed of each country's national standards orgs.
   - Based in Geneva, Switzerland (www.iso.ch)
2. ITU-T (International Telecommunications Union
   - Telecom Group
   - Technical recommendations about telephone, telegraph and data communications interfaces
   - Composed of representatives from each country in UN
   - Based in Geneva, Switzerland (www.itu.int)

3. ANSI (American National Standards Institute)
    - Coordinating organization for US (not a standards- making body)
    - www.ansi.org
4. IEEE (Institute of Electrical and Electronic Engineers)
    - Professional society; also develops mostly LAN standards
    - standards.ieee.org
5. IETF (Internet Engineering Task Force)
    - Develops Internet standards
    - No official membership (anyone welcomes)
    - www.ietf.org

2.6. Emerging Trends in Networking

- Pervasive Networking
- Integration of Voice, Video and Data
- New Information Services

- **Pervasive Networking**
    - Means “Network access everywhere”
    - Exponential growth of Network use
    - Many new types of devices will have network capability
    - Exponential growth of data rates for all kinds of networking
    - Broadband communications – Use circuits with 1 Mbps or higher (e.g., DSL)

- **Integration of Voice, Video & Data**
  - Also called "Convergence" – Networks that were previously transmitted using separate networks will merge into a single, high speed, multimedia network in the near future
  - First step – Integration of voice and data
  - Next Step – Video merging with voice and data – Will take longer partly due to the high data rates required for video
- **New Information Services**
  - World Wide Web based – Many new types of information services becoming available
  - Services that help ensure quality of information received over www
  - Application Service Providers (ASPs) – Develop specific systems for companies
  - Providing and operating a payroll system for a company that does not have one of its own
  - Information Utilities (Future of ASPs) – Providing a wide range of info services (email, web, payroll, etc.) (similar to electric or water utilities)
- **Implications for Management**
  - Embrace change and actively seek to apply networks to improve what you do – Information moved quickly and easily anywhere and anytime – Information accessed by customers and competitors globally
  - Use a set of industry standard technologies – Can easily mix and match equipment from different vendors – Easier to migrate from older technologies to newer technologies – Smaller cost by using a few well known standards

Revision Questions

Example ✎**.** What is TCP / IP?

Solution: // TCP – Transmission Control ProtocolIP – Internetwork ProtocolTCP/IP refers to a collection of protocols. The name TCP/IP is misleading because TCP and IP are only two of the many protocols inthis collection of protocols.TCP is a reliable connection-oriented protocol with the following features:

1. Allows error-free transmission.
2. Incoming byte stream is fragmented into a number of shorter messages and these are passed on to the next layer.
3. At the receiving end the TCP reassembles the messages into an output stream
4. TCP also handles flow control – to control data transfer rate so that a slow receiver is not flooded with data from a fast sender.
5. A connection must be established between the sender and the receiver before transmission begins.
6. TCP creates a virtual circuit between sender and receiver for the duration of the transmission.
7. TCP begins each transmission by alerting the receiver that segments are on their way (connection establishment).
8. Each transmission is ended with connection termination. □

EXERCISE 4. ✍ Explain layer 3 and layer 4 of OSI model.

EXERCISE 5. ✍ Explain TCP/IP model.

EXERCISE 6. ✍ List two ways in which OSI and TCP/IP reference models are same and two ways in which they are different

EXERCISE 7. ✍ How do the layers of the TCP/IP model correlate to the layers of the OSI model?

LESSON 3

Network Design

3.1. Outline

- Introduction
  - Traditional Network Design
  - Building Block Network Design
- Needs Analysis
- Technology Design
- Cost Assessment
- Designing for Network Performance

3.2. Traditional Network Design

A structured systems analysis and design process

- **Network analysis phase** : Meeting with users to determine the needs and applications Estimating data traffic on each part of the network Designing circuits needed to support this traffic and obtains cost estimates
- **Implementation phase**: Building and implementing the network
- Works well for static and slowly evolving networks (although costly and time consuming).

3.2.1. Inadequacy of Traditional Design

Forces making the traditional design approach less appropriate for many of today's networks:

- Rapidly changing technology of computers, networking devices and the circuits
  - More powerful devices, much faster circuits

- Rapidly growing network traffic
  - Difficulty of estimating demand and growth - Shorter planning periods (3 years)
- Dramatic change in the balance of costs
  - Before: Equipment; now: staff
  - Design goal: Minimize the staff time to operate (not the hardware costs) E.g., use similar standardized equipment for the ease of management

3.3. Building Block Network Design

- A simpler new approach.
- Key concept:
  - Network that use a few standard components are cheaper than (in the long run) the networks that use many different components.
- Start with a few standard components with ample capacity (without extensive traffic analysis)
  - Called: narrow and deep (few types of devices, used over and over)
  - Result: simpler design process, easily managed network
- Phases of design
  - Needs analysis, Technology design, and Cost assessment
  - Cycles through, refining the outcome of each phase

3.3.1. Phases of Building Block Design

- Needs analysis
  - Understand current and future needs
    - Classify users and applications as typical or high volume
    - Identify specific technology needs

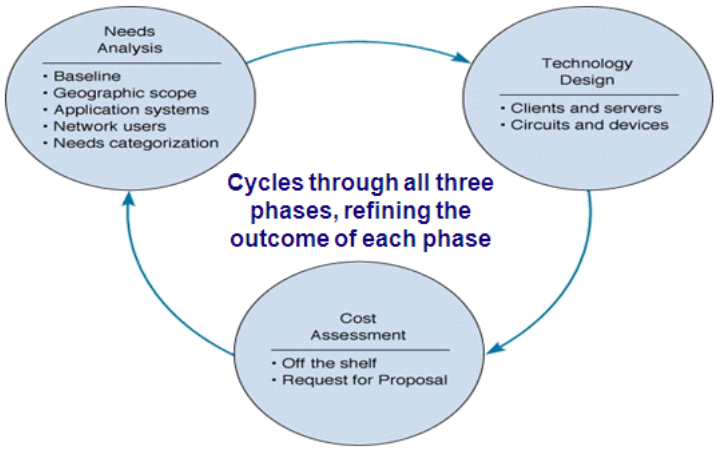


Figure 3.1: Building Block Network Design

- Technology design
  - Examine available technologies and asses which ones meet the needs
  - In case of difficulty in determining traffic needs, use more capacity (easy to grow)
- Cost assessment
  - Consider the relative cost of technology

- **Objective of Needs Analysis**
  - Objectives
    - Define the geographic scope of the network
    - Define applications and users that will use the network
  - The goal:
    - To produce a logical network design that
      - Describes what network elements will be needed to meet the organization's needs
      - Specifies no technologies nor products at this stage
      - Focuses on functionality (e.g., high speed access network)

- **First Step in Needs Analysis**

Break the network into three conceptual parts (based on their geographic and logical scope):

- Access layer - Lies closest to the user; often a LAN
- Distribution layer - Connects the access layer to the rest of the network; often a backbone network
- Core layer - Connects the different parts of the distribution layer together; often a WAN

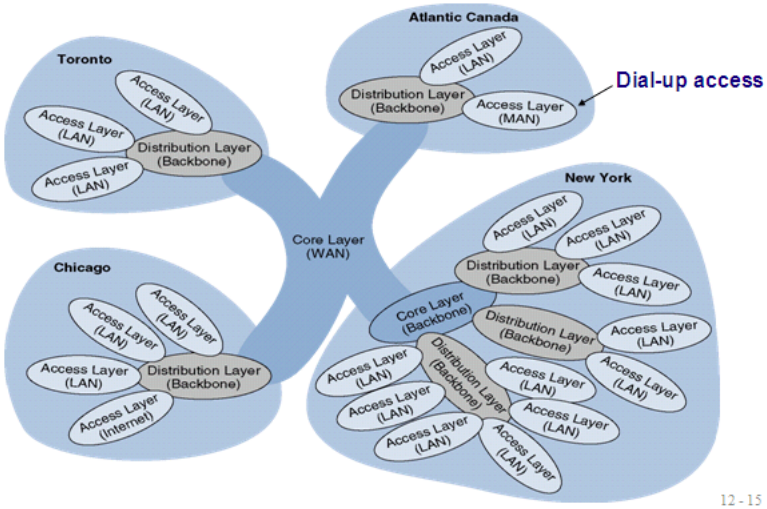
Not all layers present in all networks Small networks may not have a distribution layer

- **Next Step in Needs Analysis**
  - Identify basic technical constraint at each layer Examples: If access layer is
    - A MAN; then users need to use dial up lines
    - A LAN; no need to use T1 lines
  - Identify constraints imposed by the current network infrastructure Example: adding a new building to an existing office complex that use 100Base-T
    - Probably choose the same for new building

3.4. Design Process

- Start with the highest level - Begin by drawing a WAN connecting locations
- Next draw individual locations connected to WAN - Usually a series of diagrams, one for each location
- Gather information and characteristics of the environment - Legal requirements, regulations, building codes.

Geographic Scope



3.5. Application Systems

- Baselining
  - Review the applications currently used on the network and
  - Identify their location so they can be connected to the planned network.
- Include applications expected to be added to the network
  - Review long and short range plans.
- Also identify the hardware and software requirements and protocol type for each application
  - HTTP over TCP/IP; Windows file access

3.6. Network Users

Assess the number and type of users that will generate network traffic

- Much network traffic comes from Internet use (i.e., e-mail and WWW) In the past, application systems accounted for the majority of network traffic
- Future network upgrades will require understanding of the use of new applications Effect of video on network traffic

3.6.1. Categorizing Network Needs

Assess the traffic generated in each segment (for each application and user)

- Based on an estimate of the relative magnitude of network needs (i.e. typical vs. high volume)
- Can be problematic, but the goal is a relative understanding of network needs E.g, multimedia applications: high volume

Organize network requirements into
Mandatory, Desirable, and Wish-list requirements

- Enables development of a minimum level containing mandatory requirements (if cost is a constraint)

3.6.2. Deliverables

A set of logical network diagrams showing

- Applications
- Circuits
- Clients
- Severs

Categorized as “typical” or “high volume”. Just a conceptual plan for the network

- No physical elements specified

3.7. Technology Design

Development of a physical network (or set of possible designs)

- Specify the computers (Clients and servers) needed to support applications and users New computers Upgrades
- Specify circuits and devices (routers, gateways) to connect the computers

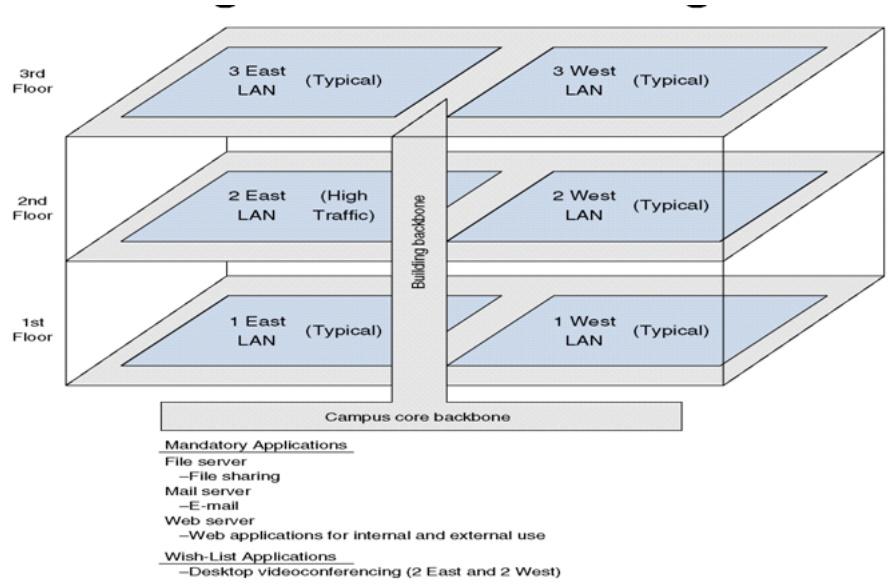


Figure 3.2: Logical Network Design

3.7.1. Designing Clients and Servers

Specification of the computers needed in terms of standard units

- Allocate “base level” client computers to “typical” users
- Allocate “base level” servers to typical applications
- Assign “advanced” computers to “high volume” users and servers
- Beware of the definition for a “typical” unit
  - Keeps changing as hardware costs continue to fall, and capabilities/capacities continue to increase

3.7.2. Designing Circuits and Devices

- Deciding on the fundamental technology and protocols e.g., Ethernet, ATM, TCP/IP
- Choosing the capacity each circuit will operate at
  - e.g., 10 Mbps, 100 Mbps, 1000 Mbps
  - Requires capacity planning

    * Assess current and future "circuit loading"
        · Amount of data to be transmitted on a circuit
        · Focus on either average or peak circuit traffic Ideal: Peak traffic
    * Estimate size and type of "standard" and "advanced" circuits for each LAN, BN, WAN Should "standard" LAN circuit be 10Base-T or higher

3.7.3. Estimating Circuit Traffic

- Average traffic: - Estimate total characters transmitted per day per circuit
- Peak traffic - Estimate maximum number of characters transmitted per two second interval
- Estimating Message volume - Count messages in a current network and multiply it with a growth rate Use analyzers if an existing network
- Precision not a major concern
    - Stair step nature of communication circuit (lease another line, or upgrade to 100Base-T)
    - Uncertainty to project future needs

3.7.4. Capacity Overbuilding Dilemma

- Cost of extra capacity vs. Cost of upgrading a network
    - Upgrading costs 50-80% more (than building it right at the first time)
    - Majority complains about being under capacity, not over capacity
- Most organizations intentionally overbuild
    - Rapid growth in demand
    - 5-50% annual growth factor, sometimes 100%
    - Difficulty in accurate prediction
- Most end up using overcapacity within 3 years
    - Turnpike effect: when the network is efficient and provides good service, it becomes heavily used

3.7.5. Network Design Tools

- Used mostly in the technology design process
- First step: Enter a diagram of the existing network
  - Created from scratch (as required by some tools), or
  - Discovered automatically (by some tools)
- Once the diagram is complete
  - Add information about the expected network traffic and
  - See if the expected level of traffic can be supported May be accomplished through simulation models
- Once simulation is complete
  - Examine results to see estimated delays and throughput
  - Change the design if necessary and rerun simulations

3.7.6. Simulation

A mathematical technique used to model the behavior of a network

- Once modeled, the network behaves as it would under real conditions
  - Simulates applications and users generating traffic and responding to messages
- Can track: Number of packets, delays experienced at each point in the network
- May be tailored
  - Enter parameter values specific to network at hand (e.g., Computer A generates 3 packets per second)

May also highlight potential trouble spots Offer suggestions in overcoming problems Increase a circuit speed from T1 to T3

3.7.7. Deliverables

A set of physical network designs

- General specifications for the hardware and software required
- Several alternative designs to do cost-benefit analysis

The crucial issue:

- Design of the network circuits and devices

A new network designed from scratch

- Important to define clients computers with care
  - A major part of the total cost

3.7.8. Cost Assessment

- Assessment of the costs of various physical network design alternatives
- Complex process; many factors; consider:
  - Circuit costs (leased circuits and purchased cabling)
  - Internetworking devices (switches and routers)
  - Hardware costs (servers, hubs, NICs & UPSs)
  - Software costs (network operating systems, application software and middleware)
  - Network management costs including special hardware, software, and training needed for network management
  - Test and maintenance costs for monitoring equipment and supporting onsite repairs
  - Operations costs to run the network

3.8. Request for Proposal (RFP)

- Used before making large network purchases
  - Specify what equipment, software, and services desired
    - Items may be categorized as mandatory, important, or desirable
    - Some RFPs may simply list requirements (no specific equipment)
- Ask vendor to provide their proposed design (if asked), specific items, and best prices

3.8.1. Outline for Request for Proposals

- Background Information
  - Organizational profile; Overview of current network; Overview of new network; Goals of the new network
- Network Requirements
  - Choice sets of possible network designs (hardware, software, circuits); Mandatory, desirable, and wish list items, Security and control requirements; Response time requirements; Guidelines for proposing new network designs
- Service Requirements
  - Implementation time plan; Training courses and materials; Support services (e.g., spare parts on site); Reliability and performance guarantees
- Bidding Process
  - Time schedule for the bidding process; Ground rules; Bid evaluation criteria; Availability of additional information
- Information Required from Vendor
  - Vendor corporate profile; Experience with similar networks; Hardware and software benchmarks; Reference list .

3.8.2. Vendor Selection Process

- Evaluate submitted proposals against specific criteria
- Select winner(s) based on criteria
- Multi-vendor selections
  - Provide better performance
    - Unlikely that one vendor makes the best in all categories
  - Tend to be less expensive
    - Unlikely that one vendor has the cheapest in all categories
  - More difficult to manage
    - If not working properly, each vendor blame each other for the problem

3.8.3. Selling the Proposal to Management

- Obtaining the support of senior management for the proposed design
  - Network treated as cost center
- Keys gaining acceptance
  - Speak their language and present the design in terms of easily understandable issues
    - Make a business case by focusing on organizational needs and goals such as
      - Comparing the growth in network use with the growth in the network budget
  - Avoid focusing on technical issues such as upgrading to gigabit Ethernet
  - Focus on network reliability
    - Mission critical applications must be always available

3.8.4. Deliverables

- An RFP
  - Issued to potential vendors.
- Revised set of physical network diagrams
  - Done after the vendor(s) selected
  - Final technology design
  - Selected components (exact products and costs)
- Business case
  - To support the network design
  - Expressed in terms of business objectives

Example ✎. What's a typical network design for a LAN with 5 Public IP's for the FW, Router, Switches?

Example ✎. How do we create a network of 100 Computers in one building from scratch?

Example ✎. Describe how you've met the challenges associated with IPv6?

Solution: It's true and the answer sounds proactive. □

Revision Questions

EXERCISE 8. ✍ What is the most important step when you are trying to get help from your ISP to stop a DDoS attack?

EXERCISE 9. ✍ A route reflector reflects routes from a route reflector client to which types of IBGP routers?

EXERCISE 10. ✍ What things should be considered when designing an enterprise network?

EXERCISE 11. ✍ What would the inbound ACL look like on your router's serial interface connected to the Internet if you decided to block RFC 1918 addresses, the bogons listed in this chapter, and RFC 2827 filtering, assuming your local IP range is 96.0.20.0/24?

EXERCISE 12. ✍ When evaluating the SYN flood protections required for a server, when might you use SYN cookies and when might you use TCP Intercept?

EXERCISE 13. ✍ When might it not be necessary to implement L2 security features on your network?

EXERCISE 14. ✍ When should you use uRPF as compared to traditional ACL filtering?Is it worth implementing Rob Thomas's entire bogon-filtering range on your Internet edge?

LESSON 4

Designing for Network Performance

Several higher level concepts used to design network for the best performance

- Managed networks
  - Network management software and standards
  - Policy-based management
- Network circuits
  - Traffic analysis
  - Service level agreements
- Network devices
  - Device latency and device memory
  - Load Balancing
- Minimizing network traffic
  - Content caching and content Delivery

4.1. Managed Networks

Network that uses **managed devices**

- Managed device: standard devices that can (in addition to performing its basic functions (switching and routing))
  - Monitors traffic flows
  - Monitors its status and other devices connected to
  - Records various data on messages it processes
  - Sends these data to manager's computer (on a request)
  - Sends alarms if a critical situation detected (such as a failing device, or unusual increase in traffic)

  - Problems detected and reported by devices themselves before problems become serious

Requires both hardware and software

- Hardware: monitor, collect, transmit
- Software: store, organize, analyze

4.2. Network Management Software

- Device (point) management software
  - Provide specific information about a device
    - Configuration, traffic, error conditions, etc
- System management software
  - aka, enterprise management software
  - Provide analysis device info to diagnose patterns
    - Prevents alarm storms (for a failure on a circuit, many connected devices sending alarms)
      - Software analyze these and correlates them and generates a single alarm to the manager
- Application management software
  - Monitor applications based on device info
  - Focus on delays and application layer packets

- **Network Management Standards**

Application layer protocols defining type of information collected and format of control messages

- Simple Network Management Protocol (SNMP)
  - Developed for Internet and LANs

  - Components of SNMP
    * Agent: collects device info and responds requests from the manager
    * Management Information Base (MIB): database at device stored by the agent
    * Network Management Station (NMS): Access MIB, sends control messages to agent

- Common Management Interface Protocol (CMIP) Developed for OSI type networks

4.3. Policy-Based Management

Enables managers to set priority policies for traffic (to take effect when congested) Example:

- Manager: order processing to have the highest priority
- Software: configure devices using QoS capabilities in ATM, TCP/IP, etc to give this application the highest priority

Expected to become more important

4.4. Network Circuits

- Play a critical role in designing network for maximum performance
- Important to size the circuit and place them to match the traffic
- Areas of concern:
  - Circuit loading and capacity planning
  - Traffic analysis, and
  - Service level agreement

4.5. Network Devices

Network devices from different vendors provide different capabilities

- Some faster, some more reliable, etc,.

Factors important in network performance

- Device latency
  - Delay imposed by device in processing messages
- Device memory
  - Size of memory in device
- Load Balancing
  - Capability in sharing the network load

4.5.1. Device Latency

- Delay imposed by device in processing messages High latency device; takes long time Low latency device: faster Wire speed: fastest device operating as fast as the circuits they connect (virtually no delays)
- Key element affecting latency: Computer processor in the device
- More important for networks with heavy traffic High latency devices may cause long traffic backups
- Less Important in low traffic networks Packets arrive less frequently and less backup delays

4.5.2. Device Memory

- Go hand-in-hand with latency
  - If a high-latency device, backed-up packets to be stored in memory;
    - Otherwise they will be lost and to be retransmitted
      - More, unnecessary traffic

        * high-latency devices need more memory

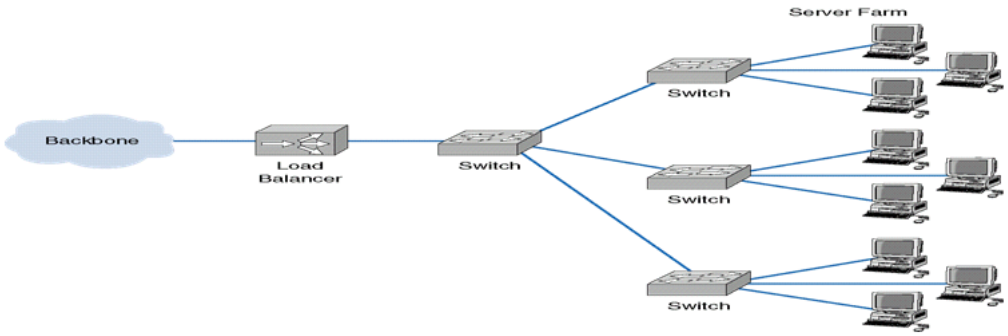
- Also important for servers

    - More memory means more files can be stored in memory

        * Requests processed more quickly Faster than hard disks

4.5.3. Load Balancing

To ensure that a request is handled immediately by a free server in the server farm



Load balancer:

- Handles all requests; selects an appropriate server based on some sequence(round-robin, etc.,)
- If server crashes, no requests are sent to that server

4.5.4. Minimizing Network Traffic

Another approach in improving network performance. Attempts to move most commonly used data closer to user - reduces traffic elsewhere

- Providing servers with duplicate copies at points closer to users

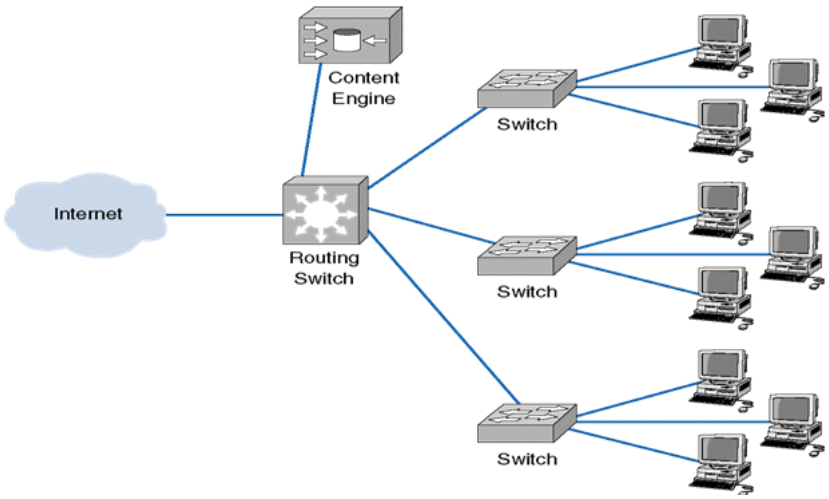
Approaches in reducing traffic

- Content caching
- Content delivery

4.5.5. Content Caching

- Basic idea: Store other people's WEB data closer to your users
  - Install a content engine (aka, cache engine) close to your Internet connection Install special content management software on the router
- Operations
- Stores requests and responses (mostly static files)
- Examines each outgoing request; if it requires a file already in cache, it responds immediately (without going to the requested site)
- Stores contents form most commonly accessed sites (updates them frequently)
- Must operate at wire speeds (otherwise degrade performance) Reduces traffic between Internet and Organization - less circuits to lease

- **Network with Content Engine**



4.5.6. Content Delivery

A special type of Internet service provided by "content delivery providers (CDPs)"

- A CDP stores Web files for its client closer to the client's potential users
- Akamai, a CDP, operates 10,000 servers located near busiest NAPs and MAEs

  - Servers contain most commonly requested web info for some busiest sites like yahoo.com
  - When a user access a client's site, a software in client's server looks for an Akamai server (closer to the user)
  - Akamai server sends the static files, the client's server sends the dynamic files of the site

- **Benefits of Content Delivery**
  - Users of the client subscribed to Akamai
    - Much faster response time (because many parts of the requested page will come form a nearby Akamai server)
  - Client organization subscribed to Akamai Less traffic for its servers
    - Need not spend as much on its server farm
    - Need less capacity on its circuits to Internet
  - ISPs providing service to users
    - Less traffic flows through their networks (unpaid traffic due to peering)

4.5.7. Implications for Management

- Develop strong relationships with only few vendors
  - Use a building block approach in designing networks
  - Use a few common, standardized technologies everywhere in the network
- Purchase technologies that will provide strong network management capabilities
  - Cost to operate is now much more expensive than the cost to purchase
- Use powerful design and management tools

- Saves money in the long run

Example ✎. Why the need for a network performance baseline?

Solution: In the simplest terms, a network performance baseline is a set of metrics used in network performance monitoring to define the normal working conditions of an enterprise network infrastructure. Engineers use network performance baselines for comparison to catch changes in traffic that could indicate a problem. Setting a network baseline also provides early indicators that application and network demands are pushing near the available capacity, giving the networking team the opportunity to plan for upgrades. Aligning network performance baselines with existing network service level agreements (SLAs) can help the IT organization stay within capacity parameters and identify problem areas that are falling out of compliance. The network monitoring challenge for engineers, however, is to define what is normal for their organization's infrastructure. □

Revision Questions

EXERCISE 15. ✍ How long must you monitor to set a network performance baseline?

EXERCISE 16. ✍ How do we Comparing AWR data with the baseline during report generation?

EXERCISE 17. ✍ List the top 10 Performance Monitor counters?

EXERCISE 18. ✍ How do we Collect data to set a network performance baseline?

EXERCISE 19. ✍ Discuss the Network performance monitoring: Taking stock and considering virtualization?

LESSON 5

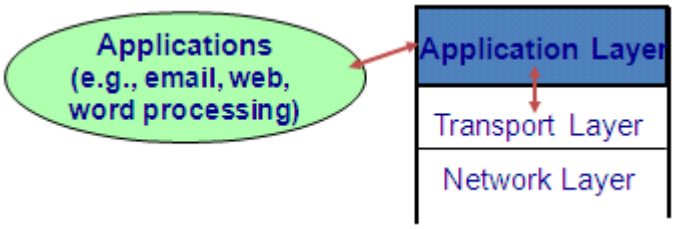
Application Layer

5.1. Outline

- Application Architectures
  Host-Based, Client-Based, and Client-Server Architectures, Choosing Architectures
- World Wide Web
  How the Web Works, Inside an HTTP Request & HTTP Response
- Electronic Mail
  How E-Mail Works, Inside an SMTP Packet
- Other Applications
  Ftp, Telnet, Instant Messaging, Videoconferencing

5.2. Application Layer - Introduction

5.2.1. Functions of Applications

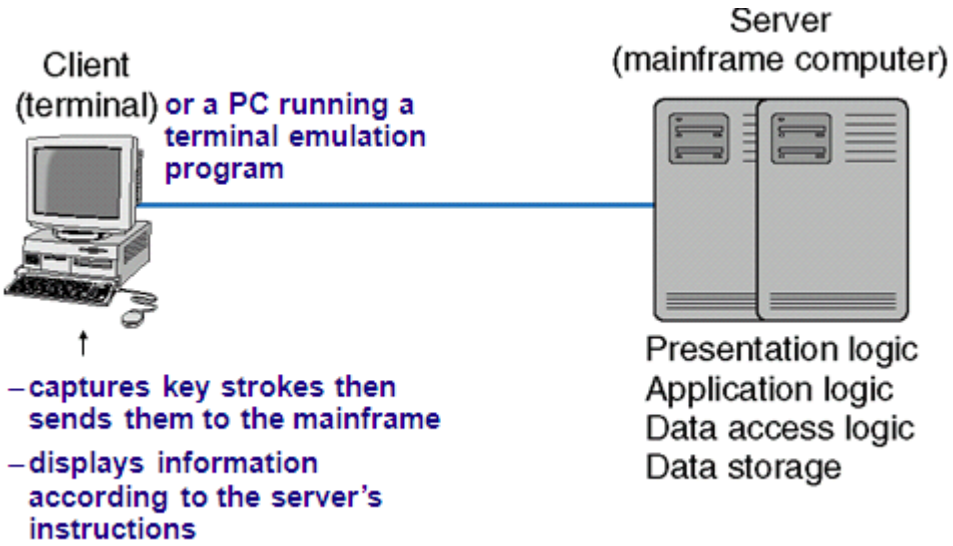


- Data storage 2 - 3
  - Storing of data generated by programs (e.g., files, records)
  - Data access logic
    - Processing required to access stored data (e.g., SQL)
  - Application logic
    - Business logic
  - Presentation logic
    - Presentation of info to user and acceptance of user commands

5.3. Application Architectures

- Determined by how functions of application programs are spread among clients and servers
  - Host-based Architectures
    - Server performs almost all functions
  - Client-based architectures
    - Client performs most functions
  - Client-server architectures
    - Functions shared between client and server

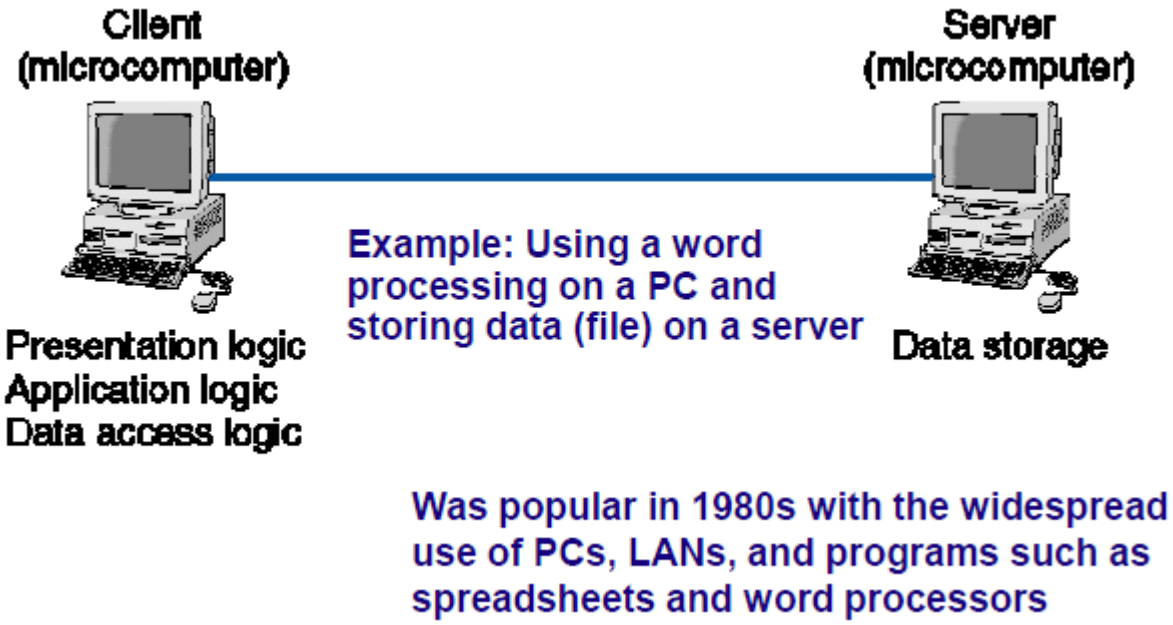
5.3.1. Host-Based Architectures



5.3.2. Problems with Host-based Arch

- Host becoming a bottleneck
  - All processing done by the host, which can severely limit network performance
- Upgrades typically expensive and "lumpy"
  - Available upgrades require big jumps in processing and memory

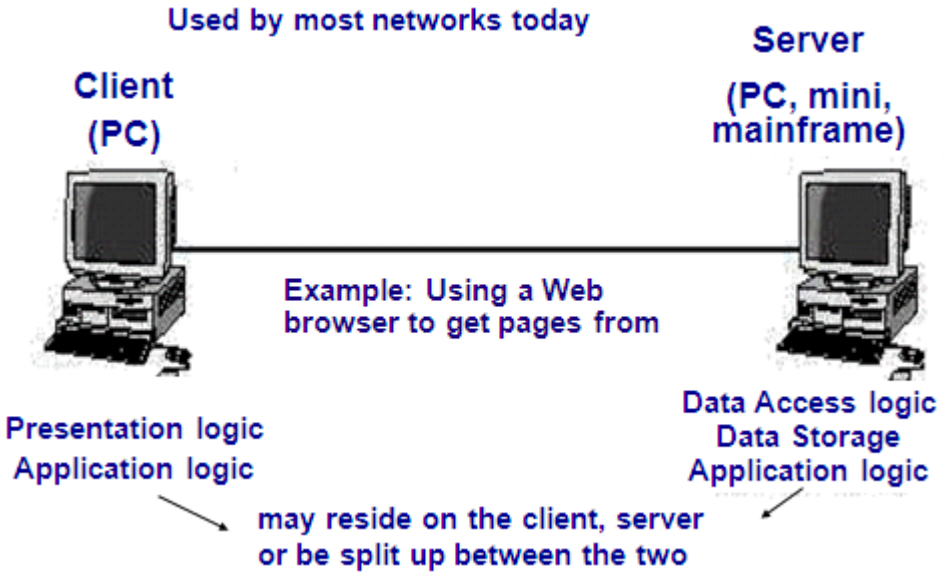
– Network demand grows more incrementally, so this often means a poor fit (too much or too little) between host performance and network demand.



5.3.3. Problems with Client-Based Arch.

- Data MUST travel back and forth between server and client
  - Example: when the client program is making a database query, the ENTIRE database must travel to the client before the query can be processed
  - Result in poor network performance

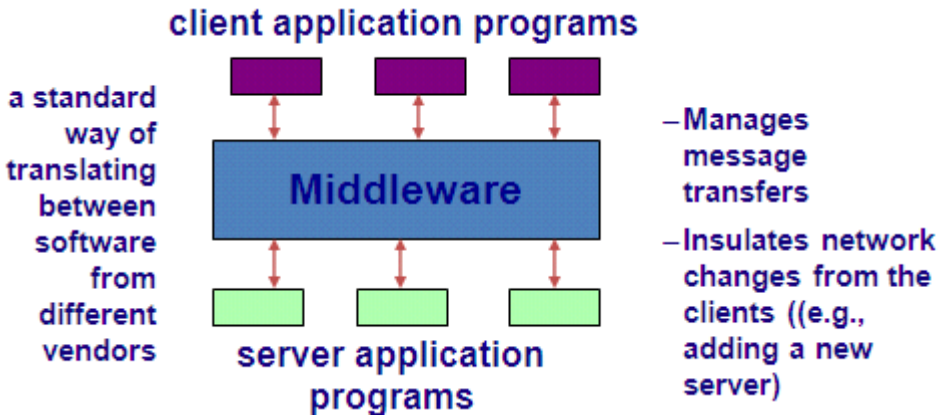
- **Client-Server Architectures**



5.3.4. Client-Server Architectures

- **Advantages**
  - More efficient because of distributed processing
  - Allow hardware and software from different vendors to be used together
- **Disadvantages**
  - Difficulty in getting software from different vendors to work together smoothly
  - May require Middleware, a third category of software

Middleware



Examples:

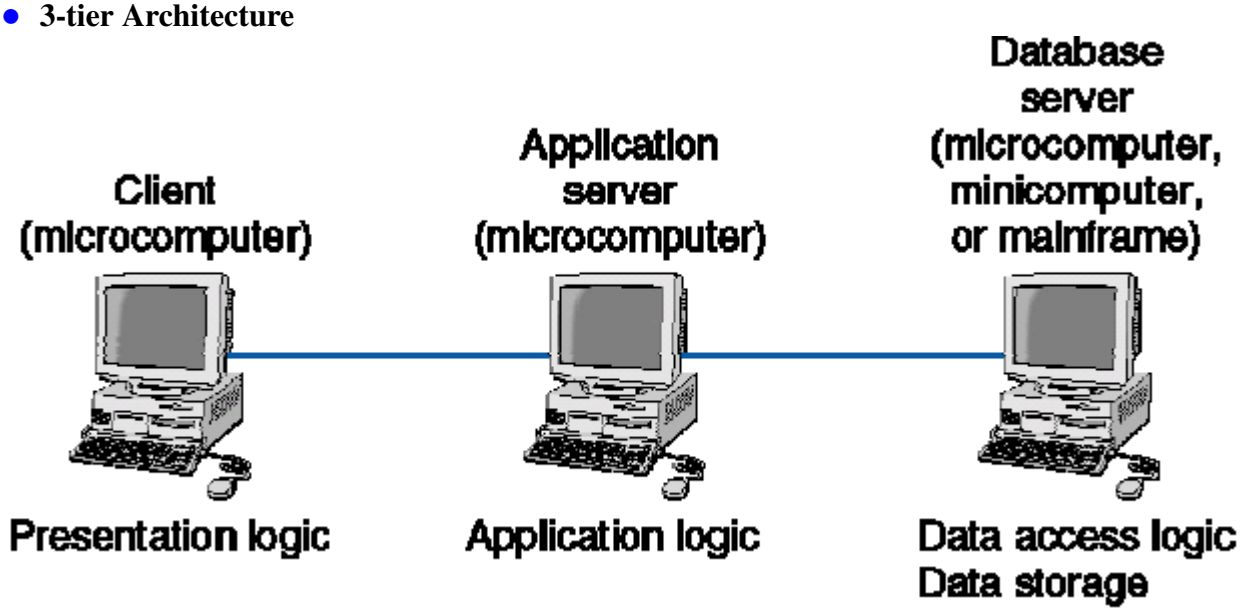
- Distributed Computing Environment (DCE)
- Common Object Request Broker Architecture (CORBA)
- Open Database Connectivity (ODBC)

- **Multi-tier Architectures**

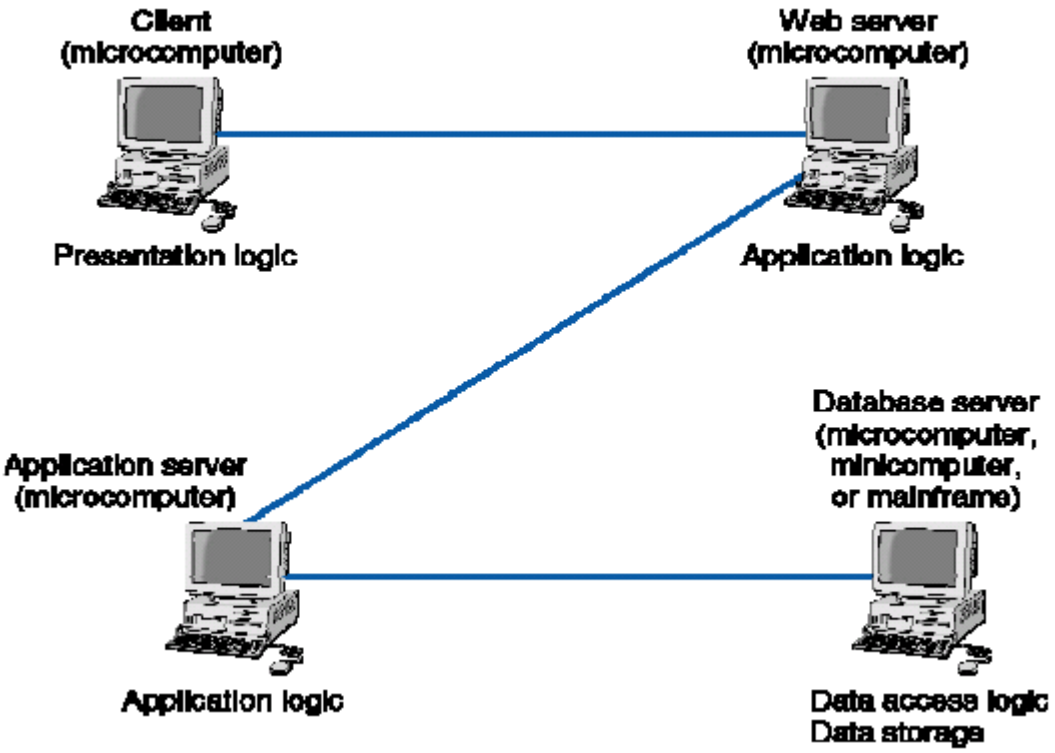
Involve more than two computers in distributing application program logic

- 2-tier architecture (architectures discussed so far)
- 3-tier architecture
  - 3 sets of computers involved
- N-tier architecture
  - more than three sets of computers used

- **3-tier Architecture**



- **N-tier Architecture 2 - 14**



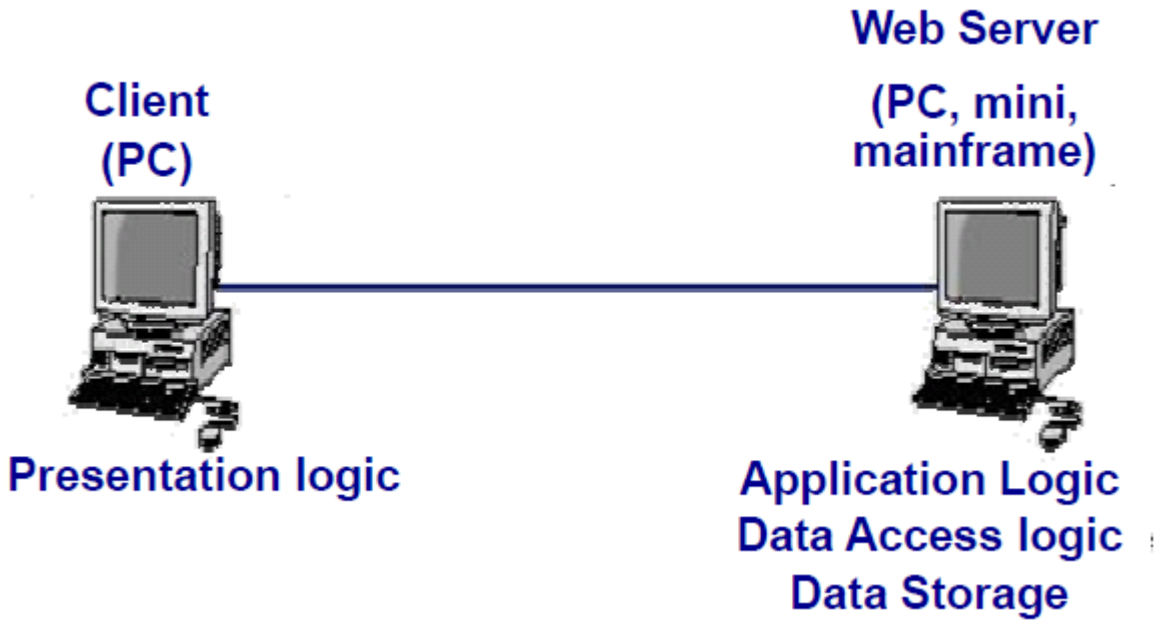
- **Multi-tier Architectures**
- **Advantages**
  - Better load balancing:

    More evenly distributed processing. (e.g., application logic distributed between several servers.)

  - More scalable:
    - Only servers experiencing high demand need be upgraded
- **Disadvantages**
  - Heavily loaded network:
    - More distributed processing more exchanges
    - Difficult to program and test due to increased complexity

- **Fat vs. Thin Clients**
  - Depends on how much of the application logic resides on the client
    - Fat client: (a.k.a., thick client)
      - All or most of the application logic
    - Thin client:
      - Little or no application logic
      - Becoming popular because easier to manage, (only the server application logic generally needs to be updated)
      - The best example: World Wide Web architecture (uses a two-tier, thin client architecture)

- **Thin-Client Example: Web Architecture**



- **Criteria for Choosing Architecture**
  - Infrastructure Cost
    - Cost of servers, clients, and circuits
    - Mainframes: very expensive; terminals, PCs: very inexpensive
  - Development Cost

  - Mainly cost of software development
  - Software: expensive to develop; off-the-shelf software: inexpensive

- Scalability
  - Ability to increase (or decrease) in computing capacity as network demand changes
  - Mainframes: not scalable; PCs: highly scalable

- **Choosing an Architecture**

	Host-Based	Client-Based	Client-Server
Cost of Infrastructure	High	Medium	Low
Cost of Development	Low	Medium	High
Scalability	Low	Medium	High

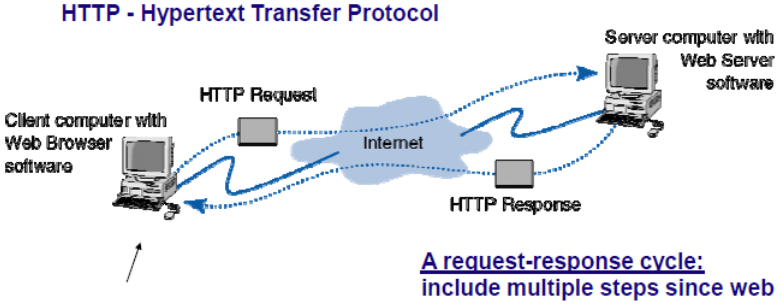
5.3.5. Applications

- World Wide Web
- E-mail
- File Transfer
- Videoconferencing
- Instant Messaging

- **World Wide Web**
  - Two central ideas:
    - Hypertext
      - A document containing links to other documents
    - Uniform Resource Locators (URLs)
      - A formal way of identifying links to other documents
    - Invention of WWW (1989)
      - By Tim Berners-Lee at CERN in Switzerland
    - First graphical browser, Mosaic, (1993)
      - By Marc Andressen at NCSA in USA; later founded Netscape

- **How the Web Works**

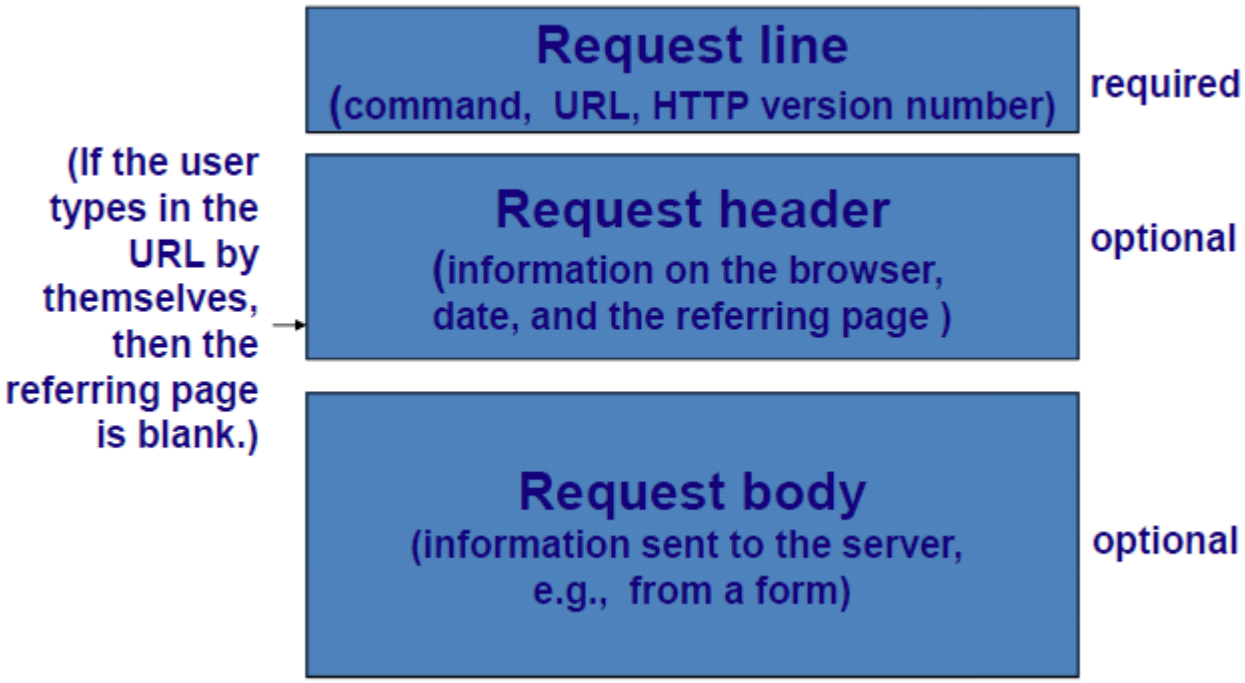
Main Web communications protocol:
HTTP - Hypertext Transfer Protocol



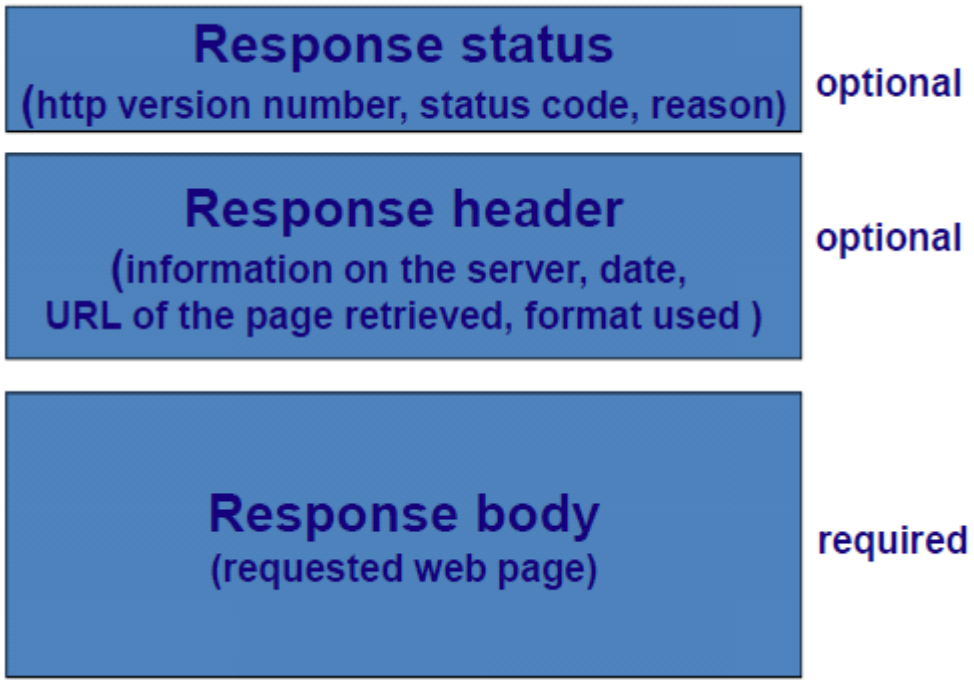
Clicking on a hyperlink or typing a URL into a browser starts a request-response cycle

A request-response cycle: include multiple steps since web pages often contain embedded files, such as graphics, each requiring a separate response.

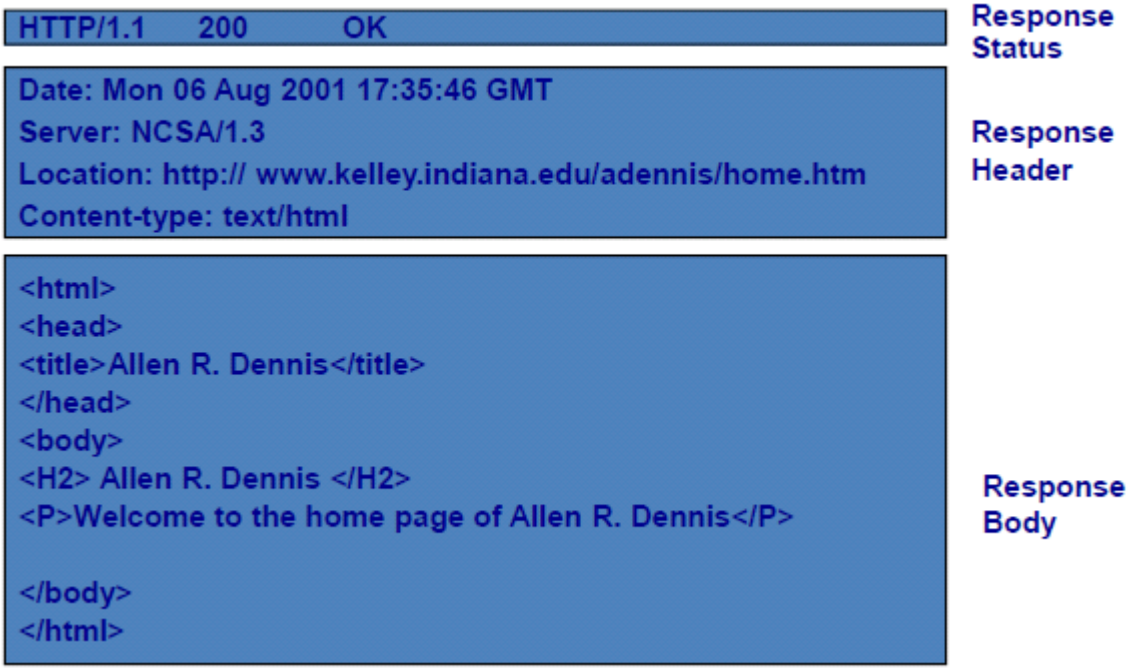
- **HTTP Request Message**



- **HTTP Response Message**



- **Example of an HTTP Response**



- **HTML - Hypertext Markup Language**
  - A protocol used to format Web pages
  - TAGs embedded in HTML documents
    - include information on how to format the file
  - Extensions to HTML needed to format multimedia files
  - XML - Extensible Markup Language
    - A new markup language becoming popular
- **Two-Tier E-mail Architecture**
  - User agents (also called e-mail clients)
    - Run on client computers
    - Send e-mail to e-mail servers
    - Download e-mail from mailboxes on those servers

    - Examples: Eudora, Outlook, Netscape Messenger

  - Mail transfer agents (also called mail server)

    - Used by e-mail servers
    - Send e-mail between e-mail servers
    - Maintain individual mailboxes

- **File Transfer Protocol (FTP)**
  - Enables sending and receiving files over the Internet
  - Requires an application program on the client computer and a FTP server program on a server
  - Commonly used today for uploading web pages
  - Many packages available using FTP

    - WS-FTP (a graphical FTP software)

  - FTP sites

    - Closed sites
      - Requires account name and password
    - Anonymous sites
      - Account name: anonymous; pwd: your email address

- **Telnet**
  - Allows one computer to log into other computers

    - Remote login enabling full control of the host

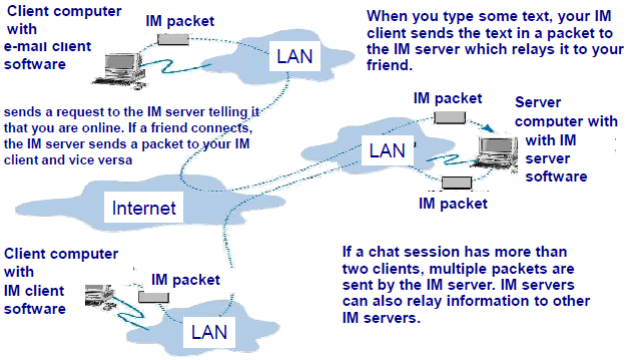
  - Requires an application program on the client computer and a Telnet server program on a server

    - Client program emulates a “dumb” terminal

- Many packages available conforming Telnet
- Requires account name and password
  - Anonymous sites
    - Account name: anonymous; pwd: your email address

- **Instant Messaging (IM)**
  - A client-server program that allows real-time typed messages to be exchanged
    - Client needs an IM client software
    - Server needs an IM server package
  - Some types allow voice and video packets to be sent
    - Like a telephone
  - Examples include AOL and ICQ
  - Two step process:
    - Telling IM server that you are online
    - Chatting

- **How Instant Messaging Works**



- **Webcasting**
  - Special type of one-directional videoconferencing
    - Content is sent from the server to users
  - Process
    - Content created by developer
    - Downloaded as needed by the user
    - Played by a plug-in to a Web browser
  - No standards for webcasting yet
    - Defacto standards: products by RealNetworks

- **Implications for Management**
  - Network must be used to provide a worry-free environment for applications
    - Network should not change the way an organization operates; application should!
    - Network should enable wide variety of applications

- Dramatic increase in number and type of applications
  - Rapid growth in amount and type of traffic
    - Different implication on network design and management
    - Increased operating cost

Revision Questions

Example . Which protocols work in application layer?

Solution: arp (address resolution protocol) rarp(reverse address resolution protocol) other as well □

EXERCISE 20. Is HTTP a transportation layer protocol or an application protocol?

EXERCISE 21. Can a web server initiate a communication with a web browser?

LESSON 6

Physical Layer

6.1. Outline

- Circuits
  - Configuration, Data Flow, Communication Media
- Digital Transmission of Digital Data
  - Coding, Transmission Modes,
- Analog Transmission of Digital Data
  - Modulation, Voice Circuit Capacity,
- Digital Transmission of Analog Data
  - Pulse Amplitude Modulation, Voice Data Transmittion, Instant Messenger Transmitting Voice Data
- Analog/Digital Modems
- Multiplexing
  - FDM, TDM, STDM, WDM,

6.2. Overview

- Includes network hardware and circuits
- Network circuits:
  - physical media (e.g., cables) and
  - special purposes devices (e.g., routers and hubs).
- Types of Circuits
  - Physical Layer Network Layer Data Link Layer – Physical circuits connect devices & include actual wires such as twisted pair wires

  - Logical circuits refer to the transmission characteristics of the circuit, such as a T-1 connection refers to 1.5 Mbps
  - Can be the same or different. For example, in multiplexing, one wire carries several logical circuits

6.3. Types of Data Transmitted

- Analog data
  - Produced by telephones
  - Sound waves, which vary continuously over time
  - Can take on any value in a wide range of possibilities
- Digital data
  - Produced by computers, in binary form, represented as a series of ones and zeros
  - Can take on only 0 and 1

6.4. Types of Transmission

- Analog transmissions
  - Analog data transmitted in analog form (vary continuously)
  - Examples of analog data being sent using analog transmissions are broadcast TV and radio
- Digital transmissions
  - Made of square waves with a clear beginning and ending
  - Computer networks send digital data using digital transmissions.
- Data converted between analog and digital formats
- Modem (modulator/demodulator): used when digital data is sent as an analog transmission

- Codec (coder/decoder): used when analog data is sent as a digital transmission

Data Type vs. Transmission Type

6.4.1. Digital Transmission: Advantages

- Produces fewer errors
  - Easier to detect and correct errors, since transmitted data is binary (1s and 0s, only two distinct values))
- Permits higher maximum transmission rates
  - e.g., Optical fiber designed for digital transmission
- More efficient
  - Possible to send more digital data through a given circuit
- More secure
  - Easier to encrypt
- Simpler to integrate voice, video and data
  - Easier to combine them on the same circuit, since signals made up of digital data

6.5. Circuit Configuration

- Basic physical layout of the circuit
- Configuration types:
  - Point-to-Point Configuration
    - Goes from one point to another
    - Sometimes called “dedicated circuits”
  - Multipoint Configuration
    - Many computer connected on the same circuit
    - Sometimes called “shared circuit”

6.6. Communications Media

Physical matter that carries transmission

- Guided media:
  - Transmission flows along a physical guide (Media guides the signal))
  - Twisted pair wiring, coaxial cable and optical fiber cable
- Wireless media (aka, radiated media)
  - No wave guide, the transmission just flows through the air (or space)
  - Radio (microwave, satellite) and infrared communications

6.6.1. Twisted Pair (TP) Wires

- Commonly used for telephones and LANs
- Reduced electromagnetic interference
  - Via twisting two wires together (Usually several twists per inch)
- TP cables have a number of pairs of wires
  - Telephone lines: two pairs (4 wires, usually only one pair is used by the telephone)
  - LAN cables: 4 pairs (8 wires)
- Also used in telephone trunk lines (up to several thousand pairs)
- Shielded twisted pair also exists, but is more expensive

6.6.2. Fiber Optic Cable

- Light created by an LED (light-emitting diode) or laser is sent down a thin glass or plastic fiber
- Has extremely high capacity, ideal for broadband
- Works better under harsh environments

  - Not fragile, nor brittle; Nit heavy nor bulky
  - More resistant to corrosion, fire, etc.,

- Fiber optic cable structure (from center):
  - Core (v. small, 5-50 microns, the size of a single hair)
  - Cladding, which reflects the signal
  - Protective outer jacket

- **Types of Optical Fiber**
  - Multimode (about 50 micron core)
    - Earliest fiber-optic systems
    - Signal spreads out over short distances (up to ~500m)
    - Inexpensive
  - Graded index multimode
    - Reduces the spreading problem by changing the refractive properties of the fiber to refocus the signal
    - Can be used over distances of up to about 1000 meters
  - Single mode (about 5 micron core)
    - Transmits a single direct beam through the cable – Signal can be sent over many miles without spreading
    - Expensive (requires lasers; difficult to manufacture)

6.7. Wireless Media

- Radio
  - Wireless transmission of electrical waves over air
  - Each device has a radio transceiver with a specific frequency
    * Low power transmitters (few miles range)

        - Often attached to portables (Laptops, PDAs, cell phones)
    - Includes
        - AM and FM radios, Cellular phones
        - Wireless LANs (IEEE 802.11) and Bluetooth
        - Microwaves and Satellites
- Infrared
    - "invisible" light waves (frequency is below red light)
    - Requires line of sight; generally subject to interference from heavy rain, smog, and fog
    - Used in remote control units (e.g., TV)

6.8. Factors Used in Media Selection

- **Type of network** - LAN, WAN, or Backbone
- **Cost** - Always changing; depends on the distance
- **Transmission distance** - Short: up to 300 m; medium: up to 500 m
- **Security** - Wireless media is less secure
- **Error rates** - Wireless media has the highest error rate (interference)
- **Transmission speeds** - Constantly improving; Fiber has the highest

6.9. Digital Transmission of Digital Data

- Computers produce binary data
- Standards needed to ensure both sender and receiver understands this data
    - Coding: language that computers use to represent letters, numbers, and symbols in a message
    - Signaling (aka, encoding): language that computers use to represent bits (0 or 1) in electrical voltage

- Bits in a message can be send in
  - A single wire one after another (Serial transmission)
  - Multiple wires simultaneously (Parallel transmission)

6.9.1. Transmission Modes

- Parallel mode – Uses several wires, each wire sending one bit at the same time as the others
  - A parallel printer cable sends 8 bits together
  - Computer's processor and motherboard also use parallel busses (8 bits, 16 bits, 32 bits) to move data around
- Serial Mode
  - Sends bit by bit over a single wire
  - Serial mode is slower than parallel mode

- **Signaling of Bits**

Digital Transmission

- Signals sent as a series of "square waves" of either positive or negative voltage
- Voltages vary between +3/-3 and +24/-24 depending on the circuit

Signaling (encoding)

- Defines what voltage levels correspond to a bit value of 0 or 1
- Examples:
  - Unipolar, Bipolar
  - RTZ, NRZ, Manchester
- Data rate: how often the sender can transmit data
  - 64 Kbps once every 1/64000 of a second

- **Signaling (Encoding) Techniques**
  - Unipolar signaling – Use voltages either vary between 0 and a positive value or between 0 and some negative value
  - Bipolar signaling
    - Use both positive and negative voltages
    - Experiences fewer errors than unipolar signaling - Signals are more distinct (more difficult (for interference) to change polarity of a current)
    - Return to zero (RZ) - Signal returns to 0 voltage level after sending a bit
    - Non return to zero (NRZ) - Signals maintains its voltage at the end of a bit
  - Manchester encoding (used by Ethernet)

6.10. Analog Transmission of Digital Data

A well known example

- Using phone lines to connect PCs to Internet
  - PCs generates digital data
  - Phone lines use analog transmission technology
  - Modems translate digital data into analog signals

Example ✎. What Is Serial Data Transmission?

Solution: Serial data transmission is a form of data transmission where by bits of characters are sent one at a time along a communication path. Serial data transmissions travel over a single wire in one direction and are often compared to data transmission. They each follow an 8 bit character. □

Revision Questions

EXERCISE 22. ✍ What are types of electronic communication media?

EXERCISE 23. ✍ How many different values can be represented by a binary word of 7 bits?

EXERCISE 24. ✍ What is the primary function of multiplexing?

EXERCISE 25. ✍ What is a Popular serial data transmission method?

EXERCISE 26. ✍ What is the difference between serial and parallel data transmission?

EXERCISE 27. ✍ what is a serial data transfer?

EXERCISE 28. ✍ What describes a popular serial data transmission method?

LESSON 7

Modulation

- Modification of a carrier wave's fundamental characteristics in order to encode information
  - Carrier wave: Basic sound wave transmitted through the circuit (provides a base which we can deviate)
- Basic ways to modulate a carrier wave:
  - Amplitude Modulation (AM) - Also known as Amplitude Shift Keying (ASK)
  - Frequency Modulation (FM) - Also known as Frequency Shift Keying (FSK)
  - Phase Modulation (PM) - Also known as Phase Shift Keying (PSK)

7.1. Modem - Modulator/demodulator

- Device that encodes and decodes data by manipulating the carrier wave
- V-series of modem standards (by ITU-T) –
  - V.22
    - An early standard, now obsolete
    - Used FM, with 2400 symbols/sec 2400 bps bit rate
  - – V.34
    - One of the robust V standards
    - Used TCM (8.4 bits/symbol), with 3,428 symbols/sec multiple data rates(up to 28.8 kbps)
    - Includes a handshaking sequence that tests the circuit and determines the optimum data rate

7.1.1. Digital Transmission of Analog Data

- Analog voice data sent over digital network using digital transmission
- Requires a pair of special devices called Codec
  - Coder/decoder
    - A device that converts an analog voice signal into digital form
    - Also converts it back to analog data at the receiving end
    - Used by the phone system

7.2. Distributed Deadlock

A deadlock is a condition in a system where a process cannot proceed because it needns to obtain a resource held by another process but it itself is holding a resource that the other process needs. More formally, four conditions have to be met for a deadlock to occur in a system:

1. Mutual exclusion A resource can be held by at most one process.
2. Hold and wait Processes that already hold resources can wait for another resource.
3. Non-preemption A resource, once granted, cannot be taken away.
4. Circular wait Two or more processes are waiting for resources held by one of the other processes.

Resource allocation can be represented by directed graphs:
P1→R1 means that resource R1 is allocated to process P1.
P1→R1 means that resource R1 is requested by process P1.
Deadlock is present when the graph has cycles. An example is shown in Figure 1.

7.2.1. Deadlocks in distributed systems

The same conditions for deadlocks in uniprocessors apply to distributed systems. Unfortunately, as in many other aspects of distributed systems, they are harder to detect, avoid, and prevent. Tannenbaum proposes four strategies for dealing with distributed deadlocks:

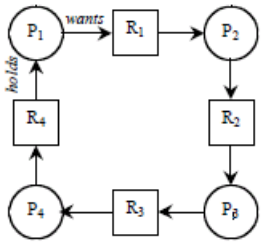


Figure 7.1: Deadlock

1. Ignorance: ignore the problem (this is the most common approach).
2. Detection: let deadlocks occur, detect them, and then deal with them.
3. Prevention: make deadlocks impossible.
4. Avoidance: choose resource allocation carefully so that deadlocks will not occur.

7.2.2. Centralized deadlock detection

Centralized deadlock detection attempts to imitate the nondistributed algorithm through a central coordinator. Each machine is responsible for maintaining a resource graph for its processes and resources. A *central coordinator* maintains the resource utilization graph for the entire system. This graph is the union of the individual graphs. If this coordinator detects a cycle, it kills off one process to break the deadlock.

In the non-distributed case, all the information on resource usage lives on one system and the graph may be constructed on that system. In the distributed case, the individual subgraphs have to be propagated to a central coordinator. A message can be sent each time an arc is added or deleted. If optimization is needed, a list of added or deleted arcs can be sent periodically to reduce the overall number of messages sent.

Suppose machine *A* has a process P0, which holds the resource *S*and wants resource *R*, which is held by P1.The local graph on A is shown in Figure 1.2. Another machine, machine B, has a process P2, which is holding resource *T* and wants resource *S*. Its local graph is shown in Figure 1.3. Both of these machines send their graphs to the central coordinator, which maintains the union (Figure 1.4). All

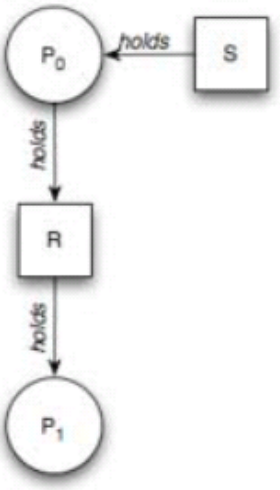


Figure 7.2: Resource graph on A.

is well. There are no cycles and hence no deadlock. Now two events occur. Process P1 releases resource R and asks machine B for resource T. Two messages are sent to the coordinator:
message 1 (from machine A): "*releasing R*"
message 2 (from machine B): "*waiting for T*"
This should cause no problems (no deadlock). However, if message 2 arrives first, the coordinator would then construct the graph in Figure 1.5 and detect a deadlock. Such a condition is known as **false deadlock**. A way to fix this is to use Lamport's algorithm to impose global time ordering on all machines. Alternatively, if the coordinator suspects deadlock, it can send a reliable message to every machine asking whether it has any release messages. Each machine will then respond with either a release message or a negative acknowledgement to acknowledge receipt of the message.

7.2.3. Distributed deadlock detection

An algorithm for detecting deadlocks in a distributed system was proposed by Chaudy, Misra, and Haas in 1983. It allows that processes to request multiple resources at once (this speeds up the growing phase). Some processes may wait for resources (either local or remote). Cross-machine arcs make looking for cycles (detecting deadlock) hard.

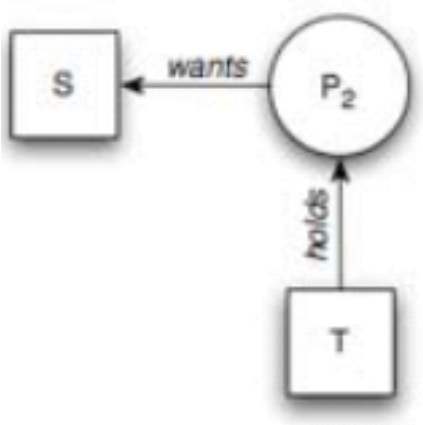


Figure 7.3: Resource graph on B.

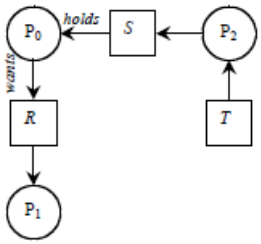


Figure 7.4: Resource graph on coordinator

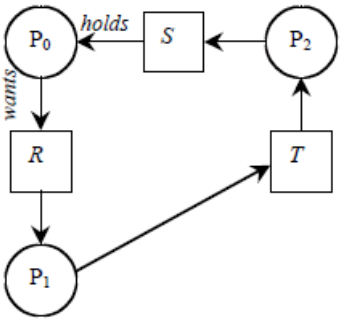


Figure 7.5: False deadlock

The algorithm works this way: When a process has to wait for a resource, a probe message is sent to the process holding the resource. The probe message contains three components: the process that blocked, the process that is sending the request, and the destination. Initially, the first two components will be the same. When a process receives the probe: if the process itself is waiting on a resource, it updates the *sending* and *destination* fields of the message and forwards it to the resource holder. If it is waiting on multiple resources, a message is sent to each process holding the resources. This process continues as long as processes are waiting for resources. If the originator gets a message and sees its own process number in the *blocked* field of the message, it knows that a cycle has been taken and deadlock exists. In this case, some process (transaction) will have to die. The sender may choose to commit suicide or a ring election algorithm may be used to determine an alternate victim (e.g., youngest process, oldest process, ...).

7.2.4. Distributed deadlock prevention

An alternative to detecting deadlocks is to design a system so that deadlock is impossible. One way of accomplishing this is to obtain a global timestamp for every transaction (so that no two transactions get the same timestamp). When one process is about to block waiting for a resource that another process is using, check which of the two processes has a younger timestamp and give priority to the older process. If a younger process is using the resource, then the older process (that wants the resource) waits. If an older process is holding the resource, the younger process (that wants the resource) kills itself. This forces the resource utilization graph to be directed from older to younger processes, making cycles impossible. This algorithm is known as the **wait-die algorithm**.
An alternative method by which resource request cycles may be avoided is to have an old process preempt (kill) the younger process that holds a resource. If a younger process wants a resource that an older one is using, then it waits until the old process is done. In this case, the graph flows from young to old and cycles are again impossible. This variant is called the **wound-wait algorithm.**

Example ✎**.** A 1.0 MHz carrier is to be amplitude modulated by music signal with frequencies varying from 50 Hz to 20 KHz. Find out the range of frequencies of the upper and lower sidebands produced. Hence find the bandwidth of the channel required to transmit this modulated signal.

Solution: USB varies from 1.00005 MHz to 1.02 MHz while the LSB stretches between 0.98 MHz and 0.99995 MHz. Bandwidth of the channel required to transmit the DSBAM is 40 kHz. □

Revision Questions

EXERCISE 29. ✍ Analogue signals are often used in preference to digital signals because they are less affected by noise?

EXERCISE 30. ✍ What is analog modulation and state various techniques?

EXERCISE 31. ✍ Explain the need of modulation and demodulation?

EXERCISE 32. ✍ A 1.0 MHz carrier is to be amplitude modulated by music signal with frequencies varying from 50 Hz to 20 KHz. Find out the range of frequencies of the upper and lower sidebands produced. Hence find the bandwidth of the channel required to transmit this modulated signal.

EXERCISE 33. ✍ A convention AM transmitter station transmits with a modulation index of 0.9. The total power transmitted is 100 kW. Find out the following:
The power carrier by the carrier?
The fraction of the total power carrying any message.
Does the total transmitted power vary with depth of modulation? Why?
Calculate total transmitted power if the modulation is 100%.

EXERCISE 34. ✍ The transmitted power of an angle modulated (FM or PM) wave is independent of the depth of modulation while that for amplitude modulation varies with the modulation index. Why?

EXERCISE 35. ✍ A 15 kHz band-limited signal is transmitted using FM. The maximum deviation permitted is 30 kHz. What is the modulation index? What will be the band-width required? Explain with respect to Carson's rule.

EXERCISE 36. ✍ State the techniques of demodulation?

EXERCISE 37. ✍ Why frequency modulation is better than amplitude modulation?

LESSON 8

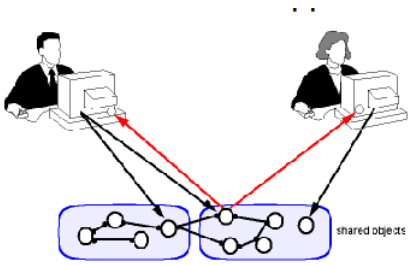
Distributed Systems

8.1. Outline

- What is a Distributed System
- Why bother with them?
- Examples of Distributed Systems Common
- Characteristics
- Summary
- What is a Distributed System?

8.2. What is Distributed?

Data are Distributed - If data must exist in multiple computers for admin and ownership reasons
Computation is Distributed - Applications taking advantage of parallelism, multiple processors, particular feature Scalability and heterogeneity of Distributed System
Users are Distributed - If Users communicate and interact via application (shared objects



8.3. History of Distributed Computing

- 1940. The British Government came to the conclusion that 2 or 3 computers would be sufficient for UK
- 1960Mainframe computers took up a few hundred square feet.

- 1970. First Local Area Networks (LAN) such as Ethernet.
- 1980. First network cards for PCs.
- 1990. First wide area networks, the Internet, that evolved from the US Advanced Research Projects Agency net (ARPANET, 4 nodes in 1969) and was, later, fueled by the rapid increase in network bandwith and the invention of the World Wide Web at CERN in 1989.

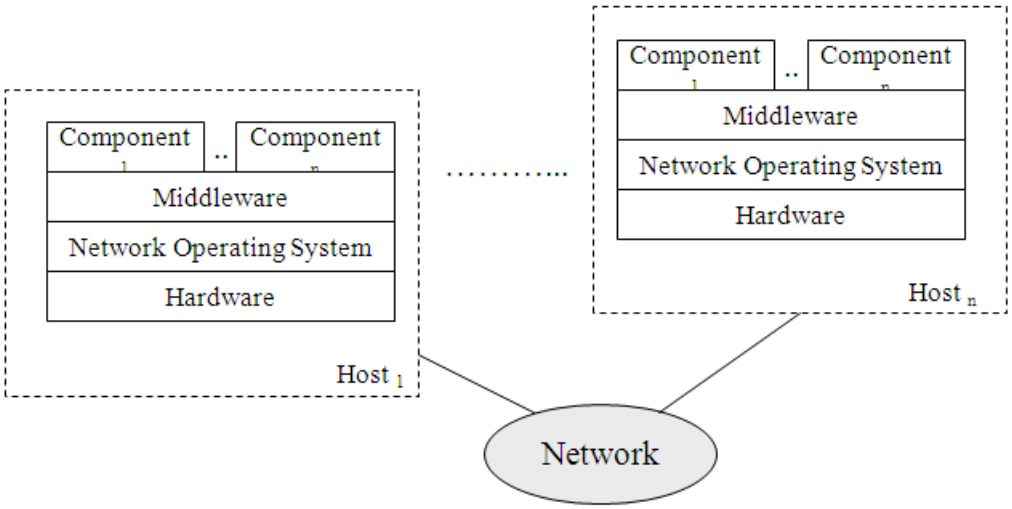
8.4. Centralised System Characteristics

- Non-autonomous parts: The system possesses full control.
- Homogeneous: Constructed using the same technology (e.g., same programming language and compiler for all parts). Component shared by all users all the time.
- All resources accessible. Software runs in a single process.
- Single Point of control.
- Single Point of failure (either they work or they do not work).

8.5. Distributed System Characteristics

- Multiple autonomous components.
- Heterogeneous. Components are not shared by all users
- Resources may not be accessible.
- Software runs in concurrent processes on different processors.
- Multiple Points of control.
- Multiple Points of failure (but more fault tolerant

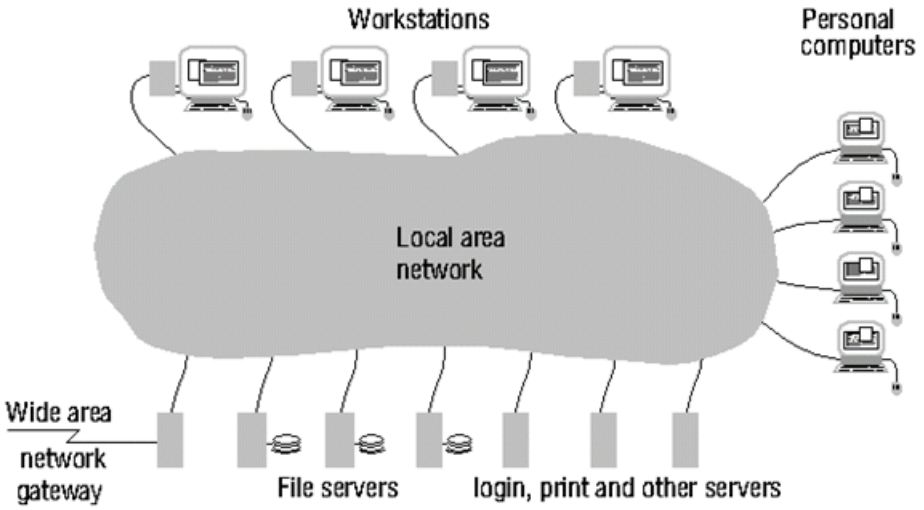
8.6. Model of a Distributed System



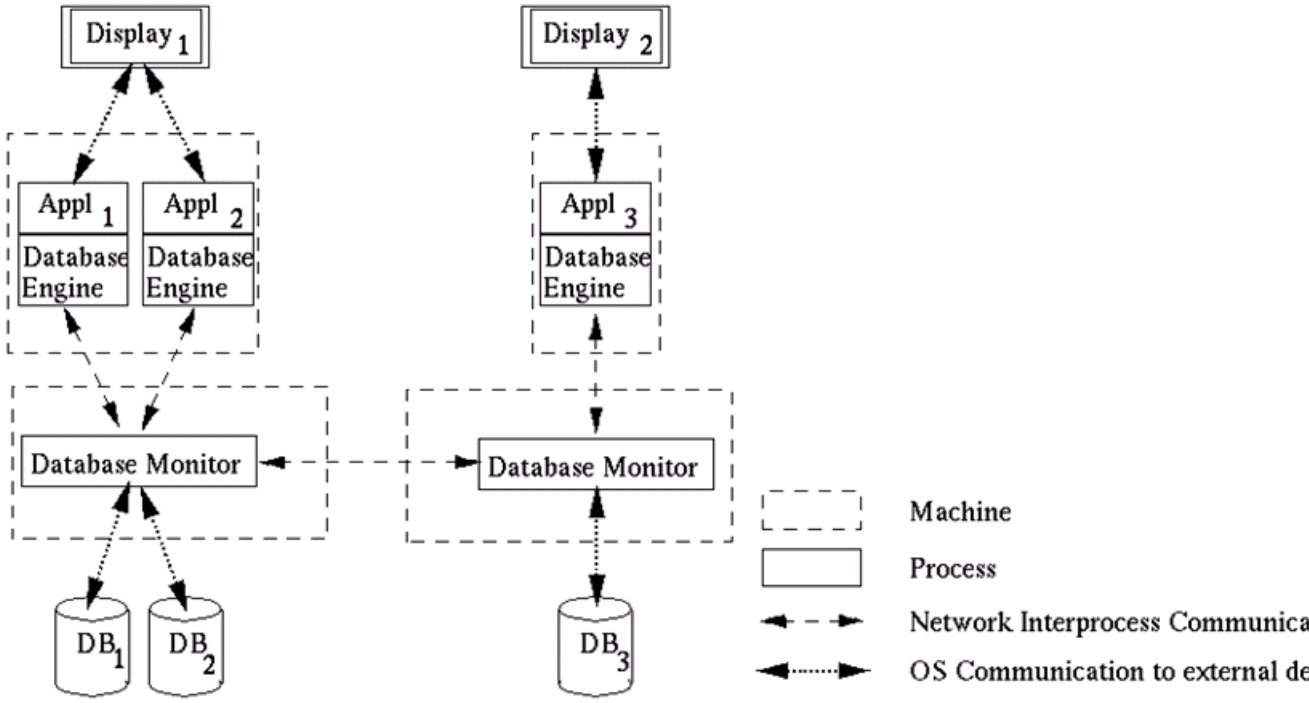
8.6.1. Examples of Distributed Systems

- Local Area Network
- Database Management System
- Automatic Teller Machine Network
- World-Wide Web

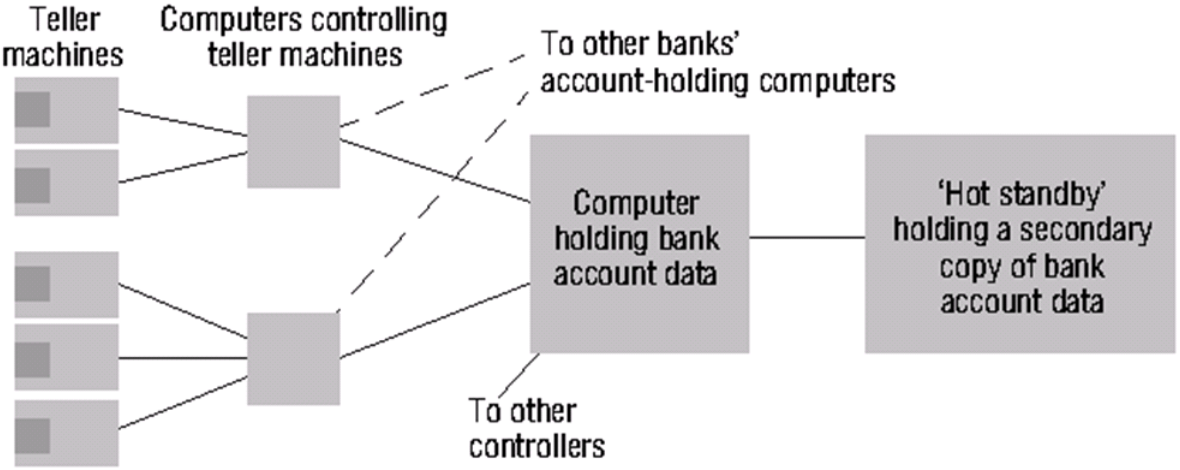
Local Area Network



Database Management System



Automatic Teller Machine Network



8.7. Common Characteristics

What are we trying to achieve when we construct a distributed system?
Certain common characteristics can be used to assess distributed systems

- Resource Sharing
- Openness
- Concurrency

- Scalability
- Fault
- Tolerance
- Transparency

8.7.1. Resource Access and Sharing

- Ability to use any hardware, software or data anywhere in the system ... once authorised!.
- Security implications: Resource manager controls access, provides naming scheme and controls concurrency.
- Resource sharing model: client/server vs n-tier architectures

8.7.2. Openness

- Openness is concerned with extensions and improvements of distributed systems
- Openness is concerned with extensions and improvements of distributed systems
- It is crucial because the overall architecture needs to be stable even in the face of changing functional requirements.

8.7.3. Concurrency

- Components in distributed systems are executed in concurrent processes.
- Components access and update shared resources (e.g. variables, databases, device drivers).
- Integrity of the system may be violated if concurrent updates are not coordinated.
  - Lost updates
  - Inconsistent analysis

8.7.4. Scalability

- Adaptation of distributed systems to

1. accommodate more users
2. respond faster (this is the hard one)

- Usually done by adding more and/or faster processors.
- Components should not need to be changed when scale of a system increases.
- Design components to be scalable!

8.7.5. Fault Tolerance

- Hardware, software and networks fail!
- Distributed systems must maintain availability even at low levels of hardware/software/ network reliability.
- fault tolerance is achieved by

1. Redundancy (replication)
2. Recovery
3. Design

8.7.6. Transparency

- Distributed systems should be perceived by users and application programmers as a whole rather than as a collection of cooperating components
- Transparency has different aspects that were identified by ANSA (Advanced Network Systems Architecture).
- These represent properties that a well-designed distributed systems should have
- They are dimensions against which we measure middleware components

8.7.7. Access Transparency

- Enables local and remote information objects to be accessed using identical operations, that is, the interface to a service request is the same for communication between components on the same host and components on different hosts.
- Example: File system operations in Unix Network File System (NFS).
- A component whose access is not transparent cannot easily be moved from one host to the other. All other components that request services would first have to be changed to use a different interface.

8.7.8. Location Transparency

- Enables information objects to be accessed without knowledge of their physical location.
- Example: Pages in the Web.
- Example: When an NFS administrator moves a partition, for instance because a disk is full, application programs accessing filEnables information objects to be accessed without knowledge of their physical location. Example: Pages in the Web. Example: When an NFS administrator moves a partition, for instance because a disk is full, application programs accessing files in that partition would have to be changed if file location is not transparent for them. es in that partition would have to be changed if file location is not transparent for them.

8.7.9. Migration Transparency

- Allows the movement of information objects within a system without affecting the operations of users or application programs.
- It is useful, as it sometimes becomes necessary to move a component from one host to another (e.g., due to an overload of the host or to a replacement of the host hardware).

- Without migration transparency, a distributed system becomes very inflexible as components are tied to particular machines and moving them requires changes in other components.

8.7.10. Replication Transparency

- Enables multiple instances of information objects to be used to increase reliability and performance without knowledge of the replicas by users or application programs.
- Example: Distributed DBMS.
- Example: Mirroring Web Pages.

8.7.11. Concurrency Transparency

- Enables several processes to operate concurrently using shared information objects without interference between them. Neither user nor application engineers have to see how concurrency is controlled.
- Example: Bank applications.
- Example: Database management system

8.7.12. Scalability Transparency

- Allows the system and applications to expand in scale without change to the system structure or the application algorithms. How system behaves with more components Similar to performance Transparency, i.e QoS provided by applications.
- Example: World-Wide-Web.
- Example: Distributed Database

8.7.13. Performance Transparency

- Allows the system to be reconfigured to improve performance as loads vary.
- Consider how efficiently the system uses resources.

- Relies on Migration and Replication transparency Example: TCP/IP routes according to traffic.
- Load Balancing.
- Difficult to achieve because of dynamism

Allows the system to be reconfigured to improve performance as loads vary. Consider how efficiently the system uses resources. Relies on Migration and Replication transparency Example: TCP/IP routes according to traffic. Load Balancing. Difficult to achieve because of dynamism

8.7.14. Failure Transparency

- Enables the concealment of faults!
- Components can be designed without taking into account that services they rely on might fail.
- Server components can recover from failures without the server designer taking measures for such recovery.
- Allows users and applications to complete their tasks despite the failure of other components.
- Its achievement is supported by both concurrency and replication transparency.

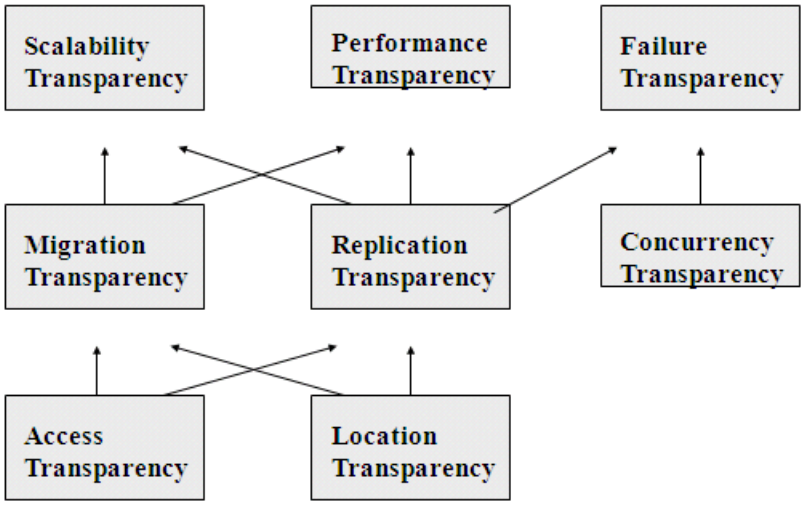
8.8. Dimensions Of Transparency

Example . What is modulation and demodulation?

Solution: Modulation is the process of altering the characteristics of the amplitude, frequency, or phase angle of the high-frequency signal in accordance with the instantaneous value of the modulating wave. Demodulation is the process of extracting the original information signal from a modulated carrier signal. □

Revision Questions

EXERCISE 38. What is a distributed system and how does it compare to a centralised system?



EXERCISE 39. ✍ What are the characteristics of distributed systems?

EXERCISE 40. ✍ What are the different dimensions of transparency?

LESSON 9

Metropolitan and Wide Area Networks

Outline

- Introduction
- Circuit Switched Networks
- Dedicated Circuit Networks
- Packet Switched Networks
- Virtual Private Networks
- Best practice MAN/WAN design
- Improving MAN and WAN Performance

9.1. Introduction

- Metropolitan area networks (MANs)
  Span from 3 to 30 miles and connect backbone networks (BNs) and LANs
- Wide area networks (WANs)
  Connect BNs and MANs across longer distances, often hundreds of miles or more
- Typically built by using leased circuits from common carriers such as AT&T
  Most organizations cannot afford to build their own MANs and WANs,

9.1.1. Introduction (Cont.)

- Focus of the lecture
  - Examine MAN/WAN architectures and technologies from a network manager point of view
    - Focus on services offered by common carriers, and how they can be used to build networks
- Regulation of services
  - Federal Communications Commission (FCC) in the US
  - Canadian Radio Television and Telecomm Commission (CRTC) in Canada
  - Public Utilities Commission (PUC) in each state
- Common Carriers
  - Local Exchange Carriers (Less) like Verizon, Bell South
  - Interexchange Carriers (IXCs) like AT&T

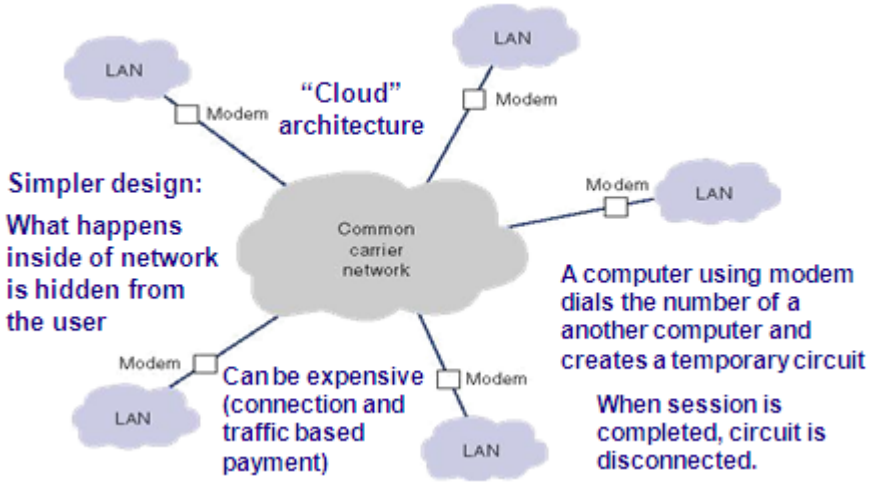
9.1.2. Services Used by MANs/WANs

- Circuit Switched Network Services
- Dedicated Circuit Networks Services
- Packet Switched Networks Services
- Virtual Private Networks Services

9.1.3. Circuit Switched Services

- Oldest and simplest MAN/WAN approach
- Uses the Public Switched Telephone Network (PSTN)
  - i.e., telephone networks
- Provided by common carriers like AT&T and Ameritech
- Basic types in use today:
  - POTS (Plain Old Telephone Service)
    - Via use of modems to dial-up and connect to ISPs
  - ISDN (Integrated Services Digital Network)

9.2. Basic Architecture of Circuit Switched Services



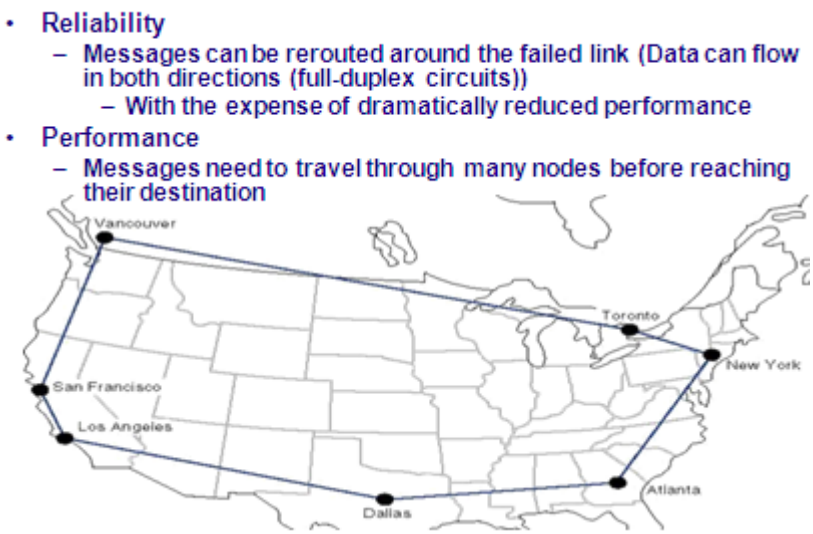
9.2.1. Broadband ISDN

- A circuit-switched service but it uses ATM to move data
- Backwardly compatible with ISDN.
- B-ISDN services offered:
  - Full duplex channel at 155.2 Mbps

  - Full duplex channel at 622.08 Mbps
  - Asymmetrical service with two simplex channels (Upstream: 155.2 Mbps, downstream: 622.08 Mbps)

- **Circuit Switched Services**
  - Simple, flexible, and inexpensive
    - When not used intensively
  - Main problems
    - Varying quality
      - Each connection goes through the regular telephone network on a different circuit,
    - Low Data transmission rates
      - Up to 56 Kbps for POTS, and up to 1.5 Mbps for ISDN
  - An alternative
    - Use a private dedicated circuit
      - Leased from a common carrier for the user's exclusive use 24 hrs/day, 7 days/week

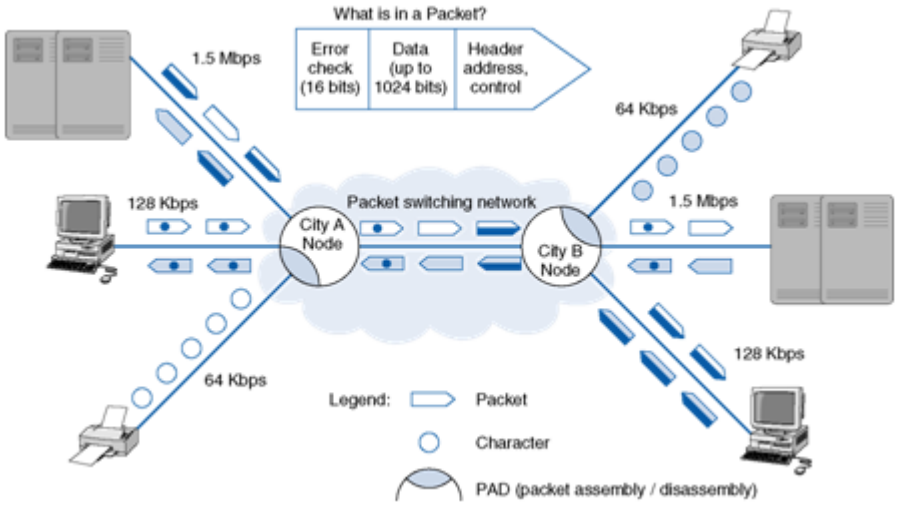
- **Ring Architecture**



9.2.2. Star Architecture

- Easy to manage
  - Central computer routes all messages in the network
- Reliability
  - Failure of central computer brings the network down
  - Failure of any circuit or computer affects one site only
- Performance
  - Central computer becomes a bottleneck under high traffic

- **Packet Switching Concepts**



- **Packet Routing Methods**
  - Describe which intermediate devices the data is routed through
  - Connectionless (Datagram)
    - Adds a destination and sequence number to each packet
    - Individual packets can follow different routes
    - Packets reassembled at destination (by using their sequence numbers)
  - Connection Oriented (Virtual Circuit (VC))
    - Establishes an end-to-end circuit between the sender and receiver (before the packets sent)
    - All packets for that transmission take the same route over the virtual circuit established
    - Same physical circuit can carry many VCs
- **Ethernet/IP Packet Networks**
  - Offer Ethernet/IP packet services for building MAN/WAN networks
    - Gigabit Ethernet fiber optic networks (bypassing common carrier network)
  - Currently offer CIR speeds from 1 Mbps to 1 Gbps at 1/4 the cost of more traditional services
  - No need to translate LAN protocol (Ethernet/IP) to the protocol used in MAN/WAN services
    - X.25, ATM, Frame Relay and SMDS use different protocols requiring translation from/to LAN protocols
  - Emerging technology; expect changes

- **VPN Types**
  - Intranet VPN
    - Provides virtual circuits between organization offices over the Internet
  - Extranet VPN
    - Same as an intranet VPN except that the VPN connects several different organizations, e.g., customers and suppliers, over the Internet
  - Access VPN
    - Enables employees to access an organization's networks from remote locations
- **MAN/WAN Design Practices**
  - Difficult to recommend best practices
    - Services, not products, being bought
    - Fast changing environment with introduction of new technologies and services from non-traditional companies
  - Factors used
    - Effective data rates and cost
    - Reliability
    - Network integration
  - Design Practices
    - Start with flexible packet switched service
    - Move to dedicated circuit services, once stabilized
    - May use both: packet switched services as backup

- **Improving MAN/WAN Performance**
  - Handled in the same way as improving LAN performance
    - By checking the devices in the network,
    - By upgrading the circuits between computers
    - By changing the demand placed on the network
- **Improving Device Performance**
  - Upgrade the devices (routers) and computers that connect backbones to the WAN
    - Select devices with lower "latency"
      - Time it takes in converting input packets to output packets
  - Examine the routing protocol (static or dynamic)
    - Dynamic routing
      - Increases performance in networks with many possible routes from one computer to another
      - Better suited for "bursty" traffic
      - Imposes an overhead cost (additional traffic)
        - Reduces overall network capacity
        - Should not exceed 20%
- **Improving Circuit Capacity**
  - Analyze the traffic to find the circuits approaching capacity
    - Upgrade overused circuits
    - Downgrade underused circuits to save cost
  - Examine why circuits are overused
    - Caused by traffic between certain locations
      - Add additional circuits between these locations

  - Capacity okay generally, but not meeting peak demand
    * Add a circuit switched or packet switched service that is only used when demand exceeds capacity
  - Caused by a faulty circuit somewhere in the network
    * Replace and/or repair the circuit
- Make sure that circuits are operating properly

9.2.3. Reducing Network Demand

- Determine impact on network
  - Require a network impact statement for all new application software
- Use data compression of all data in the network
- Shift network usage
  - From peak or high cost times to lower demand or lower cost times
  - e.g., transmit reports from retail stores to headquarters after the stores close
- Redesign the network
  - Move data closer to applications and people who use them
  - Use distributed databases to spread traffic across

- **Implications for Management**
  - Changing role of networking and telecom managers
    - Increased and mostly digitized data transmission causing the merger of these positions
  - Changing technology
    - Increasing dominance of VPNs, Frame Relay and Ethernet/IP
    - Decreasing cots of setting up MANs/WANs

- Changing vendor profiles
  - From telecom vendors to vendors with Ethernet and Internet experiences

Example . What is metropolitan area network (MAN)?

Solution: A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN). The term is applied to the interconnection of networks in a city into a single larger network (which may then also offer efficient connection to a wide area network). It is also used to mean the interconnection of several local area networks by bridging them with backbone lines. The latter usage is also sometimes referred to as a campus network. Examples of metropolitan area networks of various sizes can be found in the metropolitan areas of London, England; Lodz, Poland; and Geneva, Switzerland. Large universities also sometimes use the term to describe their networks. A recent trend is the installation of wireless MANs. □

Revision Questions

EXERCISE 41. What makes a WAN different from a LAN and MAN?

EXERCISE 42. What are the advantages and disadvantages of the following networks local area networks wide area networks and metropolitan area network metropolitan area network?

EXERCISE 43. How metropolitan area network is different from local area network?

EXERCISE 44. Can Wide Area Network become Metropolitan Area Network?

EXERCISE 45. What is the difference Controller area network and Metropolitan area network?

LESSON 10

Mutual Exclusion & Election Algorithms

10.1. Process Synchronization

Techniques to coordinate execution among processes

- One process may have to wait for another
- Shared resource (e.g. critical section) may require exclusive access

10.2. Distributed Mutual Exclusion

Assume there is agreement on how a resource is identified

- Pass identifier with requests

Create an algorithm to allow a process to obtain exclusive access to a resource

- Centralized Algorithm
- Token Ring Algorithm
- Distributed Algorithm
- Decentralized Algorithm

10.2.1. Centralized algorithm

- Mimic single processor system
- One process elected as coordinator
  - Request resource
  - Wait for response
  - Receive grant
  - access resource
  - Release resource

If another process claimed resource:

- Coordinator does not reply until release
- Maintain queue
  - Service requests in FIFO order

- **Benefits**
  - Fair
  - All requests processed in order
  - Easy to implement, understand, verify

- **Problems**
  - Process cannot distinguish being blocked from a dead coordinator
  - Centralized server can be a bottleneck

10.2.2. Token Ring algorithm

Assume known group of processes

- Some ordering can be imposed on group
- Construct logical ring in software
- Process communicates with neighbor
- Initialization
  - Process 0 gets token for resource R
- Token circulates around ring
- When process acquires token
  - Checks to see if it needs to enter critical section
  - If no, send token to neighbor
  - If yes, access resource
    - Hold token until done

Only one process at a time has token

- Mutual exclusion guaranteed

Order well-defined

- Starvation cannot occur

If token is lost (e.g. process died)

- It will have to be regenerated

Does not guarantee FIFO order

- sometimes this is undesirable

10.2.3. Ricart & Agrawala algorithm

- Distributed algorithm using reliable multicast and logical clocks
- Process wants to enter critical section:
  - Compose message containing:
    - Identifier (machine ID, process ID)
    - Name of resource
    - Timestamp (totally-ordered Lamport)
- Send request to all processes in group
- Wait until everyone gives permission
- Enter critical section / use resource
- When process receives request:
- If receiver not interested: - Send OK to sender
- If receiver is in critical section - Do not reply; add request to queue
- If receiver just sent a request as well:
  - Compare timestamps: received & sent messages

  - Earliest wins
  - If receiver is loser, send OK
  - If receiver is winner, do not reply, queue
  - No points of failure
  - A lot of messaging traffic
  - Demonstrates that a fully distributed algorithm is possible

10.2.4. Election Algorithms

Example ✎. If we are using one process as a coordinator for a shared resource . . . how do we select that one process?

Solution: All nodes currently involved get together to choose a coordinator
If the coordinator crashes or becomes isolated, elect a new coordinator
If a previously crashed or isolated node, comes on line, a new election may have to be held □

- Wired systems
  - Bully algorithm
  - Ring algorithm
- Wireless systems
- Very large-scale systems

10.2.5. Wireless Environments

- Unreliable, and nodes may move
- Network topology constantly changing Algorithm:
  - Any node starts by sending out an ELECTION message to neighbors
  - When a node receives an ELECTION message for the first time, it forwards to neighbors, and designates the sender as its parent
  - It then waits for responses from is neighbors Responses may carry resource information

- When a node receives an ELECTION message for the second time, it just OKs it

10.2.6. Very Large Scale Networks

- Sometimes more than one node should be selected
- Nodes organized as peers and super-peers
  - Elections held within each peer group
  - Super-peers coordinate among themselves

Revision Questions

Example ✎. What are some challenges in designing a distributed applicaiton?

Solution: //
Time management
Process communication
Security
Scalability
Failure handling □

EXERCISE 46. ✍ Describe how time management can be a challenge in designing a Distributed applicaiton and explain how this can be addressed?

EXERCISE 47. ✍ What are the who time management algorithms?

EXERCISE 48. ✍ What is the logical clock solution for time management issues in DS?

EXERCISE 49. ✍ Describe how Process communication can be a challenge in designing a Distributed applicaiton and explain how this can be addressed?

EXERCISE 50. ✍ Describe the types of failures that can occur in distributed systems?

EXERCISE 51. ✍ Define the happened before relation on events in a distributed system and describe how logical clocks can be used to capture this relation numerically?

EXERCISE 52. ✍ Describe the distributed mutual exclusion problem and list two correctness properties a distributed mutual exclusion algorithm must satisfy?

EXERCISE 53. ✍ Give an example execution of the bully election algorithm to illustrate how this algorithm supports dealing with process failure?

Solutions to Exercises

Exercise 2. Access to the network is provided at fixed time intervals Exercise 2

Exercise 3. Hub – Broadcasts data it receives to all devices connected to its ports. Switch – Establishes a direct connection from the sender to the destination without passing the data traffic to other networking devices. Exercise 3

Exercise 10. This type of answer lets the interviewer know more about your specific level of experience rather than just your level of technical knowledge. In just about every case, experience trumps knowledge. Exercise 10

Exercise 30. Ans. In it, the modulating technique is applied to the analog information signal. Its various techniques are:
• Amplitude modulation(AM)
• Frequency modulation(FM)
• Phase modulation(PM) Exercise 30

Exercise 31. Modulation is required to send the information over long distances as low frequency signals are not able to cover large area. While demodulation is required to get back the information sent at the receiving side. Exercise 31

Exercise 36. There are several ways of demodulation depending on how parameters of the carrier signal, such as amplitude, frequency or phase.
• For a signal modulated with a linear modulation, like AM, we can use a synchronous detector.
• For a signal modulated with an angular modulation, we must use an FM demodulator or a PM demodulator.Modulation is better as it provide more resistance to noise as compared to demodulation. Exercise 36

Exercise 37. Modulation is better as it provide more resistance to noise as compared to demodulation. Exercise 37

Exercise 46. //Some distributed algorithms depend on clock synchronization, however, full synchronization is not possible and hence presents one challenge of distributed system. Can be addressed with algorithms like Christian's algorithm (Poll central time server) or the Berkeley's algorithm (An average of all clock times). Other solutions include logical time such as lamport clocks, and enhancing them by using Vector clocks. Exercise 46

Exercise 47. //There are two synchronization methods that attempt to achieve near-full synchronization: Christian's algorithm (Poll a central time server and factor in transmission time) and Berkeley's algorithm (A central process polls all other processes and averages their clocks. Returns to each process the amount by which it must alter its clock). There is a possibility for error in both circumstances so neither can guarantee full synchronization. Exercise 47

Exercise 52. //Distributed mutual exclusion algorithms are used to ensure data consistency and are used to prevent process interference. These are often build on top of the message passing paradigm; in some algorithms using multicast, using a token held by a central server, or a token which is passed around in a ring (Possession of token allows entry to critical region). Once a process has been satisfied some condition, it can then enter a 'critical region' where it is guaranteed to be the only process allowed to access the critical region. Two correctness properties that a distributed mutual exclusion algorithm must satisfy are Safety- which ensures at most one process can be inside a critical region at any given point, and Liveness which ensures that a request to enter the critical region is eventually granted. A third possible is Maintains Happened Before Ordering so access ordering honors the ordering of requests Exercise 52