Mesleki İngilizce - Technical English

II

Prof. Dr. Nizamettin AYDIN

naydin@yildiz.edu.tr

http://www.yildiz.edu.tr/~naydin

- Notes:
  - In the slides,
    - texts enclosed by curly parenthesis, {…}, are examples.
    - texts enclosed by square parenthesis, […], are explanations related to examples.

Networks

- Learning Objectives
  - to acquire basic vocabulary related to network concepts
  - to become familiar with different technologies
  - to understanding, the limits, capabilities, and benefits of specific network hardware
- Sub-areas covered
  - Computer networks
  - Internet

Networks

- Keywords
  - Connection
    - In networking, a connection refers to pieces of related information that are transferred through a network
  - Packet
    - A packet is the most basic unit that is transferred over a network.
    - When communicating over a network, packets are the envelopes that carry your data from one end point to the other
  - Network Interface
    - A network interface can refer to any kind of software interface to networking hardware

Networks

- Keywords
  - LAN
    - stands for "local area network".
    - refers to a network or a portion of a network that is not publicly accessible to the greater internet
  - WAN
    - stands for "wide area network".
    - means a network that is much more extensive than a LAN.
  - Protocol
    - a set of rules and standards that basically define a language that devices can use to communicate.
    - There are a great number of protocols in use extensively in networking, and they are often implemented in different layers.

Networks

- Keywords
  - Bandwidth
    - the amount of data that can be carried from one point to another in a given time period
  - Topology
    - The physical layout of a network
  - Cryptography
    - the study of encryption and decryption.

Networks

- Reading text
- Pre-reading questions
  - What is a protocol?
  - Which device forwards packets between networks by processing the routing information included in the packet?
  - What is called the physical or logical arrangement of network?
  - Which data communication system spans states, countries, or the whole world?

7

Networks-Introduction

- Comparing a data network to a living organism,
  - the hardware provides the skeleton or basic infrastructure upon which the nervous system is built.
- Similarly, a few hundred meters of cable running through the walls of a laboratory is necessary
  - but insufficient to constitute a network.
- Rather, the data pulsing through cables or other media in a coordinated fashion define a network.

8

Networks-Introduction

- This coordination is provided by electronics that
  - connect workstations and shared computer peripherals with the networks
  - amplify, route, filter, block, and translate data.
- An informatics researcher should have a basic understanding of the limits, capabilities, and benefits of specific network hardware,
  - to be able to converse intelligently with hardware vendors
  - to direct the management of an information services provider.

9

Networks-Introduction

- The Internet was a natural successor to the cold war projects in the 1950s and early 1960s
- The modern Internet was the unintended outcome of two early complex systems:
  - the ARPANET (Advanced Research Project Agency Network)
  - the SAGE system (semiautomatic ground environment),
    - developed for the military in the early 1950s and 1960s, respectively.

10

Networks-Introduction

- SAGE was the national air defense system comprised of
  - an elaborate, ad hoc network of incompatible command and control computers,
  - early warning radar systems,
  - weather centers,
  - air traffic control centers,
  - ships,
  - planes,
  - weapons systems.

11

Networks-Introduction

- The communications network component of the SAGE system was comprehensive and extended beyond the border of the U.S. and included ships and aircraft.
- It was primarily a military system,
  - with a civil defense link as its only tie with civilian communications system.
- In the 1950s and 1960s, federally funded researchers at academic institutions explored ways to manage the growing store of digital data amid the increasingly complex network of computers and networks.
- One development was hypertext,
  - a cross-referencing scheme,
    - where a word in one document is linked to a word in the same or a different document.

12

Networks-Introduction

- Around the time the ARPANET was born, a number of academic researchers began experimenting with computer-based systems that used hypertext.
  - For example, in the early 1970s, a team at Carnegie-Mellon University developed ZOG,
    - a hypertext-based system that was eventually installed on a U.S. aircraft carrier.
- ZOG was a reference application that provided the crew with online documentation that was richly cross-linked to improve speed and efficiency of locating data relevant to operating shipboard equipment.

13

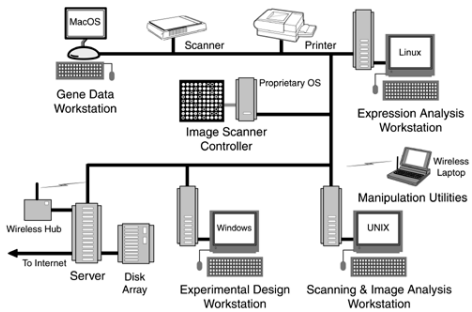
Networks-Introduction

- In addition to applications for the military, a variety of commercial, hypertext-based document management systems were spun out of academia and commercial laboratories,
  - such as the Owl Guide hypertext program from the University of Kent, England, and
  - the Notecards system from Xerox PARC in California.
- Both of these systems were essentially stand-alone equivalents of a modern Web browser,
  - but based on proprietary document formats with content limited to what could be stored on a hard drive or local area network (LAN).
- In this circuitous way, out of the quest for national security through an indestructible communications network,
  - the modern Internet was born.

14

Networks-Example

- Microarray Laboratory Network



15

Networks-Example

- The computers in a typical microarray laboratory present a mixture of
  - data formats,
  - operating systems,
  - processing capabilities.
- The network in this example (a wired and wireless local area network) supports
  - the microarray laboratory processes,
    - from experimental design and array fabrication to expression analysis and publishing of results.

16

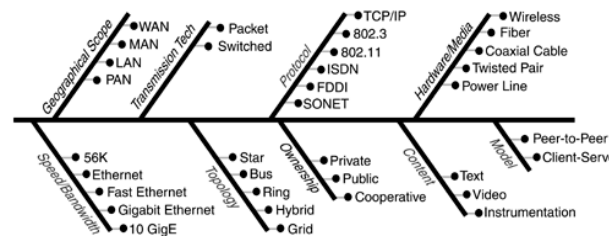
Networks

- A network architecture should be examined from the perspective of:
  - Geographical scope
  - Underlying model or models used to implement the network
  - Signal transmission technology
  - Bandwidth or speed
  - Physical layout or topology
  - Protocol or standards used to define how signals are handled by the network
  - Ownership or funding source involved in network development
  - Hardware, including
    - cables, wires, and other media used to provide the information conduit from one device to the next
  - Content carried by the network

17

Networks

- **Network Taxonomy**



18

Networks

- There are multiple networking Technologies:
  - Personal Area Network (PAN)
  - Local Area Network (LAN)
  - Metropolitan Area Network (MAN)
  - Wide Area Network (WAN)
  - Storage Area Network (SAN)
  - Enterprise private network (EPN)
  - Virtual private network (VPN)
  - Global Area Network (GAN)
  - Wireless Local Area Network (WLAN)
  - Controller Area Network (CAN)
  - Internet Area Network (IAN)

19

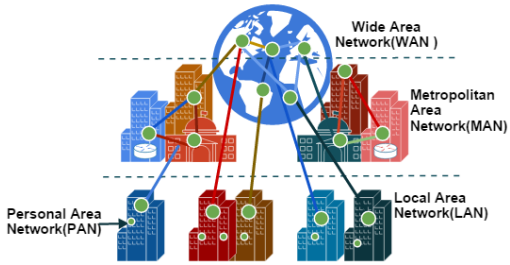
Networks

- **Geographical Scope**
- The geographical extent of a network is significant because it affects
  - bandwidth,
  - security,
  - response time,
  - the type of computing possible.
    - For example, it is only because of the high-speed Internet backbone that real-time teleconferencing and model sharing are possible on a worldwide basis.

20

Networks

- Informatics R&D incorporates network resources on worldwide (WAN), institution-wide (MAN), and laboratory-wide (LAN and PAN) levels.



21

Networks

- **PAN**
  - personal area network
- a computer network used for communication among computer devices,
  - including telephones, personal digital assistants, …
- limited to the immediate proximity of the user, or about a 10-meter radius,
- If PAN is constructed using wireless technology,
  - known as wireless personal area network (WPAN)

22

Networks

- **PAN**

23

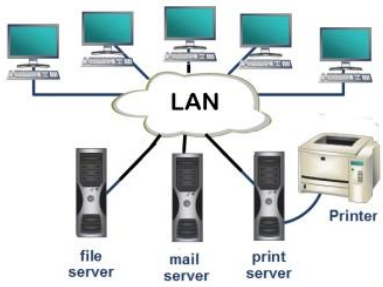
Networks

- **LAN**
  - local area network
- a network that is restricted to smaller physical areas
  - extend to about 100-meters from a central server, or a single floor in a typical research building.
    - e.g. a local office, school, or house.
- Approximately all current LANs whether wired or wireless are based on Ethernet.
- Data transfer speeds can extend to
  - 10.0 Mbps (Ethernet network)
  - 1.0 Gbps (Gigabit ethernet)
- Coaxial cable and CAT 5 cables are normally used for connection.

24

Networks

- **LAN**



25

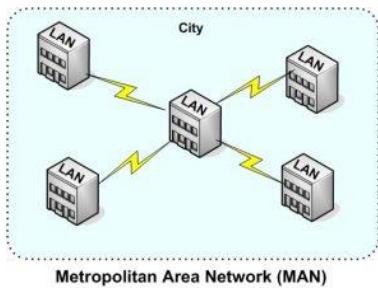
Networks

- **MAN**
  - Metropolitan Area Network
- take over where LANs leave off,
  - covering entire buildings and extending tens of kilometers.
- typically implemented with digital subscriber line (DSL), cable modem, and fixed wireless technologies.
- Several LANs are often connected to make a MAN.
  - When this configuration is used for a college campus, it is referred to as a campus area network (CAN).

26

Networks

- **MAN**



27

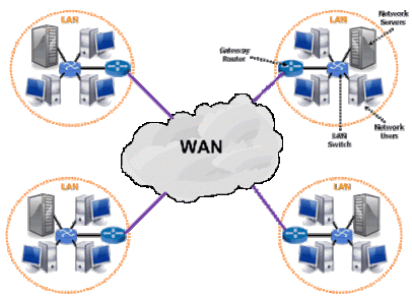
Networks

- **WAN**
  - Wide Area Network
- connects computers together over large physical distances,
  - such as entire country or entire world
- typically composed of a combination of
  - terrestrial fixed satellite systems, coaxial cable, and fiber optical cable.
- The public switched telephone network and the Internet are examples of WANs.

28

Networks

- **WAN**



29

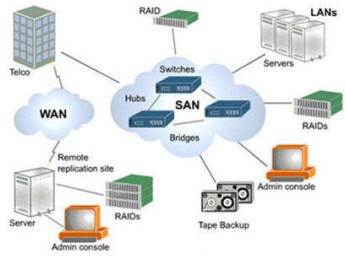
Networks

- **SAN**
  - Storage area network
- connects servers directly to devices to store data
- moves storage resources off the common user network and reorganizes them into an independent, high-performance network.
  - So, each server is allowed to access shared storage.
    - This can involve Fibre-channel connection, similar to Ethernet, to handle high-performance disk storage for application.

30

Networks

- **SAN**

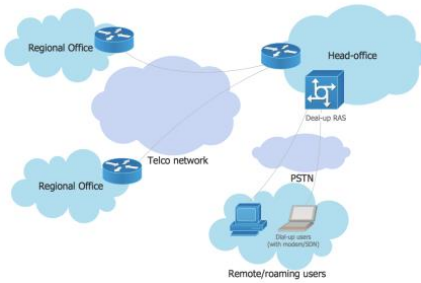


Networks

- **EPN**
  - Enterprise Private Network
- a computer network built to share computer resources among different sites
  - such as production sites, offices and shops of a business
- Some of the advantages of an EPN:
  - The messages are secure because they are encrypted.
  - They are cost effective and scalable.
  - They help to centralize IT resources.
  - They enable business continuity.

Networks

- **EPN**

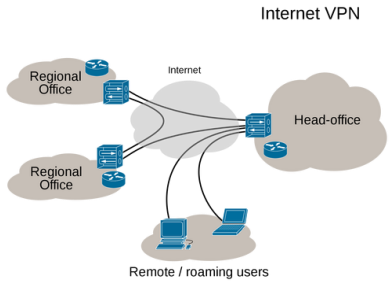


Networks

- **VPN**
  - Virtual Private Network
- an extended private network which spreads over the internet.
- Users can send and receive data across shared or public networks.
- It uses public wires
  - usually the internet to connect to a private network
    - usually a company's private network.
- The benefit of a secure VPN is its level of security to the connected systems,
  - whereas the other network infrastructure alone can not provide it.

Networks

- **VPN**



Networks

- **GAN**
  - Global Area Network
- a network composed of different interconnected networks that cover an unlimited geographical area.
  - The term is loosely synonymous with Internet,
    - which is considered a global area network.
- **BGAN**
  - Broadband Global Area Network
    - a mobile communications system created to transmit broadband wireless voice and data communications almost anywhere on the earth's surface.
  - The system, developed by Immarsat, Inc., consists of a constellation of geostationary satellites working in conjunction with portable, lightweight, surface-based terminals about the size of a laptop.

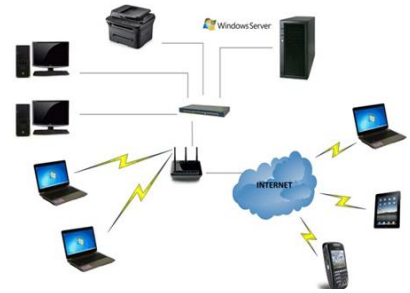
Networks

- **WLAN**
  - Wireless Local Area Network
- a wireless computer network that links two or more devices using a wireless distribution method within a limited area
  - such as a home, school, computer laboratory, or office building.
- sometimes called a local area wireless network (LAWN)
- The IEEE 802.11 group of standards specify the technologies for WLANs

37

Networks

- **WLAN**



38

Networks

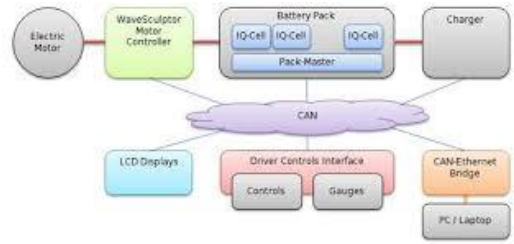
- **CAN**
  - Controller Area Network
- a serial bus network of microcontrollers that connects devices, sensors and actuators in a system or sub-system for real-time control applications.
  - Bosch originally developed the CAN in 1985 for in-vehicle networks
- Lifts and escalators use embedded CAN networks

  Hospitals use the CANopen protocol to link lift devices, such as panels, controllers, doors, and light barriers, to each other and control them.

39

Networks

- **CAN**



40

Networks

- **IAN**
  - Internet Area Network
- a concept for a communications network that connects voice and data end-points within a cloud environment over IP,
  - replacing an existing LAN, WAN or the public switched telephone network (PSTN).
- Cloud based IT & Communications interface

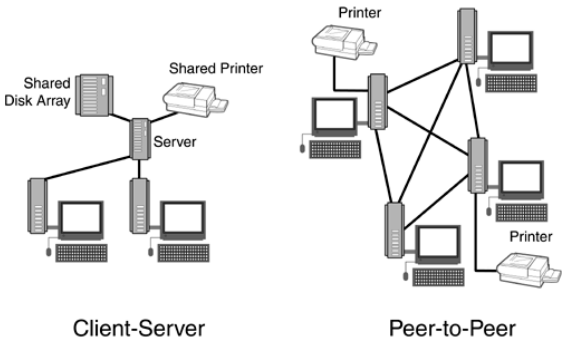
41

Communications Models

- In the traditional client-server model, a server provides data to one or more clients.
- In contrast, in a peer-to-peer network, every computer acts as a server and client to other computers on the network.
  - As such, a particular computer might function as a server one moment and as a client the next
- The simplest type of computer network to construct in a small workgroup is a peer-to-peer network.

42

Communications Models



Communications Models

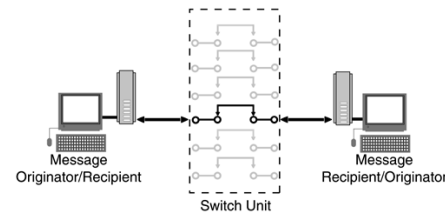
- The disadvantages of the peer-to-peer model
  - Uneven use of resources,
    - the workstations with the most relevant content are accessed more often than workstations with less frequently accessed content.
      - The result is decreased performance for computational tasks of the frequently accessed workstations.
  - Data management is more challenging.
    - Everyone in the workgroup must perform tasks such as archiving and updating antiviral utilities, for example.

Communications Models

- A client-server model employs a central server to provide programs and data files that can be accessed by client workstations on the network.
- An advantage of this model is that
  - the network operating system running on the server provides for security, tiered access privileges, and no degradation of individual workstation performance
    - because files are accessed from the server.
- In addition, the data and programs on the central server can be more easily and consistently archived, backed up, accessed, and shared.

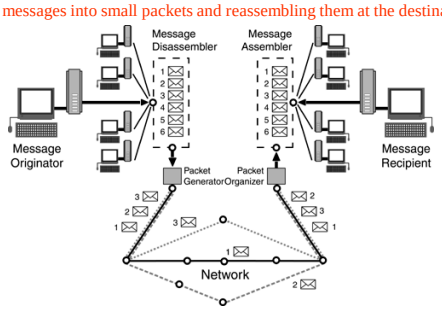
Transmissions Technology

- **Switched Communications**
  - A fixed, continuous bi-directional connection is established between the message source and recipient.



Transmissions Technology

- **Packet Communications**
  - Multiple, virtual communications channels are established by breaking up messages into small packets and reassembling them at the destination



Protocols

- Network protocols
  - formal standards and policies comprised of rules, procedures and formats that define communication between two or more devices over a network.
  - govern the end-to-end processes of timely, secure and managed data or network communication.
- The key standards organizations that define or suggest network protocols:
  - the Open Systems Interconnection (OSI) group,
  - the Institute of Electrical and Electronics Engineers (IEEE),
  - the Consultative Committee on International Telegraphy and Telephony
  - International Telecommunications Union-Telecommunications Sector
  - the American National Standards Institute (ANSI),
  - the Exchange Carriers Standards Association (ECSA),
  - the Alliance for Telecommunications Industry Solutions (ATIS)
- OSI, begun by the International Organization for Standardization in the late 1970s, defines high-level communications architectures, including the OSI Reference Model

Protocols

- **The OSI Reference Model**
  - OSI defines the communications process into seven different categories that deal with communications and network access.

Layer	Name	Focus
7	Application	Semantics
6	Presentation	Syntax
5	Session	Dialog coordination
4	Transport	Reliable data transfer
3	Network	Routing and relaying
2	Data Link	Technology-specific transfer
1	Physical	Physical connections

- The IEEE develops standards for the entire computing industry, including wired and wireless networks
  - these standards define specific low-level functionality, such as operating frequency, bandwidth, message format, signal voltage, and connector style for computer networks.
    - For example, the IEEE-802.3 10BaseT standard defines Ethernet over ordinary twisted pair cable

Key Network Protocols

- **The most important IEEE standards in biomedical informatics:**

Standard	Description
IEEE 488	Computer to electronic instrument communications; also known as GPIB and HPIB
IEEE-802	LAN and MAN standards
IEEE-802.3	Ethernet; the most common LAN specification
IEEE-802.3 10Base-T	Ethernet over twisted pair cable
IEEE-802.11	Wireless LANs
IEEE-802.11a	5 GHz, 54 Mbps wireless LAN; shorter range than 2.4 GHz systems, higher bandwidth, and more channels than WiFi
IEEE-802.11b	2.4 GHz, 11 Mbps wireless LAN; the most common, most mature; limited channels, also known as WiFi

Key Network Protocols

Standard	Description
IEEE-802.11e	2.4 GHz, 11 Mbps wireless LAN; enhanced quality of service
IEEE-802.11g	2.4 GHz, 22 Mbps wireless LAN; higher-bandwidth version of 802.11b, limited channels
IEEE-802.11i	2.4 GHz, 11 Mbps wireless LAN; enhanced security
CCITT/ITU-T ISDN	Digital communications over standard phone lines
CCITT/ITU-T X.25	Switched packet communications
ANSI FDDI	High-speed (200 Mbps) fiber backbone LAN
ECSA SONET	Very high-speed (10 Gbps) optical network standard
DARPA TCP/IP	The protocol of the Internet

Bandwidth

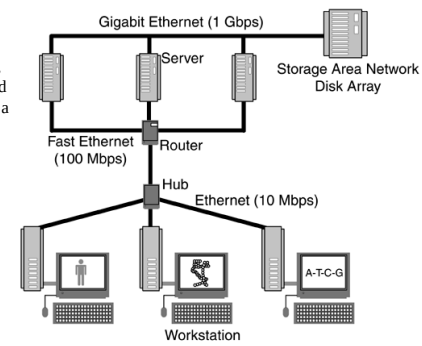
- There are three frequently used definitions of bandwidth in the context of Information Technology:
- In computer networks,
  - bandwidth is data transfer rate,
    - the amount of data that can be carried from one point to another in a given time period (usually a second).
  - Network bandwidth is usually expressed in bits per second (bps);
    - modern networks typically have speeds measured in the millions of bits per second
      - (megabits per second (Mbps)
    - or billions of bits per second
      - gigabits per second (Gbps)
  - Different applications require different bandwidths.
    - An instant messaging conversation might take less than 1000 bits per second (bps);
    - A voice over IP (VoIP) conversation requires 56 kilobits per second (Kbps) to sound smooth and clear.
    - Standard definition video (480p) works at 1 megabit per second (Mbps), but HD video (720p) wants around 4 Mbps, and HDX (1080p), more than 7 Mbps.

Bandwidth

- In signal processing/communication,
  - Bandwidth is the range of frequencies
    - the difference between the highest frequency signal component and the lowest frequency signal component
    - bandwidth is measured in hertz (cycles per second).
    - This is the original meaning of bandwidth,
      - although it is now used primarily in discussions about cellular networks and the spectrum of frequencies that operators license from various governments for use in mobile services.
- In business,
  - bandwidth is a synonym for capacity or ability.
    - In this sense, it refers to having time or staffing available to tackle something

Bandwidth

- **Network Bandwidth**
- Gigabit Ethernet, Fast Ethernet, and Ethernet provide a tiered network system that provides a compromise between system data throughput, cost, and maintenance.



Topology

- The physical layout of a network
  - a function of the practical constraints imposed by
    - the environment,
    - the protocols that must be supported,
    - the cost of installation.
- The most common protocols used with LANs, Ethernet and token ring, assume a bus and ring topology, respectively.
- The star topology is often used as a hub to connect several networks and in wireless networks,
  - where multiple devices connect via radio frequency, it links to a central wireless access point or wireless hub.

55

Topology

- Bus topology:
  - A network topology in which all nodes (stations) are connected together by a single bus.
- Mesh topology:
  - A network topology in which there are at least two nodes with two or more paths between them.
- Ring topology:
  - A network topology in which every node has exactly two branches connected to it.
- Star topology:
  - A network topology in which peripheral nodes are connected to a central node, which rebroadcasts all transmissions received from any peripheral node to all peripheral nodes on the network, including the originating node.

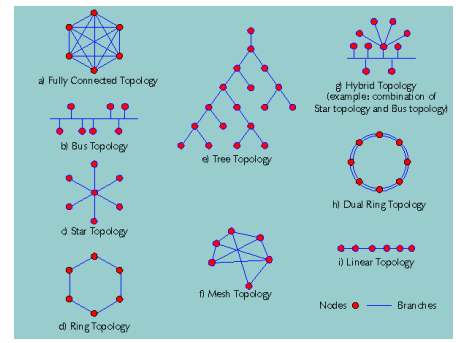
56

Topology

- Fully connected (Mesh) topology:
  - A network topology in which there is a direct path between any two nodes.
  - In a fully connected network with *n* nodes, there are *n*(*n*-1)/2 direct paths.
- Tree topology:
  - A network topology that resembles an interconnection of star networks in that individual peripheral nodes are required to transmit to and receive from one other node only, toward a central node, and are not required to act as repeaters or regenerators.
- Hybrid topology:
  - A combination of any two or more network topologies.

57

Topology



58

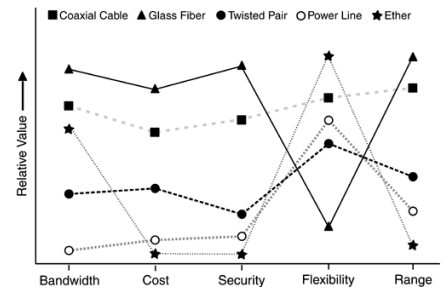
Hardware - Media

- The most common media are
  - coaxial cable,
  - twisted pair wiring,
  - fiber optics,
  - the ether (for wireless networks)
- Media Characteristics are reflected by
  - bandwidth,
  - cost,
  - security,
  - flexibility,
  - range

59

Hardware - Media

- Media Characteristics



- In this example, ether refers to wireless LAN signals

60

Hardware - Media

- **Coaxial Cable**
  - popular as a medium for LANs
  - inexpensive and provides the greatest flexibility in installation
  - the center conductor is shielded by a copper or aluminum mesh or foil,
  - provides a relatively secure connection and a high bandwidth.
  - However,
    - it's possible for someone with a sensitive receiver and antenna to remotely pick up signals traveling through coaxial cable, amplify them, and decode the digital stream

61

Hardware - Media

- **Fiber**
  - the most popular media used in networks,
  - glass fiber provides
    - the greatest bandwidth,
    - highest level of security,
    - greatest range,
    - resistance to electrical noise.
  - Although fiber provides a working range of up to several kilometers with standard electronics,
    - it's less flexible to install compared to copper cable.
    - For example, unlike twisted pair or coaxial cable, fiber can't be snaked through very tight turns because the glass fiber is more fragile than the others
  - From a security perspective, fiber is the superior medium because there is no radio frequency signal that can be intercepted by a nearby receiver

62

Hardware - Media

- **Twisted Pair**
  - the wiring used in virtually every office and residence for telephone communications,
    - is a comprise between cost, bandwidth, security, and availability.
  - more affordable than coaxial cable or fiber,
    - but the bandwidth isn't as great, and security is a much greater concern.
  - When used with radio frequency network signals,
    - twisted pair cables don't perfectly cancel out the signals traversing the two wires, but act as antennas.
    - As a result, not only are signals in the cable more readily intercepted, but the twisted pair cable is more susceptible to electrical noise in the environment.

63

Hardware - Media

- **Power Line Cable**
  - a low-cost, low-bandwidth solution to networking.
  - Although it may be suitable for exchanging text-only e-mails and other small files, the limitations of the medium prevent it from being a serious network medium for biomedical informatics applications.
  - It may be a viable as part of a redundant backup network system.
- **Ether**
  - provides the greatest flexibility,
    - but also presents the greatest security risk.
  - Typical internal installations for wireless LANs are limited to the same floor in a building.
  - However, within that space, users may have complete mobility with laptops or desktop workstations that are frequently moved.
  - Optical LANs, based on infrared (IR) links are line-of-sight only, and are limited to a single work area.

64

Hardware - Media

- Radio frequency communications are also commonly used between buildings, in the form of microwave links.
- These links tend to be line-of-sight and limited to perhaps ~50 km, depending on terrain and buildings that may interfere with line-of-sight communications.
- Unlike the radio frequency technology used with LANs, the bandwidth of these links is on the same order as coaxial cable.
- Similarly, radio frequency satellite links that extend thousands of kms support high-bandwidth transmission rates comparable to that provided by coaxial cable and fiber media.

65

Hardware - Media

- The type of media used for Internet access depends
  - primarily on the types of service available,
  - secondarily on the bandwidth, security, and cost constraints.
- The choice of media that can be used to support an internal LAN is more a function of
  - cost,
  - bandwidth requirements,
  - security,
  - ease of installation,
  - type of existing wiring, if any.

66

Network Electronics

- The media running from office to office and across the country become a useful communications channel with the addition of electronics
  - capable of sending and receiving signals through the media.
- These electronics serve a variety of functions:
  - Generating signals destined for a recipient somewhere in the network
  - Coordinating signals through media in order to minimize interference
  - Amplifying and conditioning signals so that they can continue error-free to their destination

67

Network Electronics

  - Blocking signals from certain paths to minimize interference in those paths
  - Routing signals down the quickest or least-expensive route from source to destination
  - Translating signals originally designed to work with one protocol so that they are compatible with networks designed to support other protocols
  - Connecting different networks
  - Monitoring the status of the network, including the functioning of network electronics and the amount of data on segments of the network

68

Network Electronics

- Several of the network devices

Device	Application
Bridge	Connects multiple network segments and forwards data between them
Content Filter	Prevents access of restricted external Web content
Firewall	Prevents unauthorized users from accessing the network
Gateway	Links two networks that use different protocols
Hub	Provides a central connection point for a network configured in a star topology
Modem	Connects a workstation or LAN to an outside workstation or network, such as the Internet
Monitor	Monitors activity on the network by node and by network segment

69

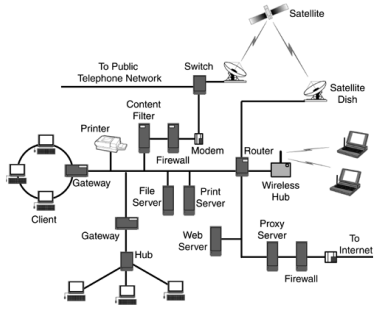
Network Electronics

Device	Application
Router	Sends data transmissions only to the portion of a network meant to receive them
Satellite	Transmits signals from a server in orbit
Server	Supplies files and applications to clients
Switch	Selects network paths at high speeds
UPS	Provides uninterruptible power for network electronics, especially servers
Wireless Hub	Provides mobile, cable-free access to servers, shared resources, and the Internet from anywhere within range of the hub
Wireless Modem	Allows workstations and laptops to communicate with a wireless hub (access point)

70

Network Electronics

- **Network Hardware**



- The physical architecture shown here may support a markedly different logical architecture.

71

Contents

- Networks are sometimes defined by the nature of the content they carry.
  - For example,
    - Some networks capable of sustained high-bandwidth connections are dedicated to video and other multimedia, whereas others are limited to text.
- Networks may also be relegated to database or equipment communications.
  - The former is especially prominent in bioinformatics, in the form of storage area networks.
    - These networks, typically based on fiber optics, are maintained for highspeed communications between disk arrays and computers involved in sequencing and other applications that require almost constant access to data stored on high-speed hard drives.

72

Security

- Network security is an increasingly important factor in informatics
  - because of the central role that online databases, applications, and groupware such as e-mail play in the day-to-day operation.
- Opening an intranet to the outside world through username and password protected restricted access may be the basis for collaboration as well as a weak point in the security of the organization.

73

Security

- Although it may be practically impossible to maintain security from professional industrial spies,
  - a variety of steps can be taken to minimize the threat posed by modestly computer-savvy activists and the most common non-directed security threats.
- These steps include
  - using antiviral utilities,
  - controlling access through the use of advanced user-authentication technologies,
  - firewalls,
  - low-level encryption technologies.

74

Security

- **Antiviral Utilities**
- The risk of virus infection can be minimized by installing virus-scanning software on servers and locally on workstations.
- The downside to this often-unavoidable precaution is decreased performance of the computers running antiviral programs, as well as the maintenance of the virus-detection software to insure that the latest virus definitions are installed.

75

Security

- **Authentication**
- The most often used method of securing access to a network is to verify that users are who they say they are.
- However, simple username and password protection at the firewall and server levels can be defeated by someone
  - who either can guess or otherwise has access to the username and password information.

76

Security

- A more secure option is to use a synchronized, pseudorandom number generator for passwords.
  - In this scheme, two identical pseudorandom number generators, one running on a credit card–sized computer and one running on a secure server, generate identical number sequences that appear to be random to an observer.
- More sophisticated methods of user authentication involve biometrics, the automated recognition of fingerprint, voice, retina, or facial features.

77

Security

- **Firewalls**
- stand-alone devices or programs running on a server that block unauthorized access to a network.
- Dedicated hardware firewalls are more secure than a software-only solution,
  - but are also considerably more expensive.
- Firewalls are commonly used in conjunction with proxy servers to mirror servers inside a firewall,
  - thereby intercepting requests and data originally intended for an internal server.
- In this way, outside users can access copies of some subset of the data on the system without ever having direct access to the data.
  - This practice provides an additional layer of security against hackers.

78

Security

- **Encryption**
- the process of making a message unintelligible to all but the intended recipient
- one of the primary means of ensuring the security of messages sent through the Internet and even in the same building.
- also one of the greatest concerns—and limitations—of network professionals.
- Although cryptography predates computers by several millennia, no one has yet devised a system that can't be defeated, given enough time and resources.
  - Every form of encryption has tradeoffs of security versus processing and management overhead, and different forms of encryption are used in different applications

Security

- **Encryption Standards**

Standard	Description
AES	Advanced Encryption Standard—Eventual replacement for DES, based on 128-bit encryption.
DES	Data Encryption Standard—Used by the government, based on 64-bit encryption.
IDEA	International Data Encryption Algorithm—Used by the banking industry, developed by the Swiss Federal Institute of Technology, 128-bit encryption.
PGP	Pretty Good Privacy—Popular on the Internet, effective, free, simple to use.
RSA	Rivest-Shamir-Adelman System—Popular in business and government.
S-HTTP	Secure Hypertext Transfer Protocol—For transmitting individual messages over the Internet.
SSL	Secure Sockets Layer—Developed by Netscape Communications Corp. for the Internet.

Security

- **Process**
- More important than the specific encryption algorithm or user-authentication technology used is the process of implementing a security strategy.
  - For example, the best firewall, proxy server, and user authentication system is valueless if a researcher has a habit of losing his secure ID card.
  - Similarly, a wireless hub capable of supporting the latest security standards is vulnerable to attack if the person who configures the hub doesn't take the time to enable the security features.
  - Similarly, a researcher who leaves her username and passwords on a Post-It Note stuck to her monitor provides a security hole for everyone from the janitorial staff to a visitor who happens to walk past her office.

Ownership

- Networks are often characterized by the way they are funded.
- Private networks are owned and managed by private corporations.
  - For example, many of the major pharmaceutical corporations have internal bioinformatics R&D groups that manage workflow and data with the help of privately owned and highly secure networks.
- These private networks may be completely isolated, connect to the Internet through a secure firewall, or communicate with academic and commercial collaborators through dedicated, secure lines.
- Private networks may also be open to researchers and other companies—for a fee.

Ownership

- Public networks such as the Internet and the public telephone network are at least partially funded by public coffers.
- They are also freely open to anyone who is capable of paying for their services.
- Cooperative networks are supported and managed by their users.
  - One of the best known cooperative networks was BITNET (Because It's Time Network), started by universities in the early 1980s.
  - Before it was replaced by NSFNET (National Science Foundation Network) in the early 1990s, it connected about 3,000 mainframe computers at universities in the U.S., Canada, South America, Europe, Asia, and Australia.

Implementation

- **The major steps in the implementation process:**
- Create a Requirements Specification.
  - This document includes a high-level description of the tasks to be supported by the network,
    - such as routing sequencing data from sequencing machines to analysis workstations and data warehouses,
      - as well as the desired response times and storage capacities.
    - For example, the requirements specification document may stipulate the need to support 35 workstations, provide access to storage in excess of 1 terabyte with an access time of less than 50 milliseconds, with tiered password protection, and secure, high-speed access to the Internet.

Implementation

- Create a Functional Specifications Document
  - that defines, in detail, how the high-level needs outlined in the requirements specification will be met.
    - This document quantifies many of the qualitative terms in the requirements specification to the degree that anyone competent in information sciences can determine exactly what equipment, personnel, and costs will be associated with the project.
- Select Hardware.
  - Assuming the functional specifications document is complete, the next step is selecting network, workstation electronics, and media.
    - Often the functional specifications document is authored with particular hardware and software in mind, which further simplifies the selection process.

Implementation

- Select Software.
  - This step of the implementation process involves selecting the network operating system, as well as database publishing software and tools such as PHP, XML, CGI, Java, or JavaScript editors and runtime systems.
- Select Utility.
  - Software and hardware utilities, such as network monitors and antiviral utilities, should be defined during the design process, not as an afterthought.

Implementation

- Select Internet Access Service.
  - Most larger institutions have high-speed Internet access available throughout their offices.
    - However, bandwidth requirements may necessitate alternate Internet services,
      - such as supplementing a corporate-wide cable modem service with a high-speed dedicated line, satellite link, or high-speed microwave link.

Management

- After a network is established, it must be managed to realize its full potential.
- Network management issues include
  - making provision for disaster recovery,
  - load balancing,
  - bandwidth management,
  - maintaining network security.
- For example, disaster recovery plans and support for inevitable network electronics and media failure should consider
  - fire, electrical disturbances, power outages, or intentional destruction.

Management

- Part of disaster recovery planning includes
  - securing redundant systems,
    - such as running extra cables when installing a wired network
  - installing a bank of 56K dial-up modems available for Internet access in the event that the high-speed Internet connection fails.
- Perhaps the greatest management challenge is maintaining adequate security.
  - This task entails monitoring the Internet on a daily basis
    - to check for word of new viruses or security holes in the operating system, and installing the appropriate software patches and utilities to address the new threats.

Grammar revision

- Comprise, can be used with the parts that make up something as the subject:
  - {Oil and coal comprise 70% of the nation's exports.}
- **Compose**
- Compose of is even more formal than consist of and comprise.
- Compose of is only used in the passive voice:
  - {Muscle is composed of different types of protein.}

91

Grammar revision

- **Comparison and contrast**
- Example: Comparison of digital and conventional cameras

FEATURE	DIGITAL	CONVENTIONAL
lens	✓	✓
viewfinder	✓	✓
requires chemical processing	x	✓
film	x	✓
transfer images directly to PC	✓	x
can delete unsatisfactory images	✓	x

- Note how we can compare and contrast these types of cameras

92

Grammar revision

- Comparing features which are similar:
  - {*Both* cameras have lenses.}
  - {*Like* the conventional camera, the digital camera has a viewfinder.}
- Contrasting features which are different:
  - {The conventional camera requires chemical processing *whereas* the digital camera does not.}
  - {The conventional camera uses film *unlike* the digital camera.}

93

Grammar revision

  - {With a digital camera you can transfer images directly to a PC *but* with a conventional camera you need to use a scanner.}
  - {With digital cameras you can delete unsatisfactory images; *however* with conventional cameras you cannot.}

94