Business Data Communications & Networking:

12th Edition

Sadiq M. Sait, PhD
Professor
College of Computer Sciences and Engineering
Director, Industry Collaboration

September 2023

Chapter 1

- Basic Concepts of Data Communications (Terminology & Acronyms)
  1. Why is it important to study
  2. Three fundamental questions this book answers
     1. How Does the Internet work?
     2. How do I design a network?
     3. How do I manage the network?

- Basic Types and Components of a DCN (Data Communication Network)
- Importance of Network Model Based on Layers

1.1 Introduction

- What Internet connection should you use?
    - DSL (Digital Subscriber Line, 1.5 Mbps – 25 Mbps)
    - Cable Modem (faster than DSL, 50 Mbps)
- What is an ISP (Internet Service Provider)?
    - What is important to choose, speed or the right ISP
- Industrial Revolutions (IRs, Disruptions)
    - First IR, machines, (new companies emerged, old ones died)
    - Second IR, how do people work with networking and data communications? (People now can be brought together which was never possible before)
        - History:
            - The year 1800, a message took a week to reach the USA
            - The year 1900, took about an hour
            - Now?

1.1 Introduction (cont.)

- DCN is truly a global area of study because
  - It enables global communication
  - New technologies and applications emerge from different countries and spread rapidly around the world:
    - Angry Birds (Unicorn), Snapchat, etc.
  - WWW
    - Swiss Lab (by who?, a physicist, Tim Berners Lee)

1.1 How does the Internet work?

- When you access a website, what happens to make the webpage appear? (Chapters 1- 5)
- Short Answer:
  - The software on your computer creates a message composed in different software languages (HTTP, TCP/IP, and Ethernet are common) that requests the page you clicked.
  - This message is then broken up into a series of smaller parts (packets).
  - Each packet is transmitted to the nearest router (a special-purpose computer) whose primary job is to find the best route (to where?) for these packets.
  - The packets move from router to router over the Internet until they reach the Web server,
  - The server puts the packets back together into the same message that your computer created.
  - The Web server reads your request and then sends the page back to you in the same way (by composing a message using HTTP, TCP/IP, and Ethernet and then sending it as a series of smaller packets back through the Internet that the software on your computer puts together into the page you requested

1.1 Q1: How does the Internet work? [SCARY] (Contd.)

- You might have heard a news story that the U.S. or Chinese government can read your email or see what Web sites you’re visiting!
- A more shocking truth is that the person sitting next to you at a coffee shop might be doing exactly the same thing—reading all the packets that come from or go to your laptop.
- How is this possible, you ask?
- After finishing Chapter 5, you will know exactly how this is possible
- Not just reading your messages, or see the sites you are visiting, but also taking over your device (ransomware)

1.1 Q2: How do I design a network? (Contd.)

- This is the focus of Chapters 6–10.
- We often think about networks in four layers.
  - Layer 1 is the Local Area Network, or the LAN (either wired or wireless), which enables users like you and me to access the network.
  - Layer 2 is the backbone network that connects the different LANs within a building.
  - The third is the core network that connects different buildings on a company’s campus.
  - The final layer is connections we have to the other campuses within the organization and to the Internet.

1.1 Q2: How do I design a network? (Contd.)

- Each of these 4 layers has slightly different concerns, so the way we design networks for them and the technologies we use are slightly different.
- Although this describes the standard for building corporate networks, you will have a much better understanding of how your wireless router at home works.
- Perhaps, more importantly, you'll learn why buying the newest and fastest wireless router for your house or apartment is probably not a good way to spend your money.

1.1 Q3: How do I manage a network? (Contd.)

- Why manage?
  - Firstly, to make sure it is secure
  - Provides good performance, and
  - Does not cost much

This is the focus of Chapters 11 and 12.

1.1 Q3: How do I manage a network? (Contd.)

- Why?
- Would it surprise you to learn that most companies spend between $1,500 and $3,500 per computer per year on network management and security?
- We spend way more on network management and security each year than we spend to buy the computer in the first place.
- And that’s for well-run networks; poorly run networks cost a lot more.
- Many people think network security is a technical problem, and to some extent, it is. However, the things people do and don’t do cause more security risks than not having the latest technology.

1.1 Q3: How do I **manage** a network? (Contd.)

- According to Symantec, one of the leading companies that sells antivirus software, about half of all security threats are **not** prevented by their software.
- These threats are called targeted attacks:
  - such as phishing attacks (which are emails that look real but instead take you to fake Web sites) or
  - ransomware (software apps that appear to be useful but actually lock your computer and demand a payment to unlock it).

Therefore, network management is as much a people management issue as it is a technology management issue.

Management Focus: 1-1 Career Opportunities

- It’s a great time to be in information technology (IT)!
- The technology-fueled new economy has dramatically increased the demand for skilled IT professions.
- According to the U.S. Bureau of Labor Statistics, the second fastest growing occupation is data communications and networking analyst, which grew by 53% by 2018 and create 150,000 new jobs with an annual median salary of $71,100—not counting bonuses.
- There are two reasons for this growth.
  - First, companies have to continuously upgrade their networks and thus need skilled employees to support their expanding IT infrastructure.
  - Second, people are spending more time on their mobile devices, and because employers are allowing them to use these personal devices at work (i.e., BYOD, or bring your own device), the network infrastructure has to support the data that flow from these devices as well as making sure that they don’t pose a security risk.
  - With a few years of experience, there is the possibility to work as an information systems manager, for which the median annual pay is as high as $117,780.

Management Focus: 1-1 Career Opportunities

- An information systems manager plans, coordinates, and directs IT-related activities so that they can fully support the goals of any business.
- Thus, this job requires a good understanding not only of the business but also of the technology so that appropriate and reliable technology can be implemented at a reasonable cost to keep everything operating smoothly and to guard against cybercriminals.
- Because of the expanding job market for IT and networking-related jobs, **certifications** (WIPRO Story) have become important.

Management Focus: 1-1 Career Opportunities: Certifications

- Most large vendors of network technologies, such as the Microsoft Corporation, IBM, EMC, Huawei, and Cisco Systems Inc., provide certification processes (usually a series of courses and formal exams) so that individuals can document their knowledge.
- Certified network professionals often earn $10,000 to $15,000 more than similarly skilled uncertified professionals—provided that they **continue** to learn and maintain their certification as new technologies emerge.
- Adapted from: http://jobs.aol.com, “In Demand Careers That Pay $100,00 a Year or More”; www.careerpath.com, “Today’s 20 Fastest-Growing Occupations”; www.cnn.com, “30 Jobs Needing Most Workers in Next Decade.”

1.2 Data Communication Networks

- Data communications? It is the movement of computer ***information*** from one point to another by means of electrical or optical transmission systems often called DCNs.
- The broader term telecommunications, includes the transmission of voice and video (images and graphics) as well as data and usually implies longer distances.
- In general, data communications networks collect data from personal computers and other devices and transmit those data to a central server or they perform the reverse process, or a combination of both.
- DCNs facilitate more efficient use of computers and improve the day-to-day control of a business by providing faster information flow.
- They also provide message transfer services to allow computer users to talk to one another via email, chat, and video streaming.

1-2 Technical Focus: Internet Domain Names

- Internet address names are strictly controlled; otherwise, someone could add a computer to the Internet that had the same address as another computer.
- Each address name has two parts, the computer name and its domain. The general format of an Internet address is therefore computer.domain.
- Some computer names have several parts separated by periods, so some addresses have the format computer.computer.computer.domain.
- For example, the main university Web server at Stanford University is called www.stanford.edu, whereas the Web server for the Kelley School of Business at IU is www.kelley.indiana .edu.
- Since the Internet began in the United States, the American address board was the first to assign domain names to indicate types of organizations.

1-2 Technical Focus: Internet Domain Names (contd.)

- U.S. domain names are
  - EDU for an educational institution, usually a university
  - COM for a commercial business
  - GOV for a government department or agency
  - MIL for a military unit
  - ORG for a non-profit organization
- As networks in other countries were connected to the Internet, they were assigned their own domain names. Some international domain names are:
  - CA for Canada; AU for Australia; UK for the United Kingdom; DE for German
- New top-level domains that focus on specific types of businesses continue to be introduced, such as AERO for aerospace companies; MUSEUM for museums; NAME for individuals; PRO for professionals, such as accountants and lawyers; BIZ for businesses
- For a full list of domain names, see www.iana.org/root/db

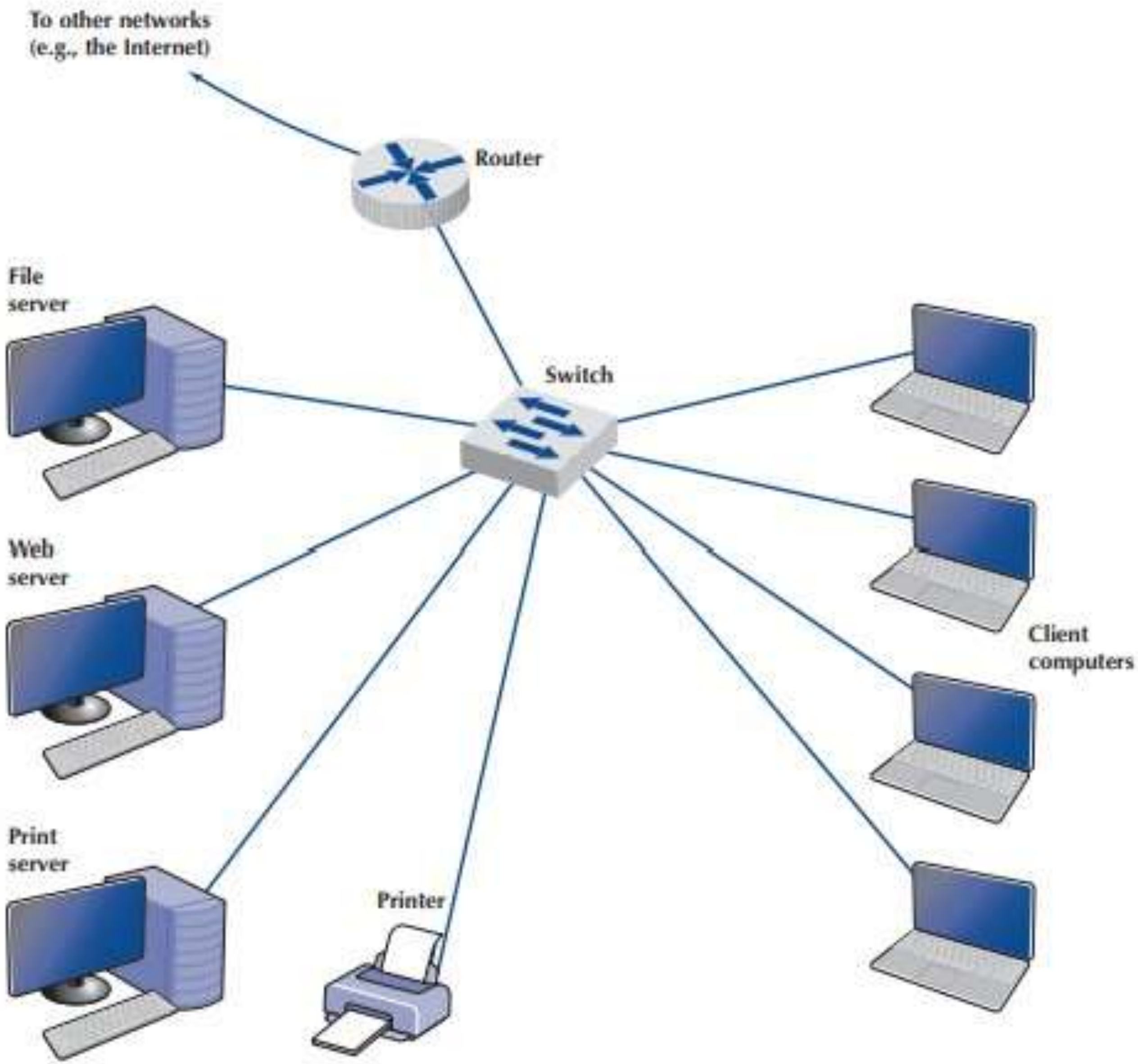
1.2.1 Components of a Network

- There are three basic hardware components for a data communications network:
  - a server (e.g., personal computer, mainframe),
  - a client (e.g., personal computer, terminal), and
  - a circuit (e.g., cable, modem) over which messages flow.
- Both the server and client also need special-purpose network software that enables them to communicate

1.2.1 Components of a Network (contd.)

- Client-Server Computing Model
- The **server** stores data or software that can be accessed by the clients.
- Several servers may work together over the network with a client computer to support the business application.
- The **client** is the input-output hardware device at the user's end of a communication circuit. **Can you think of another definition?**
- The client typically provides users with access to the network and the data and software on the server.
- The **circuit** is the pathway through which the messages travel: It is typically a copper wire, although fiber-optic cable and wireless transmission are also very common.
- Many devices in the circuit perform special functions such as switches, bridges, and routers.

Strictly speaking, a network does not need a server. Some networks are designed to connect a set of similar computers that share their data and software. Such networks are called **peer-to-peer networks** because the computers function as equals, rather than relying on a central server to store the needed data and software.



To other networks
(e.g., the Internet)
Router
File
server
Switch
Web
server
Client
computers
Print
server
Printer

1.2.1 Components of a Network (contd.): Figure 1-1: Example LAN

- Figure 1-1 shows a network that has 4 personal computers (clients) connected by a switch and cables (circuit).
- In this network, messages move through the switch to and from the computers.
- All computers share the same circuit and must take turns sending messages.
- The router is a special device that connects two or more networks. It enables computers on this network to communicate with computers on other networks (e.g., the Internet).
- There are three servers.
  - Although one server can perform many functions, networks are often designed so that a separate computer is used to provide different services.
    - The file server stores data and software that can be used by computers on the network. The print server, which is connected to a printer, manages all printing requests from the clients on the network. The Web server stores documents and graphics that can be accessed from any Web browser, such as Internet Explorer.
    - The Web server can respond to requests from computers on this network or any computer on the Internet.
    - Servers are usually personal computers (often more powerful than the other personal computers on the network) but may also be minicomputers or mainframes.

1.2.2 Types of Networks

- There are many different ways to categorize networks.
- One of the most common ways is to look at the geographic scope of the network.
- Figure 1-2 illustrates three types of networks:
  - local area networks (LANs),
  - backbone networks (BNs), and
  - wide area networks (WANs).

- The distinctions among these are becoming blurry because some network technologies now used in LANs were originally developed for WANs, and vice versa.

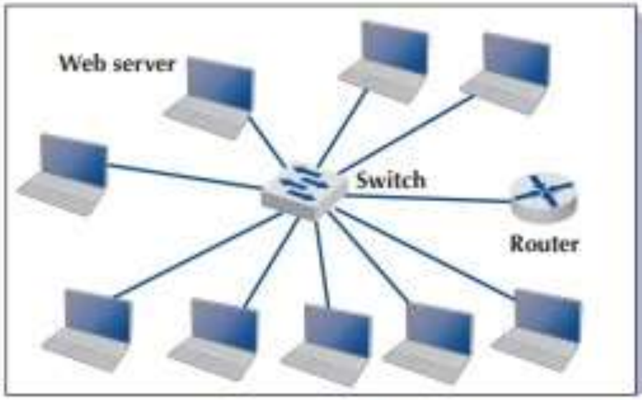
- *Any rigid classification of technologies is certain to have exceptions*

1.2.2 Types of Networks: LANs

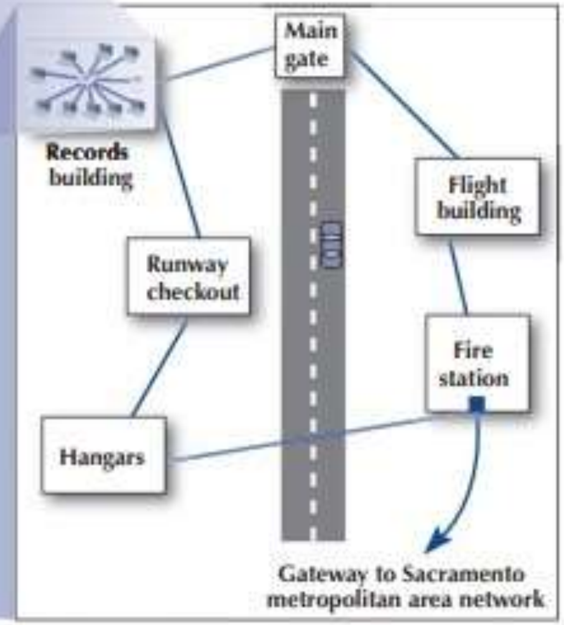
- A local area network (LAN) is a group of computers located in the same general area.
- A LAN covers a clearly defined small area, such as one floor or work area, a single building, or a group of buildings.
- LANs support high-speed data transmission compared with standard telephone circuits, commonly operating 100 million bits per second (100 Mbps).
- We will study LANs and wireless LANs in detail in Chapter 6
- Most LANs are connected to a backbone network (BN), a larger, central network connecting several LANs, other BNs, MANs, and WANs.
- BNs typically span from hundreds of feet to several miles and provide very high-speed data transmission, commonly 100 to 1,000 Mbps.
- The second diagram in Figures 1-2 shows a BN that connects the LANs located in several buildings.
- BNs are discussed in detail in Chapter 7.

1.2.2 Types of Networks: WANs

- Wide area networks (WANs) connect BNs and MANs.
- Most organizations **do not** build their own WANs by laying cable, building microwave towers, or sending up satellites (unless they have unusually heavy data transmission needs or highly specialized requirements, such as those of the Department of Defense).
- Instead, most organizations **lease** circuits from IXCs (e.g., Saudi Telecom, AT&T, Sprint) and use those to transmit their data.
- WAN circuits provided by IXCs
  - come in all types and sizes
  - typically span hundreds or thousands of miles and
  - provide data transmission rates from 64 Kbps to 10 Gbps.
- WANs are discussed in detail in Chapter 8.



Local area network (LAN) at the Records Building—one node of the McClellan Air Force Base backbone network (BN).



Backbone network (BN) at the McClellan Air Force Base—one node of the Sacramento metropolitan area network (MAN).

Wide area network (WAN) showing Sacramento connected to nine other cities throughout the United States.

1.2.2 Intranets

- Two other common terms are intranets and extranets.
- An intranet is a LAN that uses the **same technologies** as the Internet (e.g., Web servers, Java, HTML [Hypertext Markup Language]) but is open to **only** those **inside** the organization.
  - For example, although some pages on a Web server may be open to the public and accessible by anyone on the Internet, some pages may be on an intranet and therefore hidden from those who connect to the Web server from the Internet at large.
- Sometimes an intranet is provided by a completely separate Web server hidden from the Internet.
- The intranet for the Registrar at KFUPM, for example, provides information on student grades, faculty course assignments, class scheduling for future semesters (e.g., room, instructor), and discussion forums.

1.2.2 Extranets

- An extranet is similar to an intranet.
- It, too, uses the **same technologies as the Internet** but instead is provided to invited users **outside** the organization who access it over the Internet.
- It can provide access to information services, inventories, and other internal organizational databases that are provided only to **customers**, **suppliers**, or those who have **paid for access**.
- Typically, users are given accounts and passwords to gain access, but more sophisticated technologies such as smart cards or special software may also be required.
- **Many universities** provide extranets for **Web-based courses** so that only those students enrolled in the course can access course materials and discussions.

1.3 NETWORK MODELS

- What is a model?
- When do you model? (Modeling and Simulation. Digital Twins?).
- There are many ways to describe and analyze DCNs:
  - Note that all networks provide the same basic functions to transfer a message from sender to receiver.
  - But each network can use different network hardware and software to provide these functions.
  - All of these hardware and software products have to work together to successfully transfer a message.
  - One way to accomplish this is to **break** the entire set of **communications functions** into **a series of *layers***, each of which can be defined separately.
  - In this way, vendors can develop software and hardware to provide the functions of each layer separately.
  - The software or hardware can work in any manner and can be easily updated and improved, as long as the ***interface*** between that layer and the ones around it remains **unchanged**.
  - Each piece of hardware and software can then work together in the overall network.

1.3 Two Important NETWORK MODELS (contd.)

- There are many different ways in which the network layers can be designed:
  - The two most important network models are:
  - The Open Systems Interconnection (OSI) Reference model and
  - The Internet model.
- The Internet model is the most commonly used of the two; few people use the OSI model, although understanding it is important and is commonly required for network ***certification*** exams.

1.3.1 Open Systems Interconnection Reference Model

- The Open Systems Interconnection Reference Model (usually called the OSI model for short) helped change the face of network computing.
- Before the OSI model, most commercial networks used by businesses were built using **non-standardized technologies** developed by one vendor (remember that the Internet was in use at the time but was not widespread and certainly was not commercial).
- During the late 1970s, the International Organization for Standardization (ISO) created the Open System Interconnection Subcommittee.
- The sub-committees task was to develop a **framework** of standards for computer-to-computer communications.
- In 1984, this effort produced the OSI model.

Keywords: OPEN, Standard, Abstraction

1.3.1 Open Systems Interconnection Reference Model (contd.)

- The OSI model is the most talked about and most referred to network model.
- If you choose a career in networking, questions about the OSI model will be on the network certification exams offered by Microsoft, Cisco, and other vendors of network hardware and software.
- However, you will probably never use a network based on the OSI model.
- Simply put, the OSI model never caught on commercially in North America, although some European networks use it, and some network components developed for use in the United States arguably use parts of it.
- Most networks today use the ***Internet model.***
  - However, there are many similarities between the OSI model and the Internet model.
  - The OSI model has 7 layers

1-3: Layers of the OSI Network Models

OSI Model	Internet Model	Groups of Layers	Examples
7. Application Layer	5. Application Layer	*Application Layer*	Internet Explorer and Web pages
6. Presentation Layer			
5. Session Layer			
4. Transport Layer	4. Transport Layer	*Internetwork Layer*	TCP/IP software
3. Network Layer	3. Network Layer		
2. Data Link Layer	2. Data Link Layer	*Hardware Layer*	Ethernet port, Ethernet cables, and Ethernet software drivers
1. Physical Layer	1. Physical Layer		

1.3.1 Layer 1: Physical Layer

- The *physical layer*
    - Is primarily concerned with transmitting data bits (zeros or ones) over a communication circuit.
- This layer defines the rules by which ones and zeros are transmitted:
    - such as
        - voltages of electricity
        - number of bits sent per second, and
        - the physical format of the cables and connectors used

1.3.1 Layer 2: Data Link Layer

- The *data link* layer :
  - manages the physical transmission circuit in layer 1 and
  - transforms it into a circuit that is free of transmission errors as far as layers above are concerned.
- Because layer 1 accepts and transmits only a raw stream of bits without understanding their meaning or structure, the data link layer must create and recognize message **boundaries**; *that is, it must mark where a message starts and where it ends.*
- Another major task of layer 2 is to solve the problems caused by **damaged**, **lost**, or **duplicate** messages so the succeeding layers are shielded from transmission errors.
- Thus, layer 2 performs **error detection** and **correction**.
- It also decides when a device can transmit so that two computers do not try to transmit at the same time.

1.3.1 Layer 3: Network Layer

- The *network layer:*
  - Performs routing. That is, using routing tables, it determines the next computer to which the message should be sent so it can follow the ***best*** route through the network and finds the full address for that computer if needed.

1.3.1 Layer 4: Transport Layer

- It deals with end-to-end issues, such as procedures for entering and departing from the network.
- It establishes, maintains, and terminates logical connections for the transfer of data between the original sender and the final destination of the message.
- It is responsible for ***breaking*** a large data transmission into smaller *packets* (if needed), ensuring:

  - that all the packets have been received
  - eliminating duplicate packets, and
  - performing ***flow control*** to ensure that no computer is ***overwhelmed*** by the number of messages it receives.

- Although error control is performed by the data link layer, the transport layer can also perform error checking.

1.3.1 Layer 5: Session Layer

- This *layer* is responsible for:
  - Managing and structuring all sessions.
  - Session initiation must arrange for all the desired and required services between session participants, such as
    - logging on to circuit equipment,
    - transferring files, and
    - performing security checks
  - Session termination provides an orderly way to end the session, as well as a means to abort a session prematurely.
  - It may have some redundancy built in to recover from a broken transport (layer 4) connection in case of failure.
  - The session layer also handles session accounting so the correct party receives the bill (in case of billing/timing, etc.)

1.3.1 Layer 6: Presentation Layer

- This *layer:*
  - Formats the data for presentation to the user.
  - Its job is to accommodate different interfaces on different computers so the application program need not worry about them.
  - It is concerned with displaying, formatting, and editing user inputs and outputs.
    - For example, layer 6 might perform
      - Data compression
      - Translation between different data formats, and screen formatting.
      - Any function (except those in layers 1 through 5) that is requested sufficiently often to warrant finding a general solution is placed in the presentation layer, although some of these functions can be performed by separate hardware and software (e.g., ***encryption***)

1.3.1 Layer 7: Application Layer

- The *application layer:*
  - The application layer is the **end user's access** to **the network**.
  - The primary purpose is to provide a set of utilities for application programs.
  - Each user program determines the set of messages and any action it might take on receipt of a message.
  - Other network-specific applications at this layer include network monitoring and network management

The Internet Model

1.3.2 The Internet Model

- The network model that dominates current hardware and software is a more simple **five-layer Internet model**.
- Unlike the OSI model that was developed by formal committees, the Internet model **evolved** from the work of thousands of people who developed pieces of the Internet.
- The OSI model is a formal standard that is documented in one standard, but the Internet model has **never been** formally defined; it has to be interpreted from a number of standards.
  - The two models have very much in common (see Figure 1-3);
  - simply put, the Internet model collapses the top three OSI layers into one layer.
  - Because it is clear that the Internet has won the "war," we use the five-layer Internet model for the rest of this book

1.3.2 Layer 1 of the Internet Model: The Physical Layer

- The physical layer in the Internet model, as in the OSI model, is the physical connection between the sender and receiver.
- Its role is to transfer a series of electrical, radio, or light signals through the circuit.
- The physical layer includes
  - all the hardware devices (e.g., computers, modems, and switches) and
  - physical media (e.g., cables and satellites).

- The physical layer specifies the type of connection and the electrical signals, radio waves, or light pulses that pass through it. (Chapter 3)

Microsoft uses a four-layer view of the Internet for its certification exams!!

1.3.2 Layer 2 of the Internet Model: The Data Link Layer

- This layer is responsible for moving a message from one computer to the next computer in the network path from the sender to the receiver.
- The data link layer in the Internet model performs the same three functions as the data link layer in the OSI model.
  - First, it controls the physical layer by deciding when to transmit messages over the media.
  - Second, it formats the messages by indicating where they start and end (Called header and trailer (EOF)).
  - Third, it detects and may correct any errors that have occurred during transmission.

(Discuss more in Chapter 4).

1.3.2 Layer 3 of the Internet Model: The Network Layer

- The network layer in the Internet model performs the same functions as the network layer in the OSI model.
  - First, it performs routing, in that it selects the next computer to which the message should be sent.
  - Second, it can find the address of that computer if it doesn't already know it.

Chapter 5 discusses the network layer in detail

1.3.2 Layer 4 of the Internet Model: The Transport Layer

- The transport layer in the Internet model is very similar to the transport layer in the OSI model. It performs two functions.
- First, it is responsible for linking the application layer software to the network and establishing end-to-end connections between the sender and receiver when such connections are needed.
- Second, it is responsible for
  - breaking long messages into several smaller messages to make them easier to transmit and
  - then recombining the smaller messages back into the original larger message at the receiving end.
- The transport layer can also detect lost messages and request that they be resent.

(Chapter 5 discusses the transport layer in detail)

1.3.2 Layer 5 of the Internet Model: The Application Layer

- The application layer in the Internet Model combines much of what the OSI model contains in the **application, presentation,** and **session** layers.
- It is the user’s access to the network. By using the application software, the user defines what messages are sent over the network.
- Because it is the layer that most people understand best and because starting at the top sometimes helps people understand better, Chapter 2 begins with the application layer.
- It discusses the ***architecture*** of network applications and several types of network application software and the types of messages they generate.

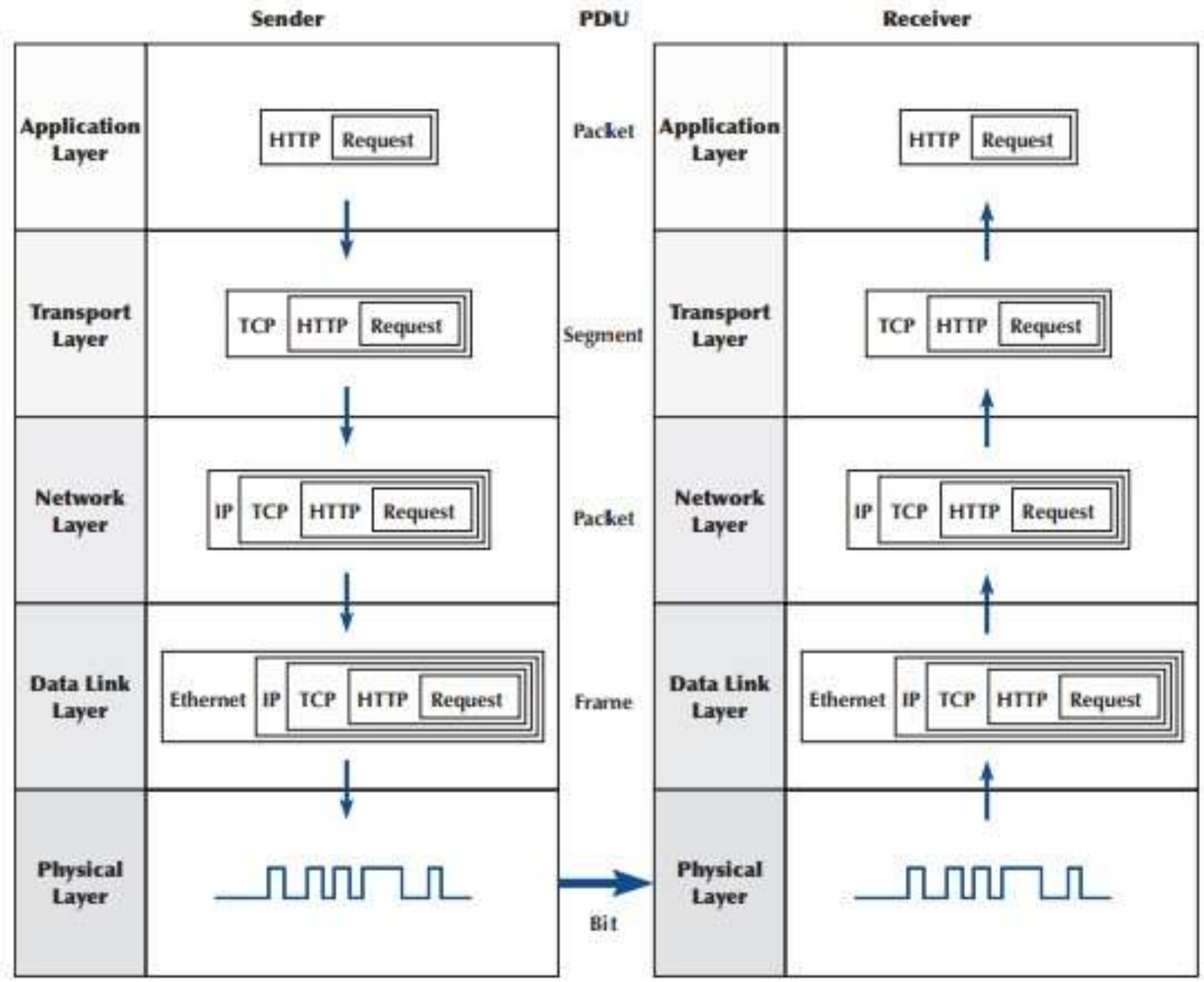
1.3.2 Groups of Layers

- The layers in the Internet are often so closely coupled that decisions in one layer impose certain requirements on other layers.
- The data link layer and the physical layer are closely **tied** together **because the data link layer controls the physical layer in terms of when the physical layer can transmit.**
- Because these two layers are so closely tied together, decisions about the data link layer often drive the decisions about the physical layer.
  - For this reason, some people **group** the physical and data link layers together and call them the **hardware layers.**
  - Likewise, the transport and network layers are so closely coupled that sometimes these layers are called the **internetwork layer**.
  - When you design a network, you often think about the network design in terms of **three** groups of layers: the **hardware layers** (physical and data link), **the internetwork layers** (network and transport), and **the application layer**

1.3.3 Message Transmission Using Layers

- *Each computer in the network has software that operates at each of the layers and performs the functions required by those layers* (the physical layer is hardware, **not** software).
- Each layer in the network uses a **formal language** or **protocol**
- **A protocol** is simply a set of rules that define what the layer will do and that provide a clearly defined set of messages that software at the layer needs to understand.
  - For example, the protocol used for Web applications is HTTP (Hypertext Transfer Protocol, which is described in more detail in Chapter 2). In general, all messages sent in a network pass through all layers.
  - All layers except the physical layer create a new **Protocol Data Unit** (PDU) as the message passes through them.
  - The PDU (or simply a packet) contains information that is needed to transmit the message through the network.
- Figure 1-4 shows how a message requesting a Web page would be sent on the Internet.

Figure 1-4


Sender
PDU
Receiver
Application Layer
HTTP Request
Packet
Transport Layer
TCP HTTP Request
Segment
Network Layer
IP TCP HTTP Request
Packet
Data Link Layer
Ethernet IP TCP HTTP Request
Frame
Physical Layer
Bit

1.3.3-1 Application Layer

- The user creates a message at the application layer using a Web browser by clicking on a link (e.g., get the home page at www.somebody.com).
- The browser translates the user's message (the click on the Web link) into HTTP.
- The rules of HTTP define a specific PDU—called an HTTP packet—that all Web browsers must use when they request a Web page.
- For now, you can think of the HTTP packet as an **envelope** into which the user's message (get the Web page) is placed.
  - This is in the same way that an envelope placed in the mail needs certain information written in certain places (e.g., return address, destination address), and so too does the HTTP packet.
- The Web browser fills in the necessary information in the HTTP packet, drops the user's request inside the packet, then passes the HTTP packet (containing the Web page request) to the transport layer

1.3.3-2 Transport Layer

- The transport layer on the Internet uses a protocol called **TCP** (Transmission Control Protocol), and it, too, has its own rules and its own PDUs.
- TCP is responsible for **breaking** large files into smaller packets and for opening a connection to the server for the transfer of a large set of packets.
- The transport layer places the HTTP packet inside a TCP PDU (which is called a TCP segment), fills in the information needed by the TCP segment **(such as?)**, and passes the TCP segment (which contains the HTTP packet, which, in turn, contains the message) to the **network layer.**

1.3.3-3 Network Layer

- The network layer on the Internet uses a protocol called IP (Internet Protocol), which has its rules and PDUs.
- IP selects the next stop on the message’s route through the network.
- It places the TCP segment inside an IP PDU, which is called an IP packet, and passes the IP packet:
  - The IP packet contains the TCP segment
  - The TCP segment contains the HTTP packet
  - The HTTP packet contains the message

- This IP packet is sent to the Data Link layer.

1.3.3-4 Data Link Layer

- If you are connecting to the Internet using a LAN, your data link layer may use a protocol called Ethernet, which also has its own rules and PDUs.
  - What is Ethernet?

- The data link layer formats the message with **start** and **stop** markers, adds **error checking information, places the IP packet inside an Ethernet PDU**, which is called an **Ethernet frame,** and instructs the physical hardware to transmit the Ethernet frame, which contains the IP packet, which contains the TCP segment, which contains the HTTP packet, which contains the message.

1.3.3-5a Physical Layer

- The physical layer in this case is a network cable connecting your computer to the rest of the network.
- The computer will take the Ethernet frame and send it as a series of **electrical pulses** through your cable to the server.
- When the server gets the message, this process is performed in **reverse**.
  - The physical hardware translates the electrical pulses into computer data and passes the message to the data link layer.

1.3.3-5b Now Things Happen in the REVERSE.

- The data link layer uses the start and stop markers in the Ethernet frame to identify the message. The data link layer checks for errors and, if it discovers one, requests that the message be **resent**.
- If a message is received without error, the data link layer will strip off the Ethernet frame and pass the IP packet (which contains the TCP segment, the HTTP packet, and the message) to the network layer.
- The network layer checks the IP address and, if it is destined for this computer, strips off the IP packet and passes the TCP segment, which contains the HTTP packet and the message, to the transport layer.
- The transport layer processes the message, strips off the TCP segment, and passes the HTTP packet to the application layer for processing.
- The application layer (i.e., the Web server) reads the HTTP packet and the message it contains (the request for the Web page) and processes it by generating an HTTP packet containing the Web page you requested.

- **Then the process starts again as the page is sent back to you.**

1.3.3-6a Pros and Cons of Using Layers

- There are three important points in this example.
  - **First**, there are many different software packages and many different PDUs that operate at different layers to successfully transfer a message. Networking is similar to the Russian matryoshka, nested dolls that fit neatly inside each other.
  - This is called **encapsulation**, because the PDU at a higher level is placed inside the PDU at a lower level so that the lower-level PDU encapsulates the higher-level one.
  - The major advantage of using different software and protocols is that it is easy to develop new software, because all one has to do is write software for one level at a time.
    - For example, the developers of Web applications do not need to write software to perform error checking or routing. Why?
    - Because those are performed by the data link and network layers.
    - Developers can simply assume those functions are performed and just focus on the application layer.
    - Likewise, it is simple to **change** the software at any level (or **add** new application protocols), as long as the **interface** between that layer and the ones around it remains unchanged.

1.3.3-6b Pros and Cons of Using Layers (contd).

- **Second**, it is important to note that for communication to be successful, each layer in one computer must be able to communicate with its matching layer in the other computer.
  - For example, the physical layer connecting the client and server must use the same type of electrical signals to enable each to understand the other (or there must be a device to **translate** between them).
    - Ensuring that the software used at the different layers is the same is accomplished by using **standards**.
  - ***A standard defines a set of rules, called protocols, that explain exactly how hardware and software that conform to the standard are required to operate.***
  - Any hardware and software that conform to a standard can communicate with any other hardware and software that conform to the same standard.

Without standards, it would be virtually impossible for computers to communicate.

1.3.3-6c Pros and Cons of Using Layers (contd).

- **Third**, the major disadvantage of using a layered network model is that it is somewhat inefficient.
- Because there are several layers, each with its own software and PDUs, sending a message involves many software programs (one for each protocol) and many PDUs.
- The PDUs add to the total amount of data that must be sent (thus increasing the time it takes to transmit), and the different software packages increase the processing power needed in computers.

Because the protocols are used at different layers and are stacked on top of one another (take another look at Figure 1-4), the set of software used to understand the different protocols is often called a **protocol stack.**

NETWORK STANDARDS

1.4.1 The Importance of Standards

- Standards are necessary for almost every business and public service entity.
  - For example, before 1904, fire hose couplings in the United States were not standard, meaning a fire department in one community could not help another.
  - The transmission of electric current was not standardized until the end of the nineteenth century, so customers had to choose between Thomas Edison's direct current (DC) and George Westinghouse's alternating current (AC).
- The primary reason for standards is to ensure that hardware and software produced by different vendors **can work together**.
  - Without networking standards, it would be difficult—if not impossible—to develop networks that easily share information.
  - Standards mean that customers are not locked into one vendor. (**OPEN**).
  - They can buy hardware and software from any vendor whose equipment meets the standard.
  - In this way, standards help to promote more competition and hold down prices.
  - The use of standards makes it much easier to develop software and hardware that link different networks because software and hardware can be developed one layer at a time.

1.4.2 The Standards Making Process

- There are two types of standards: de jure and de facto.
  - A de jure standard is developed by an official industry or a government body and is often called a **formal** standard.
  - For example, there are de jure standards for applications such as Web browsers (e.g., HTTP, HTML), for network layer software (e.g., IP), for data link layer software (e.g., Ethernet IEEE 802.3), and for physical hardware (e.g., V.90 modems).
  - De jure standards typically take several years to develop, during which time technology changes, making them less useful.
  - De facto standards are those that emerge in the ***marketplace*** and are ***supported*** by several ***vendors*** but have ***no official standing***.
    - For example, Microsoft Windows is a product of one company and has not been formally recognized by any standards organization, yet it is a de facto standard.
    - In the communications industry, de facto standards often become de jure standards once they have been widely accepted.

1.4.2 The Standards Making Process (contd).

- The de jure standardization process has three stages: (i) specification, (ii) identification of choices and (iii) acceptance.
  - The specification stage consists of developing a ***nomenclature*** and identifying the problems to be addressed.
  - In the identification of ***choices*** stage, those working on the standard identify the various solutions and choose the ***optimum*** solution from among the alternatives.
  - Acceptance, which is the most difficult stage, consists of defining the solution and getting recognized industry leaders to agree on a single, uniform solution.

As with many other organizational processes that have the potential to influence the sales of hardware and software, **standards-making processes are not immune to corporate politics** and the influence of national governments.

1.4.2a International Organization for Standardization

- One of the most important standards-making bodies is the International Organization for Standardization (ISO).
- ISO makes **technical recommendations about data communication interfaces** (see www.iso.org).
- ISO is based in **Geneva**, Switzerland.
- The membership comprises the **national standards organizations** of each ISO member country.

1.4.2b International Telecommunications Union (ITU) — Telecommunications Group

- The Telecommunications Group (ITU-T) is the technical standards-setting organization of the United Nations International Telecommunications Union
- ITU is also based in Geneva (see www.itu.int).
- ITU comprises representatives from about 200 member countries.
- Membership was originally focused on just the public telephone companies in each country, but a major reorganization in 1993 changed this, and ITU now seeks members among public- and private-sector organizations who operate computer or communications networks (e.g., RBOCs) or build software and equipment for them (e.g., AT&T).

1.4.2c American National Standards Institute

- The American National Standards Institute (ANSI) is the coordinating organization for the U.S. national system of standards for both technology and nontechnology (see www.ansi.org).
- ANSI has about 1,000 members from both public and private organizations in the United States.
- ANSI is a **standardization** organization, not a standards-making body (means what?
  - It accepts standards developed by other organizations and publishes them as American standards.
  - Its role is to ***coordinate*** the development of voluntary national standards and to interact with ISO to develop national standards that comply with ISO’s international recommendations.
  - ANSI is a **voting** participant in the ISO.

1.4.2d Institute of Electrical and Electronics Engineers (IEEE)

- The Institute of Electrical and Electronics Engineers (IEEE) is a professional society in the United States
- IEEE Standards Association (IEEE-SA) develops standards (see www.standards.ieee.org).
- The IEEE-SA is probably most known for its standards for LANs.

Other countries have similar groups; for example, the British counterpart of IEEE is the Institution of Electrical Engineers (IEE).

1.4.2e Internet Engineering Task Force (IETF)

- There are many standards organizations worldwide, but perhaps the best known is the Internet Engineering Task Force (IETF).
- The IETF sets standards that govern how much of the Internet will operate (see www.ietf.org).
- The IETF is unique in that it doesn't really have official memberships.
- Quite literally anyone is welcome to:
  - join its mailing lists
  - attend its meetings, and
  - comment on developing standards.

- The role of the IETF and other Internet organizations is discussed in more detail in Chapter 8; also, see the box entitled "How Network Protocols Become Standards?."

MF-1-2 How Network Protocols Become Standard?

- IETF sets the standards that govern how much of the Internet operates.
- The IETF, tries to seek consensus among those involved before issuing a standard.
- Usually, a standard begins as a protocol (i.e., a language or set of rules for operating) developed by a vendor (e.g., HTML [Hypertext Markup Language]).
  - Who developed HTML and HTTP?
- When a protocol is proposed for standardization, the IETF forms a working group of technical experts to study it.
- The working group examines the protocol to identify potential problems and possible extensions and improvements, and issues a report to the IETF.
- If the report is favourable, the IETF issues a Request for Comment (RFC) that describes the proposed standard and solicits comments from the entire world.
- Most large software companies likely to be affected by the proposed standard prepare detailed responses.
- Many "regular" Internet users also send their comments to the IETF.
- The IETF reviews the comments and issues a new and improved RFC, which again is posted for more comments.
- Once no additional changes have been identified, it becomes a proposed standard.

MF-1-2 How Network Protocols Become Standard? (contd).

- Usually, several vendors adopt the proposed standard and develop products based on it.
- Once at least **two** vendors have developed hardware or software based on it and it has proven successful in operation, the **proposed** standard is changed to a **draft** standard.
- This is usually the final specification, although some protocols have been elevated to **Internet standards**, which usually signifies mature standards not likely to change.
- The process **does not focus solely on technical issues**; almost *90% of the IETF's participants work for manufacturers and vendors, so market forces and politics often complicate matters.*

One former IETF chairperson who worked for a hardware manufacturer has been accused of trying to delay the standards process until his company had a product ready, although he and other IETF members deny this.

Likewise, former IETF directors have complained that members try to standardize every product their firms produce, leading to a ***proliferation*** (syn: explosion) of standards, only a few of which are truly useful.

Figure 1-5: Some Common Data Communications Standards

Layer	Common Standards
5. Application layer	HTTP, HTML (Web) MPEG, H.323 (audio/video) SMTP, IMAP, POP (e-mail)
4. Transport layer	TCP (Internet and LANs)
3. Network layer	IP (Internet and LANs)
2. Data link layer	Ethernet (LAN) Frame relay (WAN) T1 (MAN and WAN)
1. Physical layer	RS-232C cable (LAN) Category 5 cable (LAN) V.92 (56 Kbps modem)

MF-1-3 Keeping Up with Technology

- The data communications and networking arena changes rapidly.
- Significant new technologies are introduced and new concepts are developed almost every year.
- It is important for network managers to keep up with these changes.
- There are at least three useful ways to keep up with change.
  - First and foremost for users of this book is the Web site for this book, which contains updates to the book, additional sections, teaching materials, and links to useful Web sites.
  - Second, there are literally hundreds of thousands of Web sites with data communications and networking information. Search engines can help you find them.
  - A good initial starting point is the telecom glossary at www. atis.org.
  - Two other useful sites are:
    - networkcomputing.com and
    - zdnet.com.
  - Third, there are many useful magazines that discuss computer technology in general and networking technology in particular, including: (i) Network Computing; (ii) Data Communications; (iii) Info World; (iv) Info Week; and (v) CIO Magazine; etcetra.

1.4.3 Common Standards

- There are many different standards used in networking today.
- Each standard usually covers ***one layer*** in a network.
- Some of the most commonly used standards are shown in Figure 1-5.
- At this point, these models are probably just a maze of strange names and ***acronyms***
- But bythe end of the course, you will have a good understanding of each of these.
- Figure 1-5 provides a brief road map for some of the important communication technologies we discuss in this book.
- For now, there is one important message you should understand from Figure 1-5:
  - For a network to operate, many different standards must be used simultaneously. The sender of a message must use one standard at the application layer, another one at the transport layer, another one at the network layer, another one at the data link layer, and another one at the physical layer.
  - Each layer and each standard is different, but all must work together to send and receive messages.
  - Because different networks often use software and hardware designed for different standards, there is often a lot of ***translation*** between different standards

1.5 Future Trends

- The field of data communications has grown faster and become more important than computer processing itself.
- Both go hand in hand, but we **have moved** from the computer era to the communication era.
- Some also claim that the network is the computer
- Three major trends are driving the future of communications and networking:
    - ***Wireless LAN and BYOD***
    - ***The Web of Things***
    - ***Massively Online***

1.5.1a WLAN and BYOD

- Employers are encouraged to allow their employees to bring their own devices to work and use them to access data, such as their work email.
- This movement called bring your own device, or BYOD, is a great way to get work quickly done, saves money, and makes employees happy.
- But BYOD also brings its own problems. Employers need to add or expand their Wireless Local Area Networks (WLANS) to support all these new devices.

1.5.1b WLAN and BYOD (contd).

- Another important problem is **security**.
- Employees bring these devices to work so that they can access not only their email but also other critical company assets, such as information about their clients, suppliers, or sales.
- Employers face myriad decisions about how to ***manage*** access to company applications for BYOD. Companies can adopt two main approaches: (1) native apps or (2) browser-based technologies. Native apps require an app to be developed for each application that an employee might be using for every potential device that the employee might use (e.g., iPhone, Android, Windows). The browser-based approach (often referred to as responsive design using HTML5) doesn't create an app but rather requires employees to access the application through a Web browser. Both these approaches have their pros and cons, and only the future will show which one is the winner.

1.5.1c WLAN and BYOD (contd)

- What if an employee loses his or her mobile phone or tablet so that the application that accesses critical company data now can be used by anybody who finds the device?
- Will the company's data be compromised?
  - Device and data loss practices now have to be added to the general security practices of the company.
  - Employees need to have apps to allow their employer to **wipe** their phones clean in case of loss so that no company data are compromised (e.g., SOTI's MobiControl).
  - In some cases, companies require the employee to allow monitoring of the device at all times, to ensure that security risks are minimized.
    - However, some argue that this is not a good practice because the device belongs to the employee, and monitoring it 24/7 invades the employee's privacy

1.5.2a The Web of Things

- Telephones and computers used to be separate.
- Today voice and data have converged into unified communications, with phones plugged into computers or directly into the LAN using Voice over Internet Protocol (VOIP).
- What else do computers connected to networks replace? (Fax, TV, Scanner, etc). Name 3 more.
- Vonage and Skype have taken this one step further and offer telephone service over the Internet at dramatically lower prices than traditional separate landline phones, whether from traditional phones or via computer microphones and speakers.
- Computers and networks can also be built into everyday things, such as kitchen appliances, doors, and shoes.
- In the future, the Web will move from being a Web of computers to also being a Web of Things with which we interact using a computer.
- All this interaction will happen seamlessly, without human intervention. And we will get used to seeing our shoes tell us how far we walked, our refrigerator telling us what food we need to buy, and our locks opening and closing without physical keys and telling us who entered and left at what times.

1.5.2b The Web of Things (contd).

- The Web of Things is already underway.
- For example, Microsoft has an Envisioning Center that focuses on creating the future of work and play (it is open to the public).
- At the Envisioning Center, a person can communicate with his or her colleagues through digital walls that enable the person to visualize projects through simulation and then rapidly move to execution of ideas.
- In the home of the future, anyone can, for example, be a chef and adapt recipes based on dietary needs or ingredients in the pantry (see Figure 1-6) through the use of Kinect technology.
- Google is another leading innovator in the Web of Things.
  - Google has been developing a self-driving car for several years. This self-driving car not only passes a standard driving test but also spends less time in near-collision states on public roads in California and Nevada.
  - Of course, for such a car to appear in other states, technology has to be installed that allows the car to "see" the road.
  - Other car developers started installing computer technology that not only parallel parks the car but also applies brakes to avoid collisions

1.5.2c Massively Online ---- Education

- You have probably heard of massively multiplayer online games, such as World of Warcraft, where you can play with 1000s of players in real-time.
- Well, today not only games, Education too is massively online.
- Khan Academy, Lynda.com, or Code Academy have websites offering 1000s of education modules for children and adults in various fields to help them learn.
- Our class can also have an online component *(we can have a couple of classes of this course online to see the difference)!*
- We may even use the textbook online and decide whether your comments are for you only, for your instructor, or for the entire class to read.
- In addition, you may have heard about massive open online courses, or MOOCs.
  - MOOCs enable students who otherwise wouldn’t have access to elite universities to get access to top knowledge without having to pay the tuition.
  - These classes are offered by universities, such as Stanford, UC Berkeley, MIT, UCLA, and Carnegie Mellon, free of charge and for no credit (although at some universities, you can pay and get credit toward your degree).

1.5.3 Massively Online -------Election & Politics (contd).

- Politics has also moved massively online.
- President Obama reached out to the crowds and ordinary voters not only through his Facebook page but also through Reddit and Google Hangouts.
- Many other politicians use social computing to reach potential voters. Finally, massively online allows activists to reach masses of people in a very short period of time to initiate change. Examples of use of YouTube.

- So what started as a game with thousands of people being online at the same time is being reinvented for good use in (i) education, (ii) politics, and (iii) activism.
- Only the future will show what humanity can do with what massively online has to offer.

1.5.3 Massively Online ------- Infrastructure for Business (contd).

- What these three trends have in common is that there will be an increasing demand for professionals who understand the development of data communications and networking infrastructure to support this growth.
- There will be more and more need to build faster and more secure networks that will allow individuals and organizations to connect to resources, probably stored on ***cloud infrastructure*** (either private or public).
- This need will call not only for engineers who deeply understand the technical aspects of networks but also for highly social individuals who embrace technology in creative ways to allow ***businesses*** to achieve a competitive edge through utilizing this technology.

So the call is for you, read your textbook, you are in the right place at the right time

1.6 Implications for Management

- What are the key implications for management that arise from the topics discussed thus far?
- Implications that focus on
  - improving the management of networks and information systems
  - as well as implications for the management of the organization as a whole

- There are three key implications for management from this chapter.

1.6 Implications for Management: ONE (contd).

- First, networks and the Internet change almost everything.
- The ability to **quickly** and **easily** move information from distant locations and to enable individuals inside and outside the firm to access information and products from around the world changes:
  - the way organizations operate,
  - the way businesses buy and sell products, and
  - the way we as individuals work, live, play, and learn.
- Companies and individuals who embrace change and actively seek to apply networks and the Internet to better improve what they do will thrive;
- Companies and individuals who do not will gradually find themselves falling behind.

1.6 Implications for Management: TWO (contd).

- Second, today's networking environment is driven by standards.
- The use of standard technology means an organization can easily mix and match equipment from different vendors.
- The use of standard technology also means that it is easier to migrate from older technology to a newer technology, because most vendors designed their products to work with many different standards.
- The use of a few standard technologies rather than a wide range of vendor-specific proprietary technologies also lowers the cost of networking because network managers have fewer technologies they need to learn about and support.
- If your company is not using a narrow set of industry-standard networking technologies (whether those are de facto standards such as Windows, open standards such as Linux, or de jure standards such as 802.11n wireless LANs), **then it is probably spending too much money on its networks.**

1.6 Implications for Management: THREE (contd).

- Third, as the demand for network services and network capacity increases, so too will the need for storage and server space.
- Finding efficient ways to store all the information we generate will open new market opportunities (QS Data).
- Today, Google has almost a million Web servers (Google Dance, and Mirroring). If we assume that each server costs an average of $ 1000, the money large companies spend on storage is close to $ 1 Billion.
- Capital expenditure (CAPEX and OPEX) of this scale is then increased by money spent on power and staffing.
- One way companies can reduce this amount of money is to store their data using ***cloud*** computing.

SUMMARY

- **Introduction**
  - The information society, where information and intelligence are the key drivers of personal, business, and national success, has arrived.
  - Data communications is the principal enabler of rapid information exchange and will become more important than the use of computers themselves in the future.
  - Successful users of data communications, such as Wal-Mart, can gain a significant competitive advantage in the marketplace.

- **Network Definitions**
  - A local area network (LAN) is a group of computers located in the same general area.
  - A backbone network (BN) is a large central network that connects almost everything on a single company site.
  - A metropolitan area network (MAN) encompasses a city or county area.
  - A wide area network (WAN) spans city, state, or national boundaries

SUMMARY (contd).

- **Network Model**
  - Communication networks are often broken into a series of layers, each of which can be defined separately to enable vendors to develop software and hardware that can work together in the overall network.
  - In this book, we use a five-layer model.
    - The application layer is the application software used by the network user.
    - The transport layer takes the message generated by the application layer and, if necessary, breaks it into several smaller messages.
    - The network layer addresses the message and determines its route through the network.
    - The data link layer formats the message to indicate where it starts and ends, decides when to transmit it over the physical media, and detects and corrects any errors that occur in transmission.
    - The physical layer is the physical connection between the sender and receiver, including the hardware devices (e.g., computers, terminals, and modems) and physical media (e.g., cables and satellites).
    - Each layer, except the physical layer, adds a Protocol Data Unit (PDU) to the message.

SUMMARY (contdt).

- **Standards**
  - Standards ensure that hardware and software produced by different vendors can work together.
  - A de jure standard is developed by an **official industry or a government body**.
  - De facto standards are those that emerge in the marketplace and are supported by several vendors but have no official standing.
  - Many different standards and standards-making organizations exist.

- **Future Trends**
  - BYOD offers efficiency at the workplace, it also opens up the doors for security problems that companies need to consider.
  - Our interactions with colleagues and family will very likely change in the next 5–10 years because of the Web of Things, where devices will interact with each other without human intervention.
  - Finally, massively online not only changed the way we play computer games but also showed that humanity can change its history **(disruptive).**

KEY TERMS

American National Standards Institute (ANSI), Application Layer, Backbone Network (BN), Cable, Circuit, Client, Data Link Layer, Extranet, File Server, Hardware Layer, IEEE, ITU- Telecommunications Group (ITU-T), International Telecommunications Union—(ITU); Internet Engineering Task Force (IETF), Internet model, ISP, Internetwork Layer, Intranet, Seven Layer Model (ISO/OSI), LAN, Network Layer, Open Systems Interconnection Reference model (OSI model), Peer-to-Peer Network, Physical Layer, Print Server, Protocol, Protocol Data Unit (PDU), Protocol Stack, Request for Comment (RFC), Router, Server, Standards, Transport Layer, Web Server, WAN.

AND NEW KEY TERMS

CLOUD, VIRTUAL, DISRUPTIVE, IR, DSL, ISDN, CABLE MODEM, OPTIMAL PATH, RANSOMWARE, BYOD, CERTIFICATIONS, BADGES, OTT, PHISHING, OPTIMIZATION, DESIGN, COST VS PERFORMANCE, SWITCH, BRIDGE, ROUTER, P2P, HTTP/HTML, OPEN STANDARD, FLOW CONTROL, BUFFER, SATELLITE