Final Exam Review

The final exam will cover all of the chapters we discussed in class. I have condensed the PowerPoint slides into a smaller sub-set to focus on for the exam.

The format of the final is 50 multiple-choice questions.

1

Chapter 1

2

The OSI 7-layer Model

Application: provides a set of utilities used by application programs

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

Session: responsible for initiating, maintaining and terminating each logical session between sender and receiver

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

Network: responsible for making routing decisions

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

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

3

The Internet's 5-Layer Model

Application: used by application program

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

Network*: responsible for end-to-end addressing and routing, determines destination address if unknown

Data Link*: deals with message delineation, error control & network access

Physical*: defines how information will be transmitted through the network

*same as corresponding layer in OSI model

4

Why Standards?

- Standards provide a fixed way for hardware and/or software systems to communicate.
- For example, USB enables two pieces of equipment to interface even though they are manufactured by different companies.
- By allowing hardware and software from different companies to interconnect, standard help promote competition.

5

Types of Standards

- There are two main types of standards:
- **Formal**: a standard developed by an industry or government standards-making body
- **De facto**: standards that emerge in the marketplace and are widely used, but lack official backing by a standards-making body

6

Three Emerging Trends in Networking

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

7

Pervasive Networking

- The **pervasive networking** means:
  - network use will continue to grow exponentially
  - network access is everywhere
  - many new types of devices will have network capability
- Data rates for all kinds of networking will also continue to grow exponentially, reaching Gigabit per second ranges later in this decade (see Figure 1-6)

8

The Integration of Voice, Video & Data

- Also called **convergence**, integration means that telecom systems that were previously transmitted using separate networks will merge into a single, high speed, multimedia network in the near future.
- The first step is the integration of voice and data, which is already underway.
- Later, video will merge with voice and data. This step will take longer partly due to the high data rates required for video.

9

Chapter 2. Application Layer

10

Host-based Architectures

- Two main problems:
  - Since all processing is by the host, **the host becomes a bottleneck** which can severely limit network performance.
  - **Upgrades are typically expensive** and "lumpy", meaning available upgrades require big jumps in processing and memory. Network demand grows more incrementally, so this often means a poor fit (too much or too little) between host performance and network demand.

11

Client-Based Architectures

- Became important in the late 1980s with the widespread use of PCs, LANs, and low-cost PC-based application programs such as spreadsheets and word processors.
- In client-based architectures, application programs on the clients are responsible for the data access, application, and presentation logic.
- The server is responsible for data storage only (Figure 2-2).

12

Client-Based Architectures

- Main problem: the need for all of the data to travel back and forth between server and client.
- Result:poor network performance because of the bottleneck created by constantly sending large files back and forth over the network.
- Database example: query
- We got away from this b/c of cheap apps developed for PCs

13

Client-Server Architectures

- More efficient since they distribute processing between client and server.
- Another strength - they allow hardware and software from different servers to be used together
- This is also a weakness, since it is sometimes difficult to get software from different vendors to work together smoothly.
- For this reason, a third category of software, called Middleware was developed.

14

Two-tier, Three-tier and N-tier Architectures

- Figure 2-3 (page 44) gives an example of a 2-tier client-server architecture.
  - Server is resp for data; client is resp for application and presentation
- In a three-tier architecture the application program logic is split up between three computers. For example (see Figure 2-4),
  - the client handles the presentation logic.
  - an application server handles the application logic.
  - a database server handles the data storage and data access logic.
- In an N-tier architecture more than three sets of computers are used (see Figure 2-5).

15

Two-tier, Three-tier and N-tier Architectures

- The primary advantage of N-tier architectures is that they make load balancing possible. Since the application logic is distributed between several servers, processing can then be more evenly distributed among those servers.
- N-tiered architectures are also more easily scalable, since only servers experiencing high demand, such as the application server, need be upgraded.
- The primary disadvantage is that more distributed processing means a more heavily loaded network.
- It is also more difficult to program and test an N-tier architecture due to its increased complexity.

16

Choosing An Architecture

- **Cost of Development**: because software is expensive to develop, client-based and client-server architectures that use off-the-shelf software tend to be much cheaper than software solutions that require in-house development.
- Costs 2-3 times more to develop and maintain applications for client-server than server-based architectures
- Client-based apps are much cheaper b/c of GUI development tools
- Updating is more expensive in client-server b/c updates have to be made to all clients as well

17

Origin of the World Wide Web

- Invented in 1989 by Tim Berners-Lee at the Centre Européan pour Rechèrche Nucleaire (CERN) in Geneva.
- Two central WWW ideas are hyperlinks and Uniform Resource Locators (URLs).
- Mosaic, the first web reader (browser) to gain widespread use, was written in 1993 at the National Center for Supercomputing Applications (NCSA) by Marc Andressen, who later founded Netscape.

18

IMAP and POP

- Allow receiving of messages from server to client
- POP
  - The client downloads the message and deletes if from the server
- IMAP
  - Message remain on the server
  - Better for mobile users

19

Three-Tier Client-Server Architecture (Figure 2-12)

- Reading e-mail using a Web-based interface, such as Hotmail, uses a three-tier architecture. The three tiers are:
  - The client's web browser that sends HTTP requests to the Web server.
  - The Web server: 1) sends HTTP responses to the Web client and 2) translates the client's HTTP requests into SMTP packets which are then sent to the Mail server.
  - The Mail server performs the same functions as the mail server in the two-tier example.

20

Chapter 3

Physical Layer

21

The Physical Layer

- The physical layer includes network hardware and circuits.
- Network circuits include physical media (e.g., cables) and special purposes devices (e.g., routers and hubs). Networks are made of both physical and logical circuits.
  - **Physical circuits** connect devices & include actual wires.
  - **Logical circuits** refer to the transmission characteristics of the circuit, such as a T-1 connection.
- Sometimes the physical and logical circuits are the same, but they can be different. For example, in multiplexing, one wire carries several logical circuits.

22

Analog and Digital Data

- Another fundamental physical layer distinction is between digital and analog forms of data.
- Sounds waves, which vary continuously over time are **analog** data.
- Computers produce **digital** data that is in binary form:
  - ones and zeros
  - on and off

23

Advantages of Digital Transmission

- Digital transmission:
  - produces **fewer errors** than analog transmission. Because the transmitted data is binary (1s and 0s), it is easier to detect and correct errors.
  - permits **higher transmission rates**. Optical fiber, for example, is designed for digital transmission.
  - is **more efficient**. It's possible to send more data through a given circuit using digital rather than analog transmission.
  - is **more secure** since it is easier to encrypt.
  - is **easier to combine** voice, video and data on the same circuit

24

Circuit Configuration

- Two basic circuit configurations:
- **Point-to-point** connects just one sender and receiver together (Figure 3-1)
  - Need to have large amt of data to justify
- **Multipoint** (also called a shared circuit) connects a number of senders and receivers together (Figure 3-2)
  - Advantage: multipoint is cheaper and simpler to wire
  - Disadvantage: only one computer can use the circuit at a time.

25

Data Flow (Figure 3-3)

- Data can move in one direction or both directions.
- **Simplex** data flows move in one direction only.
  - Ex: radio or cable television broadcasts.
- **Half Duplex** data flows both ways, but only one direction at a time.
  - some kind of control information must also be included so that sender and receiver don't send at the same time
  - Ex: CB radio
- **Full Duplex** data flows in both directions at the same time.
- Which to use?

26

Communications Media

- Medium: the physical matter that carries the transmission. Two basic categories of media:
- **Guided media** - transmission flows along a physical guide.
  - twisted pair wiring
  - coaxial cable
  - optical fiber cable
- **Wireless media** - no wave guide and the transmission just flows through the air (or space).
  - Radio
  - Infrared
  - Microwave
  - Satellite

27

Guided Media: Twisted Pair Wires

- Twisted pair wire cables are commonly used for telephones and local area networks.
- Twisting two wires together reduces electromagnetic interference.
- TP cables have a number of pairs of wires.
  - Telephone lines have two pairs (4 wires, usually only one pair is used by the telephone)
  - LAN cables have 4 pairs
- Shielded twisted pair also exists, but is more expensive.
- TP cables are also used in telephone trunk lines and can have up to several thousand pairs.

28

Guided Media: Coaxial Cable

- Formerly common on LANs, but now disappearing
- More expensive than twisted pair, but coax is shielded, so it's less prone to interference than twisted pair.
- Coaxial Cable Structure (Figure 3-5):
  - Inner conductor
  - Insulator
  - Wire mesh ground
  - Outer protective jacket or shell

29

Guided Media: Fiber Optic Cable

- Widely used and has extremely high capacity.
- Light created by an LED or laser is sent down a thin glass or plastic fiber.
- Fiber optic cable structure (from center):
  - Core (v. small, 5-50 microns, ~ the size of a single hair)
  - Cladding, which reflects the signal
  - Protective outer jacket

30

Guided Media: Fiber Optic Cable

- Types of Optical Fiber:
  - **Multimode** is cheap, but the signal spreads out over short distances (up to ~500m)
    - Attenuation problem
  - **Graded index multimode** reduces the spreading problem by changing the refractive properties of the fiber to refocus the signal
    - can be used over distances of up to about 1000 meters.
  - **Single mode** is expensive because difficult to manufacture, but signal can be sent <= 100 kilometers without spreading
    - Uses lasers to emit light

31

Other Benefits of Fiber

- Not as fragile
- Not heavy or bulky
- More resistant to corrosion

32

Wireless Media

- **Radio**:
  - wireless transmission of electrical waves
  - includes AM and FM radio bands
    - For computer transmission, the frequency does not interfere with AM-FM
  - Signals travel a few miles
  - Microwave is also a form of radio transmission

33

Coding

- Any written language uses symbols (A,1,#), but computers send signals in 1s and 0s (bits).
- Each written character needs a bit code in order to be used by a computer. A set of these codes for a language is called a **coding scheme**.
- A **byte** is one character (usually 7-8 bits)
- Main character codes in North America:
  - **ASCII**: American Standard Code for Information Interchange, originally used a 7-bit code (128 combinations), now 8-bit version is used (256).
  - **EBCDIC**: Extended Binary Coded Decimal Interchange Code, an 8-bit code developed by IBM.

34

Transmission Modes

- Data can be sent either in serial or in parallel
- **Parallel mode** (Figure 3-10): uses several wires, each wire sending one bit at the same time as the others.
  - A parallel printer cable sends 8 bits together.
  - Other ex: Your computer's processor and motherboard
- **Serial Mode** (Figure 3-11): sends bit by bit over a single line.
- slower than parallel
- can be used over longer distances because the bits stay in the order they were sent
  - while bits sent in parallel mode tend to spread out over long distances.

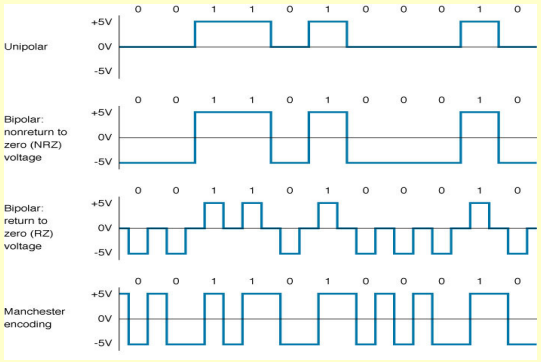
35

Digital Transmission (cont.)

- With **bipolar** signals, signals are sent using both positive and negative voltages.
- A second digital transmission factor, called **return to zero** (**RZ**) means the signal returns to the 0 voltage level after sending a bit. In **non return to zero** (**NRZ**), the signals maintains its voltage at the end of a bit.
- Ethernet uses **Manchester encoding** in which the bit value is defined by a **mid-bit transition**. A *high to low* voltage transition is a binary 0 and a *low-high* mid-bit transition defines a binary 1.

36

Figure 3-12 Digital transmission types



Carrier Waves

- Modems use carrier waves to send information (Figure 3-13).
- Each wave has three fundamental characteristics:
  - **Amplitude**, meaning the height (intensity) of the wave
  - **Frequency**, which is the number of waves that pass in a single second and is measured in Hertz (cycles/second) (**wavelength**, the length of the wave from crest to crest, is related to frequency.).
  - **Phase** the point in the wave's cycle at which a wave begins (direction it begins)
    - measured in degrees. (From example, changing a wave's cycle from crest to trough corresponds to a 180 degree phase shift).
- **Hertz** – cycles per second

38

Bit Rate vs. Baud Rate (Symbol Rate)

- **Bit** – a unit of info
- **Baud** – unit of signaling speed used to indicate the # of times per second the signal on the comm line changes
- **Bit rate** (or **data rate**) is the number of bits transmitted per second.
- **Baud rate** (same as **symbol rate**) refers to the number of symbols transmitted per second.
- Since multiple bits can be encoded per symbol, the two terms are not the same.
- For example, in Figure 3-17, the bit rate is twice the baud rate.

39

MULTIPLEXERS

- Computers have **ports**- connections to a peripheral device
- Ports are limited so multiplexers were created to allow more than one device to be connected to a port
- **Multiplexer**- device that
  - receives data from several devices,
  - compresses them into a single stream of data
  - transmits it over a single line
- Work in pairs like modems

40

MULTIPLEXERS

- Multiplexers add a code before each string of characters that tell which terminal the data is coming from
  - Multiplexer at the other end decodes the data and sends it to host
- Makes the network more efficient
  - Lines are not idle as much

41

Multiplexing

- Multiplexing means breaking up a higher speed circuit into several slower circuits.
- Multiplexers are **transparent**
- The main advantage of multiplexing is cost; multiplexing is cheaper because fewer network circuits are needed.
- Without WDM, the Internet would have collapsed in the 1990s
- There are four categories of multiplexing:
  - **Frequency division multiplexing** (FDM)
  - **Time division multiplexing** (TDM)
  - **Statistical time division multiplexing** (STDM)
  - **Wavelength division multiplexing** (WDM)

42

Chapter 4. Data Link Layer

43

Introduction

- Data link protocols have three functions:
  - Media Access Control:
    - Controlling when computers transmit.
  - Error Control:
    - Detecting and correcting transmission errors.
  - Message Delineation:
    - Identifying the beginning and end of a message.

44

Media Access Control

- Means controlling when computers transmit
- Important in situations where more than one computer wants to send data at the same time over the same circuit, such as:
  - Point-to-point half duplex links
  - Multipoint configurations in which several computers share the same circuit
- The two main MAC approaches are:
  - controlled access
  - contention

45

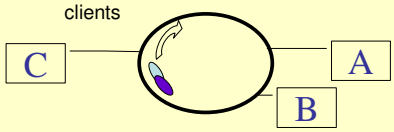
Controlled Access

- Works like a stop light
- Commonly used with access to mainframes:
  - whereby the mainframe or its front end processor determine which circuits have access to it at a given moment.
- Also used by some LAN protocols
  - token ring
  - FDDI

46

Polling

- Server periodically contacts each client to see if it wants to transmit.
- Two types of polling:
- **Roll call -** each client is checked in order to see if it wants to transmit.
  - Clients can also be prioritized
- Hub polling (also called token passing):
  - A token is passed around the network to the clients



47

Contention

- Allow computers to transmit whenever the circuit is free
- This means **collisions** can occur
- Their messages collide and have to be resent.
- Contention approaches need to have a way to decide which computer is allowed to transmit first after a collision occurs.
- Ex: Ethernet

48

Relative Performance (Figure 4-1)

- The performance of controlled access versus contention approaches depends on network conditions.
- Contention
  - better for smaller networks with relatively low usage.
- Controlled
  - better for networks with high traffic volumes where the probability of collisions is high and controlling access means the network will be more efficiently used.
- Finding the crossover point
  - Around 20 computers (more than 20 – controlled)

49

Sources of Errors (Figure 4-2)

- Sources of errors include:
  - **Line outages** in which a circuit fails
  - **White noise** caused by thermal energy (hiss)
  - **Impulse noise** (spikes) are an important source of burst errors and can be caused by lightning, power surges, and poor connections
  - **Cross-talk** occurs when one circuit picks up signals from another
  - **Echoes** are caused by poor connections causing the signal to be reflected back to the transmitting source
  - **Attenuation** is the weakening of a signal over a distance
  - **Jitter** occurs due to small variations in the amplitude, frequency, and phase of a signal
  - **Harmonic distortion** occurs when an amplifier does not correctly amplify its input signal

50

Source of Error	What causes it	How to prevent it
Line Outages	Storms, accidents	
White Noise	Movement of electrons	Increase signal strength
Impulse Noise	Sudden increases in electricity (e.g., lightning)	Shield or move the wires
Cross-talk	Multiplexer guard bands are too small or wires too close together	Increase the guard bands, or move or shield the wires
Echo	Poor connections	Fix the connections, or tune equipment
Attenuation	Gradual decrease in signal over distance	Use repeaters or amplifiers
*** Intermodulation Noise**	Signals from several circuits combine	Move or shield the wires
*** Jitter**	Analog signals change phase	Tune equipment
*** Harmonic Distortion**	Amplifier changes phase	Tune equipment

* = mostly in analog

Figure 4-2

51

Error Prevention

- Shielding
  - Adds expense and difficulty in installing
- Move cables
- Change multiplexing techniques
- Add repeaters/amplifiers
  - Noise and distortion are also amplified

52

Parity Checking (Figure 4-3)

- Parity checking is one of the oldest and simplest error detection techniques.
- In parity checking, a single bit is added to each character. For even parity, the sum of the bits (including the parity bit) remains even, for odd parity, the sum remains odd.
- At the receiving end, the parity bit is recalculated. If one bit has been transmitted in error the received parity bit will differ from the recalculated one.
- Simple, but doesn't catch all errors.
- If two (or an even number of) bits have been changed…?.
  - Is 50% effective
- Only identifies that a problem exists; does not tell where

53

Error Correction via Retransmission

- When an error is detected, it is corrected by retransmission of the data along with its error detection value.
- The process of requesting that a data transmission be resent is called an **A**utomatic **R**epeat Re**q**uest or ARQ.
- The two main ARQ protocols are:
  - Stop and Wait ARQ
  - Continuous ARQ

54

Forward Error Correction

- ARQ techniques are also called backward error correction.
- The alternative, **forward error correction**, means the receiving device can correct incoming messages itself instead of having them resent.
- Extra corrective information needs to be sent along with the data that allows the data to be checked and corrected by the receiver.
- The amount of extra information needed is usually 50-100% of the data.
- Useful for one way transmissions or when transmission times are very long (as with communications to spacecraft).

55

Forward Error Correction (Figure 4-7)

- Hamming Code. Extra parity values are calculated so that each data bit figures into two parity bit calculations.
- That means that if any one bit, either parity or data, gets changed in transmission, the change in the received data can be detected and corrected (see Figure 4-7).
- This technique, however, only works for one bit errors.

56

Asynchronous Transmission (Figure 4-9)

- Sometimes called start-stop transmission
- Computers can send whenever they need
- Each character is sent independently
- The transmission sequence:
  - begins with a start bit (for synchronization)
  - next the character is sent
  - then the parity bit
  - finally a stop bit are sent
- The start bit is usually a 0 and the stop bit a 1.

57

Synchronous Transmission

- Data is sent in a large block called a frame or packet
- Used on both point-to-point and multipoint circuits. In the latter case, addressing information needs to be included in the frame.
- Synchronous packets sometimes begin and end with a series of synchronization (SYN) characters that are used to help the receiver recognize incoming data.
- Synchronous transmission protocols can be byte-oriented, bit-oriented, or byte-count protocols.

58

Ethernet (IEEE 802.3)

- Most widely used LAN protocol.
- Developed jointly by Digital, Intel, and Xerox
- **Byte-count** with contention based media access control. (a field is included that gives length of data)
  - Any bit pattern can be transmitted
- (see Figure 4-12).
- Each frame contains:
  - MAC layer destination and source addresses (6 bytes each)
  - Length (of data) field (2 bytes)
  - Data or message field of variable length
  - Frame Check Sequence (CRC-32, 4 bytes long)

59

Chapter 5

Network and Transport Layers

60

Introduction: The Network and Transport Layers

- The **transport layer** is responsible for end-to-end delivery of messages.
- **Transport layer**
  - sets up **virtual circuits**
  - responsible for **segmentation** (breaking the message into several smaller pieces)
  - reassembly (reconstructing the original message into a single whole) at the receiving end.
- **Network layer** is responsible for
  - **addressing**
  - **routing**
- The network and transport layers also perform **encapsulation** of message segments from the application layer, passing them down to the data link layer on the sending end and passing them up to the application layer on the receiving end (see Figure 5-1)

61

Transport and Network Layer Protocols

- The following are commonly used protocol suites:
  - **TCP/IP**
  - **IPX/SPX**
  - X.25
  - SNA

62

Transmission Control Protocol/Internet Protocol (TCP/IP)

- Developed
  - in 1974
  - as part of Arpanet
  - for the U.S. Department of Defense .
- TCP/IP is the protocol used by the Internet.
- Almost 70% of all backbone, metropolitan, and wide area networks use TCP/IP.
- In 1998, TCP/IP surpassed IPX/SPX to become the most common protocol on local area networks.

63

Transmission Control Protocol (Figure 5-2)

- TCP performs **packetization**
  - breaking up the message into smaller pieces
  - numbering the segments
  - reassembling them at the destination end of the transmission
- TCP ensures that the segments are reliably delivered.
- Header fields include:
  - source and destination port identifiers
  - packet sequence number used in reassembly

64

Internet Protocol (Figures 5-3 and 5-4)

- IP is responsible for addressing and routing of packets.
- *Two versions in current in use: IPv4 & IPv6.*
- *IPv4: a 160 bit (20 byte) header, uses 32 bit addresses.*
- *IPv6: 320 bit (40 byte) header. Mainly developed to increase IP address space due to the huge growth in Internet usage during the 1990s.*
- *IPv6 uses 128 bit addresses.*
- Header fields include: source and destination addresses, packet length and packet number.

65

2. Packetization and Reassembly

- Application layer sees message as a single block (or stream) of data.
- Another transport layer job is breaking large messages into smaller pieces (**packetization**) and putting them back together at the destination (**reassembly**).
- The transport layer also decides
  - whether to deliver the incoming packets as they arrive (as with the Web pages) - or –
  - wait until the entire message arrives (as with e-mail).

66

Connection-Oriented Routing

- TCP also handles end-to-end routing, such as setting up a **virtual circuit** (called connection-oriented routing).
- All packets in a message follow the same route
- The first step in creating a virtual circuit
  - the sender to send a special **SYN packet**, which requests the virtual circuit and negotiates with the receiver over what packet size to use.
- Following this, the packets are sent one by one in order from source to destination using the continuous ARQ technique.
- Finally, a special **FIN packet** is sent by TCP to close the virtual circuit.

67

Quality of Service

- Some applications, especially real time applications (e.g., voice and video frames), require packets be delivered within a certain period of time in order to produce a smooth, continuous output (e-mail doesn't require this).
- The timely delivery of packets is called **quality of service (QoS)**. QoS routing defines **classes of service**, each with a different priority:
  - Real-time applications get the highest priority
  - a graphical file for a Web page gets a lower priority
  - E-mail gets the lowest priority (since it can wait a relatively long time before being delivered).

68

Assigning Addresses (Figure 5-6)

- The Internet uses three kinds of addresses:
  - Application layer addresses
    - Assigned by network managers
    - Users use these in applications (Ex: www.baylor.edu)
    - Some servers have more than one application layer address.
  - Network layer addresses (IP addresses)
    - Assigned by network managers, or by programs such as DHCP
    - Networks on the Internet are assigned a range of possible IP addresses
  - Data link layer addresses
    - Hardware addresses placed on network interface cards by their manufacturers
- Servers have permanent addresses, clients usually do not.
- For a message to travel from sender to receiver, these addresses must be translated from one type to another. This process is called **address resolution**.

69

Figure 5-6 Types of network addresses

Address Type	Example Software	Example Address
Application Layer	Web Browser	www.kelley.indiana.edu
Network Layer	IP	129.79.127.4
Data Link Layer	Ethernet	00-0C-00-F5-03-5A

70

Subnets

- Computers on the same LAN are usually given IP numbers with the same prefix, called a **subnet**. For example:
  - Computers in a University's Business school might be given addresses in the range: 128.192.56.x (where x is between 0 & 255)
  - While the Computer Science IP addresses could be: 128.192.55.x
- The above subnets are 128.192.56.x and 128.192.55.x, respectively.
- **Subnet masks** are used to make it easier to separate the subnet part of the address from the host part. In the above example, the subnet mask would be: 255.255.255.128

71

Dynamic Addressing

- Networks no longer give fixed addresses to clients.
- Use **dynamic addressing**, giving addresses to clients when they log in to a network.
- A small ISP, for example, might only need to assign 500 IP addresses to clients at any one time, even though it has several thousands subscribers.
- Two programs are currently in use for this:
  - bootp
  - Dynamic Host Control Protocol (DHCP).
- A client broadcasts a message requesting an IP address when it is turned on or connected.
- IP addresses can also be assigned with a time limit

72

Server Name Resolution

- Translate the destination host's domain name to its corresponding IP address
- If the desired IP address is not in the client's address table, it uses the **Domain Name Service (DNS)** to resolve the address.
- DNS works through a group of **name servers** that maintain databases which contain directories of domain names and their corresponding IP addresses.
- Organizations must supply the IP address of their DNS server if they register a domain name
- DNS servers exchange information among themselves

73

Routing

- Routing is the process of deciding what path to have a packet take through a network (Figure 5-8).
- More than one route may be possible, so routing tables were developed (Figure 5-9).
- Routing decisions on the Internet are usually handled by special purpose devices, called **routers**, that maintain their own routing tables.

74

Types of Routing

- **Centralized routing**
  - Routing decisions are made by one central computer
  - Typically used in mainframe-based networks.
- **Decentralized routing**
  - Computers making routing decisions operate independently of one another
  - **Static routing**
    - Tends to be used on relatively simple networks, uses fixed routing tables which are developed by network managers.
    - The table can change if computers are added or removed
  - **Dynamic routing**
    - Routing decisions are made dynamically
    - Is based on routing condition information exchanged between routing devices.

75

Chapter 6. Local Area Networks

76

Why use a LAN?

- Main benefits to using a LAN:
  - *information sharing*
    - file sharing, exchanging e-mail, and using the Internet
  - *resource sharing*
    - Hardware
    - Software
      - Site and user licenses

77

Peer-to-Peer Networks

- Do not use dedicated servers.
- Any computer on a peer-to-peer network can act as a client or server.
- Tend to be small networks.
- Main advantage of P2P networking is lower cost since there is no dedicated server, generally the most expensive network component.
- Main disadvantage: generally slower than dedicated server networks, since
  - each computer is less powerful
  - may be in use as a client and a server at the same time.

78

Basic LAN Components (Figure 6-1)

- The six basic LAN components are:
  1. Clients
  2. Servers
  3. Network Interface Cards
  4. Network Cables
  5. Hubs and Switches
  6. Network Operating System
- The first two were discussed in chapter 2, the rest will be discussed in this chapter.

79

Network Interface Cards

- Also called
  - network cards
  - network adapters
  - NICs
- Include a cable socket allowing computers to be connected to the network.
- NICs are part of both the physical and data link layer and include a unique data link layer address (sometimes called a MAC address)
- NICs organize data into frames and then sends them out on the network.
- Notebook computers often use NICs that are plugged into the PCMCIA port.

80

Network Operating Systems

- Software that runs the LAN
  - Server NOS
  - Client NOS
- Server NOSs enable server to execute and respond to the requests sent to them as web server, print servers, file servers, etc.
- Client NOS functions are typically included in most OS packages such as Windows 98 and Windows 2000.
  - Drive mapping (server, volume, folder)
  - Print capturing
  - Login

81

Network Profiles

- The **network profile** specifies what resources on each server are available to the network for use by other computers, including data files, printers, etc.
- Devices that are not included in the network profile can not be used over the network.
- **User profiles** describe what each user on a LAN has access to.
  - Group profiles
- Most LANs also use **auditing software** which keeps track of which user has accessed what network resource.

82

Ethernet (IEEE 802.3)

- Almost all LANs today use Ethernet
- Originally, Ethernet was jointly developed by a consortium of Digital Equipment Corp., Intel and Xerox and was standardized as **IEEE 802.3**.
- Ethernet LANs that use hubs are sometimes called **shared Ethernet**.

83

Shared Ethernet Topology (Figure 6-3)

- Ethernet's **logical topology** is a bus topology.
- This means all computers on the network receive messages from all other computers, whether the message is intended for those computers or not.
- When a frame is received by a computer, the first task is to read the frame's destination address to see if the message is meant for it or not.
- Although, a decade ago most Ethernet LANs used a physical bus, almost all Ethernets today use a **physical star topology**, with the network's computers linked into hubs.
- It is also common to link use multiple hubs to form more complex physical topologies (Figure 6-4).

84

CSMA/CD

- Stands for: **C**arrier **S**ense **M**ultiple **A**ccess w/ **C**ollision **D**etect
- **Carrier Sense**: computers listen to the network to see if another computer is transmitting before sending anything themselves.
- **Multiple Access**: all computers have access to the network medium.
- **Collision Detect**: if they detect a collision (CD), they then wait a random amount of time and resend the frame (It has to be random in order to avoid another collision).

85

Switched Ethernet Topology

- Uses switches instead of hubs
- While a hub broadcasts frames to all ports, the switch reads the destination address of the frame and only sends it to the corresponding port.
- The effect is to turn the network into a group of point-to-point circuits and to change the logical topology of the network from a bus to a star.
- The switch looks like a hub on the outside

86

Improving Server Performance: RAID

- Improving disk drive performance is especially important, since disk reads are the slowest task the server needs to do.
- Replacing one large drive with many small ones can improve server performance.
- RAID or Redundant Array of Inexpensive Disks, builds on this idea. RAID systems can be used to:
  - improve performance - and –
  - increase reliability

87

Reducing Network Demand

- Performance can also be improved by reducing network demand. This can be done by:
  - Moving more files, such as heavily used software packages to client computers.
  - Disk caching, software on client machines can also reduce server demand.
  - Moving user demands from peak times to off peak times
  - Delaying some network intensive jobs to off-peak times

88

Chapter 7

89

Wireless Ethernet (IEEE 802.11)

- Wireless LANs use:
  - radio
  - infrared
- WLANs are growing in popularity because
  - they eliminate cabling
  - facilitate network access from a variety of locations
- Most common is IEEE 802.11; also called:
  - Wireless Ethernet
  - Wireless LAN

90

Wireless LAN Topology

- WLAN topologies are the same as on Ethernet: physical star, logical bus (Figure 6-7).
- Instead of hubs, WLANs use devices called **access points** (AP).
  - Maximum transmission range is 100-500 feet
  - Usually use 2 or more together
- Each WLAN computer uses a NIC that transmits radio signals to the AP.
- Security is a potential problem
- Wireless LAN devices use the same radio frequencies, so they must take turns using the network.

91

Chapter 8

Backbone Networks

92

Backbone Network Components

- Two basic components:
  - **network cable**
  - **hardware devices** connecting it to other networks
- The backbone network's cable functions in the same way as in LANs.
- Optical fiber is mostly used
- The hardware devices can be:
  - Computers
  - Special purpose devices used for interconnecting networks including
    - Bridges
    - Routers
    - Gateways

93

Bridges (Figure 7-2)

- Bridges operate at the data link layer.
- The networks they connect together must use similar
  - data link protocols (Ethernet, Kermit, etc.)
  - network protocols (TCP/IP, IPX/SPX, etc.)
- They can connect different types of cable
- Bridges operate in a *similar* way to layer 2 switches (use Ethernet addresses to build forwarding tables)
- They learn which computers are on each side of the bridge by reading the source addresses on incoming frames and recording this information in forwarding tables.
- Once popular, bridges are losing market share to layer 2 switches as the latter become cheaper and more powerful.

94

Routers (Figure 7-3)

- Routers operate at the network layer
- Connect two or more network segments that may have
  - different data link layer protocols (Ethernet, Kermit, etc.)
  - but the same network layer protocol (TCP/IP, IPX/SPX, etc.)
- Connect different types of cabling.
- Router operations involve stripping off the header and trailer of the incoming data link layer frame and then examining the destination address of the network layer packet. The router then builds a new frame around the packet and sends it out onto another network segment.

95

Gateways

- Operate at the network layer
- More complex than routers because they provide an interface between more dissimilar networks.
  - Same or different data link and network protocols
- Same or different cable types
- Like routers, gateways only process messages that are specifically addressed to them.
- Can be used for code conversion
  - ASCII → EBCDIC for example
- Can be used to translate between protocols

96

Rack-based Collapsed Backbones

- Rack-based backbones collapse the backbone into a single room, called a **main distribution facility (MDF)** where networking equipment is connected and mounted on equipment racks (Figure 7-9).
- Devices are connected using short **patch cables**.
- Moving computers between LANs is relatively simple since equipment is all in the same location (i.e. moving a high-traffic computer to another segment)
- Physical location of computers has no influence necessarily on LAN membership
- Easy upgrade and maintenance of eqpt

97

Chapter 9. Metropolitan and Wide Area Networks

98

Introduction

- Metropolitan area networks (MANs) typically span from 3 to 30 miles and connect backbone networks (BNs), and LANs
- Wide area networks (WANs) connect BNs and MANs across longer distances
  - often hundreds of miles or more
- Most organizations cannot afford to build their own MANs and WANs, so they rent or lease circuits from common carriers
  - A common carrier is a private company that sells or leases communications services and facilities to the public. Common carriers also provide local telephone services
  - AT&T, MCI, BellSouth, PACTEL or NYNEX

99

Circuit Switched Services: Basic Architecture (Figure 8-1)

- Uses a cloud architecture
  - users connect to a network and what happens inside of the network "cloud" is hidden from the user
- A user using a computer and a modem dials the number of a another computer and creates a temporary circuit between the two.
- When the communications session is completed, the circuit is disconnected.

100

Advantages and Disadvantages of Circuit Switched Services

- Advantages:
  - Simple
  - Flexible
  - Inexpensive when not used intensively
- Two main problems with dialed circuits.
  - Each connection goes through the regular telephone network on a different circuit, which vary in quality.
  - Data transmission rates are low, from 28.8 to 56 Kbps.
- An alternative is to use a private dedicated circuit, which is leased from a common carrier for the user's exclusive use 24 hrs/day, 7 days/week.

101

Dedicated Circuit Services (Figure 8-2)

- Dedicated circuits involve leasing circuits from common carriers to create point to point links between organizational locations.
- These points are then connected together using special equipment such as routers and switches.
- Billed at a flat fee per month for which the user has unlimited use of the circuit.
- The three basic dedicated circuit architectures are ring, star, and mesh architectures.

102

Mesh Architecture (Figure 8-5)

- Mesh architectures can use either a full or partial mesh.
- It is expensive, so only partial mesh networks are set up. As long as there are alternative routes on the network, the impact of losing a circuit on the mesh is minimal.
- Combine the performance benefits of both ring and star networks and use decentralized routing, with each computer performing its own routing.
- Setting up the many alternate routes between computers on a mesh network means that creating a mesh architecture is more expensive than setting up a star or ring network.

103

Packet Routing Methods

- There are two methods for routing packets:
  - A **datagram** is a connectionless service which adds a destination and sequence number to each packet, in addition to information about the data stream to which the packet belongs. Individual packets can follow different routes before being reassembled on the destination host.
  - In a **virtual circuit** the packet switched network establishes an end-to-end circuit between the sender and receiver. All packets for that transmission take the same route over the virtual circuit that has been set up for that transmission.

104

Virtual Private Networks

- **Virtual Private Networks** (VPNs) use PVCs that run over the Internet but appear to the user as private networks.
- Packets sent over these PVCs, called **tunnels**, are encapsulated using special protocols that also encrypt the IP packets they enclose.
- The growing popularity of VPNs is based on their low cost and flexibility.
- There are two important disadvantages of VPNs:
  - the unpredictability of Internet traffic
  - the lack of standards for Internet-based VPNs, so that not all vendor equipment and services are compatible.

105

Chapter 10. The Internet

106

Basic Architecture: NAPs and national ISPs

- The Internet has a hierarchical structure.
- At the highest level are large national **Internet Service Providers** that interconnect through **Network Access Points (NAPs)**.
- http://nap.aads.net/
- There are about a dozen NAPs in the U.S., run by common carriers such as Sprint and Ameritech (Figure 9-1), and many more around the world.
- Regional ISPs interconnect with national ISPs and provide services to their customers and sell access to local ISPs who, in turn, sell access to individuals.

107

Digital Subscriber Line

- Digital Subscriber Line (DSL) is one of the most promising technologies now being implemented to significantly increase the data rates over traditional telephone lines.
- Historically, voice telephone circuits have had only a limited capacity for data communications because they were constrained by the 4 kHz bandwidth voice channel.
- Most local loop telephone lines actually have a much higher bandwidth and can therefore carry data at much higher rates.

108

Cable Modems

- One potential competitor to DSL is the "cable modem" a digital service offered by cable television companies which offers an upstream rate of 1.5-10 Mbps and a downstream rate of 2-30 Mbps.
- A few cable companies offer downstream services only, with upstream communications using regular telephone lines.

109

Internet 2 (Figure 9-11)

- New networks are being developed to develop future Internet technologies including:
  - The very high performance Backbone Network Service (vBNS) run by Worldcom. 34 universities participate.
  - The Abilene network (also called Internet 2) is being developed by the University Corporation for Advanced Internet Development (UCAID).
  - CA*Net3 is the Canadian government initiative.
- Access is through **Gigapops**, similar to NAPs, but which operate at very high speeds (622 Mbps to 2.4 Gbps) using SONET, ATM and IPv6 protocols.
- Protocol development focuses on issues like Quality of Service and multicasting.
- New applications include tele-immersion and videoconferencing.

110

Abilene Project

What is the Abilene Project?

Abilene is a high-performance network developed by the University Corporation for Advanced Internet Development (UCAID) in partnership with:

Cisco Systems
Juniper Networks
Nortel Networks
Qwest Communications
Indiana University

An important goal of the Abilene project is to provide a backbone network for Internet2. Abilene uses high-performance IP routers, accessible to gigaPoPs in several dozen locations nationwide, to support the Internet2 infrastructure. Abilene enables faculty and staff at Internet2 universities and research labs to develop advanced network services and applications.

Does the Abilene Project replace existing Internet connections?

•No, network traffic should be segmented between educational and commercial traffic.

111

Abilene Project

- **What capabilities does Abilene have beyond those of the commercial Internet?**
  - Abilene provides the advanced networking capabilities required to develop the applications and network services higher education needs to meet its research and education missions.
  - This includes the testing of new networking technologies such as Quality of Service and multicast.
  - Abilene uses high-speed Sonet facilities and IP-over-Sonet routers.
  - Abilene is operating initially at OC-48c (2.4 gigabits per second) backbone links. In parallel, we are working with our partners to deploy additional links running at 10 gigabits per second.

112

Chapter 11. Network Security

113

Why Security is Needed

- Orgs becoming more dependent on networks
- The rise of the Internet has increased vulnerability of corporate assets
- Publicized security breaches can cost $$$
- Losses resulting from the disruption of a security breach

114

Types of Security Threats

- **Disruptions** - the loss or reduction in network service.
- Some disruptions may also be caused by or result in the **destruction** of data.
- Natural (or manmade) **disasters** may occur that destroy host computers or large sections of the network.
- **Unauthorized access** is often viewed as hackers gaining access to organizational data files and resources. However, most unauthorized access incidents involve employees.

115

Security Threats

- A network security threat is any potentially adverse occurrence that can harm or interrupt the systems using the network, or cause a monetary loss to an organization.
- Once the threats are identified they are then ranked according to their occurrence.
- Figure 11-5 summarizes the most common threats to security.
- Two interesting items:
  - hacking is not the most common issue
  - greatest hacking threat is internal (70% of orgs vs 25%)

116

Risk Assessment

- **Risk assessment** is the process of making a network more secure, by comparing each security threat with the control designed to reduce it.
- One way to do this is by developing a control spreadsheet (Figure 11-3).
- Network assets are listed down the side.
- Threats are listed across the top of the spreadsheet.
- The cells of the spreadsheet list the controls that are currently in use to address each threat.

117

Network Address Translation

- **Network address translation (NAT)** is used to shield a private network from outside interference.
- An **NAT proxy server** uses an address table, translating network addresses inside the organization into aliases for use on the Internet. So, internal IP addresses remain hidden.

*

118

Honeypots

- By luring a hacker into a system, a honeypot serves several purposes:
- The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned.
- The hacker can be caught and stopped while trying to obtain root access to the system.
- By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers.
- To get around legal concerns, a warning message should be displayed saying that unauthorized access will be monitored (or something like that)

119

Linux

- What are the benefits of using Linux?
- Read pages 33-35 in the Web Server Admin textbook.

120