NEW PERSPECTIVES

Unit 3
Networks

Computer Concepts 2016

ENHANCED EDITION

3 Unit Contents

- Section A: Network Basics
- Section B: The Internet
- Section C: Internet Access
- Section D: Local Area Networks
- Section E: File Sharing

3 Section A: Network Basics

- Communication Systems
- Communication Channels
- Network Topology
- Network Nodes
- Communication Protocols

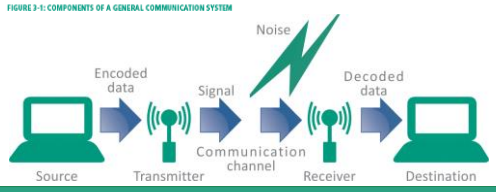
3 Communication Systems

- Networks can be classified in many ways; as a network user, you'll want to keep in mind the idea of control and how it affects your privacy and security
- A network links things together
- A **communication network** (or communication system) links together devices to data and information can be shared among them

3 Communication Systems

- In 1948, Claude Shannon, and engineer at Bell Labs, published and article describing a communication system model applicable to networks of all types
- His diagram illustrates the essence of a network:

FIGURE 3-1: COMPONENTS OF A GENERAL COMMUNICATION SYSTEM



3 Communication Systems

- Networks can be classified according to their size and geographic scope

PAN (personal area network)

PANs connect smart devices or consumer electronics within a range of about 30 feet (10 meters) and without the use of wires or cables. The reference to *personal* indicates that the network serves a single individual, rather than multiple users. A PAN could be used to sync data from a handheld device to a desktop computer, ship data wirelessly to a printer, or transmit data from a smartphone to a wireless headset.

LAN (local area network)

LANs are data communication networks that connect personal computers within a very limited geographical area—usually a single building. School computer labs and home networks are examples of LANs. Wi-Fi networks that you can access in airports, coffee shops, and other public places are LANs. The in-house networks operated by most businesses are also LANs.

WAN (wide area network)

WANs cover a large geographical area and usually consist of several smaller networks, which might use different computer platforms and network technologies. The Internet is the world's largest WAN. Other public WANs include telephone systems, cable television systems, and satellite-based communication systems.

FIGURE 3-2: NETWORK CLASSIFICATIONS

3 Communication Channels

- A **communication channel** is the medium used to transport information from one network device to another
- **Wired channels** transport data through wires and cables
- **Wireless channels** transport data from one device to another without the use of cable or wires

3 Communication Channels

- Wired channels include twisted pair wires used for telephone land lines, coaxial cables used for cable television networks, Category 6 cables used for LANs, and fiber-optic cables used for high-capacity trunk lines

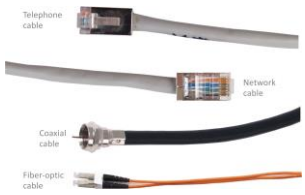


FIGURE 3-3: NETWORK CABLES

3 Communication Channels

- When you set up a wired connection, you don't have to worry about hackers intercepting your data from outside your house
- There are ways to tap into a wired network, but they require physical access to the cable or fairly sophisticated snooping equipment

3 Communication Channels

Cables can be shielded against interference and encased in protective casings for installations that are outdoors and underground.

Wired connections are dependable. Their carrying capacity and speed are not affected by airborne interference from rain, snow, or electrical devices.

Wired connections are more secure than their wireless counterparts because a device can join a wired network only if it is physically connected by a cable.

FIGURE 3-4: ADVANTAGES OF WIRED CHANNELS

3 Communication Channels

In WANs, wired installation can be costly because cables have to be suspended from poles or buried underground. They can be damaged by weather events and digging in the wrong place. Repairs to underground cables require heavy equipment to locate, access, and fix the break.

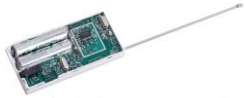
LAN devices connected by cables have limited mobility. Desktop computers tend to be better candidates for wired connections, whereas laptops, tablets, and handheld devices can retain their mobility when they are not tethered to a cable.

Cables are unsightly, tend to get tangled, and collect dust. Running cables through ceilings, walls, and floors can be challenging. Cables can also carry electrical surges that have the potential to damage network equipment.

FIGURE 3-5: DISADVANTAGES OF WIRED CHANNELS

3 Communication Channels

- The most widespread wireless channels for communication networks are radio signals and microwaves
- Most wireless channels transport data as RF signals commonly called radio waves
- RF signals are sent and received by a transceiver (a combination of a transmitter and a receiver) that is equipped with an antenna



Devices used with wireless connections are equipped with transceivers that include a transmitter for sending data and a receiver for collecting data. A transceiver has an antenna, which may be visible or may be housed out of sight within a device's system unit.

FIGURE 3-6: TRANSCEIVER-EQUIPPED DEVICES

3 Communication Channels

- Microwaves (the waves themselves, not your oven!) provide another option for transporting data wirelessly
- Microwaves are electromagnetic signals that can be aimed in a single direction and have more carrying capacity than radio waves
- Microwave installations usually provide data transport for large corporate networks

3 Communication Channels

- Advantages of wireless
  - Mobility
  - No unsightly cables
  - Less susceptible to power spikes
- Disadvantages of wireless
  - Speed
  - Range
  - Security
  - Licensing

3 Communication Channels

- **Bandwidth** is the transmission capacity of a communication channel
- Network channels that are capable of moving at least two megabits of data per second (2 Mbps) are classified as **broadband**
- Channels slower than 2 Mbps are classified as **narrowband**

3 Network Topology

- In the context of communication networks, topology refers to the structure and layout of network components, such as computers, connecting cables, and wireless signal paths
  - Point-to-point topology refers to the process of peripheral devices connecting to a host device using expansion ports, USB cables, or Bluetooth
  - Star topology connects multiple devices to each other, either as a full mesh or a partial mesh
  - The less popular bus topology connects devices in a linear sequence

FIGURE 3-8: NETWORK TOPOLOGIES

3 Network Topology

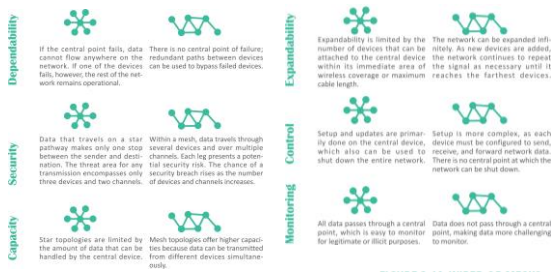


FIGURE 3-10: WIRED OR MESH?

3 Network Nodes

- Any device on a network is called a **node**
- Devices on a network are classified as DTEs or DCEs
  - **DTE** stands for data terminal equipment and can be any device that stores or generates data
  - **DCE** stands for data communication equipment; these devices control the speed of data over networks, convert signals from cables to wireless, check for corrupted data, and route data to its destination

3 Network Nodes

- A **router** is a device that controls the flow of data within a network and also acts as a gateway to pass data from one network to another
- A **modem** contains circuitry that converts the data-carrying signals from a digital device to signals that can travel over various communications channels

FIGURE 3-11: ROUTERS

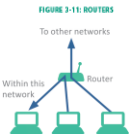
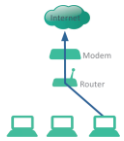


FIGURE 3-12: MODEMS



3 Network Nodes

- DCEs such as repeaters, switches, and hubs can extend the range of your home network

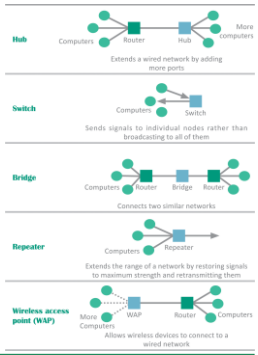


FIGURE 3-13: NETWORK DEVICES

3 Communication Protocols

- In the context of networks, a **communication protocol** refers to a set of rules for efficiently transmitting data from one network node to another
- This process is called **handshaking**
- Networks use more than one protocol, and the collection of protocols for a network is referred to as a **protocol stack**

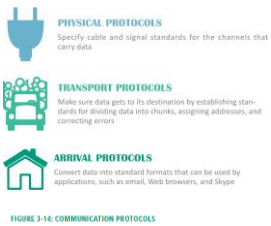


FIGURE 3-14: COMMUNICATION PROTOCOLS

3 Section B: The Internet

- Background
- Internet Infrastructure
- Packets
- Internet Addresses
- Domain Names

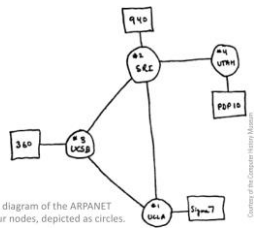
3 Background

- The history of the Internet begins in 1957
- In a response to the Soviet Union launching Sputnik, the first man-made satellite, the U.S. government resolved to improve its scientific and technical infrastructure
- One of the resulting initiatives was the Advanced Research Projects Agency (ARPA)

3 Background

FIGURE 3-16: THE ARPANET, 1969

- ARPA designed a project to help scientists communicate and share valuable computer resources, and called it The ARPANET
- The **ARPANET**, created in 1969, connected computers at UCLA, the Stanford Research Institute, the University of Utah, and UC California at Santa Barbara



The original diagram of the ARPANET included four nodes, depicted as circles.

3 Background

- Early Internet pioneers used primitive command-line user interfaces to send email, transfer files, and run scientific calculations on Internet supercomputers
- In the 1990s, software developers created new user-friendly Internet access tools, and Internet accounts became available to anyone willing to pay a monthly subscription fee

3 Background

- Today's Internet, with an estimated 500 million nodes and more than 2 billion users, is huge
- It is estimated that the Internet handles more than an exabyte of data every day; an **exabyte** is 1.074 billion gigabytes – a nearly unimaginable amount of data!

FIGURE 3-17: TODAY'S INTERNET

3 Background

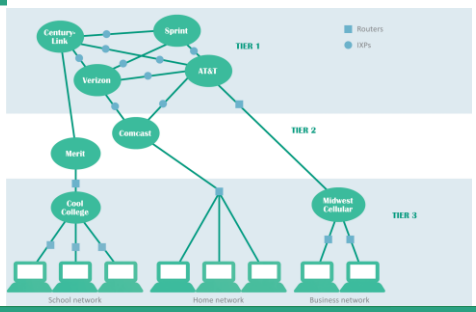
- In theory, no single person, organization, company, or government runs the Internet
- **Internet governance** is simply a set of shared protocols, procedures, and technologies that evolve through common agreement among network providers
- The organization that supervises internet addressing is **ICANN**, the Internet Corporation for Assigned Names and Numbers

3 Internet Infrastructure

- The way networks fit together is referred to as the **Internet Infrastructure**
- Tier 1 networks, such as AT&T, represent the top of the Internet hierarchy and form the **Internet backbone**, a system of high-capacity routers and fiber-optic communication links providing the main routes for data speeding across the Internet
- Networks that form the Internet are maintained by **Internet service providers** (ISPs)
- ISPs exchange data at **Internet exchange points** (IXPs)

3 Internet Infrastructure

FIGURE 3-18: INTERNET INFRASTRUCTURE



3 Internet Infrastructure

- The internet is not free; ISPs make a substantial investment in equipment and infrastructure to connect consumers
- Tier 1 ISPs own and maintain millions of dollars of data communication equipment

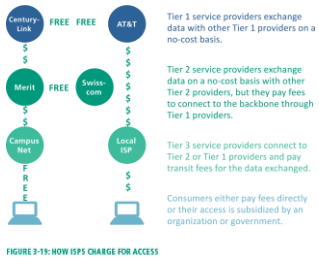


FIGURE 3-19: HOW ISPS CHARGE FOR ACCESS

3 Packets

- A **packet** is a parcel of data that is sent across a computer network; when packets reach their destination, they are reassembled into the original message according to their sequence numbers

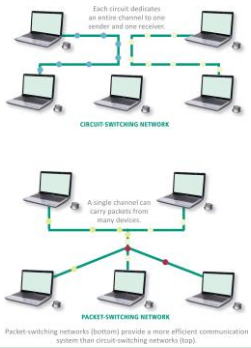
FIGURE 3-20: DATA PACKETS

Messages divided into equal-size packets are easier to handle than an assortment of small, medium, large, and extra large files.

3 Packets

- Communication networks use a technology called **circuit switching**, which establishes a private link between one telephone and another for the duration of a call
- A more efficient alterative to this process is **packet switching** technology, which divides a message into several packets that can be routed independently to their destination

FIGURE 3-21: SHIPPING PACKETS



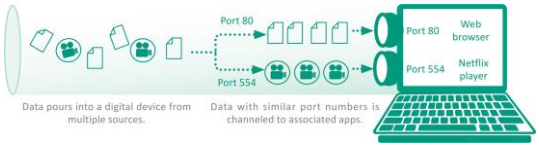
3 Packets

- One of the core Internet protocols, **TCP** (Transmission Control Protocol) is responsible for dividing files into chunks, adding headers containing information for reassembling packets in their original order, and verifying that the data was not corrupted while in transit (a process called error checking)
- **UDP** (User Datagram Protocol) is an alternative transport protocol which is faster than a TCP but does not perform error checking and cannot reorder packets

3 Packets

- A **communication port** (usually referred to simply as a *port*) is a virtual end point for data entering and leaving a digital device
- Communication ports are not a physical circuit, but rather an abstract concept of a doorway, an opening, or a portal through which data flows

FIGURE 3-22: COMMUNICATION PORTS WORK WITH DATA FOR SPECIFIC APPLICATIONS



3 Internet Addresses

- Internet Addresses are controlled by **IP** (Internet Protocol), which is part of the Internet protocol suite
- Many devices on the Internet have permanently assigned IP addresses called **static addresses**
- IP defines two sets of addresses: IPv4 and IPv6
  - **IPv4** – (Internet Protocol version 4); is the Internet address standard; uses 32-bit addresses to identify Internet connected devices
  - **IPv6** – (Internet Protocol version 6); uses 128 bits for each address; produces billions and billions of unique Internet addresses

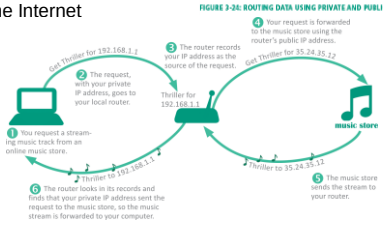
3 Internet Addresses

- Internet addresses that are temporarily assigned to a device are called **dynamic addresses**
- IP addresses can be assigned by a network administrator, but more commonly they are automatically assigned by **DHCP** (Dynamic Host Configuration Protocol)
- A **private IP address** can be allocated by any network without supervision from ICANN – but it cannot be used to send data over the Internet; it's not routable

3 Internet Addresses

- Because a private IP address cannot be routed over the Internet a local router connects instead
- The local router has a **public IP address** that is routable over the Internet

FIGURE 3-24: ROUTING DATA USING PRIVATE AND PUBLIC IP ADDRESSES

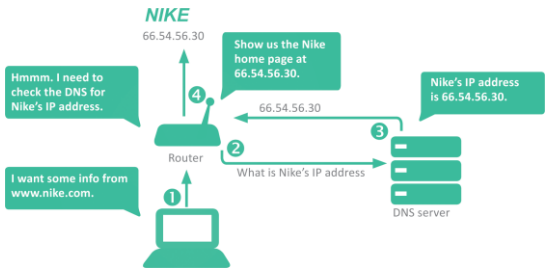


3 Domain Names

- It's hard to remember the string of numbers in an IP address; most Internet destinations also have an easy-to-remember **domain name**, such as nike.com
- The mechanism for tracking domain names and their corresponding IP addresses is called the **domain name system (DNS)**
- A domain name ends with an extension that indicates its **top-level domain**, such as .edu or .org
- **Domain name servers** are scattered around the world and maintain lists of all domain names and their corresponding IP addresses

3 Domain Names

FIGURE 3-26: HOW DOES THE DOMAIN NAME SYSTEM WORK?



3 Domain Names

- Altering DNS records can change the destination of email, browser connections, and download requests
- Unauthorized changes to the DNS are called **DNS spoofing**

FIGURE 3-27: DNS SPOOFING

3 Section C: Internet Access

- Connection Basics
- Cable Internet Service
- Telephone Network Internet Service
- Satellite Internet Service
- Mobile Broadband Service
- Wi-Fi Hotspots

3 Connection Basics

- Data travels over the Internet at an incredible speed, but that speed varies; some Internet services are faster than others
- It is easy to check the speed of your Internet connection by running a few online tests

FIGURE 3-30: IS YOUR CONNECTION FAST ENOUGH?

This speed test measured the rate of data flowing between the user's ISP in Madison, WI, and a Comcast server in Chicago, IL.

3 Connection Basics

- The most common measurement of **connection speed** is the amount of data that can be transmitted in a specified time; technically, it is a measure of capacity

FIGURE 3-31: CONNECTION SPEEDS FOR POPULAR INTERNET-BASED SERVICES

SERVICE	RECOMMENDED DOWNLOAD	RECOMMENDED UPLOAD
Skype video calling and screen sharing	300 Kbps	300 Kbps
Skype video calls (HD)	1.5 Mbps	1.5 Mbps
Skype three-person group calling	2 Mbps	512 Kbps
Netflix movie on a laptop computer	1 Mbps	--
Netflix SD movie on a TV	2 Mbps	--
Netflix 720p HD movie	4 Mbps	--
Netflix "best video and audio experience"	5 Mbps	--
YouTube basic videos	500 Kbps	--
YouTube movies, TV shows, and live events	1 Mbps	--
Amazon Prime Instant Video (SD)	900 Kbps	--
Amazon Prime Instant Video (HD)	3.5 Mbps	--

3 Connection Basics

- ISPs control connection speeds based on the service plan you've selected
- Your **bandwidth cap** is the top speed allowed by your plan
- During peak times, ISPs can place further limits on speed, a process called **bandwidth throttling**
- When Internet upload speed differs from download speed, you have an **asymmetric connection**
- When upload and download speeds are the same, you have a **symmetric connection**

3 Connection Basics

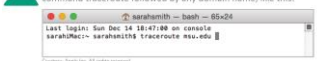
- **Ping** is utility software designed to measure responsiveness
- **Ping rate** indicates how quickly data can reach a server and bounce back to you
- **Latency** is the elapsed time for data to make a round-trip from point A to point B and back to point A
- **Jitter** measures the variability of packet latency caused when network traffic and interference can delay packets and create erratic data flow
- **Packet loss** refers to data that never reaches its destination or gets discarded because it arrives too late

3 Connection Basics

- To determine whether or not your slow Internet connection is caused by your ISP or your computer you can use a **Traceroute**, a network diagnostic tool that lists each router and server

FIGURE 3-33: WHERE DOES YOUR DATA TRAVEL?

On a Mac, open the Utilities folder, then select Terminal. Enter the command traceroute followed by any domain name, like this:

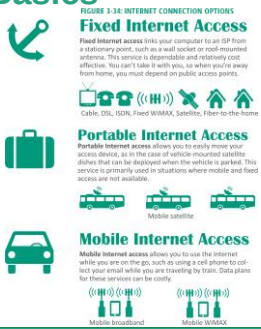


On a PC, from the Home screen, type com and choose the option for Command Prompt. Enter the command tracert followed by any domain name, like this:

3 Connection Basics

- Although public Internet access is available in many locations, such as coffee shops and libraries, most consumers like the convenience of having their own Internet connection

FIGURE 3-34: INTERNET CONNECTION OPTIONS



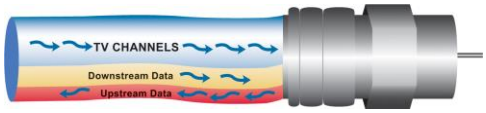
3 Cable Internet Service

- The gold standard of fixed Internet access is **cable Internet service**, which is offered by the same companies that supply cable television
- CATV stands for community antenna television
- With cables branching out from a central location, the topology of a CATV system works well as the infrastructure for a digital data network

3 Cable Internet Service

- CATV coaxial and fiber-optic cables have plenty of bandwidth to carry television signals for hundreds of channels in addition to digital data
- CATV cables provide bandwidth for television signals, incoming data signals, and outgoing data signals

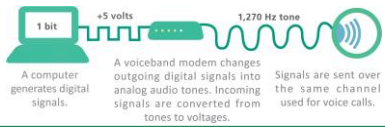
FIGURE 3-36: TV AND DATA STREAMS ON ONE CABLE



3 Telephone Network Internet Service

- Telephone companies offer four types of service: dial-up, ISDN, DSL, and FTTH
- A **dial-up** connection is a fixed Internet connection that uses a voiceband modem and the telephone company's circuit-switched network to transport data between your computer and your ISP
- A **voiceband modem** converts digital signals from a computer into audible analog signals that can travel over telephone lines

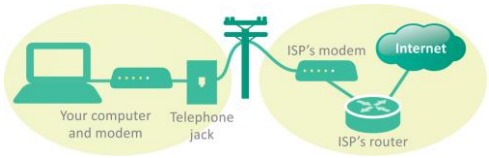
FIGURE 3-37: A VOICEBAND MODEM CHANGES VOLTAGES TO AUDIO TONES



3 Telephone Network Internet Service

- When you use a dial-up connection, a voiceband modem places a regular telephone call to your ISP; the circuit remains connected for the duration of the call to carry data between your computer and the ISP

FIGURE 3-38: DIAL-UP INFRASTRUCTURE



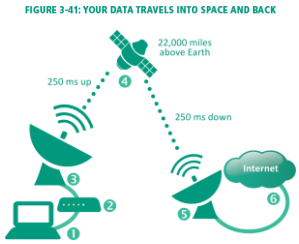
3 Telephone Network Internet Service

- **ISDN** stands for Integrated Services Digital Network; it divides a telephone line into two channels, one for data and one for voice, by using packet switching
- **DSL** (digital subscriber line) is a high-speed, digital, always-on, Internet access technology that runs over standard phone lines; it's offered by AT&T's U-verse service
- **FTTH** (fiber-to-the-home) is the use of high-capacity fiber-optic cables, rather than coaxial cables, to connect homes to broader municipal networks

3 Satellite Internet Service

- **Satellite Internet service** is a means of distributing broadband asymmetric Internet access by broadcasting signals to a satellite
- In many rural areas, satellite Internet service is the only alternative to a slow dial-up connection

FIGURE 3-41: YOUR DATA TRAVELS INTO SPACE AND BACK

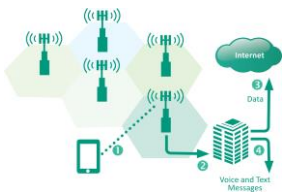


3 Mobile Broadband Service

- Mobile broadband service has become so compelling that most of the Web has undergone a visual makeover to fit the requirements of smartphone-sized screens

Cell networks transmit voice and data using radio signals; the signals flow between a device and a cellular radio tower (1), transmitters and receivers on each tower cover a specific area and use a unique frequency; data signals are passed to ground stations (2), where they are forwarded over a packet-switched network to the Internet (3); voice signals may be routed to a circuit-switched network (4)

FIGURE 3-42: FROM A CELL PHONE TO THE INTERNET



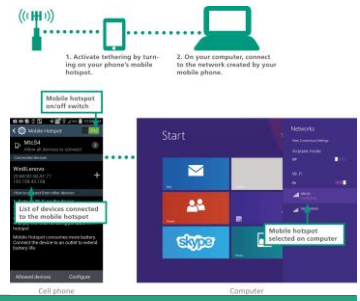
3 Mobile Broadband Service

- Mobile broadband has evolved through several generations; the most recent of these generations are 3G and 4G
  - **3G** (third generation) service was available in the U.S. beginning in 2001; common protocols include CDMA and GSM EDGE
  - **4G** (fourth generation) technologies, such as WiMAX and LTE, rolled out in 2011

3 Mobile Broadband Service

- Most of today's smartphones include a **tethering** feature that connects wirelessly with other digital devices
- Setting up tethering to create a mobile hotspot is easy, just remember though that data sent over the connection accumulates toward your monthly data usage total

FIGURE 3-43: CREATE A NETWORK WITH YOUR CELL PHONE



3 Wi-Fi Hotspots

- A Wi-Fi hotspot is a wireless local area network that offers Internet access to the public
- The network has an Internet connection and device called an access point that broadcasts Wi-Fi signals within a range of about 150 feet

3 Wi-Fi Hotspots

FIGURE 3-45: GAUGE YOUR RISK AT WI-FI HOTSPOTS

LOW **Browsing.** When using a Wi-Fi hotspot for simple browsing activities such as checking sports scores, reading Google news, and looking for directions, your security risk is fairly low if your computer's antivirus software is up to date.

LOW **Using secure sites.** Your security risk is low when you are accessing secured Web sites that have addresses beginning with HTTPS. These secured sites, which are used for activities such as online banking, accessing medical records, and making credit card purchases, encrypt the data that you enter to keep it safe from eavesdroppers.

MED **File sharing.** Eavesdroppers might be able to access the files on your computer if you have file sharing turned on. When using public networks, you should turn file sharing off. You can do so manually if your operating system does not offer that option when you connect.

HIGH **Using unsecured sites.** When you log in to unsecured sites while using public Wi-Fi hotspots, a wireless eavesdropper could potentially snag your user ID and password information, then use it later to access your accounts. Logging in to your Webmail account, for example, could be risky if your user ID and password are transmitted over an unsecured connection.

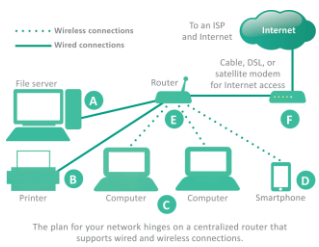
3 Section D: Local Area Networks

- LAN Basics
- Ethernet
- Wi-Fi
- Set Up Your Own Network
- Network Monitoring
- IoT Networks

3 LAN Basics

- Local area networks are often referred to as LANs
- They are designed to provide connectivity for devices within a limited area, typically within the premises of a home, office building, business, or school

FIGURE 3-47: BUILD THIS LAN



3 LAN Basics

- LANs can be classified by their protocols; Ethernet and Wi-Fi are the two most popular
- The Windows OS provides a tool for setting up a LAN called a **homegroup**; this makes it easy to share files among local computers, but does not provide Internet access
- Most LANs are set up using a router so that they have proper security and Internet access
- The circuitry that enables a device to access a LAN is called a **network interface controller** (NIC)
- NICs contain a **MAC address** (media access control address) used to identify devices on LANs

3 Ethernet

- Ethernet is a wired network technology that is defined by IEEE 802.3 standards
- Ethernet's success is attributable to several factors
  - **Easy** – it's easy to understand, implement, manage, and maintain
  - **Secure** – the wired connections in an Ethernet LAN are more secure than wireless LAN technologies
  - **Inexpensive** – as a nonproprietary technology, Ethernet equipment is available from a variety of vendors; market competition keeps prices low
  - **Flexible** – current Ethernet standards allow extensive flexibility in network configurations
  - **Compatible** – Ethernet is compatible with Wi-Fi wireless technology; it's easy to mix wired and wireless devices on a single network

3 Ethernet

- Ethernet was originally a bus topology in which computers were all strung along a cable like birds on a power line
- Today's Ethernet LANs are usually arranged in a star topology with computers wired to central switching circuitry that is incorporated in modern routers
- Data sent from a computer on the network is transmitted to the router, which then sends the data to the destination device

3 Ethernet

- Many computers have a built-in Ethernet port located on the system case; the port looks very similar to an oversized telephone jack
- If you want a wired network connection but your computer has no Ethernet port, you can purchase and install an **Ethernet adapter** (also called an Ethernet card)

FIGURE 3-51: DOES YOUR COMPUTER HAVE AN ETHERNET PORT?

FIGURE 3-52: ETHERNET ADAPTERS

Ethernet adapter for USB port

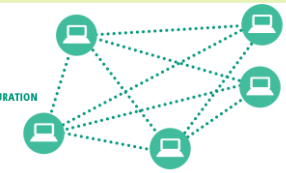
Ethernet adapter for expansion slot

3 Wi-Fi

- **Wi-Fi** refers to a set of wireless networking technologies defined by **IEEE 802.11** standards
- A Wi-Fi device transmits data as radio waves and is compatible with Ethernet, so you can use the two technologies in a single network
- You can set up Wi-Fi in two ways
  - Wireless mesh topology – devices broadcast directly to each other
  - Star topology – a centralized broadcasting device, a wireless access point, coordinates communication among network devices

3 Wi-Fi

FIGURE 3-53: WIRELESS MESH CONFIGURATION



Wireless ad-hoc networks are conceptually simple but provide few security safeguards. This type of connection is best limited to occasional use when you want to temporarily connect two computers to share a few files.

FIGURE 3-54: WIRELESS STAR CONFIGURATION

The most common wireless network technology uses a centralized device to handle data that travels from one device to another.

3 Set Up Your Own Network

- Having your own network is great, but LANs can be a security risk
- Here's how to set up your own safe and secure LAN:
  - Plug in the router and connect it to your Internet modem
  - Configure the router
  - Connect wired and wireless devices
  - Change the router password
  - Create an **SSID** (service set identifier); this will be the name of your wireless network
  - Continued…

3 Set Up Your Own Network

- Activate **wireless encryption** to scramble and unscramble data
  - **WEP** (wired equivalent privacy) is the oldest and weakest wireless encryption protocol
  - **WPA** (Wi-Fi Protected Access) and its cousins, WPA2 and PSK, offer more security
- Create a **wireless encryption key** (a network security key or password)
- Configure the **Guest Network** (a second network on your LAN's router)
- Activate **DHCP** (assigns addresses to each device that joins your network)

3 Network Monitoring

- When your network has stopped sending and receiving packets, you might be able to correct the problem by turning off your router and Internet modem, waiting a few seconds, and then turning them on again

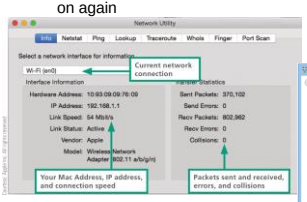


FIGURE 3-63: MAC NETWORK MONITORING

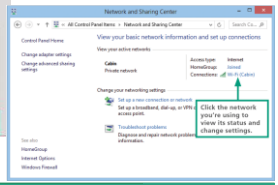


FIGURE 3-64: NETWORK AND SHARING CENTER

3 IoT Networks

- The Internet of Things (IoT) connects active sensors and passive tags to communications networks, making it easy to remotely monitor places and things
- Wi-Fi is fairly power hungry, so it's not an optimal IoT technology
- Existing wireless technologies such as **RFID** and **NFC** offer potential solutions
- Additional low-power short-range technologies developed specifically for IoT networks include **Bluetooth Smart**, **ZigBee**, and **Z-Wave**

3 IoT Networks

- A sensor, such as a thermometer or heart rate monitor, actively collects data
- A tag contains passive data; an RFID tag in a passport, for example, contains personal data, such as the name and birth date that are stored on the tag, which is read electronically
- An NFC tag might be attached to merchandise, so that you can tap it with your cell phone to see its price and specifications

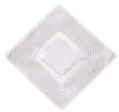


FIGURE 3-65: RFID AND NFC TAGS

3 Section E: File Sharing

- File Sharing Basics
- Accessing LAN Files
- Sharing Your Files
- Internet-based Sharing
- Torrents

3 File Sharing Basics

- File sharing allows files containing documents, photos, music, and more to be accessed from computers other than the one on which they are stored
- Sharing can take place within a LAN or across multiple networks, including the Internet

3 File Sharing Basics

- Your ability to share files with other devices on a network depends on several factors

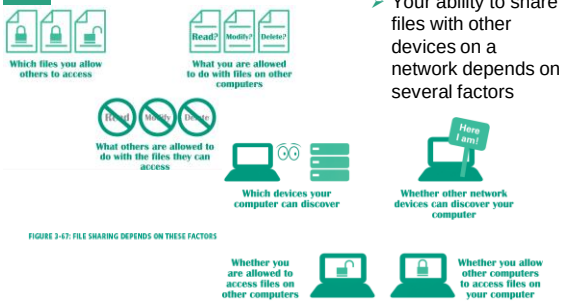
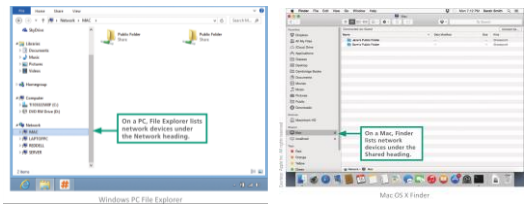


FIGURE 3-67: FILE SHARING DEPENDS ON THESE FACTORS

3 Accessing LAN Files

- To see a list of devices on your network, you can use your OS's file management utility, such or as Window's File Explorer or Mac OS X's Finder

FIGURE 3-68: FIND OTHER COMPUTERS ON A LAN



Windows PC File Explorer

Mac OS X Finder

3 Accessing LAN Files

- The network utilities provided by operating systems automatically detect other devices when network discovery is turned on
- **Network discovery** is a setting that affects whether your computer can see other devices on a network, and whether your computer can be seen by others; it works in different ways on different devices
  - Mobile devices – the OS may not offer a way to see other devices on a network
  - Macs – OS X devices have no user-modifiable network discovery settings; offers file sharing instead
  - Windows – Some OSs offer network discovery that allows users to turn it off or on

3 Sharing Your Files

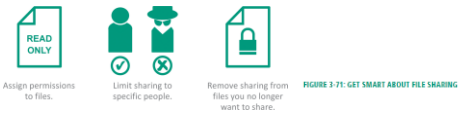


FIGURE 3-71: GET SMART ABOUT FILE SHARING

- **Permissions** specify how shared files can be used
  - Read and write permission – (full control) allows access for opening, viewing, modifying, and deleting files
  - Read permission – allows authorized people to open a file and view it, but not modify or delete it
  - Write-only permission – works like drop box, allowing people to put files in one of your folders, but not open, copy, or change any files you have stored there

3 Internet-Based Sharing

- **FTP** (File Transfer Protocol) provides a way to transfer files from one computer to another over any TCP/IP network, such as a LAN or the Internet
- You can access FTP servers with FTP client software, such as FileZilla, or with a browser
- Dropbox and similar **file hosting services** store files in the cloud

3 Torrents

- The concept of sharing files over the Internet, that started in the 1990s, spurred development of sophisticated, distributed protocols such as BitTorrent
- **BitTorrent** is a file sharing protocol that distributes the role of a file server across a collection of dispersed computers
- A BitTorrent network is designed to reduce the bandwidth bottleneck that occurs when many people attempt to download the same very large file, such as a feature-length film, or interactive 3-D computer game

3 Torrents

- **How a BitTorrent works**:
  - A BitTorrent network server breaks a movie file into pieces and begins to download those pieces to the first computer that requested the movie
  - As more computers request the file, they become part of a "swarm" that uses peer-to-peer technology to exchange movie segments with each other
  - After the server has downloaded all the segments to the swarm, its job is complete and it can service other requests
    - Cont…

3 Torrents

- The swarm continues to exchange movie segments until every computer in the swarm has the entire movie

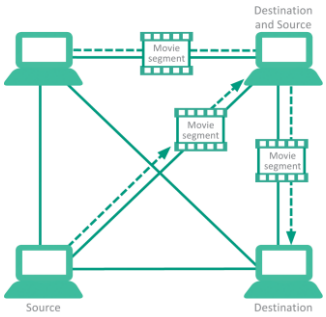


FIGURE 3-76: TORRENT PEERING FOR FILE SHARING

Every user who downloads from a torrent is automatically uploading to other users.

NEW PERSPECTIVES

Unit 3 Complete

Computer Concepts 2016