

Module 7

Introduction



"P7300543" by indrora is licensed under CC BY 2.0

Telecommunications refers to the electronic transmission and reception of signals for voice and data communications.

Telecommunications (telecom) networks play a vital role in our daily activities. From the global telecom networks that make up the Internet, to short-range wireless technologies that pass data back and forth between a mobile phone and an automobile's media system, telecommunications technologies keep people and devices continuously connected.

Today, more than 72% of U.S. citizens own a smartphone. Statistics are similar in many developed nations around the world. A recent Pew survey found that smartphone ownership rates in emerging and developing nations are rising at an extraordinary rate, climbing from a median of 21% in 2013 to 37% in 2015. The survey concludes that overwhelming majorities in almost every nation surveyed report owning some form of mobile device, even if they are not considered "smartphones."

Smartphone and tablet popularity, combined with growing cellular and Wi-Fi network availability, is creating an environment where people are no longer bound to desks or any particular location to do work and be productive. Laptop, tablet, and smartphone sales are skyrocketing while PC sales are tanking. Mobile apps, GPS, and easy access to information further support and even encourage a mobile workforce and lifestyle.

What is gained, in terms of productivity and job satisfaction, by the ability to be mobile? Is anything lost? How does mobility impact professionals in careers that interest you?

Telecommunications technologies affect our lives in many ways every day. Telecommunications technologies produced the Internet and the many ways of accessing it. These methods include wired connections through Internet service providers and wireless connections through a variety of technologies. Telecommunications technologies provide voice, video, text, and other forms of communications to a wide variety of clients worldwide, from individuals to corporate offices. From small home networks to large private global networks, telecommunications technologies give us access to public and private information, communication, and services wherever we may be, whenever we need them. This section begins by presenting the fundamental technologies that support all types of telecommunications networks. It then progresses to focus on cellular network technologies and wireless data communications.

Today, nearly all of our communication and information access is accomplished through telecommunications systems: cellular networks, Wi-Fi networks, corporate networks, metropolitan area networks, cellular networks, and of course, the Internet. The companies or entities that control these networks have tremendous responsibility and power. They control who can access information. They also control what information can travel over their networks. Issues of censorship and privacy have arisen when network providers have filtered data that flows over their networks. Internet service providers can block users who download movies from illegal sources, and cellular providers can collect confidential user information from mobile phones, including location information. Ethical issues arise

when network providers offer services only to densely populated areas in order to maximize profits, creating a digital divide.

Today, more than ever before, information is power. In order to provide information access equally to all people, governments often step in to provide incentives and regulate how telecom companies behave. Do you think this is wise? Should the market alone drive what telecom companies do? How much, if any, government intervention is required, and in what form? In their efforts to fight crime and terrorism, governments and law enforcement agencies have been known to ask telecom companies for confidential information about customers. Should government access to network information be regulated?

Lesson 7.1: Telecommunications

Lesson 7.1 Introduction



"caged sky" by mh.xbhd.org is licensed under CC BY 2.0

In telecommunications, **infrastructure** refers to the hardware, software, and protocols that support telecommunications.

Both voice and data communications have become an important part of our daily lives. Understanding the hardware, software, and protocols that support this useful technology can help you select telecommunications services that are best suited to your needs.

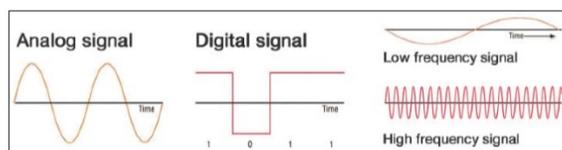
As with all forms of communications, telecommunications requires a sender, a receiver, a signal that contains information, and a medium over which the signal travels. For telecommunications to function as intended, both the sending device and the receiving device need to speak the same language. The rules that define the language of telecommunications are called protocols. Telecommunications media, such as cables and the air, carry the mostly digital signals that represent the information being sent. Telecommunications devices, such as mobile phones, routers, network adapters, Wi-Fi access points, cellular towers, and satellites, send and receive the signals, employing telecommunications software that governs their operations. Various combinations of devices, media, software, and protocols can provide varying qualities of service. This section looks at the most important components of telecommunications infrastructure and the effects they have on the quality of communications.

Reading: Telecommunications Signals

Telecommunications signals are analog or digital electronic transmissions for the purpose of communication.

Why This Matters

Companies go to great lengths to send telecommunications signals to every corner of the globe. The signals used to send information over voice and data networks can vary in speed and strength. Understanding how the speed and strength of signals impact a network's performance can help you when choosing and using network services.



Authored by: Cengage Learning License: Creative Commons Attribution 4.0 International (CC BY 4.0)

Essential Information

If you were to measure the voltage on an old-fashioned home telephone wire during a phone conversation, you would see fluctuations in voltages similar to the signal shown on the left in the figure. This type of signal is called an analog signal, and it fluctuates continuously, creating a curved waveform. Originally, many types of telecommunication, such as phones and radios, were based on analog systems because they were designed to carry the sound of a voice, and sound waves are analog signals. Today, even signals like voice that traditionally were analog are being digitized and sent using digital technology, using the same technology that computers use to communicate.

In contrast to analog systems, if you measure the voltage on network cables used to connect PCs, you will probably see something comparable to the signal in the middle of the figure. This signal, at any given time, is either high or low. This type of discrete voltage state—either high or low—is called a digital signal and has a box-like waveform. The two states are used to represent the state of a bit: high for 1 and low for 0. Digital signals are designed to carry computer data, which is digitally represented as bits.

The speed at which an electronic communications signal can change from high to low is called the signal frequency, illustrated in the figure on the right. A faster frequency means a faster data transmission rate. Signal frequency is measured in hertz (Hz), or cycles per second. In computer networks, the data transmission rate is also referred to as the bandwidth and is measured in bits per second (bps). Today's bandwidth options fall into one of two categories: narrowband or broadband.

Broadband media are those advertised by Internet service providers as “high-speed.” In home use, the terms broadband and high-speed Internet refer to a connection providing download speeds of 6 Mbps (megabits per second) up to over 100 Mbps. New 4G cellular technologies are bringing similar speeds to cellular networks. For most areas, broadband has become the norm for business, home, and mobile use. Some cities, such as Kansas City and Austin, have access to fiber networks such as those installed by Google, AT&T, and Verizon. These cities enjoy “gigabit Internet speeds” of over 1 Gbps—hundreds of times faster than typical broadband. Some rural areas, however, are still bound by the limits of old technologies that measure speed in kilobits per second rather than megabits per second. Narrowband is considered any medium with speeds in the Kbps range. With the efforts by governments to bring high-speed networking to all, narrowband connections are a shrinking minority.

Reading: Telecommunications Media

Telecommunications media include anything that carries a signal and creates an interface between a sending device and a receiving device.



"CABLE REELS" by kunst.ff is licensed under CC BY 2.0

Why This Matters

Various types of media are used for telecommunications networks. Each medium has its own characteristics, including transmission capacity, speed, convenience, and security. When developing a network, the selection of media depends on the environment and use of the network. Media should support the needs of the network users in a given environment at the least cost, taking into account possible future needs of the network. Using the wrong type of media can reduce productivity or waste money.

Essential Information

Different communications media connect systems in different ways. Some media send signals with low voltage or light along physical connections such as cables, but others send signals through the air using radio waves.

Different physical cables offer a bandwidth range from narrowband to broadband. Cables have an advantage over wireless options because some cables support much higher data transfer rates than wireless technologies and are considered by some to be more secure. The disadvantage of cables is their physical presence. Cables need to be installed, typically in an inconspicuous manner. They are run underground, undersea, and through utility tunnels; strung from pole to pole through attics and basements and above ceiling tiles; pulled down inside walls, through walls, and around the interior of a room. Depending on the environment, laying cable can take a considerable amount of time and effort. Three types of transmission cables are typically used to connect data communications devices: twisted pair copper cable, coaxial cable, and fiber-optic cable (see table below).

Types of Cable

Cable	Description
Twisted pair	Pairs of twisted wires covered with an insulating layer, used for telephone and computer networks. Available in varying categories ("cats") to support a wide range of bandwidths.
Coaxial	An inner conductor wire surrounded by insulation, a conductive shield, and a cover used for cable TV and other applications. Supports faster data speeds, but is more expensive than twisted pair.
Fiber-optic	Consists of thousands of extremely thin strands of glass or plastic bound together in a sheathing (a jacket); transmits signals with light beams. Much faster than coaxial and twisted pair, but also much more expensive. Used for backbones of telecom networks and in some wide area and local area networks.

Telecommunications signals can also travel through air using radio waves. A radio wave is an electromagnetic wave transmitted through an antenna. All wireless telecommunications—cell phones,

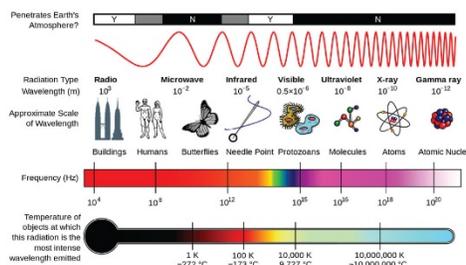
wireless Internet, AM and FM radio—make use of radio waves designated to certain frequencies. The radio spectrum is divided up by government agencies for various uses on various frequencies. In the United States, the FCC (Federal Communications Commission) oversees the radio spectrum.

Reading: Radio Spectrum

Radio spectrum, part of the electromagnetic spectrum, refers to all of the frequencies available for radio waves from about 10 KHz to 300 GHz and their assigned uses.

Why This Matters

The U.S. Federal Communications Commission (FCC) assigns different frequencies of the electromagnetic spectrum for different uses in the United States. For example, FM radio, cell phones, baby monitors, and garage door openers all operate at different radio frequencies. If these devices were on the same frequency, they would cause interference for each other, and your cell phone conversation might trigger your garage door to open. The figure, courtesy of NASA, illustrates some attributes of the seven types of waves and rays in the electromagnetic spectrum. To show all frequency assignments would take a chart several feet tall. Such a chart is available in the On the Web links below. The radio spectrum allows for many different uses of radio signals and attempts to safeguard those uses from interference.



Source: Courtesy of NASA Attribution: Public Domain

Essential Information

Thousands of radio waves are passing through the air and your body as you read this. AM and FM radio waves, television, wireless phones, wireless computer networks, global positioning systems, ham radios, CB radios, police and emergency communications, and satellite communications all make use of radio waves. All it takes to receive the information being transmitted on a specific frequency is a device with an antenna that allows you to tune in to that frequency. For example, when you tune your car radio to 98.9 FM, you are selecting the signal being broadcast at 98.9 MHz, and your receiver translates the fluctuations of the radio waves it receives into sound.

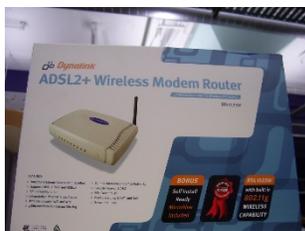
Some wireless applications require very little bandwidth. For example, AM radio requires a relatively low bandwidth to carry its low-quality mono audio signal in the low KHz range. FM radio provides a higher quality, stereo audio signal in the low MHz range. The mid MHz range is ideal for high-speed wireless Internet and cell phone use.

Waves sent at the high end of the radio spectrum, between 1 and 300 GHz, are called microwaves. These high-frequency waves have numerous uses. As you may have guessed, microwave ovens use microwaves (2.45 GHz) to cook food. Microwave signals are also used for high-speed, high-capacity communication links and satellite communications.

Above microwaves in the spectrum comes infrared light, used to send signals from television remote controls, and then visible light, ultraviolet light, x-rays, and gamma rays, none of which are commonly used to carry telecommunications signals.

Reading: Telecommunications Device

Telecommunications devices include the wide variety of computer hardware designed to support telecommunications activities for individuals and businesses.



"Waiting for Telstra" by Lachlan Hardy is licensed under CC BY 2.0

Why This Matters

Not long ago, networking devices were of interest only to network technicians. Today, the increase in home networking and wireless networks has provided a reason for everyone to acquire a basic understanding of the most common networking devices, such as modems, network adapters, access points, and others.

Essential Information

Telecommunications devices range in size and purpose from small Mi-Fi wireless adapters that fit in the palm of your hand and share a cellular connection with a computer, to satellites that manage data communications for thousands of users. A modem is a device that modulates and demodulates signals from one form to another, typically for the purpose of connecting to the Internet. The following table shows the various devices that enable computers to connect to networks and the Internet.

Network Connection Devices

Device	Description
Dial-up modem	Provides narrowband Internet connections over phone lines
Cable modem	Provides Internet access to PCs and computer networks over a cable television network
DSL modem	Similar to a cable modem but provides high-speed Internet service over telephone lines
Network adapter	A computer circuit board, PC card, or USB device installed in a computer so that the computer can be connected to a network
Network interface card (NIC)	A circuit board or PC card that, when installed, provides a port for the device to connect to a wired network with traditional network cables
Wireless adapter	A circuit board, PC card, or an external device that connects through an antenna-equipped USB port that is able to send and receive network radio signals
Cellular devices	Cellular network carriers provide several options for connecting computers to the Internet. Cellular connect cards are USB devices that connect a laptop to the Internet through a cellular data plan. Some carriers allow users to "tether" or wirelessly connect computers to mobile phones to access the Internet. Mi-Fi routers, also referred to as personal Wi-Fi hotspots, are palm-size devices that wirelessly connect computers to the Internet through a mobile phone's data service using Wi-Fi technology.

For multiple computers to communicate over a computer network, special devices are required to control the flow of bits over the telecommunications medium and to ensure that information that is sent reaches its destination quickly and securely. A number of different network control devices handle this responsibility. The table below provides brief descriptions of those that are most commonly used.

Network Control Devices

Device	Description
Hub	A small electronic box used as a central point for connecting a series of computers; sends the signal from each computer to all the other computers on the network. Hubs have largely been replaced by switches in today's networks.
Switch	A fundamental part of most networks; a switch makes it possible for several users to send information over a network at the same time. Switches direct signals to the intended recipient only.
Repeater	Connects multiple network segments; listens to each segment and repeats the signal heard on one segment onto every other segment connected to the repeater. Repeaters are helpful in situations where a weak signal requires a boost to continue on the medium.
Bridge	Connects two or more network segments, as a repeater does; a bridge also helps to regulate network traffic.
Gateway	A network point that acts as an entrance to another network.
Router	Determines the best path for passing a data packet between networks to its destination.
Wireless access point	Typically a Wi-Fi device, connected to a wired or cellular network to send and receive data to wireless adapters installed in computers and other devices; it allows devices to connect to a network wirelessly.
Firewall	Device or software that filters the information coming onto a network; it protects the network computers from hackers, viruses, and other unwanted network traffic. Many routers include firewall capabilities.

Large corporations and telecommunications companies require expensive, heavy-duty devices to manage large amounts of network data, often using microwave or satellite transmission.

Microwave transmission, also called terrestrial microwave, is a line-of-sight medium, which means that a straight line between the transmitter and receiver must be unobstructed. Microwave transmissions can be sent through the air up to distances of approximately 31 miles (50 kilometers). Microwave towers are placed along interstate highways and other unobstructed stretches to carry thousands of simultaneous communications channels.

In areas where microwave towers are impractical, or in order to send data long distances, communications satellites are employed. A communications satellite is basically a microwave station placed in outer space. Satellites receive a signal from one point on earth and then rebroadcast it at a different frequency to a different location. Most of today's satellites are owned by telecommunications companies that rent or lease them to other companies. However, several large companies have their own satellites.

Television news organizations make use of small mobile satellite systems mounted on trucks that allow them to broadcast from remote locations. Some companies lease dedicated lines from telecommunications companies to maintain long-distance connections. A T1 line supports high data transmission rates by carrying 24 signals (64 Kbps) on one line. T3 lines carry 672 signals on one line and are used by telecommunications companies; some act as the Internet backbone.

Reading: Telecommunications Software

Telecommunications software is software based on telecommunications protocols used to control, monitor, and troubleshoot data traveling over a telecommunications network.

Why This Matters

As you have no doubt learned, hardware is useless without the software necessary to drive it—and so it is with telecommunications networks. Networking software performs a number of important functions in a computer network. It monitors the load, or amount of traffic, on the network to ensure that users' needs are being met. It provides error checking and message formatting. In some cases, when there is a problem, the software can indicate what is wrong and suggest possible solutions. Networking software can also provide data information security and privacy.



Source: Apple Inc. Attribution: Fair Use

Essential Information

Telecommunications companies have many custom-designed software utilities that they use to manage the flow of data over their networks. These industrial-strength applications are the domain of the professionals that use them. This section focuses on software used in private computer networks, and leaves the industrial systems to the professionals.

Servers that manage the data flowing over networks and the Internet use operating systems created specifically for the task, sometimes called network operating systems (NOS). Network operating systems are responsible for creating data packets to send over a network; sending those packets; and receiving packets sent from other computers, or nodes, on the network. Today's PC and mobile operating systems include networking features.

Network management software allows system administrators to monitor the use of individual computers and shared hardware (such as printers), scan for viruses, and ensure compliance with software licenses. Network management software also simplifies the process of updating files and programs on network computers. Changes can be made through a communications server instead of on each individual computer. Some of the many benefits of network management software include fewer hours spent on routine tasks (such as installing new software), faster responses to problems, and greater overall network control.

Network management software isn't only for administrators. Many smartphones also have the capability to provide diagnostics, such as providing data usage information and allowing the user to set an alarm to sound when the phone is nearing its monthly data limit. This helps users avoid penalties for going over their limit.

Routers, switches, firewalls, modems, and other telecommunications devices include software interfaces that allow you to change device settings. Once the device is connected to the network, its software interface can be accessed from a network computer. A wireless access point's software can be accessed to change security settings so that unauthorized users cannot access the network. The

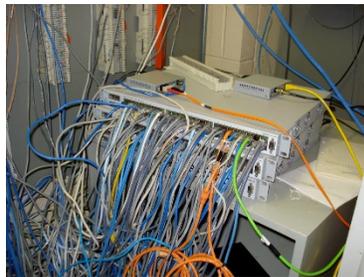
image on this page shows an Apple Airport setup utility; this is where users can configure a host of settings. A router's software can be used to divide a physical network into multiple virtual networks. A firewall's software can be used to specify which data packets to allow in and which to keep out.

A protocol is an agreed-upon format for transmitting data between two devices. A standard is an agreed-upon way of doing something within an industry. In the world of networking, protocols and standards are essential for enabling devices to communicate with each other. Protocols define the format of the communications between devices, and standards provide the physical specifications of devices and how they interconnect. The Internet uses the TCP/IP family of protocols. They have become the default protocols for most private networks as well.

Ethernet is the most widely used network standard for private networks. This standard defines the types of network interface cards, control devices, cables, and software required to create an Ethernet network. Other network standards, such as token ring, use unique hardware and software that are not compatible with Ethernet. Special devices such as routers or gateways are required to connect networks that use different standards.

Reading: Telecommunications Networks

Telecommunications networks include computing and/or communications devices connected together for communications, information, and resource sharing.



"DSC00366.JPG" by dcmorton is licensed under CC BY 2.0

Why This Matters

Telecommunications networks connect people and devices. When they are used for connecting computers, they may be referred to as computer networks. But whether they are used for communicating or computing, they use the same fundamental digital technologies and allow people to communicate and share information and resources within homes, organizations, and around the world. These networks have become an essential component in managing and organizing many facets of our professional and personal lives.

Essential Information

Within a computer network, computing resources are shared in order to maximize computing power and organizational effectiveness. You have learned that a computer includes devices for input, processing, storage, and output. These components can be distributed throughout a computer network. This is referred to as a distributed network. For instance, you may connect to your corporate network through a Wi-Fi connection and work on a server shared by all employees in the organization. In such a scenario, your computer provides the input and output devices, but the processing and storage may be handled at some other location. You may store your files on a network drive that exists on a file server and send your print jobs to a printer in a shared area of your office. A computing system may be distributed over components in one small office building or around the world on a network operated by a global corporation.

Networks are classified by size in terms of the number of users they serve and the geographic area they cover. From a network that links two personal devices that serve an individual user, to international enterprise networks that serve large corporations, to the Internet, which serves the entire world, different types of networks are uniquely designed to accommodate specific needs. Types of networks include local area networks, virtual private networks, metropolitan area networks, wide area networks, and global networks. Networks utilize security features to control and monitor access.

A local area network (LAN) is a privately-owned computer network that connects computers and devices within the same building or local geographic area. Home networks, campus networks, and office networks fall into this category. Local area networks can include personal computers, servers, printers, and other network-capable devices. Devices connect to LANs through network interface cards or wireless network adapters. Larger networks use servers to store databases, files, and software.

LANs that are designed to serve an entire city are called metropolitan area networks or MANs. Sometimes they are referred to as municipal or muni networks. A virtual private network (VPN) uses a technique called tunneling to securely send private LAN data over the Internet. A VPN may be used to connect an organization's networks dispersed around the world into a single wide area network.

A wide area network (WAN) connects LANs between cities, across countries, and around the world using microwave and satellite transmission or telephone lines. When you make a long-distance phone call, you are using a wide area network. AT&T, Verizon, Sprint, and other telecommunications companies are examples of companies that offer WAN services. Companies, organizations, and government agencies also design and implement WANs for private use.

Provided by the SeaWiFS Project, NASA/Goddard Space Flight Center, and ORBIMAGE (lines added)
A WAN that crosses an international border is considered a global or international network. The Internet is the most obvious global network, but as an increasing number of businesses enter global markets, private global networks are becoming more prevalent.

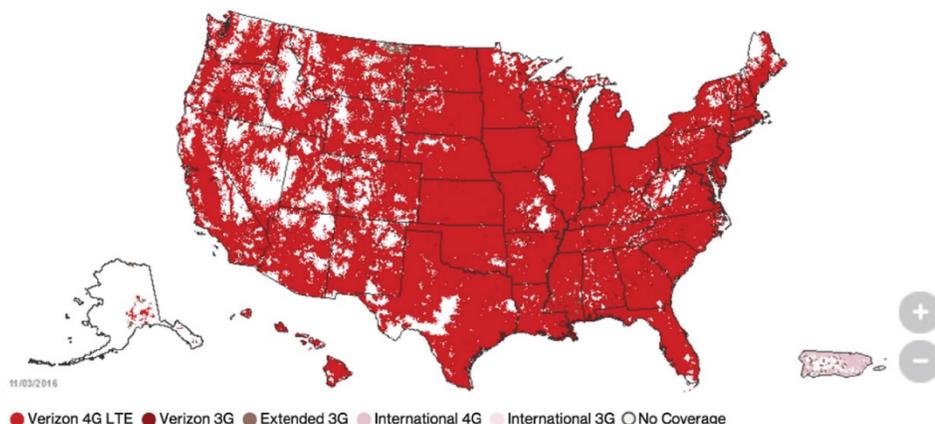
Networks require a significant amount of work to create and maintain. A network administrator, sometimes called a system administrator, is a person responsible for setting up, maintaining and securing the network, implementing network policies, and assigning user access permissions. A large organization might employ dozens of network administrators. In a small business, the business owner may take the role of network administrator. Even home networks have a network administrator—usually a family member that takes responsibility for setting up and maintaining the network.

Lesson 7.2: Cellular Networks

Lesson 7.2 Introduction

A **cellular network** is a wide area network in which a geographic area is divided into cells, with a transceiver antenna (tower) and station at the center of each cell, to support wireless mobile communications.

Cellular network technologies have altered the way people live. Originally designed to support only voice communications, cellular technology has progressed to support data communications over the Internet. Today, more people access the Internet on cellular phones than any other type of computing device. Mobile technologies allow people to work more efficiently and flexibly. Cell phones have become a necessity in many cultures. To gain the most benefits from cellular technology, it helps to understand how the technology works and what services it provides.



Source: Courtesy of 2015 Verizon Wireless Attribution: Fair Use

A cellular network is composed of many different technologies and devices. The challenge in supporting ubiquitous mobile communications is to find a method of sending and receiving telecommunications signals from devices that have a limited signal range. The solution that cellular networks provide is to cover a geographic area with many cellular towers dispersed in a honeycomb of cells, each roughly 7 miles (11 kilometers) across, so that wherever a device is within the area, it can connect with a tower. If a cell phone user travels from one cell to another, the system judges the cell phone’s location based on its signal strength and passes the phone connection from one cell tower to the next. The signals from the cells are transmitted to a receiver and integrated into the regular phone system.

Each cell tower has a transmitting and receiving range of 3–15 miles (about 5–24 kilometers) depending on geography and environment. Because it is not economically feasible to cover the entire planet with towers, cell phone usage is limited to a network’s coverage areas (see figure), which often focus on metropolitan areas and major highways. The inability to provide 100% coverage, combined with the limitations of working with wireless signals that are prone to interference, results in less-than-perfect quality of service for cell phone users. However, the quality and coverage continue to improve as cellular companies continue investing money in improving their networks.

Cell phone technologies have progressed through four generations of technologies (see table). Long Term Evolution (LTE) is a fourth-generation wireless broadband technology that provides high-speed Internet access over smartphones. LTE is being marketed by all of the popular cellular carriers as the fastest network speeds available. However, others are already experimenting with fifth-generation technologies that will provide data transfer rates up to a gigabit per second. It’s expected that 5G will be rolling out around 2020.

Cell Phone Generations

Generation	Defining Characteristics
1st	The original analog cell phone network
2nd	Digital cell phone service
3rd	First generation to deliver Internet connections to the mobile phone. Technologies such as EDGE provided still painfully slow speeds between 2 Mbps upwards to dozens of Mbps.
4th	Typically, LTE technology delivering broadband data rates in the dozens to hundreds of Mbps range
5th	Still in development, these technologies hope to provide gigabit per second speeds.

Selecting a cell phone service is no small task. The variables involved in the decision are many and complex. When you choose a cell phone service, there are three primary decisions to make:

- Choosing a carrier
- Choosing a plan
- Choosing the device, features, and services that you want

These decisions are interdependent. Each carrier offers different mobile phones and devices, and cellular services are related to device capabilities. There are two different strategies for selecting a cellular carrier. You can choose a phone or tablet first and then find out which carriers support it, or you can choose a carrier first and then choose one of the devices that the carrier supports. If you know of a phone or tablet that you simply must have, then the first strategy is for you. If you have a strong inclination for a specific carrier—for example, the carrier that Consumer Reports rates number one, or that your family and friends all use, or that you know has excellent coverage where you will be using the service—then the second strategy is for you. This section covers topics that will assist you in selecting a cellular carrier, plan, and device.

Reading: Cellular Carrier

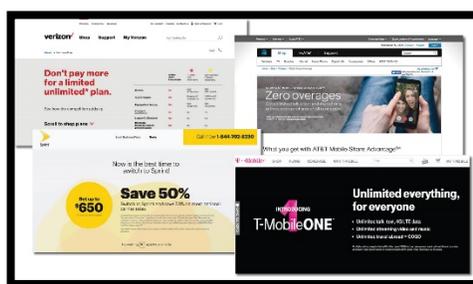
A **cellular carrier** is a company that builds and maintains a cellular network and provides cell phone service to the public.

Why This Matters

Choosing a carrier is an important step in the process of acquiring cell phone service. Since carriers require a two-year contract or provide two-year financing on phones, it becomes difficult and costly to switch if you find you've made a bad choice.

Essential Information

Many carriers provide cell phone service worldwide. The most popular U.S. carriers are Verizon and AT&T, with T-Mobile and Sprint following. Different carriers offer different cell phones, features, coverage areas, and services. It is important to take your time when selecting a carrier as your choice will define your cell phone experience. It is typically costly and inconvenient to change your carrier once you've signed a contract.



Source: Verizon, AT&T, Sprint, and T-Mobile Attribution: Fair Use

Today's cell phone networks are all digital. The predominant digital networking standards for cell phone networks are GSM and CDMA. Global System for Mobile Communications (GSM) is the most popular international standard for mobile phones, used by over a billion people across more than 200 countries. AT&T, T-Mobile, and most international carriers use GSM. The Code Division Multiple Access (CDMA) networking standard is used in the United States, where it is in equal competition with GSM. Sprint and other smaller U.S. carriers use CDMA. Gradually, all carriers are moving to LTE 4G standards.

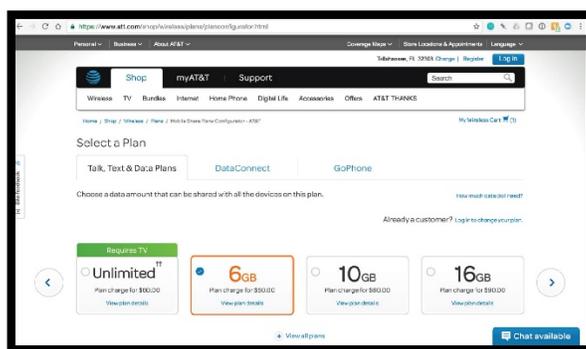
When choosing a carrier, it is useful to consult user survey data, such as that provided by Consumer Reports, as well as the opinions of friends. Check the coverage maps provided by the carriers' websites to make sure that they offer the network speed you require (3G or 4G) in the areas where you live and work. Finally, compare the carriers' network standards (GSM, CDMA, LTE), phones, rates, and plans to find out which best suit your needs in your location. Often, the hottest new models of phones launch only on one carrier. For example, Google's Pixel phone started out only on Verizon (see video), but gradually moved to the other carriers.

Reading: Cellular Plans

A **cellular plan** defines the terms of service provided by a cellular carrier to which a cellular user subscribes.

Why This Matters

Cellular carriers offer service plans for every type of phone and cell network-enabled tablet user. The trick is determining your usage habits and needs. For example, how much data do you think you will download over your phone each month? What carrier do your friends and family use? How many text messages do you send each month? Would you be interested in a package deal that includes television, home Internet, home phone, and cellular?



Source: Courtesy of AT&T Attribution: Fair Use

Essential Information

Most carriers have moved away from annual contracts that required customers to commit to the contract for two years in exchange for deeply discounted phones. Today, it's all about the data. Almost all plans purchased today include talk, text, and data. Oftentimes, talk and text have no limits, but depending on how much you pay, your data access may be limited. For example, AT&T charges \$60 per month for a plan that provides up to 6 GB of data. Although some carriers charge extra for going over your data quota, most of them now just throttle your connection speed way down when you hit your limit.

Phones can be purchased either by paying the full cost of the phone up front or through payment plans provided by the carrier. The payment plans serve a similar purpose as the old two-year contracts in that they keep customers obligated to the carrier until the phone is paid off.

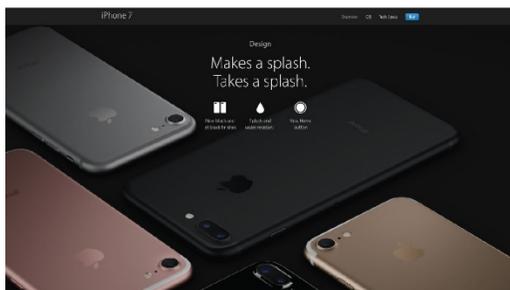
Additional lines can be added to an account at a significantly discounted price. For example, a 4 GB plan might cost around \$100 per month. Adding a second 4 GB line to the account might only add \$20 per month. Additional lines may be used for additional phones for family members or perhaps for an additional device like a tablet for yourself. If you are buying top-of-the-line phones, you can count on paying around \$25 per month per phone for two years. In this manner, a family of four could easily end up paying over \$300 per month for cellular phones and service.

Reading: Cellular Phone

Mobile phone refers to the handset used by the subscriber to communicate on a cellular network.

Why This Matters

Advances in mobile phones have been fast and furious in recent years with manufacturers such as Microsoft/Nokia, Samsung, Motorola, Pantech, Kyocera, LG, Sony, HTC, and Apple competing intensely to gain an edge in the largest technology market. Smartphone handsets range in price from less than \$100 to more than \$700 for the latest and greatest smartphones. Determining which phone best suits your needs requires some time and consideration. The biggest decision for most users is whether to choose Apple's iPhone platform or one of the many Android-based phones. The most successful phone manufacturers are Apple, which offers the iPhone, and Samsung, which offers the Galaxy-model phones running Android.



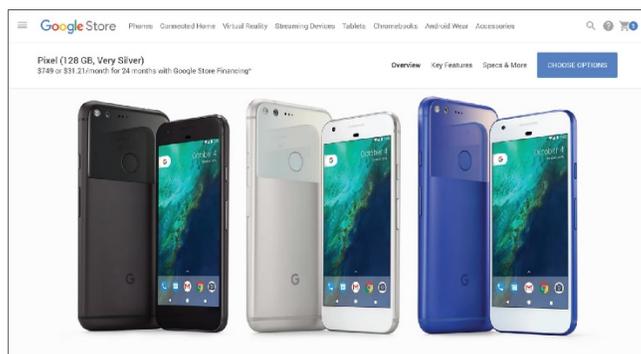
Source: Source: Apple Inc. Attribution: Fair Use

Essential Information

A mobile phone can be designed primarily for voice communication, in which case it is referred to simply as a cell phone; or it may be designed to support voice and Internet, in which case it is referred to as a smartphone.

Smartphones use a “soft” keyboard—a keyboard displayed on the touchscreen—and predictive text technology to assist with typing text. As you type, the phone guesses what word you are typing and offers to complete the word for you or to correct your spelling. Increasingly, people are dictating text into their smartphones where personal digital assistants either carry out commands or enter the text into apps.

Phones are selected by display size, network type (GSM, CDMA, 4G/LTE), processor type, features, and storage size. While smartphones are coming down in price, the real cost is in the data plan required to provide Internet access to the handset. A good smartphone will probably cost at least \$500, while the data plan to support it will add up to well over that amount over a two-year period.



Source: Courtesy of Google Attribution: Fair Use

After selecting a carrier, plan, and phone, you may wish to select cell phone accessories, such as insurance for your phone, a case to protect your phone, a car charger, or a headset or earbuds for hands-free phoning. Some U.S. states have made hands-free headsets a requirement for using cell phones while driving to help prevent distracted driving.

Lesson 7.3: Wireless Networking

Lesson 7.3 Introduction



"Laptop and working lunch. An outside table with a silver laptop, coffee and a sandwich on it." by Rob Pearce is licensed under CC BY 2.0

Wireless data communications refers to telecommunications that take place over the air to provide data and Internet access.

Access to information anywhere, anytime has been a dream for many technology enthusiasts—a dream that has become a reality. Many wireless technologies are available for accessing data and information from various locations. Those who understand those technologies can lead more productive lives.

Many wireless technologies are used to access different types of data and information from various environments. Some, like GPS, have very specific functions. Others, such as Wi-Fi and Bluetooth, have become standards used by many every day for a variety of purposes. Combined, these wireless technologies are transforming our lives by making communication and access to information effortless from any place at any time. This section covers the most useful wireless data technologies available today.

Reading: Wi-Fi

Wi-Fi (short for wireless fidelity) is wireless networking technology that uses access points to wirelessly connect users to networks within a range of 250–1,000 feet (75–300 meters).

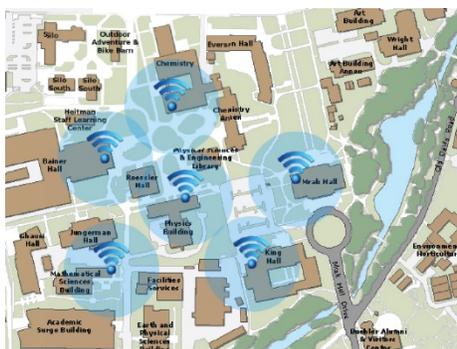
Why This Matters

Wi-Fi is the dominant technology that provides wireless Internet access in households, businesses, and public spaces. It provides certain benefits, such as high-speed Internet access, and suffers from some limitations, such as its relatively short range and its inability to support large numbers of users. Understanding Wi-Fi enables users to make the best use of the technology and make wise decisions when choosing an Internet service provider.

Essential Information

The Wi-Fi standards, also known as the 802.11 family of standards, were developed by the Institute of Electrical and Electronics Engineers (IEEE) to support wireless computer networking within a limited range at broadband speeds. There have been several versions of Wi-Fi, each increasingly more powerful. 802.11b provided 11 Mbps while 802.11g increased to 54 Mbps. 802.11n, the current popular version, is up to 600 Mbps. A number of other versions exist to address special purposes and increase

throughput and efficiency. The most recent version in development, 802.11ay, has a peak transmission rate of 20 Gbit/s. Each new version of 802.11 is backward compatible with the previous version, but needs to be connected to devices of the same version to enjoy the faster speed.



Source: Courtesy of University of California, Davis Attribution: Fair Use

Wi-Fi technology uses wireless access points that send and receive data using radio frequencies to and from computers and other digital devices equipped with Wi-Fi cards or adapters. Access points are connected to networks (via network cable) that are typically connected to the Internet. So, when connecting to an access point, a wireless user also connects to a local area network and the Internet. 802.11n Wi-Fi has a maximum range of about 820 feet (250 meters) in open areas and 230 feet (70 meters) in closed areas. Areas around access points where users can connect to the Internet are sometimes called hotspots. By positioning wireless access points at strategic locations throughout a building, campus, or city, Wi-Fi users can be continuously connected to the network and Internet, no matter where they roam on the premises. Wi-Fi is popular for businesses like Starbucks and McDonald's as well as for home networks. Wi-Fi is even available in aircraft for connecting to the Internet while in flight. The aircraft connects to the Internet via satellite or ground-based towers and then shares the connection with passengers using Wi-Fi. While free public Wi-Fi is a great convenience, there are also increased risks from hackers.

Setting up a home Wi-Fi network requires an Internet connection (typically provided by cable TV line or phone line) and a Wi-Fi router or access point. Routers are often provided by the Internet service provider, but cost around \$100 if you need to purchase your own. Routers often advertise a dual-band feature, which means they support two kinds of connections—5 GHz and 2.4 GHz—allowing for multiple devices to be supported simultaneously without slowing down the network. Routers include instructions that guide the user through the setup process using a web browser or app.

An increasing number of digital devices are incorporating Wi-Fi technology into their design. You are probably aware that laptops and desktops, smartphones, and tablets all typically include Wi-Fi capabilities. On mobile phones, Wi-Fi provides a less expensive way to connect to the Internet than through the cellular data plan. You may not be aware that some printers have built-in Wi-Fi so that you can print to them from any PC on the network. Wi-Fi capabilities can be easily added to a printer or computer by connecting a Wi-Fi adapter to the device's USB port. Video game consoles such as the Microsoft Xbox and Sony PlayStation, as well as media devices such as TiVo, Roku, and Apple TV, use Wi-Fi to connect home entertainment systems to home PCs and the Internet. Wi-Fi technology is even moving to automobiles.

Many cellular carriers allow customers to use their cellular data plan to connect their computer to the Internet. Tethering is the process of connecting a laptop or tablet computer to a mobile phone through Wi-Fi to access the Internet. Multiple computers can be connected to the Internet using a mobile hotspot, also called Mi-Fi technology. Mi-Fi uses a small pocket-size access point (or the smartphone itself) connected to the cellular network to function as a wireless router. Several users can connect to the router to share the cellular data service.

Reading: Bluetooth

Bluetooth (named after a 10th-century Danish king) enables a wide assortment of digital devices to communicate directly with each other wirelessly over short distances.



"Bluetooth dongle" by nSeika is licensed under CC BY 2.0

Why This Matters

Bluetooth is useful for passing data wirelessly over a short distance for a variety of purposes. It's used to connect mobile phones to speakers, headphones, and earbuds; to connect phones and vehicles; to share files between computers and mobile devices; to connect keyboards and mice to computers and tablets; to connect smartwatches to mobile phones; and many other specialized needs.

Essential Information

The Bluetooth specification was developed by the Bluetooth Special Interest Group (BSIG), a trade organization composed of leaders of the telecommunications, computing, and network industries, such as 3Com, Agere, Ericsson, IBM, Intel, Microsoft, Motorola, Nokia, and Toshiba.

Bluetooth-enabled devices communicate directly with each other in pairs. Up to seven devices can be paired simultaneously. The pairings can be created automatically or manually. For example, you might use a wireless headset to chat on a cell phone stored in your backpack. Many auto manufacturers offer some form of Bluetooth connectivity in at least some of their cars. In a Bluetooth-enabled Toyota Prius, for example, when you start the car, the car automatically connects with your cell phone and displays your call info on an LCD display in the dashboard. You can scroll through your address book, make calls, and check messages by using the LCD touchscreen on the dashboard, by using controls on the steering wheel, or by speaking voice commands.

Bluetooth communicates at speeds of up to 1 Mbps within a range of up to 33 feet (10 meters). Bluetooth can also be used to connect devices to a computer network. Bluetooth and Wi-Fi compete in some areas but have unique qualities. Manufacturers are installing Bluetooth chips in a wide variety of communications and computer appliances to allow device-to-device connections. For example, six participants sitting around a conference table could exchange notes or business cards among their notebooks, tablets, or smartphones. In contrast, Wi-Fi is generally used to connect devices to a computer network and the Internet.

Bluetooth is also used as a method for hackers to illegally gain access to devices. A number of cell phone viruses have spread through Bluetooth. Also, an open Bluetooth connection on a computer can be used by a hacker to access files on the computer. For these reasons, it is good to keep Bluetooth turned off when not using it; and when it is on, set it so that it is not "discoverable" by other devices.

Reading: Radio Frequency Identification

RFID, or radio frequency identification, uses tiny transponders in devices or tags that can be attached to merchandise or other objects and read wirelessly using an RFID reader, typically for inventory and supply chain management or to facilitate commercial transactions.

Why This Matters

There are two important uses for RFID technology today: It's used to identify and track products and is embedded in credit cards, cell phones, and other devices to enable wireless transactions at checkout counters and vending machines.



Source: Courtesy of Apple Inc. Attribution: Fair Use

Essential Information

For tracking merchandise, RFID tags are attached to products and/or crates and pallets so inventory can be tracked from the manufacturer to the retail store checkout counter. RFID tags consist of a transponder as small as a grain of sand, with an antenna, embedded on a paper tag. RFID readers may take the form of handheld devices or devices mounted in the doorways of loading docks or in conveyor belt systems. RFID may eventually replace the bar code as the primary identification system for merchandise because it is much more convenient and can relay more information. RFID systems are typically connected to central databases where inventory information is stored. As a tagged item progresses from manufacturing to warehouse to retail vendor to checkout counter, its database record is updated, providing up-to-the-minute information. This enables companies to gain better control over inventory, getting products to locations where they are needed just in time. Wal-Mart has required its suppliers to include RFID tags on all shipping crates and pallets.

Contactless payment systems make use of an RFID chip embedded in a credit card, ID card, or mobile phone to wirelessly send data to an RFID reader installed in a cash register, vending machine, toll booth, or other transaction location. Users can pay for merchandise by simply waving the credit card or smartphone over the reader, like the Apple Pay system shown in the figure. This form of telecommunications is referred to as near field communications (NFC), which is defined as wireless telecommunications that take place at a distance of about 8 inches (20 cm) or less. With lighter rules and restrictions governing credit card transactions, which no longer require signatures and receipts for small purchases, contactless payment systems are becoming widespread.

An obvious concern with contactless payment systems is wireless security. If your credit card or cell phone transmits private information through the air using radio signals, what's to stop a thief with a card reader from stealing that information? The credit card companies assure those concerned that they have a system in place to protect private information, but some security experts remain skeptical.

Besides its use in retail inventory control and contactless payment systems, RFID is used in a number of other areas where automatic identification is useful:

- Systems that allow vehicles to autopay at highway toll booths use an RFID device mounted on the dashboard or windshield.

- Hospitals employ RFID patient wristbands to enhance patient care and staff working conditions and to save on money and prevent mistakes.
- Airlines are integrating RFID into their baggage-handling systems to more efficiently track the location of passenger baggage.
- RFID devices are used in parking lots to track how long cars are parked and to send reminders to drivers while automatically deducting parking fees from drivers' bank accounts.
- RFID is used to track prescription medications through the supply chain and to curb drug counterfeiting and theft.
- RFID tags are being used to assist blind individuals in recognizing objects.

Other uses of RFID are more controversial. RFID chips have been embedded in the passports of international travelers. There is talk of embedding RFID tags in all automobile license plates, driver's licenses, and even currency. RFID tags injected under the skin are used to track ex-convicts and employees in high-security facilities. Privacy advocates are concerned that RFID could be used by governments and law enforcement agencies in ways that infringe on people's privacy and civil liberties.

Reading: Global Positioning System

A **GPS, or global positioning system**, uses satellites to pinpoint the location of objects on earth.



"Driving back" by orsorama is licensed under CC BY 2.0

Why This Matters

GPS technology provides useful navigation assistance in many environments for many purposes. Available in mobile phones, fitness bands, cars, aircraft, ships, and elsewhere, GPS provides a range of uses, from necessary functions, such as staying on course at sea, to fun utilities, such as tracking your run to improve your fitness. GPS has become an important part of most people's daily lives.

Essential Information

Using a GPS receiver and a network of 24 satellites, a GPS can tell you the exact location of the receiver on the earth's surface. GPS satellites orbit the earth in such a way that at any given time and location on earth, at least four satellites are visible to a GPS receiver. By measuring the distance from the receiver to each satellite and calculating those distances with the known position of each satellite, the receiver can determine its location on earth. Like the Internet, GPSs were originally developed for national security and later extended for public use.

Early GPS receivers were expensive and used only in environments where determining your location was a matter of life and death, such as with far-traveling ships. Now they are available as inexpensive, small handheld devices; as in-dashboard or on-dash devices for automobiles; and integrated into smartphones, smartwatches, and fitness bands.

GPS receivers are primarily used to assist travelers in getting from one place to another. GPS software can display a traveler's location on a city map and give suggestions for the shortest routes to destinations. Many GPS devices also integrate information about local businesses and services, such

as restaurants, retailers, and hospitals. Car rental companies provide GPS units to assist customers with navigating in an unfamiliar city. GPS has also been used to map the planet's surface.

GPS is also playing a role in social media. Geotagging is the process of adding geographic identification metadata to digital media and messages. GPSs in cell phones enable this to occur automatically if the user so chooses. On the iPhone, photos posted to Facebook, Twitter, Instagram, or Flickr can automatically be tagged with the location where they were taken. Posts on Facebook and other messaging systems can also include geotags. Using a variety of GPS software, users can quickly find nearby restaurants, hotels, or other businesses.

GPS is also playing a large role in fitness bands and apps. Using GPS in a health band or smartphone, a runner can map his or her run, capturing data such as elevation, distance, and miles per hour in order to calculate calories burned.

GPSs provide convenience and safety; however, as with all technology that accesses personal data (such as a person's location at a given time), its use may infringe on an individual's privacy. Consider, for instance, the possibility of someone stashing a GPS device in your car or backpack in order to track your movements. Also consider the common practice of cellular carriers collecting location data automatically from users.