Annabel Z. Dodd

THE ESSENTIAL GUIDE to TELECOMMUNICATIONS

SIXTH EDITION

A Completely Revised Bestseller: Extensively Updated Coverage of Wi-Fi, LTE Advanced, 5G, Broadband, Security Technologies, and the Competitive Landscape

The Essential Guide to Telecommunications

Sixth Edition

Annabel Z. Dodd

Boston • Columbus • New York • San Francisco • Amsterdam • Cape Town
Dubai • London • Madrid • Milan • Munich • Paris • Montreal • Toronto • Delhi • Mexico City
São Paulo • Sydney • Hong Kong • Seoul • Singapore • Taipei • Tokyo

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Visit us on the Web: informit.com

Library of Congress Control Number: 2018967285

ISBN-13: 978-0-13-450679-1
ISBN-10: 0-13-450679-0

2 20

This page intentionally left blank

7 Mobile and Wi-Fi Networks

In this chapter:

INTRODUCTION

Mobile devices are a central part of many people's lives. This is especially true of young people. When graduate students at a university were asked if they agree with the following statements, the majority of them agreed.

- You wake up in the middle of the night to check your phone.
- You check your smartphone within 10 minutes of going to sleep at night.
- You check your smartphone within 10 minutes of waking up every day.
- You study at cafes, and check your WeChat or Instagram accounts there too.
- You play games on your phone at the subway.
- You check for messages while walking to class.

Some students stated that they check their phones 15 and more times every hour. Young people and not-so-young people use their phones for online gaming, video streaming, and social networks. It's an integral part of their day. High usage is not confined to teenagers and twenty-somethings. It's an important part of everyday life for much of the population.

Growing capacity, availability, and ease of use enable adults as well as twenty-somethings to use cellular networks for an increasing number of functions. People use these networks to stay in contact with friends and family, receive email and text messages, and keep up-to-date on news. While waiting for an appointment in a doctor's or dentist's office, most people use their device to make the time pass faster. And people that travel often bring tablet computers on airplanes and train trips to watch downloaded videos.

The increased use of smartphones and tablet computers has created pressure on mobile carriers to add capacity by upgrading their networks to protocols that enable them to pack more traffic on the airwaves that carry wireless voice and data.

In essence, mobile networks are becoming densified, meaning cell sites with antennas and adjunct equipment are spaced closer together with each supporting higher data rates. Densification requires adding new cell sites to support gigabit data rates achievable with upgraded Long Term Evolution 4th generation (LTE) networks and new 5th generation mobile protocols. Densified wireless networks are architected with fiber-optic cables that connect heterogeneous networks (HetNets) together. The name HetNets is derived from the fact that HetNets are made up of cell sites with various amounts of coverage and antenna sizes.

There is additionally more usage over Wi-Fi networks inside homes, cafes, and buildings as people increasingly use smartphones and tablet computers for video streaming, reading newspapers, and accessing social networks within buildings. There are new and emerging protocols that support gigabit data rates and improved security in Wi-Fi networks. The same phenomenon of large increases in wireless usage is occurring inside buildings and homes as in cellular networks in wider outdoor areas. In many residences, it's not unusual for each person to have multiple devices with many in use simultaneously.

Satellites along with ground-based wireless networks are being designed and upgraded to support broadband services in areas with sparse availability of high-capacity cellular networks and broadband networks. In particular, low earth orbiting satellites (LEOs) that orbit closer to the earth than traditional satellites are being deployed. LEOs are made up of smaller, less costly satellites than traditional satellites. Because they are lower in the sky, more LEO satellites are required to cover the entire earth. However, even at the lower price, it takes a group of investors to raise additional funding to build these high-cost satellite networks.

The requirement for new satellite networks, 5th generation mobile network infrastructure, and upgrades to LTE mobile networks require ongoing investments. The same is true of infrastructure and protocol development in Wi-Fi networks. Moreover, the challenge of operating these complex networks is sparking an interest on the part of providers to use cloud-based services to manage the large numbers of dense network components.

SPECTRUM FOR WIRELESS NETWORKS—A CRITICAL ASSET

In wireless networks, spectrum consists of the invisible electromagnetic energy used to transmit signals. The spectrum over which signals are carried is a critical asset that carriers require to operate their mobile networks. All governments regulate the allocation of spectrum. This is to prevent multiple transmissions from different mobile providers from interfering with each other. Mobile networks are critical for communications in national defense and public emergencies, particularly when landline networks may not be available.

Cellular Structures—The Foundation of Mobile Networks

Cellular service was first put into operation in 1984. It uses spectrum more efficiently than earlier, non-cellular systems by enabling networks to reuse the same frequencies in non-adjacent cells within cities and towns. The reuse of frequencies within non-adjacent cells was a creative innovation that added capacity to cellular networks. AT&T's Bell Laboratories (now part of Nokia) created this first generation of cellular service. At that time, Bell Labs was owned by AT&T, which in turn owned all of the local telephone companies in the United States. Bell Labs provided the research and development for all the AT&T-owned telephone companies at that time. See the section "The Breakup of AT&T" in Chapter 3.

The Division of Airwaves into Frequencies

All wireless services operate over spectrum. Spectrum is divided into and allocated by frequencies. A *frequency* is the number of times per second that a radio wave completes a cycle. A cycle can be imagined as a letter *S* lying on its back, such that it appears similar to looking at a cross-section of an ocean swell. A cycle is complete when energy passes through an entire radio wave from the highest to the lowest portions of the wave. For a visual depiction of a complete wavelength cycle, see Figure 7-1. Frequency is measured in *hertz*, which refers to the number of complete cycles per second. Thus, for a frequency of 30 million hertz—or *megahertz* (MHz), as it is called—energy passes through 30 million resting *S*'s in one second.

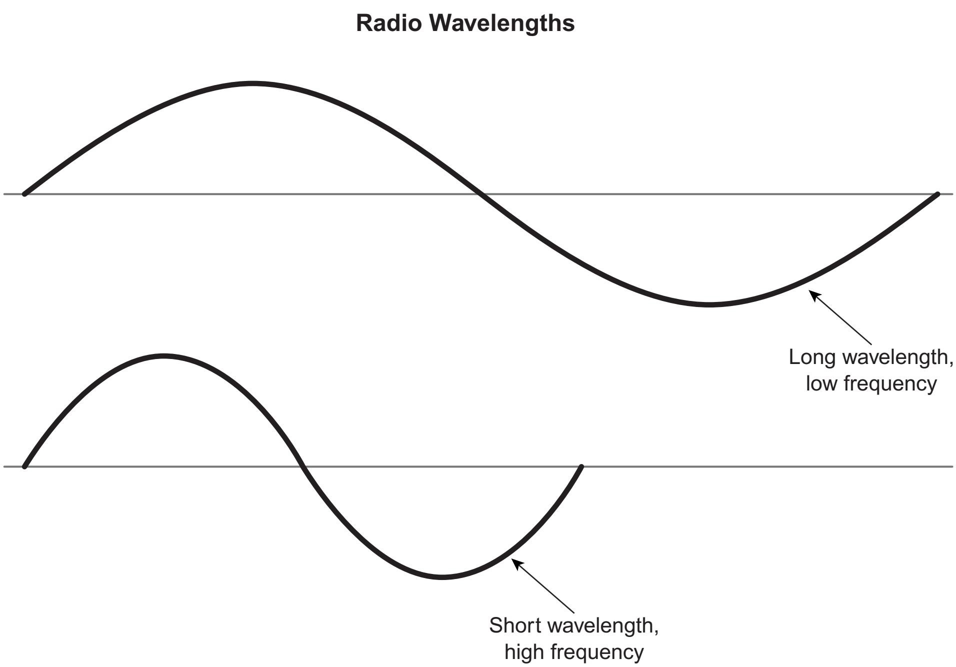


Figure 7-1 *A comparison of short, high-frequency wavelengths and long, low-frequency wavelengths.*

The Characteristics of Short and Long Wavelengths

Spectrum is divided into frequency ranges from low ranges of frequencies of about 30MHz to 300MHz allocated to government agencies, local police, highway, and state police to high frequencies such as 24 to 50 gigahertz (GHz) for fixed, point-to-point wireless service and for 5G networks. Each range of frequencies is measured by the wavelength in the range. Wavelengths in low frequencies, such as AM radio at 100Khz, measure 9,000 feet (3,000 meters) long. Higher-frequency 10Ghz wavelengths measure 1.78 inches (3 centimeters).

Because of their longer wavelengths, low-frequency signals travel farther than high-frequency signals. Their longer lengths allow them to better withstand physical barriers such as rain and other solid materials. Thus, low frequencies can penetrate walls, buildings, and similar obstacles better than high frequencies. For these reasons, broadcast services such as those for traditional TV and for TV broadcasts designed for mobile devices typically use lower frequencies.

High-speed mobile data networks operate over a variety of spectrum, such as 600MHz, 700MHz, 2.1GHz, 2.6GHz and 39GHz. Higher frequencies require more closely spaced antennas because these signals fade over shorter distances. New 5th generation mobile services will be based on high-gigahertz frequencies such as 39GHz spectrum. For the most part, cells in urban areas cover a smaller area, resulting in many small cells with small antennas rather than large towers. Smaller, closely spaced cells are needed to support dense amounts of high-data-rate mobile traffic in metropolitan areas with high-pedestrian traffic.

Spectrum Blocks

Governments allocate spectrum in chunks of frequency bands that are measured in ranges of, for example, 12-, 15-, 22-, and 30MHz. The size of the spectrum band is determined by subtracting the lowest frequency of the range from the highest frequency (highest frequency minus lowest frequency). For example, if an organization is granted the rights to use the spectrum band from 785MHz to 800MHz, it has the right to a 15MHz band (800 – 785 = 15).

Spectrum bands, which are set aside for specific services, are divided into blocks designated by letters of the alphabet. For example, within the 700MHz band (between 700MHz and 799MHz), the A block refers to a different block or range of frequencies within this larger range of frequencies than the B Block. The A Block might be allocated to one carrier in a region and the B Block to a different carrier for competing services in the same region. As new technologies are developed, certain spectrum bands are used for *shared spectrum*. With shared spectrum, sophisticated protocols in antennas send signals around signals from other traffic.

Using Numeric Designations for Roaming Compatibility

In addition to alphabetic designations for blocks of spectrum, numeric ranges are designated for particular portions of spectrum within blocks. Standards bodies designate the numeric bands of spectrum for *uplink* and *downlink* transmissions. These bands are specified by numerals. For example, the 3rd Generation Partnership Project (3GPP) designated band 13 spectrum of the 777–787MHz range for uplink transmissions.

- Uplink (UL) transmissions are those from subscribers to carriers' antennas, and
- Downlink (DL) transmissions are those from the carrier to the subscriber.

The goal is to enable equipment compatibility so that customers can more easily use their mobile devices on other networks. Mobile devices have preset designations for which frequencies are used for uplink and which are used for downlink communications. Thus, they only work on networks that use the same bands within frequencies.

The 3GPP specifies other bands, such as 12 and 17, for either uplink or downlink transmissions. Not all technologies require separate frequencies for uplink and downlink communications. In these instances, numeric designations are not required.

Using Auctions to Allocate Spectrum

Because it is finite and critical to industry, security, and emergency preparedness, all governments allocate spectrum for particular uses. Portions of the public airwaves and frequencies are allocated for satellite, broadcast TV, Wi-Fi, 4th generation, and 5th generation mobile service as well as other services.

Governments often provide spectrum at no charge when they believe it is in the national interest to foster development of new services. This happened in Asian countries such as Japan and others where the government felt it was in the national interest to foster construction of higher-capacity wireless networks. Japan's allocation of spectrum was based on the government's evaluation of organizations' ability to build and manage a cellular network. These were dubbed *beauty contests*.

Strategies to Gain Rights to Spectrum

Rules about spectrum allocations are set by the FCC and by Congress. The rights to these blocks are strategic assets that enable carriers to offer new, competitive services. Mobile carriers and governments use the following strategies to gain new spectrum:

- Purchase rights to it at government auctions
- Discontinue the use of their older cellular services and *refarm* this spectrum for more advanced protocols. Currently, mobile carriers are building LTE Advanced and 5G networks on spectrum formerly used for 2nd and 3rd generation networks. (See below for *refarming*.)
- Purchase entire companies for their spectrum
- Purchase non-cellular companies' unused spectrum (See the feature "Acquiring Spectrum by Buying Companies that Own Spectrum Suitable for 5G" later in this chapter.)

In order to free up spectrum for high-capacity mobile networks or other national needs, organizations and government agencies already using these bands must be moved to other bands.

Using Incentive Auctions to Speed Up Spectrum Availability

In February 2012, Congress allocated $7 billion for the build-out of a nationwide public safety network and authorized the use of an *incentive auction* for that purpose. In an incentive auction, entities selling spectrum to the government keep lowering their prices until the FCC determines the amount of money they collect from the auction is adequate to pay for needed spectrum from the entities giving it up.

The FCC held the first incentive auction in 2016 and announced the results in 2017. It offered the D Block of 700Mhz spectrum that analog TV stations ceded in return for spectrum for digital television. The auction raised $19.8 billion, $10.8 billion to pay for the broadcasters' spectrum and more than $7 billion that was deposited in the U.S. Treasury. AT&T won the bid in the auction held on March 29, 2016, and is in the process of building out the FirstNet network for first responders from diverse communities to communicate with each other to coordinate strategy in natural disasters and national emergencies.

This first-ever incentive auction resulted in refarming spectrum from use for analog TV channels to a national public safety network. As a result of the auction, over-the-air broadcasters changed from analog to digital TV using the spectrum given to them by the FCC. Digital airwaves have capacity for two channels in the same amount of spectrum needed for one analog channel. In addition to spectrum for the public safety network, cellular providers won spectrum for new mobile wireless licenses needed to add capacity to their cellular networks.

Auctions Held between 1998 and 2017

- In 1998, the FCC auctioned PCS 1.9GHz spectrum to open mobile services to new providers. The goal was to increase competition, thus lowering per minute prices so that more users could afford cellular service. Prior to this there were only two providers in each part of the United States: the incumbent telephone company and a single competitor.
- The FCC auctioned a 700MHz block in 2008 to a variety of carriers for higher-capacity, higher-data-rate services. Verizon Wireless won regional licenses to spectrum in the A and B blocks, and AT&T Mobility won rights in the B and C blocks. AT&T's B blocks are in a different region from Verizon's. None of the licenses cover the entire country. The auction raised $19 billion for the federal government. All of the auction winners were required to use this spectrum to build networks capable of supporting higher-speed data on next-generation LTE networks.
- In 2014 an AWS (Advanced Wireless Services) auction of 1.755 to 1.78GHz and 2.15 and 2.18GHz spectrum bands was held. Results were announced in 2015. The winners were, in decreasing order of the amount of spectrum won,

AT&T Mobility, Verizon Wireless, Dish Network, T-Mobile, U.S. Cellular, and a mix of five private companies including American Movil, a cellular company owned by Mexican mogul Carlos Slim and his family. The American Movil spectrum is used in Puerto Rico.

- In 2017, the FCC held a reverse auction of 600Mhz spectrum. T-Mobile won the largest percentage of this spectrum. AT&T and Dish Network won lesser amounts. AT&T subsequently began selling the spectrum it won because it purchased FirstNet for its nationwide spectrum. Other winners included U.S. Cellular and Comcast. Verizon did not bid, possibly because it is concentrating on building out a network of small cells using GHz spectrum able to carry large amounts of data.

Enhancing Spectral Efficiency to Increase Capacity

The ability to carry more traffic within a given amount of spectrum is crucial to keeping up with the growing amounts of mobile data traffic. Carrying more traffic using the same amount of spectrum is called *spectral efficiency*. Each successive generation of wireless protocols is more spectrally efficient than the previous one. For example, 4th generation (4G) wireless technologies are capable of carrying more high-speed wireless data and video than third-generation (3G) technologies and 5G is expected to be more spectrally efficient than 4G.

The successive spectral efficiency in newer generations of mobile services is gained by building more efficient antennas, faster chips in radios located at cell sites and in users' mobile devices.

Profits from Unused Spectrum on the Secondary Market

In addition to obtaining spectrum at auctions, carriers purchase spectrum on the secondary market from organizations that purchased it at earlier auctions but either did not build a network on it or were unsuccessful in their service offerings. For example, beginning in 2011, Dell computer owner, Michael Dell bought up TV and radio stations for the value of their spectrum, which he sold in the 2016 incentive auction for billions of dollars.

Taxpayers currently receive no revenue from the sale of unused spectrum by non-governmental organizations. In 2011, cable TV providers Comcast, Time Warner Cable, and Bright House Networks agreed to sell the spectrum that they purchased through at an auction to their joint venture, SpectrumCo, to Verizon Wireless for $3.6 billion. The cable companies earned a windfall of $1.4 billion on their $2.2 billion spectrum purchase. They subsequently built out a nationwide network of Wi-Fi sites over which cable TV subscribers reach the Internet from Wi-Fi–enabled cafes and public spots. None of this profit went to taxpayers.

To ensure that entities that purchase spectrum use it for actual mobile networks, the FCC has ruled that carriers and other winners of spectrum must use their spectrum within 12 years. If it's not used within this time frame, the FCC can reclaim the idle spectrum. This has not stopped spectrum owners from selling their spectrum at huge profits to cellular networks before the 12-year deadline.

In fact, the FCC did require that FiberTower return all of its 24GHz that it won, but on which it did not build infrastructure. It allowed FiberTower to keep its other spectrum. See below for information on AT&T's purchase of FiberTower.

NOTE Fixed Wireless to the Home (WTTH) is the use of cellular service at homes for broadband service. Fixed wireless requires dishes at subscribers' homes and equipment on telephone poles for access to the Internet. It also requires a small converter box to convert the cellular signals to those compatible with the residence's Wi-Fi signals.

Acquiring Spectrum by Buying Companies that Own Spectrum Suitable for 5G

In addition to leasing spectrum from governments, large mobile carriers purchase companies that already have underutilized or unused spectrum. In recent years Verizon Wireless and AT&T Mobility purchased companies for their high-frequency spectrum. High frequencies are suitable for building thousands of the small cells needed for 5G services in heavily trafficked downtown areas.

In early 2018, AT&T acquired FiberTower, which owned 24GHz and 39GHz spectrum. However, they only got a portion of its 39GHz spectrum and none of its 24GHz spectrum. The FCC seized the 24GHz spectrum because FiberTower hadn't utilized this spectrum. But AT&T did acquire FiberTower's 188 billion points of presence, which are used to backhaul data from cell sites to mobile network switches and core networks. AT&T also purchased Straight Path Communications in 2017 for its 29GHz and 39GHz spectrum.

Verizon bought fixed wireless company XO Communications in 2017. Its XO purchase included the rights to lease XO affiliate NextLink's 28GHz spectrum, which is located in and around large cities in the United States. These high-frequency spectrum bands are desired for 5G mobile networks. The FCC must approve these purchases of spectrum before the spectrum transfers are finalized. The Competitive Carrier Association (CCA) objected to this spectrum transfer because it had not been offered at an auction so that smaller mobile carriers would have an opportunity to bid on this valuable spectrum.

Continued

The CCA was quoted in a FierceWireless article on January 19, 2018, by Mike Dano, titled "AT&T to lose hundreds of 5G millimeter wave licenses as part of FCC/FiberTower settlement." The CCA stated "If the pending transaction [between AT&T and FiberTower] is approved, the terms of the settlement agreement will afford FiberTower a financial windfall for sitting on unconstructed licenses for years and AT&T a windfall to acquire valuable 5G spectrum." The FCC approved AT&T's purchase of FiberTower on February 12, 2018.

Synchronizing Spectrum Internationally

Spectrum allocation is administered on both an international and a national level. The International Telecommunications Union-Radiocommunication Sector (ITU-R) manages the allocation of spectrum for services such as satellite and television that cross national borders. It also acts as the umbrella for other services such as determining spectrum bands for 3rd, 4th, and 5th generation services. These functions have become more critical as subscribers worldwide depend on their mobile devices when they travel for business and leisure.

In the United States, the International Bureau of the FCC, the National Telecommunications and Information Association (NTIA), part of the Commerce Department, and the State Department work with the ITU-R. Generally, working groups comprising representatives from many countries hash out particular issues under the auspices of the ITU. Decisions on spectrum and new 4th and 5th generation protocols are made at the ITU's World Radiocommunication Conferences (WRC), held every 5 years.

Geographic Licensing Schemes

Because of its large size, and mountainous, sparsely populated areas, no single carrier's network provides complete geographic coverage across the entire United States.

There are six regional groupings in the contiguous United States and others for regional groupings such as Alaska and Hawaii. The Gulf of Mexico also retains its own grouping.

Verizon Wireless and AT&T Mobility cover almost all of the metropolitan areas in the United States, but not all of the rural areas. No other carrier has such extensive coverage or the financial wherewithal to purchase spectrum to cover these large areas. In the 2016 auction, T-Mobile was the major bidder. They scooped up almost the entire spectrum in the 600MHz range. This spectrum is particularly suited to fixed wireless in rural areas because of its ability to travel distances without fading.

Fixed wireless is important in rural areas where it's not cost effective to lay fiber to homes miles apart from each other. See Figure 7-2 for an example of fixed wireless service. Deploying fixed wireless from telephone poles to homes is many times less costly than laying fiber in rural areas. There are fewer residences in rural areas from which mobile companies can recoup the cost of constructing fiber networks to homes.

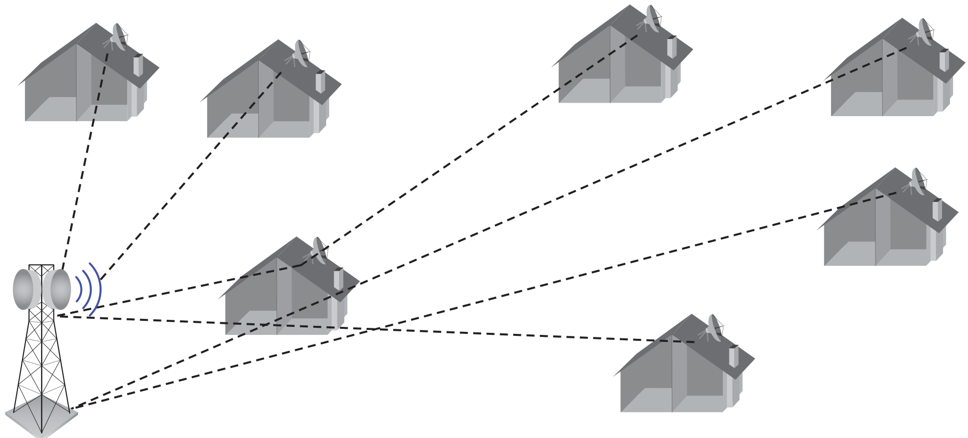


Figure 7-2 Fixed wireless in rural areas.

Mitigating Interference

When transmissions use the same frequencies in the same locations or even next to one another, they can interfere with one another. For example, if people install Wi-Fi wireless equipment such as cordless telephones as well as microwave ovens that operate at 2.4GHz near each other, they may experience operability problems. These problems are caused by interference. Newer wireless protocols have the ability to hop between channels when they sense that other signals are in the same channel.

Concerns about interference often lead to political conflicts between factions. This can occur when new uses for spectrum or new technologies are proposed. This occurred, as illustrated in the next section, when it was first proposed that white-space spectrum be allocated for other uses and also when LTE U was proposed. See Table 7-2, "LTE Types."

Unlicensed Spectrum for "Super" Wi-Fi

Governments specify portions of the spectrum for unlicensed services such as Wi-Fi and *Bluetooth*. Bluetooth is a wireless standard for communications between short distances such as wireless mouse or headsets linked to PCs and smartphones. Unlicensed spectrum is available free to companies that do not have to apply for a license to use it. This significantly lowers the cost of deploying service, but it doesn't mean the government does not regulate unlicensed spectrum. Every cellular and wireless device must be registered with the FCC and adhere to regulations on the amount of power emitted.

Devices that emit high power may interfere with nearby devices. Moreover, the government can designate bands of spectrum as unlicensed for public benefit.

In 2010, the FCC designated licensed spectrum formerly used in conjunction with analog TV as unlicensed spectrum to lower the cost of bringing new broadband services to rural areas. When broadcasters changed from analog to digital television broadcasts, The FCC auctioned off most of the 6MHz of that spectrum formerly used as *guard bands* for analog TV and still used for wireless microphones.

Guard bands, also called *white spaces*, are unused bands of frequencies surrounding each channel that prevent wireless signals from adjacent analog channels from interfering with one another. Wireless signals are not enclosed in cabling, and thus can leak or spread into adjacent spectrum. Analog signals leak more than digital signals. For this reason, when the FCC originally allocated spectrum for analog television, it set aside 6MHz of spectrum as guard bands between all adjacent TV channels.

When the FCC announced its desire to make these white spaces available for Long Term Evolution (LTE) because they were no longer used as guard bands, broadcasters and Broadway theater producers objected. They were concerned that new services in the spectrum might interfere with microphones and other equipment used at public events such as those in stadiums, concerts, and even churches. After extensive testing, including an experimental license granted in a small rural town, the FCC ruled that the former white spaces could be used as unlicensed spectrum. It ruled that it could be used for "super" Wi-Fi, a Wi-Fi standard whose signals can travel over longer distances than traditional Wi-Fi signals. "Super" Wi-Fi is the informal name for the 802.22 IEEE standard.

The FCC hoped that this spectrum would be used to bring high-speed Internet access to rural areas. Making the spectrum unlicensed further supported the goal of lowering the total cost to bring Internet access to rural areas. Because this spectrum is in the 700MHz range, which is a low frequency, the signals can travel the distances required in rural areas. Using wireless obviates the need to lay fiber-optic cabling and install costly electronic equipment near customers or directly to premises.

Power-Level Specification for Unlicensed Spectrum

Because of the potential for wireless spectrum to cause interference, governments establish rules regarding issues such as signal spreading and power limitation to protect adjacent licensed spectrum bands against egregious interference emanating from unlicensed spectrum transmissions. All equipment used in licensed and unlicensed wireless networks must meet government specifications to receive certifications. That is why even a Bluetooth mouse is certified and assigned an FCC ID number.

Roaming—Using Mobile Devices in Other Networks

Roaming is the ability to use the same mobile devices when traveling in other carriers' networks. These other networks may be within the United States or in international locations where a subscriber's mobile provider does not offer service. Roaming is important because no single carrier has coverage everywhere. Roaming is a profitable source of revenue in many parts of the world. Exceptions to this include within European Union countries, most cellular providers for traffic within India, and depending on each customer's plan, traffic within the United States.

In June of 2017, the European Union eliminated roaming surcharges for residents of the EU that travel within EU countries. Another example of no-cost roaming is T-Mobile, which offers customers on certain plans no-fee texts, voice, and data usage when they roam in 140 countries internationally.

Agreements among carriers are required for every region in which roaming is enabled. Roaming agreements spell out costs, billing, and payment terms. To illustrate the complexity of roaming arrangements, most carriers have agreements with 200 to 250 other carriers. Some carriers use brokers that already have agreements worldwide and share revenue with the broker. Thus, calls made and received while roaming are more expensive than those in the subscriber's home territory; with the additional costs covering the fees imposed by the other network.

Once the agreement has been signed and the service tested, roaming is activated. Carriers lease high-speed links to other providers such as AT&T, France Telecom, and Belgacom (in Belgium), all of which have an international presence. These links carry the actual voice and data traffic. Signaling links are also established to perform functions such as the *handshake* between the handset and the user's home carrier. The handshake verifies that users are legitimate customers of the originating network and have roaming privileges. Gateways are used to translate signaling between handshakes that use incompatible types of Session Initiation Protocol (SIP) links over which the handshake is done.

Roaming revenues are shrinking because many customers use Wi-Fi in cafes and hotels when they travel internationally. For more on Wi-Fi international networks see the section "Wi-Fi for Roaming" later in this chapter.

MORE EFFICIENT 4TH GENERATION DIGITAL NETWORKS

Mobile protocols define how data and voice are carried on cellular networks. For example, 3rd generation (3G) networks carry data and voice separately. However, 4th generation (4G) networks specify that voice and data are to be transmitted on the same spectrum streams. They essentially treat voice as data and transmit it in IP packets. This is a significant improvement in spectral efficiency that eliminated the need to set aside separate spectrum for voice calls.

All 3rd generation and newer cellular services are digital. This improves privacy as eavesdropping on digital transmissions is more difficult because the digital bits are encrypted (encryption uses mathematical algorithms to reorder bits, making them unreadable to unauthorized people) before they are transmitted over the open air between handsets and an operator's equipment. See Table 7-1 for a list of the main mobile protocols along with the various implementations within each generation.

Unlike 3rd generation protocols, which used different technologies in Europe and parts of the United States, 4G LTE is for the most part is implemented uniformly throughout the United States and Europe, as well as in Asia and parts of Africa.

NOTE All current mobile services including 2G (second-generation) services are digital. Digital mobile protocols use codecs to code analog voice into digital bits and decode them to analog at the receiving user device. Digital transmissions enable features such as caller ID, speed dialing, and voicemail message notifications. Signals for these features are carried separately in the signaling channel.

3G standards had various releases or revisions, which improved upon and increased capacity and suitability for mobile networks capable of carrying voice, video, and data. However, even in these revisions, voice is transmitted using the less-efficient circuit switching where spectrum that could be shared with data is set aside for voice. More information on 3G and 3G standards are in Table 7-6 and Table 7-7 in the "Appendix." In 4G networks, voice is carried in Internet Protocol (VoIP) packets on the same spectrum as data.

3G protocols are still available in even advanced networks because there are still older phones that are compatible with only 3G and not 4G protocols. Once mobile providers find that a large majority of subscribers have phones compatible with newer protocols, 3G spectrum will be refarmed (repurposed) for 4th and 5th generation cellular services. *Refarming* refers to using spectrum previously used to carry older generations of traffic to use with 4th and 5th generation protocols.

Table 7-1 *Main 3rd, 4th, and 5th Generation Cellular Service*

Generation	Variations	Where Used	Characteristic	Transmission
3G**	CDMA (Code Division Multiple Access)	Implemented by Sprint and Verizon in U.S. and in South Korea & other Asian countries	Data carried as digital bits	Voice transmitted on separate spectrum
	WCDMA (Wideband Code Division Multiple Access)	Implemented in Europe and most of the rest of the world	Data carried as digital bits	Voice transmitted on separate spectrum

Generation	Variations	Where Used	Characteristic	Transmission
	HSPA+ (High Speed Packet Access Plus)	Upgrade from WCDMA	Higher for data capacity than WCDMA	Voice transmitted on separate spectrum
4G	LTE* (Long-Term Evolution)	Implemented worldwide	Evolved to support 100Mbps of data downlink	Voice and data transmitted together in data packets
5G	5GNR (New Radio)	WTTH (Wireless to the Home) is the first 5G service implemented	A replacement for low-capacity copper links in rural areas	Less-costly broadband option; not as fast as fiber.

**Additional varieties of LTE are in Table 7-2, "LTE Types."*

***More details on 2G protocols and mobile services worldwide are listed in Table 7-5 in the "Appendix."*

3G Technologies—Incompatible Standards

The International Telecommunications Union (ITU) defined IMT-2000 (International Mobile Telephone) digital standards for 3rd generation voice and data on cellular networks. Unfortunately, the ITU subcommittees endorsed several different, interoperable 3G techniques due to political pressure from operators and manufacturers who wanted standards to more closely match the equipment they produced and used in their networks.

The two main standards organizations, 3rd Generation Partnership Program (3GPP) and 3rd Generation Partnership Project 2 (3GPP2), specified non-interoperable protocols and architectures (the way devices are connected together and interoperate). 3GPP (3rd Generation Partnership Project) is a collaboration agreement formed by European, Asian, and North American telecommunications standards for cellular protocols.

See Table 7-6 in the "Appendix" for more details on 3G networks.

Early LTE Implementations

The earliest version of LTE was a pre-4G service. The capacity on these early LTE implementations reached ranges between 2Mbps and 25Mbps, not the 100Mbps defined in the 4G LTE specifications. LTE's use of Multiple-Input Multiple-Output (MIMO) antennas is a key factor in increased capacities.

LTE—THE FIRST TRUE 4TH GENERATION CELLULAR PROTOCOL ....

Long-Term Evolution (LTE) is the first protocol to use spectrum more efficiently by transmitting both voice and data as IP packets over the same spectrum bands. It is no longer necessary to set aside spectrum exclusively for voice on different spectrum than that for data. LTE is additionally the first mobile protocol suitable for video and high-capacity data transmissions.

Initially, LTE protocols did not support the full 4G rates defined by standards bodies; the ITU-R specified that 4G technologies support 100Mbps downlink transmissions from the network to the user. Criteria for 4G protocols are set by the ITU-R. The ITU-R defines the capabilities required for protocols to be considered 4G, but the 3GPP (Third Generation Partnership Program), does the actual development work of how these recommendations will be implemented.

According to the ITU-R definition, which was published in November 2010, all 4G technologies must meet certain capabilities. The key 4G criteria are as follows:

- Data rates of 100Mbps downlink (from the network to the user device) for mobile devices such as those in cars or trains, and 1Gbps downlink speeds for low-mobility devices. Low mobility refers to devices used in fixed locations or portable only within a building.
- Internetworking with services based on international mobile telecommunications (IMT), earlier 3G protocols, and with services transmitted on fixed, landline networks.
- An all-IP packet infrastructure.
- Internet Protocol version 6 (IPv6) addressing, which has more addresses than IPv4. See Chapter 6, "The Internet," for information on IP addressing. See the section "Addressing Protocols" in Chapter 6 for information on IPv6 and IPv4.
- The ability to support mobile TV.
- Efficient use of spectrum.
- Worldwide roaming compatibility between mobile 4G devices.

Internetworking refers to the fact that 4G devices can seamlessly be handed over between cell sites that use 3G and 4G protocols without transmission interruptions. See Figure 7-3 for an example of a handover between 3G and 4G networks. Handovers are the process that occurs when subscribers travel between networks that support different protocols.

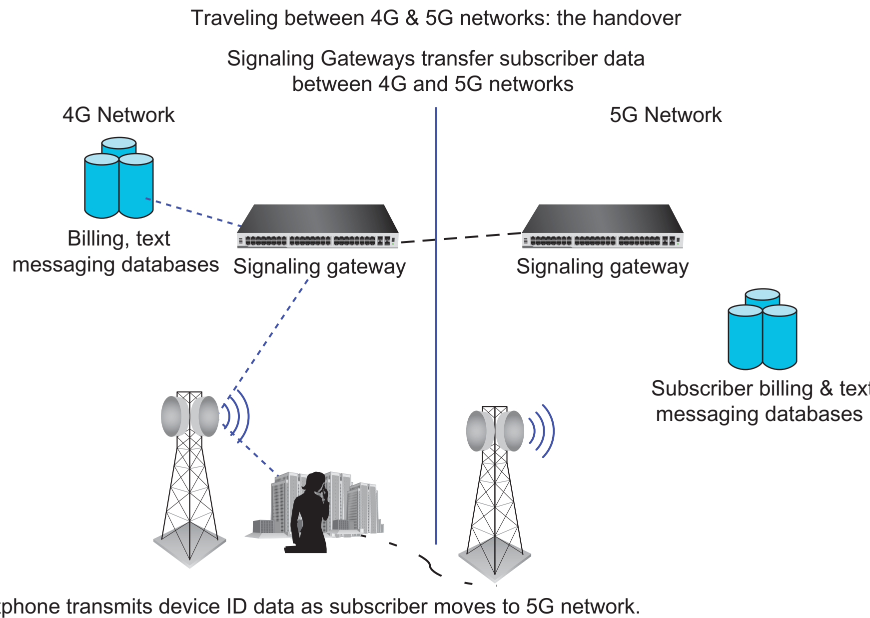


Figure 7-3 *The handover between 3G and 4G networks.*

A number of manufacturers compete with one another to supply 4G and 5G network software and hardware. These include Ericsson, Huawei, Nokia, Samsung, Xiaomi, and ZTE.

4G LTE—Designed to Transmit Data and Voice in IP Packets

4G technology was developed with the goal of supporting high-speed broadband and video transmissions. It is the first mobile protocol designed primarily to transmit data. It supports voice, but only as IP within data packets. LTE has improved antennas, and faster chips in handsets and in radios in the network. The mobile core is the mobile carrier's data center. It is equipped with servers containing databases and software to control and monitor the network as well as providing connections to other networks.

LTE is the 4G protocol adopted by carriers worldwide. Manufacturers produce a wide choice of devices for networks that use these air interfaces, because these networks represent a large pool of potential customers. Handset prices also tend to be lower because there are more choices and more competitive pressure.

LTE Capacity

LTE (Long Term Evolution) supports web surfing, mobile broadband, and Quality of Service (QoS) for video streaming. QoS saves a path in the network for each video transmission for the entire duration of the video. This provides the consistent service required for video. True IMT-Advanced, 4G LTE, based on Release 11, supports 100Mbps downloads, and is available in much of the world.

LTE is not a one-flavor protocol. It has evolved into a true 4th Generation protocol with variations. These variations are listed in Table 7-2, "LTE Types." Each variation operates on specific spectrum bands and is suited for particular applications such as low-speed Internet of Things (IoT). Another LTE variation is suitable for fixed WTTH in areas with no fiber or high-speed Internet access to homes.

NOTE

IoT is the ability of equipment and machines to communicate with each other and with central servers for monitoring and collecting information. Monitoring automobile traffic is an example of an IOT application. Collecting subway fees and parking meter credit card transactions remotely are other IOT applications.

Mobile Service in Sub-Saharan Africa

Mobile broadband is particularly significant in developing areas such as countries in sub-Saharan Africa, where high-capacity fixed broadband is not widely available. Much of the population in sub-Saharan Africa that live in cities own mobile phones, but the capabilities are limited in large part to 2G and 3G services. Exceptions are major cities in Democratic Republic of Congo, Ethiopia, Nigeria, South Africa, and Tanzania. This is starting to change as mobile operators have announced plans to build out LTE capabilities. Cell phone ownership in sub-Saharan Africa is lowest among women and children under 16.

LTE Cell Sites' Additional Functionality

An LTE cell site consists of antennas, amplifiers to adjust power levels, and a single piece of equipment, the evolved NodeB (eNodeB). The eNodeB allocates radio frequency (wireless spectrum) to users' devices and passes calls off to other cell sites and to the mobile carrier's core IP network. Importantly, the eNodeB manages Multiple-Input Multiple-Output (MIMO) antenna functions and Orthogonal Frequency-Division Multiplexing (OFDM) signaling. See the section "The LTE Orthogonal Frequency-Division Multiplexing Air Interface" later in this chapter.

Coaxial cabling connects the eNodeB to the cell site's antenna. The eNodeB contains a blade with a software-defined radio containing the air interfaces tuned to the applicable spectrum. A blade is a densely packed, horizontally placed circuit board with many ports. The modem in the software-defined radio translates radio frequency signals into those compatible with landline networks, and vice versa for outgoing traffic.

The eNodeB is also referred to as the *base station*. Together with the antennas, amplifiers, and spectrum, it is used to access the mobile network. In combination, this equipment and spectrum make up the Radio Access Network (RAN). The eNodeB manages the RAN.

LTE architecture is streamlined in terms of the amount of equipment and protocols required compared to earlier generations of mobile networks. Figure 7-4 presents a diagram of LTE architecture. This streamlining and distribution of functions at fewer servers results in data stream transmissions that use fewer protocols and equipment hops. This decreases latency (delays).

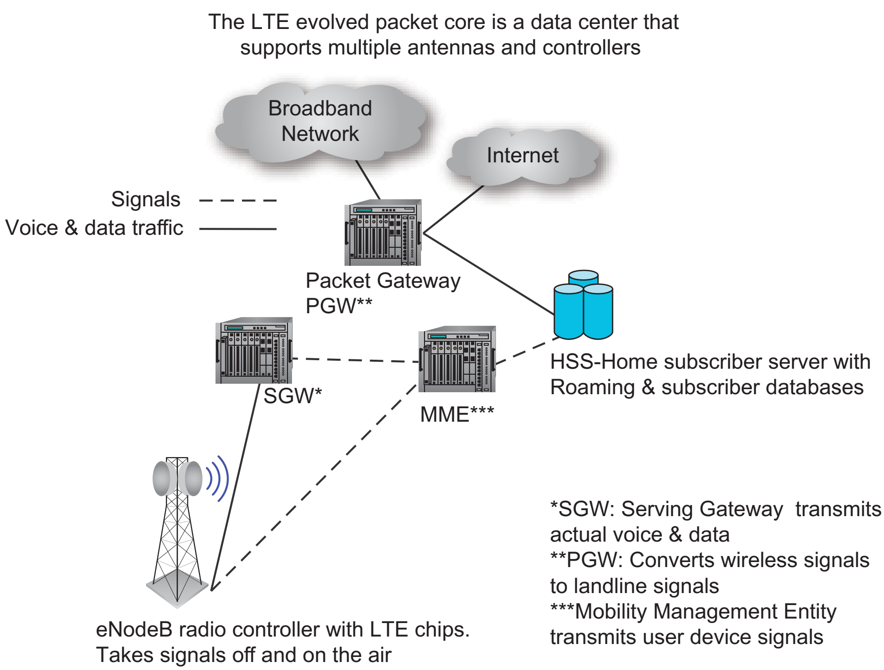


Figure 7-4 Fourth-generation (4G) Long-Term Evolution (LTE) architecture in the Radio Access Network (RAN) and the evolved packet core.

Backhaul—Connecting Cell Sites and Core Networks

In addition to managing vast amounts of cellular traffic, carriers operate large landline networks between their cell sites and their IP core. The links between cell sites and equipment in their core are referred to as *backhaul*. Backhaul is also referred to as the *transport network*. Traffic from many sites is backhauled to a central location—the operator's core network. This network transports signals between base stations and core networks. Transport networks consist of links to mobile switches and other networks. From the core, traffic is sent to the operator's mobile central office switch, the Internet, or another public data network. See Figure 7-5 for an example of backhaul links. Depending on the amount of traffic, backhaul networks use the following:

- Microwave (a Wireless Transmission Service at 44Mbps/34.4Mbps) or wireless Carrier Ethernet at speeds up to 40Gbps
- Fiber-optic cabling transmitting Gigabit Ethernet traffic
- Gigabit Ethernet and Multi-Protocol Label Switching (MPLS) (multiple 100Gbps streams with MPLS-enabled QoS capabilities) on fiber-optic cabling

A backhaul network is made up of traffic from cell sites that is aggregated and transmitted to the core.

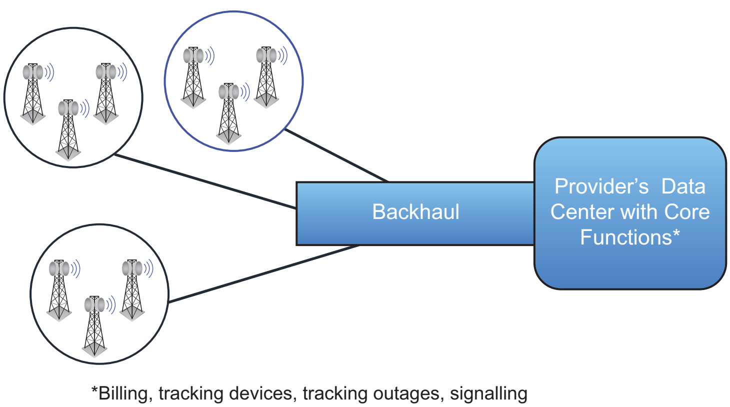


Figure 7-5 *The aggregation backhaul network consolidates traffic from multiple cells and sends it to the core.*

In the United States, most providers have upgraded much of their backhaul network to fiber. In areas of the country and worldwide where fiber is not already installed, backhaul traffic is carried by microwave and other higher-capacity wireless technologies. The higher costs for fiber are viable because more traffic is carried on these links. Fiber is likely to be more readily available in aggregation networks where carriers have previously laid fiber that often has spare capacity.

In many instances, the landline divisions of mobile carriers build these networks. When Verizon Wireless upgraded its backhaul network to fiber, it used the wholesale division of Verizon Communications to build it out. Verizon's wholesale division offers backhaul services on a wholesale basis to other providers in addition to Verizon Wireless. Cable Multiple System Operators (MSOs), AT&T, and other long-haul network carriers also provide backhaul links to mobile carriers. The traffic is transported on the same fiber that transmits traffic from landline carriers.

The Functions of Radios and Modems in Mobile Networks

Every wireless device contains a radio. Radios in mobile networks extract radio frequency signals from the air and convert them into small bits of frequency compatible with the devices. The radios then hand off slices of bits of data to modems within devices. At the transmitting end, radios convert signals to the frequencies used in the cellular network, and then transmit these wireless signals over the air.

At the receiving end, modems remove noise caused by interference and decode the radio frequency data signals into those compatible with the landline network. If the amount of noise is so great that the signal can't be decoded, the modem requests that the base station retransmit the signals. Removing the noise from signals is the most complex function in modems. At the transmitting end, modems encode (modulate) the signals to make them compatible with the radio frequency wireless network. Modems also add encryption at the transmission end for protection from eavesdroppers.

Elements of LTE Infrastructure

LTE has a simplified infrastructure and cell sites with fewer pieces of equipment to manage than early generations of mobile protocols. Moreover, LTE software and hardware can be installed on standard computer platforms so that carriers can choose from a wide range of equipment manufacturers. LTE cell sites also support more users per cell site than 3G technologies because the air interface is more flexible and uses spectrum more efficiently. See Figure 7-6 for LTE architecture.

The elements of LTE Networks are:

- The RAN is the only wireless part of mobile networks. This is the link between the user device and the antenna or tower. A base station located adjacent to the tower or antenna is dubbed an e-NodeB.

- The backhaul "hauls" traffic to the core from the RAN and vice versa. It is made up of fiber-optic cabling or high-capacity microwave.
- Fronthaul is the fiber link between antennas in Heterogeneous Networks (HetNets) LTE and 5G architecture in which small cell sites are linked to larger macro cells with fiber. The fronthaul is the fiber linking the small cells to the macro cell within the same area. These cells are controlled by base stations at the macro cell site. See the section "Heterogeneous Networks—Architectures for Densely Trafficked Areas" later in this chapter for information on HetNets.
- The evolved packet core is the mobile providers' data center with routers and software for signaling systems to manage mobile traffic and identify cell phones' owners
- Transmitting traffic to the other networks
- Converting mobile traffic to be compatible with wired networks
- Billing and tracking
- Tracking roaming by users
- Tracking and identifying applications using Deep Packet Inspection, which identifies bits inside packets

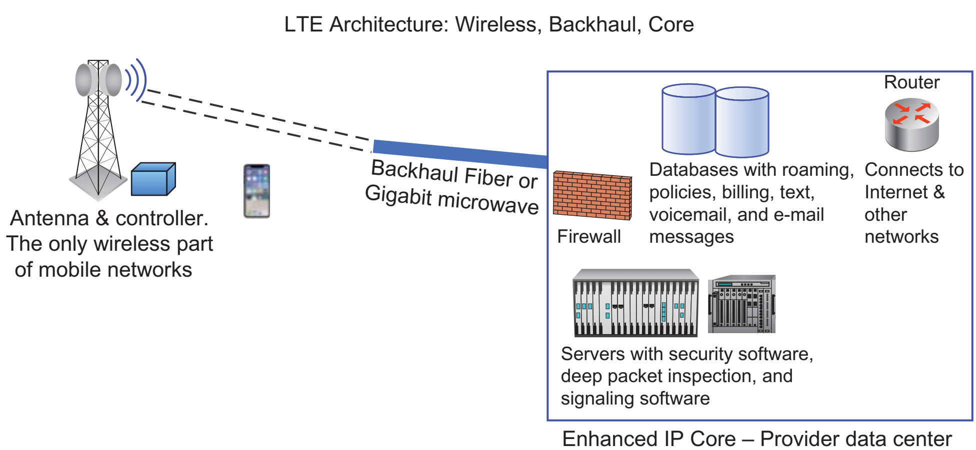


Figure 7-6 LTE architecture.

Location Indicators—Signals between Handsets and Mobile Switches

A mobile handset is essentially a radio that can be tuned to particular spectrum bands (frequencies). In order to operate in a particular area, mobile devices must have radios capable of being automatically tuned to the same spectrum as that of the radios in cell sites' base stations. In addition, each carrier must authorize every mobile handset before it's allowed on the network.

Mobile devices constantly send out signals to the nearest mobile company's switch, essentially notifying the switch of their location. For example, Verizon has five major switches in the New England states that receive signals from Verizon mobile devices. Fiber-optic cabling connects each of these switches to cell sites at the mobile carrier's towers, which tracks cell sites. The signals carried over this fiber cabling indicates each mobile handset's cell site and tower location. Moreover, each new tower is tested before it is "turned up" to ensure that the nearest 911 call center can be reached when users dial 911 when they are within range of the cell site.

NOTE

Mobile switches and the large amounts of fiber-optic cabling are critical parts of all mobile networks and they all depend on power to operate. Mobile networks are not immune to power outages caused by storms and natural disasters. Lightning strikes and snow emergencies are particular challenges because they can knock out electricity to switches and cell sites. Outages can occur at cell sites not equipped with a back-up generator. Not all carriers have adequate backup. Some have battery backup for momentary power glitches and short outages lasting only a few hours. Adequate backup is a growing challenge because of the increased number of small cells and natural disasters.

The Three Elemental Functions of the LTE IP Core

The LTE IP Core functions as mobile providers' data centers. Traffic from hundreds of cell sites passes through a mobile carrier's core network. Signaling gateways that translate protocols for 3G networks are located in the core along with 4G equipment. The LTE core network, also referred to as the *evolved packet core*, routes this traffic to data networks, the Internet, other mobile carriers, and other cell sites within the carrier's mobile network. Equipment and software located in the core also perform signaling and tracking calls for billing purposes.

A key factor in improved functioning is LTE networks' flexibility in handling voice and data is the fact that signaling messages are carried separately from user data and IP voice. Signaling messages are used to keep track of usage, perform security functions (to keep the network free from hackers and malware), authenticate users, setting up a session (voice, data, or video) and enforce policies. Policies include rules on the number of bits included in various data plans. Signaling enables carriers to monitor this volume so that a message can be sent to the user's device, notifying him that he has used up his planned quota and will be charged extra for additional transmissions.

Functions within the LTE evolved core network are divided into three functional elements. The evolved packet core contains servers for managing these elements. Two elements, the *Serving Gateway* and the *Packet Data Network Gateway*, are generally located in the same router. The functional elements making up the LTE's IP core are as follows:

- **Mobility Management Entity (MME)** This performs the signaling functions in the IP core. It sends and receives signaling information needed to set up, bill, and address calls to the eNodeB and to the Serving Gateway. In addition, the MME contains the security protocols for authentication and authorization.
- **Serving Gateway (SGW)** The SGW forwards the data and voice packets on bearer paths between the eNodeB at the cell site and the Packet Data Network Gateway. Bearer paths carry the actual user IP data. The SGW handles the protocol conversions between LTE devices and 3G systems and relays this traffic to and from the Packet Data Network Gateway and earlier- or later-generation gateways.
- **Packet Data Network Gateway (PGW)** This interfaces with the public data network (the Internet and carrier private data networks). It additionally allocates IP addresses to user devices and is responsible for policy enforcement. It can classify packets as requiring Quality of Service (QoS). It also generates usage records that it sends to the carrier's billing system, indicating levels of customer voice and data usage. The PGW has links to the roaming database for functions related to roaming and billing roaming traffic.

The PGW and SGW transmit mobile traffic to the Internet and other data networks. 3G traffic is handed off to these LTE gateways by earlier-generation controllers and signaling gateways. Note that Voice over LTE is outside of the evolved packet core.

Databases in the LTE Evolved Packet Core

Gateways in core networks connect to a variety of databases that support roaming, billing functions, voice messaging, and text messaging services. The following is a listing of key Evolved Packet Core databases in core 4G networks:

- Home Subscriber Services (HSSs)—Keep track of roamers' locations and temporary records of roaming subscribers' devices. Store telephone identities and authentication codes for digital phones. Perform security functions including authenticating that users are subscribers.
- Messaging center databases and processors—Handle text messages. Also store multimedia messages including voicemail, facsimile, and e-mail.
- Policy and Charging Rule Function (PCRF)—Contains QoS parameters and details of each subscriber's plan. A Traffic Detection Function enforces these Policy and Charging policies. The PCRF sends information to the Packet Data Network Gateway, which then forwards traffic to the Internet and broadband networks.
- Billing databases—Contain specific information on contract terms for each subscriber. The Packet Data Network (PDN) transmits usage records to the PCRF, which is connected to billing software.

In addition to above databases and functions, there are security applications in the evolved packet core. This may include firewalls that screen traffic for malware. The firewall may be located in the cloud.

Voice over LTE—Packetized Voice

Voice over LTE (VoLTE) is an international standard for transmitting voice over LTE. VoLTE codecs digitize voice and put it into packets to be transmitted along with data and video. When LTE was first available, voice was carried separately on spectrum used for older protocols.

The 3GPP developed VoLTE as a standard way to transmit VoIP. The VoLTE protocol is tightly specified so that roaming and interoperability with earlier-generation networks are possible. VoLTE is designed to interoperate with Internet Protocol Multimedia Subsystems (IMS). IMS enables applications for voice, video, and online games to be stored, billed for, and accessed on a common IP platform. See below for IMS.

Advantages of VoLTE include:

- Higher-voice quality equal to that of calls made from landline phones
- High-quality video calls
- Efficient use of the same spectrum for voice, data, and video
- A standard way of handling voice
- Faster call connection times
- Support for E-911 calls
- Spectrum previously set aside for voice can be re-used for other services

Simultaneous Voice and Data

The VoLTE protocol specifies that the same device can be used for voice and Internet access simultaneously. Prior to the advent of VoLTE, when a user received a voice call, her data connection was dropped. With VoLTE, someone using her device to browse the Internet, can answer a phone call without dropping her data connection. This is also true when a subscriber is on his phone and he looks up the weather forecast or checks his phone's calendar without dropping his voice call.

Using High-Definition Voice to Improve Quality

Voice quality on LTE has dramatically improved from that of previous mobile generations. This is due to improved codecs that compress and decompress analog voice for transmission on digital data networks. The VoLTE standard specifies improved noise cancellation. Noise cancellation distinguishes between voice and background noise and removes the noise so that voice is clearer. Matching codecs are required in the handset and in the network.

High definition voice supports higher and lower frequencies than previous mobile protocols. See Figure 7-7 for voice frequencies on VoLTE. High frequencies up to 7000Hz (think sopranos) are not cut off, and neither are lower frequencies down to 50Mz (think bass sounds). This results in clearer sounds in noisy locations. In short, users in noisy locations can hold clearer conversations on their LTE and 5G smartphones.

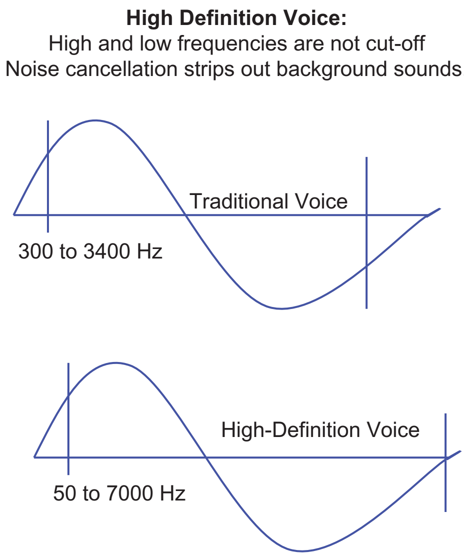


Figure 7-7 *Voice frequencies on VoLTE (high-definition voice) compared to those without VoLTE.*

Accessing Applications and VoLTE—The IP Multimedia Subsystem

IP Multimedia Subsystem (IMS) is a 3GPP open-standards architecture made up of multiple protocols and standards by which customers can access applications from many types of mobile devices. These applications include unified messaging and multiplayer games that are installed in a provider's network-connected platform. The signaling and control of IMS services are built around session initiation protocol (SIP), which is the signaling protocol used on IP networks such as the Internet for transferring traffic between carriers and for linking enterprise sites to IP networks. SIP signaling is used for functions such as setting up a video session (a call), tearing down the session, carrying numbers dialed and mobile devices' identity. For information about SIP, see the section "Session Initiation Protocol—Out-of-band Signaling" in Chapter 6.

VoLTE is based on the IMS, IP Multimedia Subsystem standard. IP IMS is access independent. See Figure 7-8 for IP Multimedia System. Access independence refers to the fact that subscribers, for example, on Gigabit Ethernet, any mobile protocol, Wi-Fi, or cable modems can access IP-based applications such as video calling or chat services on the IMS network. In contrast to IMS's goal of universal access, specialized services such as WhatsApp and Tencent's Chinese Weixin—We chat in English—IMS is meant to be globally interoperable on carriers' networks and not part of a closed network.

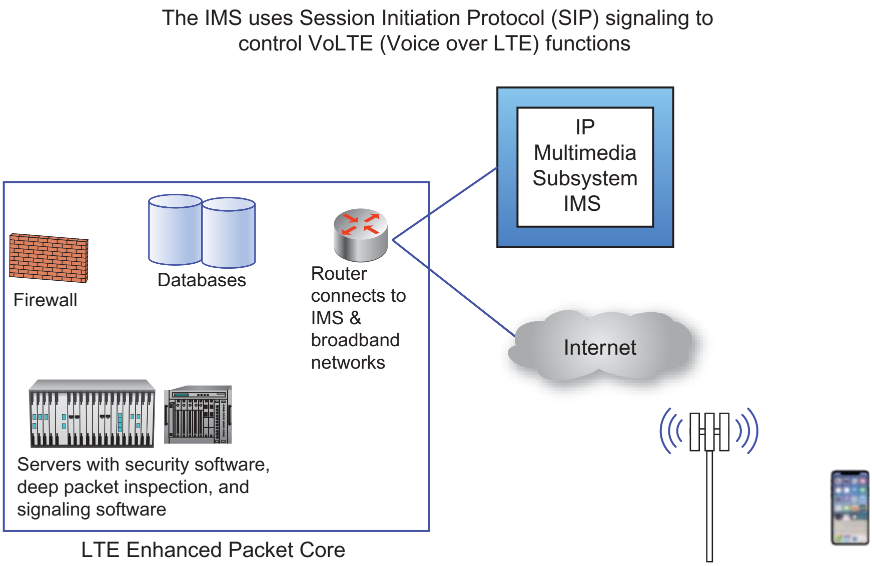


Figure 7-8 *IP Multimedia Subsystem (IMS) for mobile subscribers. A Session Border Controller converts signals from the mobile network to those compatible with VoIP equipment.*

IMS is based on IP protocols. Interoperability and control of sessions in interactive online games, conference calls, instant messages, and so on are managed in Session Border Controller (SBCs) and signaling gateways. SBCs are located at sites where carriers connect their IP networks to one another. These controllers have functions such as security, session management, policy control, and address translation. Policy control refers to the ability to prioritize certain traffic based on agreements between carriers.

The following is a sampling of applications that users can access from both mobile and landline devices:

- Presence so that subscribers are able to determine if friends and colleagues are available online
- Advertising that works across wired and wireless platforms
- Gaming so that users can participate in online games together
- Text messaging
- Video calling

Connections to Customers and Mobile Networks via the Cell Site, Towers, and Mobile Switches

A cell site is the physical area in which a set of frequencies is used. The link between users' devices and towers or antennas is the only part of mobile networks that is always wireless. The increase in data traffic in shopping malls and downtown areas with heavy pedestrian traffic areas requires dense arrays of cell sites.

The air interface between mobile handsets and equipment at antennas and towers are the only parts of mobile network that are wireless. The air interface is the wireless link between the user device and the equipment at the cell site's tower or antenna. The base station at the tower or antenna contains a radio that receives and transmits mobile traffic and amplifies (strengthens) signals. It also transmits traffic to other antennas and performs the conversion of signals between over-the-air radio frequency formats such as LTE to those compatible with landline networks, and vice-versa on the traffic between the backhaul and the base station.

REITs—A Way to Finance New Antennas and Towers

Companies such as Crown Castle and American Tower specialize in building towers and antennas. They don't offer cellular service; they lease space on their towers to mobile carriers who use the land around the towers for cell site equipment. Instead of each mobile carrier owning their own tower, these third-party companies build towers and lease shared space on them. For example, a large operator might lease space on a tall water tower for its antenna and land surrounding the tower for ancillary equipment. Carriers often share space on these towers to save costs.

Crown Castle and American Tower are structured as real estate investment firms (REITs). With REITS, outside investors underwrite tower construction by purchasing the land on which the towers and cell sites are located and leasing the space back to American Tower and Crown Castle. In return, Crown Castle and American Tower provide investors a stream of payments from their subsequent profits providing shared space on their towers to mobile carriers. Some mobile carriers including Verizon build their own towers or hire contractors to build them.

NOTE

Cell sites are the costliest part of mobile networks because there are large numbers of cell sites in 4G and especially in 5G networks. These steep costs make it challenging for all but the largest mobile providers to build out their networks for use with new generations of mobile protocols that require many more cell sites because of their use of high-frequency, gigahertz spectrum bands and the increases in the amount of data and video traffic.

In addition to the high costs of operating cell sites, mobile providers manage huge wired networks made up principally of fiber-optical cabling and some microwave links. These links connect RAN traffic to:

- Backhaul between the evolved packet core, which is a mobile carrier's data center, and cell sites
- Other cells in the mobile network
- Other mobile networks
- The Internet
- Enterprise broadband networks

Heterogeneous Networks—Architecture for Densely Trafficked Areas

Heterogeneous Networks (HetNets) is a 3GPP architecture that defines the way small cells connected to each other support mobile networks in areas with dense pockets of traffic. It is a network made up of a mix of different types of base stations and antennas, thus the term heterogeneous networks. Often these are in downtown areas in cities with large numbers of pedestrians, office buildings and apartments. HetNets are suited to handle the increasingly bandwidth-intensive traffic such as streaming video and online games. HetNets were developed to add capacity for the growth in data and video usage, not to expand coverage. HetNets are used in both LTE and 5G networks.

Capacity is important at the edge of cells where performance may degrade as traffic is handed off between cells. The main issue at the cell edge are delays when calls are handed over to adjacent cells. HetNets are additionally suited to the increasing use of high-frequency gigahertz spectrum used because gigabit spectrum is capable of handling increased traffic. However, gigabit frequencies only travel short distances before fading, thus more small, low-powered cell sites are needed to support traffic over gigahertz spectrum.

Characteristics of HetNets

HetNets are made up of large numbers of small cells controlled by larger *macro cells* to which they are connected wirelessly or by fiber-optic cabling. HetNets' low-powered cells have smaller antennas, and fewer macro cell sites with towers. The architecture includes larger macro cells that each control small cells as required by locations of dense traffic. See Figures 7-9 and 7-10 for examples of HetNets architecture.

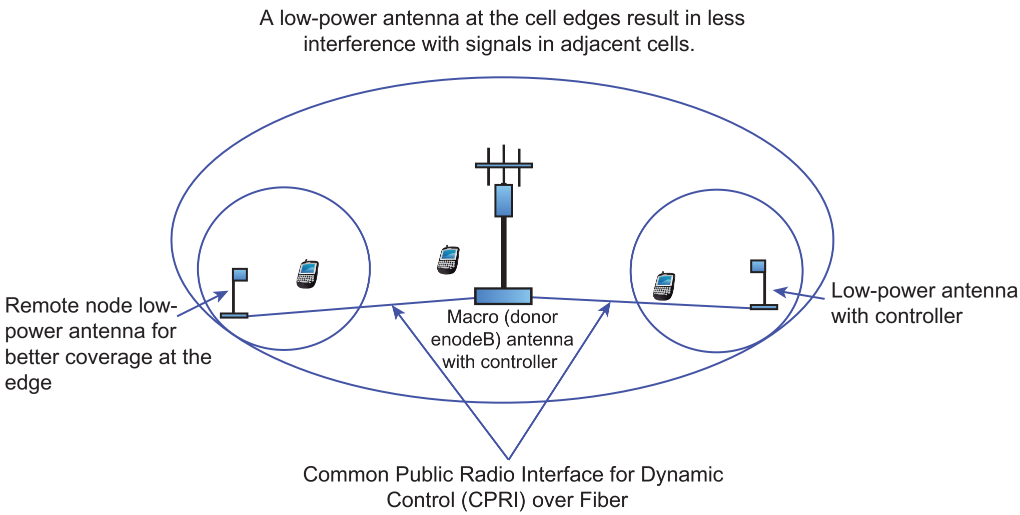


Figure 7-9 *An example of HetNet architecture.*

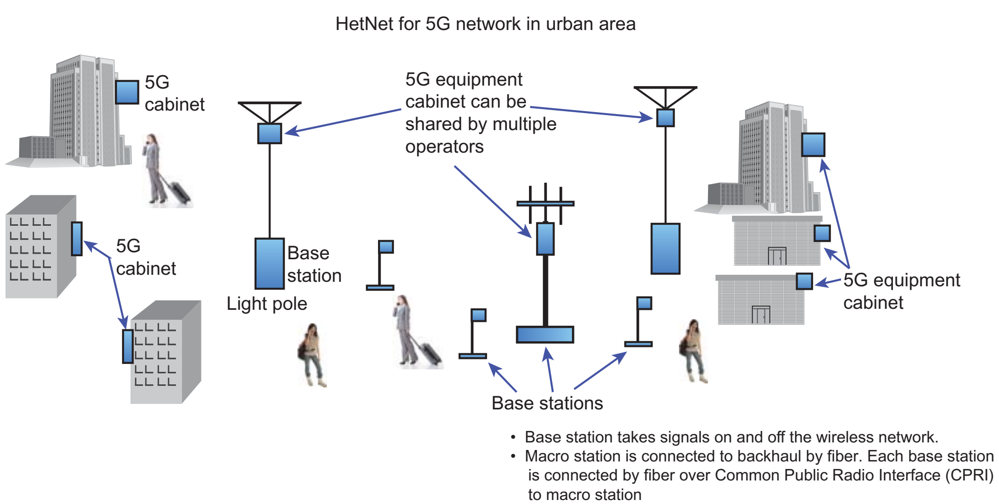


Figure 7-10 *HetNet architecture for 5G networks. (Stock photo by Chun-Tso Lin/123RF [center] and Thomas Northcut/Getty Images [left, right])*

Equipment in HetNets—Small Low-Powered Base Stations

HetNets are made up of small low-power cells. Low power results in decreased areas of coverage at each cell. Low power is important in HetNets because it is less likely to cause interference with frequencies in nearby cells. Low-power signals are not carried as far as those at higher powered cell sites. In HetNets, the macro evolved NodeB (eNodeB) provides the radio in a large cell while a low-powered macro eNodeB is in a small cell.

The following are low-powered base stations used with existing *macro* evolved NodeBs. Macro cells cover larger areas and can be connected to towers, rather than the smaller antennas seen at low-powered small cells. Macro and small cells are connected to each other either by fiber-optical cabling or mobile frequencies.

- Remote Radio Heads (RRHs) are small antennas and base stations located on outdoor furniture such as thin light poles, telephone poles, and the side of buildings.
- Micro Evolved eNodeBs (eNBs) are smaller eNBs controlled by macro eNBs
- Home eNodeBs (HeNBs) are small cells used for coverage indoors in a closed service group within, for example, office buildings. HeNBs are also termed Femtocells.
- RNs (Relay Nodes) cells are Pico cells that serve smaller groups than femtocells. These are also in a closed service group within buildings.

In addition to the above base stations, HetNets are made up of:

- *Macro cells* control traffic to small, remote cells
- Fiber connections between the small cells and to macro cells over the *CPRI* (*Common Public Radio Interface*). CPRI is a specification for carrying traffic between small cells and to macro cells. It was developed by the following consortium of mobile equipment manufacturers: Ericsson, NEC, Alcatel Lucent (now part of Nokia), and Nokia. It was intended as a replacement for coaxial cabling.
- *Backhaul* fiber-optic cabling where aggregated traffic from multiple macro cells is transmitted to the mobile core. Backhaul traffic may also be carried on high-capacity wireless radios. Higher capacity radios are available that support full duplex Gigabit Ethernet at 10 Gbps. In duplex services, sending and receiving signals are sent simultaneously over the same channels.

A Deeper Dive into HetNets—Pico and Femtocells

Pico and femtocells are small cell sites installed in residences, enterprises, arenas, and outdoor areas within buildings to improve cellular reception. Femtocells cover larger areas and can handle more users (about 100). Pico cells are used in smaller sites such as homes with fewer users than femtocells (five or six users). Both technologies provide relatively low-cost ways to add coverage inside buildings and outdoors. Building owners rely on carriers to provide pico and femtocells because only carriers have rights to spectrum used for mobile services. Femtocells can cover about 5,000 square feet and pico cells about 2,000 square feet. Like traditional base stations, pico cells support multiple standards LTE and 5G networks as well as multiple frequencies.

New buildings that require coverage often use Wi-Fi rather than pico or femtocells within office buildings. The Wi-Fi service is connected to the LAN, which links Wi-Fi traffic to the external broadband network. This eliminates the need to coordinate installation with a mobile carrier to access their spectrum. Staff with cell phones can now enable voice over Wi-Fi to use their smartphones for voice calls as well as data.

Mobile providers and tower companies install pico cells that are used for outdoor coverage. They can be attached to telephone poles, thin poles, and multistory buildings in densely populated areas with high concentrations of mobile traffic. This solution is an inexpensive way to gain capacity by reusing a carrier's spectrum within a smaller area than that covered by larger *macrocells*. A macrocell site is a cell site with a larger antenna and a controller that covers a larger area and can handle more traffic. Pico cells require local electricity and connections back to the mobile carrier's equipment.

Femtocells and Pico Cell Gateways

Femtocell traffic within buildings is routed within secure, encrypted software tunnels over a customer's broadband connections to a carrier's data center. At the data center, femtocell traffic is routed to a gateway. The gateway removes the surrounding bits in the tunnel and sends the femtocell traffic to the carrier's core network. The gateway transmits traffic from thousands of femtocells either to the Internet or, for voice calls, to the mobile switching center.

A key enabling technology that makes femtocells and pico cells feasible are the software algorithms that detect signals from macrocells. Traffic at the edge of the cell has the potential to interfere with frequencies in macrocells because signals can "bleed" into surrounding areas. Improved software algorithms in femtocells and pico cells have the capability to sense both the frequencies and the power levels in the microcell and adjust them as required so that the femtocell signals don't interfere with the macrocell traffic.

Femtocells and pico cells can sense the radio conditions in adjacent cell sites before they start transmitting. This so-called "Network Listen" scan enables the femtocell to, for example, raise its power if the signal from the surrounding macrocell is strong, or conversely, reduce its power if the signal from the macrocell site is weak.

This decreases interference and improves voice quality and data speeds for mobile users in the vicinity—both those served by the femtocells as well as those in the surrounding macro network.

Cellular on Wheels—Short-Term Coverage for Sporting Events, Concerts and Natural Disasters

During a sporting event or concert that attracts thousands of people, mobile carriers often bring in temporary service in the form of Cellular Service on Wheels (COWs). COWs are also deployed during natural disasters such as earthquakes, or hurricanes that may knock out cellular service. COWs are trucks equipped with antennas and base stations that can be quickly deployed.

However, for COWs to be effective, roads must be passable for the truck with the COW to reach hard-hit areas. This is a problem during natural disasters when roads may be washed out or made impassable, as occurred in the aftermath of the 2018 hurricane in the Florida panhandle and Gulf Coast areas. Many sections of the fiber network connecting cell towers to the core cell network were also damaged. Repairing and laying new fiber is a time-consuming endeavor.

Using Distributed Antenna Systems for In-Building and Subway Coverage

Distributed Antenna Systems (DAS) are an alternative for coverage within buildings. DASs consist of *repeaters* connected to coaxial or fiber-optic cabling in buildings. A repeater amplifies cellular signals transmitted throughout buildings, subways, or stadiums by equipment that the cellular carrier supplies. Repeaters are located throughout the building and transmit Radio Frequency (RF) signals to the macrocell. Unlike super femto cells, they don't actually offload traffic from the larger cellular network because they are not capable of reusing spectrum. They are connected to building broadband services to offload traffic from carriers' backhaul networks.

DASs are also located in subway systems where traditional cell sites don't generally reach or provide adequate coverage. Municipalities negotiate contracts for carriers to install the cabling over which the repeaters are connected and the signals travel. The carrier installs antennas that provide the cellular signals. In some of these systems, particularly public spaces such as subways and airports, multiple carriers are connected to the DAS. This enables travelers and multiple mobile carriers' subscribers to use their mobile devices in these locations. An example of a DAS is the one installed at the Kinnick Stadium in the University of Iowa. In this DAS, fiber is used between repeaters, and coaxial cable is installed for the final 30 to 40 feet to antennas and base stations.

Building Out Mobile Networks without the Challenge of getting Permissions from Municipalities

Prior to 2018, arranging permission from municipalities to run fiber and place antennas needed for the thousands of new small cells carriers are building for HetNets in LTE and 5G networks was the biggest challenges in upgrading mobile networks. Rights of way for the increased fiber needed to connect small cells to macro cells were one issue. Another was zoning regulations and other permissions that often cause major delays in building infrastructure. Officials in cities with historic buildings were reluctant to have equipment mounted on them. In residential areas, neighbors don't want antennas near their homes because of fears that the radiation from antennas may be harmful. It took years to negotiate these issues with municipalities.

Running fiber required permission from cities to use their rights of way. In cities with fiber already running in conduits under the ground, mobile providers negotiate the monthly fees that municipalities charge in return for space to lay fiber within these conduits. In an effort to speed up the process, telecom and cellular firms lobbyed the FCC to issue rules that restrict local municipalities from oversight of 5G gear. In 2018 the FCC issued rules that eliminate the majority of these delays in getting permission to place 5G gear by restrictions on local cities and towns efforts to impose fees and zoning rules on 5G infrastructure.

Frequency- and Time-Division Air Interfaces in LTE

The 3GPP standards group has defined two different *air interfaces* for LTE. An air interface is the way signals are transmitted between cell sites and user equipment. The most common air interfaces are Frequency Division Multiplexing and Time Division Multiplexing.

Frequency-Division Multiplexing (FD-LTE) is the most commonly implemented air interface. FD-LTE uses one frequency band for down-link from the cell site to the user device and another set of frequencies on the uplink from the user device to the network.

Frequency-Division Multiplexing (FDM) requires paired frequencies, which means that one spectrum band is used for the downlink and another band is used for the uplink. See Figure 7-11 for an example of FDM and TDM. When mobile carriers that use FD-LTE acquire new spectrum, they obtain one band specified by the government for uplink service and a different band specified for downlink service. Most of the rest of the world, including AT&T and Verizon, have implemented FD-LTE.

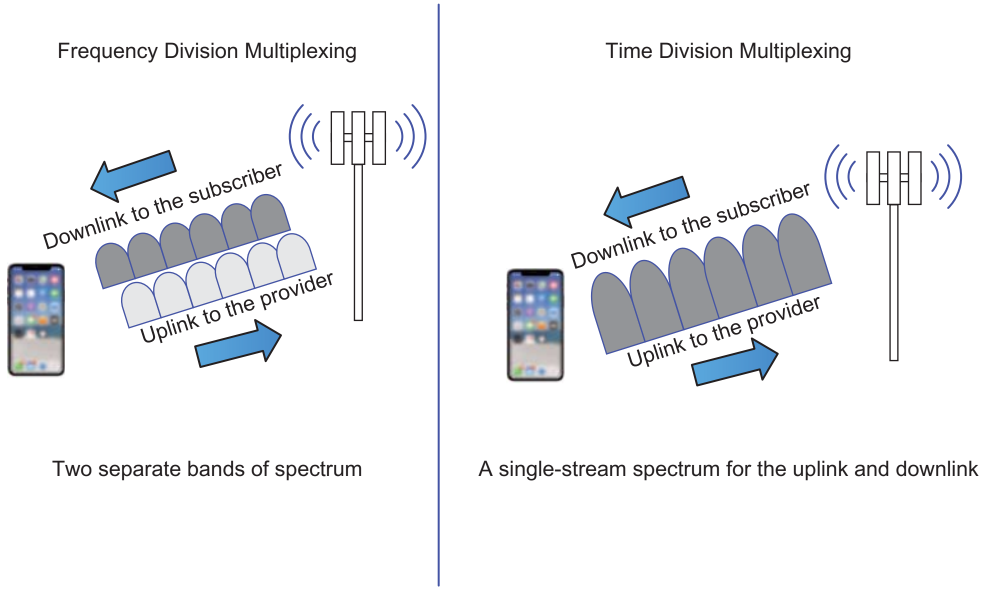


Figure 7-11 *Frequency Division-LTE compared to the Time Division air interface.*

In contrast to Frequency Division Multiplexing, TD-LTE uses the same set of frequencies for uplink and downlink transmissions. Time-Division Multiplexing (TD-LTE) is also referred to as Time-Division Duplex (TDD). TD-LTE does not require paired spectrum, and unlike FD-LTE, it is asymmetric; a different amount of spectrum can be used in the downlink and in the uplink. This is more spectrally efficient and flexible. For example, more spectrum can be allocated to the downlink than the uplink. China Mobile, the largest mobile carrier in the world, and some carriers in the rest of Asia use TD-LTE.

Core networks are the same for both types of LTE. The same network core and backhaul support both Frequency Division and Time Division air interfaces. However, radios in users' devices must have chips to match the type of air interface for their devices to access the cell sites. Chip designers have integrated both TD and FDD into their platforms so that carriers are able to support both types of LTE. Carriers able to support both FDD and TD-LTE support roaming for users with either type of handset.

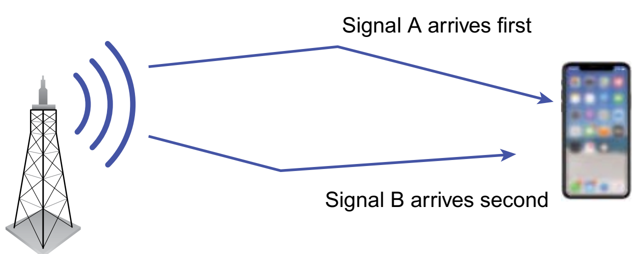
4G Multiple-Input Multiple-Output Antennas

LTE is designed to operate with Multiple-Input Multiple-Output (MIMO) antennas in base stations. MIMO antennas benefit by having more than one antenna and multiple receive/send channels. Thus, they can carry as many separate streams of voice or data as they have input/output channels. Each stream of traffic is carried on a separate frequency. An 8×8 antenna has eight antennas and handsets communicating with it also have eight antennas. This is analogous to multilane highways with eight lanes in each direction.

MIMO antennas are available in 2×2, 4×4 and 8×8 send/receive channels. The 8×8 antenna is specified for LTE Advanced, the 100Mbps, true-4G air interface. As antennas become more powerful, with additional antennas, it is technically challenging to equip handsets with multiple antennas because space is required between them to avoid signal interference. See Massive MIMO below for information on antennas suitable for 5th generation (5G) networks' high-frequency bands.

The LTE Orthogonal Frequency-Division Multiplexing Air Interface

Orthogonal Frequency-Division Multiplexing (OFDM) is the air interface used in LTE mobile broadband protocols. It is not used in earlier protocols and is an important factor in increasing capacity in mobile networks. OFDM increases spectral efficiency by sending several multiplexed streams of data over separate, narrow bands of spectrum simultaneously in orthogonal streams. Orthogonal streams are those that are transmitted at right angles to one another. Figure 7-12 illustrates an example of orthogonal streams in OFDM.



- Multiple streams of data at slightly different frequencies arrive at their destination at different times
- Receiver decodes signal A and then signal B

Figure 7-12 *Streams of bits sent by using the Orthogonal Frequency-Division Multiplexing (OFDM) protocol.*

In addition, guard bands between each stream of data are not required, which is an important factor underpinning the spectral efficiency of OFDM. Guard bands are unused channels of spectrum that provide a buffer between streams to protect data from interference. Guard bands carry no data. This narrowband, efficient use of spectrum is the main reason why LTE supports many more users in each cell site than the 3G technologies.

> NOTE Throughout this book, the term “carrier” has been used almost exclusively in relation to network service providers. However, as it applies to telecommunications, the term actually has two meanings. Thus, in addition to describing a network service provider, it can also refer to slices of spectrum as it does in Orthogonal Frequency-Division air interfaces.

A Variety of LTE Flavors

The evolution of LTE includes technical standards approved and developed by the 3GPP 3rd Generation Partnership Project, a worldwide technical standards group made up of representative of telephone companies from all over the world. See Table 7-2 for LTE types. Some are being implemented on shared Wi-Fi spectrum and others are based on high-frequency Gigahertz spectrum. Data on Gigahertz spectrum is able to travel only short distances before fading. However, it supports higher data rates.

Table 7-2 LTE Types

Name of LTE	Use of LTE	Spectrum Type	Other info
LTE A (Advanced)	Aggregates multiple spectrum streams into a single high-capacity stream	Most spectrum bands	Combining (aggregating) multiple streams of data to achieve more capacity in the air interface.
LTE LAA (License Assisted Access)	In tests to use 5 GHz unlicensed spectrum bands	5GHz	Used in small cells to increase LTE availability.
LTE U (Unlicensed)	LTE used in unlicensed spectrum In tests for this spectrum for added capacity	1.710–1.755 and 2.110–2.155GHz 5 GHz	Wi-Fi providers are concerned about interference from Wi-Fi networks in the same spectrum.
CBRS Citizens Band Radio Service	5G Fixed Wireless service for rural broadband access	3.5GHz	Uses different spectrum from 27MHz used by truckers to communicate with each other.
LTE Cat-MI & M2	Computer chips for enhanced machine to machine* communications	Various spectrum bands previously used in 2G networks	For low-power, low-bandwidth applications where batteries last 5 to 10 years. May be replaced by NB-LTE. In tests for Internet of Things applications.

Name of LTE	Use of LTE	Spectrum Type	Other info
LTE–NB LTE Narrow Band	May replace LTE Cat-M1 and M2	Spectrum previously used in 2G Networks	Internet of Things, e.g. remote meter reading.
LTE C-RAN Cloud Radio Area Network**	The core is managed from the cloud. LTE is at the cell site.	2.3GHz, 2.5/2.6GHz, and 3.5GHz, Verizon testing CRAN in 28GHz and 39GHz bands	Remote management at telecoms' cloud-based data centers. Billing and other functions in cloud.
VoLTE Voice Over LTE	A way to transmit voice in the same format as data, in IP packets	Uses the same spectrum as the LTE network on which it's transmitted	Depends on a type of SIP signaling in each carrier's IP IMS

**Machine-to-machine services include monitoring of automobile and truck fleets, alarms, and electric meters.*

***Can also refer to centralized Radio Access Network in heterogeneous networks. See above for HetNets.*

5G MOBILE NETWORKS—SMALL CELLS; ADDITIONAL CAPACITY

Fifth Generation protocols support gigabit data rates that are key to carrying the massive amounts of future streaming, gaming, and Internet traffic from mobile devices. Most mobile providers are now testing 5G networks, which will be available in a limited number of areas in 2019 with predictions of wide availability in 2020.

Massive MIMO Antennas for 5G Networks

The 5G specification includes *Massive MIMO* antennas, each with 16×16 send/receive channels. In addition to more send/receive antennas, massive MIMO antennas can handle traffic in a 360-degree pattern: a full circumference of the antenna. Thus, in addition to handling 16 send and 16 receive streams of traffic, massive MIMO antennas provide service to traffic in all directions of the antenna, in 360 degrees.

5G New Radio Service and 5G Applications

Fifth Generation NR (New Radio) will be one of the first types of 5G service available. 5G NR will be used over high frequency 28GHz and 39GHz spectrum capable of transmitting gigabit data rates. These high data rates are made possible by aggregating carriers (channels) together. AT&T and others are now testing applications on 5G NR. One future use is for controlling applications within cities to manage operations, including traffic congestion. Other applications envisioned on 5G are self-driving cars and trucks, the Internet of Things, and monitoring healthcare patients wearing wirelessly connected devices including blood pressure monitors.

C-RAN Centralized or Cloud-Based Radio Access Networks in 5G Networks

C-RAN in 5G networks refers to the management of the radio access network's antenna, and controller centrally. C-RAN management is already occurring where mobile network providers manage multiple HetNets and traditional cell sites from within their data center. The signals that enable centralized management are transmitted over fiber-optic links from macrocells. These signals are monitored by engineers at computer screens at data centers. Cloud C-RANs are in the early stages of implementation and are planned for the future as a way to manage the complex 5G infrastructure. Because there is no agreed-upon standard, equipment from different vendors might not be able to interoperate. Cloud RANs will additionally use virtualized components for ease of replacement and space conservation. The radio access networks will consume less space because they will be represented in software, not hardware.

Interoperability and Fall Back on 5G Mobile Networks

A major concern around 5G networks is that different telecom companies' implementations may differ in small ways. This can result in non-interoperability between their networks. Thus, data and voice traffic might not be seamlessly transferred between providers without dropping calls or causing delays in data sessions.

Another feature that needs to be compatible between mobile networks is fall back. Fall back is the ability to transition to earlier generations of service as subscribers move from cell site to cell site. A subscriber that starts a call in a part of the network already using 5G service needs to be able to continue the data session, voice call, or Internet browsing when they walk or ride to an area with LTE service. All of these and other facets of compatibility are in the process of being ironed out. But, earlier network implementations may hit some bumps.

Device Compatibility—A Multi-Year Gap

A major issue in upgrading from LTE to 5G is when 5G-compatible smartphones, tablet computers, and laptops with 5G radios on chips in the device will be available.

Without 5G chips in mobile devices, they aren't able to achieve gigabit data rates or any other features available in 5G networks.

This is the reason that cellular providers continue to support older mobile protocols when new ones become available. It can take 5 years for the majority of subscribers to upgrade to new generations of cellular service.

Killing Lost or Stolen Portable Computers Using GPS

A majority of security lapses can be attributed to the loss or theft of corporate laptops and smartphones. Confidential corporate information and private e-mail messages are often stored on these devices. Currently, mobile carriers have the ability to remotely disable and determine the location of mobile handsets, laptops with cellular chips, and tablets when corporations report them lost.

Global Positioning System (GPS) chips within these devices enable organizations to locate them so that data can be deleted, or the device can be locked. For the carrier to locate a device, it must be turned on and within the carrier's coverage area. Thus, if a device is turned off, it cannot be located.

Killing and locating lost devices is enabled in all current mobile networks. These networks depend on GPS to synchronize the timing in their networks so that signals arrive at their destination only once for functions that require precise timing. GPS-equipped mobile networks can be used to provide location information, as well. Location-based applications that use GPS include applications that give parents the ability to track their children's locations and to find friends who are in the area.

Pedestrian Injuries While Walking, Talking, and Texting

Walking while using mobile devices is a serious safety issue. The National Highway Traffic Safety Administration (NHTSA) estimates that 5,000 people were killed and 76,000 pedestrians were injured in 2016 while using mobile devices. Another problem with using mobile phones while walking is that distracted drivers using cell phones or even changing a radio station might miss a stop sign or just not see a pedestrian in a crosswalk. Injuries from distracted walking included bumping into someone else, tripping, sprains, broken bones, concussions, and spinal cord injuries.

A study published in Safety Science on February 2016 found that talking on mobile phones resulted in the most injuries. Texting and viewing content on mobile phones resulted in fewer injuries and listening to music had the least impact on walkers. To combat distracted walking, Honolulu imposes fines of up to $99 on pedestrians that text while crossing intersections. In Boston and New York legislators are studying the issue.

THE INTERNET OF THINGS (IOT)

Wireless networks have progressed from enabling people to speak together without being tethered to wires, to transmitting data at broadband rates, and now to machines autonomously communicating with each other via the Internet of Things. According to Verizon in their January 1, 2017, *Data Breach Digest,*

> *IoT, "the Internet of Things" [is] a term that describes a network of physical objects connected to the Internet. These may be discrete items like building automation solutions. Embedded in each device are electronics capable of network conductivity along with sensors or other features.*

Most IOT devices have embedded batteries on chips that operate over LTE–NB (narrowband) standard. Early implementations of IoT used LTE–M1 or M2, which required a gateway to translate between the network and the devices. The fact that LTE–NB does not require a gateway makes it less costly to manage and implement because there is one less piece of equipment to install and monitor.

Embedded software in IoT devices can be updated and monitored by centralized servers. Remotely monitored devices include automobiles, drones, parking meters, gas and electric meters, municipal traffic signals, water towers, and soil conditions and farms. A list of IOT applications are included in Table 7-3.

Table 7-3 Examples of IoT Applications

IoT Applications	Purpose	Comments
Self-driving cars, battery powered cars	Decrease congestion on city roads and air pollution	Improved batteries and Graphical Processing chips (GPUs) on which developers apply machine learning so that GPUs "recognize" road conditions, obstructions, and traffic signals. Nvidia computer chips have these capabilities.
Hybrid battery, Electric self-driving cars	Decrease air pollution; if battery not available car runs on gasoline	Graphical processing chips as described above.
Self-driving, battery powered trucks	Save costs on hiring drivers; fewer accidents	Trucks can travel for more hours because driver fatigue is not an issue.

IoT Applications	Purpose	Comments
Drones (unmanned aircraft)	Track wildfires and mudslides; Monitor soil conditions, and livestock on farms, military surveillance	An improved way to manage natural disasters and agricultural productivity; used to automate armies for attacks and reconnaissance.
Parking meters	Automate collection of parking meter fees	Save municipalities' expense of manually collecting coins in meters.
Industrial robots	Control manufacturing systems; speed up warehouse functions	Industrial robots are used in automotive plants and other manufacturing systems to speed up processes and save money on salaries
Subway fare collection	Transit passengers use payment software in smartphones to access subway trains	Diminish delays at subway entrances; lessen fraud; require less staff. Enabled by Near Field Communications (NFC), a low-power, short-range communications protocol.
Industry	Automate lighting and heating control systems; monitor manufacturing systems	Save costs on utilities and manage manufacturing quality.
Highway toll collection	Eliminate toll booths and traffic delays caused by manually collecting tolls	All cars need transponders that identify their license plate number for billing purposes.
Smart cities	Monitor traffic, water, and safety, elevated trams and underground high-speed transportation systems	Future projects aimed at making cities more livable with new types of off-road transportation to lessen traffic gridlock
Medical devices in hospitals	Automate data collection and inventory of equipment for more accurate data	Sensors on equipment identify each wheelchair and other equipment. Heart and blood pressure monitors send data and alarms to central computers and nurse stations.

Information and Privacy on IoT Services

With the millions of devices connected to the Internet using IoT LTE–NB in the future, major challenges will be keeping these networks secure and private.

Security in IoT Networks

There is no easy answer for securing Internet-connected IoT networks. Devices connected to the Internet are open and inherently vulnerable. The first step in ensuring security is to encrypt IoT information as it's transmitted. This ensures privacy. However, it doesn't mean that hackers can't disrupt services. Many organizations including major telecom providers such as Verizon Wireless are developing security protocols for Internet of Things networks.

Privacy on Connected Devices

In addition to security, IoT devices that collect data with identifiable information have the potential for companies to store vast amounts of private information about people using IoT equipment and other equipment that collects information about customers. Computers in cars are a prime example of equipment with the ability to collect information about where people drive.

This information and more like it provide data about consumers' buying habits as well as the routes they take. This information can help companies choose locations for billboards and retail operations.

Marketing companies sell this information and give a share of the revenue to car manufacturers: a lucrative opportunity for marketers and car manufacturers, a loss of privacy for consumers.

Unmanned Aircraft; Drones—Military and Commercial Applications

Drones are unmanned aircraft equipped with cameras and remotely controlled from the ground. Commercial drones can do more than deliver packages, which they are not suited for because most packages are too heavy for the lightweight, 55-pound drones. Drones are used in commercial and military applications. Some of these include monitoring combat zones for threats and enemies, and surveying natural disasters such as wildfires, mudslides, earthquakes, and hurricanes. In 2017's Hurricane Harvey in Puerto Rico, drones provided cell service. The drones were tethered to antennas and radios for temporary cell service and communications. The drones additionally captured images of oil damage and electrical outages. Movie directors and journalists use drones to record overhead views and difficult to reach high-altitude locations.

In the future it is likely that cameras within drones will transmit information to public safety officials. Thus, drones will track criminals so that helicopters won't be needed. Often helicopters crash during pursuits of criminals, killing or severely injuring pilots or even people on the ground. One of the security precautions being developed will track drones in restricted airspace such as military bases and commercial airports where saboteurs might launch drones to compromise safety in these areas.

Battery Life

Inadequate battery life is a major issue with smartphone and tablet computer owners, self-driving car and truck developers, and myriad other services that depend on battery life. Battery technology has not kept up with users' dependence on mobile services and development of new, automated technologies. People are more dependent on portable devices for their voice and text communications as well as social networking, music, and increasingly, for video. They also use these devices on Wi-Fi networks and for video conferences.

Data applications require more power from the device. Bandwidth-heavy applications such as Internet access, video, and e-mail drain batteries more quickly than voice calls. This is because voice requires fewer bits than data when transmitted. In addition, large color displays drain batteries more quickly than the less-sophisticated screens on earlier devices. Thus, as people become increasingly dependent on mobile devices for more functions, it is important to find ways to extend battery life.

A current focus is on ways to design mobile handsets that use power more efficiently. One such technology extinguishes screen backlighting when it is not required. The technology senses ambient lighting to determine when backlighting is needed. It maintains color by creating brighter color pixels so that mobile devices don't draw current from backlights in daylight.

Another way that manufacturers design handsets to improve power management is by including automatic sensing circuitry that shuts down memory, processors, and peripherals when a handset is not transmitting. For example, if the user is not in a Wi-Fi zone, the Wi-Fi circuitry is disabled so that it does not draw power when it can't even be used. Most smartphones and tablet computers include this form of power management. Other manufacturers are developing new screen technologies that consume less power.

More Convenient Way to Charge Batteries

Electronics companies have developed more convenient ways to charge smartphones. There are wireless charging devices on the market able to charge phones placed on top of them. So, instead of tossing a phone in a kitchen drawer or on a dresser in the evening before going to bed, users are able to simply place it on a small charging device and have a fully charged tablet or smartphone waiting for them in the morning. The charging device itself must be plugged into an electrical outlet.

Charging mobile devices gradually wears down the battery and shortens its life. Over time, batteries hold charges for shorter amounts of time. This is because every charge deposits chemicals on the device's contacts. These chemicals corrode the contacts creating resistance to the charge. A lithium-ion (Li-ion) battery experiences corrosion in a different manner, but it, too, becomes resistant to charges. Thus, less voltage reaches the circuitry that carries the current to the battery. Voltage refers to the "pressure" of the electricity flowing through the handset's circuits. Low "pressure" or voltage means that less electricity is reaching the battery.

People that need more battery power than that built into the phone purchase battery packs that clip onto their mobile devices or mobile phone cases already equipped with battery packs.

APPLICATIONS AND SERVICES

Applications on mobile devices attract customers, generate revenue, and are a tool for retaining customers.

Mobile Payments

Mobile handsets can be utilized for mobile banking, financial transactions, contactless payments at retail outlets, and instead of cash at subways and toll roads. These mobile payment options include the following:

- **Payments for mass transit** Users can pass their smartphone near a reader to pay for subway, bus, and train transportation instead of using tokens or purchasing monthly passes. Apps on mobile phones can take advantage of a short-range wireless technology called Near Field Communications (NFC) to interact with the reader. The user simply needs to pass her phone within 1.56 inches (4 cm) of the payment reader.
- **Check deposits** Smartphone apps use the device's camera to take a picture of the check and then transmit the image to the user's bank for deposit.
- **Money transfers directly to a mobile phone in a developing country** When a relative or friend sends money to a person in a developing country via Western Union, the electronic cash is sent directly to the receiver's handset. MoreMagic, a Massachusetts software developer, created this application.
- **Online payments** People surfing the Internet on their smartphone can make online purchases through PayPal rather than having to type in their credit card number along with their name, postal address, and e-mail address.

All of these transactions require some type of software platform that sits between credit card processing companies or banks and the mobile network. The platform must have integrated security protocols and the ability to communicate with the financial institutions that process payments. They also need to communicate with servers at merchants' sites and devices that act as "readers" of the mobile device making the transaction.

Each mobile handset and reader requires chips with NFC capability or special software. The cost of these readers is often a stumbling block for retailers because they need to place one at every cash register. Alternatively, readers can be embedded in portable devices that sales associates use to process credit card sales. Another challenge for retailers is that there is no agreed-upon standard software platform. Thus, different chips and software are required for Apple OS and Android operating systems because different carriers and mobile operating systems adopt different software.

Machine-to-Machine Communications between Devices with Embedded Radios

Machine-to-machine (M2M) mobile services refer to services that automatically monitor the status of other systems or send software updates to devices. An example of an M2M service is a central system that monitors vending machines remotely to determine inventory levels and diagnose possible problems. Another example of M2M traffic is automatic monitoring of residential electric meters.

Both of these applications require software platforms and radios at customer data centers as well as software and radios in the device to be updated or managed. Software is required in the vending machines and meters that are able to connect to a mobile network. However, these upgrades might require large investments. This is true when new software is added to a utility's meters. There is a potential to save on operational costs by eliminating the need for technicians to manually read the meters. It also has the potential to enable utilities to use energy more efficiently by monitoring the grid and adjusting power distribution accordingly.

These transmissions are carried over a mobile carrier's second-generation network. Many of the current applications do not transmit enormous amounts of data. M2M applications represent a revenue opportunity for mobile carriers. One reason is that there are many more machines than there are end users, and many machines now include software that can be upgraded for over-the-air diagnosis and updates.

Automobiles are examples of systems that contain more and more software, including in-car entertainment systems that require automatic over-the-air updates. Many new cars include options for touch screens on dashboards to activate various networked functions and entertainment systems. These include in-car Wi-Fi hotspots for passengers, outside sensors, rear-view cameras to assist in parking, and embedded GPSs.

Another advantage to carriers of M2M service is the ease of support. Currently, carriers operate large customer service centers for responding to questions about billing and technical issues. Customer service for M2M service is lower than that for handsets because inquiries and customer service requests are only required for the centralized staff members who manage these applications for customers.

Using Prepaid Mobile Services

Prepaid wireless services are those for which customers pay in advance for mobile voice and/or data services. Prepaid service is most widely offered to customers who do not have credit and who pay cash for service. They "top up" their service, making additional payments when they need more minutes.

This contrasts with the postpaid cellular model by which customers are billed for and pay for services *after* the end of the monthly billing period. In the prepaid model customers give providers a credit card number that is billed every month. Most mobile providers in the United States rely on postpaid customers for the bulk of their revenue, but many offer prepaid as a way to round out their offerings.

With postpaid plans, customers receive monthly bills and often sign one- or two-year contracts for their service. The consumption of prepaid service is particularly high in developing countries such as India, Bangladesh, and many African countries. Prepaid is important in areas where most people don't have credit cards or bank accounts.

The advantages of prepaid for carriers are mainly the elimination of the costs associated with issuing bills and collecting overdue payments. For some carriers, it's a way to attract lower-income or immigrant customers who don't have credit. In countries where mobile penetration is high and most people already have existing postpaid service, prepaid is another way to add customers.

Whether purchasing prepaid directly through a carrier or through a reseller, customers are connected to a prepaid platform, which authenticates their device and tracks usage to determine either whether to charge a credit card or if the subscriber's amount of time or usage has been used up. The prepaid platform is connected to the carrier's core mobile network. Wal-Mart sells prepaid services using Straight Talk's prepaid platform.

WI-FI STANDARDS, ARCHITECTURE, AND THEIR USE IN CELLULAR NETWORKS ....

Residential consumers and enterprise staff expect the same level of mobility within homes and work environments as they experience in mobile cellular networks such as those operated by Verizon Wireless and AT&T Mobility. Wi-Fi provides short-range wireless service within these locations. Wi-Fi networks are widely deployed in cafes, libraries, and municipalities as a service to customers and city and town residents.

The 802.11 Wi-Fi Standard

The designation 802.11 refers to the family of Institute of Electrical and Electronics Engineers (IEEE) standards around which most Wireless Local Area Networks are built. Wi-Fi, short for wireless fidelity, is widely accepted worldwide with small variations. Table 7-4 lists the earliest commonly installed 802.11 network protocols.

Table 7-4 802.11 Wireless Local Area Network (Wi-Fi) Standards

Standard	Top Speed	Achievable Speed	Number of Channels*	Frequency Band
802.11a	54Mbps	25Mbps	24	5GHz
802.11b	11Mbps	5Mbps	3	2.4GHz
802.11g	54Mbps	12- to 25Mbps	3	2.4GHz

**The number of channels varies internationally.*

A Deeper Dive into Wi-Fi Standards

The standards presented in Table 7-3 refer to the frequencies, speeds, and number of channels in each Wi-Fi standard. Other 802.11 standards that specify capabilities such as security, Quality of Service (QoS), and internetworking with cellular networks are listed in Table 7-8 in the "Appendix" section at the end of this chapter. Wi-Fi networks in enterprises commonly support all three of the standards plus additional standards that specify higher data rates.

The frequency of a signal impacts its range (how far it is able to travel). Signals in lower-frequency bands travel farther than those in higher bands because these waves are longer (refer to Figure 7-1). The 802.11b and 802.11g standards cover a range of about 100 to 150 feet; 802.11a covers only about 75 feet. Because they cover smaller areas, networks that utilize 802.11a antennas require more antennas. Equipment that supports both standards is referred to as dual-band equipment. As its name implies, dual-band equipment supports two frequency bands. Tri-band support is now common as well.

The higher speeds achieved by 802.11a and 802.11g are possible because both are based on Orthogonal Frequency-Division Multiplexing (OFDM). This is because OFDM sends multiple streams of bits simultaneously. See the section "The LTE Orthogonal Frequency-Division Multiplexing Air Interface" earlier in this chapter to read more about OFDM in LTE networks.

NOTE

In order for user smartphones and other devices to access any Wi-Fi standard, the user device must contain a computer chip that matches the 802.11 standard, e.g. 802.11a, 802.11n and 802.11ac as well as other newer Wi-Fi standards.

The following factors impact achievable speeds:

- Network congestion
- The distance from antennas
- Overhead, which is the number of bits required in packet headers for information such as addressing and error correction
- Interference from thick walls or other material and glare from windows are factors that can also decrease range

Worldwide, the number of channels available in each standard varies. When governments set requirements for the number of channels that can be used for each standard, they do not always do it uniformly. The standards themselves often define flexible requirements.

Range and Capacity of 802.11n

The 802.11n standard is a Wi-Fi standard that is backward-compatible with 802.11a, b, and g networks. It enables Wi-Fi networks to cover longer distances by overcoming a certain amount of interference. It also increases achievable speeds, increases throughput (user data minus packet headers), and supports more users per access point than earlier Wi-Fi networks. Improvements in the number of users supported in a given amount of airspace are critical as the number of users and applications on Wi-Fi networks increase. 802.11n and 802.11ac mentioned below operate on 5Ghz frequencies.

Using MIMO Antennas to Carry More Traffic

Improvement in antennas is the reason 802.11n and 802.11ac use spectrum more efficiently and overcome many "dead spots." A dead spot is an area that access points don't cover because of interference from building materials or the distance from an antenna. The 802.11n access points use MIMO antennas, which were not available in earlier Wi-Fi networks to simultaneously transmit multiple streams at different frequencies within a single channel. 802.11n is being replaced by the higher-capacity 802.11ac described below. Access points that support both 802.11ac and 802.11n are widely available. These are compatible with user devices with only 802.11n computer chips.

MIMO antennas are classified by the number of transmit and receive antennas installed within access points and user devices.

- 2×2 antennas have two transmit and two receiver antennas.
- 2×3 antennas have two transmit and three receiver antennas.

- 3×3 antennas have three transmit and three receiver antennas.
- 4×4 antennas have four transmit and four receiver antennas.
- 8x8 antennas have eight transmit and eight receiver antennas.

Wi-Fi routers with more antennas support more capacity and higher data rates. To achieve the highest speeds and capacity, user devices as well as access points must have an equal number of antennas. See Figure 7-13 for an example of a Wi-Fi access point.

Figure 7-13 *A Wi-Fi access point. (Courtesy of Linksys)*

The increasing capabilities of Wi-Fi networks have resulted in greater dependence on wireless networks. This is particularly true in mobile environments such as hospitals, factories, and educational institutions where employees often do not have a fixed desk at which to send and receive data. In addition, staff members in organizations now assume that they can take advantage of wireless access for tablets and smartphones during meetings, at lunch, and wherever they are within their building or within their organization's campus.

Multi-User MIMO—Improvements in MIMO

Multi-User MIMO (MU MIMO) supports transmissions to more than one user device at a time. Without MU MIMO, transmissions are sent to different devices serially, one at a time. MU MIMO antennas operate at the 5GHz bands of spectrum that support gigabit data rates. MU MIMO equipped routers are referred to as Wave 2 or Wave 3 equipment.

802.11ac (Wi-Fi 5) Gigabit Data Rates, Beamforming, and Bonding

The 802.11ac Wi-Fi standard, now dubbed Wi-Fi 5 by the Wi-Fi Alliance supports bonding, Multi-User MIMO, and gigabit data rates. 802.11ac supports *beamforming,* the ability to focus a signal directly to the end-user device rather than transmitting wireless signals addressed to a particular device in all directions at once. Beamforming transmits separate streams to individual users within the same spectrum. This decreases congestion.

802.11ac achieves high data rates in part due to its modulation, the way bits are carried on the wireless streams. 256 Quadrature Amplitude Modulation (QAM) carries many more bits by varying the amplitude, the height, of each wave in the data stream.

Channel bonding enables high data rates by combining multiple streams into a single stream. However, bonding channels together results in fewer channels available to other devices in the network decreasing capacity to other devices in the Wi-Fi network.

NOTE

An *extender* is essentially a repeater. It "repeats" signals to extend their range, the distance they can travel before fading. For example, if a home has two stories, but the router is on the first floor, the extender will connect to the home's Wi-Fi routers and send Wi-Fi signals to, for example, the smartphone in the office on the second floor. In this way, both end-user devices on the first and second floor have good access to the Wi-Fi network. Extenders plug directly into electrical outlets. They are not equipped to attach to cabling.

User Devices—Capacity Requirements

The growing numbers of connected wireless devices require high-capacity Wi-Fi. It's not uncommon for families and students to have a total of five devices connected to Wi-Fi networks. This is an issue in student apartments where each person may have their own four or five devices. Thus, Wi-Fi networks able to support increases in wireless traffic are becoming crucial. The following is a list of wireless devices commonly used in homes, universities, and enterprises:

- Laptops
- Desktop Computers
- Connected environmental controls
- Networked light switches
- Cellular modems

- Smartphones
- Tablet computers
- Televisions
- Set-top boxes connected to HDTVs for streaming TV and movies from the Internet, via, for example, Roku, Comcast's Xbox, and Apple TV set-top boxes
- Printers
- Low-power medical devices used to monitor conditions remotely; for example, blood pressure and glucose monitors

Wi-Fi in Universities, Hospitals, and Warehouses

Large universities, hospitals, and warehouses have extensive Wi-Fi networks because their staff for the most part aren't at assigned desks where they are able to answer telephone calls, or in medical settings where they can look up patient records and reactions to medication. In large university campuses with multiple classroom buildings, access points are placed on every classroom's ceiling.

Students at these universities assume Internet access is available for research on topics covered in classrooms, and for research in the library. At one large university, the library has two floors with books, and another entire floor with carrels where students and faculty study, do research, and access the Internet. Wi-Fi is additionally available for guests and neighborhood residents who are able to hop on a "guest" segment of Wi-Fi where they can reach the Internet, but not any private, confidential files or databases. In a similar manner, hospitals have Wi-Fi throughout their administrative offices and patient floors. Like universities, they provide guest Wi-Fi for visitors and patient rooms. In warehouses, Wi-Fi is used for communicating with automated systems that track packages.

Wi-Fi Architecture in Enterprises

Wi-Fi networks are within buildings but are connected by cabling to the wired LAN. All Wi-Fi networks have access points and user devices. The computer chips in portable user devices must be compatible with that used in the base station and access point. For example, a user device cannot use 802.11ac capabilities without an 802.11ac chip in their device. Enterprise Wi-Fi networks have multiple access points and often controllers that direct traffic to particular access points. Central monitoring software can be used to remotely change access point configurations and monitor traffic on the Wi-Fi network.

Wi-Fi access points are connected to switches in each floor's wiring closets. See Figure 7-14 for an example of a connection between access points and the wired local area network. The point is, Wi-Fi is a way to connect internal wireless transmissions to enterprise LANs, which then transmit Wi-Fi–originated traffic to the Internet or to staff within the building or campus. A Wi-Fi controller or router is plugged into a port on Ethernet switches at enterprises.

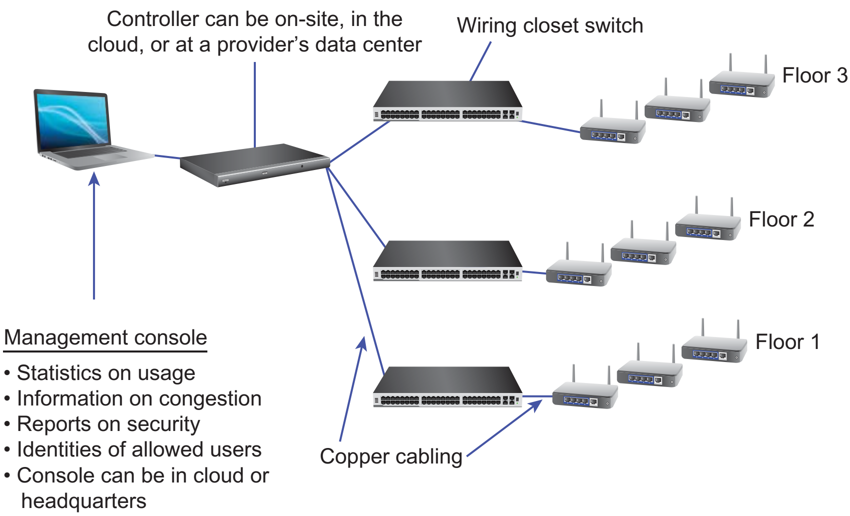


Figure 7-14 *Wi-Fi connections to the wired LAN in an enterprise's wiring closet.*

Wi-Fi in Homes

In a similar manner to enterprises, Wi-Fi access points connect to LANs within homes. However, LANs within homes are less complex and the access points are generally less robust, with fewer features and for the most part less complex security. In homes, Wi-Fi–equipped gear such as printers, laptops, and smartphones have internal Wi-Fi computer chips. The Wi-Fi router is directly cabled to cable modems or equipment associated with the fiber-optic cabling in the outside network.

Mesh Networks—Every Device to Every Device: Controller-Less Architecture

The main difference between centralized and mesh architecture is that in mesh networks traffic does not go through a controller. Rather, each access point has the intelligence to directly connect traffic to other access points. The software essentially establishes a point-to-point connection for the duration of the data session. It eliminates congestion at a central point while at the same time avoiding a single point of failure. If an access point fails, data is routed around the failure to another access point. The ability to route traffic around failures and coverage gaps and interference from thick walls or walls that contain wire, and large homes with three stories make them suitable for these environments and also for outdoor areas.

Moreover, access points in mesh networks filter out traffic from untrusted sources such as *rogue access points*. A rogue access point is an unauthorized access point installed by an employee. Figure 7-15 presents an overview of a Wi-Fi mesh network. In homes, people use a software app on their smartphone that is provided by their Wi-Fi vendor to set up the mesh network. The user selects a centralized location for the first access point and plugs it into power. The app then uses its intelligence to recommend locations for the other access points.

There is currently no mesh networking standard for all of the functions required in mesh networks. Thus, the entire network must now be provided by a single vendor. The current standard only specifies how the link layer puts the data on and takes it off the Wi-Fi network. A new certification program called *Wi-Fi Certified Home Design* is still evolving that may enable access points from diverse manufacturers to interoperate together. This will enable people and institutions to use equipment from different vendors to interoperate with each other.

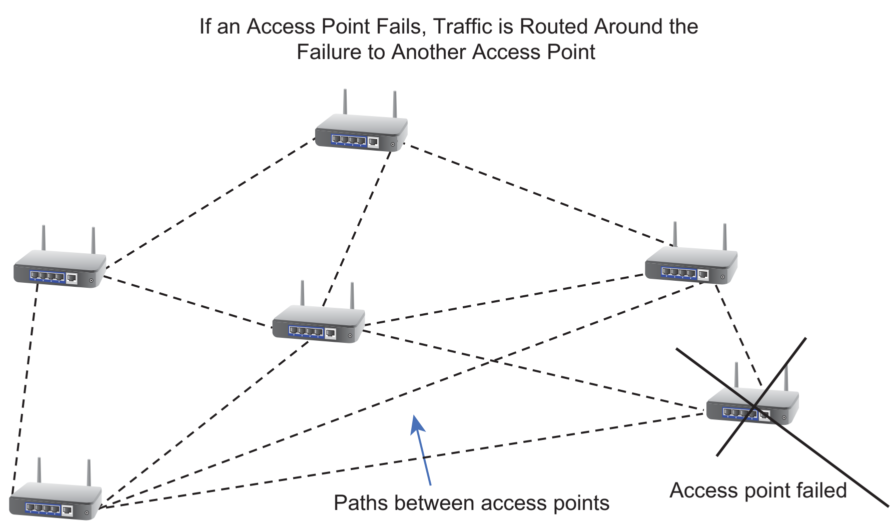


Figure 7-15 *An example of a mesh Wi-Fi network with every access point to every access point connection. (Courtesy of NETGEAR)*

Band Steering, Client Steering and Time Synch in Mesh Networks

Mesh networks include both band steering and client steering.

- In *band steering* the network is able to route the same traffic between 2.4GHz and 5GHz depending on band availability.
- *Client steering* connects clients (user devices) to the access point that has the strongest signal strength and the least congestion.
- *Time synch* is a Wi-Fi capability used in mesh networks to distribute and synchronize traffic. It enables clients to connect to multiple access points at the same time and an application in a server. Over-the-top streaming where speakers and audio are synchronized down to a microsecond so that characters' speech is coordinated with the way actors speak is an example of time synch.

Devices on Wi-Fi Networks—Access Points and Controllers

Access points translate between Wi-Fi wireless signals and Ethernet LAN signals and vice versa. An access point has an antenna and chips with 802.11a, 802.11b, 802.11g, and 802.11n, or 802.11ac protocols. Access points for the residential market also include routers with ports to which Ethernet cables are connected. The router aggregates traffic and sends it to the Internet via Gigabit Ethernet on fiber cable, or cable modems.

Access points for corporations are more expensive and feature-rich than those sold to residential customers. They contain higher-functioning security capabilities, such as intrusion detection and protection, the ability to detect hacker attacks, and Quality of Service (QoS) needed for voice and video. There are also robust access points for outdoor locations that are made to withstand harsh environmental conditions. For example, an enterprise might want outdoor coverage on a campus with multiple buildings. Each access point requires electrical power.

Cabling and Electrical Requirements

In a similar manner to cellular networks, all Wi-Fi networks require wired connections to switches, controllers and data centers, and electricity to power access points. Access points in organizations are connected to the LAN via a data jack and, from there, to unshielded twisted-pair (UTP) copper wire connection to the local wiring closet. Electrical and cabling requirements represent an often-overlooked cost in implementing Wi-Fi networks. The power each access point requires can be located remotely in wiring closets on each floor or locally by nearby electrical outlets. For local power, new outlets might be needed.

Wi-Fi Controllers

Non-mesh Wi-Fi in small and medium-sized organizations have controllers that manage access points and monitor the network. Non-mesh Wi-Fi networks require that traffic be routed through centralized controllers. The controllers are part of core switches or separate devices. If they are part of separate devices, they sit between the wireless and wired parts of networks. They are programmed with specifications of the level of access different staff are allowed. They act as gateways to the network, allowing access only to certain users. They often allow access to particular applications on a per-user basis. In addition, centralized controllers authenticate users and access points. Importantly, they can identify unauthorized rogue access points that staff may bring to work. They also pinpoint areas of congestion and gather statistics on usage into reports.

Cloud Service and Virtualization for Wi-Fi Management

Controllers can be installed as virtual entities represented in software on servers. This lowers the cost of Wi-Fi networks by eliminating a separate server and additional utility fees for air conditioning and electricity. This is often possible because more of the functions are distributed to access points rather than contained in central controllers.

Some Wi-Fi manufacturers provide an option called Software as a Service. This is a cloud offering in which the Wi-Fi manufacturer manages the controller and reporting functions at its own data center. For more information on cloud computing and virtualization, see the section “Computing and Enabling Technologies” in Chapter 1.

Securing Wi-Fi Networks—WPA3

The openness of Wi-Fi networks makes them vulnerable to hackers. Access points continually broadcast their network’s Service Set Identifier (SSID) and Wi-Fi devices respond to these broadcasts. These broadcast messages are vulnerable to eavesdroppers and can result in attempted and successful logons by unauthorized users. Unlike wired networks, there are no natural boundaries such as those around fiber and copper cables. Thus, in apartment buildings and businesses, signals often easily leak into adjacent units and outside areas. This is why most users keep their Wi-Fi networks password protected. A password is a start, but other factors such as strong encryption and ease of implementing security are important ways to keep Wi-Fi networks safe from hackers.

The Wi-Fi Protected Access 2 (WPA2) security standard was established in 2004 and is currently used. In 2018, the Wi-Fi Alliance announced an updated security protocol, WPA3. The Wi-Fi Alliance is an organization supported by equipment vendors worldwide. It defines Wi-Fi standards and certifies equipment that meets the standards. The Wi-Fi Alliance specified the following WPA3 improvements:

- 192-bit encryption (a possibility of 192 combinations of zeros and ones for every bit that is encrypted). WAP2 has 128-bit encryption.
- Personal, individualized encryption on transmissions at places such as cafes, libraries, and airports. This will enable users to safely use Wi-Fi in public places.
- Simplified ways to set up security to ensure that more small organizations and households actually use and implement security.
- To block access to the Wi-Fi network after too many tries at guessing the password.
- Simplified ways to set up devices that don't have screens such as home assistants like Google's Alexa and connected light switches.
- Easier ways to test Wi-Fi networks when they are reconfigured.

Employees that don't have the newest smartphones and laptops won't be able to take advantage of Wi-Fi Protected Access 3. WPA3 was available in equipment late in 2018. User devices without WPA3 will be able to continue using WPA2. The same is true of older controllers, routers, and access points. For WPA3 to operate, each of these pieces of gear must have WPA3 computer chips. However, the Wi-Fi Alliance has announced that they will continue to support and enhance security and other features on WPA2.

Using Wi-Fi to Offload Traffic from Congested Mobile Networks

To ease congestion caused by increased tablet and smartphone traffic, carriers often supplement mobile services in densely populated areas with Wi-Fi in airports, train stations, and cafés where mobility is not required. In addition, Wi-Fi hotspots relieve backhaul congestion by transmitting traffic back to carriers' data centers over broadband links rather than on the mobile network.

Comcast and Charter operate large networks of Wi-Fi–equipped facilities. Instead of purchasing costly spectrum, these cable TV providers have built out a network of thousands of hotspots throughout the United States. The network is available to

Comcast customers that download the Comcast App to their smartphone, laptop, or tablet computer.

Wi-Fi equipment is less costly than base stations in mobile networks and spectrum is free. While cellular service excels at covering large areas, Wi-Fi service does extremely well at providing coverage inside buildings where it is relatively inexpensive to add access points.

This trend has been made possible by the advent of handsets with chips that support both Wi-Fi and mobile air interfaces. These interfaces are now tightly integrated and have the capability to automatically hand traffic off between cell sites and Wi-Fi networks. They additionally support both voice and data. However, using voice on Wi-Fi networks drains batteries more quickly than on mobile networks.

The downside of operating large numbers of small cell sites and hotspots is maintenance. Large carriers can have 50,000 of these sites to manage. Many mobile operators outsource management of their hotspots to other firms.

Worldwide Roaming on Wi-Fi

When people travel internationally or within the United States they expect Wi-Fi to be available so that they avoid the extra fees wireless providers charge for using cell phones over LTE and other mobile protocols in other networks.

Providers such as AT&T and Comcast offer large networks of Wi-Fi hotspots that are located mainly in the United States. However, using a smartphone in other countries can be problematic with the exception of hotels that offer in-building Wi-Fi either at no charge or at low daily rates.

Enterprises that have business in international locations often sign up for Wi-Fi roaming from aggregators such as iPass and Boingo. Wi-Fi aggregators have agreements with independent hotspots to manage their hotspots and for roaming between their locations. iPass manages over 64 million hotspots in more than 160 countries in which their customers' employees roam. Boingo has more than one million hotspots.

In addition to roaming internationally, Boingo offers Wi-Fi service in airports for travelers to download video and other content before boarding their airplane. The airport service is a collaboration with Comcast.

The Wi-Fi Alliance sets standards for roaming between Wi-Fi access points. Wi-Fi roaming involves middlemen. Intermediaries provide authentication that determines if the device belongs to a legitimate network provider. The intermediary also handles accounting functions related to billing.

Wireless Internet Service Providers

A Wireless Local-Area Network (Wi-Fi) hotspot is a public area where people with Wi-Fi–equipped laptops, tablet computers, and smartphones can access the Internet.

The Wi-Fi hotspot business is multilayered and includes aggregators, cellular providers, and companies that supply back-office services such as billing, roaming, and secure access to corporate networks from hotspots. Hotspot operators are also referred to as Wireless Internet Service Providers (WISPs).

The largest hotspot operator in the United States is AT&T Wi-Fi Services (formerly Wayport before AT&T purchased it in 2008). AT&T Wi-Fi Services is an aggregator. Aggregators install hardware and Internet access for hotspot services and resell it to other providers who provide billing, marketing, and customer service to end users. AT&T offers Wi-Fi access directly to its own subscribers as well as on a wholesale basis to other providers. These providers in turn offer it to their own customers. T-Mobile USA also owns an extensive number of hotspots. It offers the service at no charge to its subscribers.

SATELLITES—GEOSYNCHRONOUS AND LOW EARTH ORBITING

Geosynchronous satellites orbit 22,300 miles above the earth's surface. Because of this distance, each satellite can beam signals to a very large area; therefore, less equipment is required for coverage. This makes satellite service attractive for rural and difficult-to-cable areas.

Satellite Networks

Satellite networks are composed of a hub, the satellites themselves, and receiving dish antennas. Receiving antennas also are called *ground stations*. Receivers on antennas convert Radio Frequency (RF) wireless signals to electrical signals. The transmitter on the antenna converts electrical signals to RF signals. The point from which broadcasts originate is the hub on the ground. The hub has a large dish, routing equipment, and fiber links to the enterprise's headquarters for commercial customers. All communications broadcast from the hub travel up to the satellite and then down to the ground stations (the satellite dishes).

Satellites are used to broadcast television and radio signals and to transmit positioning information to aircraft and air traffic controllers. Satellites are particularly suited to broadcast signals to large areas for applications such as weather monitoring, mapping, and military surveillance.

NOTE The area satellites cover is directly related to how high in the sky they are located. Consider a flashlight: Holding it higher enables it to illuminate a large area. If the flashlight is held low, closer to a tabletop, for example, the beam and coverage area shrinks.

Low Earth Orbiting Satellites—Fewer Delays; More Satellites; 200 to 1,200 Miles High

Smaller, lower-cost satellites about the size of a shoebox have spurred an increase in the number of satellites launched into low earth orbits. *Low earth orbiting* (LEO) satellites are more suitable for broadband because they are launched into orbits 200 to 1,200 miles high, rather than geosynchronous satellites. Therefore, signals from low earth orbiting satellites travel a shorter distance than satellites in higher orbits.

Orbiting closer to the earth results in smaller coverage areas than for satellites located further from the earth. Thus, LEO companies invest in launching large numbers of satellites in order to cover more sections of the planet. LEO satellite owners include Aereon, OneWeb, and Viasat. Viasat is owned by satellite provider Iridium. Because of the multiple billions of dollars it costs to launch even a LEO satellite network, these companies often require backing from a variety of investors.

High-Frequency Satellite Service within Airplanes for Internet Access

Satellite service is used to transmit TV, movies, and data signals to Wi-Fi access points on airplanes. These satellites operate on the higher-frequency K_a band at 17.3–31.0 GHz spectrum. This enables them to support the high bandwidths required for on-demand services. There is essentially a Wi-Fi router with an antenna located on top of the airplane's fuselage. The antenna is protected by a 4-inch to ½-inch thin case called a radome. Wi-Fi antennas within the plane distribute signals to passengers' devices in the aircraft's cabin. Satellite providers with these higher-frequency satellites also market their services to rural areas for Internet access. Companies that provide entertainment and data services on airplanes include Gogo, Inmarsat Plc, iPass, Panasonic, and Viasat.

The challenge in providing data service in an airplane is the fact that both the airplane and the satellite travel at high speeds. This means that the airplane antenna must maintain contact with satellites that are also moving.

Satellite providers with these high-frequency satellites also market their services to rural areas and developing countries that have limited or no cable TV service. Dish Network and AT&T-owned DirecTV distribute television signals in rural areas where cable TV is not available. These services are prone to disruptions in heavy fog.

APPENDIX

Table 7-5 Mobile Services Worldwide

Technology	Frequencies	Features	Comments
Second-Generation (2G) Cellular Service			
Digital cellular service (CDMA, Time-Division Multiple Access [TDMA], Global System for Mobile Communications [GSM] and Integrated Digital Enhanced Network [iDEN])	UL: 824MHz to 849MHz DL: 869MHz to 894MHz	Digital service with more capacity than analog service. Provides advanced features such as caller ID and Short Message Service (SMS).	CDMA, TDMA, GSM, and iDEN are digital cellular air interfaces.
Personal Communication Service (PCS)	UL: 1.85GHz to 1.91GHz DL: 1.93GHz to 1.99GHz	PCS added more digital spectrum, competitors, and innovative services, driving prices down.	PCS refers to higher-frequency 1.9GHz services. Second- and 4th-generation services operate on PCS frequencies.
GSM	UL: 890MHz to 915MHz DL: 935MHz to 960MHz	A cellular digital technology. The same handsets can be used in all countries that use GSM multiplexing.	Standard used in Europe, the Far East, Israel, New Zealand, and Australia. Also used by T-Mobile and AT&T Mobility in the United States.
Digital Cellular System (DCS)	UL: 1.71GHz to 1.785GHz DL: 1.805GHz to 1.880GHz	DCS service added more digital spectrum for most existing carriers and a few new entrants.	DCS refers to higher-frequency 1.8GHz services in Europe. GSM is considered a DCS air interface.

Technology	Frequencies	Features	Comments
Enhanced Specialized Mobile Radio (ESMR)	UL: 806MHz to 821MHZ DL: 851MHz to 866MHz	Nextel (now part of Sprint Nextel) services operate on these frequencies.	Nextel and other SMR operators use iDEN technology developed by Motorola to support voice, paging, push-to-talk, and messaging on the same telephone. Also suitable for 4G service.
2.5-generation services (2.5G)		Many GSM mobile operators deployed these packet data services in the interim to 3G. They use the same spectrum as GSM. This is a lower-cost solution than 3G but with less efficient spectrum utilization.	
GPRS	Same as GSM, DCS, and PCS	General Packet Radio Service	Appropriates voice channels for data; 40- to 60Kbps.
EDGE		Enhanced Data Rates for GSM Evolution	Data speeds of about 110Kbps. Requires fewer voice channels for data than GPRS.
**Third-generation services (3G)*		3G packs more services into a given amount of spectrum than 2.5G technology.	

Table 7-6 3G Services and Spectrum

Technology	Frequencies	Features	Comments
WCDMA, also called UMTS CDMA2000 1X CDMA2000 1xEV-DO UMTS TDD TD-SCDMA	IMT-2000 bands: **UMTS:** Uplink: 1.885GHz to 2.025GHz (in the United States: 1.71GHz to 1.755GHz) Downlink: 2.11GHz to 2.17GHz (in the United States: 2.11GHz to 2.155GHz)	More capacity for voice, higher-speed data, acceptable video, low-latency applications, and so on. Standards bodies have specified all of these frequency bands for 3G services.	Carriers launched value-added 3G services to generate higher revenues. CDMA2000 1xEV-DO (data optimized) is always combined with CDMA2000 1X (voice and data) on a single chip.

Table 7-6 (Continued)

Technology	Frequencies	Features	Comments
	CDMA2000: 450MHz (NMT), 800MHz, 1.7GHz (Korea), 1.9GHz (PCS), and 2.1GHz (UMTS) **UMTS TDD:** 1.885GHz to 1.92GHz or 2.01GHz to 2.025GHz (primary), plus 2.3GHz to 2.4GHz (secondary) **TD-SCDMA:** TBD (China)		WCDMA is normally combined with GSM on a single chip for voice services. UMTS TDD uses one frequency band for uplink and downlink data transmissions. The Chinese government commercialized TD-SCDMA, a homegrown version of UMTS TDD.

Table 7-7 Releases and Revisions to 3G Cellular Services

Name of Service and Release	Downlink Data Rates: From the Network to the Subscriber	Uplink Data Rates: From the Subscriber to the Network
CDMA2000 Releases (1.25MHz Channel Bandwidth)		
CDMA2000 1X (Release 0) Doubles voice capacity	Peak data rate: 153.6Kbps Average data rate: 64Kbps	Peak data rate: 153.6Kbps Average data rate: 64Kbps
CDMA2000 1xEV-DO (Release 0) Data optimized High data rate (HDR)	Peak data rate: 2.4Mbps Average data rate: 500Kbps to 1Mbps	Peak data rate: 384Kbps Average data rate: 144Kbps
CDMA450 Same features as other CDMA standards but operates in lower frequencies so that fewer base stations are needed	Same as 1X and 1xEV-DO	Same as 1X and 1xEV-DO. Deployed mainly in rural areas because of its capability to cover large areas.
CDMA2000 1xEV-DO (Revision A) or CDMA2000 DO Rev. A Supports low-latency (delay) data in a single 1.25MHz channel.	Peak data rate: 3.1Mbps Average data rate: 1.8Mbps	Peak data rate: 1.8Mbps Average data rate: 630Kbps per sector (standard) Average data rate: 1.325Mbps per sector

Name of Service and Release	Downlink Data Rates: From the Network to the Subscriber	Uplink Data Rates: From the Subscriber to the Network
WCDMA Releases (5MHz Channel Bandwidth)		
WCDMA (Release 99)	Peak data rate: 2Mbps Average data rate: 220Kbps	Peak data rate: 384Kbps Average data rate: 64Kbps
WCDMA (Release 4) Enables operators to prioritize data services per customer subscription choices.	Peak data rate: 2Mbps Average data rate: 384Kbps	Same as WCDMA (Release 99)
WCDMA (Releases 5 and 6) HSPD/UPA (high-speed downlink/uplink packet access) Doubles the uplink speed	Peak data rate: 14Mbps Average data rate: 2Mbps	Uplink: 1.4Mbps

Table 7-8 802.11 (Wi-Fi) Standards

802.11 Standard	Description
802.11ac	A Wi-Fi standard designed to provide gigabit speeds on Wi-Fi networks. A replacement for 802.11n.
802.11ad	A Wi-Fi standard gigabit short range of only 30 feet, data rates over the 60 GHz spectrum bands. Envisioned as a replacement for HDMI cables and other short-range applications.
802.11af	A Wi-Fi standard designed to operate in the white space 700MHz spectrum freed up by TV broadcasters. It has low power requirements, supports longer-life batteries
802.11ah	A Wi-Fi standard for low sub-gigahertz bandwidth applications
802.11ai	A standard that supports the discovery and initial connectivity to the Wi-Fi network.
802.11ay	An IEEE draft of a standard that will have four times the data rates of 802.11ad. It uses bonding to achieve data rates of 20 to 40 GBPS. It has a range of 300 to 500 meters (327 to 547 yards).
802.11ax	A proposed standard that will operate in support of 10Gbps in the 5GHz bands and slower data rates in the 2.4GHz bands. It supports interoperability and *time synch*, which is used to synchronize timing in mesh architectures. 802.11ax gear is expected to be widely available in 2019. The Wi-Fi Alliance rebranded 802.11ax as Wi-Fi 6.

Table 7-8 (Continued)

802.11 Standard	Description
802.11aq	An IEEE standard to allow devices to detect which networks are available before users connect to these services.
802.11az	A proposed standard that will make it faster for Wi-Fi networks to locate devices and connect devices to Wi-Fi networks when they are moving. Uses power efficiently by reverting to sleep mode when not active.
802.11d	A standard that supports the capability for Wi-Fi devices to operate in different countries that require different power levels and frequencies. Enables equipment to be adjusted according to the rules of each country.
802.11e	A Quality of Service (QoS) standard, the Wi-Fi Multimedia (WMM) section of 802.11e that defines prioritizing voice and video. Was approved October 2004.
802.11f	A standard that supports the capability for access points from different manufacturers to interoperate in the same Wireless Local Area Network (Wi-Fi).
802.11h	A proposal that defines ways for 802.11a networks to dynamically assign packets to other channels if there is interference with other access points and services such as radar, medical devices, and satellite transmissions. In some countries, radar and satellite use the same frequencies as 802.11a.
802.11i	A standard for improved security. It's also referred to as Wireless Protected Access 2 (WPA2) and Wi-Fi Protected Access 3 (WPA3).
802.11k	A Wi-Fi standard for roaming between access points. Provides information to Wi-Fi management systems so they can balance traffic between access points.
802.11n	A standard to increase throughput—actual user data transmitted, and the range covered by each access point. Improvements achieved through enhancements in antennas that decrease effects of interference. In new devices replaced by 802.11ac.
802.11p WAVE (Wireless Access for Vehicular Environments)	A standard for vehicle-to-vehicle and vehicle-to-roadside structures, and vehicle safety services. It enables communications between vehicles and roadside access points or other vehicles.
802.11r	The standard that defines methods for switches to quickly hand off sessions between access points so that users don't have to be authenticated again. This is important to avoid delays for traffic between access points.

802.11 Standard	Description
802.11s	An IEEE networking standard used in mesh networks. It defines how access points access Wi-Fi in community-wide Wi-Fi networks, large homes, and buildings.
802.11u	An IEEE standard that enables automatic interworking between cellular and Wi-Fi networks. A user's mobile device with embedded Wi-Fi with 802.11u can automatically switch to Wi-Fi when it's in a Wi-Fi hotspot that has an agreement with the user's carrier. This is part of the Wi-Fi Alliance initiative known as Hot Spot 2.0 to simplify cellular devices' Wi-Fi access.
802.11v	Improves the ability to manage Wi-Fi networks by enabling statistics gathering and power management that will improve battery life. A must in client devices and access points.
802.11w	A standard used for security that protects Wi-Fi devices from attackers with spoofed (fake) addresses.
802.11x	A proposed security standard for authentication and security to prevent unauthorized packets from entering wired LANs from Wi-Fi networks. It's an alternative to creating virtual private networks.
Control and Provisioning of Wireless Access Points (CAPWAP)	An IEEE standard for Wi-Fi switches to control access points by centralizing intelligence in one device, a controller.
Unlicensed Mobile Access (WMA)	A way to route cell phone traffic over Wi-Fi networks. The cellular network maintains control of calls so that it can bill for traffic.
Wi-Fi Direct	A Wi-Fi standard that enables any device with Wi-Fi Direct software to communicate directly with another device. This allows a laptop to act as an access point so that nearby computers can also access the Internet. Can be used for printing directly from a smartphone to a printer.