This is “A Manager’s Guide to the Internet and Telecommunications”, chapter 12 from the book Getting the Most Out of Information Systems (index.html) (v. 1.4).

Chapter 12

A Manager's Guide to the Internet and Telecommunications

12.1 Introduction

There's all sorts of hidden magic happening whenever you connect to the Internet. But what really makes it possible for you to reach servers halfway around the world in just a fraction of a second? Knowing this is not only flat-out fascinating stuff; it's also critically important for today's manager to have at least a working knowledge of how the Internet functions.

That's because the Internet is a platform of possibilities and a business enabler. Understanding how the Internet and networking works can help you brainstorm new products and services and understand roadblocks that might limit turning your ideas into reality. Marketing professionals who know how the Internet reaches consumers have a better understanding of how technologies can be used to find and target customers. Finance firms that rely on trading speed to move billions in the blink of an eye need to master Internet infrastructure to avoid being swept aside by more nimble market movers. And knowing how the Internet works helps all managers understand where their firms are vulnerable. In most industries today, if your network goes down then you might as well shut your doors and go home; it's nearly impossible to get anything done if you can't get online. Managers who know the Net are prepared to take the appropriate steps to secure their firms and keep their organization constantly connected.

12.2 Internet 101: Understanding How the Internet Works

LEARNING OBJECTIVES

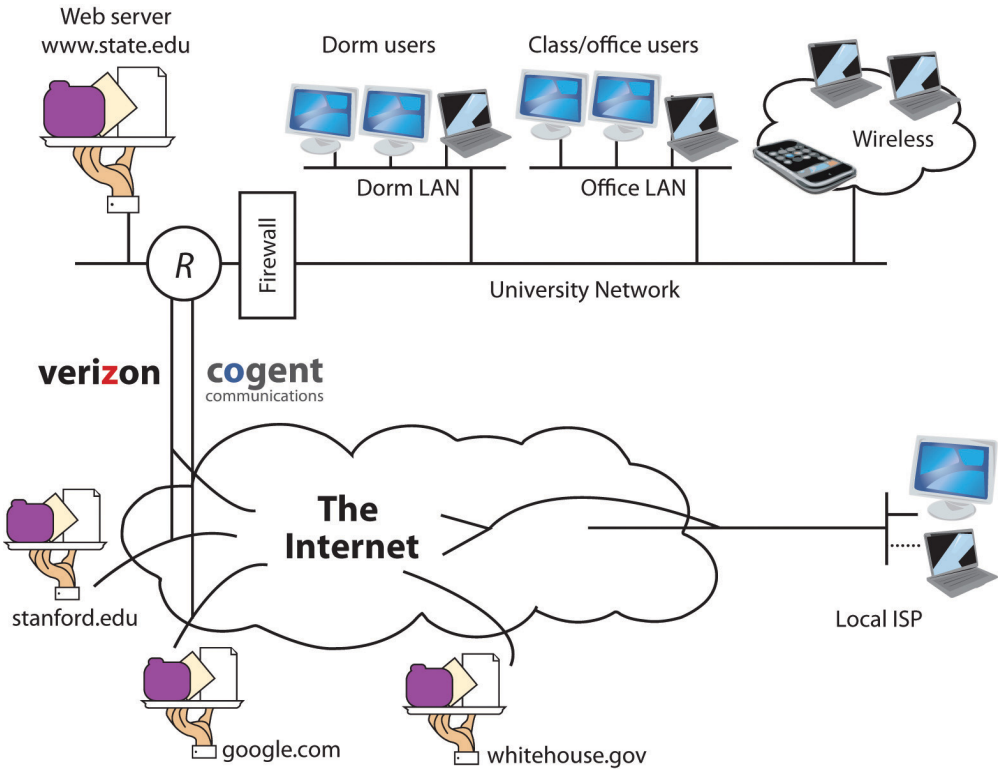
1. Describe how the technologies of the Internet combine to answer these questions: What are you looking for? Where is it? And how do we get there?
2. Interpret a URL, understand what hosts and domains are, describe how domain registration works, describe cybersquatting, and give examples of conditions that constitute a valid and invalid domain-related trademark dispute.
3. Describe certain aspects of the Internet infrastructure that are fault-tolerant and support load balancing.
4. Discuss the role of hosts, domains, IP addresses, and the DNS in making the Internet work.

The Internet is a network of networks—millions of them, actually. If the network at your university, your employer, or in your home has Internet access, it connects to an **Internet service provider (ISP)**[1]. Many (but not all) ISPs are big telecommunications companies like Verizon, Comcast, and AT&T. These providers connect to one another, exchanging traffic, and ensuring your messages can get to any other computer that's online and willing to communicate with you.

The Internet has no center and no one owns it. That's a good thing. The Internet was designed to be redundant and fault-tolerant—meaning that if one network, connecting wire, or server stops working, everything else should keep on running. Rising from military research and work at educational institutions dating as far back as the 1960s, the Internet really took off in the 1990s, when graphical Web browsing was invented, and much of the Internet's operating infrastructure was transitioned to be supported by private firms rather than government grants.

1. An organization or firm that provides access to the Internet.

Figure 12.1



The Internet is a network of networks, and these networks are connected together. In the diagram above, the "state.edu" campus network is connected to other networks of the Internet via two ISPs: Cogent and Verizon.

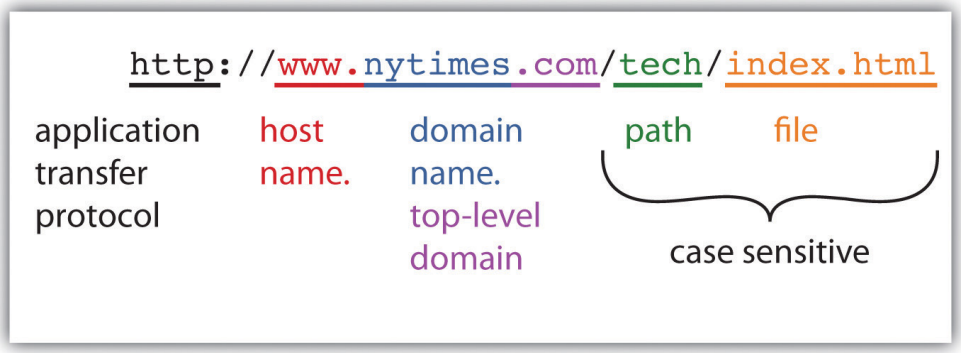
Enough history—let's see how it all works! If you want to communicate with another computer on the Internet then your computer needs to know the answer to three questions: What are you looking for? Where is it? And how do we get there? The computers and software that make up Internet infrastructure can help provide the answers. Let's look at how it all comes together.

The URL: "What Are You Looking For?"

When you type an address into a Web browser (sometimes called a **URL**[2] for *uniform resource locator*), you're telling your browser what you're looking for. Figure 12.2 "Anatomy of a Web Address" describes how to read a typical URL.

2. Often used interchangeably with "Web address," URLs identify resources on the Internet along with the application protocol need to retrieve it.

Figure 12.2 *Anatomy of a Web Address*



The URL displayed really says, "Use the Web (http://) to find a host server named 'www' in the 'nytimes.com' network, look in the 'tech' directory, and access the 'index.html' file."

The http:// you see at the start of most Web addresses stands for **hypertext transfer protocol**[3]. A **protocol**[4] is a set of rules for communication—sort of like grammar and vocabulary in a language like English. The http protocol defines how Web browser and Web servers communicate and is designed to be independent from the computer's hardware and operating system. It doesn't matter if messages come from a PC, a Mac, a huge mainframe, or a pocket-sized smartphone; if a device speaks to another using a common protocol, then it will be heard and understood.

The Internet supports lots of different applications, and many of these applications use their own application transfer protocol to communicate with each other. The server that holds your e-mail uses something called *SMTP*, or simple mail transfer protocol, to exchange mail with other e-mail servers throughout the world. **FTP**[5], or file transfer protocol, is used for—you guessed it—file transfer. FTP is how most Web developers upload the Web pages, graphics, and other files for their Web sites. Even the Web uses different protocols. When you surf to an online bank or when you're ready to enter your payment information at the Web site of an Internet retailer, the http at the beginning of your URL will probably change to https (the "s" is for secure). That means that communications between your browser and server will be encrypted for safe transmission. The beauty of the Internet infrastructure is that any savvy entrepreneur can create a new application that rides on top of the Internet.

3. Application transfer protocol that allows Web browsers and Web servers to communicate with each other.

4. Enables communication by defining the format of data and rules for exchange.

5. Application transfer protocol that is used to copy files from one computer to another.

Hosts and Domain Names

The next part of the URL in our diagram holds the host and domain name. Think of the domain name as the name of the network you're trying to connect to, and think of the host as the computer you're looking for on that network.

Many domains have lots of different hosts. For example, Yahoo!'s main Web site is served from the host named "www" (at the address http://www.yahoo.com), but Yahoo! also runs other hosts including those named "finance" (finance.yahoo.com), "sports" (sports.yahoo.com), and "games" (games.yahoo.com).

Host and Domain Names: A Bit More Complex Than That

While it's useful to think of a host as a single computer, popular Web sites often have several computers that work together to share the load for incoming requests. Assigning several computers to a host name offers **load balancing**[6] and **fault tolerance**[7], helping ensure that all visits to a popular site like http://www.google.com won't overload a single computer, or that Google doesn't go down if one computer fails.

It's also possible for a single computer to have several host names. This might be the case if a firm were hosting several Web sites on a single piece of computing hardware.

Some domains are also further broken down into subdomains—many times to represent smaller networks or subgroups within a larger organization. For example, the address http://www.rhsmith.umd.edu is a University of Maryland address with a host "www" located in the subdomain "rhsmith" for the Robert H. Smith School of Business. International URLs might also include a second-level domain classification scheme. British URLs use this scheme, for example, with the BBC carrying the commercial (.co) designation—http://www.bbc.co.uk—and the University of Oxford carrying the academic (.ac) designation—http://www.ox.ac.uk. You can actually go 127 levels deep in assigning subdomains, but that wouldn't make it easy on those who have to type in a URL that long.

6. Distributing a computing or networking workload across multiple systems to avoid congestion and slow performance.

7. The ability of a system to continue operation even if a component fails.

Most Web sites are configured to load a default host, so you can often eliminate the host name if you want to go to the most popular host on a site (the default host is

almost always named "www"). Another tip: most browsers will automatically add the "http://" for you, too.

Host and domain names are not case sensitive, so you can use a combination of upper and lower case letters and you'll still get to your destination.

I Want My Own Domain

You can stake your domain name claim in cyberspace by going through a firm called a *domain name registrar*. You don't really buy a domain name; you simply pay a registrar for the right to use that name, with the right renewable over time. While some registrars simply register domain names, others act as **Web hosting services**[8] that are able to run your Web site on their Internet-connected servers for a fee.

Registrars throughout the world are accredited by **ICANN (Internet Corporation for Assigning Names and Numbers)**[9], a nonprofit governance and standards-setting body. Each registrar may be granted the ability to register domain names in one or more of the Net's generic top-level domains (gTLDs), such as ".com," ".net," or ".org." There are dozens of registrars that can register ".com" domain names, the most popular gTLD.

Some generic top-level domain names, like ".com," have no restrictions on use, while others limit registration. For example, ".edu" is restricted to U.S.-accredited, postsecondary institutions. ICANN has also announced plans to allow organizations to sponsor their own top-level domains (e.g., ".berlin," or ".coke").

There are also separate agencies that handle over 250 different two-character country code top-level domains, or ccTLDs (e.g., ".uk" for the United Kingdom and ".jp" for Japan). Servers or organizations generally don't need to be housed within a country to use a country code as part of their domain names, leading to a number of creatively named Web sites. The URL-shortening site "bit.ly" uses Libya's ".ly" top-level domain; many physicians are partial to Moldova's code (".md"); and the tiny Pacific island nation of Tuvulu might not have a single broadcast television station, but that doesn't stop it from licensing its country code to firms that want a ".tv" domain name.K. Maney, "Tuvalu's Sinking, But Its Domain Is on Solid Ground," *USA Today*, April 27, 2004. Recent standards also allow domain names in languages that use non-Latin alphabets such as Arabic and Russian.

Domain name registration is handled on a first-come, first-served basis and all registrars share registration data to ensure that no two firms gain rights to the same name. Start-ups often sport wacky names, partly because so many domains with common words and phrases are already registered to others.

8. A firm that provides hardware and services to run the Web sites of others.

9. Nonprofit organization responsible for managing the Internet's domain and numbering systems.

While some domain names are held by legitimate businesses, others are registered by investors hoping to resell a name's rights.

Trade in domain names can be lucrative. For example, the "Insure.com" domain was sold to QuinStreet for $16 million in fall 2009.B. Bosker, "The 11 Most Expensive Domain Names Ever," *The Huffington Post*, March 10, 2010. But knowingly registering a domain name to profit from someone else's firm name or trademark is known as **cybersquatting**[10] and that's illegal. The United States has passed the Anticybersquatting Consumer Protection Act (ACPA), and ICANN has the Domain Name Dispute Resolution Policy that can reach across boarders. Try to extort money by holding a domain name that's identical to (or in some cases, even similar to) a well-known trademark holder and you could be stripped of your domain name and even fined.

Courts and dispute resolution authorities will sometimes allow a domain that uses the trademark of another organization if it is perceived to have legitimate, nonexploitive reasons for doing so. For example, the now defunct site Verizonreallysucks.com was registered as a protest against the networking giant and was considered fair use since owners didn't try to extort money from the telecom giant.D. Streitfeld, "Web Site Feuding Enters Constitutional Domain," *The Washington Post*, September 11, 2000. However, the courts allowed the owner of the PETA trademark (the organization People for the Ethical Treatment of Animals) to claim the domain name peta.org from original registrant, who had been using that domain to host a site called "People Eating Tasty Animals."D. McCullagh, "Ethical Treatment of PETA Domain," *Wired*, August 25, 2001.

Trying to predict how authorities will rule can be difficult. The musician Sting's name was thought to be too generic to deserve the rights to Sting.com, but Madonna was able to take back her domain name (for the record, Sting now owns Sting.com).R. Konrad and E. Hansen, "Madonna.com Embroiled in Domain Ownership Spat," *CNET*, August 21, 2000. Apple executive Jonathan Ive was denied the right to reclaim domain names incorporating his own name, but that had been registered by another party and without his consent. The publicity-shy design guru wasn't considered enough of a public figure to warrant protection.D. Morson, "Apple VP Ive Loses Domain Name Bid," *MacWorld*, May 12, 2009. And sometimes disputing parties can come to an agreement outside of court or ICANN's dispute resolution mechanisms. When Canadian teenager Michael Rowe registered a site for his part-time Web design business, a firm south of the border took notice of his domain

10. Acquiring a domain name that refers to a firm, individual, product, or trademark, with the goal of exploiting it for financial gain. The practice is illegal in many nations, and ICANN has a dispute resolution mechanism that in some circumstances can strip cybersquatters of registered domains.

name—Mikerowesoft.com. The two parties eventually settled in a deal that swapped the domain for an Xbox and a trip to the Microsoft Research Tech Fest.M. Kotadia, "MikeRoweSoft Settles for an Xbox," *CNET*, January 26, 2004.

Path Name and File Name

Look to the right of the top-level domain and you might see a slash followed by either a path name, a file name, or both. If a Web address has a path and file name, the path maps to a folder location where the file is stored on the server; the file is the name of the file you're looking for.

Most Web pages end in ".html," indicating they are in **hypertext markup language**[11]. While http helps browsers and servers communicate, html is the language used to create and format (render) Web pages. A file, however, doesn't need to be .html; Web servers can deliver just about any type of file: Acrobat documents (.pdf), PowerPoint documents (.ppt or .pptx), Word docs (.doc or .docx), JPEG graphic images (.jpg), and—as we'll see in Chapter 13 "Information Security: Barbarians at the Gateway (and Just About Everywhere Else)"—even malware programs that attack your PC. At some Web addresses, the file displays content for every visitor, and at others (like amazon.com), a file will contain programs that run on the Web server to generate custom content just for you.

You don't always type a path or file name as part of a Web address, but there's always a file lurking behind the scenes. A Web address without a file name will load content from a default page. For example, when you visit "google.com," Google automatically pulls up a page called "index.html," a file that contains the Web page that displays the Google logo, the text entry field, the "Google Search" button, and so on. You might not see it, but it's there.

Butterfingers, beware! Path and file names are case sensitive—amazon.com/books is considered to be different from amazon.com/BOOKS. Mistype your capital letters after the domain name and you might get a 404 error (the very unfriendly Web server error code that means the document was not found).

11. Language used to compose Web pages.

IP Addresses and the Domain Name System: "Where Is It? And How Do We Get There?"

The IP Address

If you want to communicate, then you need to have a way for people to find and reach you. Houses and businesses have street addresses, and telephones have phone numbers. Every device connected to the Internet has an identifying address, too—it's called an *IP (Internet protocol) address*.

A device gets its **IP address**[12] from whichever organization is currently connecting it to the Internet. Connect using a laptop at your university and your school will assign the laptop's IP address. Connect at a hotel, and the hotel's Internet service provider lends your laptop an IP address. Laptops and other end-user machines might get a different IP address each time they connect, but the IP addresses of servers rarely change. It's OK if you use different IP addresses during different online sessions because services like e-mail and Facebook identify you by your username and password. The IP address simply tells the computers that you're communicating with where they can find you right now. IP addresses can also be used to identify a user's physical location, to tailor search results, and to customize advertising. See Chapter 14 "Google in Three Parts: Search, Online Advertising, and Beyond" to learn more.

The original and still widely used format for IP addresses is known as IPv4. Under IPv4, IP addresses are expressed as a string of four numbers between 0 and 255, separated by three periods. Want to know which IP address your smartphone or computer is using? Visit a Web site like ip-adress.com (one "d"), whatismyipaddress.com, or ipchicken.com.

12. A value used to identify a device that is connected to the Internet. IP addresses are usually expressed as four numbers (from 0 to 255), separated by periods.

The Internet Is Full—We've Run Out of IP Addresses

If you do the math, four combinations of 0 to 255 gives you a little over four billion possible IP addresses. Four billion sounds like a lot, but the number of devices connecting to the Internet is exploding! Internet access is now baked into smartphones, tablets, televisions, DVD players, video game consoles, utility meters, thermostats, appliances, picture frames, and more. Another problem is a big chunk of existing addresses weren't allocated efficiently, and these can't be easily reclaimed from the corporations, universities, and other organizations that initially received them. All of this means that we've run out of IP addresses. In February 2011 the last batches were made available to regional Internet registries.J. Biggs, "Everybody Panic: Why We're Running Out of IP Addresses and What's Going to Happen Now," *CrunchGear*, February 2, 2011.

There are some schemes to help delay the impact of this IP address drought. For example, a technique known as **NAT (network address translation)**[13] uses a gateway that allows multiple devices to share a single IP address. But NAT slows down Internet access and is complex, cumbersome, and expensive to administer.S. Shankland, "Google Tries to Break IPv6 Logjam by Own Example," *CNET*, March 27, 2009.

The only long-term solution is to shift to a new IP scheme. Fortunately, one was developed more than a decade ago. IPv6 increases the possible address space from the 2^{32} (4,294,967,296) addresses used in the current system (called IPv4) to a new theoretical limit of 2^{128} addresses, which is a really big number—bigger than 34 with 37 zeros after it. That's more IPv6 addresses than there are gains of sand on the earth.V. Kopytoff, "Happy IPv6 Day," *New York Times*, June 8, 2011.

But not all the news is good. Unfortunately, IPv6 isn't backward compatible with IPv4, and the transition to the new standard has been painfully slow. This gives us the equivalent of many islands of IPv6 in a sea of IPv4, with translation between the two schemes happening when these networks come together. Others consider it the equivalent of two Internets with a translation bridge between IPv4 and IPv6 (and that bridge introduces a delay).M. Peckham, "World IPv6 Launch: Only The Biggest Change to the Internet Since Inception," *Time*, June 6, 2012. While most modern hardware and operating systems providers now support IPv6, converting a network to IPv6 currently involves a lot of cost with little short-term benefit.S. Shankland, "Google Tries to Break

13. A technique often used to conserve IP addresses by maps devices on a private network to single Internet-connected device that acts on their behalf.

IPv6 Logjam by Own Example," *CNET*, March 27, 2009. Upgrading may take years.B. Arnoldy, "IP Address Shortage to Limit Internet Access," *USA Today*, August 3, 2007.

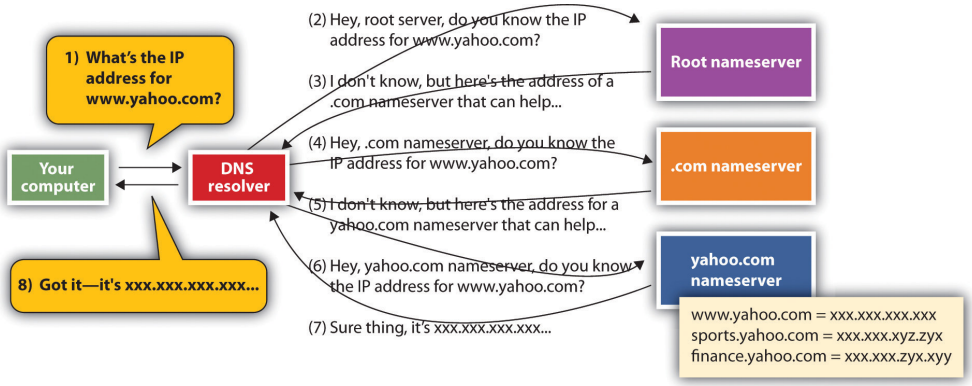
Some organizations have stepped up to try to hasten the transition. Facebook, Google, Microsoft, Yahoo!, and some of the Internet's largest networks have made most of its services IPv6 accessible, the U.S. government has mandated IPv6 support for most agencies, China has spurred conversion within its borders, and Comcast and Verizon have major IPv6 rollouts under way. While the transition will be slow, when wide scale deployment does arrive, IPv6 will offer other benefits, including potentially improving the speed, reliability, and security of the Internet.

The DNS: The Internet's Phonebook

You can actually type an IP address of a Web site into a Web browser and that page will show up. But that doesn't help users much because four sets of numbers are really hard to remember.

This is where the **domain name service (DNS)**[14] comes in. The domain name service is a distributed database that looks up the host and domain names that you enter and returns the actual IP address for the computer that you want to communicate with. It's like a big, hierarchical set of phone books capable of finding Web servers, e-mail servers, and more. These "phone books" are called *nameservers*—and when they work together to create the DNS, they can get you anywhere you need to go online.

Figure 12.3



14. Internet directory service that allows devices and services to be named and discoverable. The DNS, for example, helps your browser locate the appropriate computers when entering an address like http://finance.google.com.

When your computer needs to find the IP address for a host or domain name, it sends a message to a DNS resolver, which looks up the IP address starting at the root nameserver. Once the lookup has taken place, that IP address can be saved in a holding space called a cache, to speed future lookups.

To get a sense of how the DNS works, let's imagine that you type www.yahoo.com into a Web browser. Your computer doesn't know where to find that address, but when your computer connected to the network, it learned where to find a service on the network called a DNS resolver. The DNS resolver can look up host/domain name combinations to find the matching IP address using the "phone book" that is the DNS. The resolver doesn't know everything, but it does know where to start a lookup that will eventually give you the address you're looking for. If this is the first time anyone on that network has tried to find "www.yahoo.com," the resolver will contact one of thirteen identical root nameservers. The root acts as a lookup starting place. It doesn't have one big list, but it can point you to a nameserver for the next level, which would be one of the ".com" nameservers in our example. The ".com" nameserver can then find one of the yahoo.com nameservers. The yahoo.com nameserver can respond to the resolver with the IP address for www.yahoo.com, and the resolver passes that information back to your computer. Once your computer knows Yahoo!'s IP address, it's then ready to communicate directly with www.yahoo.com. The yahoo.com nameserver includes IP addresses for all Yahoo!'s public sites: www.yahoo.com, games.yahoo.com, sports.yahoo.com, finance.yahoo.com, and so on.

The system also remembers what it's done so the next time you need the IP address of a host you've already looked up, your computer can pull this out of a storage space called a **cache**[15], avoiding all those nameserver visits. Caches are periodically cleared and refreshed to ensure that data referenced via the DNS stays accurate.

Distributing IP address lookups this way makes sense. It avoids having one huge, hard-to-maintain, and ever-changing list. Firms add and remove hosts on their own networks just by updating entries in their nameserver. And it allows host IP addresses to change easily, too. Moving your Web server off-site to a hosting provider? Just update your nameserver with the new IP address at the hosting provider, and the world will invisibly find that new IP address on the new network by using the same old, familiar host/domain name combination. The DNS is also fault-tolerant—meaning that if one nameserver goes down, the rest of the service can function. There are exact copies at each level, and the system is smart enough to move on to another nameserver if its first choice isn't responding.

15. A temporary storage space used to speed computing tasks.

But What If the DNS Gets Hacked?

A hacked DNS would be a disaster! Think about it. If bad guys could change which Web sites load when you type in a host and domain name, they could redirect you to impostor Web sites that look like a bank or e-commerce retailer but are really set up to harvest passwords and credit card data.

This exact scenario played out when the DNS of NET Virtua, a Brazilian Internet service provider, was hacked via a technique called *DNS cache poisoning*. Cache poisoning exploits a hole in DNS software, redirecting users to sites they didn't request. The Brazilian DNS hack redirected NET Virtua users wishing to visit the Brazilian bank Bradesco to fraudulent Web sites that attempted to steal passwords and install malware. The hack impacted about 1 percent of the bank's customers before the attack was discovered.D. Godin, "Cache-Poisoning Attack Snares Top Brazilian Bank," *The Register*, April 22, 2009.

The exploit showed the importance of paying attention to security updates. A few months earlier, a group that *Wired* magazine referred to as "A Secret Geek A-Team"J. Davis, "Secret Geek A-Team Hacks Back, Defends Worldwide Web," *Wired*, Nov. 24, 2008. had developed a software update that would have prevented the DNS poisoning exploit used against NET Virtua, but administrators at the Brazilian Internet service provider failed to update their software so the hackers got in. An additional upgrade to a DNS system, known as DNSSEC (domain name service security extensions), promises to further limit the likelihood of cache poisoning, but it may take years for the new standards to be rolled out everywhere.J. Hutchinson, "ICANN, Verisign Place Last Puzzle Pieces in DNSSEC Saga," *NetworkWorld*, May 2, 2010.

KEY TAKEAWAYS

- The Internet is a network of networks. Internet service providers connect with one another to share traffic, enabling any Internet-connected device to communicate with any other.
- URLs may list the application protocol, host name, domain name, path name, and file name, in that order. Path and file names are case sensitive.
- A domain name represents an organization. Hosts are public services offered by that organization. Hosts are often thought of as a single computer, although many computers can operate under a single host name and many hosts can also be run off a single computer.
- You don't buy a domain name but can register it, paying for a renewable right to use that domain name. Domains need to be registered within a generic top-level domain such as ".com" or ".org" or within a two-character country code top-level domain such as ".uk," ".ly," or ".md."
- Registering a domain that uses someone else's trademark in an attempt to extract financial gain is considered cybersquatting. The United States and other nations have anticybersquatting laws, and ICANN has a dispute resolution system that can overturn domain name claims if a registrant is considered to be cybersquatting.
- Every device connected to the Internet has an IP address. These addresses are assigned by the organization that connects the user to the Internet. An IP address may be assigned temporarily, for use only during that online session.
- We're running out of IP addresses. The current scheme (IPv4) is being replaced by IPv6, a scheme that will give us many more addresses and additional feature benefits but is not backward compatible with the IPv4 standard. Transitioning to IPv6 will be costly, take time, and introduce delay when traffic transfers between IPv4 and IPv6 networks.
- The domain name system is a distributed, fault-tolerant system that uses nameservers to map host/domain name combinations to IP addresses.

QUESTIONS AND EXERCISES

1. Find the Web page for your school's information systems department. What is the URL that gets you to this page? Label the host name, domain name, path, and file for this URL. Are there additional subdomains? If so, indicate them, as well.
2. Go to a registrar and see if someone has registered your first or last name as a domain name. If so, what's hosted at that domain? If not, would you consider registering your name as a domain name? Why or why not?
3. Investigate cases of domain name disputes. Examine a case that you find especially interesting. Who were the parties involved? How was the issue resolved? Do you agree with the decision?
4. Describe how the DNS is fault-tolerant and promotes load balancing. Give examples of other types of information systems that might need to be fault-tolerant and offer load balancing. Why?
5. Research DNS poisoning online. List a case, other than the one mentioned in this chapter, where DNS poisoning took place. Which network was poisoned, who were the victims, and how did hackers exploit the poisoned system? Could this exploit have been stopped? How? Whose responsibility is it to stop these kinds of attacks?
6. Why is the switch from IPv4 to IPv6 so difficult? What key principles, discussed in prior chapters, are slowing migration to the new standard?
7. Test to see if networks that you frequently use (home, school, work, mobile) are ready for IPv6 by visiting http://test-ipv6.com/ (or a similar site). Search online to see if your service provider has posted details outlining their IPv6 transition strategy and be prepared to share your results with the class. Do you use other products not tested by the Web site mentioned above (e.g., network-enabled video games or other software)? Search online to see if your favorite products and services are IPv6 ready.

12.3 Getting Where You're Going

LEARNING OBJECTIVES

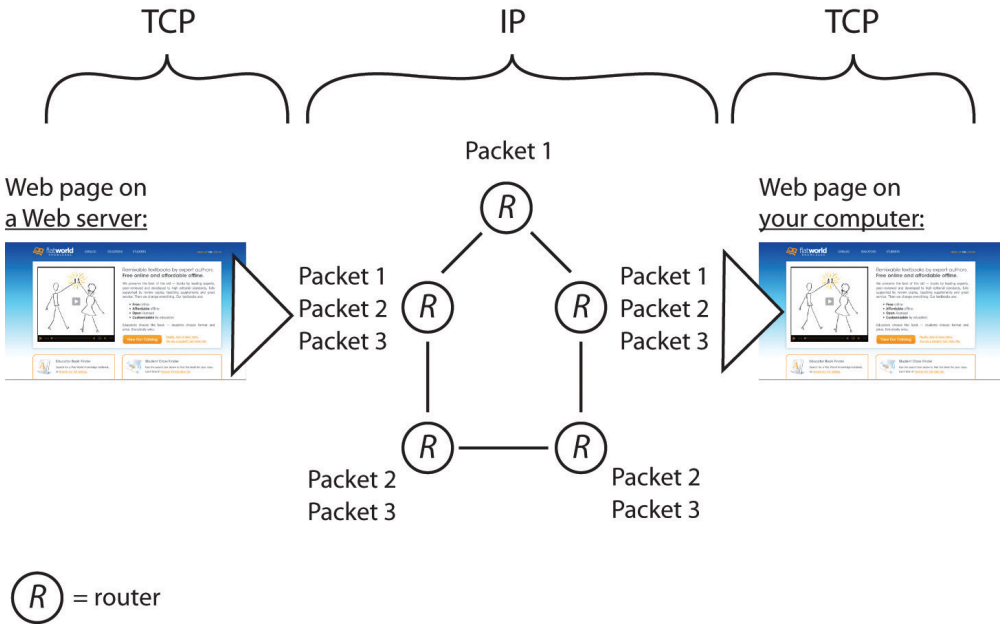
1. Understand the layers that make up the Internet—application protocol, transmission control protocol, and Internet protocol—and describe why each is important.
2. Discuss the benefits of Internet architecture in general and TCP/IP in particular.
3. Name applications that should use TCP and others that might use UDP.
4. Understand what a router does and the role these devices play in networking.
5. Conduct a traceroute and discuss the output, demonstrating how Internet interconnections work in getting messages from point to point.
6. Understand why mastery of Internet infrastructure is critical to modern finance and be able to discuss the risks in automated trading systems.
7. Describe VoIP, and contrast circuit versus packet switching, along with organizational benefits and limitations of each.

TCP/IP: The Internet's Secret Sauce

OK, we know how to read a Web address, we know that every device connected to the Net needs an IP address, and we know that the DNS can look at a Web address and find the IP address of the machine that you want to communicate with. But how does a Web page, an e-mail, or an iTunes download actually get from a remote computer to your desktop?

For our next part of the Internet journey, we'll learn about two additional protocols: TCP and IP. These protocols are often written as TCP/IP and pronounced by reading all five letters in a row, "T-C-P-I-P" (sometimes they're also referred to as the *Internet protocol suite*). TCP and IP are built into any device that a user would use to connect to the Internet—from handhelds to desktops to supercomputers—and together TCP/IP make Internet working happen.

Figure 12.4 TCP/IP in Action



In this example, a server on the left sends a Web page to the user on the right. The application (the Web server) passes the contents of the page to TCP (which is built into the server's operating system). TCP slices the Web page into packets. Then IP takes over, forwarding packets from router to router across the Internet until it arrives at the user's PC. Packets sometimes take different routes, and occasionally arrive out of order. TCP running on the receiving system on the right checks that all packets have arrived, requests that damaged or lost packets be resent, puts them in the right order, and sends a perfect, exact copy of the Web page to your browser.

TCP and IP operate below http and the other application transfer protocols mentioned earlier. **TCP (transmission control protocol)**[16] works its magic at the start and endpoint of the trip—on both your computer and on the destination computer you're communicating with. Let's say a Web server wants to send you a large Web page. The Web server application hands the Web page it wants to send to its own version of TCP. TCP then slices up the Web page into smaller chunks of data called **packets (or datagrams)**[17]. The packets are like little envelopes containing part of the entire transmission—they're labeled with a destination address (where it's going) and a source address (where it came from). Now we'll leave TCP for a second, because TCP on the Web server then hands those packets off to the second half of our dynamic duo, IP.

It's the job of **IP (Internet protocol)**[18] to route the packets to their final destination, and those packets might have to travel over several networks to get to where they're going. The relay work is done via special computers called **routers**[19], and these routers speak to each other and to other computers using IP (since routers are connected to the Internet, they have IP addresses, too. Some are even

16. Works at both ends of most Internet communication to ensure a perfect copy of a message is sent.

17. A unit of data forwarded by a network. All Internet transmissions—URLs, Web pages, e-mails—are divided into one or more packets.

18. Routing protocol that is in charge of forwarding packets on the Internet.

19. A computing device that connects networks and exchanges data between them.

named). Every computer on the Internet is connected to a router, and all routers are connected to at least one (and usually more than one) other router, linking up the networks that make up the Internet.

Routers don't have perfect, end-to-end information on all points in the Internet, but they do talk to each other all the time, so a router has a pretty good idea of where to send a packet to get it closer to where it needs to end up. This chatter between the routers also keeps the Internet decentralized and fault-tolerant. Even if one path out of a router goes down (a networking cable gets cut, a router breaks, the power to a router goes out), as long as there's another connection out of that router, then your packet will get forwarded. Networks fail, so good, fault-tolerant network design involves having alternate paths into and out of a network.

Once packets are received by the destination computer (your computer in our example), that machine's version of TCP kicks in. TCP checks that it has all the packets, makes sure that no packets were damaged or corrupted, requests replacement packets (if needed), and then puts the packets in the correct order, passing a perfect copy of your transmission to the program you're communicating with (an e-mail server, Web server, etc.).

This progression—application at the source to TCP at the source (slice up the data being sent), to IP (for forwarding among routers), to TCP at the destination (put the transmission back together and make sure it's perfect), to application at the destination—takes place in both directions, starting at the server for messages coming to you, and starting on your computer when you're sending messages to another computer.

UDP: TCP's Faster, Less Reliable Sibling

TCP is a perfectionist and that's what you want for Web transmissions, e-mail, and application downloads. But sometimes we're willing to sacrifice perfection for speed. You'd make this sacrifice for streaming media applications like Windows Media Player, Real Player, Internet voice chat, and video conferencing. Having to wait to make sure each packet is perfectly sent would otherwise lead to awkward pauses that interrupt real-time listening. It'd be better to just grab the packets as they come and play them, even if they have minor errors. Packets are small enough that if one packet doesn't arrive, you can ignore it and move on to the next without too much quality disruption. A protocol called **UDP (user datagram protocol)**[20] does exactly this, working as a TCP stand-in when you've got the need for speed, and are willing to sacrifice quality. If you've ever watched a Web video or had a Web-based phone call and the quality got sketchy, it's probably because there were packet problems, but UDP kept on chugging, making the "get it fast" instead of "get it perfect" trade-off.

20. Protocol that operates instead of TCP in applications where delivery speed is important and quality can be sacrificed.

VoIP: When Phone Calls Are Just Another Internet Application

The increasing speed and reliability of the Internet means that applications such as Internet phone calls (referred to as *VoIP*, or **voice over Internet protocol**[21]) are becoming more reliable. That doesn't just mean that Skype becomes a more viable alternative for consumer landline and mobile phone calls; it's also good news for many businesses, governments, and nonprofits.

Many large organizations maintain two networks—one for data and another for *POTS* (plain old telephone service). Maintaining two networks is expensive, and while conventional phone calls are usually of a higher quality than their Internet counterparts, POTS equipment is also inefficient. Old phone systems use a technology called *circuit switching*. A "circuit" is a dedicated connection between two entities. When you have a POTS phone call, a circuit is open, dedicating a specific amount of capacity between you and the party on the other end. You're using that "circuit" regardless of whether you're talking. Pause between words or put someone on hold, and the circuit is still in use. Anyone who has ever tried to make a phone call at a busy time (say, early morning on Mother's Day or at midnight on New Year's Eve) and received an "all circuits are busy" recording has experienced congestion on an inefficient circuit-switched phone network.

But unlike circuit-switched counterparts, Internet networks are packet-switched networks, which can be more efficient. Since we can slice conversations up into packets, we can squeeze them into smaller spaces. If there are pauses in a conversation or someone's on hold, applications don't hold up the network. And that creates an opportunity to use the network's available capacity for other users. The trade-off is one that swaps circuit switching's quality of service (QoS) with packet switching's efficiency and cost savings. Try to have a VoIP call when there's too much traffic on a portion of the network and your call quality will drop. But packet switching quality is getting much better. Networking standards are now offering special features, such as "packet prioritization," that can allow voice packets to gain delivery priority over packets for applications like e-mail, where a slight delay is OK.

When voice is digitized, "telephone service" simply becomes another application that sits on top of the Internet, like the Web, e-mail, or FTP. VoIP calls between remote offices can save long distance charges. And when the

21. Transmission technologies that enable voice communications (phone calls) to take place over the Internet as well as private packet-switched networks.

phone system becomes a computer application, you can do a lot more. Well-implemented VoIP systems allow users' browsers access to their voice mail inbox, one-click video conferencing and call forwarding, point-and-click conference call setup, and other features, but you'll still have a phone number, just like with POTS.

What Connects the Routers and Computers?

Routers are connected together, either via cables or wirelessly. A cable connecting a computer in a home or office is probably copper (likely what's usually called an Ethernet cable), with transmissions sent through the copper via electricity. Long-haul cables, those that carry lots of data over long distances, are usually fiber-optic lines—glass lined cables that transmit light (light is faster and travels farther distances than electricity, but fiber-optic networking equipment is more expensive than the copper-electricity kind). Wireless transmission can happen via Wi-Fi (for shorter distances), or cell phone tower or satellite over longer distances. But the beauty of the Internet protocol suite (TCP/IP) is that it doesn't matter what the actual transmission media are. As long as your routing equipment can connect any two networks, and as long as that equipment "speaks" IP, then you can be part of the Internet.

In reality, your messages likely transfer via lots of different transmission media to get to their final destination. If you use a laptop connected via Wi-Fi, then that wireless connection finds a base station, usually within about three hundred feet. That base station is probably connected to a local area network (LAN) via a copper cable. And your firm or college may connect to fast, long-haul portions of the Internet via fiber-optic cables provided by that firm's Internet service provider (ISP).

Most big organizations have multiple ISPs for redundancy, providing multiple paths in and out of a network. This is so that if a network connection provided by one firm goes down, say an errant backhoe cuts a cable, other connections can route around the problem (see Figure 12.1).

In the United States (and in most deregulated telecommunications markets), Internet service providers come in all sizes, from smaller regional players to sprawling international firms. When different ISPs connect their networking equipment together to share traffic, it's called **peering**[22]. Peering usually takes place at neutral sites called *Internet exchange points* (IXPs), although some firms also

22. When separate ISPs link their networks to swap traffic on the Internet.

have private peering points. Carriers usually don't charge one another for peering. Instead, "the money is made" in the ISP business by charging the end-points in a network—the customer organizations and end users that an ISP connects to the Internet. Competition among carriers helps keep prices down, quality high, and innovation moving forward.

Finance Has a Need for Speed

When many folks think of Wall Street trading, they think of the open outcry pit at the New York Stock Exchange (NYSE). But human traders are just too slow for many of the most active trading firms. Over half of all U.S. stock trades and a quarter of worldwide currency trades now happen via programs that make trading decisions without any human intervention.H. Timmons, "A London Hedge Fund that Opts for Engineers, Not M.B.A.'s," *New York Times*, August 18, 2006. There are many names for this automated, data-driven frontier of finance—algorithmic trading, black-box trading, or high-frequency trading. And while firms specializing in automated, high-frequency trading represent only about 2 percent of the trading firms operating in the United States, they account for about three quarters of all U.S. equity trading volume.R. Iati, "The Real Story of Trading Software Espionage," *Advanced Trading*, July 10, 2009.

Programmers lie at the heart of modern finance. "A geek who writes code—those guys are now the valuable guys" says the former head of markets systems at Fidelity Investments, and that rare breed of top programmer can make "tens of millions of dollars" developing these systems.A. Berenson, "Arrest Over Software Illuminates Wall St. Secret," *New York Times*, August 23, 2009. Such systems leverage data mining and other model-building techniques to crunch massive volumes of data and discover exploitable market patterns. Models are then run against real-time data and executed the instant a trading opportunity is detected. (For more details on how data is gathered and models are built, see Chapter 11 "The Data Asset: Databases, Business Intelligence, and Competitive Advantage".)

Winning with these systems means being quick—very quick. Suffer delay (what techies call *latency*) and you may have missed your opportunity to pounce on a signal or market imperfection. To cut latency, many trading firms are moving their servers out of their own data centers and into **colocation facility**[23]. These facilities act as storage places where a firm's servers get superfast connections as close to the action as possible. And by renting space in a "*colo*," a firm gets someone else to manage the electrical and cooling issues, often providing more robust power backup and lower energy costs than a firm might get on its own.

Equinix, a major publicly traded IXP and colocation firm with facilities worldwide, has added a growing number of high-frequency trading firms to a roster of customers that includes e-commerce, Internet, software, and telecom

23. Sometimes called a "colo," or carrier hotel; provides a place where the gear from multiple firms can come together and where the peering of Internet traffic can take place. Equipment connecting in colos could be high-speed lines from ISPs, telecom lines from large private data centers, or even servers hosted in a colo to be closer to high-speed Internet connections.

companies. In northern New Jersey alone (the location of many of the servers where "Wall Street" trading takes place), Equinix hosts some eighteen exchanges and trading platforms as well as the NYSE Secure Financial Transaction Infrastructure (SFTI) access node.

Less than a decade ago, eighty milliseconds was acceptably low latency, but now trading firms are pushing below one millisecond into microseconds.I. Schmerken, "High-Frequency Trading Shops Play the Colocation Game," *Advanced Trading*, October 5, 2009. So it's pretty clear that understanding how the Internet works, and how to best exploit it, is of fundamental and strategic importance to those in finance. But also recognize that this kind of automated trading comes with risks. Systems that run on their own can move many billions in the blink of an eye, and the actions of one system may cascade, triggering actions by others.

The spring 2010 "Flash Crash" resulted in a nearly 1,000-point freefall in the Dow Jones Industrial Index, it's biggest intraday drop ever. Those black boxes can be mysterious—months after the May 6th event, experts were still parsing through trading records, trying to unearth how the flash crash happened.E. Daimler and G. Davis, "'Flash Crash' Proves Diversity Needed in Market Mechanisms," *Pittsburgh Post-Gazette*, May 29, 2010; H. Moore, "'Flash Crash' Anniversary Leaves Unanswered Questions," *Marketplace Radio*, May 5, 2011. Regulators and lawmakers recognize they now need to understand technology, telecommunications, and its broader impact on society so that they can create platforms that fuel growth without putting the economy at risk.

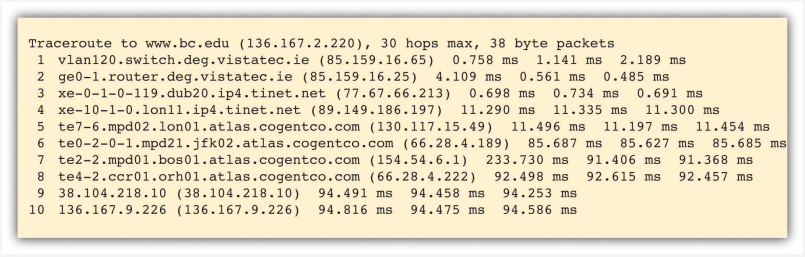
Watching the Packet Path via Traceroute

Want to see how packets bounce from router to router as they travel around the Internet? Check out a tool called *traceroute*. Traceroute repeatedly sends a cluster of three packets starting at the first router connected to a computer, then the next, and so on, building out the path that packets take to their destination.

Traceroute is built into all major desktop operating systems (Windows, Macs, Linux), and several Web sites will run traceroute between locations (traceroute.org and visualroute.visualware.com are great places to explore).

The message below shows a traceroute performed between Irish firm VistaTEC and Boston College. At first, it looks like a bunch of gibberish, but if we look closely, we can decipher what's going on.

Figure 12.5



```
Traceroute to www.bc.edu (136.167.2.220), 30 hops max, 38 byte packets
 1  vlan120.switch.deg.vistatec.ie (85.159.16.65)  0.758 ms  1.141 ms  2.189 ms
 2  ge0-1.router.deg.vistatec.ie (85.159.16.25)  4.109 ms  0.561 ms  0.485 ms
 3  xe-0-1-0-119.dub20.ip4.tinet.net (77.67.66.213)  0.698 ms  0.734 ms  0.691 ms
 4  xe-10-1-0.lon11.ip4.tinet.net (89.149.186.197)  11.290 ms  11.335 ms  11.300 ms
 5  te7-6.mpd02.lon01.atlas.cogentco.com (130.117.15.49)  11.496 ms  11.197 ms  11.454 ms
 6  te0-2-0-1.mpd21.jfk02.atlas.cogentco.com (66.28.4.189)  85.687 ms  85.627 ms  85.685 ms
 7  te2-2.mpd01.bos01.atlas.cogentco.com (154.54.6.1)  233.730 ms  91.406 ms  91.368 ms
 8  te4-2.ccr01.orh01.atlas.cogentco.com (66.28.4.222)  92.498 ms  92.615 ms  92.457 ms
 9  38.104.218.10 (38.104.218.10)  94.491 ms  94.458 ms  94.253 ms
10  136.167.9.226 (136.167.9.226)  94.816 ms  94.475 ms  94.586 ms
```

The table above shows ten hops, starting at a domain in vistatec.ie and ending in 136.167.9.226 (the table doesn't say this, but all IP addresses starting with 136.167 are Boston College addresses). The three groups of numbers at the end of three lines shows the time (in milliseconds) of three packets sent out to test that hop of our journey. These numbers might be interesting for network administrators trying to diagnose speed issues, but we'll ignore them and focus on how packets get from point to point.

At the start of each line is the name of the computer or router that is relaying packets for that leg of the journey. Sometimes routers are named, and sometimes they're just IP addresses. When routers are named, we can tell what network a packet is on by looking at the domain name. By looking at the router names to the left of each line in the traceroute above, we see that the first two hops are within the vistatec.ie network. Hop 3 shows the first router outside

the vistatec.ie network. It's at a domain named tinet.net, so this must be the name of VistaTEC's Internet service provider since it's the first connection outside the vistatec.ie network.

Sometimes routers names suggest their locations (oftentimes they use the same three character abbreviations you'd see in airports). Look closely at the hosts in hops 3 through 7. The subdomains dub20, lon11, lon01, jfk02, and bos01 suggest the packets are going from Dublin, then east to London, then west to New York City (John F. Kennedy International Airport), then north to Boston. That's a long way to travel in a fraction of a second!

Hop 4 is at tinet.net, but hop 5 is at cogentco.com (look them up online and you'll find out that cogentco.com, like tinet.net, is also an ISP). That suggests that between those hops peering is taking place and traffic is handed off from carrier to carrier.

Hop 8 is still cogentco.com, but it's not clear who the unnamed router in hop 9, 38.104.218.10, belongs to. We can use the Internet to sleuth that out, too. Search the Internet for the phrase "IP address lookup" and you'll find a bunch of tools to track down the organization that "owns" an IP address. Using the tool at whatismyip.com, I found that this number is registered to PSI Net, which is now part of cogentco.com.

Routing paths, ISPs, and peering all revealed via traceroute. You've just performed a sort of network "CAT scan" and looked into the veins and arteries that make up a portion of the Internet. Pretty cool!

If you try out traceroute on your own, be aware that not all routers and networks are traceroute friendly. It's possible that as your trace hits some hops along the way (particularly at the start or end of your journey), three "*" characters will show up at the end of each line instead of the numbers indicating packet speed. This indicates that traceroute has timed out on that hop. Some networks block traceroute because hackers have used the tool to probe a network to figure out how to attack an organization. Most of the time, though, the hops between the source and destination of the traceroute (the steps involving all the ISPs and their routers) are visible.

Traceroute can be a neat way to explore how the Internet works and reinforce the topics we’ve just learned. Search for traceroute tools online or browse the Internet for details on how to use the traceroute command built into your computer.

There’s Another Internet?

If you’re a student at a large research university, there’s a good chance that your school is part of Internet2. Internet2 is a research network created by a consortium of research, academic, industry, and government firms. These organizations have collectively set up a high-performance network running at speeds of up to one hundred gigabits per second to support and experiment with demanding applications. Examples include high-quality video conferencing; high-reliability, high-bandwidth imaging for the medical field; and applications that share huge data sets among researchers.

If your university is an Internet2 member and you’re communicating with another computer that’s part of the Internet2 consortium, then your organization’s routers are smart enough to route traffic through the superfast Internet2 backbone. If that’s the case, you’re likely already using Internet2 without even knowing it!

KEY TAKEAWAYS

- TCP/IP, or the Internet protocol suite, helps get perfect copies of Internet transmissions from one location to another. TCP works on the ends of transmission, breaking up transmissions up into manageable packets at the start and putting them back together while checking quality at the end. IP works in the middle, routing packets to their destination.
- Routers are special computing devices that forward packets from one location to the next. Routers are typically connected with more than one outbound path, so in case one path becomes unavailable, an alternate path can be used.
- UDP is a replacement for TCP, used when it makes sense to sacrifice packet quality for delivery speed. It's often used for media streaming.
- TCP/IP doesn't care about the transition media. This allows networks of different types—copper, fiber, and wireless—to connect to and participate in the Internet.
- The ability to swap in new applications, protocols, and media files gives the network tremendous flexibility.
- Decentralization, fault tolerance, and redundancy help keep the network open and reliable.
- VoIP allows voice and phone systems to become an application traveling over the Internet. This is allowing many firms to save money on phone calls and through the elimination of old, inefficient circuit-switched networks. As Internet applications, VoIP phone systems can also have additional features that circuit-switched networks lack. The primary limitation of many VoIP systems is quality of service.
- Many firms in the finance industry have developed automated trading models that analyze data and execute trades without human intervention. Speeds substantially less than one second may be vital to capitalizing on market opportunities, so firms are increasingly moving equipment into collocation facilities that provide high-speed connectivity to other trading systems.

QUESTIONS AND EXERCISES

1. How can the Internet consist of networks of such physically different transmission media—cable, fiber, and wireless?
2. What is the difference between TCP and UDP? Why would you use one over the other?
3. Would you recommend a VoIP phone system to your firm or University? Why or why not? What are the advantages? What are the disadvantages? Can you think of possible concerns or benefits not mentioned in this section? Research these concerns online and share your finding with your instructor.
4. What are the risks in the kinds of automated trading systems described in this section? Conduct research and find an example of where these systems have caused problems for firms and/or the broader market. What can be done to prevent such problems? Whose responsibility is this?
5. Search the Internet for a traceroute tool, or look online to figure out how to use the traceroute command built into your PC. Run three or more traceroutes to different firms at different locations around the world. List the number of ISPs that show up in the trace. Circle the areas where peering occurs. Do some of the "hops" time out with "*" values returned? If so, why do you think that happened?
6. Find out if your school or employer is an Internet2 member. If it is, run traceroutes to schools that are and are not members of Internet2. What differences do you see in the results?

12.4 Last Mile: Faster Speed, Broader Access

LEARNING OBJECTIVES

1. Understand the last-mile problem and be able to discuss the pros and cons of various broadband technologies, including DSL, cable, fiber, and various wireless offerings.
2. Describe 3G and 4G systems, listing major technologies and their backers.
3. Understand the issue of Net neutrality and put forth arguments supporting or criticizing the concept.

The **Internet backbone**[24] is made of fiber-optic lines that carry data traffic over long distances. Those lines are pretty speedy. In fact, several backbone providers, including AT&T and Verizon, are rolling out infrastructure with 100 Gbps transmission speeds (that's enough to transmit a two-hour high-definition [HD] movie in about eight seconds).T. Spangler, "Cisco Clarifies 100-Gig AT&T Backbone Claim," *Multichannel News*, March 9, 2010; Zacks.com, "AT&T Tests 100 Gb Ethernet in Move toward Faster Internet," *SeekingAlpha*, March 10, 2010. But when considering overall network speed, remember **Amdahl's Law**[25]: a system's speed is determined by its slowest component.G. Gilder, *Telecosm: How Infinite Bandwidth Will Revolutionize Our World* (New York: Free Press, 2000). More often than not, the bottleneck isn't the backbone but the so-called **last mile**[26], or the connections that customers use to get online.

High-speed last-mile technologies are often referred to as *broadband Internet access* (or just **broadband**[27]). What qualifies as broadband varies. In 2009, the Federal Communications Commission (FCC) redefined broadband as having a minimum speed of 768 Kbps (roughly fourteen times the speed of those old 56 Kbps modems). Other agencies worldwide may have different definitions. But one thing is clear: a new generation of bandwidth-demanding services requires more capacity. As we increasingly consume Internet services like HD streaming, real-time gaming, video conferencing, and music downloads, we are in fact becoming a bunch of voracious, bit-craving gluttons.

With the pivotal role the United States has played in the creation of the Internet, and in pioneering software, hardware, and telecommunications industries, you might expect the United States to lead the world in last-mile broadband access. Not even close. A recent study ranked the United States twenty-sixth in download

24. High-speed data lines provided by many firms all across the world that interconnect and collectively form the core of the Internet.

25. A system's speed is determined by its slowest component.

26. Technologies that connect end users to the Internet. The last-mile problem refers to the fact that these connections are usually the slowest part of the network.

27. Broadly refers to high-speed Internet connections and is often applied to "last-mile" technologies.

speeds,S. Lawson, "US Ranks 26th in New Broadband Index," *Computerworld*, May 25, 2010. while others have ranked the United States far behind in speed, availability, and price.S. Hansell, "The Broadband Gap: Why Is Theirs Faster?" *New York Times*, March 10, 2009.

Sounds grim, but help is on the way. A range of technologies and firms are upgrading infrastructure and developing new systems that will increase capacity not just in the United States but also worldwide. Here's an overview of some of the major technologies that can be used to speed the Internet's last mile.

Understanding Bandwidth

When folks talk about **bandwidth**[28], they're referring to data transmission speeds. Bandwidth is often expressed in bits per second, or bps. Prefix letters associated with multiples of bps are the same as the prefixes we mentioned in Chapter 5 "Moore's Law: Fast, Cheap Computing and What It Means for the Manager" when discussing storage capacity in bytes: Kbps = thousand bits (or kilobits) per second, Mbps = million bits (or megabits) per second, Gbps = billion bits (or gigabits) per second (or terabit), and Tbps = trillion bits (or terabits) per second.

Remember, there are eight bits in a byte, and one byte is a single character. One megabyte is roughly equivalent to one digital book, forty-five seconds of music, or twenty seconds of medium-quality video.R. Farzad, "The Truth about Bandwidth," *BusinessWeek*, February 3, 2010. But you can't just divide the amount of bytes by eight to estimate how many bits you'll need to transfer. When a file or other transmission is sliced into packets (usually of no more than about 1,500 bytes), there's some overhead added. Those packets "wrap" data chunks in an envelope surrounded by source and destination addressing and other important information.

Here are some rough demand requirements for streaming media. For streaming audio like Pandora, you'd need at least 150 Kbps for acceptable regular quality, and at least 300 Kbps for high quality.Pandora, "Frequently Asked Questions," http://blog.pandora.com/faq. For streaming video (via Netflix), at a minimum you'd need 1.5 Mbps, but 3.0 Mbps will ensure decent video and audio. For what Netflix calls HD streaming, you'll need a minimum of 5 Mbps, but would likely want 8 Mbps or more to ensure the highest quality video and audio.LG Knowledge Base, "Bandwidth Needed for Instant Streaming," http://lgknowledgebase.com/kb/index.php?View=entry&EntryID=6241.

Cable Broadband

Roughly 90 percent of U.S. homes are serviced by a cable provider, each capable of using a thick copper wire to offer broadband access. That wire (called a **coaxial cable**[29] or *coax*) has shielding that reduces electrical interference, allowing cable signals to travel longer distances without degrading and with less chance of interference than conventional telephone equipment.

28. Network transmission speeds, typically expressed in some form of bits per second (bps).

29. Insulated copper cable commonly used by cable television providers.

One potential weakness of cable technology lies in the fact that most residential providers use a system that requires customers to share bandwidth with neighbors. If the guy next door is a BitTorrent-using bandwidth hog, your traffic could suffer.R. Thompson, "DSL Internet vs. Cable Internet," *High Speed Internet Access Guide*, March 23, 2010.

Cable is fast and it's getting faster. Many cable firms are rolling out a new technology called DOCSIS 3.0 that offers speeds up to and exceeding 50 Mbps (previous high-end speeds were about 16 Mbps and often much less than that). Cable firms are also creating so-called *fiber-copper hybrids* that run higher-speed fiber-optic lines into neighborhoods, then use lower-cost, but still relatively high-speed, copper infrastructure over short distances to homes.S. Hansell, "The Broadband Gap: Why Is Theirs Faster?" *New York Times*, March 10, 2009. Those are fast networks, but they are also very expensive to build, since cable firms are laying entirely new lines into neighborhoods instead of leveraging the infrastructure that they've already got in place.

DSL: Phone Company Copper

Digital subscriber line (DSL)[30] technology uses the copper wire the phone company has already run into most homes. Even as customers worldwide are dropping their landline phone numbers, the wires used to provide this infrastructure can still be used for broadband.

DSL speeds vary depending on the technology deployed. Worldwide speeds may range from 7 Mbps to as much as 100 Mbps (albeit over very short distances).S. Hansell, "The Broadband Gap: Why Is Theirs Faster?" *New York Times*, March 10, 2009. The Achilles heel of the technology lies in the fact that DSL uses standard copper telephone wiring. These lines lack the shielding used by cable, so signals begin to degrade the further you are from the connecting equipment in telephone company offices. Speeds drop off significantly at less than two miles from a central office or DSL hub. If you go four miles out, the technology becomes unusable. Some DSL providers are also using a hybrid fiber-copper system, but as with cable's copper hybrids, this is expensive to build.

The superspeedy DSL implementations that are popular in Europe and Asia work because foreign cities are densely populated and so many high-value customers can be accessed over short distances. In South Korea, for example, half the population lives in apartments, and most of those customers live in and around Seoul. This density also impacts costs—since so many people live in apartments, foreign carriers run fewer lines to reach customers, digging up less ground or stringing wires across fewer telephone poles. Their U.S. counterparts by contrast need to

30. Broadband technology that uses the wires of a local telephone network.

reach a customer base sprawled across the suburbs, so U.S. firms have much higher infrastructure costs. S. Hansell, "The Broadband Gap: Why Is Theirs Faster?" *New York Times*, March 10, 2009.

There's another company with copper, electricity-carrying cables coming into your home—the electrical utility. BPL, or broadband over power line, technology has been available for years. However, there are few deployments because it is considered to be pricier and less practical than alternatives.R. King, "Telecom Companies Scramble for Funding," *BusinessWeek*, August 3, 2009.

Fiber: A Light-Filled Glass Pipe to Your Doorstep

Fiber to the home (FTTH)[31] is the fastest last-mile technology around. It also works over long distances. Verizon's FiOS technology boasts 50 Mbps download speeds but has tested network upgrades that increase speeds by over six times that.S. Higginbotham, "Verizon Tests 10 Gbps to the Home. Yeah, You'll Have to Share," *GigaOM*, December 17, 2009. The problem with fiber is that unlike cable or DSL copper, fiber to the home networks weren't already in place. That means firms had to build their own fiber networks from scratch.

The cost of this build out can be enormous. Verizon, for example, has spent over $23 billion on its FTTH infrastructure. However, most experts think the upgrade was critical. Verizon has copper into millions of homes, but U.S. DSL is uncompetitive. Verizon's residential landline business was dying as users switch to mobile phone numbers, and while mobile is growing, Verizon Wireless is a joint venture with the United Kingdom's Vodaphone, not a wholly owned firm. This means it shares wireless unit profits with its partner. With FiOS, Verizon now offers pay television, competing with cable's core product. It also offers some of the fastest home broadband services anywhere, and it gets to keep everything it earns.

Google is also in the process of bringing high-speed fiber to the home in several U.S. communities, including Kansas City, Kansas, and Kansas City, Missouri. Google deems its effort an experiment—it's more interested in learning how developers and users take advantage of ultrahigh-speed fiber to the home (e.g., what kinds of apps are created and used, how do usage and time spent online change), rather than becoming a nationwide ISP itself. Google says it will investigate ways to build and operate networks less expensively and plans to share findings with others. The Google network will be "open," allowing other service providers to use Google's infrastructure to resell services to consumers. The firm has pledged to bring speeds of 1 Gbps at competitive prices to at least 50,000 and potentially as many as 500,000 homes. Over 1,100 U.S. communities applied to be part of the Google experimental fiber network.M. Ingersoll and J. Kelly, "Think Big with a Gig: Our Experimental

31. Broadband service provided via light-transmitting fiber-optic cables.

Fiber Network," The Google Blog, February 2, 2010; L. Rao, "The Final Tally: More Than 1100 Cities Apply for Google's Fiber Network," *TechCrunch*, March 27, 2010.

Wireless

Mobile wireless service from cell phone access providers is delivered via cell towers. While these providers don't need to build a residential wired infrastructure, they still need to secure space for cell towers, build the towers, connect the towers to a backbone network, and license the **wireless spectrum**[32] (or airwave frequency space) for transmission.

We need more bandwidth for mobile devices, too. AT&T now finds that the top 3 percent of its mobile network users gulp up 40 percent of the network's capacity (thanks, iPhone users), and network strain will only increase as more people adopt smartphones. These users are streaming Major League Baseball games, exploring the planet with Google Earth, watching YouTube and Netflix, streaming music through Pandora, and more. Get a bunch of iPhone users in a crowded space, like in a college football stadium on game day, and the result is a network-choking data traffic jam. AT&T estimates that it's not uncommon for 80 percent of game-day iPhone users to take out their phones and surf the Web for stats, snap and upload photos, and more. But cell towers often can't handle the load.R. Farzad, "AT&T's iPhone Mess," *BusinessWeek*, February 3, 2010. If you've ever lost coverage in a crowd, you've witnessed mobile network congestion firsthand. Trying to have enough capacity to avoid congestion traffic jams will cost some serious coin. In the midst of customer complaints, AT&T committed to spending $18 billion on network upgrades to address its wireless capacity problem.C. Edwards and O. Kharif, "Sprint's Bold Play on a 4G Network," *BusinessWeek*, March 30, 2010.

Table 12.1 Average Demand Usage by Function

Usage	Demand
Voice Calls	4 MB/hr.
iPhone Browsing	40–60 MB/hr.
Net Radio	60 MB/hr.
YouTube	200–400 MB/hr.
Conventional mobile phones use an estimated 100 MB/month, iPhones 560 MB/month, and iPads almost 1 GB/month.	

Source: R. Farzad, "The Truth about Bandwidth," *BusinessWeek*, February 3, 2010.

32. Frequencies used for communication. Most mobile cell phone services have to license spectrum. Some technologies (such as Wi-Fi) use unlicensed public spectrum.

We're in the midst of transitioning from third generation (*3G*) to fourth generation (*4G*) wireless networks. 3G systems offer access speeds usually less than 2 Mbps (often a lot less).K. German, "On Call: Welcome to 4G," *CNET*, March 9, 2010. While variants of 3G wireless might employ an alphabet soup of technologies—EV-DO (evolution data optimized), UMTS (universal mobile telecommunications systems), and HSDPA (high-speed downlink packet link access) among them—3G standards can be narrowed down to two camps: those based on the dominant worldwide standard called *GSM* (global system for mobile communications) and the runner-up standards based on *CDMA* (code division multiple access). Most of Europe and a good chunk of the rest of the world use GSM. In the United States, AT&T and T-Mobile use GSM-based 3G. Verizon Wireless and Sprint use the CDMA 3G standard. Typically, handsets designed for one network can't be used on networks supporting the other standard. CDMA has an additional limitation in not being able to use voice and data at the same time.

But 3G is being replaced by high-bandwidth 4G (fourth-generation) mobile networks. 4G technologies also fall into two standards camps: LTE (Long Term Evolution) and WiMAX (Worldwide Interoperability for Microwave Access).

LTE looks like the global winner. In the United States, every major wireless firm, except for Sprint, is betting on LTE victory. Bandwidth for the service rivals what we'd consider fast cable a few years back. Average speeds range from 5 to 12 Mbps for downloads and 2 to 5 Mbps for upload, although Verizon tests in Boston and Seattle showed download speeds as high as 50 Mbps and upload speeds reaching 25 Mbps.K. German, "On Call: Welcome to 4G," *CNET*, March 9, 2010.

Competing with LTE is WiMAX; don't confuse it with Wi-Fi. As with other 3G and 4G technologies, WiMAX needs cell towers and operators need to have licensed spectrum from their respective governments (often paying multibillion-dollar fees to do so). Average download and upload speeds should start out at 3–6 Mbps and 1 Mbps, respectively, although this may go much higher.N. Lee, "Sprint's 4G Plans Explained," *CNET*, May 19, 2010.

WiMAX looks like a particularly attractive option for cable firms, offering them an opportunity to get into the mobile phone business and offer a "quadruple play" of services: pay television, broadband Internet, home phone, and mobile. Comcast and Time Warner have both partnered with Clearwire (a firm majority-owned by Sprint), to gain access to WiMAX-based 4G mobile.

4G could also rewrite the landscape for home broadband competition. If speeds increase, it may be possible for PCs, laptops, and set-top boxes (STB) to connect to the Internet wirelessly via 4G, cutting into DSL, cable, and fiber markets.

Satellite Wireless

Wireless systems provided by earth-bound base stations like cell phone towers are referred to as *terrestrial wireless*, but it is possible to provide telecommunications services via satellite. Early services struggled due to a number of problems. For example, the first residential satellite services were only used for downloads, which still needed a modem or some other connection to send any messages from the computer to the Internet. Many early systems also required large antennas and were quite expensive. Finally, some services were based on satellites in geosynchronous earth orbit (GEO). GEO satellites circle the earth in a fixed, or stationary, orbit above a given spot on the globe, but to do so they must be positioned at a distance that is roughly equivalent to the planet's circumference. That means signals travel the equivalent of an around-the-world trip to reach the satellite and then the same distance to get to the user. The "last mile" became the last 44,000 miles at best. And if you used a service that also provided satellite upload as well as download, double that to about 88,000 miles. All that distance means higher latency (more delay).G. Ou, "Why Satellite Service Is So Slow," *ZDNet*, February 23, 2008.

A firm named O3b Networks thinks it might have solved the challenges that plagued early pioneers. O3b has an impressive list of big-name backers that include HSBC bank, cable magnate John Malone, European aerospace firm SES, and Google.

The name O3b stands for the "Other 3 Billion," of the world's population who lack broadband Internet access, and the firm hopes to provide "fiber-quality" wireless service to more than 150 countries, specifically targeting underserved portions of the developing world. These "middle earth orbit" satellites will circle closer to the earth to reduce latency (only about 5,000 miles up, less than one-fourth the distance of GEO systems). To maintain the lower orbit, O3b's satellites orbit faster than the planet spins, but with plans to launch as many as twenty satellites, the system will constantly blanket regions served. If one satellite circles to the other side of the globe, another one will circle around to take its place, ensuring there's always an O3b "bird" overhead.

Only about 3 percent of the sub-Saharan African population uses the Internet, compared to about 70 percent in the United States. But data rates in the few places served can cost as much as one hundred times the rates of comparable systems in the industrialized world.G. Lamb, "O3b Networks: A Far-Out Plan to Deliver the Web," *Christian Science Monitor*, September 24, 2008. O3b hopes to change that equation and significantly lower access rates. O3b customers will be local telecommunication firms, not end users. The plan is for local firms to buy O3b's services wholesale and then resell it to customers alongside rivals who can do the same thing, collectively providing more consumer access, higher quality, and lower

prices through competition. O3b is a big, bold, and admittedly risky plan, but if it works, its impact could be tremendous.

Wi-Fi and Other Hotspots

Many users access the Internet via **Wi-Fi**[33] (which stands for *wireless fidelity*). Computer and mobile devices have Wi-Fi antennas built into their chipsets, but to connect to the Internet, a device needs to be within range of a *base station* or *hotspot*. The base station range is usually around three hundred feet (you might get a longer range outdoors and with special equipment; and less range indoors when signals need to pass through solid objects like walls, ceilings, and floors). Wi-Fi base stations used in the home are usually bought by end users, then connected to a cable, DSL, or fiber provider.

And now a sort of mobile phone hotspot is being used to overcome limitations in those services, as well. Mobile providers can also be susceptible to poor coverage indoors. That's because the spectrum used by most mobile phone firms doesn't travel well through solid objects. Cell coverage is also often limited in the United States because of a lack of towers, which is a result of the *NIMBY problem* (not in my backyard). People don't want an eighty-foot to four-hundred-foot unsightly tower clouding their local landscape, even if it will give their neighborhood better cell phone coverage.G. Dechter and O. Kharif, "How Craig McCaw Built a 4G Network on the Cheap," *BusinessWeek*, May 24, 2010. To overcome reception and availability problems, mobile telecom services firms have begun offering femtocells. These devices are usually smaller than a box of cereal and can sell for $150 or less (some are free with specific service contracts). Plug a femtocell into a high-speed Internet connection like an in-home cable or fiber service and you can get "five-bar" coverage in a roughly 5,000-square-foot footprint.C. Mims, "A Personal Cell Phone Tower," *Technology Review*, April 7, 2010. That can be a great solution for someone who has an in-home, high-speed Internet connection, but wants to get phone and mobile data service indoors, too.

Net Neutrality: What's Fair?

33. A term used to brand wireless local-area networking devices. Devices typically connect to an antenna-equipped base station or hotspot, which is then connected to the Internet. Wi-Fi devices use standards known as IEEE 802.11, and various version of this standard (e.g., b, g, n) may operate in different frequency bands and have access ranges.

Across the world, battle lines are being drawn regarding the topic of Net neutrality. Net neutrality is the principle that all Internet traffic should be treated equally.M. Honan, "Inside Net Neutrality," *MacWorld*, February 12, 2008. Sometimes access providers have wanted to offer varying (some say "discriminatory") coverage, depending on the service used and bandwidth consumed. But where regulation stands is currently in flux. In a pivotal U.S. case, the FCC ordered Comcast to stop throttling (blocking or slowing down) subscriber access to the peer-to-peer file sharing service BitTorrent. BitTorrent users can consume a huge amount of bandwidth—the service is often used to transfer large files, both legitimate (like

version of the Linux operating system) and pirated (HD movies). Then in spring 2010, a federal appeals court moved against the FCC's position, unanimously ruling that the agency did not have the legal authority to dictate terms to Comcast."What Is Net Neutrality?" *The Week*, April 7, 2010.

On one side of the debate are Internet service firms, with Google being one of the strongest Net neutrality supporters. In an advocacy paper, Google states, "Just as telephone companies are not permitted to tell consumers who they can call or what they can say, broadband carriers should not be allowed to use their market power to control activity online."Google, "A Guide to Net Neutrality for Google Users," 2008, http://www.docstoc.com/docs/1064274/A-Guide-to-Net-Neutrality-for-Google-Users. Many Internet firms also worry that if network providers move away from flat-rate pricing toward usage-based (or metered) schemes, this may limit innovation. Says Google's Vint Cerf (who is considered one of the "fathers of the Internet" for his work on the original Internet protocol suite) "You are less likely to try things out. No one wants a surprise bill at the end of the month."M. Jesdanun, "As the Internet Turns 40, Barriers Threaten Growth," *Technology Review*, August 31, 2009. Metered billing may limit the use of everything from iTunes to Netflix; after all, if you have to pay for per-bit bandwidth consumption as well as for the download service, then it's as if you're paying twice.

The counterargument is that if firms are restricted from charging more for their investment in infrastructure and services, then they'll have little incentive to continue to make the kinds of multibillion-dollar investments that innovations like 4G and fiber networks require. Telecom industry executives have railed against Google, Microsoft, Yahoo! and others, calling them free riders who earn huge profits by piggybacking off ISP networks, all while funneling no profits back to the firms that provide the infrastructure. One Verizon vice president said, "The network builders are spending a fortune constructing and maintaining the networks that Google intends to ride on with nothing but cheap servers....It is enjoying a free lunch that should, by any rational account, be the lunch of the facilities providers."A. Mohammed, "Verizon Executive Calls for End to Google's 'Free Lunch,'" *Washington Post*, February 7, 2006. AT&T's previous CEO has suggested that Google, Yahoo! and other services firms should pay for "preferred access" to the firm's customers. The CEO of Spain's Telefonica has also said the firm is considering charging Google and other Internet service firms for network use.I. Lunden, "Broadband Content Bits: Web Drama Investment, PPL Video Store, Telefonica to Charge?" *paidContent:UK*, February 11, 2010.

ISPs also lament the relentlessly increasingly bandwidth demands placed on their networks. Back in 2007, YouTube streamed as much data in three months as the world's radio, cable, and broadcast television channels combined stream in one year,B. Swanson, "The Coming Exaflood," *Wall Street Journal*, January 20, 2007. and

YouTube has only continued to grow since then. Should ISPs be required to support the strain of this kind of bandwidth hog? And what if this one application clogs network use for other traffic, such as e-mail or Web surfing? Similarly, shouldn't firms have the right to prioritize some services to better serve customers? Some network providers argue that services like video chat and streaming audio should get priority over, say, e-mail which can afford slight delay without major impact. In that case, there's a pretty good argument that providers should be able to discriminate against services. But improving efficiency and throttling usage are two different things.

Internet service firms say they create demand for broadband business, broadband firms say Google and allies are ungrateful parasites that aren't sharing the wealth. The battle lines on the Net neutrality frontier continue to be drawn, and the eventual outcome will impact consumers, investors, and will likely influence the continued expansion and innovation of the Internet.

Summing Up

Hopefully, this chapter helped reveal the mysteries of the Internet. It's interesting to know how "the cloud" works but it can also be vital. As we've seen, the executive office in financial services firms considers mastery of the Internet infrastructure to be critically important to their competitive advantage. Media firms find the Internet both threatening and empowering. The advancement of last-mile technologies and issues of Net neutrality will expose threats and create opportunity. And a manager who knows how the Internet works will be in a better position to make decisions about how to keep the firm and its customers safe and secure, and be better prepared to brainstorm ideas for winning in a world where access is faster and cheaper, and firms, rivals, partners, and customers are more connected.

KEY TAKEAWAYS

- The slowest part of the Internet is typically the last mile, not the backbone. While several technologies can offer broadband service over the last mile, the United States continues to rank below many other nations in terms of access speed, availability, and price.
- Cable firms and phone companies can leverage existing wiring for cable broadband and DSL service, respectively. Cable services are often criticized for shared bandwidth. DSL's primary limitation is that it only works within a short distance of telephone office equipment.
- Fiber to the home can be very fast but very expensive to build.
- An explosion of high-bandwidth mobile applications is straining 3G networks. 4G systems may alleviate congestion by increasing capacities to near-cable speeds. Fentocells are another technology that can improve service by providing a personal mobile phone hotspot that can plug into in-home broadband access.
- The two major 3G standards (popularly referred to as GSM and CDMA) will be replaced by two unrelated 4G standards (LTE and WiMAX). GSM has been the dominant 3G technology worldwide. LTE looks like it will be the leading 4G technology.
- Satellite systems show promise in providing high-speed access to underserved parts of the world, but few satellite broadband providers have been successful so far.
- Net neutrality is the principle that all Internet traffic should be treated equally. Google and other firms say it is vital to maintain the openness of the Internet. Telecommunications firms say they should be able to limit access to services that overtax their networks, and some have suggested charging Google and other Internet firms for providing access to their customers.

QUESTIONS AND EXERCISES

1. Research online for the latest country rankings for broadband service. Where does the United States currently rank? Why?
2. Which broadband providers can service your home? Which would you choose? Why?
3. Research the status of Google's experimental fiber network. Report updated findings to your class. Why do you suppose Google would run this "experiment"? What other Internet access experiments has the firm been involved in?
4. Show your understanding of the economics and competitive forces of the telecom industry. Discuss why Verizon chose to go with fiber. Do you think this was a wise decision or not? Why? Feel free to do additional research to back up your argument.
5. Why have other nations enjoyed faster broadband speeds, greater availability, and lower prices?
6. The iPhone has been called both a blessing and a curse for AT&T. Why do you suppose this is so?
7. Investigate the status of mobile wireless offerings (3G and 4G). Which firm would you choose? Why? Which factors are most important in your decision?
8. Name the two dominant 3G standards. What are the differences between the two? Which firms in your nation support each standard?
9. Name the two dominant 4G standards. Which firms in your nation will support the respective standards?
10. Have you ever lost communication access—wirelessly or via wired connection? What caused the loss or outage?
11. What factors shape the profitability of the mobile wireless provider industry? How do these economics compare with the cable and wire line industry? Who are the major players and which would you invest in? Why?
12. Last-mile providers often advertise very fast speeds, but users rarely see speeds as high as advertised rates. Search online to find a network speed test and try it from your home, office, mobile device, or dorm. How fast is the network? If you're able to test from home, what bandwidth rates does your ISP advertise? Does this differ from what you experienced? What could account for this discrepancy?
13. How can 4G technology help cable firms? Why might it hurt them?
14. What's the difference between LEO satellite systems and the type of system used by O3b? What are the pros and cons of these efforts? Conduct some additional research. What is the status of O3b and other satellite broadband efforts?

15. What advantages could broadband offer to underserved areas of the world? Is Internet access important for economic development? Why or why not?
16. Does your carrier offer a fentocell? Would you use one? Why or why not?
17. Be prepared to debate the issue of Net neutrality in class. Prepare positions both supporting and opposing Net neutrality. Which do you support and why?
18. Investigate the status of Net neutrality laws in your nation and report your findings to your instructor. Do you agree with the stance currently taken by your government? Why or why not?