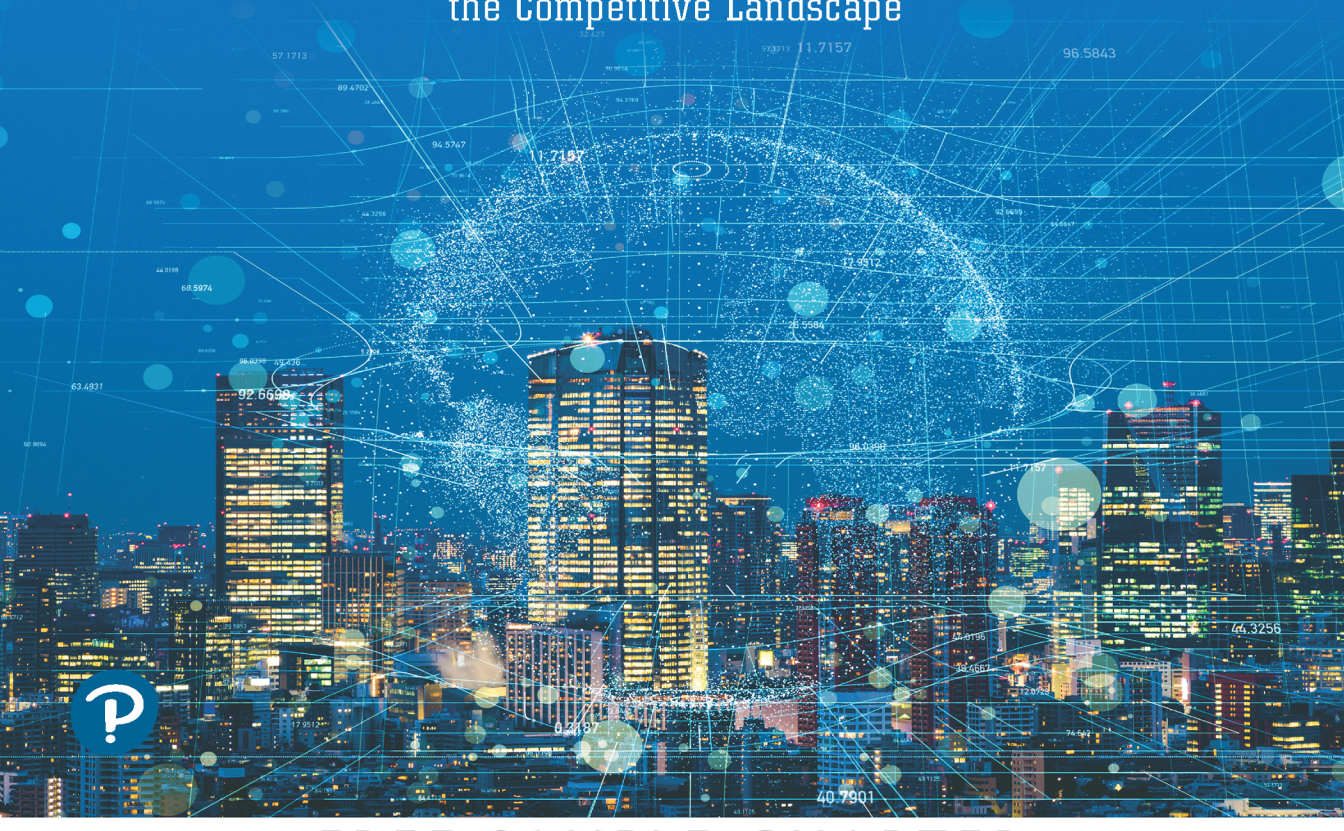
Annabel Z. Dodd

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



FREE SAMPLE CHAPTER

SHARE WITH OTHERS

PRAISE FOR *THE ESSENTIAL GUIDE TO TELECOMMUNICATIONS, SIXTH EDITION*

"Dodd's The Essential Guide to Telecommunications *provides the history and context that make a fundamental underpinning of modern business more accessible to technologists and businesspeople alike. This new edition of her primer is an essential reference in the continuously evolving communications landscape."*

—Tom Hopcroft, President and CEO,
Mass Technology Leadership Council

"Annabel Dodd's book is a clear guide and big-picture view of technologies and industries. It is an up-to-date guide for anyone who wants to be familiar with important innovations and key technologies. This is truly an industry bible for mobile, Internet, and networking services."

—Hiawatha Bray, Technology Reporter,
The Boston Globe

"Ms. Dodd's aptly titled The Essential Guide to Telecommunications *has been my bible for all things telecom since my days as an AT&T transmission network engineer nearly twenty years ago. Exhaustively and meticulously researched, concisely written for lay folks and techs/engineers alike, this book aids me in my current role as an IT Support Technician II when discussing new technology with our telecommunications department. Thank you to Ms. Dodd for keeping us all current!"*

—Todd Garbarini, IT Support Technician II
Commvault Systems, Inc.

"The Essential Guide to Telecommunications *is probably one of the most useful and well-written books on our telecom bookshelf. Annabel Z. Dodd does a great job of capturing a snapshot of the current telecom industry. Even those with little or no technical training should be able to understand the text. This is the perfect book for salespeople who want to learn more about the products and services they are selling, or for those who just want to keep up to date on the latest in telecom technology."*

—William Van Hefner, President,
Vantek Communications, Inc.

"Ms. Dodd continues to provide an excellent and thorough text on the telecommunications industry. As in her previous editions, she presents a good balance of technical and business-related information that is readily understandable by anyone with an interest in this key component of today's business environment. In her new edition, she has captured many of the recent changes in this dynamic field, which will affect every company in the years ahead. I strongly recommend her book to anyone who wants a better understanding of telecommunications."

—Joe McGrath, VP, Sage Pharmaceuticals, Inc.

"Annabel Dodd has a unique knack for explaining complex technologies in understandable ways. This latest revision of her book covers the rapid changes in the fields of broadband, cellular, and streaming technologies; newly developing 5G networks; and the constant changes happening in both wired and wireless networks. She also explains the consolidation going on in the industry, the impacts of social media, and software control and virtualization of provider networks. This book is a must-read for anyone wanting to understand the rapidly evolving world of telecommunications in the 21st century!"

—David Mash, Retired Senior Vice President for
Innovation, Strategy, and Technology
at Berklee College of Music

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

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 19

To Bob, Judy, Nancy, Laura, Steve, Bobby, Elizabeth,
Julia, Gabriel, Ari, Michael, Moses, Delancey, and Harry

This page intentionally left blank

Contents

Part II
Industry Overview and Regulations 123

Preface

When *The Essential Guide to Telecommunications* was first published in 1997, broadband and cellular networks were many times less complex. Voice calls were carried separately from data traffic, and e-mail required arcane commands and was used mostly at universities. The federal government had recently deregulated telecommunications and opened it to competitors. Deregulation opened voice and data networks to new competitors. These competitors competed with established providers for subscribers by offering lower prices. This competition drove innovation and resulted in the build-out of high-speed fiber-optic networks. Large incumbents responded with their own network improvements and lowered prices. A similar pattern occurred in cellular networks after 1999.

In the years since 1997, most small and medium-sized and even some large competitors were either acquired by large incumbents or went out of business. These incumbents also acquired other large providers that were formerly part of the Bell system. The result of these mergers is that today's telecommunications, cellular, and cable TV markets have far fewer competitors: mainly AT&T, CenturyLink, Comcast, and Verizon. Partly as a result of minimum competition, prices for broadband services are higher compared with most of the world.

Social networking, cloud, and Office software conglomerates Amazon, Facebook, and Microsoft have built large, cloud-located networks of data centers. Their services have disrupted commerce in each of their fields. Microsoft operates one of the four largest cloud services in the United States. It offers a platform on which developers customize Microsoft applications for enterprise customers. Additionally, their Teams service is used by enterprises to make low-cost international voice calls and video conference calls and collaborate on joint projects.

Google, which was started by Stanford graduate students, operates the largest search service in the United States. The founders used software to search the web and keep repositories of web site addresses. It quickly became an enormous company, whose popularity grew through word of mouth. They are now a huge conglomerate that earns billions of dollars each year through the advertising on their site.

Amazon was started by Jeff Bezos. Its cloud-based retail service is another example of a business that has had an enormous impact. Brick and mortar retailers have lost millions of dollars, chains have gone out of business, and many have closed a number of their stores. Amazon is still innovating with its home automation offering Alexa, its fast turnaround delivery service, its purchase of Whole Foods, and its entrance in drug deliveries for hospitals.

And AT&T and Verizon are building large fiber networks and cellular infrastructure to carry new generations of mobile networks. T-Mobile and Sprint are building out their cellular networks as well.

However, the number of choices consumers and enterprise customers have for their Internet access and broadband services as well as their mobile services has decreased and will shrink more if T-Mobile is granted permission to acquire Sprint's cellular network. If the Sprint acquisition is approved, the number of mobile operators for nationwide coverage will shrink from four to three. This is a significant change, one that may lead to higher prices for the students and young people that flock to T-Mobile for its low prices.

New 5th generation mobile networks promise to support higher data rates than ever before. However, these upgrades are costly, and require thousands of additional cell sites and antennas, particularly in downtown urban areas with large amounts of foot traffic. Mobile providers are additionally upgrading current 4th generation cellular networks. Both of these efforts will support higher speeds, some up to a gigabit per second. As capacity on mobile networks increases, they will support streaming video and, in some cases, broadband links to residential subscribers' homes.

Because of the greater capacity in mobile networks, many young people and students depend wholly on mobile networks for messaging, streaming, and social network access. Teens and twenty-somethings for the most part use Snapchat and Instagram (part of Facebook) social networks rather than Facebook and Twitter. Snapchat is newer, launched in 2011, and appeals to young people for its more visual service where users upload videos and photos, rather than biographies and other written material as on Facebook and other social networks.

Streaming services were first envisioned by Reed Hastings, the CEO and founder of Netflix. Netflix initially mailed DVDs to subscribers in iconic red envelops and stated at the time that Netflix would stream TV shows and movies when Wi-Fi became robust enough to support video traffic. Netflix is a disruptive service that changed user behavior and disrupted traditional sales of DVDs and movie theaters. Streaming caused Blockbuster, the largest seller of DVDs, which had outlets on every corner, to go out of business and movie theaters had to close many of their theaters due to fewer people going to movies. Netflix is now an international business with service in nearly 200 countries.

A core strategy of Netflix, Hulu, Amazon, and their competitors is to attract subscribers by offering popular TV shows and movies. Netflix was initially able to license the TV series and movies it offered from content providers such as Disney, Time Warner, and Universal Studios. As these companies started offering their own streaming services or were bought by larger companies, for example, AT&T and Comcast, less content became available for competing streaming providers. As a result, Netflix, Amazon, and others have poured billions of dollars into creating original content to attract subscribers. Content is a critical factor in people's decision to either drop cable TV or subscribe to smaller cable TV packages.

Software is the driving force in managing today's broadband and LAN (local area networks) networks. Broadband networks controlled by software are referred to as wide area software defined networks (W-SDNs). SDNs are also implemented in enterprise networks. Both implementations are controlled from central terminals programmed with commands that direct traffic to avoid routes with outages and congestion. Software is used to manage complex high-capacity broadband networks. Functions previously installed on proprietary hardware can be abstracted in non-proprietary hardware. These network functions include routers, servers dedicated to security, and gateways that translate between networks that use different protocols. Another way that networks are enabled to carry more traffic is the network equipment connected to fiber-optic cabling that enables gigabit and even terabit data rates. A terabit is equal to a thousand gigabits.

Networks that connect people have made the world smaller and opened up communications worldwide. However, the common protocols used on the Internet where everyone is connected to everyone else means that networks are inherently open to hackers who use these common protocols as a way to hack into organizations' networks.

Organizations large and small have experienced security breaches. Some breaches have resulted in the loss of millions of peoples' private information including their social security numbers. In addition, security breaches have cost enterprises millions of dollars in bad publicity and stolen intellectual property. To avoid major hacking attacks, enterprises hire outside consultants, and strengthen their security staff. They also educate users to the danger of opening attachments from people they don't know. These phishing emails contain malware able to contaminate entire networks. However, there is no 100 percent guarantee that any of these steps will protect an organization from a determined hacker. But organizations with strong security recover faster, and detect attacks more quickly.

This page intentionally left blank

Acknowledgments

Thank you to all of the many people that took the time to share important information about technology and government regulations. Staffs at the FCC and the Massachusetts Department of Telecommunications and Cable provided clear explanations of national and state regulations. Marketing Consultant David Gitner was a terrific source of information on storage systems. Geoff Bennett, Director, Solutions and Technology at Infinera, provided clear information about fiber-optic multiplexers, and Mike Quan, cofounder of Boston 360, illuminated information about virtual reality. James Chapman, Senior Product Manager at Ipswich, spoke with me about network management systems. Bob Xavier, Director, Systems and Networks at Berklee College of Music, gave me a tour of Berklee's IT department and discussed the issues involved in managing merging IT systems when colleges merge.

As always, Carly Premo Mello, IT Director, and Jamie V. Schiavone, Network Manager for Framingham, Massachusetts, discussed the challenges of managing security and storage networks. Joe Mulvey, IT director for Newton, Massachusetts, and his staff spent time discussing their broadband, Wi-Fi, and IT structures and gave me a tour of their data center. Mark Roberts, the Chief Marketing Officer at the former Shortel (now Mitel), discussed specialty applications using VoIP technology. All of these people provided insights into real-world issues.

Thank you also to Fernando Mousinho, Cisco Systems Director of Product Management for Endpoints, for his lucid explanation of Cisco Systems' office products and video conferencing services. Many thanks to Dave Parks, former Director of Segment Marketing at Ciena Corporation, for his generosity in providing information on Ciena's broadband hardware and software. Dave has been an enormous source of information for earlier editions of my book as well as for this sixth edition as has Joe McGrath, VP of Information Technologies, Sage Therapeutics. Thanks to Kevin Klett, VP of Product Management & Marketing at 128 Technology for his lucid explanations of their stateful routing software.

Thanks to Rick Swiderski, VP and General Manager at NEP Group, for his informative discussions of the challenges facing rural telephone companies. His first-hand knowledge was tremendously helpful. Thanks also to Kurt Raaflaub, head of strategic solutions marketing at ADTRAN. Kurt and his staff provided important information on the use of copper cabling connections to fiber cabling to bring high-speed broadband to rural areas. Glenn Axelrod of Axelrod Broadcast Solutions illuminated the details behind multiplexing technologies used in cable TV networks. Sal Tuzzeo at Nielsen discussed consumer trends in viewing television. Thanks as well to Joanta Stanke, Research Director at Point Topic Ltd,, for her information and graphic on Internet access patterns worldwide. Special appreciation to Mohammad Zulqarnain, Distinguished Architect of Global Solutions at Verizon Communications. Mohammad illuminated the important features and advantages of software defined networks. He further provided examples of how enterprises and branch offices are deploying the technology.

A special thank you to Tom Case, Chief Information Officer for the town of Lexington Massachusetts, who met with me and discussed the day-to-day issues involved in designing and maintaining municipal networks. A thank you also to Donna Drudik and Jim Thompson, California 911 Telecommunications Engineers, for discussing the importance and time criticality for handling calls to 911 emergency centers. Jim also provided information on technologies used for deploying emergency telecommunications services for handling text messages, mobile, and landline calls at emergency call centers. Thanks to Ben, vice president of security for a major financial company. Ben illuminated the challenges and technologies deployed to protect enterprises from hackers. And appreciation to Keith Wise for valuable assistance with the Study Guide.

And finally, thank you to the many people I spoke with that preferred to not have their names used. I appreciate the information each of you shared. Most importantly, thank you to my husband Bob Dodd who read everything I wrote multiple times and provided common sense advice on how to improve sections to clarify important concepts.

About the Author

Photo courtesy of Annabel Z. Dodd

Annabel Z. Dodd is on the faculty at Northeastern University's School of Professional Studies, where she teaches courses on data networks in the Master's Degree Program in Informatics. In addition to her university teaching, Annabel presents seminars to organizations worldwide. Her webinar on LTE Essentials for USTelecom attracted over 900 people.

Annabel has been an adjunct professor in the Master of Science in Technology Management program at the State University of New York at Stony Brook, where she taught in a joint program with The Institute of Industrial Policy Studies, Seoul, South Korea. In addition, the Fundación Innovación Bankinter selected her to participate in their Future Trends Forum in Madrid in 2004, 2005, and 2007. Formerly in marketing at New England Telephone (now Verizon Communications) and Telecommunications Manager at Dennison Manufacturing Company (now Avery Dennison), Dodd was honored by the Massachusetts Network Communications Council as Professor of the Year. *The Essential Guide to Telecommunications* has been translated into nine languages since its first edition, which was published in 1997.

Part IV

The Internet and Cellular Networks

This page intentionally left blank

6 The Internet

In this chapter:

INTRODUCTION

The Internet is the single most important innovation of the 21st century. It's a ubiquitous network available in much of the world, and a disruptive technology that has displaced many traditional retail businesses and services. It has created the perception that the world is smaller and changed how we communicate, shop, and spend leisure time. It has upended numerous industries, shrunk distances, led to new industries, and enabled improved communications across countries, between countries, and between continents. According to an international university student from China:

> *I am my parent's only child, and the ability to make free video calls over the Internet to them weekly is the thing that most helps me stay in touch with them and share my experiences. Knowing that I will chat with them every week makes my parents and myself less lonely.*

Technologies used in the Internet are radically changing the ways consumers access and view movies and television shows and negatively affected movie theater attendance. People can now view high-definition movies and television on their widescreen TVs in the comfort of their living rooms. Many additionally have high-end audio systems to supplement their viewing experience. Increases in the number of people using streaming, the high video and audio quality, and improvements in actual content have all precipitated large decreases in the numbers of adults that go to movie theaters and lower profits for movie theaters. Attendance at movie theaters has dropped steadily since 2016 and is expected to continue dropping as more people adopt streaming.

The Internet has radically changed how companies conduct commerce. The Internet is the main vehicle by which businesses contact customers, handle customer service, and interact with internal staff. The Internet is particularly attractive to young people, many of whom grew up with the Internet as a part of their daily lives. Web sites that are well designed and make it easy for customers to find what they need and to check out, lessen customers' desire to actually speak with or e-mail a customer service rep. A well-designed, easy-to-use web site, an extranet, saves costs for businesses. Extranets are online e-commerce sites where consultants, partners, and customers access particular databases and services.

The Internet is not a single entity. It is made up of multiple large networks connected to each other by routers and switches and with growing amounts of capacity enabled by the following advancements: fiber-optic cabling, and more powerful servers and computer chips, all of which have resulted in higher-capacity broadband fiber-optic networks.

Streaming is a major disrupter of home entertainment and pay-TV. It has been enabled by both the Internet and home Wi-Fi. The number of people using streaming services has grown every year since Netflix first offered it in 2007 and many analysts expressed skepticism over its future. Streaming is widely available worldwide in

developed countries in Asia, Europe, the Americas, and some countries in Africa. The rise of streaming has caused the bankruptcy of Blockbuster and other DVD retailers, and decreased the number of people subscribing to cable TV packages. Importantly, it's changed the way people get their home entertainment.

Because of its acceptance, pay-TV providers now offer their own streaming services with content they create, own, or lease. For example, Verizon owns Yahoo!, and AOL, which they merged into their Oath unit, and AT&T, which owns DirecTV, purchased Time Warner, the owner of HBO. Furthermore, Comcast owns NBC and Universal, with its cache of movies and television shows. Thus, the three largest broadband providers own and create content through their subsidiaries. This results in competition between content providers Amazon, Netflix, and other streaming content companies including Facebook, and large telephone, cable TV, and satellite companies over which Amazon, Netflix, and others stream movies to homes and apartments. This often creates a situation where pay TV providers compete with the very organizations that stream movies and TV shows over their networks.

To prevent large telecoms from slowing down or blocking competitors' content, the Obama era FCC instituted *network neutrality*. Under network neutrality rules, owners of broadband (pay-TV providers) are not allowed to slow down or block competitors' content. Cable TV providers, however, lobbied for the elimination of network neutrality, stating that they should be compensated for carrying streaming traffic. The Federal Communications Commission eliminated network neutrality in 2017. However, their ruling is being adjudicated in courts and in legislatures in the United States.

Worldwide connectivity has led to the challenges of keeping networks secure and information private. Organizations, individual subscribers, and governments grapple with keeping information secure and employees' and customers' personal data private. Hackers know how internal networks are architected and where to look for vulnerabilities. Furthermore, malicious employees and staff errors add another layer of complexity in maintaining secure networks. Keeping enterprises 100 percent secure is almost impossible. Hacking is profitable and not often punished. Thus, hackers have a huge incentive to steal information they sell, or otherwise profit from illegal tampering with businesses' computer data and networks. It's an ongoing race between hackers finding new and novel ways to interrupt and steal information and to damage and hijack networks, vs. enterprises and governments keeping networks safe.

WHAT IS THE INTERNET?

The term Internet is derived from *inter* and *network*. It's a vast network of globally interconnected networks. If one part of the Internet is down, routers send traffic on alternate routes. It's a survivable, robust network with parts of it able to function during natural disasters and attacks. The United States Department of Defense funded the original Internet with the intention of having a robust network able to survive an attack

or national disaster. They awarded money to the University of California at Santa Barbara for the purpose of developing a resilient network. In addition, faculty in the IT department at the University of Michigan collaborated on new protocols to be used in the Internet.

At that time, 1969 until the mid-1990s, researchers at universities and government agencies were the main users of the Internet. They used it to collaborate on research. Additionally, staff at universities used the Internet to access early forms of electronic mail (e-mail) using arcane commands such as k to display the previous message and n to display the next message. Logging into the Internet and using e-mail acquired a user-friendly interface when Tim Burners Lee developed the Nexus *browser* in 1989. Examples of browsers include Chrome, Internet Explorer, and Safari. Mosaic and Netscape were early browsers. Easily accessible, user-friendly browsers are a large part of the reason that the Internet was widely adopted.

Features of the Internet

The following are some of the most prominent features of the Internet:

- It uses a common set of IP protocols
- It is a packet network
- Routers send packets on the least congested routes
- Routers send packets around disabled, broken links
- It has defined protocols, such as IPv4 and IPv6 for addressing
- It can grow to keep up with growing amounts of traffic
- The backbone is made up of fiber-optical cabling connected to electronics in which capacity can be increased, often using software at remote data centers
- The United States federal government does not regulate the Internet
- Because of the simplicity of its protocols, IP, TCP, and HTML markup language, the entire world can communicate over the Internet
- Voice, video, and data are transmitted on the Internet
- Carriers exchange traffic at peering points

Protocols Used on the Internet

The single most important factor in the worldwide spread of the Internet is the standard, easily implemented protocols used on the Internet. Worldwide, all countries use

the same IP protocols to transmit data across their sections of the Internet. This means that people access broadband in a uniform way regardless of their location. When the Internet was designed, simplicity was purposely kept in mind so that the networks could be uniformly and easily duplicated. The fact that these designs are accepted worldwide has been a critical factor in adoption.

The following are examples of the Internet protocols:

- **Internet Protocol:** IP is a "best effort" protocol. When a message is sent over the Internet, it is broken up into packets. Each packet is sent on a different route and reassembled at the receiving end in the correct order. If there is congestion the router drops packets. The dropped packets are not resent. This is why IP is known as a best effort transmission protocol.
- **HTTP:** HyperText Transport Protocol links are the standard way documents are moved around the Internet.
- **HTML:** HyperText Markup Language is used to compose web pages. It is not, strictly speaking, a protocol.
- **TCP:** Transmission Control Protocol provides error checking on messages sent over the Internet. It is a connection-oriented protocol. Messages are sent between sending and receiving computers on the Internet that communicate whether the message was received or whether errors occurred. If there are errors, bits are retransmitted.
- **IPv4** and **IPv6:** Internet Protocol v4 and v6 define the numeric structure of Internet addresses. The newer IPv6 was launched in 2012. It specifies longer addresses and is being implemented by Internet providers and telephone companies. It has capacity for more IP addresses than the shorter IPv4 structure.

The Impact of Capacity—The Availability of Broadband Networks

An important factor in the wide use of the Internet in everyday life and business is the availability of high-capacity broadband and cellular services. This availability exists in Western Europe, North America, much of Asia, parts of Africa, and in the Middle East. The capacity and availability of the networks that make up the Internet are enabled by technologies such as fiber-optic cabling and the supporting electronics connected to it: lower-cost, smaller graphical processor chips in wireless handsets and laptops; faster computers; and improved compression to support multimedia video streaming and high-capacity content downloads. These improvements, along with search engines, enhance the user experience for consumers and businesses alike, as do improvements in web site designs.

The Public Network Prior to the Internet

At the time the Internet was developed and through the 1990s, the public switched telephone network, which carried only voice, was made up of large central offices called *tandem offices*. Smaller central offices were connected in a hub-and-spoke design to each tandem office. If the tandem office crashed, all the local central offices were also out of service. The designers of the Internet wanted to avoid this centralized control where an outage at a central or tandem office disabled large swaths of the public telephone network.

The Internet—A Distributed Network with No Central Control

The Internet is a distributed network with no single ISP (Internet Service Provider) or other entity controlling it. It's a distributed network in which multiple carriers manage particular parts of the network. If a router crashes, other routers send traffic along alternate paths in the Internet's backbone. The backbone is the part of the Internet that carries traffic across the country between cities and states, and between countries.

Although the Internet was designed to function when any route crashes, if the central databases that hold IP addresses are disabled, the Internet won't function. See the section "The Criticality of Root Servers" below for information on root servers.

Largest Carriers Worldwide—Backbone Providers

The telephone companies with the largest Internet backbones in the United States are Sprint, Verizon, CenturyLink (through its purchase of Level3), and AT&T. There are a number of local carriers (ISPs) that connect users to the Internet because no single provider has service everywhere.

According to the May 24, 2017, article by Antoine Gara in the *Forbes* online article, "The World's Largest Telecom Companies: AT&T & Verizon Top China Telecom," the following are the largest telephone companies by total revenue worldwide. The list includes their headquarters locations. However, most of them have services in other countries as well:

- AT&T—U.S.
- Verizon—U.S.
- China Mobile—Hong Kong, China
- Nippon Telegraph & Telecom—Japan
- Softbank—Japan

- Deutshe Telekom—Germany
- Telefonica—Spain
- KDDI—Japan
- China Telecom—China

Using Search Engines to Unleash Vast Stores of Information

The introduction of sophisticated search engines by organizations such as Google, Microsoft, and Yahoo! (part of Verizon) made browsing the Internet convenient by organizing the enormous amounts of information available on the Internet. Search engines from Google and Baidu in China and others including DuckDuck Go Search, Bing (part of Microsoft), Dogpile Search, Yippy Search, and Webopedia Search earn revenue from advertising on their sites and from ranking companies that pay fees for higher placements (rankings) in search results.

Page ranking refers to the placement on a web page of search results. Ranking a product or service higher places it closer to the top of search results, with a higher likelihood of people clicking on the link. In addition to paying for higher ranks, ranking is done by analyzing the number of other sites that link to a particular site. For example, if someone searches for Greek restaurants in San Francisco, the Google engine looks at and ranks the restaurants partially on how many sites link to particular Greek restaurants in San Francisco and the type of sites linking to it.

Google not only earns the highest search-engine-based advertising revenue in the United States, but because of its many acquisitions, it has the potential to skew results of searches in favor of its own sites. When search results are returned, search engines such as Google can rank their own sites higher than those of competitors. Google's search engines are located in hundreds of countries worldwide in addition to its presence in the United States.

Over the years, Google's owner Alphabet acquired many software companies, including the following:

- Zagat (restaurant and hotel reviews)
- Android operating system software for smartphones
- Adsense (Google's network for advertising sales)
- DoubleClick (advertising network used to target ads to particular classes of people)
- Google Maps (GPS plus local guides and advertising)

- Keyhole Technologies, Zipdash Inc., and Where2 LL2 (software that forms the basis of Google Maps)
- ITA (airline flight aggregation information)
- Motorola Mobility (mobile devices; patents for mobile services)
- YouTube (online videos and streaming TV)
- Waze GPS (global positioning service)
- Zipdash (now part of Google's location services)

In addition to possibly skewing search results toward their own sites, search engines have implications for privacy. Marketers can determine the following based on terms people search on:

- Gender
- Income Range
- Health
- Type of computer (Mac or Microsoft Windows)
- Location

This information may be shared with advertisers who target ads at particular demographics based on search history. For example, they might show pop-up and sidebar ads on the Internet based on people's purchasing history. See the section "Privacy" below.

Search Engines—Mathematical Algorithms and Page Ranking

Google, a unit of Alphabet, attracts the most search engine traffic worldwide. Baidu in China is second and Microsoft's Bing and Verizon's Yahoo! are third and fourth respectively. Search software uses mathematical algorithms and page ranking to determine search results. Proprietary mathematical algorithms analyze keywords, titles, site structures, and descriptions to determine which sites fit the search terms specified by Internet users. They look at headlines, bolding, and the proximity of words to each other for relevance of textual data on the page.

Search engines have massive indexes (lists) in databases of past searches and URLs, or locations of web sites. They additionally have the ability to find and add new web sites and discover sites that are removed. This is done by *spiders*, software

that continuously and automatically crawl through the Internet looking for new and updated sites.

Search Revenue—Advertising, Page Ranking, and Software Licensing

Google has the largest revenue from search worldwide, primarily from advertising on its sites. As reported by its parent company, Alphabet, it had $26 billion in total sales for the quarter ending June 30, 2017. Of that total, $25.8 billion was from search: advertising, software licensing, and page ranking.

Search companies earn revenue by a combination of ads, favorable ranking of web sites in search results, and licensing software to other search companies and to enterprises. Large enterprises deploy the licensed search software to assist staff in finding information on health and retirement benefits, information about departments, and directories of employee addresses and telephone numbers.

Investigations into Google Search Practices

In June 2017, the European Union fined Google $5 billion for favoring its own companies in search results. The European Union judged that Google demoted rivals' links in favor of its own company's links and search results. This is important because the top 10 ranked search results receive about 90 percent of all clicks. The EU's investigation was prompted by complaints from EU companies, that search results were skewed in Google's favor and that EU companies' results were demoted to lower rankings on search result pages. For example, Google might rank its own flight information service higher than a competitive flight information service. The EU complaint stated in part that Google was using anti-competitive tactics to take advantage of its 90 percent market share in searches.

As a result of the EU fine and agreement, Google stated that it would let companies bid for the top placement in search, rather than ranking search results by links to products retailers who had paid Google to rank high in searches. Google further agreed to make some changes in its search shopping methodologies, and to stop promoting its own shopping services while demoting rivals' comparison sites.

The EU left it up to Google to create its own solutions to these issues. Per EU competition commissioner Margrethe Vestager, if the EU is not satisfied with Google's changes made within 90 days of the fine, the EU will fine Google up to 5 percent of its total global search revenue each day. The EU hired accounting firm KPMG and search engine optimization marketing company Mavens to monitor Google's search results for compliance with the EU agreement. Despite this agreement, Google has stated that it will continue to challenge the fine in the courts.

In addition to the EU's investigation into Google's search practices, in 2016 the EU filed anti-trust charges against Google over its dominant position in search on Android operating system mobile phones and tablet computers. The complaint alleged that Google is monopolistic in requiring that Android phone manufacturers pre-load the Google Chrome browser and Google Search on phones. The charges are further based on Google's practice of offering financial incentives to carriers and manufacturers to make Google's search services the only pre-loaded search on mobile phones. In 2016, Russia filed a similar anti-trust complaint against Google's policies on mobile phones and tablet computers. In 2017, Google and Russia reached a settlement where Google agreed to pay Russia $7.8 million to settle the claim.

Internet2—A Non-Commercial Outgrowth of the Internet

Internet2 is the predecessor of the Internet. In contrast to the public Internet, it is a non-profit private network. Internet2 was established as a way for university and research professionals to collaborate over a private connected network. Internet2 is the largest private network in the world. The scope of Internet2 has grown from university and research organizations to include corporations, and private and governmental national research entities in over 100 countries.

A core group of Internet2 technology staff maintain and upgrade the network to include high data rate services including SDN and Gigabit Ethernet. In addition to the local data centers at members' locations, Internet2 maintains a central data center at Indiana University. An important focus of operations at the data center is maintaining the security and privacy of information transmitted over Internet2 links.

In the United States, Internet2 drops are located in metropolitan areas on the east and west coasts, as well as throughout populated areas along the southern coast. There are fewer Internet2 locations in less densely populated cities in the midwest.

Collaboration and research data transmitted over Internet2 includes cooperation between branches of large universities. For example, many universities now have branches throughout urban and rural areas, as well as in distant cities of large countries. Internet2 also links university sites in distant continents. Scientists and researchers are able to partner with distant colleagues on designing new drugs and other innovative technologies using Internet2 links.

STREAMING—A DISRUPTIVE TECHNOLOGY

Streaming media, also called Over-the-Top (OTT), refers to television, movies, and music streamed directly to people's homes and apartments from the Internet. OTT streaming has had and is continuing to have a direct impact on decreased cable TV

and broadcast TV revenues and is a leading cause in the decline of movie theater attendance as more people abandon cable TV and move to Netflix, Amazon, and YouTube TV for movies and TV shows.

Growth in Streaming

Streaming entertainment from the Web to televisions is a key application that is growing year after year and causing losses for pay-TV (cable TV, telephone companies, and satellite TV) providers. However, not all subscribers that stream have "cut the cord" on all pay-TV. According to an October 27, 2017, article by Wayne Friedman in *TELEVISIONNewsDaily*, "53% of U.S broadband homes subscribe to pay TV as well as to OTT streaming." But streaming hours grew 100 percent from 2016 to 2017, according to the article, "Streaming Hours Up Over 100% in 2017, Study Says," by Alex Weprin. The article cited Conviva for the statistics and for the statement that live sports were an important driver of the increase.

However, in increasing numbers, subscribers are canceling their pay-TV service. According to a September 13, 2017, *Variety* article by Todd Spangler, "Cord-Cutting Explodes: 22 Million U.S. Adults Will Have Canceled Cable, Satellite TV by End of 2017," the 22 million people that have canceled their pay service is a cumulative total of subscribers that rely entirely on streaming options. These statistics were credited to eMarketer. Added to these losses is the fact that growing numbers of children and young adults are growing up assuming that they can access all their television shows and movies on their mobile devices and computers via streaming. To wit, a September 15, 2017, *USA Today* article cited statistics from Videology that 9 percent of Millennials plan to cancel their cable TV subscriptions in 2017. This does not include the young adults, college students, and children who already rely entirely on streaming.

Additional studies have tracked the rise of streaming and the decline in pay-TV usage:

- A 2017 survey conducted by Hub Entertainment Research found that 52 percent of respondents watched their favorite shows online rather than through their cable TV set-top box. This causes lower revenue for cable TV as subscribers sign up for lower cost, less inclusive pay-TV packages. This statistic was published in *DigitalNews* in an article published on November 9, 2017, by Alex Weprin, "Study OTT Overtakes Set-Top Box as Source for Favorite Shows."
- A survey done by Videology found that only one third of Millennial males intend to subscribe to pay-TV in 2017. Adam Levy cited these statistics in a September 15, 2017, article in *USA Today* titled, "Cost Is Not Why More Millennials Than Ever Are Cutting the Cord."

Easier Set-Up and Increased Internet Uptake

When over-the-top streaming was first available in 2007, accessing it from traditional televisions was complicated because at that time most televisions did not have the HDMI (High Definition Multimedia Interface) ports needed for set-top boxes such as Apple TVs and Roku. With the universal availability of HDMI ports on new televisions, this requirement is no longer a major impediment to the adoption of streaming. In addition, increased capacity in broadband networks and growth in broadband adoption are factors in the growth of streaming. According to Netflix, Inc. CFO David B. Wells on their October 16, 2017, third-quarter earnings call:

> *I think, in general, it is the continued adoption of Internet entertainment that is driving our growth.*

Accessing Streaming—Connected TVs, Game Consoles, and Mobile Devices

Subscribers access streaming media on mobile devices as well as on flat-panel televisions. Streaming movies and TV shows to tablet computers and smartphones is particularly useful when traveling. In addition, university students who may not have television in their dorms often stream to laptop computers, smartphones, and tablet computers. An additional option for connecting to streaming service is via game consoles connected to televisions. Subscribers to streaming can easily log into their streaming service from game consoles such as the Sony Wii and the PlayStation Vue. Two examples of services compatible with game consoles are Netflix and Hulu movies and TV shows, which have been made compatible with game consoles so that they can be streamed directly to them.

Another way streaming is becoming more widely available is via Internet-connected televisions, also referred to as smart TVs. Internet-connected televisions have menu-driven screens for surfing the Internet and selecting programming. New smart TVs also have Roku software integrated. This eliminates the requirement for an HDMI cable and a physical set-top box because Roku features are built into the TV. Consumers can use the televisions' remote controls to click on icons from sites such as Netflix, Amazon, and Hulu to stream movies and television shows to their TV. These televisions connect to the Internet via home wireless networks or by connecting Ethernet cabling to the Ethernet port on their television. The cable is then plugged into to their Wi-Fi router and their cable TV or broadband modem.

Set-Top Boxes for OTT Streams

Apple TV, Roku, Google Chrome, and Amazon Fire are examples of set-top boxes made expressly for over-the-top streaming. Each of these devices has software with options for accessing content from a specific list of providers. The set-top boxes plug into the HDMI (High Definition Multimedia Interface) port on flat screen televisions. Streaming content is sent to subscribers' set-top boxes via their Wi-Fi networks.

Roku's Business Model

Roku set-top boxes were first available in 2007 when Roku was a unit of Netflix. Netflix sold it in 2009 because they were concerned that owning a streaming device might put them in conflict with hardware providers such as Apple. Netflix traffic accounts for a third of content streamed over Roku set-top boxes. And Roku leases space in Netflix's headquarters location in Los Gatos California.

While Roku sells the most streaming devices in the United States, ahead of Amazon, Google, and Apple, the majority of its annual revenue is not from hardware sales. Rather, Roku makes the bulk of its revenue from platform sales. Platform sales consist of advertising, sales of its partners' content sold through Roku's software, and subscriptions on its hardware. It additionally has its own streaming service from which customers can stream movies and TV shows.

In addition to streaming on connected TVs and its set-top boxes, Roku has put its name on co-branded televisions manufactured by Insignia, Sharp, TCL, and others. These televisions have Roku software pre-installed, which enables consumers to use Roku without adding an external set-top box. Televisions with embedded Roku software display the Roku menu at start-up. Embedding software in televisions is a way to keep customers tied to Roku.

Another way that Roku makes content available is by formatting a selection of movies and TV for mobile operating systems. Customers that stream to mobile smartphone and tablet computers download a Roku app (a small application) to their mobile device. Movies and TV shows streamed to smartphones and tablets are formatted to appear on the particular device and operating system used on the device to which the movie, TV shows or music are streamed.

In addition to the United States, Roku streaming players and software are sold under the Roku brand in Canada, Mexico, the United Kingdom, France, and the Republic of Ireland.

Keeping and Attracting Subscribers—The Criticality of Content

Quality content that appeals to a wide range of people is an important strategy in attracting and keeping subscribers. The number of over-the-top providers in the United States competing for subscribers is on the rise. Whereas in the early days of streaming, Netflix was able to license content from studios including Disney and Universal, as these contracts expired, many studios stopped licensing content to Netflix and others in favor of streaming their own offerings.

Both Amazon and Netflix are building up their collections of original content as well as attempting to license rights to content from other studios. Netflix announced plans at their October 2017 third quarter investor conference to spend up to $8 billion in 2017 for original content. This is riskier than purchasing existing known hits, but with less licensed content available, it is a necessary strategy.

Disney, with whom Netflix previously had a contract, opted to not renew its licensing agreement with Netflix in 2017. Disney has instead started its own streaming service with content from its movies, TV shows, and its ESPN sports division. In 2017, Disney purchased the studio library of 21st Century Fox. The content that Disney gained includes Fox's movies (*Star Wars*, *Avatar*, and *X-Men*), television (*The Simpsons*, *This is Us* and *Modern Family*). Importantly, the Fox acquisition strengthens Disney's international presence in India and other non-European countries. In a similar strategy, Comcast purchased Universal Studios in 2011 for their NBC television and Universal Studios' libraries of movies. They recognized the importance of content to round out their offerings of cable TV service.

The issue of content is also complicated by the fact that some cable TV providers also own rights to movies and TV series and/or national broadcasters. In January 2011, Comcast received approval from United States regulators to purchase a controlling stake (51 percent) in NBC Universal, which owns Universal Media Studios and Universal Pictures' Focus Features; the NBC broadcast network; and cable networks USA, Bravo, and CNBC. It is part owner of the Weather Channel and majority owner of MSNBC.

Major content providers and a partial list of what they own include the following.

- Time Warner owned the most content in the United States and Canada. Some of its properties were HBO Films, CNN, New Line Cinema, 10 percent of Hulu, TBS, Turner Entertainment, and Warner Bros. Animation. It owns CW Television Network jointly with CBS Corporation. AT&T purchased Time Warner in 2018.
- Comcast with its NBCUniversal division owns NBC, MSNBC, NBCSN, E! CNBC, Telemundo, Bravo, USA Network, DreamWorks Animation, The Weather Channel, 30 percent of Hulu, and Universal Studios along with their parks and resorts. It is the largest broadcasting and cable television

conglomerate by revenue in the world. In 2018 it purchased Sky, a pay-TV service available throughout Europe.

- See below for Walt Disney Company's purchase of 21st Century Fox's library of films and television content.
- Viacom is an international cable TV and content company. It owns Comedy Central, MTV, Spike, Nickelodeon, VIVA, Paramount Pictures, BET, and VH1, as well as others. Privately owned National Amusements, Inc. owns a majority of Class A common stock in Viacom. National Amusements is controlled by the Sumner Redstone family, which also owns movie theater companies.
- CBS mainly produces commercial television and radio shows. It owns CW Television Network jointly with Warner Brothers, CBS films, Smithsonian Network, UPN, Infinity Broadcasting, Viacom Outdoor, Showtime Networks, Simon and Schuster Publishing, and Paramount's television studio. National Amusements is a parent company of CBS as well as Viacom.
- Sony Pictures Entertainment is a wholly owned subsidiary of Tokyo based Sony Corporation through its Sony Pictures Entertainment Division. It owns Columbia Pictures, TriStar Pictures, Sony Classic Pictures, Dutch production company 2waytraffic N.V., and Sony Pictures Animation. Sony also manufactures Bravia TVs, Blu-ray players, and the PlayStation game console. It is offers its content through its Internet-connected televisions, Blu-ray players, and home entertainment systems.
- The Walt Disney Company owns the ABC broadcast network, ESPN, The Disney Channel, A&E Network, Touchstone Pictures, Lucasfilm, Maker Studios, Marvel Entertainment, and Pixar. It is part owner of Lifetime Entertainment, the History Channel, A&E Networks, and Freeform, 60 percent of Hulu, and 14 theme parks worldwide. In 2018 Disney purchased 21st Century Fox which included part ownership of National Geographic Partners. Blue Sky which produces and distributes motion pictures worldwide, its film libraries, and Fox Home Entertainment. The purchase did not include Fox's TV or sports stations. The Walt Disney Company is the second biggest conglomerate by revenue in the world.

A large part of the reason subscribers enjoy streaming is the absence of commercials in most offerings. Traditional network, cable TV, and satellite TV programs have 20 minutes of commercials in every hour of non-premium programs. The exceptions are pay-TV premium channels such as HBO and Starz for which subscribers pay extra fees.

A Snapshot of Companies that Offer Streaming

Although, it has the largest customer base of streaming customers worldwide, Netflix does have competition. According to market research group Parks Associates, there are over 200 streaming services in the United States alone. This statistic was published in the December 19, 2017, *Wall Street Journal* article by Sarah Rabil, "Streaming's Goldrush Upends TV." According to audience measurement firm CommScore as published in the April 10, 2017, TechCrunch.com article by Sarah Perez, "Netflix Reaches 75% of Streaming Users, but YouTube is Catching Up," Netflix currently has 75 percent of customers that stream in the United States. The article further stated that of the Wi-Fi–equipped homes in the United States, 53 percent of them use streaming services. As more homes are equipped with Wi-Fi, the number of people streaming content will continue to grow.

And competitive streaming providers are gaining market share:

- Amazon offers free streaming for its Prime customers. Prime customers pay $100 annually for no-fee fast deliveries, plus other privileges including free downloads to Amazon's Kindle e-reader.
- Facebook Watch offers sports videos, short form videos of 5 to 10 minutes in length, and its own original content of 20- to 30-minute videos.
- Hulu offerings include content from broadcasters and access to live sporting and other events.
- HBO Now is free to people that subscribe to their pay HBO pay-TV offerings.
- Sling TV includes content from live broadcasts plus many pay-TV channels, and streaming sporting events.
- The Walt Disney Company has announced its intent to offer streaming channels with its own content including ESPN and 20th Century Fox's original content, which it is purchasing from 21st Century Fox.
- Google's YouTube TV includes broadcast stations and pay-TV channels such as ESPN and the Disney Channel.

Ad Revenue on Streaming Services

OTT streaming is available with subscription fees without commercials, or free but with commercials. Social network giant Facebook has announced its intention to offer longer form streaming video supported by advertising. Hulu, majority-owned by the Walt Disney Company and Comcast with minority ownership by AT&T, offers options for low-cost subscriptions that include ads or higher-cost subscriptions with limited, brief ads. Hulu has access to premium and broadcast TV content through its broadcast and studio owners' libraries of content.

Streaming Worldwide

Streaming services are available in most regions worldwide, including Europe, India, China, North and South America, and parts of Africa. Netflix alone offers service in 190 countries worldwide. In developing countries such as India and where its available in Africa, coding techniques used in streaming media enable users with slow-speed mobile and wired broadband connections to receive television shows and movies of adequate resolution. Coding techniques that use compression to shrink the number of bits enable many subscribers that would otherwise not have access to receive an acceptable quality of streaming. According to Netflix Chief Product Officer, Gregory K. Peters:

> *Encodes we're using are super-efficient so that we can provide a really, really, high-quality video experience, and with lesser and less bits.*

Netflix is a global entity with over-the-top streaming available worldwide. Its online streaming service is compatible with more than 100 formats on devices such as the Apple iPad and iPod, mobile handheld devices, Roku devices, and game consoles such as the Microsoft Xbox, Nintendo Wii, and Sony PlayStation.

Ease of Use and Technological Enablers

It is no longer necessary to connect laptops to high-definition televisions to stream movies from the Internet to the TV. Dedicated set-top devices such as the Roku and Apple TV are easily linked to flat-panel televisions via the High-Definition Multimedia Interface (HDMI) video interface and audio cable.

Significant technological improvements have occurred that enable multimedia streaming on the Internet in homes and consumer equipment that simplifies streaming to mobile devices and TVs. These innovations include the following:

- Dedicated electronic devices, such as set-top boxes from Apple TV and Roku that connect directly to televisions for streaming TV shows and movies from the Internet.
- Adaptive bit rate streaming software on content providers' and cloud servers that dynamically alter the speed of video streams to match consumer devices and bandwidth. This provides a more consistent video stream with fewer disruptions.
- Improvements with respect to in-home wireless Wi-Fi networks.
- The availability of Internet-connected televisions with icons on the start-up screen for Netflix, YouTube, Hulu, Amazon, Roku, and others that negate the requirement for a set-top box dedicated to streaming.

- The attractiveness, sound quality, and lower prices in home entertainment sound systems with the capability for high-definition images on large flat-screen televisions that make home viewing attractive.
- Over-the-top streaming directly to portable, wireless devices including tablet computers and smartphones with enhanced resolution.

Cable providers and telephone companies that own local broadband facilities now compete with companies such as Netflix with its 100 million subscribers worldwide and Amazon Prime. Netflix and its competitors have an advantage in not needing to build broadband infrastructure to support their services. This eliminates the significant capital investment required to build a network, and lowers the barriers to entry into the market. Competitors such as these are referred to as *over-the-top* (OTT) providers. See Figure 6-1 for a diagram of OTT streaming. It is one impetus for people to opt for high-speed Internet access. In a quote from Netflix CFO David B. Wells at the Netflix 2017 third-quarter investor's conference, he says:

> *When we try to explain the quarter-to-quarter perturbations or some of the lumpiness in our net additions, we tend to use explanations that sort of focus on the incremental, which could be content slate or a particular title that had some notable strength. But I think, in general, it is the continued adoption of Internet entertainment that is driving our growth,*

Time Warner's HBO GO.com division makes no-fee HBO content available online to cable TV subscribers of HBO. Subscribers that pay for HBO can watch any HBO Go content streamed on the Internet. Comcast and other cable companies now embrace TV over the Internet as a strategy to retain profits and subscribers for their pay-TV services in the face of competition from OTT providers.

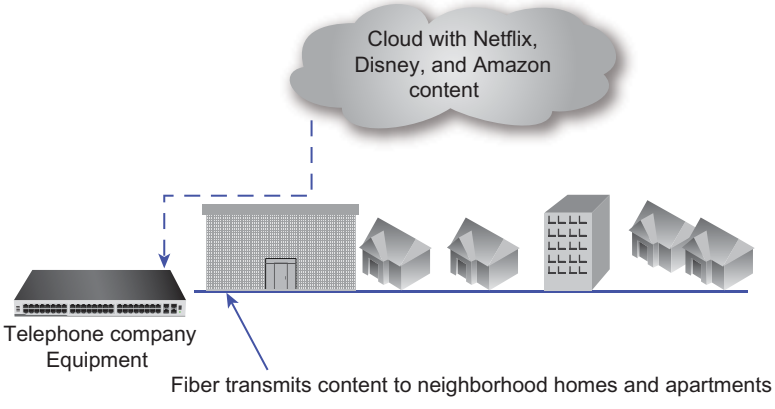


Figure 6-1 Over-the-top streaming between the content provider and residential locations.

Specialized set-top boxes for streaming make it convenient for customers to receive streamed video from the Internet. Set-top devices have interfaces that enable communications between homes' Wi-Fi networks and televisions. The set-top boxes interface wirelessly to home Wi-Fi networks as well televisions. The set-top box connects to the television's HDMI port. These set-top boxes commonly also have an Ethernet interface to connect the TV to a residential network's Ethernet cabling if it's available. Blu-ray players with Wi-Fi and Ethernet interfaces can also be used to stream content from the Internet, as can Internet-connected TVs.

Pay-TV—Skinny Bundles Plus Streaming on Set-Top Boxes

Pay-TV providers (cable and satellite TV) companies have a two-pronged strategy to retain customers that are increasingly moving to OTT streaming to save money on high pay-TV prices and to watch the appealing and more flexible viewing options available by streaming. Pay-TV companies now offer options for lower-cost, pared-down bundles plus streaming services such as Netflix included on their set-top boxes.

To lower prices, and retain customers, they are offering subscribers "skinny" packages that include just the broadcast stations; ABC, NBC, CBS, Fox, The CW, Telemundo, Univision, and the non-commercial PBS, plus HBO or another premium station. Previously, subscribers had to pay for an entire tier of cable channels in order to have the option to subscribe to commercial-free premium stations HBO or Starz.

Technical Challenges

Chris O'Brien, founder of Motionbox (now part of Snapfish, a Hewlett-Packard company) and SoftCom (now part of Interactive Video Technologies), stated in a telephone interview that

> *the challenge today is keeping up with the incredible diversity of tablets, mobile phones, and other devices. All of these different devices are creating an enormous challenge for video publishers, which convert the video into formats compatible with all the different screens and display capabilities.*

This is complicated by the fact that there is no single format that can be displayed on devices from different manufacturers. Tablets from companies such as Apple, Samsung, and Dell all use a different format, as do mobile devices that use different operating systems and are connected to mobile networks based on differing protocols.

Even using the same type of compression is no guarantee of compatibility. If otherwise compatible audio and video codecs are stored in a different container (file) format, the video cannot be played. A container is a server with multiple small programs

that share an operating system. See the section "Containers: A Newer Form of Server Virtualization" in Chapter 1, "Computing and Enabling Technologies," for a description of containers. Desktop computers with the same type of audio and video compression as iPods won't be able to play the same video if the container format in which the compression is stored is different.

There are a number of audio/video container formats (QuickTime, Windows Media Video [WMV], ASF, AVI, and more), and each of these can contain a variety of different audio and video codecs. So, for example, H.264 video with AAC audio in an MPEG4 container might play on your desktop player but not on your iPod, even though they both support H.264 video with AAC audio. Again, this is because they are stored in different containers.

Conversion and Distribution Engines to Process Video

Because of challenges in distributing video content to match the many formats used worldwide, specialized companies such as Brightcove and Ooyala manage the conversion and distribution of video for many online video distributors, including cable TV operators. Other examples are media companies such as online newspapers and magazines, pay-TV operators, and broadcasters.

Authentication and Reporting

Video processing engines perform other tasks associated with distributing video. When cable subscribers watch programs from televisions connected to broadband, the authentication software built into a set-top box automatically sends messages to the cable provider's networks verifying that this is a legitimate customer with a subscription for particular services such as video-on-demand (VOD).

Authentication is more complex when subscribers attempt to view content from other devices such as a tablet computer. The authentication software needs to determine if this device belongs to a legitimate subscriber. Authenticating a set-top box associated with a particular subscriber is simpler because it involves only a single set-top box, at a fixed location.

THE STRUCTURE OF THE INTERNET

The Internet is made up of edge and backbone routers that direct traffic based on addresses contained within the headers of data packets. In an effort to reduce delays, Content Delivery Networks (CDNs) install servers at their own locations and that of the carrier's site at the Internet's edges, thus placing content closer to the end users that request it.

Edge Routers

Edge routers are located at the edge of a carrier's network where they connect to customers and to other routers. They are often located at Points of Presence (POPs) where multiple providers connect to the Internet.

The edge of a network needs to support complex applications, protocols, and video. Edge routers must support multiple protocols, including Internet Protocol version 6 and version 4 (IPv6 and IPv4), Multi-Protocol Label Switching (MPLS), Wide Area Software Defined Networking (WA SDNs), and complex accounting software to track packet usage per customer. On MPLS networks, edge routers attach labels as described in Chapter 5, "Broadband Network Services," that include information regarding addresses, protocol, and Quality of Service (QoS). For more information about IPv4 and IPv6 addressing protocols, see the section "Address Structures" later in this chapter.

In addition, edge routers commonly handle aggregated Digital Subscriber Line Access Multiplexer (DSLAM) traffic in various formats; therefore, routers need to support both newer and older variations of IP and Wide Area Software Defined Networking (WA SDN). See Chapter 5 for a discussion of WA SDN.

Edge routers also use addressing information to determine how to handle the data. See Figure 6-2 for an example of a router.

Figure 6-2 *An edge router programmed with the features listed above. These features are not present in backbone routers. (Courtesy of Cisco Systems, Inc. Unauthorized use not permitted.)*

Services on edge routers include the following (if a router is used in the core, it does not require the extensive services listed here):

- Authentication that verifies the sender is indeed who he identifies himself to be when he logs on to networks.
- Protected session setup that confirms that each multimedia session conforms to the features and QoS allowed to the computer making the request. This protects against fraud and ensures accurate billing.

- Network Address Translation (NAT) addressing that translates external IP addresses to internal IP addresses, and vice versa.
- Support for IPv4 and IPv6 addressing. IPv6 is designed to replace IPv4; it supports many more IP addresses than IPv4's 4.3 billion addresses.
- Layer 2 switching for creating Virtual Private Networks (VPNs) to communicate directly with databases and applications in data centers. (See Chapter 5 for a description of VPNs.)
- Firewall software that protects networks from hackers.
- Accounting to track subscriber packet usage in the event that carriers charge for usage.
- QoS per application and per user for VoIP and video.

In addition to more intelligence, there are requirements for greater capacity in routers. This is caused by increasing use of video conferencing, greater demand for video streaming by residential customers, access to cloud-based services, and growth in mobile smartphone Internet browsing. Router ports now commonly support multiple 10Gbps as well as 100Gbps services. Total capacity of edge routers ranges from 1 to 3 terabits per second (Tbps). A terabit is the equivalent of 1,000 gigabits.

Aggregation Routers in Core Networks

Core routers carry the highest concentration of traffic. A single core router connects to multiple edge routers, aggregates traffic from these edge routers, and then sends it to distant cities and countries. If a single router doesn't have the capacity to handle this aggregated traffic, multiple routers can be networked together. When this is done, the networked routers function as a single entity with a single management interface. This simplifies the carrier's operations, upgrades, and remote diagnostics.

Networking routers together is commonly done through virtualization. (See the section "Virtual Network Function [VNF]—Transforming Hardware Nodes into Software Functions" in Chapter 4, "Managing Broadband Networks" for information on virtualization.) Virtualization enables multiple functions including routers to appear as individual pieces of hardware on servers that can be networked together. In addition, traffic is balanced among all the networked routers. If one router fails, the others absorb its traffic.

Ensuring Reliability in the Core and Edge

Routers sold to carriers and to large web sites such as Google and Amazon are designed for "*five 9s*" of reliability. This means that they offer 99.999 percent uptime. They are sold with *hot-swappable cards* that connect to other services and networks. If a card

fails, it can be replaced without taking the router out of service. They are also offered with options for duplicate processor cards and often come standard with dual power supplies. Power supplies connect to sources of electricity. It's also common for carriers to install duplicate routers that can be seamlessly brought online in the event of a failure. Duplicate routers are crucial at the edge, where if the router fails, all other networks and customers connected to it lose service.

Enhancing Internet Performance by Using Content Delivery Networks

Content Delivery Networks (CDNs) provide a number of services at the edge of the Internet that alleviate congestion on the Internet's backbone. In its simplest form, a CDN reduces congestion by decreasing the distance that the traffic must travel. One way they accomplish this is by storing frequently requested web pages at their servers, nearer to the end users, often in a service provider's location. This is referred to as *caching*. Many enterprises with large web sites use CDNs to replicate their web content at many edge locations to prevent delays at their web or e-commerce sites. For traffic that traverses the Internet backbone, CDNs use mathematical algorithms to map out the best paths for traffic to take.

Exchanging Data at Peering Points

Large multinational carriers are referred to as Tier 1 carriers. Tier 1 carriers own the majority of the high-speed lines that make up the Internet backbone. These carriers, all of whose networks are international, include Nippon Telegraph and Telephone Corporation (NTT) in Japan; Telefónica in Spain and Latin America; Deutsche Telekom in Germany; France Telecom in France; and AT&T, Sprint, and Verizon in the United States.

Regional carriers—which are referred to as Tier 2 carriers—also own core, backbone facilities. Comcast and Charter are considered Tier 2 carriers because their networks do not cover the entire country and they purchase backbone capacity from Tier 1 carriers. These Tier 1 and Tier 2 carriers interconnect with other carriers in places where they do not have coverage. These interconnections are referred to as peering points.

Network service providers transfer Internet Protocol (IP) traffic among one another at peering sites. Peering sites are also referred to as Internet exchanges and Network Access Points (NAPs). ISPs lease ports on the routers of other providers as a means of transferring IP traffic between networks. This enables carriers to send traffic that originated from their own customers to areas where they do not have network facilities, as demonstrated in Figure 6-3.

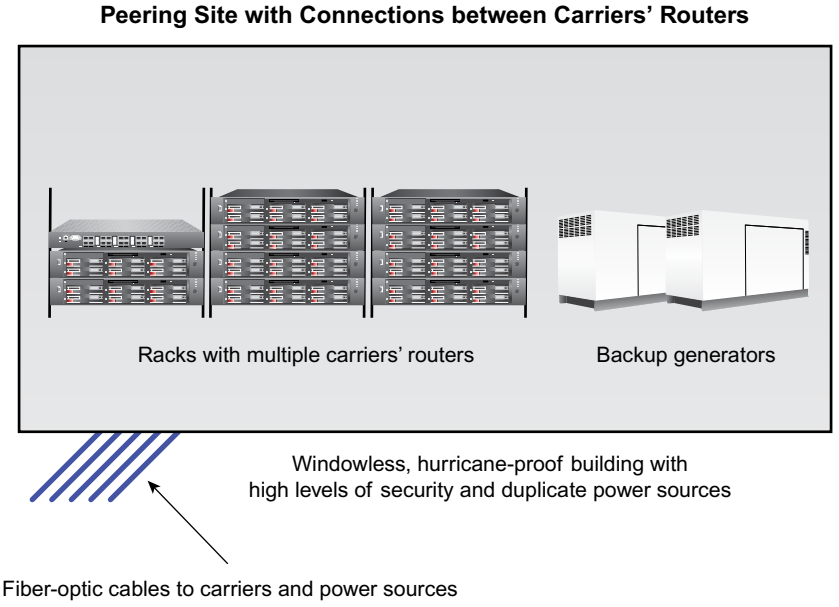
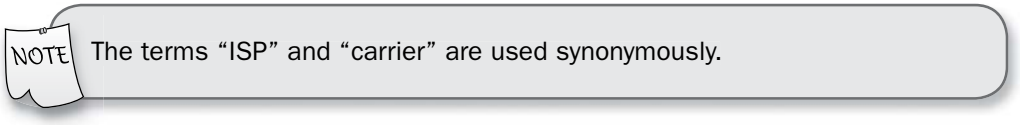


Figure 6-3 *Traffic at peering points is routed between the facilities of multiple network operators.*



Carriers that own peering points charge other carriers for connections to ports on their routers. However, traffic at these peering centers has the potential to create delays in the Internet if carriers lease too few ports from one another in an attempt to save money. If carriers exchange about the same amount of traffic, they often don't charge one another under this arrangement. Security, routing, traffic policing, and Network Address Translation (NAT) take place at peering points.

Address Structures

Two universal addressing schemes, IPv4 and IPv6, are used to transmit messages from computers, smartphones, and tablet computers worldwide. The system of routing messages based on IP addresses is managed by 12 organizations that administer 13 clusters of servers, called *root servers*.

The Criticality of Root Servers

The root name server system was implemented in the 1990s. The Internet cannot function without root servers, which route messages to the correct organization. Root servers are critical for the sustainability, capacity, and survivability of the Internet. To lessen the system's vulnerability to malicious actions such as Denial-of-Service (DoS) attacks, wherein millions of fake messages bombard a site, root servers balance incoming messages among multiple servers within each root. If one server within the root is brought down, other servers within the root handle the traffic. Ensuring protection against hackers is an ongoing endeavor.

The 13 Root Servers Worldwide

The *Domain Name System* (DNS) is the umbrella name of the Internet's capability to translate alpha characters to numeric IP addresses within root servers. Carriers and organizations send traffic addressed to locations outside their networks to one of the 13 sets of root servers, usually the one nearest to them, to determine where to route these messages. The root servers, which are massive databases, translate alphabetic hostnames (gmail.com) into numeric IP addresses (193.22.1.126), and vice versa. Root servers are connected to peering exchanges where large carriers exchange traffic with each other. Each of the 12 organizations that operate the root servers has root servers located in multiple cities or countries. They each operate between 2 and 196 locations.

Examples of organizations that operate the 13 root servers are:

- Each of the following organizations operates two sets of root servers:
  - Information Sciences Institute manages root servers U.S. Army Research Lab, which operates root servers in Los Angeles U.S.A. and in Miami U.S.A.
  - U.S. Army Research Lab manages root servers in Aberdeen Proving Ground, U.S. and San Diego, U.S.
- WIDE operates 196 root servers, the most of any operator

Tracking and Managing Top-Level Domains

The Internet Corporation for Assigned Names and Numbers (ICANN) is the organization responsible for managing the technical aspects of the databases of domain names in root servers. It in effect manages the Internet's address book. In a web or

e-mail address such as name@companyname.com, the .com portion is the *top-level domain name*, and *companyname* is the domain name, which is also referred to as the *secondary-level domain name*. Every country has a top-level domain name. For example, for China, it's .cn; for Russia, it's .ru. In the United States, some top-level domain names include .edu and .mil for educational and military institutions, and.gov for the government.

Voting ICANN board members were appointed by the United States Department of Commerce until 2009 when the Department of Commerce had sole responsibility for these policies. However, increasing criticism by other countries regarding what they felt to be too much control by the United States of major aspects of the Internet has led to the establishment of international review and policy determination.

Two years after 2013 when Edward Snowden revealed multiple instances of United States government surveillance of other countries and their leaders, the international community began organizing increased efforts for representatives from additional countries to manage ICANN. After years of negotiations, technical leaders from multiple countries agreed on a framework where control of top level domains would be managed by an international group of technical people, governments, and representatives from private companies. A group made up of these representatives now controls ICANN.

The Inclusion of Non-Western Domain Names

Initially, addressing systems used only the Roman alphabet character set (A–Z, a–z, the digits 0–9, and the hyphen). However, pressure from countries that use other character systems eventually led to the inclusion of other alphabets for addresses. These non-Roman alphabets include Arabic, Persian, Chinese, Russian, Japanese, and Korean. China, South Korea, and Arabic-speaking nations had already started assigning non-Roman domain names. These addresses introduced the possibility of duplicate domain names because they were outside of the root system. This created pressure for ICANN to alter their addressing requirements and make the technical changes in the root system that translations from other alphabets require.

Transitioning to IPv6

The main addressing scheme used on the Internet was initially IPv4. IPv4 was developed in the 1970s and addresses are only 32 bits long. On January 31, 2011, the Internet Assigned Numbers Authority (IANA), which managed the central supply of Internet addresses at that time, gave out the last of their IPv4 addresses to each of the five regional Internet registries. By April 2011, the Asia Pacific region had given out

all of their addresses, and the remaining four registries distributed all of their addresses within the next few years, Capacity is being depleted by the addition of new Internet-enabled wireless devices and the growing number of Internet users, particularly in Asia.

To ensure that they will be able to get new IP addresses, most organizations are now transitioning to the newer 128-bit IPv6 protocol, which is capable of accommodating billions of additional addresses. Most carriers have transitioned to IPv6. The IPv6 IEEE standard was published in 1998.

Most new routers, web browsers, and computers are compatible with both IPv4 and IPv6. The transition to IPv6 can be complex because it means assigning new addresses to every device with an IP address, including routers, firewalls, network management software, and all servers, including e-mail servers. In addition, it's not a simple matter to determine which applications and devices are compatible with IPv6. Enterprises that transition to IPv6 often need to be able to handle messages that are still in the older IPv4 scheme. Encapsulating IPv6 addresses within IPv4 can address this problem. There are also software packages that support both protocols.

SECURITY: CONNECTED, UBIQUITOUS NETWORKS—VULNERABLE TO MALICIOUS HACKERS

Hackers exploit the inherent openness of the Internet and common protocols to steal personal and corporate information, earning billions of dollars from selling information they steal. Hacking into networks and selling information is not only lucrative, it's comparatively punishment free. Hackers are rarely caught and jailed for stealing personally identifiable information such as Social Security numbers, birthdays, and intellectual property from businesses. For one thing, it's not always easy to trace IP addresses back to their origin; secondly, many countries from which hackers launch attacks don't have extradition treaties with Europe and the United States. Without a treaty, attacked countries are not able to extradite hackers and bring them to trial. This prevents hackers from countries such as Russia, China, and Iran from being brought to trial in countries such as the United States and many in Europe in which hacking attacks occurred.

Extradition treaties are agreements between countries whereby a country in which a crime took place can receive permission to bring criminals back to trial in the country of their suspected crime.

Methods Hackers Use to Attack and Infiltrate Networks

The following are the most common ways that hackers attack networks:

- Phishing emails
- Stolen passwords
- Weak Wi-Fi security
- Incorrectly configured software
- Unpatched software applications with known vulnerabilities
- Ransomware that encrypts organizations' computer files, making these files unreadable
- Distributed Denial of Service where massive amounts of hacker traffic block legitimate users' access

The Five Rs of Information Security

Managing security in government agencies, enterprises and commercial organizations requires 24-hour-a-day scrutiny. Organizations must put in place the tools to *resist* multiple types of attacks. They need the capability to *recognize* when they've been attacked. Viruses have been known to hide in corporate software undetected for months and even years. Additionally, companies need to *respond* to, and *recover* from attacks. Many also seek legal *redress* by attempting to identify attack perpetrators and initiate legal proceedings against them.

Resistance to Hacking

Resistance to hacking is an important way to safeguard private information about personnel, customers, and intellectual property containing product and software designs crucial to organizations' business success. Firewalls are one way organizations screen incoming traffic for known viruses. Firewalls are software- or hardware-programmed to block incoming known viruses and malware. In addition to firewalls, organizations typically have specialized appliances with security software that identifies and blocks malware.

Because of the criticality of security, large and medium-sized organizations hire Chief Security Officers and specialized security staff that monitor incoming and outgoing traffic to keep information secure. The jobs of Chief Security Officers and their staff are increasingly complex due to the fact that employees now access organizations' data stored on the cloud, at hosting centers, and branch offices, as well as at company servers and computers. Staff access this data from mobile as well as

landline devices and from remote locations as well as from headquarters. There are multiple places where viruses can infect internal networks. To protect data stored in the cloud, organizations use a combination of, for example, Amazon cloud security software and/or security software designed to operate in the cloud. Security software can additionally be located on servers to protect particular applications and at remote branch offices.

Specialized Security Software

Specialty security software is also available for e-mail and other applications. In addition to security software, firms hire outside organizations to conduct security audits to identify weaknesses that leave the organization vulnerable to attacks. Auditors might identify out-of-date software that needs to be patched, or they might find unauthorized wireless devices without the requisite security software.

As security programs become more sophisticated, hackers find new ways to get around them by creating increasingly sophisticated malware. It is an ongoing challenge to respond to every new type of security breach with improved defenses. This is a particularly difficult challenge because there is generally a lag between when a new software bug or worm is discovered and a software patch is created to guard against it. It's also time-consuming to add patches to not only software security but also application programs such as browsers that might introduce security vulnerabilities. One advantage of Software as a Service (applications in the cloud) is that the cloud provider adds patches to these applications, thus eliminating breaches caused by software with known vulnerabilities.

Intentional and Inadvertent Security Breaches by Insiders

Employees who have been fired or those who feel entitled to access information are frequent causes of these incidents. An employee with high-level authorization to sensitive data can copy it or corrupt it in some way. The employee might then provide the sensitive data to competitors or cyber criminals.

Employees who change jobs are often in the position to copy entire files and use them in their new positions. They might use information such as lists of customers to help them succeed in their new job. They additionally may sell inside information or use it to start a competing company.

In other instances, employees inadvertently open infected e-mail attachments. They might unknowingly insert infected portable storage devices such as USB flash drives into network-connected computers. These viruses can then spread through a corporate network. To prevent this from happening, organizations often purchase security software that automatically screens e-mail attachments, laptops, and external devices for known malware. They can also install software that prevents USB devices from being inserted into LAN-connected computers.

Other inadvertent security lapses caused by insiders include lost laptops, smartphones, tablet computers, backup disks, or flash drives containing files with medical and demographic patient data or other private or strategic information.

User training is an important strategy toward preventing inadvertent security breaches and in gaining the cooperation of employees in adhering to corporate practices. If employees understand the crucial nature of lost data, they might take extra precautions to protect it. This can include measures as simple as not taking strategic information out of the organization, reporting losses immediately, and not leaving passwords on sticky notes under keyboards. They will also be more careful in not allowing unauthorized outsiders entry into the organization. This can be something as fundamental as not allowing people without badges to walk into secure areas behind them. Another point that should be stressed is not leaving unattended computers active so that other users have access to strategic information and e-mail messages. To prevent this, some organizations configure their computers to time out and enter a password-protected standby mode if they are inactive for a specified amount of time, or they institute rules that all employees must shut down their computers at night.

Training Employees on Security Best Practices

Because employee actions can seriously impair security, training all personnel on the importance of security including strong passwords, ways to recognize to phishing, safeguarding passwords, and the importance of using encryption on company data stored on smartphones or tablets. Depending on the industry, there may be legal requirements on managing personal employee and customer information. For example, certain industries such as the medical and financial fields are required to keep client data stored on their computers private. Training on steps to protect this data is critical. According to a Chief Security Officer at a large credit union:

> *User education is required by financial service regulations and is most effective. Training is the single most important way to prevent phishing attacks. We conduct security training every single month—with a new module monthly on some aspect of security. It's cloud-based education software that takes 5 to 10 minutes to complete. It has a small quiz 2 weeks after the security module has been made available. Staff with a perfect score on the quiz have an opportunity to be in a pool for a gift card drawing. People really like it and it keeps security fresh in their head. New employees are required to attend a classroom when they start at the company. We try to keep them engaged so they retain the security information. The quizzes and prizes keep staff engaged so they retain the information.*

Recognition of a Hacking Attack—Tactics for New Types of Viruses

Just knowing when an organization has been infected with rogue, malignant data is one of the most difficult aspects of security management. Malware can lurk in company networks undetected for years. This occurred in the 2017 Equifax and the 2016 Yahoo! attacks. Publicity about customers whose private information has been compromised can cost companies millions of dollars in damages and legal fees responding to lawsuits, and from harm to a company's reputation.

In past years, organizations have screened traffic for known viruses. This is no longer as effective as other strategies because of the tens of thousands of known viruses. Newer security software is able to differentiate a list of applications and bitstreams from new, unrecognized data streams. The security software quarantines unrecognized traffic until security staff determines whether the streams contain viruses or are permitted traffic. Never-before-seen attacks are known as *zero day attacks.* As extra protection, large organizations often have their broadband provider screen known (zero list) viruses and the enterprises inspect and quarantine the whitelist of unrecognized bit patterns that may contain viruses.

Responding to an Attack

To limit damage from malware, organizations use security software to monitor all incoming and outgoing traffic. Security software is able to issue alerts to specified telephone or mobile numbers, or send e-mails to security staff. Once alerted, staff can take action against the attack. For example, infected computers and servers can be taken offline until the malware is erased from all hard drives and disks connected to it.

Many organizations use Intrusion Detection System (IDS) software or devices to monitor traffic and attempt to block Distributed Denial of Service attacks of millions messages meant to block legitimate incoming traffic. These systems monitor packets for malware and report them. Intrusion Detection and Intrusion Prevention Systems (IDPSs) attempt to stop these attacks as well as identify and report them. Often these types of software can divert the attacking bits to a part of the LAN separated from legitimate servers and computers. However, this is one of the most difficult breaches to protect against as automated bots, short for robots, are programmed to send millions of simultaneous strings of data to enterprises. This makes the network unavailable to legitimate incoming and outgoing traffic.

Security Software

Security software can be embedded in virtualized servers and containers with other applications or in a standalone appliance (a computer with a dedicated application).

There is a trend to embed security in multifunctional devices. Routers are often equipped with firewalls, and Local Area Network (LAN) switches also contain optional security software.

There is also specialty security for e-mail and other applications. Security software can be used to encrypt files containing passwords to protect the files from snoopers and employees not authorized to view sensitive files with personal information or intellectual property. This is important because many employees, contractors, and business partners now access files remotely and are allowed access only to particular applications and files.

In addition to all of these practices, firms hire outside organizations to conduct a security audit to identify weaknesses that leave the organization vulnerable to attacks. Auditors might identify out-of-date software that needs to be patched, or they might find unauthorized wireless devices.

Most security software and hardware products and services offer software that generates audit trails. Software records display indications of security breaches. Paying attention to them is an aid to identifying network weaknesses. In IT departments with large workloads, this does not always happen.

Encryption is the use of mathematical algorithms to make files unreadable except to users who have the software, the key, necessary to decrypt the files. Encryption is also used on files transmitted between corporate sites and between remote staff and their offices.

Block Chain

Block Chain is new a security protocol now being tested to manage data, track assets, and process financial transactions between banks. It is a distributed protocol without a central entity managing the interactions between nodes (computers). All data transmitted is encrypted when it is sent and decrypted at each node through which the data passes. All nodes along the transmission path must verify the data is not spam or fake in any way. Block Chain is made up of three main components: a network of computers, a protocol, and a way to reach consensus.

Block Chain is envisioned for tracking assets and shipments, and for money transfers between banks. It is also the basis for digital cryptocurrencies. In tests of financial transactions between clearing houses, transactions that formerly took 3 days to complete, were done in just seconds.

Continued

Other applications for Block Chain include tracking assets within organizations and payments between people and institutions; all can be completed without a central clearinghouse. Block Chain transactions and tracking are done through the use of a ledger, which has copies of all transactions and merchandise tracking steps. Each node (computer) in the chain of communications has a copy of the entire ledger and takes part in verifying each transaction.

One challenge in implementing Block Chain is that all of the nodes in each transaction need to be based on compatible network operating systems, network protocols, and back-office systems. Cryptocurrency tokens that are used for financial transactions include Bitcoin, Zeash, Monero, Ripple, and Ether.

Block Chain is architected in a mesh configuration with all nodes and institutions able to communicate with each other without a central entity managing the interactions. Each node verifies and authenticates the data as it is transmitted through networks. Platforms that use Block Chain operates on include Ethereum, Cardano, and Shuttle Fund.

It's likely that there will be additional applications for Block Chain, which is a security protocol. It's not known what the future of cryptocurrencies is.

Mounting Defenses via Firewalls

Firewalls are used to screen incoming messages for known viruses, worms, and *Trojan horses*. Trojan horses are computer programs that appear to have useful functions but actually contain malicious code. A video sent from Facebook can have a Trojan horse embedded within it. Some firewalls can also detect anomalies that are indicative of an attack, including packets that are too short. Firewalls can be in the form of software located at the ISP, the cloud, or at enterprise locations.

Protection from Internal Sabotage

The human factor is the weakest link in securing networks. Current technology is unable to prevent humans from acting in opposition to policy. Many human errors that result in security lapses are inadvertent. However, there are malicious employees who purposely steal or copy intellectual property or insert malware into computer files. An important safeguard against malicious employees is careful screening and reference checks before hiring staff.

An additional way to guard corporate data is a need to know policy that allows employees to access only applications that they need for their job. Other strategies include setting up rules such as not allowing the use of thumb drives in USB ports on computers, and building in alerts if a thumb drive is inserted into a staff person's computer. In addition, security staff can revoke all passwords and access to files as soon as a person's employment is terminated. Some organizations have security personnel walk fired staff or staff that quit their job out the door to ensure that they don't take company computers and/or files with them when they leave.

Recovery from Ransomware and Other Hacks

Recovery from attacks containing malware requires organizations to rid their network of corrupted files and computers that have viruses and other malware that enables hackers to spy on computer files. If duplicate files are stored offsite, the damaged disks containing viruses can be wiped clean or removed and replaced with the back-up files.

Ransomware attacks occur when a user clicks on a phishing link in their email that sends her to a malicious web site. The web site then automatically downloads encryption software to the user's computer and to other computers connected to the same LAN segment. The encrypted files are unusable because in most instances only the hacker has the software key that can *decrypt* (unlock) the files. Hackers behind ransomware attacks demand a payment in return for decrypting files to make them readable. This is a common ploy used against mostly small but also large organizations.

Small organizations are likely to pay the ransom to get use of their files back. Larger companies are more likely to have backups to the encrypted files, thus making them more immune to ransomware. An exception is Uber, which secretly paid a $100,000 ransom to a hacker in 2016 and only disclosed the breach in November of 2017. Uber is now facing five lawsuits because of its delay in reporting the breach.

In a minority of attacks, hacked companies have access to the decryption keys that can unlock the particular encryption used on their files. This is because they belong to a ransom security organization that stores decryption keys for a limited number of encryption codes. No More Ransom is an example of an organization specializing in decryption and protection against ransomware.

Redress—Taking Legal Action Against Hackers

Redress is the ability to take legal action against hackers and bring them to trial. One challenge in taking legal action against people responsible for hacking is the lack of extradition treaties between many western countries with China, Iran,

North Korea, and Russia. Thus the hackers originating attacks from these countries don't necessarily face trials and legal actions for their crimes of hacking into organizations in Europe and the Americas. Many of the hackers in these countries have the blessing of their government to steal data useful in manufacturing or weapons development.

When a hacker is brought to trial, building an airtight case is challenging. Hard drives containing viruses must be preserved exactly as they were following the attack. Computer forensics, evidence on computers, and storage systems must be conserved and presented in court. Any evidence of tampering with the evidence can invalidate the court proceeding.

Cyber Terrorism between Countries

In the past, countries engaged in spying and sabotage by planting agents in other countries. They hoped to learn strategic information about their enemies and potential enemies through networks of spies who often disguised themselves as friendly citizens. Some spies went beyond gaining information to planning acts of sabotage that damaged property, such as roads, bridges, and factories. These same countries also used networks of agents to ferret out spies trying to infiltrate their own institutions. All of these strategies still exist, but they are supplemented by cyber terrorism. Most cyber terrorism is conducted via the Internet.

Acts of cyber terrorism can also be implemented by using *sneaker attacks*, whereby inside employees are co-opted by foreign governments or terrorist groups to learn government secrets, plant software bugs in computer-controlled weapons systems, or copy strategic information inside the organization. This strategy is used to circumvent security measures whereby strategic departments such as armed forces or defense departments attempt to shield themselves by bypassing the Internet for all data communications. Entities such as these communicate to other locations on private lines that they lease or build. These networks only connect to other trusted departments or perhaps suppliers.

Cyber terrorism attacks not only cause computers systems to malfunction; they can also disable computer-controlled weapons systems. This is what occurred when North Korea launched its WannaCry worm that infiltrated computers networks worldwide. A *worm* is a software bug programmed to be activated at a later time. Worms are also referred to as bots. However, bots are more complex than worms and can do more damage. The May 2017 WannaCry attack was so sophisticated that many security experts thought a government, not an individual, planned it. WannaCry attacked hospitals, banks, and over 300 computers in hundreds of countries worldwide. Microsoft had issued a patch, which it classified as critical. However, it was ignored by many organizations, highlighting the criticality of keeping patches up-to-date.

PRIVACY

Privacy is the ability of people to control who sees information about them. It includes the ability to not share private information such as social security numbers, birthdates, job applications, and medical information. Privacy often conflicts with merchants' desire to use personal data for business purposes.

For example, information about consumer buying habits is a source of valuable information for advertisers who purchase ad space on the Internet. However, it can also create issues for people concerned about privacy. Software used by marketers is able to add small software files to browsers. These software files track which sites an individual visits. For example, if a user clicks an ad containing a video that uses Adobe's Flash or HTML5, the advertiser can compile a list of sites that he visits after clicking the ad. With this information, it can display ads based on what these habits suggest about his interests. For instance, advertisers might display ads about sporting events to people who visit sports-oriented sites.

When a shopper purchases, say, a skirt online or even browses for skirts, advertising networks can automatically display ads about these types of clothing to the purchaser when they visit other sites. In addition, information gathered in this manner from social networks is a powerful way to attract advertisers. In turn, advertising networks that use bots, small programs programmed to automatically collect information, place ads at many different sites and help amass large databases of demographic information about users' browsing and purchasing habits.

Another way that marketers collect information about users is from online games on social networks such as Facebook. Every time a Facebook member downloads a game application, the game developer acquires information about the game player. Developers track the user's data, compile it into lists along with information about other users, and then sell the data to marketers.

Web Site Tracking, Connected Devices, and Free Search Engines

The growth in numbers of computerized connected devices such as home thermostats connected to the Internet are sources where providers can collect information that can be sold to marketers. Toys are an example of Internet-connected items that have the potential to compromise children's privacy. Toy company Genesis manufactures an Internet-connected doll that answers questions children ask it. The questions are transmitted via the Internet to Nuance, a speech recognition company. Nuance sends back answers to their Genesis dolls.

A lack of enforcement in search engines, social networking applications, and e-commerce sites can compromise privacy. Advertising on search sites and social

networks is a large percentage of web sites' business. According to Google owner Alphabet's annual report, Google earned 84 percent of its $34 billion revenue from advertising in the first quarter of 2018.

Merchants that advertise on these venues gain information about consumer behavior often in exchange for providing free services to consumers. These services include free online games, flight information, and travel advice. Information on consumer behavior is compiled in massive databases and sold to advertising partners.

Additional connected devices collect information about consumers. Web sites sell this information to marketing companies that use data analytics to spot trends in user behavior that they use to target specific groups of individuals for marketing and to develop new services. The following are examples of where personal data is collected and organizations that amass data:

- Connected TVs that send data on Internet links on which viewers click. In 2017, the U.S. Federal Trade Commission (FTC) fined television manufacturer Vizio $2.2 million for collecting information about customers' viewing habits without first getting their permission.
- Overhead drones are able to collect data using sophisticated long range cameras.
- Credit bureaus have massive amounts of information about people. In the Equifax security breach made public in 2017, 143 million personally identifiable Social Security numbers were stolen.
- Automated toll scanners have the ability to track where cars have traveled by scanning license plate numbers.
- Late model cars with diagnostic software are able to track cars' routes and owners' driving habits.

In addition to the above, Verizon's Oath as well as other companies provide free e-mail. They state that they do not actually read the content in these messages. However, many do track user data. France's privacy watchdog fined Google $165,516 in 2017, claiming Google amassed large amounts of user data for advertising purposes without getting users' permission to collect the data. The privacy watchdog also accused Google of collecting data on sites users visited on the Internet. Subscribers to Verizon Wireless's Up reward program receive credit for every $300 they spend on Verizon Wireless services. The credits can be used for free concert tickets, movie premieres and phone upgrades. Verizon uses the data they collect in the Up ptrogram for the advertising businesses they acquired from Yahoo! and AOL.

THE IMPACT OF E-COMMERCE

E-commerce is a major factor, but not the only factor, in the drop in numbers of shoppers actually going to brick-and-mortar retail stores. Retailers that sell clothing, electronic devices, groceries, and pharmaceuticals are all suffering a loss in the amount of foot traffic. According to market research firm Statista, Retail e-commerce accounted for 10 percent of total retail sales in the third quarter of 2017. Providers of non-Internet outlets including travel agencies, book stores, and many magazines and newspaper subscriptions have been losing business to e-commerce since the early 2000s.

In addition to its impact on retail sales, e-commerce has affected how people of all ages find dating partners through web sites such as Match.com and Tinder. Additional drivers of e-commerce are massively multiplayer online games, online gambling, and pornography.

Combining Online Services with On-Site Stores

Online services provide convenience. People can access them at any time of day and from anywhere they have a broadband wireless or wireline Internet connection. Web site owners can also enhance their sites with photographs, video, and links to other locations. However, there are advantages of having both online and physical stores.

Amazon is a high-profile example of a business that initially started as an online-only business that has morphed into a combination of online and on-site retail stores. They purchased Whole Foods in 2017 as one way to establish a foothold in brick-and-mortar retailing. One of the advantages of this combination is the availability of a place where customers can pick-up packages ordered online. The ability to pick up packages at brick-and-mortar stores avoids the problem of stolen packages. Families where both people work often don't have anyone at home during daytime hours when merchandise is dropped off and left outside. This is an issue for people that live in apartment buildings as well.

Amazon is using its own retail outlets as well as its Whole Foods division, as drop-off points for deliveries. Customers are notified when a package is available at a Whole Foods location or an Amazon Go store near them for pick-up. An individual locker at stores avoids the issue of lost and stolen packages. As a rule these orders do not incur delivery fees.

Amazon, which until recently has had an online-only presence, is now opening Amazon Go brick-and-mortar convenience stores with automation that does away with the necessity of cashiers and checkout lines. Rather, people make purchases simply by taking merchandise off shelves after scanning their smartphones into a reader to enter

the store. Facial recognition is used to match individual shoppers with their credit card data on their mobile phone. In contrast, Wal-Mart has closed stores, built up its e-commerce web site, and purchased Jet.com, presumably as a vehicle for distributing products ordered online in the United States. In 2018 they acquired Flipkart Pvt Ltd, the largest online commerce site in India and an Amazon competitor there.

Currently, the Amazon Go store is not available to people without a smartphone with a credit card associated with it. Roughly 67 percent of the population had smartphones by early of 2018 according to consulting firm Statista. But, per Statista only 23.16 percent of retail sales were paid for using mobile payments.

FOSTERING CIVIC PARTICIPATION AND ENGAGEMENT—ONLINE FORUMS

Not all web activity is designed with a profit motive. Many blogs and mailing lists are started to further social causes or provide support and information to communities. Numerous online forums are non-profits: They generate no profit to people that start and support them; they simply disseminate information on topics of interest. For example, new mothers living in Brooklyn, New York, organized a neighborhood mailing list using the Google Group application to set up the mailing list and invite people to join. The list quickly grew to 120 mothers who all had babies around the same time and who lived in the same neighborhood of mostly townhouses and a few apartment buildings.

Town E-Mail Lists to Keep Communities Informed

Other examples of e-mail lists that provide a community forum are those organized around city and local services. One New England city, Framingham, Massachusetts, uses E-Democracy software to support citizen discussions. E-Democracy forums now host 50 forums in 17 locations across three countries: the United States, New Zealand, and the United Kingdom. The first one, a forum with information about elections, was started in 1994 in Minneapolis.

The city of Framingham has three E-Democracy e-mail forums: Framgov (Framingham government), Frambors (short for Framingham Neighbors), and Nobscot Neighbors to which residents can subscribe.

- Framgov is a forum in which people express opinions about upcoming votes by City officials, including taxes and recent government decisions. It is additionally a forum in which news and announcements about local government and schools as well as opinions about ordinances up for a vote are posted.

- Frambors is a forum for subscribers to ask for recommendations for service providers such as plumbers, contractors, electricians, beauty shops, and nearby restaurants. It provides a place to post opinions about services with which locals are happy as well as those they feel are unsatisfactory. Service providers often respond on Frambors to these comments. Frambors has more than 1,700 subscribers.
- Nobscot Neighbors is a forum at which people that live in the Nobscot section of North Framingham discuss zoning, new building permits, and traffic in their neighborhood.

The following is a quote from the moderator, Linda Dunbrack, who established the Frambors, Framgov, and Nobscot Neighbors online forums after the founder of the original forum died. At that point maintaining the forum founder's server was no longer feasible. The statement was written when the forums were established.

> *After Founder Steve Orr's unexpected death, we wanted to find a way to carry on the legacy of his community email list Frambors. After considering a variety of options, we decided to move the list to a non-profit host called E-Democracy.org.*
>
> *Steve Clift, Executive Director and Founder of E-Democracy, was a huge support as we made the transition, and helped us to make the transition as smooth and as painless as possible. According to the E-Democracy web site, "It is an organization dedicated to promoting civic engagement." It seemed to be a perfect fit, and comes with software and support that is customized to the needs of local issues forums.*

Creating the policies that govern it are critical. On Frambors, Framcom, and Nobscot Neighbors, the policy is that posts may not make personal slurs about another person that has posted a comment. Another example of such a policy decision is that all messages must be signed in the body of the message. This is different from the comment sections of newspaper articles where virtually all messages are anonymous and people feel free to say anything that's on their minds, often with little consideration. On the one hand, signing can inhibit those people who are uncomfortable with the loss of their anonymity, resulting in lowered written participation. On the other hand, signing messages has resulted in changing the whole tone of the conversation; civility, care in detail, and a number of other subtle characteristics all contribute to a marked degree of integrity in the list as a whole. The moderator of each forum first warns, and then disallows people from a list in which they post disparaging remarks about a specific person.

NETWORK NEUTRALITY

Network neutrality is the concept of broadband providers treating all traffic equally. It applies to people's ability to access the content they choose from wired as well as mobile devices. The following are the basic tenets of network neutrality:

- Treat all users' traffic in an equal manner.
- Prohibit slowing down traffic to particular web sites.
- Prohibit blocking lawful content from any provider.
- Prohibit blocking access to lawful content or service.
- Network operators are required to publicly disclose actual attainable speeds on their networks as well as reasonable network-management practices and terms of service.
- Landline network operators are not allowed to block lawful content, applications, or services, subject to reasonable network management. Operators of wireless networks are not allowed to block access to lawful web sites, subject to reasonable network management. Wireless operators are additionally not allowed to block applications that compete with their own voice or video telephony services.
- Providers of fixed broadband are not allowed to discriminate in transmitting lawful network traffic over a consumer's broadband access service.

During the Obama presidency, the primarily Democratic United States Federal Communications Commission (FCC) enacted the above network neutrality rules for wireline and mobile companies.

The Issues Surrounding Network Neutrality

However, in 2018, the Republican majority in the FCC rescinded network neutrality rules specifying that ISPs (Internet Service Providers) that provide access to the Internet (essentially telephone companies) must notify customers of their network policies. They additionally changed the classification of the Internet from telecommunications provider to information service. This is significant because the FCC regulates telecommunications services and not information services. The FCC order was titled "Restoring Internet Freedom Order." In overturning network neutrality on July 17, 2017, Ajit Pai, the chair of the FCC, stated:

> *Today, we take a much-needed first step toward returning to the successful bipartisan framework that created the free and open Internet and, for*

> *almost 20 years, saw it flourished. By proposing to end the utility-style regulatory approach that gives government control of the Internet, we aim to restore the market-based policies necessary to preserve the future Internet Freedom, and to reverse the decline in infrastructure investment, innovation, and options for consumers put into motion by the FCC in 2015.*

The two main issues around network neutrality are that some large ISPs such as AT&T, Comcast, and Verizon control networks throughout the USA and sell movies and television content. Comcast acquired content through its partial ownership of Hulu, and its 2011 purchase of NBC Universal. Comcast and AT&T transmit Netflix, Amazon, and Roku's content. These companies are competitors with whom these and other ISPs compete to attract streaming customers. Moreover, the merger between AT&T and Warner Brothers means that AT&T owns content including HBO and HBO NOW. Thus, they too will compete with streaming companies.

Network Neutrality Rationale—Compensation for Adding Network Capacity

Carriers that provide broadband and/or mobile network infrastructure have lobbied the federal government to overturn the Obama-era network neutrality rules. ISPs' public statements are that they should be compensated for investing in new equipment to carry the added traffic created by streaming services. The number of streaming providers and its percentage of streaming traffic are both growing. Thus, ISPs want to be paid for carrying this additional streaming traffic to homes in neighborhoods and over cellular networks. Below is a December 14, 2017, statement by CEO Jonathan Spalter of the USTelecom, a trade association made up mainly of broadband service providers, made the day after the FCC overturned network neutrality and classified the Internet as an information service, not a telecommunications service. The FCC is empowered to regulate only telecommunications services, not information services. The Federal agency referenced below is the FTC (Federal Trade Commission):

> *Today, the future of our open, thriving internet has been secured. The nation's top consumer protection agency now has jurisdiction over fairness and neutrality across the Internet; ensuring consistent rules apply to all players, including the most powerful online companies. And America's broadband providers—who have long supported net neutrality protections and have been committed to continuing to do so—will have renewed confidence to make the investments required to strengthen the nation's networks and close the digital divide, especially in rural communities. It's a great day for consumers and our innovation economy.*

The major carriers are in favor of eliminating network neutrality. They want to be compensated for upgrades to their networks to accommodate increased traffic. Currently,

most wireline access in the United States offer tiered unlimited plans for residential customers. Thus, most of these customers have no incentive to cut back on streaming because they pay a flat fee for broadband capacity however much capacity they use.

Pro Network Neutrality Proponents Against Fees and Throttling

Network neutrality proponents are concerned that network service providers have a monopoly or near monopoly on infrastructure and might slow down (throttle) or even block competitors' traffic in favor of their own services without concerns that subscribers will move to a different ISP. This puts competitive services at a disadvantage against the services offered by broadband providers and might lock consumers out of new, possibly lower-cost, offerings. This could be a problem for streaming providers because they are likely to pass on some of these costs to their customers. It will additionally increase consumer and enterprise costs for broadband connections because ISPs will have the option to charge content providers for not slowing down their traffic. This, essentially, creates a fast lane in networks for large content providers that are able to pay these fees.

Web site owners such as Zappos and content providers such as Netflix, Amazon, and Facebook profit from services they sell over the Internet. They pay for connections from their site to the Internet via local carriers. When these carriers transfer traffic to other networks needed to reach customers, neither the other network owners nor the carrier connected to the subscriber are compensated. See Figure 6-1 in the section "Streaming—A Disruptive Technology" in this chapter, which illustrates Netflix and others' streaming traffic connections to telephone companies' equipment.

Zero Rating

Zero rating is the process whereby ISPs and cellular providers exempt consumers from data fees and data caps for certain services, including unlimited video streaming. Carriers sometimes exclude their own content from data caps limits or fees for data. This is what AT&T instituted when it eliminated data caps from its DirecTV service. In a similar vein, Comcast eliminated data caps for its Stream TV service.

Another instance of zero rating is AT&T Mobility's 2012 announcement of a plan to shift some of its data network costs to developers whose customers generate the traffic. Under the plan, developers will have the option of paying fees to AT&T Mobility for cellular traffic generated by their applications. The applications for which developers pay usage fees will not count toward customers' data plans. Critics of the plan charge that it favors established developers that can afford the fees, which results in free usage for their customers.

The Have's vs. the Have Nots: First Class and Everyone Else

Many consumer watchdog organizations feel that creating exceptions for certain possibly lucrative applications will in effect create two different Internet classes of network services. They fear that the part of the network providing priority "first class" treatment for new applications will take increasing amounts of capacity away from ordinary applications and bog them down. This is because without network neutrality, carriers are free to charge content providers extra for not throttling the movies and TV shows carried over the Internet to subscribers.

Content providers such as Netflix and Amazon may pass on these fees they incur to customers. For many ISPs, competition for their wired broadband services has been non-existent or in a minority of locations; they have one competitor or at the most two competitors. This means they can demand concessions from Netflix and Amazon and their competitors without losing broadband customers. This makes it easy for them to make whichever policies are advantageous to them and to block content from providers that won't pay a premium for faster transmission. Customers in these locations have no or limited options for ISPs to use.

Prioritizing certain applications over others has the potential to increase congestion and slow down traffic that is not prioritized. It additionally has raises the possibility of a slowdown innovation and competition by making it costly for start-ups to pay for specialized treatment for the traffic they generate. Owners of smaller web sites as well as start-ups may not have the money to pay broadband networks for not slowing down their traffic.

Attempts to Overturn the Repeal of Network Neutrality

Opponents of the FCC's cancellation of network neutrality are currently pursuing two options for overturning this ruling. A coalition of 21 states' Attorney Generals plus Washington DC are suing the FCC over its cancellation of network neutrality. In addition to the states' efforts, Internet activists have also initiated suits to overturn the FCC's ruling. These include Mozilla Corp. (the producer of Firefox), the Open Technology Institute (part of the New America Foundation), Public Knowledge, the Free Press, and The Internet Association whose members include Google, Facebook, and Amazon.

There are additionally legislative efforts in the Senate to overturn the FCC's cancellation of network neutrality. However, even if the Senate succeeds, there is the hurdle of passing the bill in the House of Representatives. And, the president has the power to veto the legislation if it passes both houses.

Most ISPs agree that both wireless and wireline carriers should adhere to rules on transparency and that transparency should apply to network management and disclosure in understandable language about conditions and characteristics of their networks. Network management refers to a carrier's efforts to handle congestion and security threats. However, transparency means that ISPs will disclose throttling. It does not mean that they will not throttle or block certain traffic.

THE DIGITAL DIVIDE: BANDWIDTH, SKILLS, AND COMPUTERS

Most middle- and high-income residents in urban and suburban areas have Internet access with adequate capacity. This is not always the case with residents in rural areas where, if broadband services are available, they are often costly and slow compared to service in more developed regions. The slow speeds discourage users from signing up for these services because services such as video depend on a higher capacity to work well.

For low-income groups, costs for computers and broadband can be prohibitive, given their limited resources. These circumstances contribute to what has been termed the *digital divide*, by which segments of populations do not have equal access to Internet and computer services. These populations are essentially locked out of online educational services, the ability to apply for and look for jobs online, and other services such as instructional materials and electronic training for their children.

While the digital divide between wealthy and poor residents is decreasing, as of January 2018, FCC member Jessica Rosenworcel stated that there are still over 24 million Americans and 12 million children with no broadband services. Government policies and allocation of resources have a major impact on bandwidth availability. Countries can provide free computer training for the unemployed to open up new opportunities for them. Training can enable the unemployed to apply online, which opens additional opportunities.

The digital divide is more than the simple measurement of whether or not Internet access is available. The digital divide is further measured by the following:

- **The amount of available bandwidth** This is the network capacity in terms of bits per second and cost per kilobit or per megabit compared to urban sections of a country. In 2018, the FCC in defined broadband bandwidth as 25/3—25 megabits downstream to subscribers and 3 megabits upstream to the Internet.
- **The quality of computer equipment available to users** Is it compatible with the latest browsers and is it capable of handling video?
- **The availability of training** Do users know how to navigate the Internet to accomplish their goals?

The digital divide in the United States is decreasing in part because of the use of fixed wireless technologies in rural areas. AT&T, CenturyLink, Verizon, and Frontier all have stated their intention to increase broadband capacity in rural areas using new, higher capacity fixed wireless. See Chapter 7, "Mobile and Wi-Fi Networks," for information on fixed wireless technologies. However, according to Pew Research Center's 2016 surveys, the digital divide in the United States is most pronounced in:

- Minority populations
- Groups with lower incomes

- Residents in rural areas
- People with disabilities including those with low vision, hearing loss, and physical limitations
- Seniors—particularly lower-income, less-educated seniors

Economic policies make a difference in the availability of broadband. Tax credits for new networks encourage carriers to upgrade equipment and infrastructure. Outright subsidies are a more direct option for improving networks. Countries such as Australia, China, and Japan have underwritten the cost of building fiber-optic or advanced mobile networks in rural areas. Improved broadband is one step in bringing remote areas into the online economy.

Community resources can bridge some of the gaps in the digital divide. In the United States, public libraries provide free Internet access, computers, and often training in how to use them. This is particularly critical in areas where residents do not have up-to-date computers or the expertise to access the Internet. In an effort dubbed "The Library of Things," some libraries lend technology gear to families to promote computer literacy and Internet access. For example, they lend portable Wi-Fi hot spots so that people without Wi-Fi can access the Internet from a computer and Roku set-top boxes so people can try out streaming.

Internet Pricing and Competition

The cost of Internet access is a factor in increasing or lessening the digital divide. In 2017 the United States had the 12th highest average Internet speed worldwide according to speed monitoring company Ookla in the December 17, 2017, article at *recode*, "Global Internet Speeds Got 30% Faster in 2017," by Rani Molla. In contrast, the average cost in the United States—$66.17—was 114th highest in the world out of a total of 196 countries surveyed. Iran and the Russian Federation were among the 113 countries with lower-cost Internet access. This statistic was published in the *Forbes* November 22, 2017, article, "The Most and Least Expensive Countries for Broadband," by Niall McCarthy. The source for the statistic was consulting firm Statista.

Because people in many areas of the United States have few or no choices for an ISP, there is little incentive for carriers to lower their prices so that it is more affordable for lower-income people. Another factor on higher prices in rural areas is the higher cost to cable rural areas. These steep costs result from the fact that there are fewer customers per square mile in sparsely populated areas so ISPs don't earn enough revenue from the few customers to make it worthwhile to lay fiber and charge lower prices in these areas.

INTRANETS AND EXTRANETS

An *intranet* is the use of web technology for the sole, dedicated use of single site and multisite organizations. Intranets are a way to collaborate, distribute information, software, and other services within an organization using web-like software tools.

Extranets extend the reach of intranets from internal-only communications to sharing documents, fixing software bugs, and providing information for business-to-business transactions. Online banking is an example of an extranet.

Intranets

When they were first developed, intranets, which are based on web technology, served as repositories of centralized information. Intranets are still a single source of an organization's information. However, they are now as a whole better organized so that employees can find what they are looking for faster. Clear organization of information is an important area where intranets can excel. In large organizations this is not always the case, as some departments do not always update intranets with the latest information. Having management to which the intranet is important creates a culture where departments update their intranet when needed. Examples of intranet software include Facebook's Workplace collaboration and networking software, Microsoft's Teams, Axero, Jostle, MyHub, and Intranet Connections.

Collaboration where people in distant offices can work jointly on projects and reports is an important way to improve productivity. Some additional intranet functions include:

- Staff reading documents and agreeing on or modifying parts
- Commenting on sections of documents by employees who work at different physical locations to foster working together on joint projects
- Discussion forums
- Content approval flows by appropriate staff
- Calendaring for setting up meetings

Intranet functions that support employee functions include:

- Online training that users can complete on the intranet
- Posting internal job openings
- Providing company-recommended software and updates that employees can download to their computers

- Checking whether user applications need updating and that all security patches are in place when employees log on to the intranet
- Managing human resources functions such as accessing pay stubs and appraisals, making changes to tax forms, changing user addresses, and selecting benefits
- Enabling the ability to submit time cards and expense reports on the intranet
- Making available corporate documents, such as organizational practices, required documents, templates for résumés and sales proposals, technical magazines, and corporate directories
- Establishing wikis with information about particular technologies or work-related information

In addition, intranets at global organizations often mimic web functions by providing social networking functions. The directory might have fields in which people can list special interests such as trekking or music. Employees can form groups around these interests.

Firewall and other security software control staff members' access to corporate information on intranets. Restrictions can be applied to prevent employees from accessing inappropriate databases and applications. Not everyone has access to all files. Rather, employees can be placed in groups based on the applications to which they are allowed access.

Potential Issues with Intranets

The most common complaints about intranets are the difficulties in keeping them updated. Time and attention devoted to organizing information often depends on whether top management buy into the intranet as a priority. If the information on the intranet is out of date, the intranet loses much of its value. Organizations without either management support or tools to support automated or simple maintenance and implementation might have intranets do little to enhance employee productivity.

In some organizations, every department posts their own updates. If updates are cumbersome and time-consuming to make, they might not be posted in a timely fashion. To make it easier to update intranets, organizations can deploy software packages such as Adobe Dreamweaver, Microsoft SharePoint Designer, and Expression Web, all of which have user-friendly interfaces that make it easier to update intranets and extranets. Often, a centralized IT organization manages the intranet and sets technical standards for it. Having a single-password, single-sign-on procedure for a uniform intranet saves time on calls from users who forgot their passwords.

Extranets—Saving Money on Customer Service

Extranets use a web interface for secure access by customers, business partners, and temporary employees. Organizations typically limit access to applications more so than intranets because they are used with outside individuals and organizations. Individual vendors or partners have access only to specific applications. Access to extranets is generally password-protected or password-plus-token. A token is a small device about the size of a large house key that generates random numbers at predefined intervals. Users key in the number displayed on their token plus their password to access applications.

Online banking is an example of an extranet service that saves staffing costs. Customers transfer money between accounts, pay bills, and gain instant, graphical interfaces to the status of their accounts. This is highly advantageous to banks because it saves money on financial transactions as well as staffing costs. Moreover, banks' extranets are a way to solicit business. They offer customers services such as loans, home mortgages, and other financial instruments. Banks and other organizations also offer customers online bank statements and electronic bills through their extranets. These electronic services save mailing expenses and printing costs.

The following is a quote from an employee on the benefits of their extranet, which is used for business to business transactions:

> *In my company, each of the customers is given a special identification number and access to a specific application. The customer can use his identification number and log bugs and issues that he sees in our product. The customer can specify the importance of the bug and keep track of the progress made on its resolution.*

Because of security concerns, many extranets are located at web hosting sites. The hosting company's customer has his own computer at the hosting company. High-speed Carrier Gigabit Ethernet capacity lines connect the hosting company to the Internet backbone. Companies often remotely upload or download information to their host-located computer via Carrier Gigabit Ethernet. Online learning is an example of an extranet service. It provides web-like access to educational material for school staffs and students. This is an advantage to schools that offer it because it enables them to offer their courses to students that are not within commuting distance of the college or university. In addition to supplying extranet software, online-learning companies offer to host the application at their own site.

Index

Numbers

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z