CHAPTER 1

Living in a Network-Centric World

Cisco Press is committed to providing the Cisco Networking Academy community with quality products to support teaching and learning the online curriculum.

To address the needs of the early adopters of the new CCNA curriculum, we are making available prepublication drafts of some of the manuscript chapters. Classes can review and use these materials while Cisco Press completes the book development process and gets the books printed and bound. Given the timeframe though, please be aware that the chapter you are about to read is not fully proofread at this stage.

To order the final published book, please go to http://www.ciscopress.com/title/9781587132087.

Objectives

Upon completion of this chapter, you will be able to answer the following questions:

- How do networks impact our daily lives?
- What is the role of data networking in the human network?
- What are the key components of a data network?
- What are the opportunities and challenges posed by converged networks?
- What are the characteristics of network architectures?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary.

data network *page 4*
network *page 4*
Internet *page 4*
download *page 5*
instant messaging *page 5*
real-time *page 5*
blogs *page 5*
podcasts *page 5*
wikis *page 6*
collaboration tool *page 6*
Packet Tracer *page 7*
intranet *page 8*
extranet *page 8*
wireless technology *page 8*

We now stand at a critical turning point in the use of technology to extend and empower the human network. The globalization of the Internet has succeeded faster than anyone could have imagined. The manner in which social, commercial, political, and personal interactions occur is rapidly changing to keep up with the evolution of this global network. In the next stage of our development, innovators will use the Internet as a starting point for their efforts—creating new products and services specifically designed to take advantage of the network capabilities. As developers push the limits of what is possible, the capabilities of the interconnected networks that form the Internet will play an increasing role in the success of these projects.

This chapter introduces the platform of data networks upon which social and business relationships increasingly depend. The material lays the groundwork for exploring the services, technologies, and issues encountered by network professionals as they design, build, and maintain the modern network.

Communicating in a Network-Centric World

Humans are social animals who depend on the interaction with others for daily needs. Throughout human history, people, with few exceptions, have depended on the structure of various community networks for safety, food, and companionship. People have been networking for a very long time.

The ways in which humans interact are constantly changing. As technical developments throughout history have come about, the methods of human communication have developed as well. At one time, sounds and gestures were all humans used to communicate, but now the Internet allows people to instantaneously share all types of communication—written, pictures, sound, and video—with thousands of people near and far away using computers.

Networks Supporting the Way We Live

Just a few years ago, people communicated mostly on a local level because communicating with people far away was complicated and expensive. People talked in person or used the telephone for most voice communication, the postal service delivered most of the written messages, and the television broadcast one-way video communication. Each of these methods is still working, but all three of them are converging into web-based communication technologies. The extended reach and the reduced cost of communication through the Internet has changed the way businesses interact with their customers, the way people share information and resources, and the way friends and families stay close to each other.

As with every advance in communication technology, the creation and interconnection of robust data networks are having a profound effect. Early ***data networks*** were limited to exchanging character-based information between connected computer systems. Current ***networks*** have evolved to carry voice, video streams, text, and graphics between many different types of devices. Previously separate and distinct communication forms have converged onto a common platform. This platform provides access to a wide range of alternative and new communication methods that enable people to interact directly with each other almost instantaneously.

The use of the ***Internet*** spread quickly as connectivity became available in the 1990s. The early users of the World Wide Web were mostly university researchers exchanging information, but other people and businesses quickly figured out how to take advantage of web-based communications. This sparked the creation of many new businesses and careers.

The immediate nature of communications over the Internet encourages the formation of global communities. These communities foster social interaction that is independent of location or time zone.

Technology is perhaps the most significant change agent in the world today, as it helps to create a world in which national borders, geographic distances, and physical limitations become less relevant and present ever-diminishing obstacles. The creation of online communities for the exchange of ideas and information has the potential to increase productivity opportunities across the globe. As the Internet connects people and promotes unfettered communication, it presents the platform on which to run businesses, to address emergencies, to inform individuals, and to support education, science, and government.

The Internet has quickly become an integral part of our daily routines. The complex interconnection of electronic devices and media that comprises the network is transparent to the millions of users who make it a valued and personal part of their lives.

Data networks that were once the transport of information from business to business are now also used to improve the quality of life for people everywhere. In the course of a day, resources available through the Internet can help you do the following:

- Decide what to wear using online current weather conditions
- Find the least-congested route to your destination, displaying weather and traffic video from webcams
- Check your bank balance and pay bills electronically
- Receive and send e-mail at an Internet cafe over lunch
- Obtain health information and nutritional advice from experts all over the world, and post to a forum to share related health or treatment information

- ***Download*** new recipes and cooking techniques to create a spectacular dinner
- Post and share your photographs, home videos, and experiences with friends or with the world
- Use Internet phone services
- Shop and sell at online auctions
- Use instant messaging and chat for both business and personal use

Examples of Today's Popular Communication Tools

As in the past with novel technologies like the telephone and television, the general public readily adapted the Internet into daily use. The existence and broad adoption of the Internet has ushered in new forms of communication that empower individuals to create information that can be accessed by a global audience. Popular communication tools include instant messaging, blogs, podcasts, and wikis.

Instant messaging (IM) is not a new technology, but recent enhancements have increased its user base. IM is ***real-time*** text communication between two or more users. Based on the earlier service known as Internet Relay Chat (IRC), it has expanded to include voice, photo and video sharing, and file transfers. IM is different than e-mail in that e-mail can be delayed when sent, but IM is, as its name implies, instantaneous. IM is an increasingly popular tool used by customer service centers to assist customers and friends in communicating with each other.

The first generation of web use was as a place for people to find static information, educational resources, and business information. But web content is changing from a place for people to get information to a place for people to contribute information as well. The users of the web are, in many ways, becoming the creators of the content. The emergence and use of social software tools such as blogs, podcasts, and wikis enable the interaction and contribution of users.

Blogs, also known as weblogs, are web pages where people can publish their personal opinions and thoughts about any conceivable topic. Blogs, for better or worse, allow unfiltered and unedited publication of ideas from experts and nonexperts alike. This is important because it demonstrates a shift from reliance on traditional media content from experts to a reliance on other users to provide their personal knowledge.

Podcasting is an audio-based medium that originally enabled people to record audio and convert it for use with iPods—small, portable devices for audio playback manufactured by Apple. The ability to record audio and save it to a computer file is not new. However, podcasting allows people to deliver their recordings to a wide audience. The audio file is placed

on a website (or blog or wiki), where others can download it and play the recording on their computers, laptops, and iPods.

Wikis are another example of publicly created web content. Individuals create blogs, but wiki web pages are created and edited by groups of people sharing information. The best known example of a wiki is the Wikipedia, an online encyclopedia made up of public contributions edited by the public users. Thousands of people contribute their specialized knowledge to the Wikipedia, and anyone can access the information at no cost. Many groups create their own wikis for member instruction, and many organizations create limited wikis as an internal collaboration tool. A ***collaboration tool*** is web-based software that allows people to work together on a project over the web.

Networks Supporting the Way We Learn

The advances in the Internet and collaboration tools have been the force behind major changes in education. As web reliability and access have increased, more institutions have come to depend on technology to perform core educational functions. For example, distance education was once limited to correspondence, videos, or video and audio conferences. With newer collaboration tools and stronger web technologies, online learning can engage remote students in interactive learning and real-time assessment. The classes can use document sharing, wikis, online video, and online testing software to enhance learning opportunities. Student learning is becoming less dependent on location and schedule, which opens courses to potential students who previously could not attend classes.

The methods of both face-to-face and online instruction are changing with the introduction of web tools such as wikis. Traditionally, a teacher provided course content and the class might have benefited from some discussions. With online tools equally available to all students, many classes focus on sharing the opinions and expertise of students. This is a significant change for many students and instructors, but it is an example of the impact of technical change on society's traditions.

The administration side of instruction has also changed. You might have enrolled in this course on the web and paid with an online bank account. Your final grades might be posted on a school web site, and you might have never had a face-to-face meeting with your advisor. This is the business side of education, and it is changing as new management tools become available.

The structure of this course is an example of the influence the changes of the web have had on instruction. The Cisco Networking Academy Program, which offers this course, is an example of a global online learning experience. The instructor provides a syllabus and establishes a preliminary schedule for completing the course content. The Academy program supplements the expertise of the instructor with an interactive curriculum that provides

many forms of learning experiences. The program provides text, graphics, animations, and a simulated networking environment tool called ***Packet Tracer***. Packet Tracer provides a way to build virtual representations of networks and emulate many of the functions of networking devices.

Students can communicate with the instructor and fellow students using online tools like e-mail, bulletin/discussion boards, chat rooms, and instant messaging. Links provide access to learning resources outside the courseware. Blended e-learning provides the benefits of computer-based training while retaining the advantages of instructor-led curriculum. Students have the opportunity to work online at their own pace and skill level while still having access to an instructor and other live resources.

In addition to the benefits for the student, networks have improved the management and administration of courses as well. Some of these online functions include enrollment, assessment delivery, and grade books.

In the business world, the use of networks to provide efficient and cost-effective employee training is increasing in acceptance. Online learning opportunities can decrease time-consuming and costly travel yet still ensure that all employees are adequately trained to perform their jobs in a safe and productive manner.

Online courseware and delivery offer many benefits to businesses, including the following:

- **Current and accurate training materials:** Collaboration among vendors, equipment manufacturers, and training providers ensures that the courseware is up to date with the latest processes and procedures. When errors in materials are found and corrected, the new courseware is immediately available to all employees.
- **Availability of training to a wide audience:** Online training is not dependent on travel schedules, instructor availability, or physical class size. Employees can be given deadlines by which training is to be completed, and the employees can access the courseware when it is convenient.
- **Consistent quality of instruction:** The quality of the instruction does not vary as it would if different instructors were delivering an in-person course. The online curriculum provides a consistent core of instruction to which instructors can add additional expertise.
- **Cost reduction:** In addition to reducing the cost of travel and the lost time associated with travel, there are other cost-reducing factors for business related to online training. It is usually less expensive to revise and update online courseware than it is to update paper-based material. Facilities to support in-person training can also be reduced or eliminated.

Many businesses also provide customer training online. This courseware enables the customers to use the products and services provided by the business in the best manner, reducing calls to the help lines or customer service centers.

Networks Supporting the Way We Work

Advances in computer networks have had a tremendous impact on businesses. Many economists attribute much of the economic growth of the last couple of decades to increased productivity in business stemming from improved business technologies.

Many companies use collaboration software packages that allow distributed work groups—people working together but not in the same physical location—to interactively create documents and contribute to projects in real time. These collaboration tools demonstrate the global nature of online business and are now essential to large and small businesses alike.

Different companies use different types of networks. Employees can meet on the Internet or they can join a restricted group on a company ***intranet***, which allows only internal employee access. Another type of network is an ***extranet***, a type of network that allows outside vendors special access to limited information in a company.

To reap the benefits of these technology tools, businesses must provide the continuing training and education of workers. The ability to learn and adopt new ways to implement technology into the workplace is a valuable skill sought after by most employers.

Most of the preceding examples highlight the benefits that larger corporations experience from computer networks. Networks also have enabled small businesses to achieve success. Consider these scenarios based on small businesses stories:

- A small bookstore owner has been struggling to survive in a business location that sees a decline in foot traffic and forecasts going out of business within a year. As he prepares to close the store, he lists his rare book inventory on the web. Over a couple of months, the web traffic grows and he gets better prices for his books. Soon the web traffic outpaces foot traffic. Within four months, he relocates to a much less expensive location and shifts the business focus to web-based retailing of rare books. By adapting to changing technologies, the bookseller is thriving in a more lucrative sector of the business.

- On a fishing boat off the coast of Alaska, the crew picks the best fish from a catch and puts them, still alive, into a special holding tank on the boat. Looking into the tank is a webcam, connected to the web using ***wireless technology*** through satellite. Meanwhile, at a top-quality restaurant in Washington, D.C., the owner wants only the finest-quality fish served on her menu. She browses the web to her favorite provider, who links her to the fisherman on his boat in Alaska. She is able to pick the fish she wants. Arrangements

are made with a shipping company for overnight delivery. The restaurant owner tracks the shipment on the web, and when she sees that it will arrive in time for dinner, she edits and prints the menu. In this scenario, two businesses thousands of miles apart use networks to work together to provide a top-quality product for the best price.

Not more than a decade or so ago, neither of these scenarios would be possible. These success stories, along with thousands of others like them, happened because people used networking technologies in imaginative ways to succeed in business.

Networks Supporting the Way We Play

You have learned how networks provide learning and business opportunities, but they offer plenty of recreation options as well. Travel sites can respond to last-minute market conditions for hotel, flight, and cruise availability, which benefits both sellers and consumers. Media and entertainment companies provide websites that offer books, games, TV shows, and movies. The music industry provides songs for download. While the web has helped the music industry reach new audiences and cut costs, record companies have also faced new challenges, such as music-sharing sites and copyright issues. Online auction sites provide an excellent venue for hobbyists and collectors to exchange information and items safely and securely.

Some of the most innovative developments in network technology come about trying to satisfy the voracious appetite of the entertainment sector. Online game companies are constantly pushing for better bandwidth and faster processing to improve their products, and online gamers are willing to spend the money necessary to buy the latest equipment that will improve their gaming experience.

Movie rentals and video-sharing and -distribution systems are newer web technologies that are quickly evolving as faster web connections become more widespread.

Communication: An Essential Part of Our Lives

Communication in our daily lives takes many forms and occurs in many environments. We have different expectations depending on whether we are chatting through the Internet or participating in a job interview. Each situation has its corresponding expected behaviors and styles.

These expectations are the rules of communication, and some of the elements are universal. Taking a closer look at the way humans communicate will introduce many of the necessary elements of network communication as well.

What Is Communication?

People have many ways of communicating with each other. Whether the communication is verbal or nonverbal, face-to-face or over the telephone, or in a handwritten letter or in a chat room, successful communication requires common rules.

The rules of communication are also known as protocols. Some of the protocols required for communication to occur include the presence of

- An identified sender and receiver
- An agreed-upon method of communicating (face-to-face, telephone, letter, photograph, and so on)
- Common language and grammar
- An agreed-upon speed and timing of delivery (for example, "Please slow down so that I can understand you.")
- Confirmation or acknowledgment requirements (for example, "Is that clear?" "Yes, thank you.")

Not all communications have the same agreed upon protocols. For example, an important legal letter can require a signature and response from the recipient, but personal letters need no such acknowledgment.

People are unaware of many of the rules they follow while communicating because they are ingrained in language and culture. Tone of voice, pausing between thoughts, and polite ways to interrupt are just a few examples of implicit rules that humans follow.

Quality of Communication

Computers and computer networks have no such ingrained communication knowledge, but similar protocols are still required for network devices to communicate. Successful communication between computer network devices, just as is true with communication between people, occurs when the meaning of the message understood by the recipient matches the meaning intended by the sender.

There are many potential barriers to successful communication between computers on a network. The process of sending a message on a computer network can be complex and have many steps and conditions, and any step poorly performed or condition not properly met can potentially ruin the message. The steps and conditions, or factors, can be separated into internal and external groups.

The external factors stem from the complexity of the network and the number of devices handling the message en route to the destination. Examples of external factors include the following:

- The quality of the pathway between the sender and the recipient
- The number of times the message has to change form
- The number of times the message has to be redirected or readdressed
- The number of other messages being transmitted simultaneously on the communication network
- The amount of time allotted for successful communication

Internal factors include the following:

- The size of the message
- The complexity of the message
- The importance of the message

More complex messages can be more difficult for the recipient to completely understand, and larger messages have greater potential to be distorted or incomplete at the destination.

The Network as a Platform

The ability to reliably communicate to anyone, anywhere, is becoming increasingly important to our personal and business lives. Adding to the demand of immediacy is the requirement that different types of messages, such as phone, text, and video, be accommodated as normal forms of communication. To support the immediate delivery of the millions of various messages being exchanged among people all over the world, we rely on a web of interconnected networks. The following sections describe communication over networks, different elements that make up a network, and convergence.

Communicating over Networks

Networks directly impact how we live, and the role of networks is increasingly important to people in all parts of the world. The task of reliably delivering millions of messages simultaneously would be too much for any one network to perform. Therefore, a web of smaller, interconnected networks of various sizes and capabilities delivers the many messages and data streams around the world.

Elements of a Network

The webs of data or information networks vary in size and capabilities, but all networks have four basic elements in common:

- **Rules or agreements:** Rules or agreements (protocols) govern how the messages are sent, directed, received, and interpreted.
- **Messages:** The messages or units of information travel from one device to another.
- **Medium:** A medium is a means of interconnecting these devices, that is, a medium can transport the messages from one device to another.
- **Devices:** Devices on the network exchange messages with each other.

Figure 1-1 depicts a small network featuring rules, messages, a medium, and two devices.

Figure 1-1 Elements of a Network

Early networks had varying ***standards*** and, as a result, could not communicate easily with each other. Now global standardization of these elements enables easy communication between networks regardless of the equipment manufacturer.

People use many technologies and devices that they do not completely understand. Driving a car, for example, is a common function for many people. When a driver starts a car, puts it into gear, and steps on the gas, many systems begin to work together. The car moves because an ignition system started the car, a fuel system regulates power, electrical systems run lights and gauges, and a complex transmission chooses appropriate gears to make the car move as directed by the driver. All of this happens under the hood and out of sight and

mind to the driver, who focuses on the task of driving safely to a destination. Most drivers know little or nothing about how a car works but are still able to use it effectively for their own purpose.

Computer networks are similar to cars in the example. Two people communicating on end devices in different networks can do so only if many complex processes are successfully completed. These processes include a message, some form of media, various devices, and protocols working together.

Message

Messages is a generic term that encompasses web pages, e-mail, instant messages, telephone calls, and other forms of communication enabled by the Internet. The message must be one that the network can carry. First, the messages must be supported in software at the end devices. Instant messaging and chat, for example, require some software setup before a session can begin. Different software is required for audio and video conferencing. These software programs that support communication functions are called services, and to initiate a message, a service must be installed. Examples of services include e-mail, IP telephony, and use of the World Wide Web.

It does not matter whether the message is text, voice, or video, because all forms are converted into ***bits***, ***binary***-coded digital signals, to be carried over a wireless, copper, or fiber-optic connection. The digital signal can change with the media, but the original message content will remain intact.

Medium

The medium that physically carries the message can change several times between the sender and the receiver. Network connections can be wired or wireless.

In wired connections, the medium is either copper, which carries electrical signals, or optical fiber, which carries light signals. Copper medium includes cables, such as twisted-pair telephone wire, coaxial cable, or most commonly, what is known as Category 5 unshielded twisted-pair (UTP) cable. Optical fibers, thin strands of glass or plastic that carry light signals, are another form of networking media.

In wireless connections, the medium is the Earth's atmosphere, or space, and the signals are microwaves. Wireless media can include the home wireless connection between a wireless router and a computer with a wireless network card, the terrestrial wireless connection between two ground stations, or the communication between devices on Earth and satellites. In a typical journey across the Internet, a message can travel across a variety of media.

Devices

Several devices, such as switches and routers, work to see that the message is properly directed from the ***source***, or originating device, to the destination device. At the destination network there can be more switches, cable, or perhaps a wireless router that will deliver the instant message to the receiver.

Graphics and icons are common when reading about networks. Icons, or small pictures, arranged to represent a network's layout, can greatly clarify information about the design of the network. Figure 1-2 shows various network device symbols. The desktop, laptop, and IP phone represent end-user devices, whereas the rest of the icons depict network equipment or media used to connect the end devices. These icons do not refer to specific models or features on devices, which can vary greatly. Table 1-1 briefly describes the network symbols.

Figure 1-2 Network Device Symbols

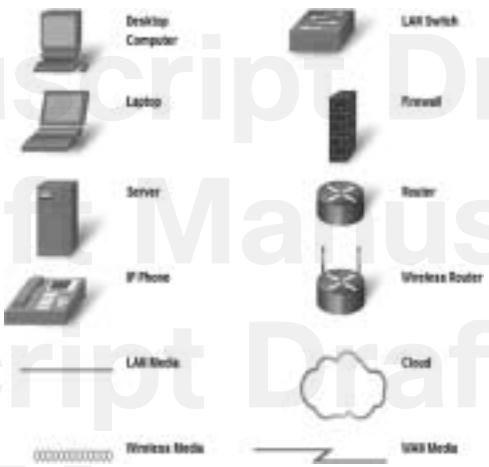


Table 1-1 Internal and External Factors Affecting Successful Communication

Symbol	Description
Desktop computer	A common computer used in a home or office
Laptop	A portable computer
Server	A computer dedicated to providing application services to end users on a network
IP phone	A digital telephone that carries voice as data over data networks instead of analog phone lines
LAN media	Local-area network media, usually copper cable
Wireless media	Depicts local-area network wireless access
LAN switch	The most common device for interconnecting local-area networks
Firewall	A device that provides security to networks
Router	A device that helps direct messages between networks
Wireless router	A specific type of router often found in home networks
Cloud	A symbol used to summarize a group of networking devices out of local management control, often the Internet itself
WAN media	One form of wide-area network (WAN) interconnection, represented by the lightning bolt–shaped line

The standardization of the various elements of the network enables equipment and devices created by different companies to work together. Experts in various technologies can contribute their best ideas on how to develop an efficient network, without regard to the brand or manufacturer of the equipment.

Rules

All communication processes happen, as far as humans can tell, in an instant, and tens of thousands of processes can happen in a single second. To work properly, the network processes must be tightly controlled. Rules govern every step of the process, from the way cables are designed to the way the digital signals are sent. These rules are called protocols, and the communications industry has standardized most of them to allow people in different

places with different equipment to communicate. The most common protocols are ***IP (Internet Protocol)*** and ***TCP (Transmission Control Protocol)***. These protocols work together and are usually known as the TCP/IP protocol stack. TCP/IP works along other protocols, for example, Extensible Messaging and Presence Protocol (XMPP), which is an instant messaging protocol, to provide communication rules involving different services. Table 1-2 lists some common services and the protocols that support them.

Table 1-2 Services and Their Protocols

Service	Protocol ("Rule")
World Wide Web (WWW)	HTTP (Hypertext Transport Protocol)
E-mail	SMTP (Simple Mail Transport Protocol) and POP (Post Office Protocol)
Instant message (Jabber, AIM)	XMPP (Extensible Messaging and Presence Protocol) and OSCAR (Open System for Communication in Realtime)
IP telephony	SIP (Session Initiation Protocol)

People often only picture networks in the abstract sense: We create and send a text message, and it almost immediately shows up on the destination device. Although we know that between our sending device and the receiving device there is a network over which our message travels, we rarely think about all the parts and pieces that make up that infrastructure. The following list ties together how the elements of networks—devices, media, and services—are connected by rules to deliver a message:

1. An end user types an instant message to a friend using an application on a PC.
2. The instant message gets converted into a format that can be transmitted on the network. All types of message formats—text, video, voice, or data—must be converted to bits before being sent to their destinations. After the instant message is converted to bits, it is ready to be sent onto the network for delivery.
3. The network interface card (NIC) inside the PC generates electrical signals to represent the bits and places the bits on the medium so that they can travel to the first network device.
4. The bits are passed from device to device in the local network.

5. If the bits need to leave the local network, they leave through a router connecting to a different network. There can be dozens, even hundreds, of devices handling the bits as they are routed to their destination.
6. As the bits get close to their destination, they once again get passed through local devices.
7. Finally, the NIC on the destination device accepts the bits and converts them back into a readable text message.

Converged Networks

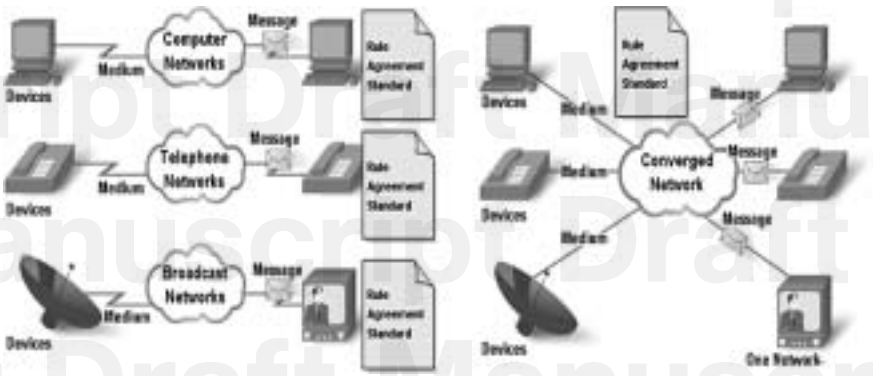
Communication technologies evolved at different times and in different places in the twentieth century. Many developments in radio broadcast technology were driven by military necessity, yet developments in broadcast television grew to answer a market demand. The telephone evolved as a wired technology and then as a wireless technology. Computer communication developments came much later in the century. For example, the first text e-mail message was sent in the 1960s, but e-mail did not become popular until the 1980s. Now it is quite common to use a computer for instant messaging, telephone calls, and video sharing.

The technology and protocols of each of these communication methods developed largely independent of each other, and most users of TV, telephone, and computer services pay different providers for each service. But recent developments in each area have driven broadcast and telephony to the digital technology already used by computers. This coming together of technologies onto a digital platform is called ***convergence***.

Convergence occurs when telephones, broadcasts, and computer communications all use the same rules, devices, and media to transport their messages. On a converged network, or platform, different devices, such as televisions or cell phones, will use a common network infrastructure to communicate.

Figure 1-3 demonstrates the concept of nonconverged systems on the left and a converged network on the right.

Figure 1-3 Convergence



Network technologies are still evolving and converging. As improvements occur, the services offered will expand beyond communications and into shared applications. The convergence of the different types of communications networks onto one platform represents the first phase in building the intelligent information network. We are currently in this phase of network evolution. The next phase will be to consolidate not only the different types of messages onto a single network but to also consolidate the applications that generate, transmit, and secure the messages onto integrated network devices. Not only will voice and video be transmitted over the same network, the devices that perform the telephone switching and video broadcasting will be the same devices that route the messages through the network. The resulting communications platform will provide high-quality application functionality at a reduced cost.

The Internet is the prime example of converging technologies. Web sites on which users interact through web phone and video-sharing sites are among the most popular on the web, and few existed just a couple of years ago. Considering how quickly these services became popular on the web, it makes sense to expect new services to change the way people work and play on the web.

The Architecture of the Internet

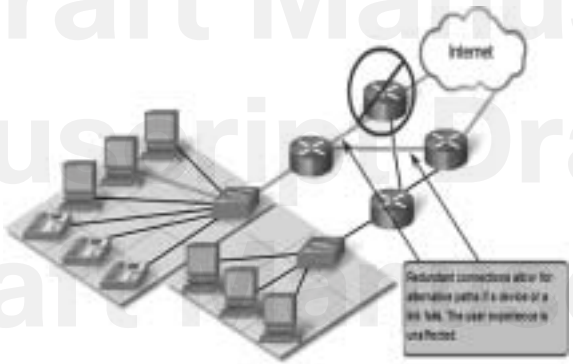
The term *network architecture* refers to the conceptual plans on which a physical network is built. Just as a building's architect must consider the function of the building and the expected needs of a building's users, so too must network architects design the Internet to accommodate the needs of the web and its users. The Internet has far exceeded the original expectations of size and use, which is a testament to how strong the foundations of the Internet were planned and implemented.

The Network Architecture

The Internet's design meets four fundamental expectations: fault tolerance, scalability, quality of service (QoS), and security. These topics are introduced here, and their implementation is discussed in the following section.

Fault tolerance, simply stated, means that the Internet will continue to function normally even when some of the components of the network fail. ***Redundancy***, or the duplication of equipment and media, is a key factor in fault tolerance. If a server fails, a redundant server performing the same functions should be able to pick up the work until repairs are made. If a data link fails on a fault-tolerant network, messages will be routed to the destination on a duplicate route. Figure 1-4 depicts a fault-tolerant network with a failed network router.

Figure 1-4 Fault Tolerance



Scalability describes the network's ability to grow and react to future changes. A scalable network can accept new users and equipment without having to start over on the design. As mentioned earlier, it is certain that changes in the ways networks are used will occur, and having an adaptable, or scalable, network will allow the insertion of new users without having to rebuild the entire network. A scalable network will be able to grow internally and externally, joining other networks to form an ***internetwork*** that can grow to keep pace with user demand.

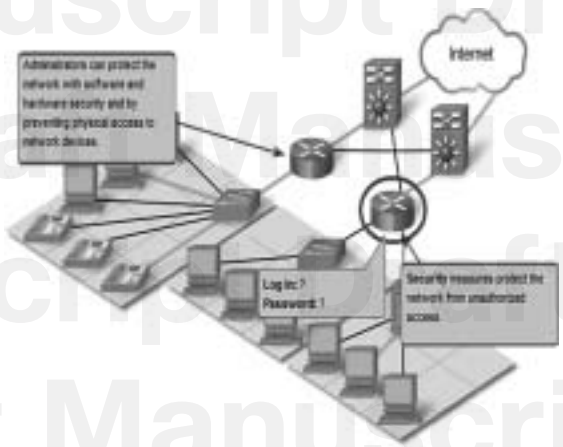
QoS indicates the performance level of services offered through the network. Services such as live video or voice can require more resources than services such as e-mail. Because many technologies are converged onto one platform, the separation of types of services on that platform can allow higher priority for one service over another. For example, a network administrator can determine that the data from attendees of a web meeting has priority over e-mail service. Configuring devices to prioritize types of data is an example of QoS.

Network security is essential if the public is to have confidence when using the Internet. People using the Internet to do business demand security for their financial transactions, and government and businesses that require personal information (for example, a hospital or doctor's office) must provide the protection of their clients' privacy. Just as citizens of a town expect safety and security, so does the community of web users. Without it, just like citizens of a town, the users will find another place to do business. Encrypted messages and the use of security devices at the gate of a local network are methods of implementing security.

Encryption and firewalls are not necessarily enough to protect a network, however. The security and privacy expectations that result from the use of internetworks to exchange confidential and business-critical information exceed what the current architecture can deliver. As a result, much effort is being devoted to this area of research and development. In the meantime, many tools and procedures are being implemented to combat inherent security flaws in the network architecture.

Figure 1-5 indicates how firewall settings on a router add security to network architecture by controlling network access.

Figure 1-5 Network Security



Fault-Tolerant Network Architecture

The architects of the Internet began their designs with fault tolerance as a high priority. The Internet came about when the United States Department of Defense (DoD) planners wanted to design a communication medium that could withstand widespread destruction of telephone and other communication infrastructure.

Circuit-Switched, Connection-Oriented Networks

The existing infrastructure at the time was a circuit-switched, connection-oriented network. Phone operators and primitive dial systems connected telephone calls by setting up a temporary circuit that was a physical connection on which the phone signal would travel from sender to receiver. The technology is connection oriented because any physical disconnect or service problem between the two users will drop the call. This would require initiating a new call and the provisioning of a new circuit.

The circuit-switched design provided new service to customers, but it had flaws as well. For example, only one phone call occupied each circuit, and no other calls could use the circuit until the previous call ended. This inefficiency limited the capacity of the phone system and made it expensive, especially for long-distance calls. From the DoD perspective, the system was vulnerable to easy disruption from enemy attacks.

Packet-Switched, Connectionless Networks

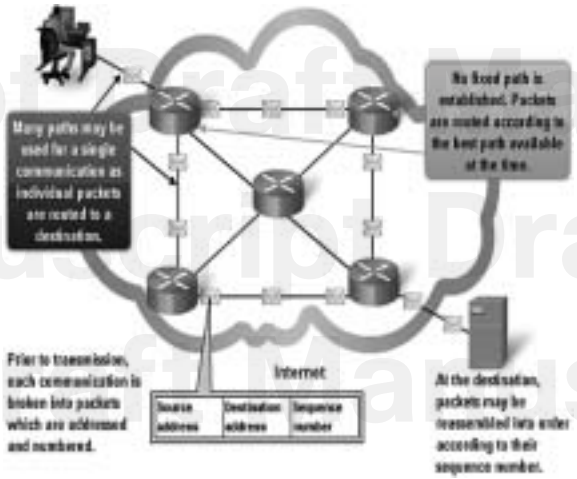
The answer to the fault tolerance issue was converting to a packet-switched, connectionless network. On a packet-switched network, a single message is broken into small blocks of data, known as ***packets***, which address information for the sender and the receiver. The packets then travel through one or more networks along various paths and reassemble at the destination.

The packets travel independently of each other and often take different routes to a destination. Messages are usually broken into thousands of packets, and it is common for some of them to be lost along the way. Protocols allow for this and contain methods for requesting retransmission of packets lost en route.

Packet-switched technology is connectionless because it does not require an active connection for the call to go through. This allows more efficiency than circuit-switched networks because multiple users can use network circuits simultaneously. Packet-switched technology is fault tolerant because it avoids the perils of relying on a single circuit for service reliability. If one network path fails, another network path can deliver the entire message.

Figure 1-6 depicts a packet-switched network with several alternative routes between the source and destination.

Figure 1-6 Packet-Switched Network



Packet-switched networks are the standard for the Internet, but a niche market remains for circuit-switched networks. Circuit-switched networks today allow circuit failure and session reestablishment, and some customers like the reliability and security that come from modern dedicated circuits. Circuit-switched connections are more expensive than packet-switched networks, but many institutions require the constant circuit availability and security and are willing to pay the extra price.

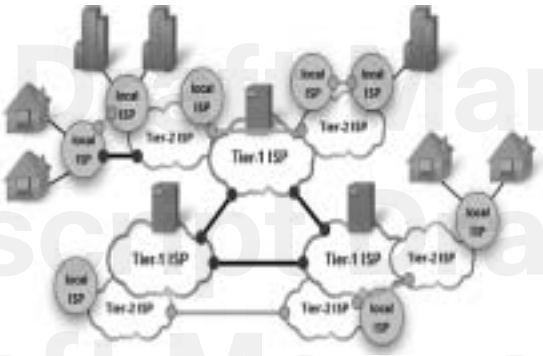
Scalable Network Architecture

A scalable network is able to grow without undergoing fundamental change at its core. The Internet is an example of scalable design. The Internet has grown exponentially in the last decade or so, and the core design is unchanged. The Internet is a collection of many private and public networks interconnected by routers.

Large tier-1 Internet service providers (ISP) house the largest domain servers that track Internet addresses. That information is replicated and shared in the lower tiers in the system. This hierarchical, multitiered design allows most traffic to be processed away from the upper-tier servers. This distribution of processing work means that changes made at the lower tiers, such as adding a new ISP, do not affect the upper levels.

Figure 1-7 demonstrates the hierarchical design of the web. Traffic between lower tiers can bypass the upper-tier servers in the Internet. This allows upper tiers to work more efficiently as well as to provide alternate paths for peak web traffic.

Figure 1-7 Hierarchical Internet



While the Internet is a collection of independently managed networks, the growth of the web is possible because of individual network managers adhering to standards that allow interconnectivity and scalability. The network managers must also be adaptable to new standards and protocols that enhance the usability of the Internet. Networks that do not adhere to standards can encounter communication problems when connecting to the Internet.

Providing Quality of Service

When the Internet first came into public use, people were amazed at the new tasks they could do and were tolerant of delays and dropped messages. Now, however, users have adapted to higher speeds and a greater ***quality of service (QoS)***.

QoS refers to the mechanisms that manage congested network traffic. Congestion is caused when the demand on the network resources exceeds the available capacity. There are some constraints on network resources that cannot be avoided. Constraints include technology limitations, costs, and the local availability of high-bandwidth service. Network ***bandwidth*** is the measure of the data-carrying capacity of the network. When simultaneous communications are attempted across the network, the demand for network bandwidth can exceed its availability. The obvious fix for this situation is to increase the amount of available bandwidth. But, because of the previously stated constraints, this is not always possible.

Using QoS, a manager can choose which traffic gets priority for processing in the network. For example, most people expect telephone service to be reliable and clear. Many companies want to save money by moving their long-distance phone calls onto the Internet using Voice over Internet Protocol (VoIP) services. If the users cannot distinguish any difference between regular phones and VoIP phones, they will not mind the change. But if network

congestion causes the VoIP phones to experience delays and dropped calls, users will return to the old expensive service. The network administrator must ensure that the quality of voice service is as high as possible, and she can do this by giving voice traffic priority over other web traffic.

Different companies and institutions have different needs and priorities. Some companies might prioritize voice traffic, others might want to give priority to video traffic, and still others might want to give priority to traffic carrying financial data. These various needs can be met by classifying network traffic and assigning priorities to each classification.

Classification of traffic means putting web traffic into categories. Because so many types of web traffic exist, assigning each its own priority is not practical. Thus, using one category for time-sensitive traffic such as voice and video and another category for less sensitive traffic like e-mail and document transfers is a way to sort traffic into manageable groups. Not every network will have the same priorities, and different institutions will assign data types into different categories according to their needs. After traffic types are categorized, they can be put into queues.

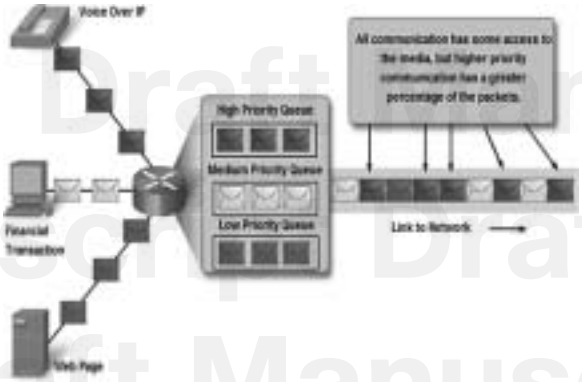
Examples of priority decisions for an organization might include

- **Time-sensitive communication:** Increase priority for services like telephony or video distribution.
- **Non-time-sensitive communication:** Decrease priority for web page retrieval or e-mail.
- **High importance to organization:** Increase priority for production control or business transaction data.
- **Undesirable communication:** Decrease priority or block unwanted activity, like peer-to-peer file sharing or live entertainment.

To get in a queue means to get into a line. An example of ***priority queuing*** can be found at an airport check-in counter. There are two classes of passengers in queues: a queue for coach passengers and a separate queue at the end of the counter for first class passengers. When airline agents become available, they will choose to help passengers from the first class queue ahead of someone who has been waiting longer in the coach class queue. The coach class passengers are still important and the agents will eventually help them, but the airlines give priority to first class passengers because they value the extra revenue those customers bring to the company.

In networking priority, queuing is much the same as the airline ticket counter process. Network managers assign priorities to traffic categories and allow the more important categories to have better access to the network's bandwidth. Figure 1-8 demonstrates different classes of traffic having different priority access to bandwidth.

Figure 1-8 Priority Queuing



Consider the earlier example of VoIP traffic at a company. If voice traffic has better access to company bandwidth than other traffic, the voice quality will be better and the users are more likely to be satisfied. Satisfied users will use the VoIP service and save the company money. Reduced costs and better service are the major incentives for network managers to provide QoS.

Providing Network Security

The Internet has proven to be fertile ground for business, and business-to-business transactions and e-commerce are sustaining significant growth every year. The same environment that attracts legitimate business, however, also attracts scam artists and vandals. Compromising the integrity of company assets could have serious business and financial repercussions. As a result, network security is a major concern of web providers and users, and web safety is a key part of any network management plan.

A network security breach can lead to a variety of serious consequences, including the following:

- Network outage, causing a loss of communication and business transactions
- Loss of personal or business funds
- Theft of intellectual property such as project bids, patents, and strategic plans
- Exposure of confidential customer data

Each of these examples could cause a customer to lose confidence in the company and hasten a move to a more reliable vendor. To provide security, a network manager must address two areas:

- Network infrastructure security
- Content security

Securing the network infrastructure means protecting the devices from outside contact. Locking computer room doors and using quality password protection on network equipment and software are simple steps that can go a long way to securing an infrastructure.

Securing network content means protection of data stored on network devices and the protection of packets carrying data into or out of the network. Content security on a network means ensuring confidentiality, maintaining communication integrity, and ensuring network availability.

Ensuring Confidentiality

Data privacy is maintained by allowing only the intended and authorized recipients—individuals, processes, or devices—to read the data. Different methods ensure data confidentiality. Having a strong system for user ***authentication***, enforcing passwords that are difficult to guess, and requiring users to change passwords frequently help restrict access to communications and to data stored on network-attached devices. Where appropriate, encrypting content ensures confidentiality and minimizes unauthorized disclosure or theft of information.

Maintaining Communication Integrity

Data integrity means having the assurance that the information has not been altered in transmission, from origin to destination. Data integrity can be compromised when information has been corrupted—willfully or accidentally—before the intended recipient receives it.

Source integrity is the assurance that the identity of the sender has been validated. Source integrity is compromised when a user or device fakes its identity and supplies incorrect information to a recipient.

Digital signatures, hashing algorithms, and checksum mechanisms provide source and data integrity across a network to prevent unauthorized modification of information.

Ensuring Availability

Making sure that resources are available to authorized users is an important part of a security plan. If a network is unavailable to a company using web-based business practices, the business can be slowed to a halt. Computer virus attacks and denial of service (DoS) attacks can bring a network down. A DoS attack occurs when outside computers flood a network

with so many requests for service that valid users cannot access the network resources. Tools to combat virus and DoS attacks include antivirus software on servers and desktops, and ***firewalls***, which are routers and servers that are network gatekeepers that analyze traffic entering and exiting a network. Building fully redundant network infrastructures, with few ***single points of failure*** that can bring the network down, can reduce the impact of these threats.

Fault tolerance, scalability, quality of service, and security are foundations on which to build a reliable and useful network. You will learn more about these in greater depth in this book and online course and in later courses.

Trends in Networking

Making precise predictions about the distant future of technology is a difficult task. Looking at current trends can show near-term developments that are on the horizon and the career opportunities that can be available to you.

Where Is It All Going?

The convergence of the many different communication media onto a single network platform is fueling exponential growth in network capabilities. Three major trends are contributing to the future shape of complex information networks:

- Increasing number of mobile users
- Proliferation of network-capable devices
- Expanding range of services

The following sections describe each trend and its possible impact.

Mobile Users

The trend of mobile use is contributing to changes in the traditional workplace from one where workers travel to a central office to one where the office travels with the worker. More mobile workers can use handheld devices such as cell phones, laptops, and personal digital assistants (PDA), which have evolved from luxury gadgets to necessary tools. Increased wireless service in metropolitan areas has unleashed people from their wired computers and freed them to work away from their desks.

Mobile workers and those who rely on handheld devices require more mobile connectivity to data networks. This demand has created a market for wireless services that have greater flexibility, coverage, and security.

New and More Capable Devices

The computer is only one of many devices on today's information networks. A proliferation of new technologies takes advantage of available network services.

Homes and small offices have access to services such as wireless technology and increased bandwidth that were once available only to corporate offices and educational institutions. Web-enabled phones give users access to Internet applications and e-mail anywhere in cell phone range.

The functions performed by cell phones, PDAs, organizers, and pagers are converging into single handheld devices with continuous connectivity to providers of services and content. These devices, once thought of as "toys" or luxury items, are now an integral part of how people communicate. In addition to mobile devices, we also have VoIP devices, gaming systems, and a large assortment of household and business gadgets that can connect and use network services.

Increased Availability of Services

The widespread acceptance of technology and the fast pace of innovation in network-delivered services create a spiraling dependence. To meet user demands, new services are introduced and older services are enhanced. As the users come to trust these expanded services, they want even more capabilities. The network then grows to support the increasing demand. People depend on the services provided over the network, and therefore depend on the availability and reliability of the underlying network infrastructure.

These highly mobile users and their increasingly capable devices require more complex services that are reliable and secure. As these improved tools and services become available to the public, the public demand for network bandwidth will increase as well.

These increases in demand point to growing networks and the new opportunities that will come with them. The challenge of keeping pace with an ever-expanding network of users and services is the responsibility of trained network and IT professionals.

Networking Career Opportunities

The implementation of new technologies is constantly changing the fields of information technology (IT). Network architects, information security managers, and e-commerce specialists are joining software engineers and database administrators in the IT workplace.

As non-IT fields, such as hospital management and education, become more technical in nature, the need for IT professionals with backgrounds in diverse fields such as medicine and education will increase.

Summary

Data networks play an increasing role in the way humans communicate with each other. The Internet and local networks directly impact the way people live, learn, and work.

The process for delivering messages across a computer network involves protocols defining agreements on how to deliver the message between user devices across a medium. The type of media and the devices used to deliver the message are subject to appropriate protocols as well.

Converged data networks can provide different types of services, including text, voice, and video messages between end users. Converged networks provide businesses with an opportunity to reduce costs and offer users a variety of services and content. However, the design and management of converged networks require extensive networking knowledge and skills if all services are to be delivered as expected to users.

A network's architecture must provide scalability, fault tolerance, quality of service, and security.

QoS is an important part of network planning that can affect user productivity. Prioritization of network data can allow an efficient balance of data types flowing through the network.

Security of network infrastructure and content will continue to be an essential element of a successful network, as it directly affects user confidence.

Labs

The labs available in the companion *Network Fundamentals, CCNA Exploration Labs and Study Guide* (ISBN 1-58713-203-6) provide hands-on practice with the following topics introduced in this chapter:

Lab 1-1: Networks Supporting the Way We Live (1.1.1.4)

Use satellite imagery available through the Internet to explore your world.

Lab 1-2: Providing Network Security (1.4.5.3)

Upon completion of this activity, you will be able to use the SANS website to quickly identify Internet security threats and explain how threats are organized.

Lab 1-3: Using Collaboration Tools—IRC and IM (1.6.1.1)

In this lab, you will define Internet Relay Chat (IRC) and Instant Messaging (IM). You will also list several misuses and data security issues involving IM.

Lab 1-4: Using Collaboration Tools—Wiki and Web Logs (1.6.2.1)

In this lab, you will define the terms *wiki* and *blog*. You will also explain the purpose of a wiki and blog and understand how these technologies are used for collaboration.

Many of the hands-on labs include Packet Tracer companion activities, where you can use Packet Tracer to complete a simulation of the lab. Look for this icon in the *Network Fundamentals, CCNA Exploration Labs and Study Guide* (ISBN 1-58713-203-6) for hands-on labs that have Packet Tracer companion activities.

Check Your Understanding

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. The section "Check Your Understanding and Challenge Questions Answer Key" at the end of this chapter lists the answers.

1. Which form of communication is a real-time, text-based communication type used between two or more people who use mostly text to communicate?

   A. Weblogs
   B. Wikis
   C. Instant messaging
   D. Podcasting

2. Which type of network provides customers with limited access to corporate data such as inventory, parts lists, and orders?

   A. Intranet
   B. Extranet
   C. Internetwork
   D. Internet

3. _____ are collaborative web pages created and edited by users.

4. What prioritizes traffic and its characteristics to manage data?

   A. Network administration
   B. Network traffic
   C. QoS strategy
   D. Network evaluation

5. Rules that govern the process of network communication are called _____.

6. What network traffic processes must be in place for quality of service strategies to work correctly? (Choose two.)

   A. Traffic is classified based on quality of service requirements.
   B. Priorities are assigned to each classification of application data.
   C. Web traffic is always assigned to a high-priority queue for processing.
   D. Digital movies are always assigned to the high-priority queue for processing.
   E. E-mail traffic is always assigned to the low-priority queue.

7. Copper cables and fiber-optic cables are two types of network _____.

8. What are two components of network architecture? (Choose two.)

   A. People that comprise the human network
   B. Built-in growth potential
   C. Data transfer across the network
   D. Redundant technologies
   E. Corporations that operate and maintain the data network

9. Symbols that graphically represent network devices and media are called _____.

10. For which three reasons were circuit-switched, connection-oriented technologies rejected when the Internet was being developed? (Choose three.)

A. Circuit-switched technologies required that a single message be broken up into multiple message blocks that contain addressing information.

B. Early circuit-switched networks did not automatically establish alternative circuits in the event of circuit failure.

C. Circuit-switched technologies required that an open circuit between network endpoints be established even if data was not being actively transferred between locations.

D. The quality and consistency of messages transmitted across a connection-oriented, circuit-switched network cannot be guaranteed.

E. The establishment of simultaneous open circuits for fault tolerance is costly.

11. For which three reasons was a packet-switched, connectionless data communications technology used when developing the Internet? (Choose three.)

A. It can rapidly adapt to the loss of data transmission facilities.

B. It efficiently utilizes the network infrastructure to transfer data.

C. Data packets can travel multiple paths through the network simultaneously.

D. It allows billing of network use by the amount of time a connection is established.

E. It requires that a data circuit between the source and destination be established before data can be transferred.

12. A _____ is a device that helps direct messages between networks.

13. What is the role of QoS in a converged network?

A. Ensures that all traffic above available bandwidth levels is dropped

B. Establishes delivery priorities for different types of communication in a network

C. Determines precise priorities for all types of network communication

D. Allows unused bandwidth to be shared by other organizations within the network

14. Which term describes a common platform for diverse communication types?

A. Scalability

B. Convergence

C. Fault tolerance

D. Quality of service

15. Connectionless messages are broken into _____.

16. Which of the following pertains to network infrastructure security?

A. A competitor accesses sensitive information through an unsecured wireless network.
B. Builders accidentally cut a network cable while digging.
C. A disgruntled employee alters information in a customer database.
D. A secretary sends confidential information in a reply to an e-mail that falsely appears to come from her boss.

Challenge Questions and Activities

These questions require a deeper application of the concepts covered in this chapter. You can find the answers at the end of this chapter.

1. A worker is assigned to work on a project with another employee from a different city. During online meetings, there are periods of sketchy video and garbled voice communications. Which combination of the following conditions could cause this?

A. Poor scalability in network design
B. Poor security, allowing someone to download music and video files at work
C. Lack of redundant links to the firewall
D. Poor QoS

2. Which pair of terms describes a network communication in which a bank has 24-hour exclusive access to an ATM? (Choose one.)

A. Connectionless and packet-switched
B. Packet-switched and connection-oriented
C. Circuit-switched and connection-oriented
D. Circuit-switched and connectionless

Look for this icon in *Network Fundamentals, CCNA Exploration Labs and Study Guide* (ISBN 1-58713-203-6) for instructions on how to perform the Packet Tracer Skills Integration Challenge for this chapter.

To Learn More

To learn more about a milestone in the history of communications, read about Claude Shannon and his famous paper, "A Mathematical Theory of Communication."

Check Your Understanding and Challenge Questions Answer Key

Check Your Understanding

1. C. Instant messaging is the only answer that is both text-based and real-time.
2. B. An extranet provides as-needed access for external vendors and customers to a secure corporate network. An intranet is for internal users.
3. Wikis
4. C. Considering the importance of traffic flow when managing data is a function of a quality of service (QoS) strategy. Network administrators would evaluate the network traffic to determine a QoS strategy.
5. protocols
6. A, B. A quality of service strategy first classifies traffic based on requirements and then assigns priorities to the classifications as is needed by the owners of the network. The network administrator can give different priorities to e-mail, web traffic, and movies.
7. media
8. B, D. Two components of a network's architecture are scalability, which is planning for growth, and fault tolerance, which includes redundant links. The other answers describe either users of the network or the product of it (data transfer).
9. icons
10. B, C, and E. Circuit-switched networks did not automatically establish alternative circuits in the event of circuit failure and required that an open circuit between network endpoints be established, even if data was not being actively transferred between locations. Also, the establishment of simultaneous open circuits for fault tolerance is costly.
11. A, B, C. Packet-switched, connectionless data communications technology can rapidly adapt to the loss of data transmission facilities and efficiently utilizes the network infrastructure to transfer data, and data packets can travel multiple paths through the network simultaneously. D and E refer to connections being established, which is not the nature of connectionless data communications.

12. router

13. B. QoS establishes priorities for different communications. It is not required to rate all network communication, just to give priority to what is deemed important.

14. B. Convergence is combining different technologies, such as telephone, video, and text, on one network platform.

15. packets

16. B. Only the cut cable pertains to infrastructure security. The others refer to content security. The unsecured wireless network might be allowed in network plans, but care must be taken to keep sensitive information beyond its reach.

Challenge Questions and Activities

1. B, D. It is possible that music and video downloads could take too much bandwidth and processing, disrupting the conference. Better QoS would give the video session priority over the download and avoid disruption.

2. C. The connection is established and exclusive, so it is privately circuit switched. Circuit-switched connections are connection oriented.