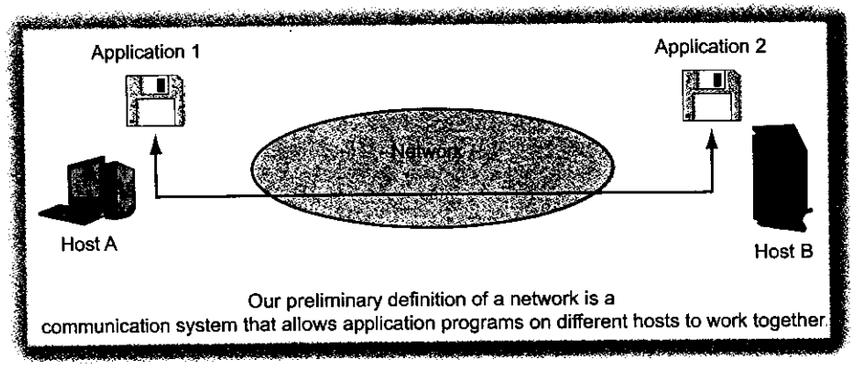


Figure 1-1 Black Box View of Networks

A Focus on Applications

Note that this definition focuses on *applications*. When you type the URL of a webserver into your browser, you don't care about how the Internet works—only that a webserver thousands of miles away can send you the information you need. To users, everything else is as exciting as plumbing.

We will spend most of our time in this course looking inside the *Network* bubble in Figure 1-1. As a networking professional, you will be on the team that keeps the bubble working invisibly to users. However, it is important to begin with your goal in mind. In networks, that means thinking about applications.

Hosts

Note that **host** is a general term for devices attached to a network. These devices can be large servers. They can also be small desktop PCs, notebooks, small personal digital assistants, and even cellular mobile telephones. In the future, even coffee makers[1] and many other small devices may be connected to the Internet.

TEST YOUR UNDERSTANDING

1. a) What is the book's preliminary definition of *network*? b) Why does the definition focus on applications? c) What is a host? d) Is your PC at home a host when you use it on a network? Explain. e) Is your mobile phone a host when you use it on a network? Explain.

[1]In fact, a protocol for controlling remote coffee pots has already been created. L. Masinter, *Hyper Text Coffee Pot Control Protocol (HTCPCP/1.0)*, RFC 2324 (informational), April 1, 1998. This is an informational request for comments, not a standards-track proposal. You should also note that the protocol was released on April 1—a date called April Fool's Day in many countries and celebrated as a time for playing jokes on people.

Networked Application Standards (Protocols)

Networked applications are applications that require networks to function. The most obvious example is the World Wide Web. Without the Internet, having a browser on your PC host would be useless.

> Networked applications are applications that require networks to function.

Network standards govern the exchange of messages between hardware or software processes on different hosts. Network standards are also called **protocols.**[2]

> Network standards, which are also called protocols, are sets of rules that govern the exchange of messages between hardware or software processes on different hosts.

If you want to call someone on the telephone, there have to be certain human behavioral protocols that govern the interactions. Most importantly, you both need to speak the same language. There are also subtle behavioral standards for turn-taking and other aspects of the conversation that you follow automatically through experience, but which would be rather complex to describe.

Human Protocols versus Network Protocols

Human communication protocols can be complex and ill-defined because people are intelligent and can cope with complexity, ambiguity, and speech errors. In contrast, computers are stupid (as you learned in your first programming course). Consequently, standards agencies must define network protocols very precisely and usually limit standards to a small number of commands and responses to commands.

HTTP Request-Response Cycle

The Hypertext Transfer Protocol (HTTP) that governs the World Wide Web is a very simple protocol at its core. As Figure 1-2 shows, the browser begins every HTTP interaction by sending an HTTP request message to the webserver application program. Typically, this message asks for a file. The webserver application sends back an HTTP response message, which delivers the file or gives an error code. This ends the HTTP **request–response cycle.**

In contrast to HTTP, many application standards, such as the Simple Mail Transfer Protocol (SMTP) standard for e-mail transmissions, typically require a dozen or more exchanges for a message transmission. Each exchange depends on previous exchanges in the session.

Client/Server Protocols

By the way, HTTP is called a **client/server** protocol because of the way its two application programs relate to each other. The browser is a client, in the sense that it receives services.

[2]Technically speaking, not all network standards are protocols. However, most network standards *are* protocols, and all of the standards in this book are protocols.

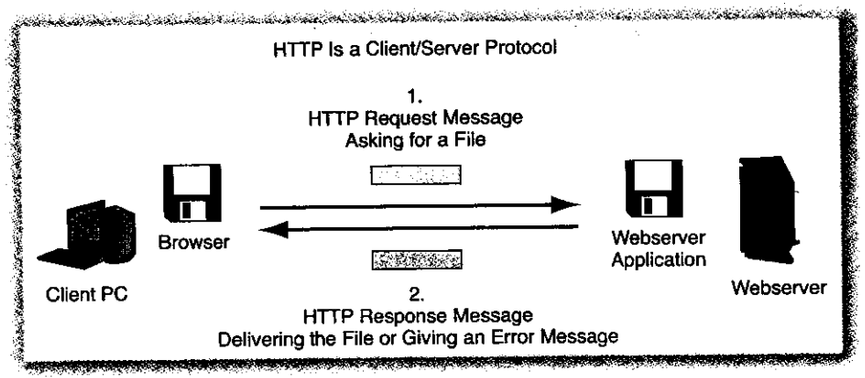


Figure 1-2 Hypertext Transfer Protocol (HTTP)

The webserver is a server because it provides service to clients. Most application program standards today are client/server protocols; but as we will see in Chapter 11, not all are.

> In client/server applications, the server program provides services to the client application program. For the WWW, the browser is the client and the webserver is the server.

Many Application Standards

Each application has a different standard. There are many applications, so there are many application protocols. In fact, there are more standards for applications than there are for any other aspect of networking.

Proprietary Standards and Open Standards

There are two types of standards. **Proprietary standards** are created by a vendor to connect the vendor's own products together. Although a vendor may allow other manufacturers to use its proprietary standards for free or upon payment of royalty fees, the vendors that create proprietary standards control these standards, leaving other vendors vulnerable to changes in sharing policies.

In contrast, **open standards** are created by international standards agencies that are not under the control of a vendor. With open standards, vendors can develop products secure in the knowledge that a single vendor will not arbitrarily change those standards.

Open standards allow competition among vendors. Competition tends to reduce prices. It also protects the firm in case its usual vendor goes out of business. In the longer term, it fosters the development of features as vendors struggle to differentiate themselves. These features often are standardized in later versions of the protocol. HTTP is an open standard.

It's All about Standards

Standards are fundamental to networking. In the next chapter, we will look at network standards in some depth, including how they are developed and how standards agencies create *standards architectures* to bring order to the dozens or hundreds of standards they produce. In the chapters following that, we will see many protocols. In Chapter 11, after we have looked at protocols below the standards layer, we will return to application standards.

TEST YOUR UNDERSTANDING

2. a) What is a networked application? b) What is the book's definition of a *network standard*? c) What is a protocol? d) Why must network protocols be specified very precisely? Give a detailed answer. e) What are client/server applications? f) Are there few or many application standards? Explain. g) Distinguish between proprietary and open standards. h) What are the benefits of open standards?

The ARPANET and the Internet

Around 1970, the U.S. **Defense Advanced Research Projects Agency** (**DARPA**) created the **ARPANET**[3] to connect the researchers it funded. This network was restricted to people working on DARPA contracts, although this rule was not tightly enforced. In any case, DARPA funded many computer science researchers, so the ARPANET itself became widely used in computer science.

During the 1970s, several other research networks emerged, such as CSNET, which was open to all computer scientists, and BITNET in the world of social science and business research.[4] In 1980, DARPA changed the ARPANET into the backbone of a new international internet (network of networks), the **Internet.** Later, in the 1990s, commercial networks were allowed to connect to the Internet, and the Internet as we know it today emerged.[5] The Internet is an almost entirely commercial venture. There is almost no government money still flowing in to run the Internet.

Figure 1-3 The ARPANET and the Internet (Study Figure)

ARPANET
- Created by the Defense Advanced Research Projects Agency (DARPA) around 1970

Soon, Many Other Networks Appeared
- Tower of Babel—no interconnection

DARPA Created the Internet in 1980 to Connect Networks Together
- Initially used only by researchers
- Became commercial in the 1990s
- Today, the Internet is commercial
- Almost no government money flowing in to run the Internet

[3] Why not DARPANET? In the early years, the agency was simply the Advanced Research Projects Agency of the Department of Defense.

[4] *BIT* stood for "Because it's time!" Business researchers and social sciences wanted in on the action.

[5] Actually, there was an intermediate step. In 1988, the National Science Foundation reengineered and took over the backbone, calling it NSFNET. NSFNET specifically prohibited commercial traffic. This led to the creation of commercial ISPs, which are discussed later in the chapter. In April 1995, NSFNET was retired and the commercial ISPs ran the Internet in the United States. Similar government-to-commercial enterprise transitions quickly took place in other countries.

File Transfer Protocol (FTP)

E-Mail

The World Wide Web (WWW)

The Internet versus the Web
- The Internet is the transmission infrastructure
- The WWW is one of many applications that use the Internet for transmission

E-Commerce
- Buying and selling on the Internet

Figure 1-4 Traditional Internet Applications (Study Figure)

Traditional Internet Applications

Although the Internet is attractive because it allows users to reach millions of other hosts, the Internet became massive in large part because of the applications it offered in its infancy and that it has added over the years.

File Transfer Protocol (FTP)

One initial purpose of the ARPANET was to allow researchers in different locations to transfer large files to each other. Consequently, the ARPANET offered the **file transfer protocol (FTP).** FTP could transfer large files even if there were errors or breaks in the transmission. In addition, FTP could run on any host on the ARPANET, regardless of the computer's operating system. FTP is still popular today.

E-Mail

Before the ARPANET, individual servers had e-mail that allowed users of a single server to send messages to each other. Shortly after the ARPANET emerged, Ray Tomlinson of BBN decided on his own initiative to extend these e-mail so that users could send e-mail to users on different servers. On individual servers, your e-mail address was your user name. Tomlinson realized that Internet e-mail would also have to specify the host name. Looking at his keyboard, he saw a little-used character. He used that character to express a user's e-mail address as *username@mailserver.* Tomlinson's unauthorized e-mail system was soon used everywhere, leading to its rapid standardization. It is difficult to find a business card today that does not have the person's e-mail address.

The World Wide Web (WWW)

The most popular application on the Internet today is the **World Wide Web (WWW),** which uses HTTP as its communication protocol. Using only your browser, you can get access to over a hundred million webservers around the world. On the Web, you can get news, search for information, and even watch repeats of your favorite television

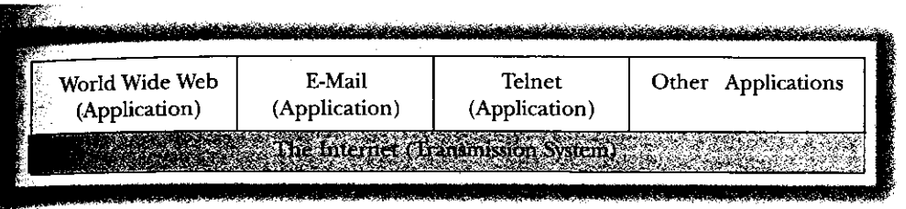


Figure 1-5 The Internet versus the World Wide Web (and other applications)

shows. While FTP and e-mail were born in the 1970 s, Tim Berners-Lee did not create the WWW until the early 1990 s. However, its growth since then has been explosive.

The Internet versus the World Wide Web

The 'Web is so popular that some people mistake it for the entire Internet. However, many other applications use the Internet. The Internet is a transmission system. It delivers the messages of all applications without prejudice or even awareness of the application message content. The Internet, then, has a transmission level that is universal and an application level that is particular to each application—WWW, Telnet, e-mail, and so forth.

E-Commerce

Initially, the 'Web was simply a system for delivering files to browsers. Soon, however, it became the basis for **e-commerce,** which is buying and selling over the Internet. As we will see in Chapter 11, e-commerce builds on top of the World Wide Web, adding the functionality needed to handle catalogs, purchasing by credit cards, access to multiple other servers to get the information to satisfy the order, and many other things.

TEST YOUR UNDERSTANDING

3. a) Distinguish between the ARPANET and the Internet. b) What is the purpose of FTP? c) How did ARPANET e-mail extend traditional server e-mail? d) Distinguish between the World Wide Web and HTTP. e) When did the World Wide Web appear? f) Distinguish between the World Wide Web and the Internet. g) Distinguish between e-mail and the Internet. h) How are WWW service and e-commerce service related?

Newer Internet Applications

While the World Wide Web, e-mail, and other traditional core applications are still very widely used, the Internet today also offers many newer applications, some of which are already used heavily.

Instant Messaging (IM)

It is difficult to find a college student's PC that does not have an active **instant messaging (IM)** window. People in the user's circle of friends can send messages at any time, leading to an exchange of text messages or even a voice conversation. IM users can also

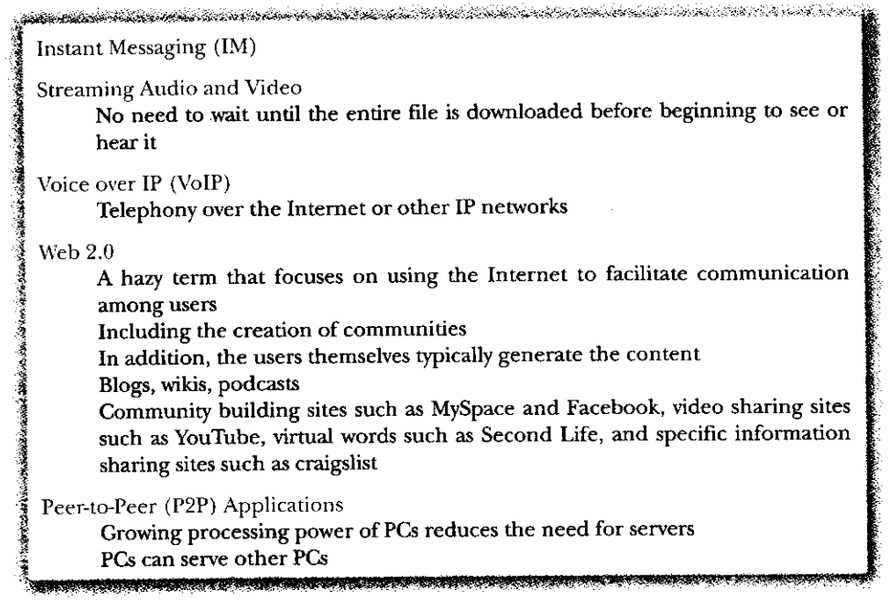


Figure 1-6 Newer Internet Applications (Study Figure)

transfer files to one another.[6] This real-time message delivery stands in stark contrast to e-mail, in which most people only check their mailboxes sporadically for new mail.

Streaming Audio and Video

Downloading audio and video to PCs is very popular today. If you just want to want to listen to a song or watch a rerun of a television show, waiting for an entire file to download before you can hear or see it is inconvenient. With **streaming media**, you do not have to wait for the entire file to be downloaded. After you download a few seconds of the file, you begin to hear it or see it on your system. As you listen to or see the file, more of it is downloaded in the background. The net result is that you hear or see the entire file with only a brief lag at the beginning. Streaming media have long been used in education and training on a limited basis. Now that many people are using streaming media applications, their use in education and training may increase.

Voice over IP (VoIP)

Another new popular application is **voice over IP (VoIP)**. Using a computer with multimedia hardware, users can place calls to people on the Internet and in some services to people on the traditional Public Switched Telephone Network (PSTN). Companies hope that VoIP can dramatically reduce the costs of long-distance and international telephone calling. As we will see in Chapter 6, many corporations are moving rapidly into VoIP for their corporate communication.

Web 2.0

The term **Web 2.0** was coined by O'Reilly Media in 2005. It is a fairly complex idea,[7] but one of its key elements is that users develop or enhance content, instead of the website owner controlling all of the content. Web 2.0 applications include blogs, wikis such as Wikipedia, podcasts, RSS feeds, social networking sites such as MySpace, video sharing sites such as YouTube, virtual worlds such as Second Life, and specific sharing sites such as craigslist.

> One characteristic of Web 2.0 is that users develop or enhance content, instead of the website owner controlling all of the content.

Peer-to-Peer (P2P) Applications

In client/server applications, the user PC receives service from a centralized server. Traditionally, this was necessary because user PCs were underpowered and had to depend on servers. However, most PCs today have far more hard disk space than they can use, as well as spare processing power (especially when they are not being used by their owners). Instead of relying on servers, PC users can now provide services to one other. These PC-to-PC applications are called **peer-to-peer (P2P)** applications.

P2P applications have something of a bad name because the first widely used P2P applications were created for illegal file downloading—first for music files and later for movies. However, corporations are beginning to see the legitimate potential of P2P applications. This includes legitimate corporate file sharing applications. It also includes shared processing power. For instance, many financial firms (which do heavy mathematical modeling) spread the processing load across their idle PCs to contain costs. The unused processing power, storage, and network connectivity of user PCs collectively has been called the dark matter of IT. It may very well be that most processing power and storage in firms lies on user PCs. P2P applications can exploit this underused resource to save corporations money by reducing the need to purchase expensive servers.

TEST YOUR UNDERSTANDING

4. a) Distinguish between e-mail and IM. b) Distinguish between the traditional downloading of complete media files and streaming media. c) What is the benefit of streaming media? d) Describe VoIP. e) What benefits do companies hope to get from VoIP? f) Users create or enhance website content in _____ applications. g) Distinguish between client/server applications and P2P applications. h) What benefit do corporations see in peer-to-peer applications?

Corporate Networked Applications

So far, we have been looking at applications that you probably use as a student and in your personal life outside school. However, corporations also have specific applications

[6] In many cases, users multitask by communicating by IM while doing other things, such as talking on the telephone. Many IM users feel that multitasking is NBD, but IMHO it is rude to IM while on the phone with someone else, and there is 411 to back that up. Quite simply, humans have limited attention, and TNSTAAFL. Yes, I know, WDALMIC?

[7] For more information, see Tim O'Reilly, "What is Web 2.0," September 30, 2005. http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html

Applications Specific to Businesses
- Can consume far more corporate network resources than traditional and new Internet applications combined

Transaction-Processing Applications
- High-volume repetitive clerical transaction applications
- Accounting, payroll, billing, etc.

Enterprise Resource Planning (ERP) Applications
- Serve individual business functions while providing integration between functional modules

Organizational Communication Applications
- E-mail, etc.
- Groupware
  - Integrate multiple types of communication, organize communication for retrieval, and provide multiple ways to disseminate and retrieve information

Converged Networks
- Voice and video have traditionally used different networks than data
- Convergence: Moving voice/video and data networks to a single network
- Can save the corporation a great deal of money by having only a single network
- Many technical issues remain

Figure 1-7 Corporate Network Applications (Study Figure)

that they need on both the Internet and on their internal networks. In most large organizations, these corporate network applications consume much more traffic than traditional and new Internet applications combined.

Transaction-Processing Applications

When corporate information systems began, the focus was on transaction-processing applications, which are clerical applications with high volumes of simple repetitive transactions, such as for payroll, billing, and accounts payable applications. Today, we call such applications **transaction-processing applications.** Although they are not exciting, they consume a good portion of a corporation's network resources and need to be addressed carefully in network planning. Poor network performance for transaction processing applications can be extremely costly to corporations in terms of lost productivity.

Enterprise Resource Planning (ERP) Applications

Originally, companies purchased "best of breed" transaction processing applications for individual business functions, such as payroll and inventory management. However, many corporate processes cut across functions, and if a corporation has selected applications on a function-by-functions basis, these applications probably will have a difficult time working together, if they can interoperate at all. Many firms now have or are beginning to install **enterprise resources planning (ERP)** applications that serve individual business functions while providing smooth integration between functional modules. These are also called **enterprise applications.**

Organizational Communication Applications

Organizations use e-mail and other traditional communication applications, but they also need more structured communication for project management and other disciplined processes. **Groupware** applications integrate multiple types of communication, organize communication for retrieval, and provide multiple ways to share information.

> Groupware applications integrate multiple types of communication, organize communication for retrieval, and provide multiple ways to share information.

Converged Voice/Data Networks

Most organizations today have two networks—one for voice and one for data. As we will see in Chapter 6, telephony traditionally has used very different technology than have data networks. However, the growth of VoIP has led to hope for **converged networks** that can serve both voice and data. Having only a single network should lower technology and management costs. However, voice and video have special needs which raise technical issues that have not been entirely solved.

TEST YOUR UNDERSTANDING

5. a) What are the characteristics of transaction processing applications? b) Why do companies purchase enterprise resource planning (ERP) applications? c) What are groupware applications? d) What is the potential benefit of voice/data convergence?

File Service

So far, we have looked at Internet applications and "big" corporate applications. However, there is another networked application that almost everyone uses in corporations: file service. As Figure 1-8 shows, **file service** is provided by a **file server;** in effect, it provides users with a shared hard drive that is accessible over a network.

> As Figure 1-8 shows, file service is provided by a file server; in effect, it provides users with a shared hard drive that is accessible over a network.

File Service for Data

On your PC's local hard drive, you store many data files—word-processing documents, spreadsheets, photographs, movies, and so forth. The figure shows that you can do the same thing on a file server. You are given a certain amount of space on the file server's hard drive, and file service manages your access to that space.

Backup Your file server's systems administrator (the person who manages the file server) probably backs up the file server every night. (In contrast, you probably back up your own hard drive once a lifetime). It is a good idea to copy files you work on to the file server. In fact, you might never want to store files on your local hard drive—but always store them on the file server.

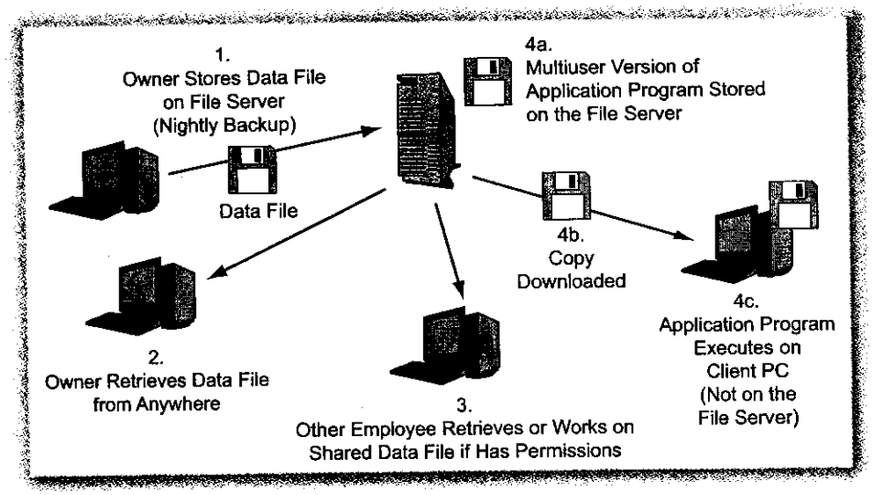


Figure 1-8 File Service

Access from Anywhere When you are away from your office, you may need some of your office files. Most file servers allow remote access so that you can retrieve your files anywhere there is a network connection.

Sharing with Security If you wish, you can allow other people to share some or all of your files. While you might be reluctant to do so for your main files, the systems administrator can set up directories for specific purposes, such as projects. You can then decide who may and who may not access that directory. You can also limit what authorized users can do in the directory. In some cases, you will want to give others read-only access so that they can only read files and cannot create new files, delete files, modify files, or take other actions. In other cases, you will allow them to take actions beyond mere reading.

File Service for Programs

Programs are merely files or collections of files, so you can store them on a file server.

Multiuser Software: Install Once In fact, you can purchase a multiuser copy of a program and install it once on a file server, instead of having to install a copy on each PC individually. (Of course, multiuser copies are more expensive than the normal single-user copies sold in stores.) The labor savings from not doing multiple PC installations is substantial.

Execution on the Client PC On your PC, when you execute a program saved on your local hard drive, that program is copied into RAM for execution. A file server, again, is like a remote hard drive. When you run a program stored on a file server, the file server sends your PC a copy of the program, and your PC stores it in RAM for execution.

This surprises many people. They assume that, because the file server is usually a more powerful computer than your desktop PC, the file server will do the "heavy work" of executing programs. Instead, your "little" PC has to do the processing. If this seems strange, remember that a file server is only a remote disk drive.

TEST YOUR UNDERSTANDING

6. a) To what PC component does a file server correspond? b) What are the three advantages of file service for data files? c) What is the advantage of storing multiuser versions of programs on a file server? d) When you run a program that is stored on a file server, where does the program execute—on the file server or on your PC?

Hints for Readers

KEYWORDS

Words shown in boldface are **keywords.** You will see a keyword printed in boldface on the page where the keyword is first defined or at least characterized. Pages where this occurs are numbered in boldface in the book's Index. When you look for a term in the Index, you should go to the boldface page number first. You can also go to the book's Glossary to get a definition of a keyword. There is a searchable version of the Glossary on the book's website.

KEY POINTS

In some cases, key points are set centered on the page, in smaller print, and with paragraph borders, as shown below. These are important points that you should stress when you study.

Points shown this way are important points that you should stress when you study.

TEST YOUR UNDERSTANDING QUESTIONS

At the end of many subsections, there are Test Your Understanding questions. Students who do the best in courses typically stop when they encounter Test Your Understanding questions and answer them before going on. In networking, concepts build on one another. If you understand each section as you go, you will be much more effective when you study later sections.

BOXES: ADVANCED MATERIAL

This material is being presented in a box. In this case, and in some other cases, the boxed material is designed to give you perspective or guidance. In most cases, however, the boxes contain advanced material. You can get a good understanding of each chapter without the advanced information in boxes, but the boxed material will give you a better understanding.

FOOTNOTES

This book uses footnotes to provide references or to provide explanations that are beyond the scope of the book, but that some readers may find interesting. None of the questions in the book's test bank asks about material in footnotes, but your instructor may include the material in footnotes in some of his or her own test questions.

Quality of Service (QoS)
    Indicators of network performance

Metrics
    Ways of measuring specific network quality-of-service variables

Figure 1-9 Network Quality of Service (QoS)

NETWORK QUALITY OF SERVICE (QoS)

In the early days of the ARPANET and the Internet, networked applications amazed new users. However, these users soon said, "Too bad this thing doesn't work better." Today, though, networking is a mission-critical service for corporations. If the network breaks down, much of the organization comes to a halt. Today, networks must work, and they must work *well.* Companies are concerned with network **quality-of-service (QoS)** measures, that is, indicators of network performance. Companies typically use a number of QoS **metrics** (measures) to quantify their quality of service so that they can set targets and determine whether they have met those targets.

TEST YOUR UNDERSTANDING

7. a) What are QoS measures? (Do not just spell out the acronym.) b) How are QoS metrics used?

Transmission Speed

There are many ways to measure how well a network is working. The most fundamental metric is speed. Just as the first question people ask about a newborn baby is whether it is a boy or a girl, the first thing that people ask when they encounter a new network is, "How fast is it?"

Bits per Second (bps)

Transmission speed[8] normally is measured in **bits per second (bps).** A **bit** is either a one or a zero. Obviously, a single bit cannot convey much information. Speeds today range from thousands of bits per second to trillions of bits per second. To simplify the writing of transmission speeds, professionals add metric prefixes to the base unit, bps. For example, Figrue 1-10 shows that in increasing factors of 1000 (not 1024 as with computer memory), we have **kilobits per second (kbps), megabits per second (Mbps), gigabits per second (Gbps),** and **terabits per second (Tbps).**

Speeds are measured in factors of 1000, not 1024.

[8]Purists correctly point out that *speed* is the wrong word to use to describe transmission rates. At faster transmission rates, bits do not physically travel faster. The sender merely transmits more bits in each second. Transmission rates are like talking faster, not running faster. However, transmission rates are called transmission speeds almost universally, so we will follow that practice in this book.

Speed
    Normally measured in bits per second (bps) *not* bytes per second
        Metric suffixed in increasing units of 1,000 (not 1,024)
        The metric abbreviation for kilo is lower-case k

1 kbps	1,000 bps	kilobits per second
1 Mbps	1,000 kbps	megabits per second
1 Gbps	1,000 Mbps	gigabits per second
1 Tbps	1,000 Gbps	terabits per second

    Sometimes, speed is measured in bytes per second, Bps, compared with bps
        Bps usually is seen only in file transfers

Expressing Speed in Proper Notation

As Written	Places before Decimal Point	Properly Written
23.72 Mbps	2	23.72 Mbps
2,300 Mbps	4	2.3 Gbps
0.5 Mbps	0 (leading zeros do not count)	500 kbps

There must be one to three spaces before the decimal point
    Leading zeros do not count
There must be a space between the number and the units
    12 Mbps is proper; 12Mbps is improper
If the number is decreased by 1,000 (4523 becomes 4.523), then the suffix must be increased by 1,000 (Mbps to Gbps)
    4,523 Mbps becomes 4.523 Gbps
If the number is increased by 1,000 (0.45 becomes 450), then the suffix must be decreased by 1,000 (Mbps to kbps)
    0.45 Mbps becomes 450 kbps

Rated Speed and Throughput
    Rated Speed
        The speed a system should achieve according to vendor claims or to the standard that defines the technology
    Throughput
        The data transmission speed a system actually provides to users
    Aggregate versus Rated Throughput on Shared Lines
        The aggregate throughput is the total throughput available to all users
        The individual throughput is an individual's share of the aggregate throughput

Figure 1-10 Transmission Speed (Study Figure)

Note that, consistent with metric notation, kilo is abbreviated as lower-case k instead of upper-case K. (In the metric system, K is the metric abbreviation for Kelvins, a measure of temperature.) Computer scientists often write K, but this is because they do not know the metric system. Networking people are smarter.

Bytes per Second

Although transmission speed is almost always measured in bits per second, it is occasionally measured in **bytes per second.** (A byte is eight bits.) While *bits per second* is written as bps, *bytes per second* is written as **Bps.** About the only time you will see Bps is in file transfers because file sizes normally are measured in bytes.

Writing Numbers in Proper Notation

The basic rule for writing speeds (and metric numbers in general) in proper notation is that there should be one to three places before the decimal point and that there should be a space between the number and the units. Figure 1-10 illustrates how to write speeds properly.

To write a speed in proper notation, there should be one to three places before the decimal point, and there should be a space between the number and the units.

- ➤ Given this rule, 23.72 Mbps is fine (two places before the decimal point).
- ➤ However, 2300 Mbps has four places before the decimal point (2300.00), so it should be rewritten as 2.3 Gbps (one place before the decimal point).
- ➤ Also, 0.5 Mbps has zero places to the left of the decimal point. (Leading zeros do not count.) It should be written as 500 kbps (three places).

Note also that there must be a space between the numerical prefix (23.72, etc.) and its metric suffix (Mbps, etc.). So 23.72 Mbps is proper, but 23.72Mbps is improper.

Suppose you have the speed 4,523 kbps. To get the number (4,523) right, you divide it by 1,000 to get 4.523. If you *divide the number* by 1,000, then you must *multiply the suffix* (kbps) by 1,000 to get Mbps. In proper notation, then, the number is 4.523 Mbps.

To give another example, suppose you have 0.45 Mbps. You need to *multiply the number* (0.45) by 1,000, getting 450. You then have to *divide the suffix* (Mbps) by 1,000 to give you kbps. The number in proper notation, then, is 450 kbps.

Rated Speed versus Throughput

Talking about transmission speed can be tricky. A network's **rated speed** is the speed it *should* achieve according to vendor claims or to the standard that defines the technology. For a number of reasons, networks often fail to deliver data at their rated speeds. In contrast to rated speed, a network's **throughput** is the data transmission speed that the network *actually* provides to users.

Note: Some students find the distinction between rated speed and throughput difficult to learn. However, we must use this distinction throughout the book, so be sure to take the time to understand it.

Network Demand, Budgets, and Decisions (see Figure 1-12)
- Network demand is growing explosively, while network budgets are growing slowly
- This creates a cost squeeze that affects every decision
- Overspending in one area will result in the inability to fund other projects

Systems Development Life Cycle Costs
- Hardware: Full price: base price and necessary options
- Software: Full price: base price and necessary options
- Labor costs: Networking staff and user costs
- Outsourcing development costs
- Total development investment

Systems Life Cycle (SLC) Costs
- System development life cycle versus system life cycle
- Total cost of ownership (TCO)
  - Total cost over entire life cycle
  - SDLC costs plus carrier costs
    - Carrier pricing is complex and difficult to analyze
    - Must deal with leases

Figure 1-11 Cost (Study Figure)

Throughput is the data transmission speed that a network **actually** provides to users.

Aggregate versus Individual Throughput

When a transmission line on a network is **multiplexed,** this means that several conversations between users will share the line's throughput. Consequently, it is important to distinguish between a line's **aggregate throughput,** which is the total it provides to all users who share it, and the **individual throughput** that single users receive as their shares of the aggregate throughput. As you learned as a child, sharing is theoretically good, but it means that you get less.

TEST YOUR UNDERSTANDING

8. a) In what units is transmission speed normally measured? b) Is speed normally measured in bits per second or bytes per second? c) Give the names and abbreviations for speeds in increasing factors of 1000. d) What is 55,000,000,000 bits per second with a metric suffix? e) Write out 100 kbps in bits per second (without a metric suffix). f) Write the following speeds properly: 0.067 Mbps, 23,000 kbps, 45.62 Gbps, and 13kbps.
9. a) Distinguish between rated speed and throughput. b) Distinguish between individual and aggregate throughput.

Cost

Network Demand, Budgets, and Decisions

Although speed is important, so is cost. Most of us would like to drive Ferraris. Few of us need a high-performance car, however, and fewer could afford one.

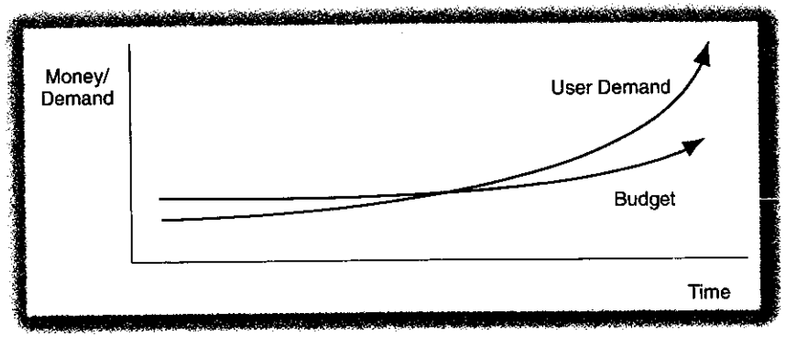


Figure 1-12 Network Demand and Budget

Figure 1-12 shows how demand and budget for network services are increasing over time. Demand, of course, is growing very rapidly. Everybody wants network applications and high-speed service. However, network budgets generally are growing slowly, if they are growing at all.

This creates a cost squeeze that governs every aspect of network management thinking. Network managers need to limit what they do and purchase only what they need. Overspending on one project will leave managers unable to do another project. In addition, corporations are requiring strong justification for new services and existing services alike.

In this book, you will encounter many questions asking you to compare alternative technologies that could be used to serve a need. In general, an answer to such a question will be wrong if it omits relative costs.

Systems Development Life Cycle (SDLC) Costs

You are undoubtedly familiar with the systems development life cycle (SDLC). When you begin a project, you need to consider the cost of the system during its development.

Hardware Costs Consider what happens when you buy a personal computer. You first have to take hardware into account. When you look at the price of a computer, this may not include a display, and it usually does not include a printer. The **base price** is the price before adding components that will be needed in actual practice. In contrast, the **full price** of the hardware is the price of a complete working system. The distinction between base price and full price is also applicable to network hardware, including the switches and routers we will see later in this chapter.

Software Costs After your first computer purchase, you realize that the software can be almost as expensive as the hardware. You have to consider the software you will need very carefully and understand the cost of that software. Individual software products, furthermore, often have misleading base prices that do not include all necessary components. Network product software decisions are similarly complex.

Labor Costs in Development Although hardware and software costs are complex and difficult to measure, these problems pale before the problems involved in estimating labor costs in development. Planning, procurement, installation, configuration, testing, programming, and other labor costs can easily exceed hardware and software costs.

User costs should also be considered because the time that users spend on the system's development during requirements definition and later development states is substantial and is not free to the company, any more than network staff time is free.

Outsourcing Development Costs If the company outsources some or all of the development costs, then outsourcing costs need to be considered in the overall picture.

Total Development Investment To evaluate potential projects, the networking staff must forecast the total development investment—the total of hardware, software, and labor costs during development. These expenditures truly are investments that should pay off over the life of the project.

Systems Life Cycle (SLC) Costs

The preoccupation of information systems professionals with the systems development life cycle has always puzzled networking professionals, who note that most costs come *after* the SDLC has finished. Training IS (information system) students in SDLC costs, but not in operational work and costs afterward, is like training doctors only in obstetrics and ignoring care after birth.

It is important to consider **system lifecycle costs,** which are costs over a system's entire life—not just during the systems development period. The cost of a system over the entire life cycle is called the **total cost of ownership (TCO).**

Operating and management costs usually are very important over the system life cycle. When making equipment and software purchases, it is important to consider how much labor is involved in operating and managing the equipment and software. These costs must be considered very carefully in product selection.

One new factor in systems life cycle analysis is carrier costs. If you must deal with a communications carrier to carry your signals from one corporate site to another, then you also have to consider carrier pricing. This is rarely easy to do, and it is even harder to compare the prices of alternative carriers offering roughly the same service, because of the wording in their contracts. In addition, you usually have to sign equipment leases or service agreements that lock you in for various periods of time, sometimes up to several years.

TEST YOUR UNDERSTANDING

10. a) Compare network demand trends and network budget trends. b) What are the implications of these trends? c) What period of a network's life does the SDLC cover? d) Why are hardware and software base prices often misleading? e) List the four categories of SDLC costs. f) Why must user costs be considered?

11. a) Distinguish between the systems development life cycle and the system life cycle. b) What is the total cost of ownership (TCO)? c) Why should operating and management costs be considered, in addition to hardware, software, and transmission costs, in purchasing decisions? d) What additional cost factor comes into SLC costs, compared with SDLC costs? e) Why must carrier contracts be entered into carefully?

Other Quality-of-Service Metrics

Availability

Although speed and cost are fundamental, there are several other important measures for how a network is working. One of these is metrics is **availability,** which is the percentage of time that the network is available for use. In contrast, **downtime** is the percentage of time that the network is not available.

Ideally, systems would be available 100% of the time, but that is impossible in reality. On the Public Switched Telephone Network, the availability target usually is 99.999%. This is known as the "five nines." Data networks generally have lower availability, but are under pressure to improve their availability, given the cost of network downtime to firms today.[9]

Figure 1-13 Other Quality-of-Service Metrics (Study Figure)

- Speed
- Cost
- Availability
  - The percentage of time a network is available for use
  - Downtime is the amount of time a network is unavailable (minutes, hours, days, etc.)
- Error Rates
  - Packet error rate: the percentage of packets lost or damaged
  - Bit error rate: the percentage of bits lost or damaged
- Latency and Jitter
  - Latency
    - Delay, measured in milliseconds
  - Jitter
    - Variation in latency between successive packets
    - Makes voice sound jittery
- Service Level Agreements
  - Guarantees for performance
  - Penalties if the network does not meet its service metrics guarantees
  - Guarantees specify worst cases (no worse than)
    - Lowest speed (e.g., no worse than 1 Mbps)
    - Maximum latency (e.g., no more than 125 ms)
  - Often written on a percentage basis
    - No worse than 100 Mbps 99.5% of the time

Error Rates

We will see later in this chapter that hosts send data in small messages called packets. Ideally, all packets would arrive intact, but this does not always happen. The **packet error rate** is the percentage of packets that are lost or damaged during delivery. The **bit error rate,** in turn, is the percentage of bits that are lost or damaged.

Most networks today have very low average error rates. However, when network traffic is very high, error rates can soar because the network has to drop the packets it cannot handle. Companies must measure error rates when traffic levels are high in order to have a good understanding of error rate risks.

Latency and Jitter

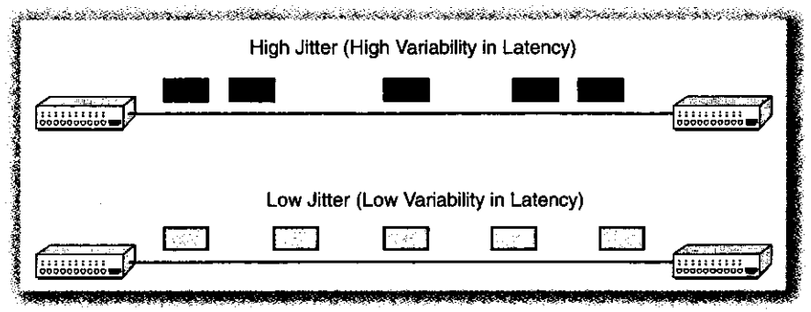
When packets move through the network, they will encounter some delays. The amount of delay is called **latency.** Latency is measured in **milliseconds (ms).** A millisecond is a thousandth of a second. When latency reaches about 125 milliseconds, turn-taking in telephone conversations becomes difficult.

A related concept is **jitter,** which Figure 1-14 illustrates. Jitter occurs when the latency between successive packets varies. Some packets will come too far apart in time, others too close in time. While jitter does not bother most applications, VoIP and streaming media are highly sensitive to jitter. If the sound is played back without adjustment, it will speed up or slow down hundreds of times per second. These speed changes make voice sound jittery.

Service Level Agreements

When you buy some products, you receive a guarantee promising that they will work and specifying penalties if they do not work. In networks, service providers often

Figure 1-14 Jitter



[9]On a more detailed basis, availability can be discussed in terms of the mean time to failure (MTTF) and the mean time to repair (MTTR). The former asks how frequently downtime occurs. The latter asks how long service is down after a failure begins. Frequent short failures may be preferable to infrequent, but very long, outages.

provide **service level agreements (SLAs),** which are contracts that guarantee levels of performance for various metrics such as speed and availability. If a service does not meet its SLA guarantees, the service provider must pay a **penalty** to its customers.

SLAs guarantees are expressed as *worst cases.* An SLA might guarantee that speed will be *no lower* than a certain amount, that the latency will be *no higher* than a certain value, and so forth.

SLAs guarantees are expressed as **worst cases.**

In addition, SLAs have percentage-of-time elements. For instance, an SLA on speed might guarantee a speed of at least 480 Mbps 99.9% of the time. This means that the speed will nearly always be at least 480 Mbps, but may be slower 0.1% of the time without incurring penalties.

TEST YOUR UNDERSTANDING

12. a) What is availability? b) What is downtime? c) What are the "five nines"? d) Does corporate network availability usually meet the five nines expectation of the telephone network? e) What are packets? f) Distinguish between the packet error rate and the bit error rate. g) When should error rates be measured? Why? h) What is latency? i) In what units is latency measured? j) What is jitter? k) For what applications is jitter a problem?

13. a) What are service level agreements? b) Does an SLA measure the best case or the worst case? c) Would an SLA measure the highest latency or the lowest latency? d) Would an SLA guarantee a lowest availability or a highest availability? e) What happens if a carrier does not meet its SLA guarantee? f) If carrier speed falls below its guaranteed speed in an SLA, under what circumstances will the carrier *not* have to pay a penalty to the customers?

SECURITY

In addition to network quality of service, corporations today are extremely concerned with network security. Attacks by external and internal adversaries can be extremely expensive for corporations. We will look at network security in depth in Chapter 9. For now, however, we will discuss a few security concepts that we will see in this book before we reach Chapter 9.

Authentication

In a famous Peter Steiner cartoon in *The New Yorker,* a dog is sitting at a computer keyboard. The dog brags to another dog in the room: "On the Internet, nobody knows you're a dog."[10] In a network, a host cannot see the user trying to log into it. To **authenticate** the user—that is, have the user prove his or her identity—the server needs proof of identity, most commonly, a password.

In general, a person trying to establish his or her identity is called the **supplicant,** and the device attempting to authenticate the user is called the **verifier.** The supplicant sends **credentials** (proofs of identity) to the verifier, and the verifier checks these credentials. If authentication is done well, impostors will not be able to pose as legitimate users.

[10] *The New Yorker,* vol. LXIX, no. 20, July 5, 1993, p. 61.

Security
- Attacks can be extremely expensive
- Companies need to install defenses against attacks
- Chapter 9 discusses network security in depth

Authentication
- Supplicant attempts to prove its identity to a verifier
- Example: user logging into a server is a supplicant; the server is a verifier
- Proofs of identity are called credentials
- If authentication is done well, impostors will not be able to pose as legitimate users.

Cryptographic Protections
- Eavesdroppers may intercept your messages
  - Read and even change messages
  - Send new messages impersonating the other side
- Cryptography is the use of mathematics to protect information in storage or in transit
  - Also when in storage
- Encryption for confidentiality
  - An eavesdropper cannot read encrypted messages
  - Legitimate receiver, however, can decrypt the message

Firewalls
- Examines each passing packet
- Drops and logs provable attack packets
- It lets other packets get through

Host Hardening
- Some attacks will inevitably get past safeguards and reach hosts
- Hosts must be hardened to withstand attacks
- Hardening is a set of protections we will see in Chapter 9
  - Example: installing antivirus software on the host
  - Example: downloading security updates

Figure 1-15 Network Security (Study Figure)

Cryptographic Protections

When you transmit packets, there is a danger that an eavesdropper will intercept them. The eavesdropper will then be able to read your sensitive information and even change packets to send false information to the receiver. The interceptor will also be able to send new messages in your name. To address these threats, network planners turn to **cryptography,** which is the use of mathematics to protect information in storage or in transit.

Cryptography is the use of mathematics to protect information in storage or in transit.

The most obvious cryptographic protection is **encryption for confidentiality.** Encryption for confidentiality effectively scrambles messages so that interceptors cannot read them. The legitimate receiver, of course, can **decrypt** messages and read them.

Firewalls

Another security tool is the firewall. A **firewall** examines each packet passing through it. If a packet is a **provable attack packet,** the firewall drops and logs the packet. Otherwise, it lets the packet through.

Host Hardening

Although firewalls will stop most attacks, some attack packets will inevitably get through to clients and servers. In Chapter 9, we will see a number of ways to **harden** hosts so that they can withstand attacks. An obvious example of host hardening is installing antivirus software on desktop and notebook PCs. Another example is downloading security updates for software running on the host.

TEST YOUR UNDERSTANDING

14. a) What is authentication? b) Why is authentication needed? c) Describe these authentication terms: supplicant, verifier, and credentials. d) What is cryptography? e) What does confidentiality mean in transmission? f) What do firewalls do? g) What types of packets do firewalls drop? (Be very specific.) h) Why is host hardening necessary?

SWITCHED NETWORKS

Now that we have looked at networked applications and quality-of-service metrics, we can finally begin to look at how networks do their jobs. We will look first at simple *switched* networks and then at more complex *routed* networks, which are also called internets.

Ethernet Switching with a Single Switch

There are several switched network technologies. We will focus on Ethernet switching, which most corporations use for networking within their buildings. In the smallest Ethernet networks, all host computers connect to a single Ethernet switch, which handles the transmission of messages between hosts. Figure 1-16 shows one of these small Ethernet networks.

A switch has multiple **ports** (connection points for transmission lines). The company must make a switching decision when a frame comes into one port. The decision is what port to use to send the frame back out. How does it make this **switching decision**? The answer is that it uses the destination address that must appear in each message.

In Ethernet, each host has a unique **Ethernet address,** which looks something like C3–2D–55–3B-A9–4F.[11] (We will look at Ethernet addresses more closely in Chapter 4.) When a source host sends an Ethernet message, the message has a destination Ethernet address, which specifies the Ethernet address of the destination host. This is like the address on a postal envelope.

When the switch receives a message, the switch looks at the destination address. In this example, the destination Ethernet address is C3–2D–55–3B-A9–4F. As the figure shows, the switch has a switching table that tells the switch what port to use to send the frame back out. For C3–2D–55–3B-A9–4F, the associated port is port 15. The switch sends the frame out through that port, to the destination host.

[11] As we will see in Chapter 4, Ethernet addresses are also called MAC addresses and, sometimes, physical addresses.

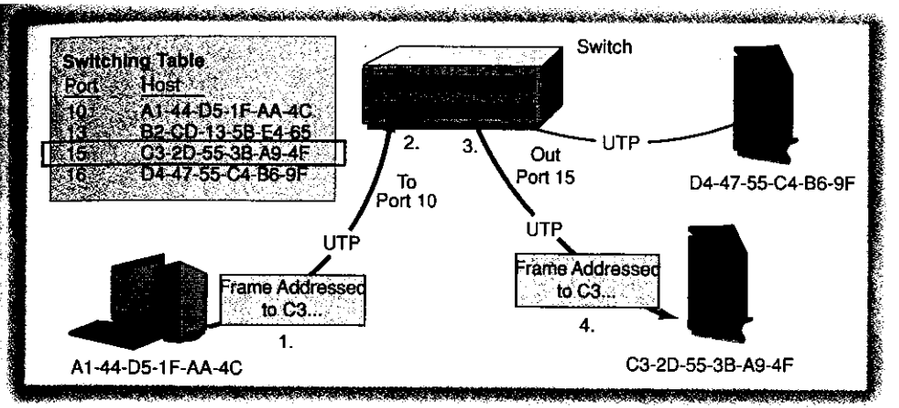


Figure 1-16 Ethernet Switching

TEST YOUR UNDERSTANDING

15 a) On a switch, what is a port? b) What is a switching decision? c) On what do Ethernet switches base switching decisions? d) What does an Ethernet switch do after it reads the destination Ethernet address in an arriving frame?

Workgroup Switches and Core Switches

In all but the smallest Ethernet networks, there are multiple Ethernet switches. Each switch sends a message closer to its final destination. Think of a railroad boxcar that passes through several switching yards along the way to its destination. Boxcars are analogous to messages, and rail yards are analogous to switches.

Figure 1-17 shows a switched network in a multistory building. The figure shows a workgroup switch on each floor. A **workgroup switch** is one that connects PCs and servers to the network. There is a core switch down in the basement equipment room. **Core switches** connect switches to other switches and to other devices (called routers) that we will see later in this chapter.

- When the wired client on Floor 1 transmits a message to the server on Floor 2, the client sends the message to the workgroup switch on its floor.
- That workgroup switch realizes that it cannot deliver the message directly to a computer attached to it. The workgroup switch then forwards the message to the core switch in the basement equipment room.
- The core switch sends the message to the workgroup switch on Floor 2.
- The workgroup switch sends the message on to the server.

TEST YOUR UNDERSTANDING

16. a) Distinguish between core and workgroup switches. b) In Figure 1-17, how many workgroup switches are there? c) How many core switches? d) Suppose that there is a server connected to Workgroup Switch 1. Through what switches will messages travel if they are sent by the wireless client on that floor?

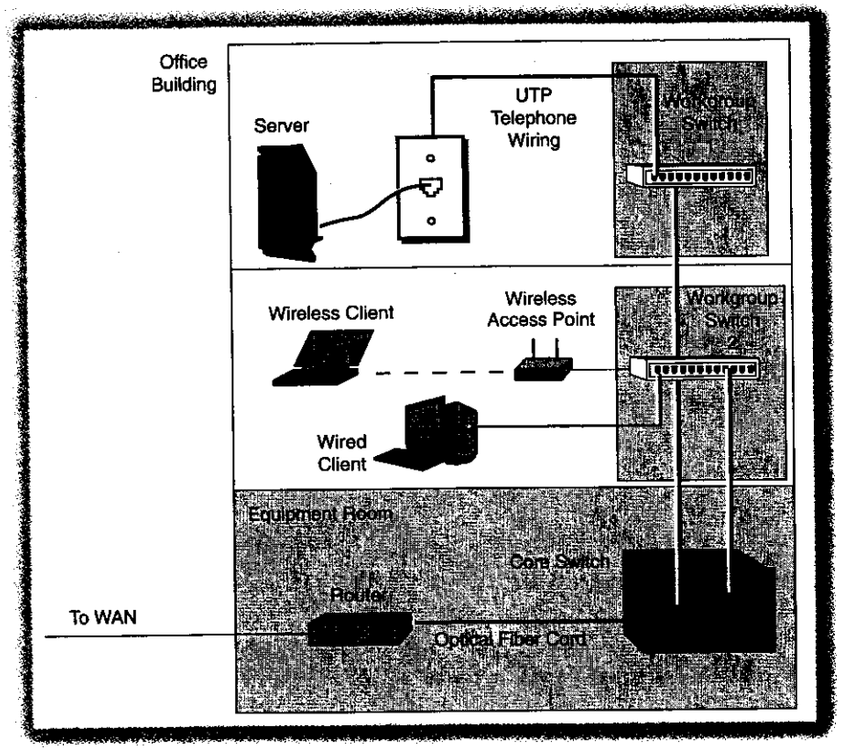


Figure 1-17 Switched Network in a Multistory Building

Access Lines, Trunk Lines, and Multiplexing

Access Lines

The devices in Figure 1-17 are connected by transmission lines. The transmission lines *between hosts and workgroup switches* are called **access lines** because they give a host access to the network. In the figure, the horizontal lines on the first and second floors of the building are access lines.

Most access lines use **4-pair unshielded twisted pair (UTP)** copper wiring, which is illustrated in Figure 1-18. This type of wiring looks like your home telephone wiring but is somewhat thicker and terminates in thicker connectors. The building in Figure 1-17 also augments its wired network with a wireless access point that allows wireless PCs to connect to the building's server on the wired network.

Trunk Lines

In turn, transmission *between switches* takes place over **trunk lines.** These are the vertical lines in Figure 1-17. As we will see in Chapters 3 and 4, trunk lines in local area

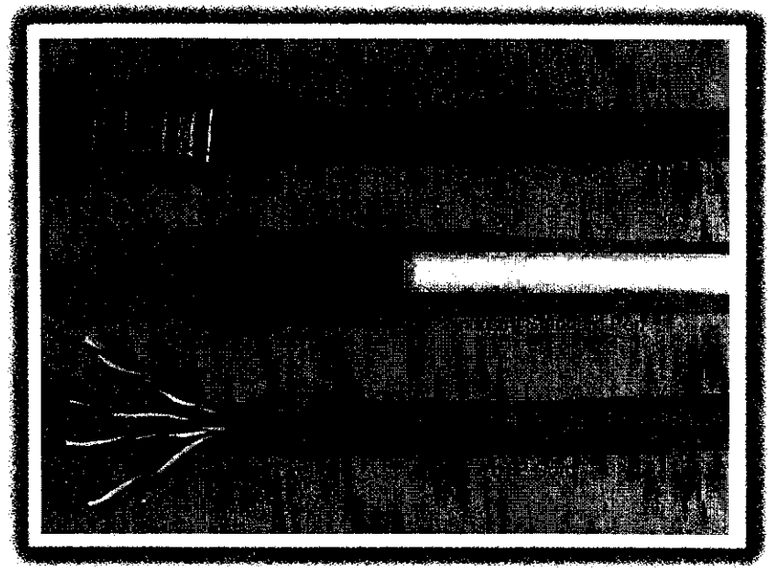


Figure 1-18 Four-Pair Unshielded Twisted Pair (UTP) Copper Wiring

networks can either use 4-pair UTP or optical fiber (which transmits signals as light pulses through a thin flexible glass rod).

Access lines typically serve a single host. However, trunk lines must carry the transmissions of many hosts. Consequently, trunk lines usually need to have much higher transmission speeds than do access lines.

TEST YOUR UNDERSTANDING

17. a) Distinguish between access lines and trunk lines. b) Which type of line needs higher speeds—access lines or trunk lines? Why? c) What type of line is the connection between the Server host and Workgroup Switch 2 in Figure 1-17? d) What type of line is the connection between Workgroup Switch 1 and the Core Switch in Figure 1-17? e) What transmission media do most access lines use? f) Is the 4-pair UTP cord coming out of your PC and plugging into the network wall jack a trunk line or an access line? Explain.

Packet Switching

All switches today, except many of those used for telephony, use a process called packet switching. Packet switching grew from an earlier technology, **message switching.** In message switching, entire messages were sent through switched networks.

Unfortunately, messages varied from short to very long. This created two problems. First, it created problems for trunk lines. Trunk lines **multiplex** (mix) the traffic of many conversations between pairs of hosts. It is much cheaper to have messages

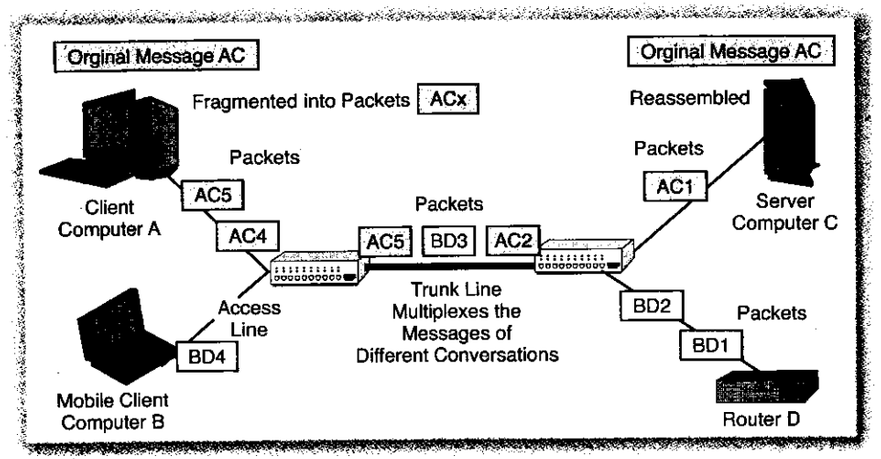


Figure 1-19 Packet Switching and Multiplexing

share a single large line than to have a different line for each message. (Think how expensive it would be if every car on a freeway had its own lane.) Unfortunately, for obscure statistical reasons,[12] it is difficult to fill trunk lines efficiently when messages have very different lengths and when some of them are very long.

A second problem with message switching is that, if there was even a single-bit error, the entire message had to be retransmitted. In long messages, the probability of an error was significant, and frequent retransmissions added to transmission inefficiency.

Figure 1-19 shows that most data networks today use a more sophisticated transmission method called **packet switching.** In packet switching, the source host breaks long application messages into a number of short messages. We have seen earlier that these short messages are generically called **packets.** The host sends each packet out separately. (Think of cars leaving individually to go to a restaurant after a football game.)

Statistically, packet switching can fill multiplexed trunk lines more efficiently than message switching can, driving down trunk line costs. In addition, if there is a transmission error, only the single short packet containing the error needs to be transmitted—not the entire original message. This also reduces trunk line costs by avoiding long retransmissions.

Now for something really confusing: In switched networks, packets are called **frames.** In other words, switched networks do packet switching, but they call their packets frames. This is done to confuse networking students, and it usually succeeds.

In switched networks, packets are called frames. So switched networks do use packet switching, but they call their packets frames.

---

[12]To give a very loose comparison, you can fill a jar more fully with sand than with rocks.

TEST YOUR UNDERSTANDING

18. a) What is multiplexing? b) What is the benefit of multiplexing? c) What is packet switching? d) What does packet switching do to application messages? e) Distinguish between message switching and packet switching. f) Why is packet switching better than message switching? g) What are packets called in switched networks?

ROUTED NETWORKS (INTERNETS)

Routers and Routed Networks

By the 1980s, there were many switched network technologies. They were deeply incompatible, and it was impossible for a host on one type of switched network to communicate with a host on another type of switched network. Even networks that used the same switching technology were rarely connected together. The situation was a networking Tower of Babel.

The solution to this inability to communicate across networks was developed by Vint Cerf and Bob Kahn.[13] As Figure 1-21 shows, their solution was to add another level of transmission functionality on top of switched networks by connecting networks with devices called **routers.** Cerf and Kahn originally called routers **gateways**—a term that still sees some use. Networks like the Internet, then, are **routed networks.** They are also called internets because they are networks of networks.

Figure 1-20 Routed Networks (Study Figure)

- The 1980s: A Switched Tower of Babel
- Routers and Routed Networks
  - Routers connect different switched networks together
  - Routed networks are also called internets
  - Routers are more complex (and expensive) than switches
    - Designed to work no matter how complex the network
    - Require more hands-on administration than switches
- IP Addresses
  - IP addresses
  - Switched network addresses
  - Two addresses for each host
- Packets and Frames
  - Packets are called frames in switched networks
  - Packets are called packets in routed networks
  - A packet is carried in a frame within each switched network

[13]V. Cerf and R. Kahn, "A Protocol For Packet Network Intercommunication," *IEEE Transactions on Communication*, vol. C-20, no. 5, May 1974, pp. 637–648.

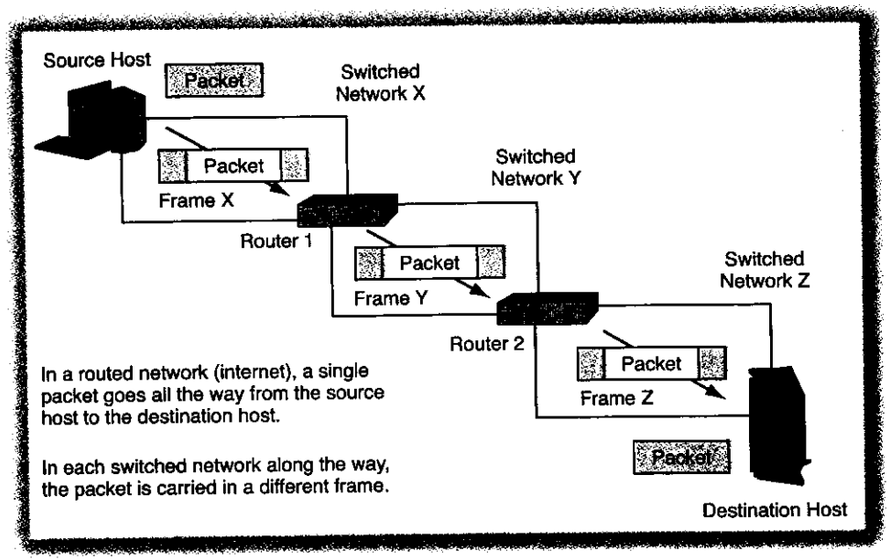


Figure 1-21 Routed Network (Internet)

This leads to the following definition of a routed network: A routed network (internet) is a group of networks connected by routers so that any application on any host on any switched network in the internet can communicate with any application on any other host on any other switched network in the internet.

> A routed network (internet) is a group of networks connected by routers so that any application on any host on any switched network in the internet can communicate with any application on any other host on any other switched network in the internet.

Routed networks perform packet switching. However, while packets are called frames in switched networks, packets are called packets in routed networks.

How are switching and routing different? Most importantly, switching usually is simple and therefore inexpensive. In contrast, we will see in Chapter 8 that router forwarding decisions are complex, which translates into more processing power per packet handled and therefore higher cost. In addition, while switches rarely need management attention once installed, routers need frequent management work. Networking professionals say, "Switch where you can; route where you must." However, routed networks can be extremely large and still be manageable. This is not always the case for switched networks.

TEST YOUR UNDERSTANDING

19. a) Give a definition for *routed network*. b) Is there a distinction between the terms *routed network* and *internet*? If so, what is it? c) In an internet, what device connects networks together? d) Routed networks do packet switching. On routed networks, what are packets called? e) When is a packet called a packet, and when is a packet called a frame? f) Why do networking specialists say, "Switch where you can; route where you must"? g) For what kinds of networks are routed internets especially good?

IP Addresses

Switched Network Addresses

Before routed networks appeared, hosts already had addresses on their switched networks. For instance, on Ethernet switched networks, hosts had 48-bit addresses that were expressed for people in hexadecimal notation. An example is A1–BB–1F–F1–33–CE. Different switched networks had different addressing schemes. For instance, most Frame Relay switched networks had 10-bit addresses called data link control indicators (DLCIs). There was no way to translate between addresses on different types of existing switched networks, and new switched networks (with new addressing schemes) were still emerging.

IP Addresses

Cerf and Kahn addressed this problem by giving each host a second address—a globally unique **IP address.** (IP is the abbreviation for the Internet Protocol, which is the standard created to deliver messages across the networks in an internet.) An IP address is a string of 32 bits, but people have difficulty remembering or writing a stream

Figure 1-22 The Internet (Study Figure)

Hosts
- All computers on any internet are called hosts, including client PCs, personal digital assistants, mobile phones, etc.

Internet Service Providers (ISPs)
- Provide access to the Internet
- Carry your traffic
- Network access points (NAPs) connect the ISPs together
  - Smaller ISPs must pay settlement charges
- You and organizations pay for the ISP operations

Internet Access Lines
- Connect you to your ISP

How the Internet Is Financed
- Through ISP subscriber payments
- Like the telephone network
- Almost no government money involved

The TCP/IP Standards
- The set of protocols that governs the Internet
- Standards for both applications and packet delivery
- Created by the Internet Engineering Task Force (IETF)

of bits. Routers work directly with 32-bit strings, but inferior biological entities express IP addresses in **dotted decimal notation,** which consists of four numerical segments separated by dots. An example is 128.171.17.13.

Two Addresses for Each Host

Consequently, every host on a routed network has two addresses—an address on its individual switched network and a universal IP address that is unique across all switched networks within the routed network.

TEST YOUR UNDERSTANDING

20. a) What is a host's address on the Internet or an internet? b) What is a host's address on an Ethernet network? c) How many bits long is an IP address? d) How are IP addresses presented for human reading? e) Why did Cerf and Kahn create a second address for each host instead of just using the host's existing address on its switched network as its routed network address?

Packets and Frames

Packets

We saw earlier that most switched networks today use packet switching, but call their packets *frames.* Routed networks also use packet switching but call their packets *packets.* If you are confused and somewhat outraged by this apparently stupid inconsistency, you are to be commended for your understanding.

Frames and Packets

Figure 1-20 shows the relationship between packets in a routed network and frames in a switched network. The packet travels end-to-end between the source and destination hosts. Routers pass the packet from one to another along the way. As the packet goes from one router to another, it must travel through a switched network.

The figure shows that the packet travels within a different frame in each switched network. Consequently, when a host transmits a packet to another host, there will be only one packet, but there may be many frames, one in each switched network along the way. If five switched networks separate the source host from the destination host, there will be one packet along the way, but there will be five frames.

TEST YOUR UNDERSTANDING

21. a) What are messages called in internets? b) Distinguish between frames and packets. c) In an internet, the source and destination hosts are separated by five networks (including their own networks). When the source host transmits, how many packets will travel through the internet? d) How many frames?

The Internet Today

The largest routed network (internet) today, of course, is the global Internet you use every day. In this book, we will spell *internet* in lower case to refer to any routed network, and we will spell *Internet* in upper case to refer to the global Internet.

In this book, we will spell **internet** in lower case to refer to any routed network, and we will spell **Internet** in upper case to refer to the global Internet.

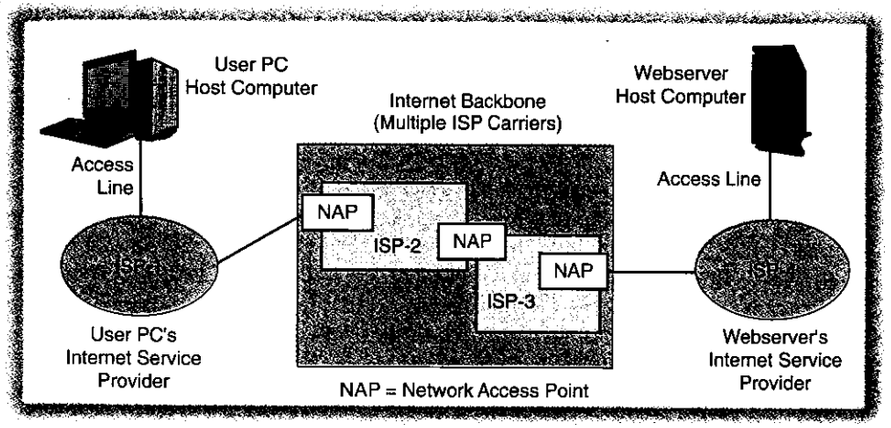


Figure 1-23 The Internet

Internet Service Providers (ISPs)

Figure 1-22 shows the Internet today. It shows that the Internet consists of many commercial carriers called **Internet service providers (ISPs).** Each ISP is a large routed network. In fact, several ISPs span a dozen or more countries.

To connect to the Internet, you *must* connect to an ISP. ISPs are correctly called the on-ramps to the Internet. ISPs also carry your messages to the destination host and the destination host's messages back to your PC.

If the source and destination hosts use different ISPs, their packets (messages) are exchanged between ISPs at **network access points (NAPs).**[14] It is common for packets to pass through several NAPs along their journeys. This may seem like an awkward way of operating the Internet, but it allows for competition and flexibility. It is also how the worldwide telephone network operates, as we will see in Chapter 6.

Internet Access Lines

You also need an access line to your ISP. This can be your regular telephone line, a cable television system connection, or even a wireless connection. Sometimes, ISP fees include access line fees. In other cases, they do not.

Financing the Internet

Who pays for all of this? The answer is that you do. The fees that subscribers pay fund their own ISPs. For home networks, the monthly fee is only about $10 to $70. Larger organizations, however, such as universities and major corporations, pay several million dollars per year to their ISPs.

[14] ISPs of comparable traffic exchange volume will transfer packets without any payments to each other. ISP pairs that send different amounts of traffic have settlement fees.

Engineering Task Force (IETF).[15] We will look at the TCP/IP standards in Chapter 2 and more extensively in Chapters 8 and 10.

Host Names and the Domain Name System (DNS)

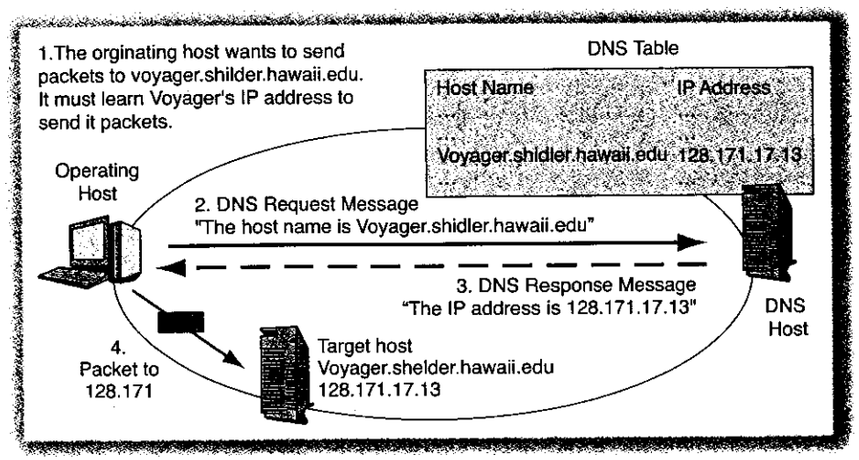
As we saw earlier, every host on a routed network needs an IP address. Unfortunately, an IP address, even in dotted decimal notation, is difficult for people to remember. Consequently, many hosts are given **host names,** which are easier for people to remember. Some examples of host names are google.com, www.msn.com, and panko.shidler.hawaii.edu.

Although host names are easy to remember, the IP address is still the host's official address. If you have a host's host name, you must learn its IP address before you can send it packets. To give an analogy, if you want to call someone whose name you know, you must learn their telephone number.

To continue the telephone example, you can call the directory information number and tell the operator the person's name. The operator will look up the name in the directory database and read you the person's telephone number.

Similarly, if your computer needs to look up a host name's IP address, it contacts a **domain name system (DNS)** server, as Figure 1-23 shows. It sends the server the host name. The DNS server looks up this host name and sends back the IP address. The host that sends the DNS request message can now communicate with the named host. In Chapter 10, we will see how DNS works in more detail.

Figure 1-23 Domain Name System (DNS)



[15]Originally, DARPA paid Bolt Beranek and Newman (now BBN Technologies) to create standards for the operation of the Internet. Stewardship of these standards was then passed to the IETF.

TEST YOUR UNDERSTANDING

22. a) What are the two basic services offered by ISPs on the Internet? b) What are NAPs? c) Why are NAPs crucial to universal connectivity on the Internet? d) What kind of line is needed to connect to an ISP? e) What set of protocols governs Internet transmission? f) What standards agency creates these standards? g) How is the Internet funded?
22. a) What is a host's official address on the Internet? b) Why are host names used? c) When you type a host name for a computer in a URL, what does your computer have to do? d) What type of server is needed?

LANS AND WANS

We have distinguished between switched networks and routed networks (internets). Both types of networks should be further divided into local area networks (LANs) and wide area networks (WANs). Consequently, there can be switched LANs, routed LANs, switched WANs, and routed WANs. The Internet is a routed WAN.

Local Area Networks (LANs)

Local area networks (LANs) are networks that operate on the **customer's premises**—the land and buildings owned by the LAN user. The premises may be a single house or

Figure 1-25 LANs and WANs (Study Figure)

Category	Local Area Networks	Wide Area Networks
Abbreviation	LAN	WAN
Can use switched network technology?	Yes	Yes
Can use routed network technology?	Yes, especially in large LANs	Yes, in fact, that is what the Internet is
Distance span	Customer premises (apartment, office, building, campus, etc.)	Between sites within a corporation or between different corporations
Implementation	Self	Carrier with rights of way
Ability to choose technologies	High	Low
Need to manage technologies	High	Low
Cost per bit transmitted	Low	High with arbitrary changes
Therefore, typical transmission speed	Usually 100 Mbps to 10 Gbps	About 256 kbps to 50 Mbps

apartment. They may also be a small business, an office building, or a university campus. The customer's premises are also called the customer's site.

LANs are networks that operate on the customer's premises (site).

Due to the fact that the LAN operates on the customer's premises, the user company can select whatever technology it wishes to use. Of course, everything you own ends up owning you, and companies also need to install, operate, and maintain their LANs themselves.

Small LANs are likely to be switched LANs. Larger LANs are likely to use routers to divide the LAN into smaller switched networks that are linked together into a local internet.

Wide Area Networks (WANs)

While LANs carry traffic *within* sites, **wide area networks (WANs)** carry traffic *between* sites. These sites might be sites of the same company, sites of different businesses, or company sites and the access sites of Internet service providers.

WANs connect different sites.

Companies do not have legal **rights of way** to lay wires outside of their sites. (Imagine how your neighbors would feel if you started laying wires across their yards.) Consequently, for wide area networking, companies must use **carriers,** which are organizations to which the government gives transmission rights of way. In return for receiving these rights of way, carriers agree to be regulated by the government. This regulation affects both service offerings and prices.

For WANs, companies must use carriers with rights of way.

Carriers are likely to offer only a few services. Consequently, customers must adapt their network plans to the services offered by carriers to which the customers have access. In addition, carrier prices tend to be high and to change rapidly in ways that are only slightly (if at all) related to changes in technology and costs. Finally, carriers often require contracts lasting months or even years. This can lock the firm into a high-priced contract (think of most mobile phone contracts), but at least this gives predictability in pricing.

Cost per Bit and Transmission Speed

When you place a long-distance call, you pay more per minute than you do when you place a local call. Consequently, when you place long-distance calls, you tend to make fewer and shorter calls. In general, when the unit price rises, unit demand decreases.

The same economic logic works for networking. In local area networks, the cost per bit transmitted is far lower than it is in wide area networks. Consequently, companies tend to build LANs that give speeds ranging between 100 Mbps and 10 Gbps, while they tend to limit WAN speeds to between 256 kbps and about 50 Mbps.

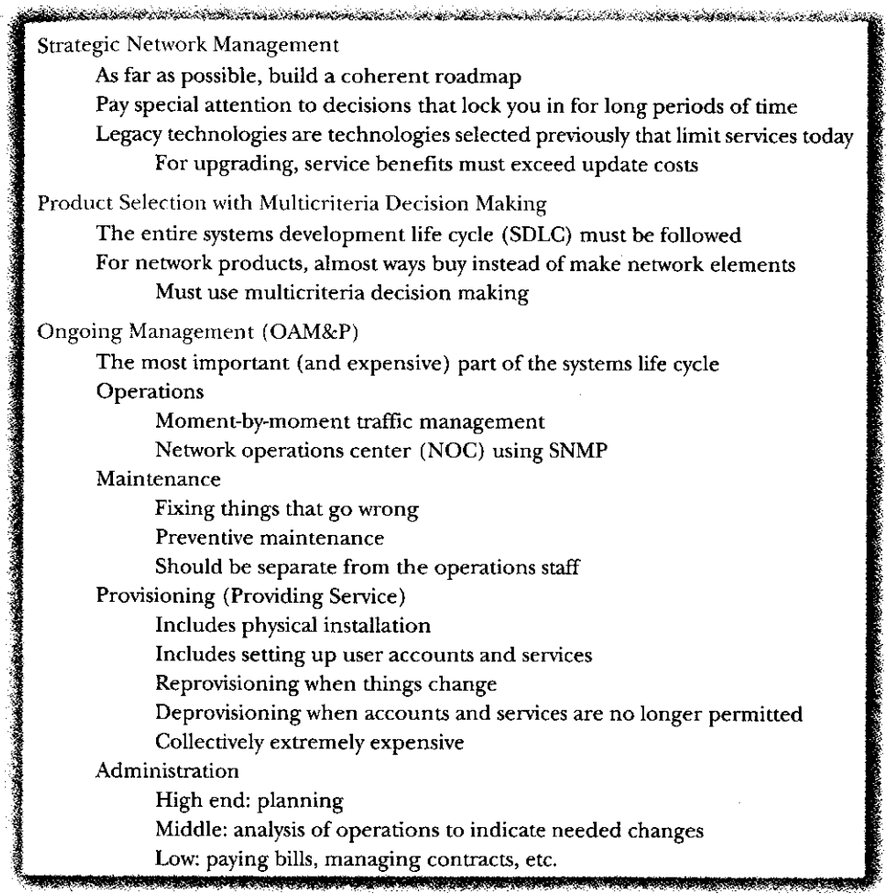


Figure 1-26 Network Management (Study Figure)

Companies tend to build LANs that give speeds ranging between 100 Mbps and 10 Gbps, while they tend to limit WAN speeds to between 256 kbps and about 50 Mbps.

TEST YOUR UNDERSTANDING

24. a) What are LANs? b) What is a WAN? c) When are carriers needed? d) What are rights of way? e) Does a company have more control over LANs or WANs? f) Compare typical LAN and WAN speeds. g) Why are typical WAN speeds slower than typical LAN speeds? Give a complete and logical answer.

Although technology is the most visible aspect of networking, management is the most important aspect of networking. The best-managed networks provide far better service to users at much lower costs than do the worst-managed networks.

Strategic Network Planning

Network technology is changing rapidly. Business requirements are changing even more rapidly. In some cases, the network administrator can only react to unexpected events. However, as far as possible, the network administrator must engage in **strategic network planning** that anticipates changes and builds a roadmap to guide the network in a coherent way for several years.

In strategic planning, an important goal is to identify *current decisions that will lock the firm in for a long period of time.* For instance, if a company pursues a particular technology, this might lock the firm into a particular vendor or at least a particular standard for several years. Although all strategic planning decisions are important, lock-in decisions are the most crucial and should receive the greatest amount of attention. A wrong choice can have dire consequences.

> In strategic planning, an important goal is to identify current decisions that will lock the firm in for a long period of time.

Another important focus for strategic networking planning is on the firm's existing legacy technologies. Legacy technologies are technologies that were selected by your predecessor. Although they probably were good choices at the time, they are now obsolete and impose limits on the services that the networking function can provide. Updating legacy technologies is attractive from a service viewpoint, but the cost of the upgrade must justify the added services. No firm can afford to upgrade all of its legacy network systems immediately.

TEST YOUR UNDERSTANDING

25. a) Why is it important to carefully consider decisions that will lock the firm in for a long period of time? b) What are legacy technologies? c) Should legacy technologies be upgraded if they interfere with services?

Product Selection with Multicriteria Decision Making

Once a project is selected and initiated, the network staff must go through the traditional systems development life cycle to implement the project. Given that almost all readers know about the systems development life cycle, we will not discuss it in detail.

In software development projects, there usually is a **make-versus-buy decision.** Should the programming staff create the software itself, or should the company purchase the software? In networking projects, this decision rarely makes sense. User companies like banks and retail stores do not have the technical expertise to make their own switches and routers. Instead, they must *select* and *buy* these technologies. Consequently, in this book, we will look at the factors you need to understand when you make purchasing decisions involving several alternative technologies.

		Product A		Product B	
Criterion	Criterion Weight (Max: 5)	Product Rating (Max: 10)	Criterion Score	Product Rating (Max: 10)	Criterion Score
Functionality	5	9	45	7	35
Availability	2	7	14	7	14
Cost	5	4	20	9	45
Ease of Management	4	8	32	6	24
Electrical Efficiency	1	9	9	8	8
[illegible]			120		126

Figure 1-27 Multicriteria Decision Making in Purchase Decisions

When making purchasing decisions, companies tend to use **multicriteria decision making,** which Figure 1-27 illustrates. In this approach, the company decides what product characteristics will be important in making the purchase. Things that are important in the purchasing decision are called **criteria.**

Of course, costs are important—both purchase costs and ongoing costs. However, other decision criteria are also important. In Figure 1-27, the criteria for the product are functionality, availability, cost, ease of management, and electrical efficiency.

Next to each criterion is the **criterion weight.** This weight gives the relative importance of each criterion compared with those of other criteria. Here, weights range from 1 to 5. Note that cost and functionality have the largest weights (5), emphasizing their importance.

For each product (there are only two in the figure), the evaluation team gives the product a **rating** for each decision criterion. In this example, the ratings range from 1 to 10, with higher values indicating higher value. More functionality is better, so higher numbers in ratings reflect greater functionality. In contrast, for cost, lower cost is better, so higher rated values must indicate lower cost.

After filling in the ratings on all criteria for all products, the network staff computes the **criterion score** for each product. To do this, the staff multiplies the criterion weight times the rating for that product in that criterion. It then totals the criterion scores into a **total score.**

In Figure 1-27, Product A has a total score of 120, while Product B has a total score of 126. Speaking simplistically, Product B appears to be a better choice. However, the two total scores are very close. Numbers must never drive our thinking. A closer look shows that Product A has very good functionality and ease of management, although its cost is high. Product B has poorer scores on functionality and ease of management. It may be possible to negotiate a lower price on Product A and redo the analysis.

TEST YOUR UNDERSTANDING

26. a) What is the make-versus-buy decision? b) For routers and switches, do firms usually make or buy? c) We are considering products A, B, and C. Our criteria are price, performance, and reliability, with weights of 20%, 40%, and 40%, respectively. Product A's evaluation scores on these three criteria are 8, 6, and 6, respectively. For B, the values are 6, 8, and 8. For C, they are 7, 7, and 7. Present a multicriteria analysis of the decision problem, in tabular form and showing all work. Interpret the table.

Operational Management

After a network component is in place, it probably will be used for many years. During its **operational life,** there will be substantial labor costs. We will classify these costs in a way that telecommunications carriers have traditionally done—in terms of **operations, administration, maintenance, and provisioning (OAM&P).**[16]

Operations and the Simple Network Management Protocol (SNMP)

You probably have seen pictures of **network operations centers (NOCs)** for major telecommunications carriers. These are large rooms with dozens of monitors showing the conditions of various parts of the network. Most corporations also have network operations centers. These corporate NOCs are smaller, usually having only about a half dozen monitors.

For remote device management, most NOCs use the **simple network management protocol (SNMP),** which is illustrated in Figure 1-28. In the NOC, there is a computer that runs a program called the **manager,** which manages a large number of **managed devices,** such as switches, routers, servers, and PCs.

Actually, the manager does not talk directly with the managed devices. Rather, each managed device has an **agent,** which is hardware, software, or both. The manager talks to the agent, which in response talks to the managed device.

The network operations center constantly collects data from the managed devices, using SNMP **Get** commands. It places this data in a **managed information base (MIB).** Data in the MIB gives NOC managers a detailed picture of the traffic flowing through the network. This can include failure points, links that are approaching their capacity, or unusual traffic patterns that may indicate attacks on the network.

In addition, the manager can send **Set** commands to the switches and other devices within the network. Set commands can reroute traffic around failed equipment or transmission links, reroute traffic around points of congestion, or turn off expensive transmission links during periods when less expensive links can carry the traffic adequately.

Normally, the manager sends a command and the agent responds. However, if the agent senses a problem, it can send a **trap** command on its own initiative. The trap command gives details of the problem.

Maintenance

You have undoubtedly seen telephone company maintenance trucks on their way to downed transmission lines, broken transformers, or other trouble spots. In addition to fixing equipment failures, telephone companies do preventative maintenance to prevent future failures.

In the same way, companies often have to fix their internal corporate network switches and other physical components. They also have to handle software problems. Although the network operations center can fix some problems remotely, most firms have separate NOC and maintenance staffs. The NOC staff usually is heavily occupied with the moment-by-moment operation of the network, and it makes sense to have other networking professionals focus on maintenance.

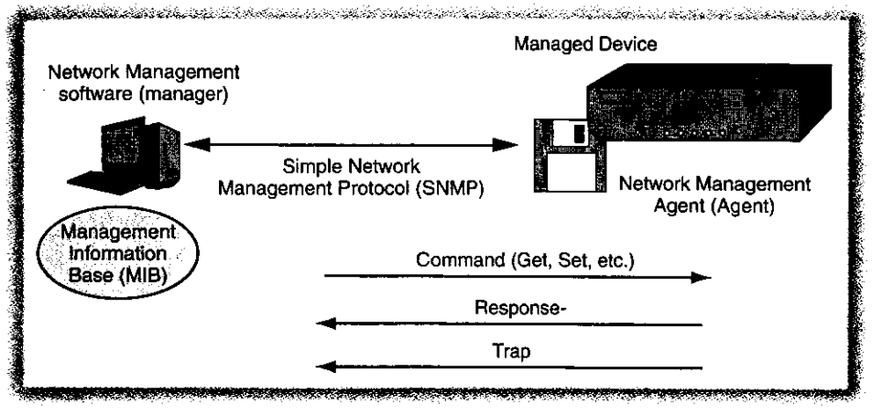


Figure 1-28 Simple Network Management Protocol (SNMP)

Provisioning

If you get cable television service, the cable company has to **provision** your residence—that is, set up service. This includes physical setup (running the coaxial cable into your home). It also involves setting up your account on the company's computers. The cable company also has to reprovision customers when they change their service by adding channels, dropping optional services, or switching pricing plans.

Within a corporate network, provisioning may involve the installation of additional switches, networks, and transmission lines to serve new users. In networks, every time a new user joins the firm, the company has to provision service for that user. In fact, provisioning has to be done for every user account on every server and access point on the network.

Furthermore, once a user is provisioned for a particular resource, he or she may have to be **reprovisioned** if his or her authorizations change—say, if he or she is upgraded from read-only data access to full read/write access. The user also has to be reprovisioned if he or she changes jobs within a firm, joins project teams, or does many other things. Users also have to be **deprovisioned** when they leave project teams or leave the company entirely. Contractors and other outside organizations also have to be provisioned, reprovisioned, and deprovisioned when they start to work, change the way they work, or stop working with a company.

[16]Many firms describe their ongoing work in terms of the ISO Telecommunications Management Network Model. In this model, these activities are called FCAPS, which stands for *fault management, configuration management, accounting management, performance management,* and *security management.*

Administration

Operations, maintenance, and provisioning involve real-time work to keep the network running. Administration tasks include "everything else."

- At the high end, administration includes network planning and project management.
- In the middle, administration includes the collection of performance data, maintenance data, and other data on the network for use in planning.
- At the low end, it includes paying bills to vendors and telephone companies, monitoring proposals and contracts, doing network budgeting, comparing network budgets with actual costs, and doing other "business" work.

TEST YOUR UNDERSTANDING

27. a) List the main elements in an SNMP network management system. b) Does the manager communicate directly with the managed device? Explain. c) Distinguish between Get and Set commands. d) Where does the manager store the information it receives from Get commands? e) What kinds of messages can agents initiate?
28. a) For what is OAM&P an abbreviation in ongoing management? b) Distinguish between operations and maintenance. c) What is provisioning? d) When may reprovisioning be necessary? e) When may deprovisioning be necessary? f) List at least one administrative task at the high end, in the middle, and at the low end.

The Conclusion Section

The Conclusion section wraps up the chapter and helps you reflect on what you have learned.

SYNOPSIS

The Synopsis gives the highlights of the chapter. Reading it after you study the body of the chapter will help you see how things fit together. Studying only the Synopsis, CliffsNotes® style, may seem attractive, but if you don't understand the chapter well, you won't understand many of the key points. Also, while the points in the synopsis are especially important, they represent only a fraction of what you will have to know on an exam.

END OF CHAPTER QUESTIONS

Test Your Understanding questions are limited to helping you understand basic concepts. At the end of the chapter, there are questions that help you reflect on and integrate what you have learned. Do these only after you have mastered the individual concepts in the chapter.

THOUGHT QUESTIONS

Thought Questions are general questions that require you to integrate what you have learned. Learning individual facts in isolation will not be enough to answer thought questions (or to prepare you for your career). Thought questions that include the words, "what do you think" generally have no right or wrong answers. They require you to come to a reasoned opinion, hopefully after considering all sides of the issue.

TROUBLESHOOTING QUESTIONS

Troubleshooting Questions help you apply what you have learned to real-world situations. Networks are complex aggregations of devices and transmission lines. When problems occur, you will need to use your detailed knowledge and your understanding of the situation to come up with several possible causes and then systematically eliminate causes until you have found the correct one.

DESIGN QUESTIONS

Design Questions give you a description of a situation and ask you to design a solution that meets a person's or organization's needs. This is the real litmus test for whether you have understood the material in the chapter. Design requires you to put together all of the bits and pieces in the chapter. Keep in mind that designers are governed by their worst moments. If you leave out something important, the client will be faced with a system that will not work without an additional unplanned investment. Clients recoup their additional expenses through lawsuits against designers.

PERSPECTIVE QUESTIONS

Perspective Questions help you to reflect on your experience in working through the chapter. What surprised you? What was hardest for you? These questions help you as you restudy the material later.

PROJECTS

Some chapters have projects that involve research into a topic.

HANDS-ON EXERCISES

Hands-On Exercises ask you to use your computer or another device to accomplish something specific, such as to see whether your computer's connection to the network is working or to figure out why you cannot reach a webserver that you normally can reach.

CONCLUSION

Synopsis

The chapter began with a focus on applications. Networks exist to allow application programs on different hosts to work together. (The term *host* is used for any computer attached to a network, regardless of the host's size.) In this chapter, we looked at a number of traditional Internet applications, newer Internet applications, and other corporate applications. The discussion was intended to emphasize the wide variety of applications that networks must serve.

One theme in the discussion of applications was network standards, which are also known as protocols. Open standards allow products from different vendors to work together. This spurs competition and product advancement. We will look more closely at standards in Chapter 2.

We spent almost half of the chapter looking for applications of various types. We looked at the traditional and new Internet applications that you are familiar with as an individual. We also looked briefly at corporate applications, such as transaction processing and converged network applications. We also saw the advantages of file service for both data files and program files.

Today, networks are mission-critical corporate infrastructures. They must work, and they must work well. We looked at several quality-of-service (QoS) metrics, including speed, cost, availability, error rate, latency, jitter, and security. We also looked at service level agreements (SLAs), which are vendor warranties for QoS. SLAs specify the maximum amount of time that a worst-case condition (low speed, high latency, etc.) may exist.

Packet switching involves fragmenting a long message into smaller messages called packets and then sending these packets individually. Packet switching creates very efficient multiplexing, greatly reducing transmission costs.

We looked at the technology of switched networks, which use simple devices called switches to forward packets. One oddity of terminology is that in switched networks, packets are called *frames*. We saw that each frame carries the switched address of the destination device for the frame—a destination host or a router within the switched network. Switches along the way read the destination address to decide which port to use to send the frame back out.

During the 1980s, numerous switched networks appeared, using many different technologies. The solution to the chaos this created was to integrate multiple switched networks into routed networks, also called internets. This was made possible by the invention of sophisticated devices called routers. Routers are much more expensive than switches because of the need to move messages across multiple switched networks. In routed networks, messages actually are called packets. One packet travels from the source host to the destination host. In each switched network along the way, the switch is carried in a different packet. In a routed network, every host has two addresses. One is its address on its own switched network. The other is its globally unique IP address on the Internet.

We looked at the Internet very briefly. We saw that to use the Internet, you need an access line and an Internet service provider (ISP). Your ISP gives you access to the Internet and carries your messages. If the other server you are trying to reach is served by a different ISP, that is fine because ISPs interconnect with one another at network access points (NAPs).

We noted that local area networks (LANs) and wide area networks (WANs) could be either switched or routed. LANs operate on the customer premises. This allows the user organization to choose any technology it wishes. WANs carry traffic between customer sites. Companies do not have rights of way to lay transmission lines beyond their premises, so WAN transmission is done by carriers. The cost per bit transmitted is higher in WANs than in LANs, so WAN speeds usually are much lower than LAN speeds.

We ended the chapter with a discussion of network management, including strategic network planning, multicriteria decision making for product selection, and OAM&P (operations, administration, maintenance, and provisioning).

End-of-Chapter Questions

THOUGHT QUESTIONS

1. a) The telephone system has an availability of 99.999 percent. How much downtime is that per year? b) With an availability of 99.9 percent, how much downtime is that per year? c) With an availability of 99 percent, how much downtime is that per year?
2. Is minimizing the cost per bit transmitted more important in LANs or WANs? Justify your answer.
3. Create a table comparing switched and routed networks across the various dimensions discussed in the chapter (name of message, etc.).

TROUBLESHOOTING QUESTIONS

Troubleshooting is identifying and fixing problems. Troubleshooting is an important skill, and we will see troubleshooting questions throughout this textbook. Research has shown that people often make fundamental mistakes when they do troubleshooting. Most fundamentally, they usually consider only one or two possible causes for their problem. Often, the one or two possible causes they consider are incorrect. Consequently, they often waste time trying to solve the wrong problem. Only later do they realize that they need to consider additional possibilities. Premature focusing on one or two possible causes tends to extend downtime needlessly and sometimes leads to "solutions" that fail to fix the real problem.

In troubleshooting questions, you will be expected to create multiple hypotheses, not just one or two. It is almost always best to draw a diagram of all of the components of a system to broaden your perspective. After you develop multiple possible causes of the problem, you can then use logic or experimentation to prioritize them and eliminate false causes.

1. Here is a sample troubleshooting problem for you to solve. You have been using a telephone modem to access the Internet. The modem's rated download speed is 56 kbps. You switch to a cable modem, which should allow you to receive at 3 Mbps. In general, your download speed for webpages is faster than it was with your telephone modem; however, your actual download rates usually vary from only 500 kbps to 1.5 Mbps.
   a) List likely reasons for your not being able to get a full 3 Mbps. **Do NOT just come up with one or two possible explanations.** *Hint:* Consider Figure 1-24, which shows the Internet.
   b) Assess the likelihood of each alternative, given the facts in the problem description and any other analysis you can consider.
2. Your DSL line has a listed speed of 500 kbps. However, when you make downloads, a speed counter tells you that you are receiving only 50 kBps. Can you explain this apparent inconsistency?

PERSPECTIVE QUESTIONS

1. What was the most surprising thing you learned in this chapter?
2. What was the most difficult material for you in this chapter?

PROJECTS

1. Do a report on streaming video formats.
2. Do a report on some aspect of Web 2.0 (its definition, wikis, blogs, etc.).

GETTING CURRENT

Go to the book website's New Information and Errors pages for this chapter to get new information since this book went to press and to correct any errors in the text.

TROUBLESHOOTING QUESTIONS

1. A tester shows that a UTP cord has too much interference. What might be causing the problem? Give at least two alternative hypotheses, and then describe how to test them.
2. What kinds of errors are you likely to encounter if you run a length of UTP cord 200 meters? (Recall that the standard calls for a 100-meter maximum distance.)

HANDS-ON EXERCISE

Chapter 3a discusses how to connectorize bulk UTP cabling. To try it out, you will need a box of bulk UTP cabling, a wire cutter, a wire stripper, a crimper, a bag of RJ-45 connectors, and a tester (because only about half of connections done by novices work). All of this will set you back about $300. When you know this, the price of UTP patch cables, which are cut, connectorized, and tested at the factory, seems more reasonable, doesn't it?

PERSPECTIVE QUESTIONS

1. What was the most surprising material for you in this chapter?
2. What was the most difficult thing for you in this chapter?

PROJECT

Write a one-page research report on Category 7 STP or small form factor optical fiber connectors.

GETTING CURRENT

Go to the book website's New Information and Errors pages for this chapter to get new information since this book went to press and for corrections to any errors in the text.

Hands-On: Cutting and Connectorizing UTP[1]

INTRODUCTION

Chapter 3 discussed UTP wiring in general. This chapter discusses how to cut and connectorize (add connectors to) solid UTP wiring.

SOLID AND STRANDED WIRING

Solid-Wire UTP versus Stranded-Wire UTP

The TIA/EIA-568 standard requires that long runs to wall jacks use **solid-wire UTP,** in which each of the eight wires really is a single solid wire.

However, patch cords running from the wall outlet to a NIC usually are **stranded-wire UTP,** in which each of the eight "wires" really is a bundle of thinner wire strands. So stranded-wire UTP has eight bundles of wires, each bundle in its own insulation and acting like a single wire.

Relative Advantages

Solid wire is needed in long cords because it has lower attenuation than stranded wire. In contrast, stranded-wire UTP cords are more flexible than solid-wire cords, making them ideal for patch cords—especially the one running to the desktop—because they can be bent more and still function. They are more durable than solid-wire UTP cords.

[1]This material is based on the author's lab projects and on the lab project of Prof. Harry Reif of James Madison University.

Solid-Wire UTP

- Each of the eight wires is a solid wire
- Low attenuation over long distances
- Easy to connectorize
- Inflexible and stiff—not good for runs to the desktop

Stranded-Wire UTP

- Each of the eight "wires" is itself several thin strands of wire within an insulation tube
- Flexible and durable—good for runs to the desktop
- Impossible to connectorize in the field (bought as patch cords)
- Higher attenuation than solid-wire UTP—Used only in short runs
  - From wall jack to desktop
  - Within a telecommunications closet (see Chapter 3)

Figure 3a-1 Solid-Wire and Stranded-Wire UTP (Study Figure)

Adding Connectors

It is relatively easy to add RJ-45 connectors to solid-wire UTP cords. However, it is very difficult to add RJ-45 connectors to stranded-wire cords. Stranded-wire patch cords should be purchased from the factory precut to desired lengths and preconnectorized.

In addition, when purchasing equipment to connectorize solid-wire UTP, it is important to purchase crimpers designed for solid wire.

CUTTING THE CORD

Solid-wire UTP normally comes in a box or spool containing 50 meters or more of wire. The first step is to cut a length of UTP cord that matches your need. It is good to be a little generous with the length. This way, bad connectorization can be fixed by cutting off the connector and adding a new connector to the shortened cord. Also, UTP cords should never be subjected to pulls (strain), and adding a little extra length creates some slack.

STRIPPING THE CORD

Now the cord must be stripped at each end using a **stripping tool** such as the one shown in Figure 3a-2. The installer rotates the stripper once around the cord, scoring (cutting into) the cord jacket (but not cutting through it). The installer then pulls off the scored end of the cord, exposing about 5 cm (about two inches) of the wire pairs.

Figure 3a-2 Stripping Tool

It is critical not to score the cord too deeply, or the insulation around the individual wires may be cut. This creates short circuits. A really deep cut also will nick the wire, perhaps causing it to snap immediately or later.

WORKING WITH THE EXPOSED PAIRS

Pair Colors

The four pairs each have a color: orange, green, blue, or brown. One wire of the pair usually is a completely solid color. The other usually is white with stripes of the pair's color. For instance, the orange pair has an orange wire and a white wire with orange stripes.

Untwisting the Pairs

The wires of each pair are twisted around each other several times per inch. These must be untwisted after the end of the cord is stripped.

Ordering the Pairs

The wires now must be placed in their correct order, left to right. Figure 3a-3 shows the location of Pin 1 on the RJ-45 connector and on a wall jack or NIC.

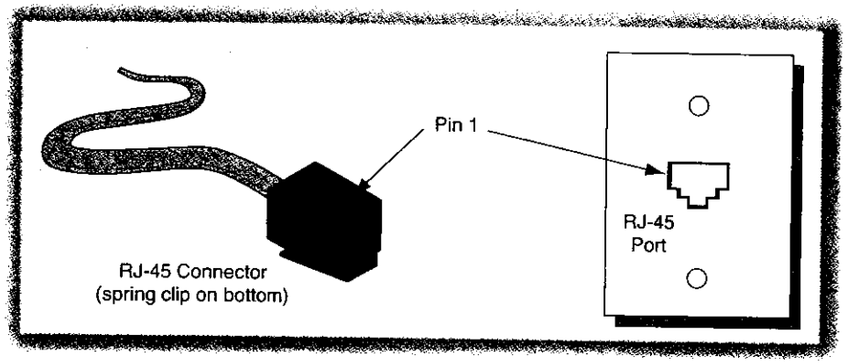


Figure 3a-3 Location of Pin 1 on an RJ-45 Connector and Wall Jack or NIC

Which color wire goes into which connector slot? The two standardized patterns are shown in Figure 3a-4. The T568B pattern is much more common in the United States.

The connectors at both ends of the cord use the same pattern. If the white-orange wire goes into Pin 1 of the connector on one end of the cord, it also goes into Pin 1 of the connector at the other end.

Figure 3a.4 T568A and T568B Pin Colors

Pin*	T568A	T568B
1	White-Green	White-Orange
2	Green	Orange
3	White-Orange	White-Green
4	Blue	Blue
5	White-Blue	White-Blue
6	Orange	Green
7	White-Brown	White-Brown
8	Brown	Brown

Note: Do not confuse T568A and T568B pin colors with the TIA/EIA-568 Standard.

Cutting the Wires

The length of the exposed wires must be limited to 1.25 cm (0.5 inch) or slightly less. After the wires have been arranged in the correct order, a cutter should cut across the wires to make them this length. The cut should be made straight across, so that all wires are of equal length. Otherwise, they will not all reach the end of the connector when they are inserted into it. Wires that do not reach the end will not make electrical contact.

ADDING THE CONNECTOR

Holding the Connector

The next step is to place the wires in the RJ-45 connector. In one hand, hold the connector, clip side down, with the opening in the back of the connector facing you.

Sliding in the Wires

Now, slide the wires into the connector, making sure that they are in the correct order (white-orange on your left). There are grooves in the connector that will help. Be sure to push the wires all the way to the end or proper electrical contact will not be made with the pins at the end.

Before you crimp the connector, look down at the top of the connector, holding the tip away from you. The first wire on your left should be mostly white. So should every second wire. If they are not, you have inserted your wires incorrectly.[2]

Some Jacket Inside the Connector

If you have shortened your wires properly, there will be a little bit of jacket inside the RJ-45 connector.

CRIMPING

Pressing Down

Get a really good **crimping tool** (see Figure 3a-5). Place the connector with the wires in it into the crimp and push down firmly. Good crimping tools have ratchets to reduce the chance of your pushing down too tightly.

Making Electrical Contact

The front of the connector has eight pins running from the top almost to the bottom (spring clip side). When you **crimp** the connector, you force these eight pins through the insulation around each wire and into the wire itself. This seems like a crude electrical connection, and it is. However, it normally works very well. Your wires are now connected to the connector's pins. By the way, this is called an **insulation displacement connection (IDC)** because it cuts through the insulation.

[2]Thanks to Jason Okumura, who suggested this way of checking the wires.

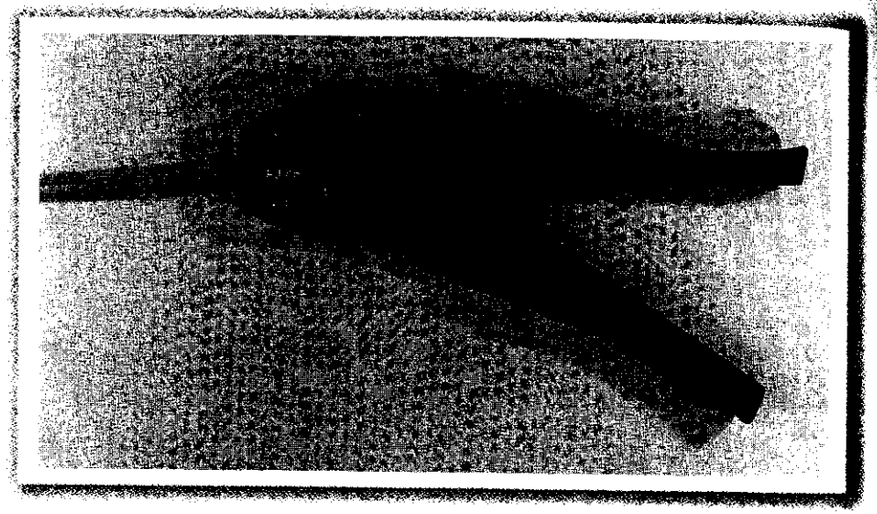


Figure 3a-5 Crimping Tool

Strain Relief

When you crimp, the crimper also forces a ridge in the back of the RJ-45 connector into the jacket of the cord. This provides **strain relief,** meaning that if someone pulls on the cord (a bad idea), they will be pulling only to the point where the jacket has the ridge forced into it. There will be no strain where the wires connect to the pins.

TESTING

Purchasing the best UTP cabling means nothing unless you install it properly. Wiring errors are common in the field, so you need to test every cord after you install it. Testing is inexpensive compared to troubleshooting subtle wiring problems later.

Testing with Continuity Testers

The simplest testers are **continuity testers,** which merely test whether the wires are arranged in correct order within the two RJ-45 connectors and are making good electrical contact with the connector. They cost only about $100.

Testing for Signal Quality

Better testers cost $500 to $2,000 but are worth the extra money. In addition to testing for continuity problems, they send **test signals** through the cord to determine whether the cord meets TIA/EIA-568 signal quality requirements. Many include **time domain reflectometry (TDR),** which sends a signal and listens for echoes in order to measure the length of the UTP cord or to find if and where breaks exist in the cord.

TEST YOUR UNDERSTANDING

1. a) Explain the technical difference between solid-wire UTP and stranded-wire UTP. b) In what way is solid-wire UTP better? c) In what way is stranded-wire UTP better? d) Where would you use each? e) Which should only be connectorized at the factory?
2. If you have a wire run of 50 meters, should you cut the cord to 50 meters? Explain.
3. Why do you score the jacket of the cord with the stripping tool instead of cutting all the way through the jacket?
4. a) What are the colors of the four pairs? b) If you are following T568B, which wire goes into Pin 3? c) At the other end of the cord, would the same wire go into Pin 3?
5. After you arrange the wires in their correct order and cut them across, how much of the wires should be exposed from the jacket?
6. a) Describe RJ-45's insulation displacement approach. b) Describe its strain relief approach.
7. a) Should you test every cord in the field after installation? b)For what do inexpensive testers test? c) For what do expensive testers test?