

12. To decrypt an encrypted message, just select the text in the email (you need to select the entire message from BEGIN PGP MESSAGE to END PGP MESSAGE). Copy the message to clipboard via CTRL+ C. Right click Kleopatra icon on your status bar, and then select Clipboard and Decrypt & Verify. This is very similar to how you encrypted the message. The decrypted message will be stored in the clipboard. To read it, just paste it to Word or any other text editor. You are done!

DELIVERABLES

1. Create your PGP key pair using Kleopatra. Post the asc file of your public key on a server/class website as instructed by your professor.
2. Import a certificate (public key) of your professor to Kleopatra. Send your instructor an encrypted message that contains information about your favorite food, hobbies, places to travel, and so on.
3. Your professor will send you a response that will be encrypted. Decrypt the email and print its content so that you can submit a hard copy in class.

¹ This chapter was written by Alan Dennis and Dwight Worker.

² CERT maintains a Web site on security at www.cert.org. Another site for security information is www.infosyssec.net.

³ The statistics in this chapter are based on surveys conducted by CSO magazine (www.csionline.com) and the Computer Security Institute (www.gocsi.com).

⁴ John J. Tkacik Jr., "Trojan Dragon: China's Cyber Threat," *Backgrounder*, no. 2106, February 2008, The Heritage Foundation.

⁵ CERT has developed a detailed risk assessment procedure called OCTAVESM, which is available at www.cert.org/octave.

⁶ We should point out, though, that the losses associated with computer fraud are small compared with other sources of fraud.

⁷ There are many good business continuity planning sites such as www.disasterrecoveryworld.com.

⁸ Most routers and firewalls manufactured by Linksys (a manufacturer of networking equipment for home and small office use owned by Cisco) use NAT. Rather than setting the internal address to 10.x.x.x, Linksys sets them to 192.168.1.x, which is another subnet reserved for private intranets. If you have Linksys equipment with a NAT firewall, your internal IP address is likely to be 192.168.1.100.

⁹ For an example of one CERT advisory posted about problems with the most common DNS server software used on the Internet, see www.cert.org/advisories/CA-2001-02.html. The history in this advisory shows that it took about eight months for the patch for the previous advisory in this family (issued in November 1999) to be installed on most DNS servers around the world. This site also has histories of more recent advisories.

¹⁰ For more information on cryptography, see the FAQ at www.rsa.com.

¹¹ If you use Windows, you can encrypt files on your hard disk: Just use the Help facility and search on encryption to learn how.

¹² There are several versions of 3DES. One version (called 3DES-EEE) simply encrypts the message three times with different keys as one would expect. Another version (3DES-EDE) encrypts with one key, decrypts with a second key (i.e., reverse encrypts), and then encrypts with a third key. There are other variants, as you can imagine.

¹³ The rules have been changed several times in recent years, so for more recent information, see www.bis.doc.gov.

¹⁴ Rivest, Shamir, and Adleman have traditionally been given credit as the original developers of public key encryption (based on theoretical work by Whitfield Diffie and Martin Hellman), but recently declassified material has revealed that public key encryption was actually first developed years earlier by Clifford Cocks based on theoretical work by James Ellis, both of whom were employees of a British spy agency.

¹⁵ For more on the PKI, go to www.ietf.org and search on PKI.

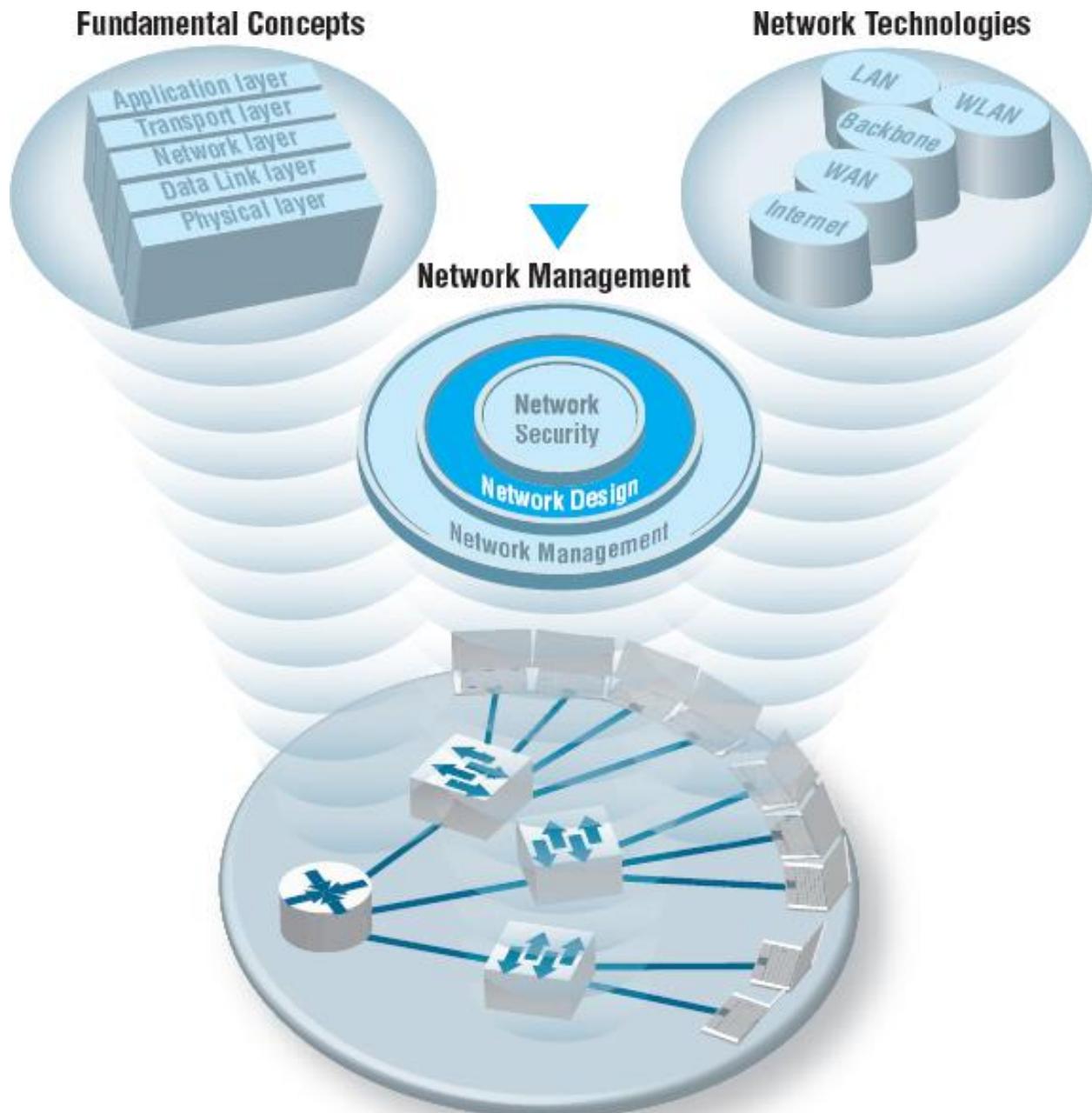
¹⁶ For example, Cisco posts the public keys it uses for security incident reporting on its Web site; go to www.cisco.com and search on “security incident response.” For more information on PGP, see www.pgp.org and www.pgp.com.

¹⁷ This is done using the Diffie-Hellman process; see the FAQ at www.rsa.com.

¹⁸ For more information about social engineering and many good examples, see *The Art of Deception* by Kevin Mitnick and William Simon.

CHAPTER 11

NETWORK DESIGN



The Three Faces of Networking

NETWORK MANAGERS perform two key tasks: (1) designing new networks and network upgrades and (2) managing the day-to-day operation of existing networks. This chapter examines network design. Network

design is an interative process in which the designer examines users' needs, develops an initial set of technology designs, assesses their cost, and then revisits the needs analysis until the final network design emerges.

OBJECTIVES ▼

- Be familiar with the overall process of designing and implementing a network
- Be familiar with techniques for developing a logical network design
- Be familiar with techniques for developing a physical network design
- Be familiar with network design principles
- Understand the role and functions of network management software
- Be familiar with several network management tools

CHAPTER OUTLINE ▼

11.1 INTRODUCTION

11.1.1 The Traditional Network Design Process

11.1.2 The Building-Block Network Design Process

11.2 NEEDS ANALYSIS

11.2.1 Geographic Scope

11.2.2 Application Systems

11.2.3 Network Users

11.2.4 Categorizing Network Needs

11.2.5 Deliverables

11.3 TECHNOLOGY DESIGN

11.3.1 Designing Clients and Servers

11.3.2 Designing Circuits and Devices

11.3.3 Network Design Tools

11.3.4 Deliverables

11.4 COST ASSESSMENT

11.4.1 Request for Proposal

11.4.2 Selling the Proposal to Management

11.4.3 Deliverables

11.5 DESIGNING FOR NETWORK PERFORMANCE

11.5.1 Managed Networks

11.5.2 Network Circuits

11.5.3 Network Devices

11.5.4 Minimizing Network Traffic

11.5.5 Green IT

11.6 IMPLICATIONS FOR MANAGEMENT

11.1 INTRODUCTION

All but the smallest organizations have networks, which means that most network design projects are the design of upgrades or extensions to existing networks, rather than the construction of entirely new networks. Even the network for an entirely new building is likely to be integrated with the organization's existing backbone or WAN, so even new projects can be seen as extensions of existing networks. Nonetheless, network design is very challenging.

11.1.1 THE TRADITIONAL NETWORK DESIGN PROCESS

The **traditional network design process** follows a very structured systems analysis and design process similar to that used to build application systems. First, the network analyst meets with users to identify user needs and the application systems planned for the network. Second, the analyst develops a precise estimate of the amount of data that each user will send and receive and uses this to estimate the total amount of traffic on each part of the network. Third, the circuits needed to support this traffic plus a modest increase in traffic are designed and cost estimates are obtained from vendors. Finally, 1 or 2 years later, the network is built and implemented.

This traditional process, although expensive and time consuming, works well for static or slowly evolving networks. Unfortunately, networking today is significantly different from what it was when the traditional process was

developed. Three forces are making the traditional design process less appropriate for many of today's networks.

First, the underlying technology of the client and server computers, networking devices, and the circuits themselves is changing very rapidly. In the early 1990s, mainframes dominated networks, the typical client computer was an 8-MHz 386 with 1 megabyte (MB) of random access memory (RAM) and 40 MB of hard disk space, and a typical circuit was a 9,600-bps mainframe connection or a 1-Mbps LAN. Today, client computers and servers are significantly more powerful, and circuit speeds of 100 Mbps and 1 Gbps are common. We now have more processing capability and network capacity than ever before; both are no longer scarce commodities that we need to manage carefully.

Second, the growth in network traffic is immense. The challenge is not in estimating today's user demand but in estimating its rate of growth. In the early 1990s, email and the Web were novelties primarily used by university professors and scientists. In the past, network demand essentially was driven by predictable business systems such as order processing. Today, much network demand is driven by less predictable user behavior, such as email and the Web. Many experts expect the rapid increase in network demand to continue, especially as video, voice, and multimedia applications become commonplace on networks. At a 10 percent growth rate, user demand on a given network will increase by one-third in three years. At 20 percent, it will increase by about 75 percent in three years. At 30 percent, it will double in less than three years. A minor mistake in estimating the growth rate can lead to major problems. With such rapid growth, it is no longer possible to accurately predict network needs for most networks. In the past, it was not uncommon for networks to be designed to last for 5 to 10 years. Today, most network designers use a 3- to 5-year planning horizon.

11.1 AVERAGE LIFE SPANS

MANAGEMENT FOCUS

A recent survey of network managers found that most expect their network hardware to last three to five years—not because the equipment wears out, but because rapid changes in capabilities make otherwise good equipment obsolete.

Life expectancy for selected network equipment:

Rack mounted switch 4.5
years

Chassis switch 4.5
years

Backbone router 5
years

Branch office router 4
years

As Joel Snyder, a senior partner at OpusOne (a network consulting firm), puts it: “You might go buy a firewall for a T-1 at a remote office and then two weeks later have your cable provider offer you 7 Mbps.”

Wi-Fi access point 3
years

Desktop PC 3.5
years

Laptop PC 2.5
years

Mainframe 8.5
years

SOURCE: "When to Upgrade," *Network World*, November 28, 2005, pp. 49–50.

Finally, the balance of costs have changed dramatically over the past 10 years. In the early 1990s, the most expensive item in any network was the hardware (circuits, devices, and servers). Today, the most expensive part of the network is the staff members who design, operate, and maintain it. As the costs have shifted, the emphasis in network design is no longer on minimizing hardware cost (although it is important); the emphasis today is on designing networks to reduce the staff time needed to operate them.

The traditional process minimizes the equipment cost by tailoring the equipment to a careful assessment of needs but often results in a mishmash of different devices with different capabilities. Two resulting problems are that staff members need to learn to operate and maintain many different devices and that it often takes longer to perform network management activities because each device may use slightly different software.

Today, the cost of staff time is far more expensive than the cost of equipment. Thus, the traditional process can lead to a false economy—save money now in equipment costs but pay much more over the long term in staff costs.

11.1.2 THE BUILDING-BLOCK NETWORK DESIGN PROCESS

Some organizations still use the traditional process to network design, particularly for those applications for which hardware or network circuits are unusually expensive (e.g., WANs that cover long distances through many different countries). However, many other organizations now use a simpler approach to network design that we call the **building-block process**. The key concept in the building-block process is that networks that use a few standard components throughout the network are cheaper in the long run than networks that use a variety of different components on different parts of the network.

Rather than attempting to accurately predict user traffic on the network and build networks to meet those demands, the building-block process instead

starts with a few standard components and uses them over and over again, even if they provide more capacity than is needed. The goal is simplicity of design. This strategy is sometimes called “narrow and deep” because a very narrow range of technologies and devices is used over and over again (very deeply throughout the organization). The results are a simpler design process and a more easily managed network built with a smaller range of components.

In this chapter, we focus on the building-block process to network design. The basic design process involves three steps that are performed repeatedly: needs analysis, technology design, and cost assessment ([Figure 11.1](#)). This process begins with **needs analysis**, during which the designer attempts to understand the fundamental current and future network needs of the various users, departments, and applications. This is likely to be an educated guess at best. Users and applications are classified as typical or high volume. Specific technology needs are identified (e.g., the ability to dial in with current modem technologies). The next step, **technology design**, examines the available technologies and assesses which options will meet users’ needs. The designer makes some estimates about the network needs of each category of user and circuit in terms of current technology (e.g., 100Base-T, 1000Base-T) and matches needs to technologies. Because the basic network design is general, it can easily be changed as needs and technologies change. The difficulty, of course, lies in predicting user demand so one can define the technologies needed. Most organizations solve this by building more capacity than they expect to need and by designing networks that can easily grow and then closely monitoring growth so they expand the network ahead of the growth pattern.

In the third step, **cost assessment**, the relative costs of the technologies are considered. The process then cycles back to the needs analysis, which is refined using the technology and cost information to produce a new assessment of users’ needs. This in turn triggers changes in the technology design and cost assessment and so on. By cycling through these three processes, the final network design is settled ([Figure 11.2](#)).

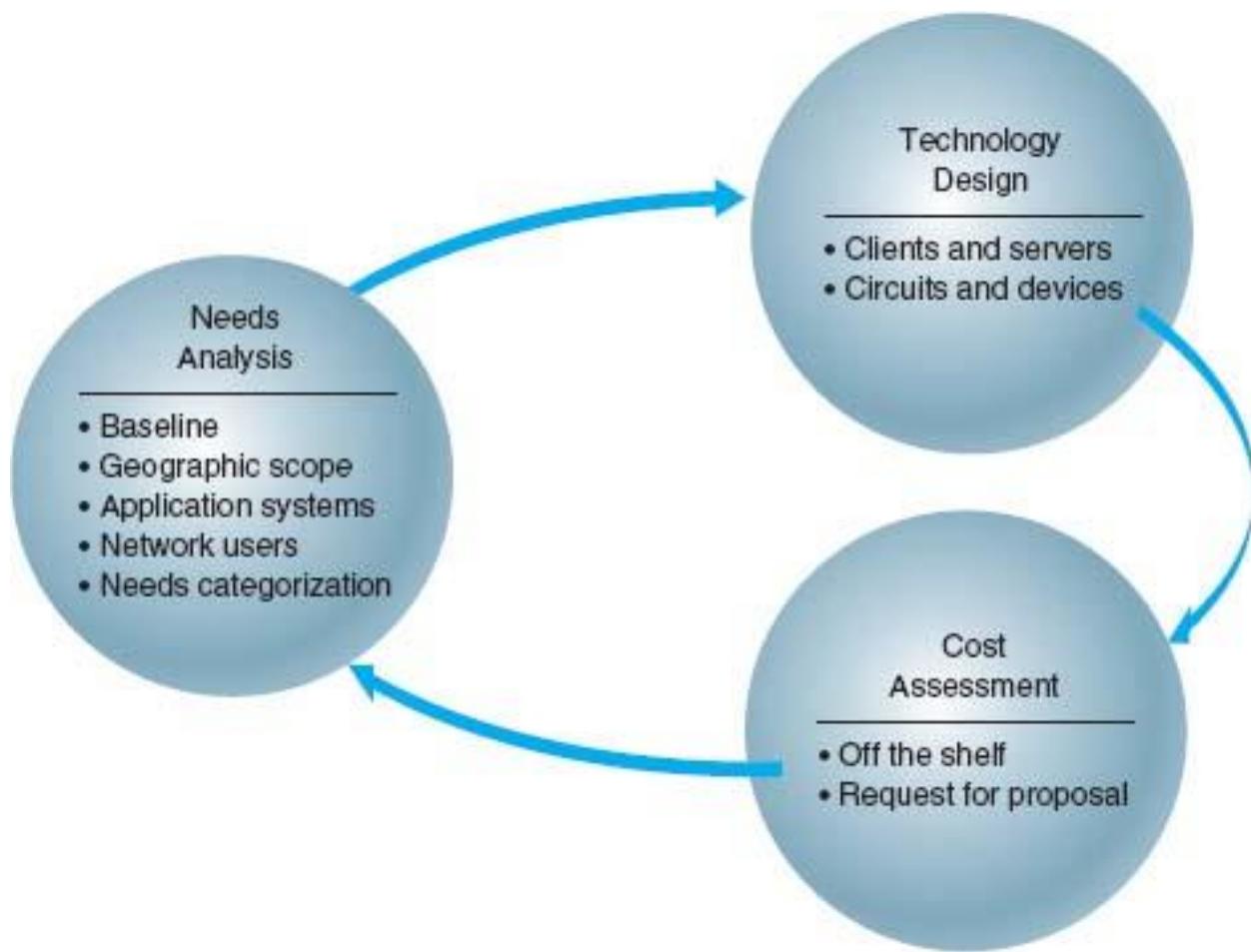


FIGURE 11.1 Network design

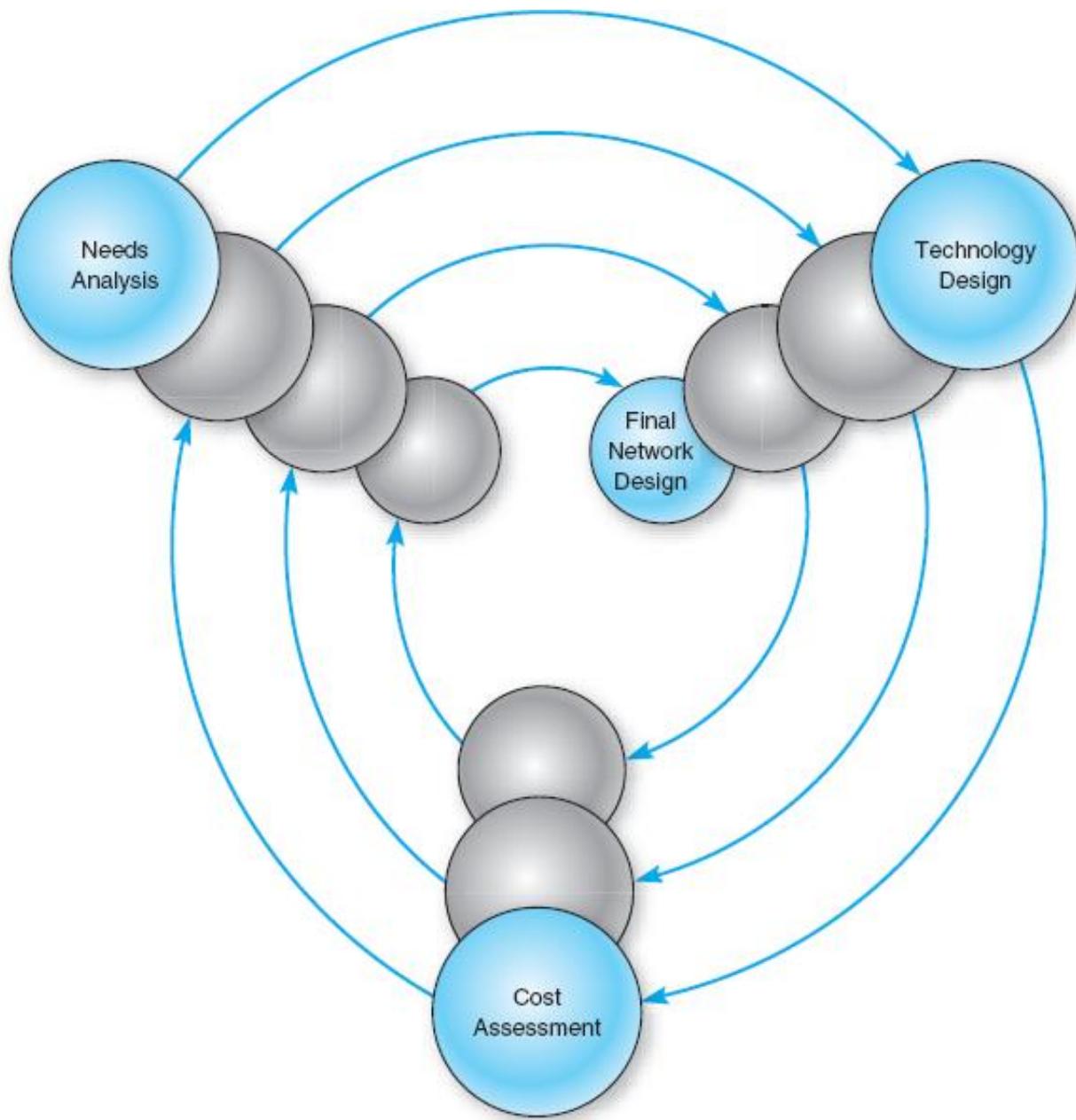


FIGURE 11.2 The cyclical nature of network design

11.2 NEEDS ANALYSIS

The goal of needs analysis is to understand why the network is being built and what users and applications it will support. In many cases, the network is being designed to improve poor performance or enable new applications to be used. In other cases, the network is upgraded to replace unreliable or aging equipment or to standardize equipment so that only one type of

equipment, one protocol (e.g., TCP/IP, Ethernet), or one vendor's equipment is used everywhere in the network.

Often, the goals in network design are slightly different between LANs and backbones (BNs) on the one hand and WANs on the other. In the LAN and BN environment, the organization owns and operates the equipment and the circuits. Once they are paid for, there are no additional charges for usage. However, if major changes must be made, the organization will need to spend additional funds. In this case, most network designers tend to err on the side of building too big a network—that is, building more capacity than they expect to need.

In contrast, in most WANs, the organization leases circuits from a common carrier and pays for them on a monthly or per-use basis. Understanding capacity becomes more important in this situation because additional capacity comes at a noticeable cost. In this case, most network designers tend to err on the side of building too small a network, because they can lease additional capacity if they need it—but it is much more difficult to cancel a long-term contract for capacity they are not using.

Much of the needs analysis may already have been done because most network design projects today are network upgrades rather than the design of entirely new networks. In this case, there is already a fairly good understanding of the existing traffic in the network and, most important, of the rate of growth of network traffic. It is important to gain an understanding of the current operations (application systems and messages). This step provides a **baseline** against which future design requirements can be gauged. It should provide a clear picture of the present sequence of operations, processing times, work volumes, current communication network (if one exists), existing costs, and user/management needs.

Whether the network is a new network or a network upgrade, the primary objective of this stage is to define (1) the **geographic scope** of the network and (2) the users and applications that will use it.

The goal of the needs analysis step is to produce a **logical network design**, which is a statement of the network elements needed to meet the needs of the organization. The logical design does not specify technologies or products to be used (although any specific requirements are noted).

Instead, it focuses on the fundamental functionality needed, such as a high-speed access network, which in the technology design stage will be translated into specific technologies (e.g., switched 100Base-T).

11.2.1 GEOGRAPHIC SCOPE

The first step in needs analysis is to break the network into three conceptual parts on the basis of their geographic and logical scope: the access layer, the distribution layer, and the core layer, as first discussed in [Chapter 7](#).¹ The **access layer** is the technology that is closest to the user—the user's first contact with the network—and is often a LAN or a broadband Internet connection. The **distribution layer** is the next part of the network that connects the access layer to the rest of the network, such as the BN(s) in a specific building. The **core layer** is the innermost part of the network that connects the different distribution-layer networks to each other, such as the primary BN on a campus or a set of WAN circuits connecting different offices together. As the name suggests, the core layer is usually the busiest, most important part of the network. Not all layers are present in all networks; small networks, for example, may not have a distribution layer because their core may be the BN that directly connects the parts of the access layer together.

Within each of these parts of the network, the network designer must then identify some basic technical constraints. For example, if the access layer is a WAN, in that the users need to connect to the network over a broadband connection, this provides some constraints on the technologies to be used; one usually could not use 100Base-T Ethernet, for example. Likewise, if the access layer is a LAN, it would be silly to consider using T1 circuits.

Sometimes, the current network infrastructure also imposes constraints. For example, if we are adding a new building to an existing office complex that used 100Base-T in the access-layer LANs, then we will probably choose to use 100Base-T for the access layer in the new building. All such constraints are noted.

It is easiest to start with the highest level, so most designers begin by drawing a network diagram for any WANs with international or countrywide

locations that must be connected. A diagram that shows the logical network going between the locations is sufficient. Details such as the type of circuit and other considerations will be added later. Next, the individual locations connected to the WAN are drawn, usually in a series of separate diagrams, but for a simple network, one diagram may be sufficient.

At this point, the designers gather general information and characteristics of the environment in which the network must operate. For example, they determine whether there are any legal requirements, such as local, state/provincial, federal, or international laws, regulations, or building codes, that might affect the network.

Figure 11.3 shows the initial drawing of a network design for an organization with offices in four areas connected to the core network, which is a WAN. The Toronto location, for example, has a distribution layer (a BN) connecting three distinct access-layer LANs, which could be three distinct LANs in the same office building. Chicago has a similar structure, with the addition of a fourth access part that connects to the Internet; that is, the organization has only one Internet connection, so all Internet traffic must be routed through the core network to the Chicago location. The Atlantic Canada network section has two distinct access layer parts; one is a LAN and one access layer is a WAN (e.g., DSL). The New York network section is more complex, having its own core network component (a BN connected into the core WAN), which in turn supports three distribution-layer BNs. Each of these support several access-layer LANs.

11.2.2 APPLICATION SYSTEMS

Once the basic geographic scope is identified, the designers must review the list of applications that will use the network and identify the location of each. This information should be added to the emerging network diagrams. This process is called *baselining*. Next, those applications that are expected to use the network in the future are added.

In many cases, the applications will be relatively well defined. Specific internal applications (e.g., payroll) and external applications (e.g., Web servers) may already be part of the “old” network. However, it is important to review the organization’s long-range and short-range plans concerning

changes in company goals, strategic plans, development plans for new products or services, projections of sales, research and development projects, major capital expenditures, possible changes in product mix, new offices that must be served by the communications network, security issues, and future commitments to technology. For example, a major expansion in the number of offices or a major electronic commerce initiative will have a significant impact on network requirements.

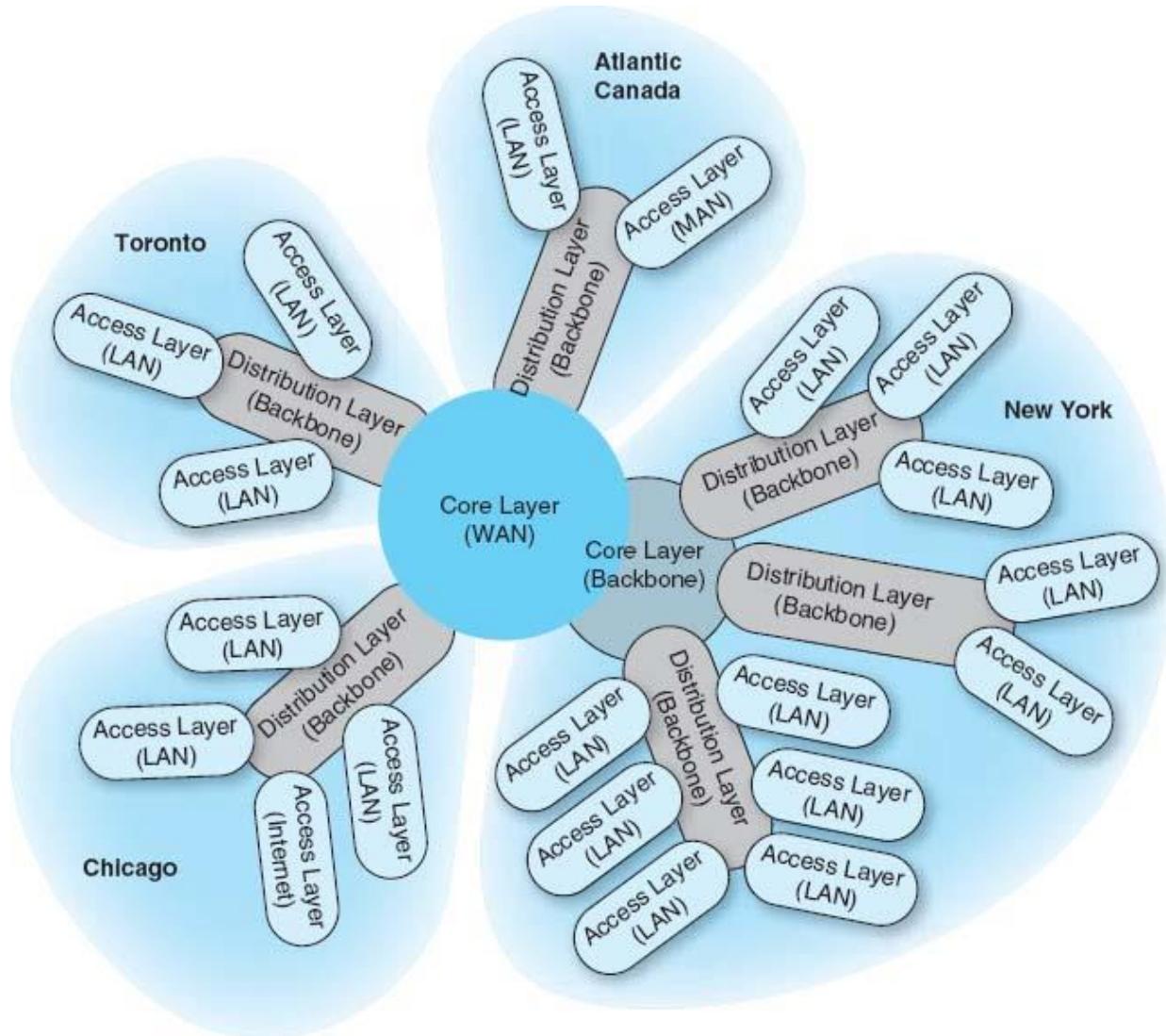


FIGURE 11.3 Geographic scope. LAN = local area network; MAN = metropolitan area network; WAN = wide area network

It also is helpful to identify the hardware and software requirements of each application that will use the network and, if possible, the protocol each application uses (e.g., HTTP over TCP/IP, Windows file access). This

knowledge helps now and will be particularly useful later when designers develop technological solutions.

11.2.3 NETWORK USERS

In the past, application systems accounted for the majority of network traffic. Today, much network traffic is produced by the discretionary use of the Internet. Applications such as email and the Web are generating significant traffic, so the network manager is no longer in total control of the network traffic generated on his or her networks. This is likely to continue in the future as network-hungry applications such as desktop videoconferencing become more common. Therefore, in addition to understanding the applications, you must also assess the number and type of users that will generate and receive network traffic and identify their location on the emerging network diagram.

11.2.4 CATEGORIZING NETWORK NEEDS

At this point, the network has been designed in terms of geographic scope, application systems, and users. The next step is to assess the relative amount of traffic generated in each part of the network. With the traditional design approach, this involves considerable detailed analysis. With the building-block approach, the goal is to provide some rough assessment of the relative magnitude of network needs. Each application system is assessed in general terms to determine the amount of network traffic it can be expected to generate today and in the future, compared with other applications. Likewise, each user is categorized as either a typical user or a high-traffic user. These assessments will be refined in the next stage of the design process.

This assessment can be problematic, but the goal is some relative understanding of the network needs. Some simple rules of thumb can help. For example, applications that require large amounts of multimedia data or those that load executables over the network are likely to be high-traffic applications. Applications that are time sensitive or need constant updates (e.g., financial information systems, order processing) are likely to be high-traffic applications.

Once the network requirements have been identified, they also should be organized into **mandatory requirements**, **desirable requirements**, and **wish-list requirements**. This information enables the development of a minimum level of mandatory requirements and a negotiable list of desirable requirements that are dependent on cost and availability. For example, desktop videoconferencing may be a wish-list item, but it will be omitted if it increases the cost of the network beyond what is desired.

At this point, the local facility network diagrams are prepared. For a really large network, there may be several levels. For example, the designer of the network in [Figure 11.3](#) might choose to draw another set of diagrams, one each for Toronto, Chicago, Atlantic Canada, and New York.

Conversely, the designer might just add more detail to and develop separate, more detailed diagrams for New York. The choice is up to the designer, provided the diagrams and supporting text clearly explain the network's needs.

11.2.5 DELIVERABLES

The key deliverable for the needs assessments stage is a set of logical network diagrams, showing the applications, circuits, clients, and servers in the proposed network, each categorized as either typical or high traffic. The logical diagram is the conceptual plan for the network and does not consider the specific physical elements (e.g., routers, switches, circuits) that will be used to implement the network.

[Figure 11.4](#) shows the results of a needs assessment for one of the New York parts of the network from [Figure 11.3](#). This figure shows the distribution and access parts in the building with the series of six access LANs connected by one distribution BN, which is in turn connected to a campus-area core BN. One of the six LANs is highlighted as a high-traffic LAN, whereas the others are typical. Three mandatory applications are identified that will be used by all network users: email, Web, and file sharing. One wish-list requirement (desktop videoconferencing) is also identified for a portion of the network.

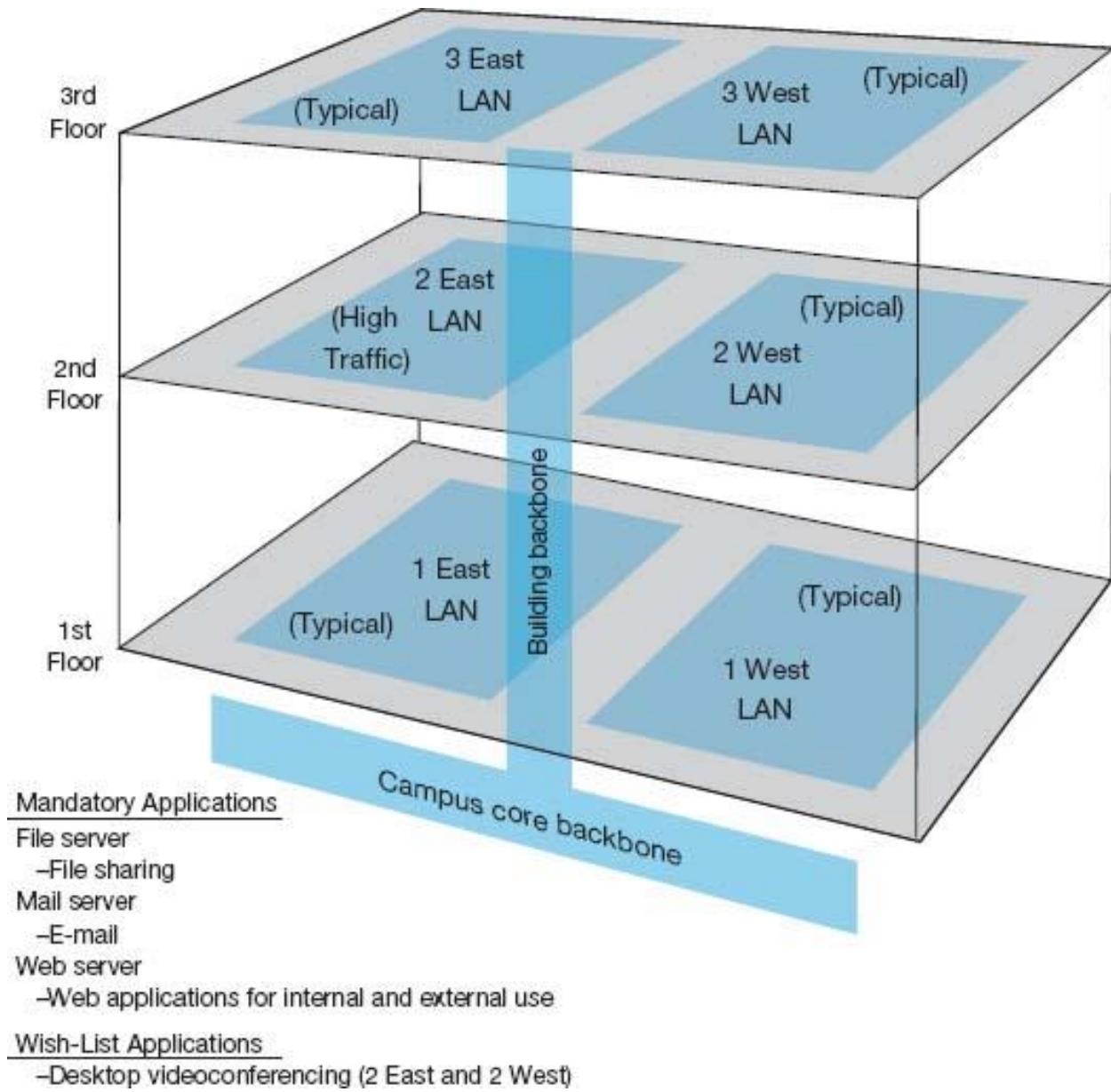


FIGURE 11.4 Sample needs assessment. LAN = local area network

11.3 TECHNOLOGY DESIGN

Once the needs have been defined in the logical network design, the next step is to develop a **physical network design** (or set of possible designs). The physical network design starts with the client and server computers needed to support the users and applications. If the network is a new network, new computers will need to be purchased. If the network is an existing network, the servers may need to be upgraded to the newest

technology. Once these are designed, then the circuits and devices connecting them are designed.

11.3.1 DESIGNING CLIENTS AND SERVERS

The idea behind the building-block approach is to specify needs in terms of some standard units. Typical users are allocated the base-level client computers, as are servers supporting typical applications. Users and servers for applications needing more powerful computers are assigned some advanced computer. As the specifications for computers rapidly improve and costs drop (usually every six months), today's typical user may receive the type of computer originally intended for the advanced user when the network is actually implemented, and the advanced users may end up with a computer not available when the network was designed.

11.3.2 DESIGNING CIRCUITS AND DEVICES

The same is true for network circuits and devices (e.g., hubs, routers, switches). There are two interrelated decisions in designing network circuits and devices: the fundamental technology and protocols (e.g., Ethernet, T1, TCP/IP) and the capacity of each circuit (e.g., 100 Mbps, 1000 Mbps). These are interrelated, because each technology offers different circuit capacities.

Designing the circuit capacity means **capacity planning**, estimating the size and type of the standard and advanced network circuits for each type of network (LAN, BN, WAN). For example, should the standard LAN circuit be shared or switched 100Base-T? Likewise, should the standard BN circuit be 100Base-T or 1GbE?

This requires some assessment of the current and future **circuit loading** (the amount of data transmitted on a circuit). This analysis can focus on either the *average* circuit traffic or the *peak* circuit traffic. For example, in an online banking network, traffic volume peaks usually are in the midmorning (bank opening) and just prior to closing. Airline and rental car reservations network designers look for peak volumes before and during holidays or other vacation periods whereas telephone companies normally have their

highest peak volumes on Mother's Day. Designing for peak circuit traffic is the ideal.

The designer usually starts with the total characters transmitted per day on each circuit or, if possible, the maximum number of characters transmitted per two-second interval if peaks must be met. You can calculate message volumes by counting messages in a current network and applying some estimated growth rate. If an existing network is in place, network monitors/analyzers (see [Chapter 12](#)) may be able to provide an actual circuit character count of the volume transmitted per minute or per day.

A good rule of thumb is that 80 percent of this circuit loading information is easy to gather. The last 20 percent needed for very precise estimates is extremely difficult and expensive to find. However, precision usually is not a major concern because of the staircase nature of communication circuits and the need to project future needs. For example, the difference between 100Base-T and 1GbE is quite large, and assessing which level is needed for typical traffic does not require a lot of precision. Forecasts are inherently less precise than understanding current network traffic. The **turnpike effect** is an expression that means that traffic increases much faster than originally forecast. It comes from the traffic forecasting that was done for the construction of the early interstate highways. When a new, faster highway (or network) is built, people are more likely to use it than the old slow one because it is available, is very efficient, and provides new capabilities. The annual growth factor for network use may vary from 5 to 50 percent and, in some cases, may exceed 100 percent for high-growth organizations.

Although no organization wants to overbuild its network and pay for more capacity than it needs, in most cases, upgrading a network costs 50 to 80 percent more than building it right the first time. Few organizations complain about having too much network capacity, but being under capacity can cause significant problems. Given the rapid growth in network demand and the difficulty in accurately predicting it, most organizations intentionally overbuild (build more capacity into their network than they plan to use), and most end up using this supposedly unneeded capacity within 3 years.

11.3.3 NETWORK DESIGN TOOLS

Network modeling and design tools can perform a number of functions to help in the technology design process. With most tools, the first step is to enter a diagram or model of the existing network or proposed network design. Some modeling tools require the user to create the network diagram from scratch. That is, the user must enter all of the network components by hand, placing each server, client computer, and circuit on the diagram and defining what each is (e.g., 10Base-T, frame relay circuit with a 1-Mbps committed information rate).

Other tools can “discover” the existing network; that is, once installed on the network, they will explore the network to draw a network diagram. In this case, the user provides some starting point, and the modeling software explores the network and automatically draws the diagram itself. Once the diagram is complete, the user can then change it to reflect the new network design. Obviously, a tool that can perform network discovery by itself is most helpful when the network being designed is an upgrade to an existing network and when the network is very complex.

Once the diagram is complete, the next step is to add information about the expected network traffic and see if the network can support the level of traffic that is expected. **Simulation**, a mathematical technique in which the network comes to life and behaves as it would under real conditions, is used to model the behavior of the communication network. Applications and users generate and respond to messages while the simulator tracks the number of packets in the network and the delays encountered at each point in the network.

Simulation models may be tailored to the users' needs by entering parameter values specific to the network at hand (e.g., this computer will generate an average of three 100-byte packets per minute). Alternatively, the user may prefer to rely primarily on the set of average values provided by the network.

Once the simulation is complete, the user can examine the results to see the estimated response times throughout. It is important to note that these network design tools provide only estimates, which may vary from the actual results. At this point, the user can change the network design in an

attempt to eliminate bottlenecks and rerun the simulation. Good modeling tools not only produce simulation results but also highlight potential trouble spots (e.g., servers, circuits, or devices that experienced long response times). The very best tools offer suggestions on how to overcome the problems that the simulation identified (e.g., network segmentation, increasing from T1 to T3).

11.3.4 DELIVERABLES

The key deliverable is a set of one or more physical network designs. Most designers like to prepare several physical designs so they can trade off technical benefits (e.g., performance) against cost. In most cases, the critical part is the design of the network circuits and devices. In the case of a new network designed from scratch, it is also important to define the client computers with care because these will form a large portion of the total cost of the network. Usually, however, the network will replace an existing network and only a few of the client computers in the existing network will be upgraded.

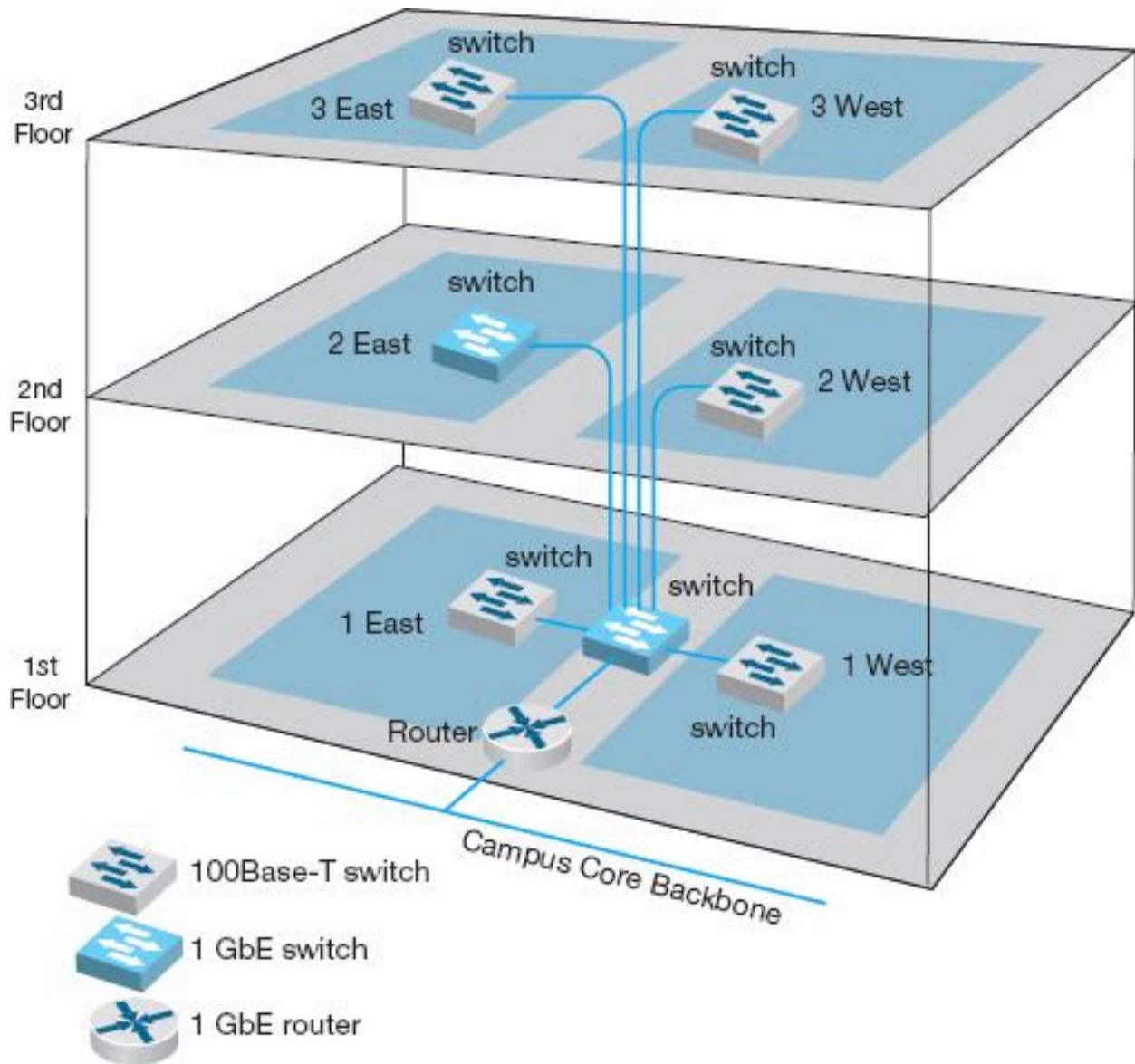


FIGURE 11.5 Physical network design

Figure 11.5 shows a physical network design for the simple network in Figure 11.4. In this case, a 1GbE collapsed backbone is used in the distribution layer, and switched 100Base-T Ethernet has been chosen as the standard network for typical users in the access layer. High-traffic users (2 East) will use 1GbE. The building backbone will be connected directly into the campus backbone using a router and will use fiber-optic cable to enable the possible future addition of desktop videoconferencing.

11.4 COST ASSESSMENT

The purpose of this step is to assess the costs of various physical network design alternatives produced in the previous step. The main items are the costs of software, hardware, and circuits. These three factors are all interconnected and must be considered along with the performance and reliability required. All factors are interrelated with regard to cost.

Estimating the cost of a network is quite complex because many factors are not immediately obvious. Some of the costs that must be considered are

- Circuit costs, including costs of circuits provided by common carriers or the cost of purchasing and installing your own cable
- Internetworking devices such as switches and routers
- Hardware costs, including server computers, NICs, hubs, memory, printers, uninterruptible power supplies, and backup tape drives
- Software costs for network operating system, application software, and middleware
- Network management costs, including special hardware, software, and training needed to develop a network management system for ongoing redesign, monitoring, and diagnosing of problems
- Test and maintenance costs for special monitoring equipment and software, plus the cost of onsite spare parts
- Costs to operate the network

11.4.1 REQUEST FOR PROPOSAL

Although some network components can be purchased off the shelf, most organizations develop a **request for proposal (RFP)** before making large network purchases. RFPs specify what equipment, software, and services are desired and ask vendors to provide their best prices. Some RFPs are very specific about what items are to be provided in what time frame. In other cases, items are defined as mandatory, important, or desirable, or several scenarios are provided and the vendor is asked to propose the best solution. In a few cases, RFPs specify generally what is required and the vendors are asked to propose their own network designs. Figure 11.6 provides a summary of the key parts of an RFP.

Once the vendors have submitted their proposals, the organization evaluates them against specified criteria and selects the winner(s). Depending on the scope and complexity of the network, it is sometimes necessary to redesign the network on the basis of the information in the vendors' proposals.

One of the key decisions in the RFP process is the scope of the RFP. Will you use one vendor or several vendors for all hardware, software, and services? Multivendor environments tend to provide better performance because it is unlikely that one vendor makes the best hardware, software, and services in all categories. Multivendor networks also tend to be less expensive because it is unlikely that one vendor will always have the cheapest hardware, software, and services in all product categories.

Multivendor environments can be more difficult to manage, however. If equipment is not working properly and it is provided by two different vendors, each can blame the other for the problem. In contrast, a single vendor is solely responsible for everything.

11.4.2 SELLING THE PROPOSAL TO MANAGEMENT

One of the main problems in network design is obtaining the support of senior management. To management, the network is simply a cost center, something on which the organization is spending a lot of money with little apparent change. The network keeps on running just as it did the year before.

The key to gaining the acceptance of senior management lies in speaking management's language. It is pointless to talk about upgrades from 100 Mbps to 1GbE on the backbone because this terminology is meaningless from a business perspective. A more compelling argument is to discuss the growth in network use. For example, a simple graph that shows network usage growing at 25 percent per year, compared with network budget growing at 10 percent per year, presents a powerful illustration that the network costs are well managed, not out of control.

Information In a Typical Request for Proposal

- Background information
 - Organizational profile
 - Overview of current network
 - Overview of new network
 - Goals of new network
- Network requirements
 - Choice sets of possible network designs (hardware, software, circuits)
 - Mandatory, desirable, and wish-list items
 - Security and control requirements
 - Response-time requirements
 - Guidelines for proposing new network designs
- Service requirements
 - Implementation time plan
 - Training courses and materials
 - Support services (e.g., spare parts on site)
 - Reliability and performance guarantees
- Bidding process
 - Time schedule for the bidding process
 - Ground rules
 - Bid evaluation criteria
 - Availability of additional information
- Information required from vendor
 - Vendor corporate profile
 - Experience with similar networks
 - Hardware and software benchmarks
 - Reference list

FIGURE 11.6 Request for proposal

Likewise, a focus on network reliability is an easily understandable issue. For example, if the network supports a mission-critical system such as order processing or moving point-of-sale data from retail stores to corporate offices, it is clear from a business perspective that the network

must be available and performing properly, or the organization will lose revenue.

11.4.3 DELIVERABLES

There are three key deliverables for this step. The first is an RFP that goes to potential vendors. The second deliverable, after the vendor has been selected, is the revised physical network diagram (e.g., [Figure 11.5](#)) with the technology design complete. Exact products and costs are specified at this point (e.g., a 16-port 100Base-T switch). The third deliverable is the business case that provides support for the network design, expressed in business objectives.

11.5 DESIGNING FOR NETWORK PERFORMANCE

At the end of the previous chapters we have discussed the best practice design for LANs, backbones, WANs, and WLANs and examined how different technologies and services offered different effective data rates at different costs. In the backbone and WAN chapters we also examined different topologies and contrasted the advantages and disadvantages of each. So at this point, you should have a good understanding of the best choices for technologies and services and how to put them together into a good network design. In this section, we examine several higher-level concepts used to design the network for the best performance.

11.5.1 MANAGED NETWORKS

The single most important element that contributes to the performance of a network is a **managed network** that uses **managed devices**. Managed devices are standard devices, such as switches and routers, that have small onboard computers to monitor traffic flows through the device as well as the status of the device and other devices connected to it. Managed devices perform their functions (e.g., routing, switching) and also record data on the messages they process. These data can be sent to the network manager's computer when the device receives a special control message requesting the data, or the device can send an **alarm** message to the

network manager's computer if it detects a critical situation such as a failing device or a huge increase in traffic.

In this way, network problems can be detected and reported by the devices themselves before problems become serious. In the case of the failing network card, a managed device could record the increased number of retransmissions required to successfully transmit messages and inform the network management software of the problem. A managed hub or switch might even be able to detect the faulty transmissions from a failing network card, disable the incoming circuit so that the card could not send any more messages, and issue an alarm to the network manager. In either case, finding and fixing problems is much simpler, requiring minutes not hours.

Network Management Software A managed network requires both hardware and software: hardware to monitor, collect, and transmit traffic reports and problem alerts, and network management software to store, organize, and analyze these reports and alerts. There are three fundamentally different types of network management software.

Device management software (sometimes called *point management software*) is designed to provide information about the specific devices on a network. It enables the network-manager to monitor important devices such as servers, routers, and gateways, and typically report configuration information, traffic volumes, and error conditions for each device. Figure 11.7 shows some sample displays from a device management package running at Indiana University. This figure shows the amount of traffic in terms of inbound traffic (light gray area) and outbound traffic (dark gray line) over several network segments. The monthly graph shows, for example, that inbound traffic maxed out the resnet T3 circuit in week 18.

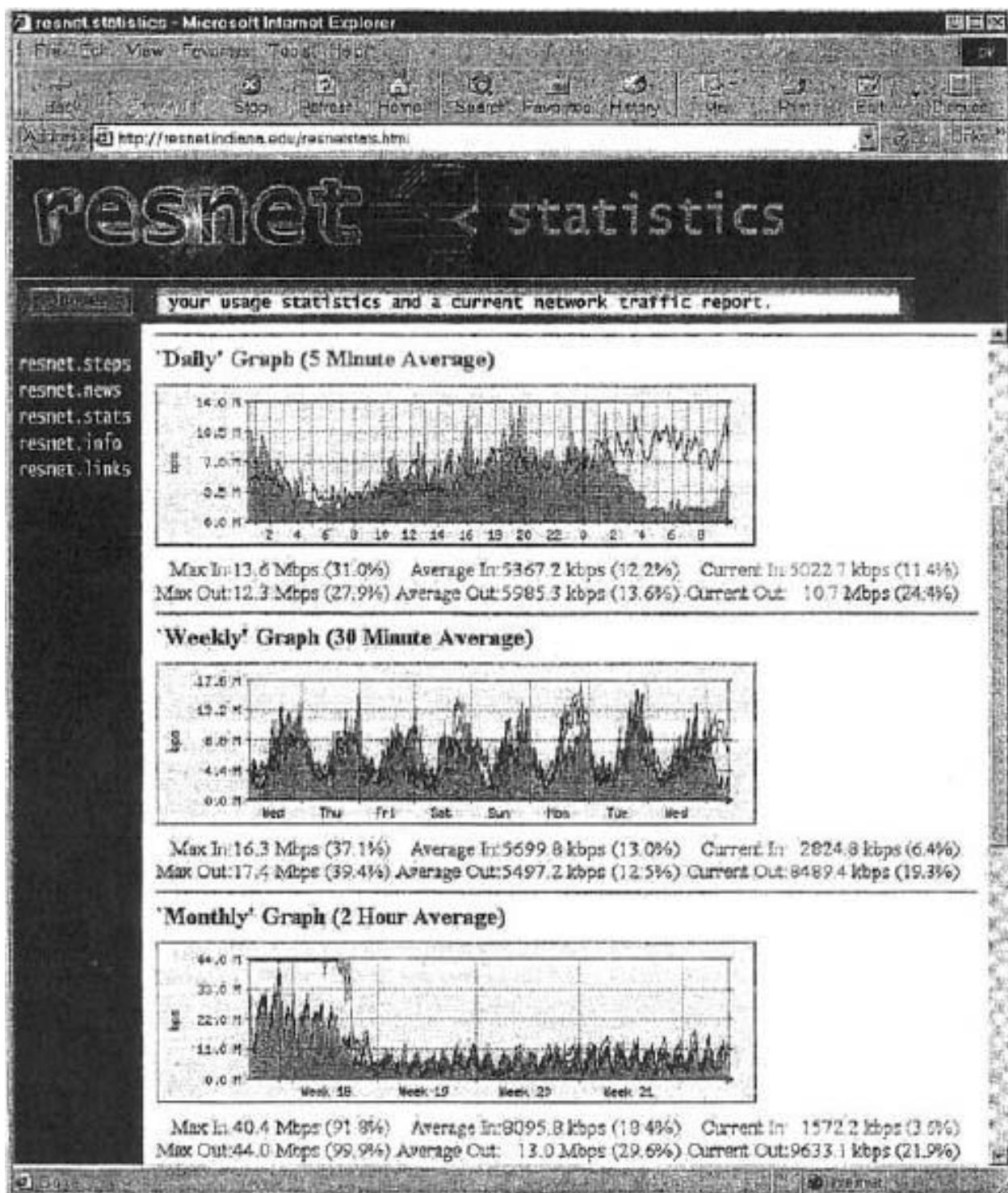


FIGURE 11.7 Device management software

System management software (sometimes called *enterprise management software* or a *network management framework*) provides the same configuration, traffic, and error information as device management systems, but can analyze the device information to diagnose patterns, not

just display individual device problems. This is important when a critical device fails (e.g., a router into a high-traffic building). With device management software, all of the devices that depend on the failed device will attempt to send warning messages to the network administrator. One failure often generates several dozen problem reports, called an **alarm storm**, making it difficult to pinpoint the true source of the problem quickly. The dozens of error messages are symptoms that mask the root cause. System management software tools correlate the individual error messages into a pattern to find the true cause, which is called **root cause analysis**, and then report the pattern to the network manager. Rather than first seeing pages and pages of error messages, the network manager instead is informed of the root cause of the problem. Figure 11.8 shows a sample from HP.

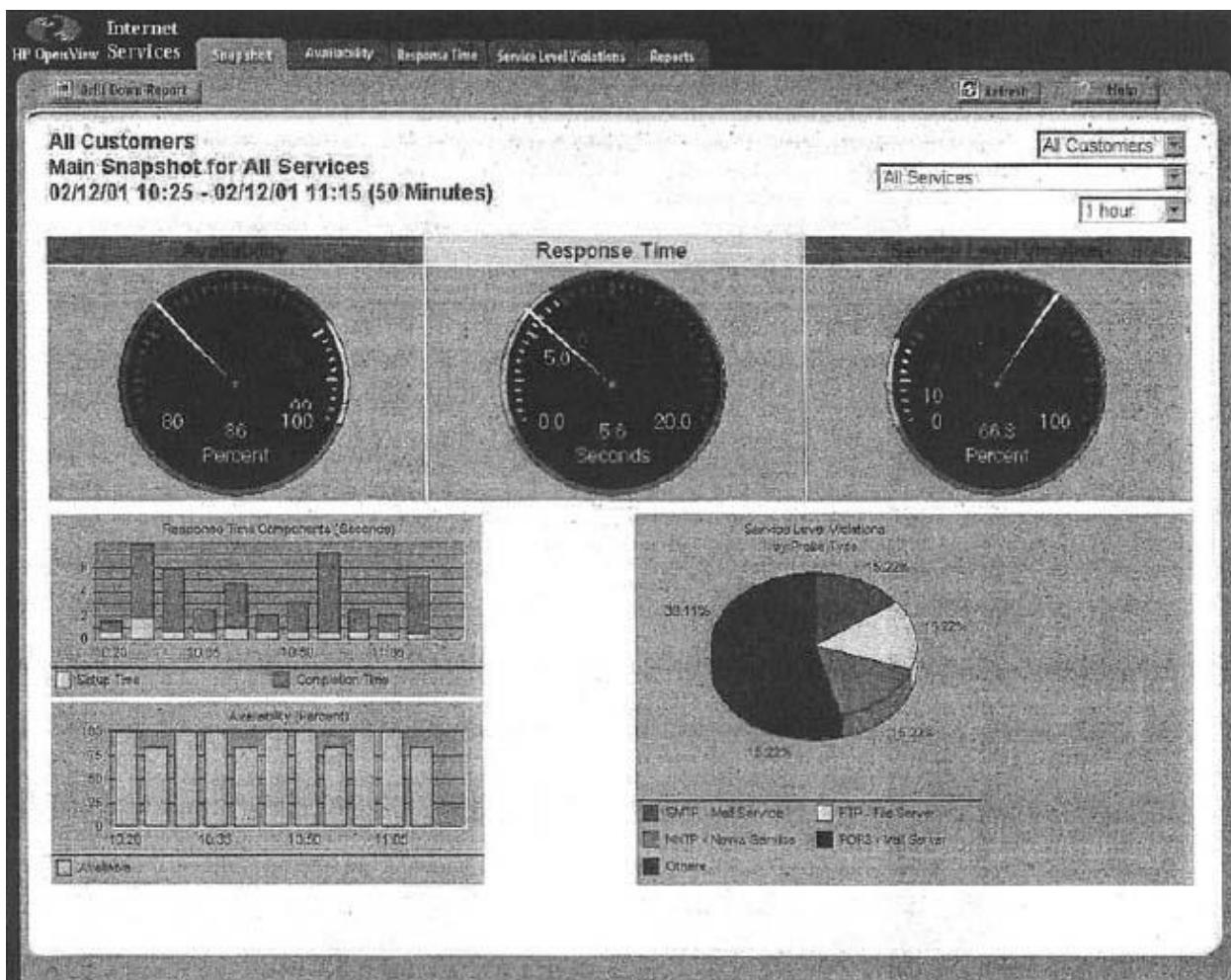


FIGURE 11.8 Network management software

Source: HP OpenView

Application management software also builds on the device management software, but instead of monitoring systems, it monitors applications. In many organizations, there are mission-critical applications that should get priority over other network traffic. For example, real-time order-entry systems used by telephone operators need priority over email. Application management systems track delays and problems with application layer packets and inform the network manager if problems occur.

Network Management Standards One important problem is ensuring that hardware devices from different vendors can understand and respond to the messages sent by the network management software of other vendors. By this point in this book, the solution should be obvious: standards. A number of formal and de facto standards have been developed for network management. These standards are application layer protocols that define the type of information collected by network devices and the format of control messages that the devices understand.

The two most commonly used network management protocols are **Simple Network Management Protocol (SNMP)** and **Common Management Interface Protocol (CMIP)**. Both perform the same basic functions but are incompatible. SNMP is the Internet network management standard, whereas CMIP is a newer protocol for OSI-type networks developed by the ISO. SNMP is the most commonly used today although most of the major network management software tools understand both SNMP and CMIP and can operate with hardware that uses either standard.

Originally, SNMP was developed to control and monitor the status of network devices on TCP/IP networks, but it is now available for other network protocols (e.g., IPX/SPX). Each SNMP device (e.g., router, gateway, server) has an **agent** that collects information about itself and the messages it processes and stores that information in a central database called the **management information base (MIB)**. The network manager's management station that runs the **network management software** has access to the MIB. Using this software, the network manager can send

control messages to individual devices or groups of devices asking them to report the information stored in their MIB.

Most SNMP devices have the ability for **remote monitoring (RMON)**. Most first-generation SNMP tools reported all network monitoring information to one central network management database. Each device would transmit updates to its MIB on the server every few minutes, greatly increasing network traffic. RMON SNMP software enables MIB information to be stored on the device itself or on distributed **RMON probes** that store MIB information closer to the devices that generate it. The data are not transmitted to the central server until the network manager requests, thus reducing network traffic (Figure 11.9).

Network information is recorded based on the data link layer protocols, network layer protocols, and application layer protocols, so that network managers can get a very clear picture of the exact types of network traffic. Statistics are also collected based on network addresses so the network manager can see how much network traffic any particular computer is sending and receiving. A wide variety of alarms can be defined, such as instructing a device to send a warning message if certain items in the MIB exceed certain values (e.g., if circuit utilization exceeds 50 percent).

As the name suggests, SNMP is a simple protocol with a limited number of functions. One problem with SNMP is that many vendors have defined their own extensions to it. So the network devices sold by a vendor may be SNMP compliant, but the MIBs they produce contain additional information that can be used only by network management software produced by the same vendor. Therefore, while SNMP was designed to make it easier to manage devices from different vendors, in practice this is not always the case.

Policy-Based Management With **policy-based management**, the network manager uses special software to set priority policies for network traffic that take effect when the network becomes busy. For example, the network manager might say that order processing and videoconferencing get the highest priority (order processing because it is the lifeblood of the company and videoconferencing because poor response time will have the greatest impact on it). The policy management software would then configure the

network devices using the quality of service (QoS) capabilities in TCP/IP and/or ATM and/or its VLANs to give these applications the highest priority when the devices become busy.

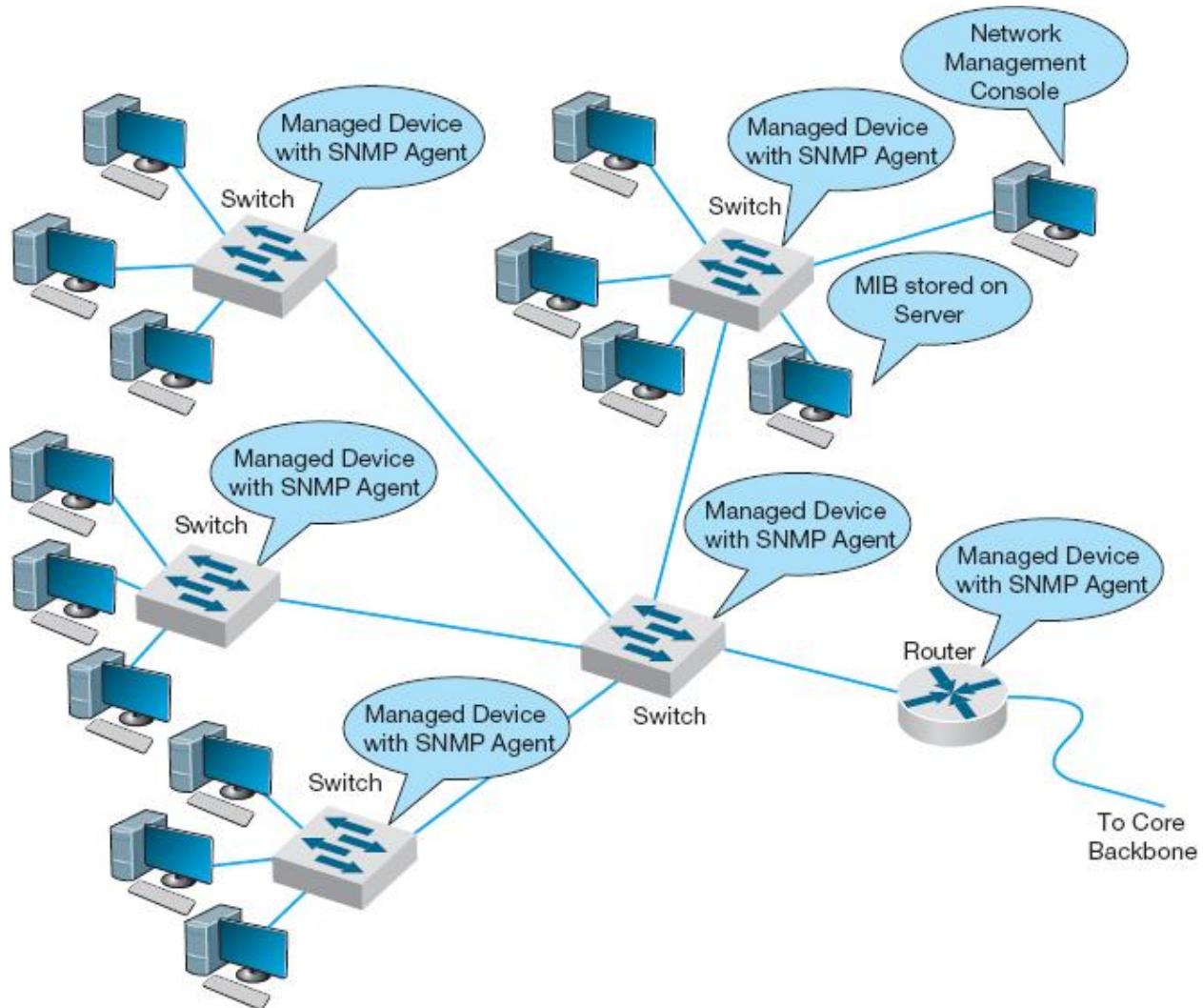


FIGURE 11.9 Network Management with Simple Network Management Protocol (SNMP).
MIB = management information base

11.5.2 NETWORK CIRCUITS

In designing a network for maximum performance, it is obvious that the network circuits play a critical role, whether they are under the direct control of the organization itself (in the case of LANs, backbones, and WLANs) or leased as services from common carriers (in the case of WANs). Sizing the circuits and placing them to match traffic patterns is important. We discussed circuit loading and capacity planning in the earlier sections. In

this section we also consider traffic analysis and service level agreements, which are primarily important for WANs, because circuits are most important in these networks in which you pay for network capacity.

Traffic Analysis In managing a network and planning for network upgrades, it is important to know the amount of traffic on each network circuit to find which circuits are approaching capacity. These circuits then can be upgraded to provide more capacity and less-used circuits can be downgraded to save costs. A more sophisticated approach involves a **traffic analysis** to pinpoint *why* some circuits are heavily used.

11.2 NETWORK MANAGEMENT AT ZF LENKSYSTEME

MANAGEMENT FOCUS

ZF Lenksysteme manufactures steering systems for cars and trucks. It is headquartered in southern Germany but has offices and plants in France, England, the United States, Brazil, India, China, and Malaysia. Its network has about 300 servers and 600 devices (e.g., routers, switches).

ZF Lenksysteme had a network management system, but when a problem occurred with one device, nearby devices also issued their own alarms. The network management software did not recognize the interactions among the devices and the resulting alarm storm meant that it took longer to diagnose the root cause of the problem.

The new HP network management system monitors and controls the global network from one central location with only three staff. All devices and servers are part of the system, and interdependencies are well defined, so alarm storms are a thing of the past. The new system has cut costs by 50 percent and also has extended network management into the production line. The robots on the production line now use TCP/IP networking, so they can be monitored like any other device.

SOURCE: ZF Lenksysteme, HP Case studies, hp.com. 2010.

For example, [Figure 11.10](#) shows the same partial mesh WAN we showed in [Chapter 8](#). Suppose we discover that the circuit from Toronto to Dallas is heavily used.

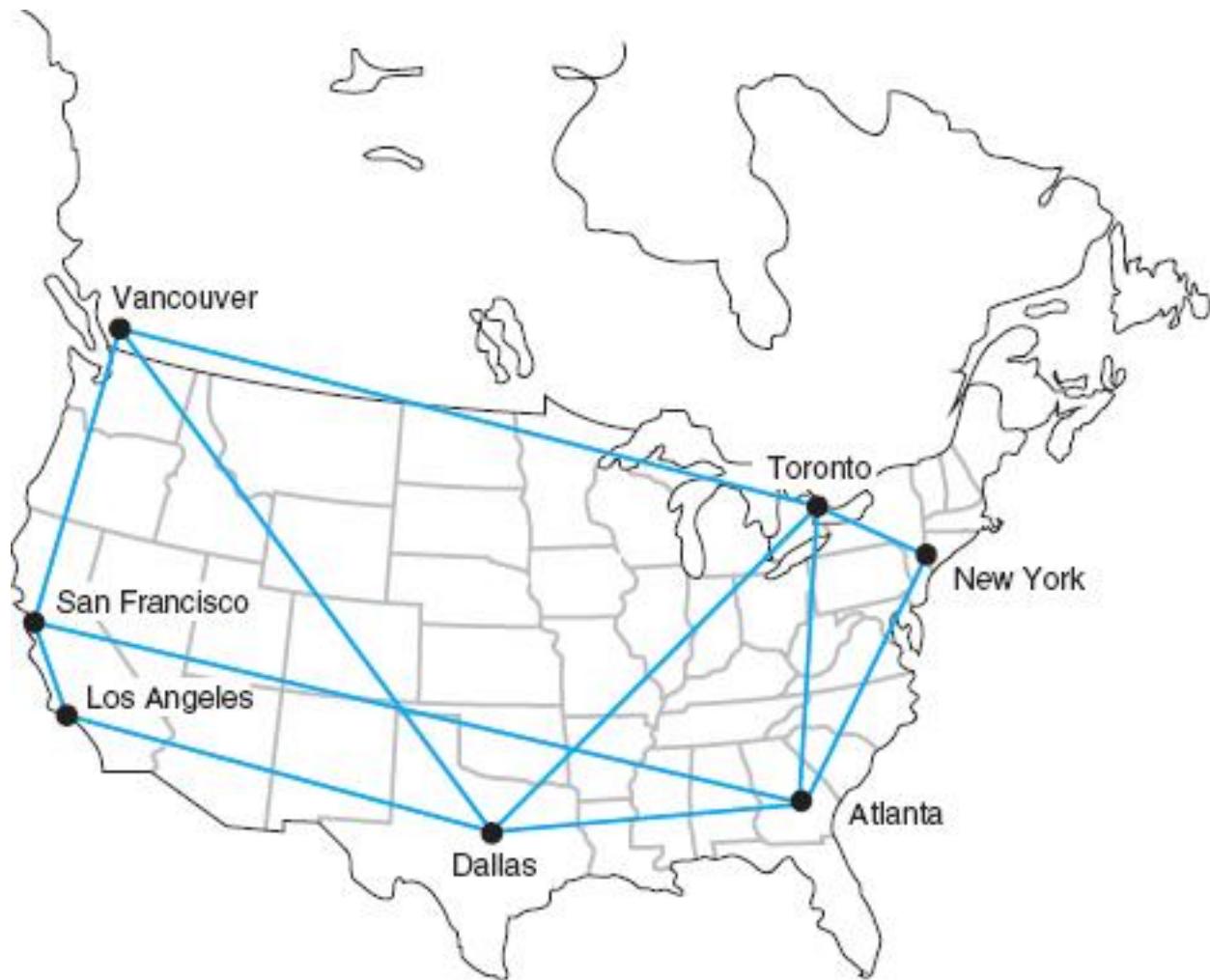


FIGURE 11.10 Sample wide area network

The immediate reaction might be to upgrade this circuit from a T1 to a T3. However, much traffic on this circuit may not originate in Toronto or be destined for Dallas. It may, for example, be going from New York to Los Angeles, in which case the best solution is a new circuit that directly connects them, rather than upgrading an existing circuit. The only way to be sure is to perform a traffic analysis to see the source and destination of the traffic.

Service Level Agreements Most organizations establish a **service-level agreement (SLA)** with their common carrier and Internet service provider.

An SLA specifies the exact type of performance that the common carrier will provide and the penalties if this performance is not provided. For example, the SLA might state that circuits must be available 99 percent or 99.9 percent of the time. A 99 percent availability means, for example, that the circuit can be down 3.65 days per year with no penalty, while 99.9 percent means 8.76 hours per year. In many cases, SLA includes maximum allowable response times. Some organizations are also starting to use an SLA internally to clearly define relationships between the networking group and its organizational “customers.”

11.5.3 NETWORK DEVICES

In previous chapters, we have treated the devices used to build the network as commodities. We have talked about 100Base-T switches and routers as though all were the same. This not true; in the same way that computers from different manufacturers provide different capabilities, so too do network devices. Some devices are simply faster or more reliable than similar devices from other manufacturers. In this section we examine four factors important in network performance: device latency, device memory, load balancing, and capacity management.

Device Latency **Latency** is the delay imposed by the device in processing messages. A high-latency device is one that takes a long time to process a message, whereas a low-latency device is fast. The type of computer processor installed in the device affects latency. The fastest devices run at **wire speed**, which means they operate as fast as the circuits they connect and add virtually no delays.

For networks with heavy traffic, latency is a critical issue because any delay affects all packets that move through the device. If the device does not operate at wire speed, then packets arrive faster than the device can process them and transmit them on the outgoing circuits. If the incoming circuit is operating at close to capacity, then this will result in long traffic backups in the same way that long lines of traffic form at tollbooths on major highways during rush hour.

Latency is less important in low-traffic networks because packets arrive less frequently and long lines seldom build up even if the device cannot

process all packets that the circuits can deliver. The actual delay itself—usually a few microseconds—is not noticeable by users.

Device Memory Memory and latency go hand-in-hand. If network devices do not operate at wire speed, this means that packets can arrive faster than they can be processed. In this case, the device must have sufficient memory to store the packets. If there is not enough memory, then packets are simply lost and must be retransmitted—thus increasing traffic even more. The amount of memory needed is directly proportional to the latency (slower devices with higher latencies need more memory).

Memory is also important for servers whether they are Web servers or file servers. Memory is many times faster than hard disks so Web servers and file servers usually store the most frequently requested files in memory to decrease the time they require to process a request. The larger the memory that a server has, the more files it can store in memory and the more likely it is to be able to process a request quickly. In general, it is always worthwhile to have the greatest amount of memory practical in Web and file servers.

Load Balancing In all large-scale networks today, servers are placed together in **server farms** or **clusters**, which sometimes have hundreds of servers that perform the same task. Yahoo.com, for example, has hundreds of Web servers that do nothing but respond to Web search requests. In this case, it is important to ensure that when a request arrives at the server farm, it is immediately forwarded to a server that is not busy—or is the least busy.

A special device called a **load balancing switch** or **virtual server** acts as a router at the front of the server farm ([Figure 11.11](#)). All requests are directed to the load balancer at its IP address. When a request hits the load balancer it forwards it to one specific server using its IP address.

Sometimes a simple round-robin formula is used (requests go to each server one after the other in turn); in other cases, more complex formulas track how busy each server actually is. If a server crashes, the load balancer stops sending requests to it and the network continues to operate without the failed server. Load balancing makes it simple to add servers (or remove servers) without affecting users. You simply add or remove the

server(s) and change the software configuration in the load balancing switch; no one is aware of the change.

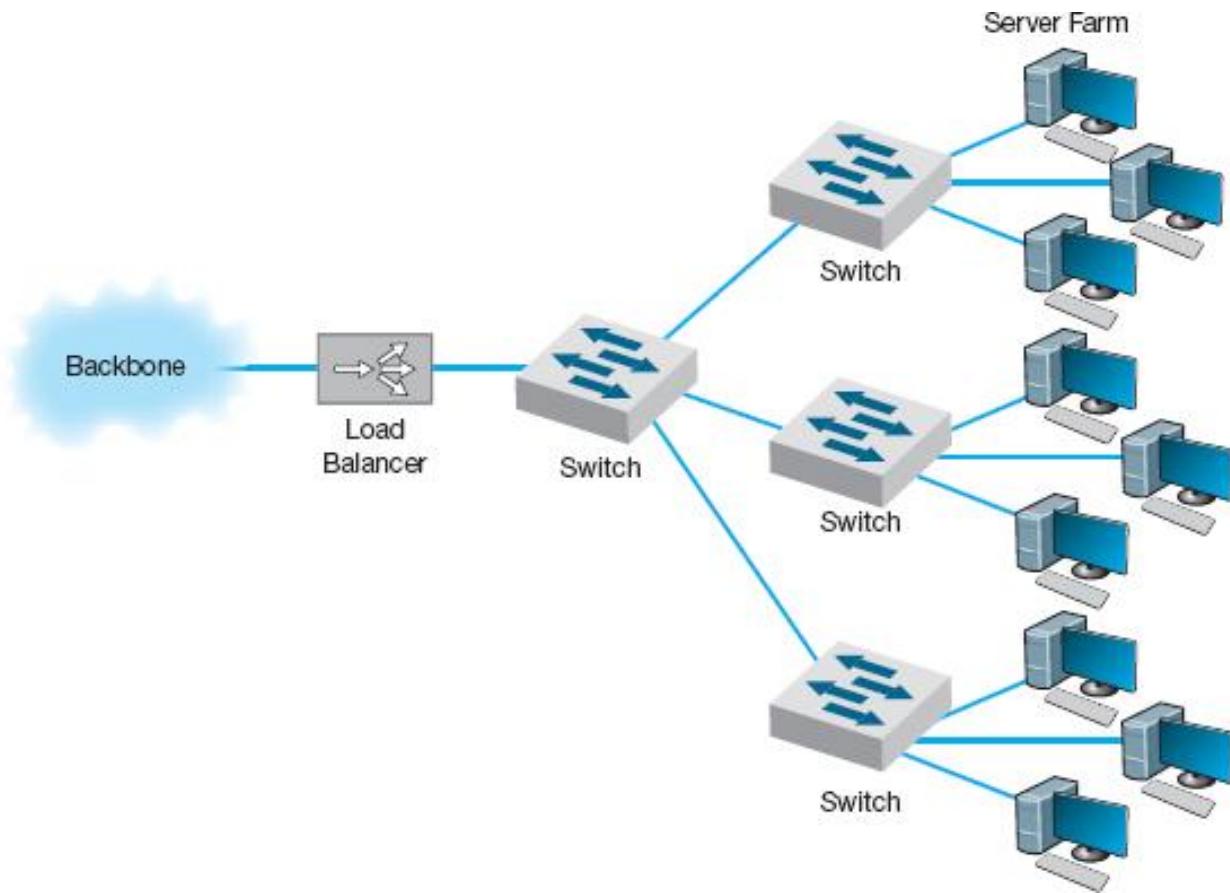


FIGURE 11.11 Network with load balancer

Server Virtualization Server virtualization is somewhat the opposite of server farms and load balancing. **Server virtualization** is the process of creating several logically separate servers (e.g., a Web server, an email server, a file server) on the same physical computer. The virtual servers run on the same physical computer, but appear completely separate to the network (and if one crashes it does not affect the others running on the same computer).

Over time, many firms have installed new servers to support new projects, only to find that the new server was not fully used; the server might only be running at 10 percent of its capacity and sitting idle for the rest of the time. One underutilized server is not a problem. But imagine if 20 to 30 percent of a company's servers are underutilized. The company has spent too much money to acquire the servers, and, more importantly, is continuing to

spend money to monitor, manage, and update the underused servers. Even the space and power used by having many separate computers can noticeably increase operating costs. Server virtualization enables firms to save money by reducing the number of physical servers they buy and operate, while still providing all the benefits of having logically separate devices and operating systems.

Some operating systems enable virtualization natively, which means that it is easy to configure and run separate virtual servers. In other cases, special purpose virtualization software (e.g., VMware) is installed on the server and sits between the hardware and the operating systems; this software means that several different operating systems (e.g., Windows, Mac, Linux) could be installed on the same physical computer.

Capacity Management Most network traffic today is hard to predict. Users choose to download large software or audio files or have instant messenger voice chats. In many networks, there is greater capacity within a LAN than there is leading out of the LAN into the backbone or to the Internet. In [Figure 11.5](#), for example, the building backbone has a capacity of 1 Gbps, which is also the capacity of just one LAN connected to it (2 East). If one user in this LAN generates traffic at the full capacity of this LAN, then the entire backbone will become congested, affecting users in all other LANs.

Capacity management devices, sometimes called **bandwidth limiters** or **bandwidth shapers**, monitor traffic and can act to slow down traffic from users who consume too much capacity. These devices are installed at key points in the network, such as between a switch serving a LAN and the backbone it connects into, and are configured to allocate capacity based on the IP address of the source (or its data link address) as well as the application in use. The device could, for example, permit a given user to generate a high amount of traffic for an approved use, but limit capacity for an unofficial use such as MP3 files. [Figure 11.12](#) shows the control panel for one device made by *NetEqualizer*.

11.5.4 MINIMIZING NETWORK TRAFFIC

Most approaches to improving network performance attempt to maximize the speed at which the network can move the traffic it receives. The opposite—and equally effective approach—is to minimize the amount of traffic the network receives. This may seem quite difficult at first glance—after all, how can we reduce the number of Web pages people request? We can't reduce all types of network traffic, but if we move the most commonly used data closer to the users who need it, we can reduce traffic enough to have an impact. We do this by providing servers with duplicate copies of commonly used information at points closer to the users than the original source of the data. Two approaches are emerging: content caching and content delivery.

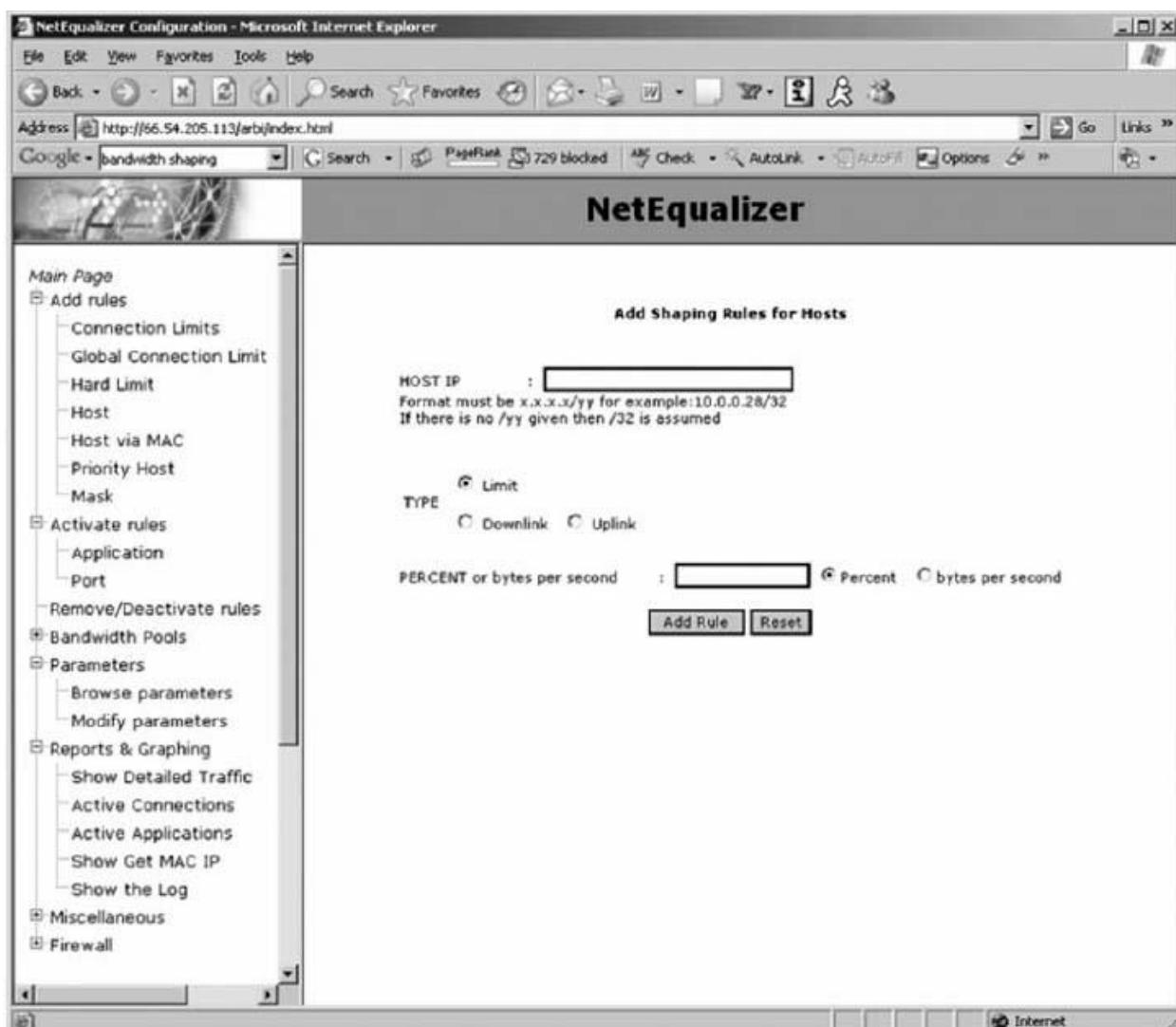


FIGURE 11.12 Capacity management software

Content Caching The basic idea behind **content caching** is to store other people's Web data closer to your users. With content caching, you install a **content engine** (also called a *cache engine*) close to your Internet connection and install special content management software on the router ([Figure 11.13](#)). The router or routing switch directs all outgoing Web requests and the files that come back in response to those requests to the cache engine. The content engine stores the request and the static files that are returned in response (e.g., graphics files, banners). The content engine also examines each outgoing Web request to see if it is requesting static content that the content engine has already stored. If the request is for content already in the content engine, it intercepts the request and responds directly itself with the stored file, but makes it appear as though the request came from the URL specified by the user. The user receives a response almost instantaneously and is unaware that the content engine responded. The content engine is *transparent*.

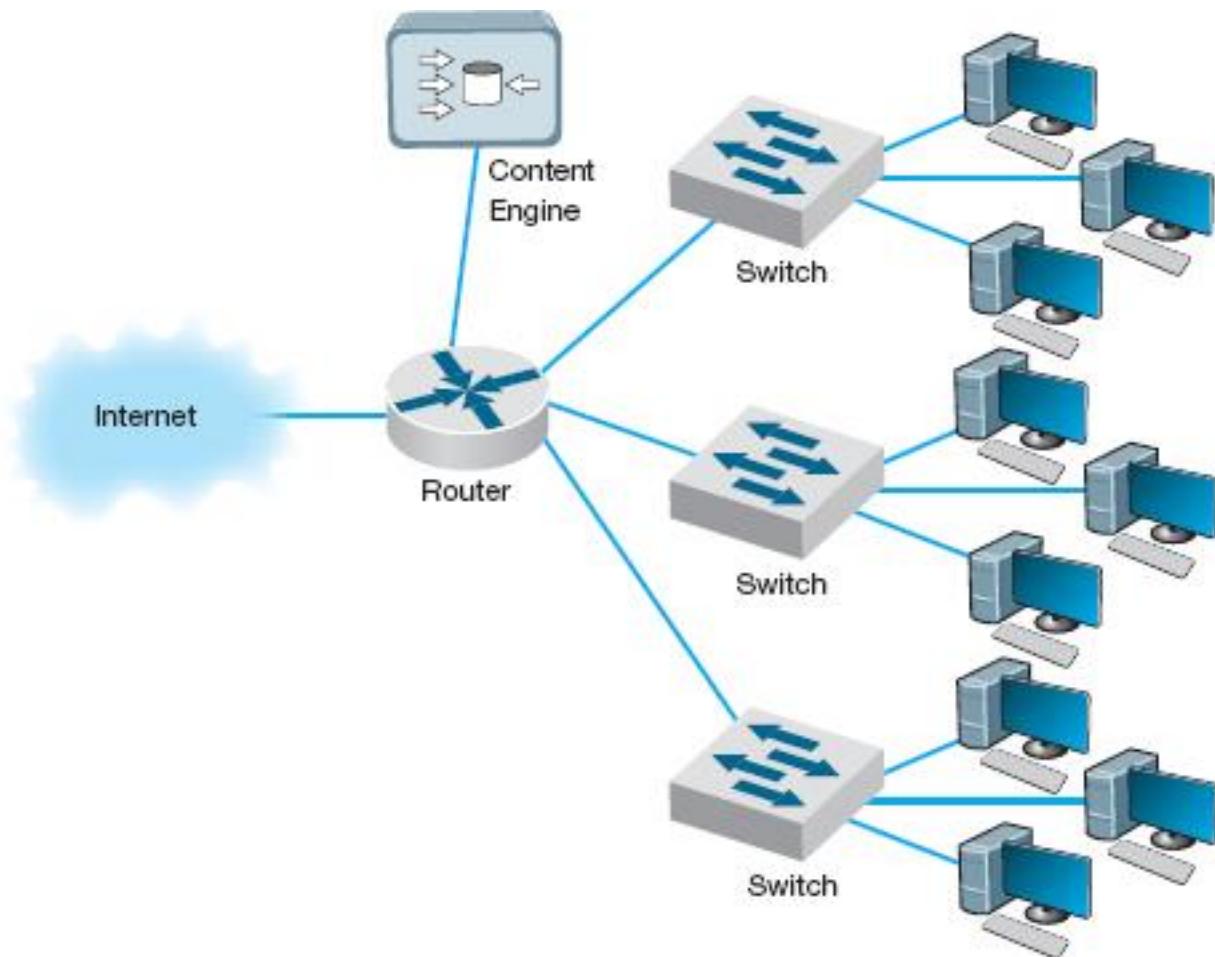


FIGURE 11.13 Network with content engine

Although not all Web content will be in the content engine's memory, content from many of the most commonly accessed sites on the Internet will be (e.g., [yahoo.com](#), [google.com](#), [Amazon.com](#)). The contents of the content engine reflect the most common requests for each individual organization that uses it, and changes over time as the pattern of pages and files changes. Each page or file also has a limited life in the cache before a new copy is retrieved from the original source so that pages that occasionally change will be accurate.

For content caching to work properly, the content engine must operate at almost wire speeds, or else it imposes additional delays on outgoing messages that result in worse performance, not better. By reducing outgoing traffic (and incoming traffic in response to requests), the content engine enables the organization to purchase a smaller WAN or MAN circuit into the Internet. So not only does content caching improve performance, but it can also reduce network costs if the organization produces a large volume of network requests.

Content Delivery **Content delivery**, pioneered by **Akamai**,² is a special type of Internet service that works in the opposite direction. Rather than storing other people's Web files closer to their own internal users, a **content delivery provider** stores Web files for its clients closer to their potential users. Akamai, for example, operates almost 10,000 Web servers located near the busiest Internet NAPs, and other exchanges. These servers contain the most commonly requested Web information for some of the busiest sites on the Internet (e.g., [yahoo.com](#), [monster.com](#), [ticketmaster.com](#)).

11.3 LOAD BALANCING AT BRYAM HEALTHCARE

MANAGEMENT FOCUS

Bryam Healthcare is a medical supply company serving more than 300,000 customers from 17 operating centers. When its sales representatives began complaining about the slow response times for email, Web, and

other key applications, Anthony Acquanita, Byram's network manager, realized that the network architecture had reached its limits.

The old architecture was a set of four servers each running specific applications (e.g., one email server, one Web server). At different points in the week, a different server would become overloaded and provide slow response times for a specific application—the email server first thing Monday morning as people checked their email after the weekend, for example.

The solution was to install a load balancing switch in front of the servers and install all the major applications on all the servers. This way when the demand for one application peaks, there are four servers available rather than one. Because the demand for different applications peaks at different times, the result has been dramatically improved performance, without the need to buy new servers. The side benefit is that it is now simple to remove one server from operations at nonpeak times for maintenance or software upgrades without the users noticing (whereas in the past, server maintenance meant disabling an application (e.g., email) for a few hours while the server was worked on).

SOURCE: “Load Balancing Boosts Network,” *Communications News*, November 2005, pp. 40–42.

When someone accesses a Web page of one of Akamai's customers, special software on the client's Web server determines if there is an Akamai server containing any static parts of the requested information (e.g., graphics, advertisements, banners) closer to the user. If so, the customer's Web server redirects portions of the request to the Akamai server nearest the user. The user interacts with the customer's Web site for dynamic content or HTML pages with the Akamai server providing static content. In [Figure 11.15](#), for example, when a user in Singapore requests a Web page from [yahoo.com](#), the main [yahoo.com](#) server farm responds with the dynamic HTML page. This page contains several static graphic files. Rather than provide an address on the [yahoo.com](#) site, the Web page is

dynamically changed by the Akamai software on the yahoo.com site to pull the static content from the Akamai server in Singapore. If you watch the bottom action bar closely on your Web browser while some of your favorite sites are loading, you'll see references to Akamai's servers. On any given day, 15–20 percent of all Web traffic worldwide comes from an Akamai server.

Akamai servers benefit both the users and the organizations that are Akamai's clients, as well as many ISPs and all Internet users not directly involved with the Web request. Because more Web content is now processed by the Akamai server and not the client organization's more distant Web server, the user benefits from a much faster response time; in [Figure 11.15](#), for example, more requests never have to leave Singapore.

11.4 CONTENT CACHING AT THE SALT LAKE CITY OLYMPIC GAMES MANAGEMENT FOCUS

The 2002 Olympic Winter Games in Salt Lake City needed a network infrastructure that would deliver real-time results, athlete biographies, transportation information, competition schedules, medal counts, competition results, and more to thousands of users (media, Olympic athletes, and staff) at sporting venues, Olympic villages, administrative offices, media centers, and external Web sites. The network had to guarantee maximum reliability 24 hours a day, seven days a week.

The Salt Lake City Olympic Committee established a primary data center with two high-performance load balancing switches in a standby/failover configuration supporting a server farm (see [Figure 11.14](#)) so that if one switch failed, the standby switch would detect the failure and automatically take over. The load balancing capability of the switches ensured that incoming traffic was routed to the least busy server, thereby ensuring maximum performance.

The primary data center was connected via a pair of routers (again in a standby/failover configuration) through T-3 lines to a secondary data center with a similar structure that would be used in the event of problems with the

primary data center. The primary data center was connected via a pair of T-1 lines to the Media Center, to the Athletes Village, and to each of the 10 Competition Venues.

The network at the Media Center, the Athletes Village, and Competition Venues had a similar standby paired router/paired switch configuration, with the addition of a content engine to reduce traffic over the T-1 lines to the primary data center.

The resulting network design ensured maximum reliability due to the paired circuits/routers/switches to all locations. The content engines also provided increased reliability and significantly reduced network traffic to the primary data center, thus reducing the capacity needed by the circuits and servers.

SOURCE: “IKANO Deploys Cisco Content Networking Solutions,” www.cisco.com, 2004.

The client organization benefits because it serves its users with less traffic reaching its Web server; Yahoo! for example, need not spend as much on its server farm or the Internet connection into its server farm. In our example, the ISPs providing the circuits across the Pacific benefit because now less traffic flows through their network—traffic that is not paid for because of Internet peering agreements. Likewise, all other Internet users in Singapore (as well as users in the United States accessing Web sites in Singapore) benefit because there is now less traffic across the Pacific and response times are faster.

11.5.5 GREEN IT

Green IT is the design and use of information technology to improve environmental sustainability. Much of Green IT focuses on reducing the amount of power consumed by and heat produced by network devices (because increased heat means the increased need for air conditioning, which requires power). Some network devices (e.g., servers, switches, routers) are designed to reduce power consumption and heat production.

For example, smaller devices tend to require less electricity than larger devices.

One of the most important steps in Green IT is server virtualization, which we discussed previously. Server virtualization reduces the number of physical servers and thus is likely to have a large impact. Fewer computers means less energy and less heat.

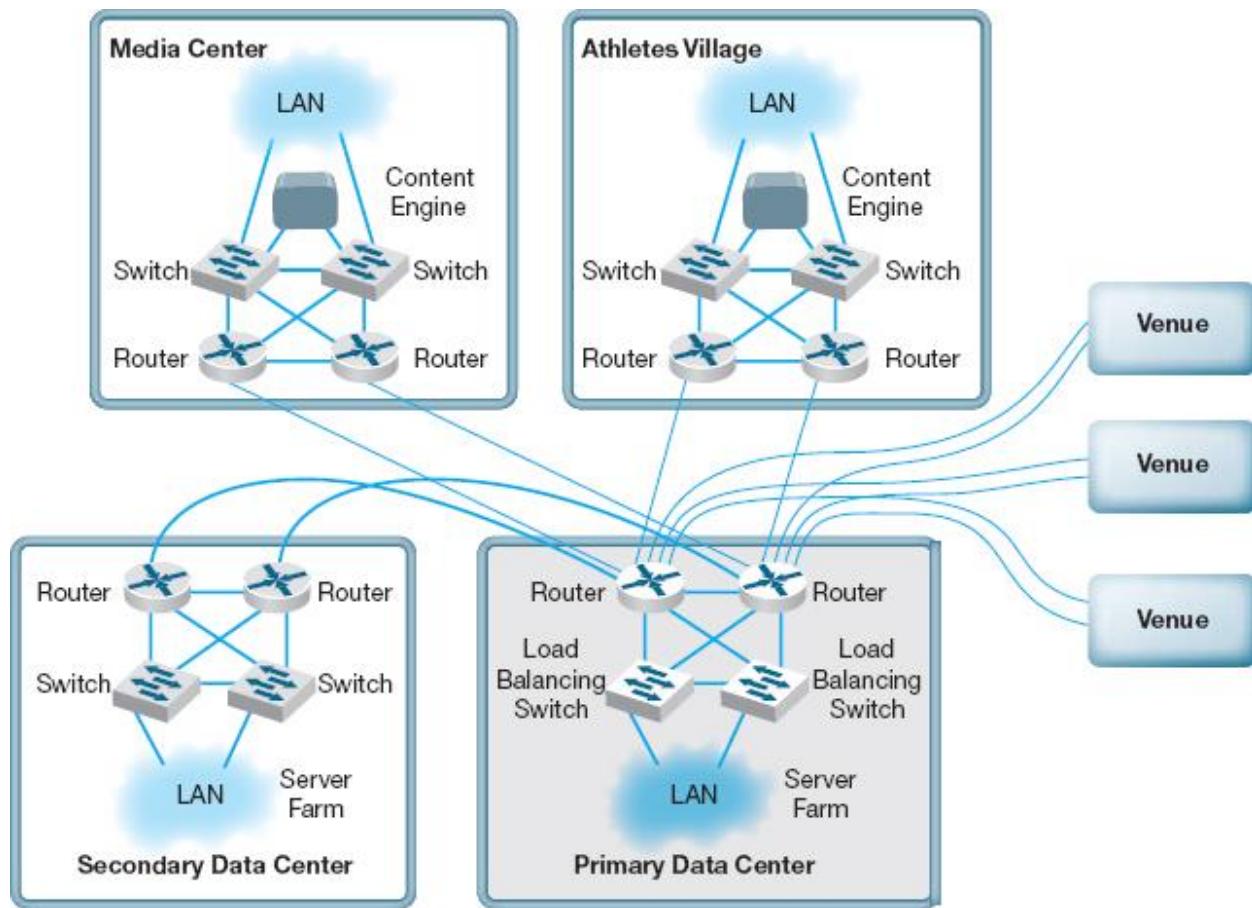


FIGURE 11.14 Olympic network. LAN = local area network

The use of content delivery is a similar Green IT strategy, as it means fewer less-used servers spread around the Internet.

Software can be installed that shuts off components within the device (e.g., a monitor or hard disk) after a certain time of inactivity to save energy. The newest Ethernet standard (IEEE 802.3az), for example, defines a change to the Ethernet protocol that permits NICs and switches to go into sleep mode to save energy when not transmitting. LANs are typically never used at 100 percent of capacity (most network circuits are active less than 10

percent of the time), so there is considerable potential to cut energy consumption.

Experts estimate that about 20 percent of the energy used in a typical office building is generated by IT. Thus, moving to green IT can save significant operating costs, as well as being better for the environment.

11.6 IMPLICATIONS FOR MANAGEMENT

Network design was at one time focused on providing the most efficient networks custom tailored to specific needs. Today, however, network design uses a building-block approach. Well-designed networks use a few common, standardized, network technologies over and over again throughout the network even though they might provide more capacity than needed. Under ideal circumstances, the organization will develop deep relationships with a very small set of vendors.

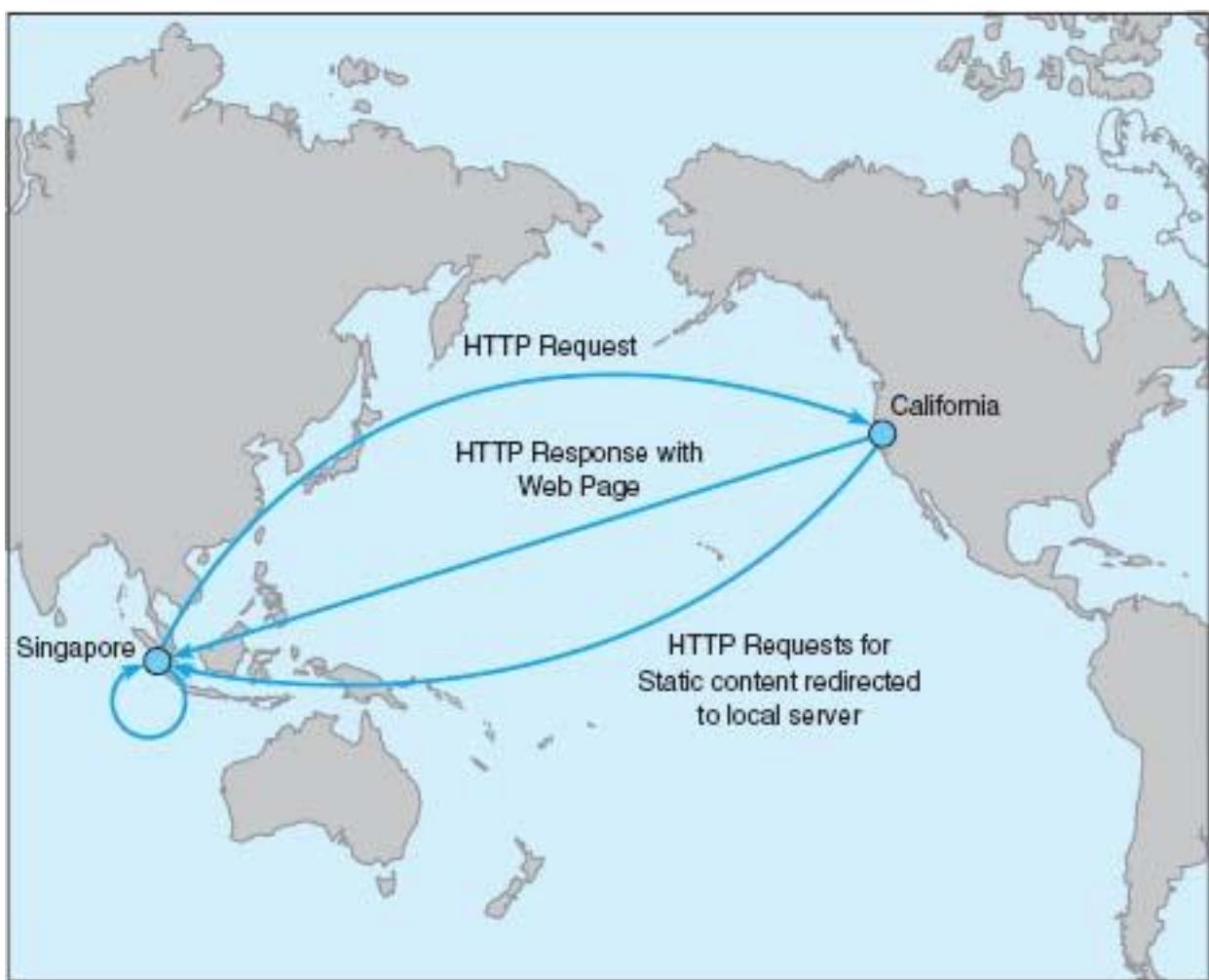


FIGURE 11.15 Network with content delivery

As the cost to operate and maintain networks gradually becomes more expensive than the cost to purchase network technologies in the first place, good network design commonly results in the purchase of more expensive equipment in order to save significantly more money in reduced network management costs over the life of the network. While there is a temptation to go with the lowest bidder and buy inexpensive equipment, in many cases this can significantly increase the lifecycle cost of a network. The use of sophisticated network design tools and network management tools has become a key part of almost all new networks installed today.

11.5 CONTENT DELIVERY AT BEST BUY

MANAGEMENT FOCUS

Best Buy operates more than 1150 retail electronic stores across the United States and Canada, and has an extensive online Web store offering more than 600,000 products. Its Web store hosts more than 4000 million visits a year, more than all of its 1150 physical stores combined.

Best Buy wanted to improve its Web store to improve customer experience and reduce operating costs. Akamai's extensive content delivery presence in North America enabled Best Buy to improve the speed of its Web transactions by 80 percent, resulting in substantial increases in sales. The shift to content delivery has also reduced the traffic to its own servers by more than 50 percent, reducing its operating costs.

SOURCE: Akamai Helps Best Buy, Akamai case studies, akamai.com, 2008.

11.6 IT'S EASY BEING GREEN

MANAGEMENT FOCUS

Avnet, Inc., located in Phoenix Arizona, is one of the largest distributors of electronic components, technology solutions, and computer products in the world. Through its supply chain, Avnet connects the world's leading technology manufacturers with customers in more than 70 countries. Avnet was ranked for two consecutive years as No.1 in its industry by Fortune magazine's list of "Most Admired Companies." However, its success reaches beyond its specialization. Avnet is also one of the leaders in Green IT and was selected as the winner of InfoWorld's 2009 "Best Practices in Green Computing, Energy Efficiency and the Datacenter."

According to the IT Director of the Data Center Operations, Bruce Gorshe, Avnet implemented many innovative solutions in the Data Center to be green—both with the IT itself and the building where the datacenter is located. First, by creating a heavily virtualized environment with 24 VMware ESX hosts, Avnet was able to reduce power consumption by 44 percent per image. Second, by developing a script that runs on all its desktops and laptops and places idle systems in hibernation during nonbusiness hours, the data center is able to reduce power consumption from 137 Watts to 1 Watt per computer. Third, re-foaming the data center ceiling and applying additional insulation allowed the cooling costs to go down by \$7500 per year and also increased the longevity of the cooling system and roof. Finally, by switching to new more efficient lighting, related costs were reduced by 30 percent. This effort led to savings of more than \$5 million in power supply for the data center. Thus, Green IT is not only good for the environment but also for the company that implements it.

SOURCE: www.avnet.com, 2011.

SUMMARY

Traditional Network Design The traditional network design approach follows a very structured systems analysis and design process similar to that used to build application systems. It attempts to develop precise estimates of network traffic for each network user and network segment. Although this is expensive and time consuming, it works well for static or

slowly evolving networks. Unfortunately, computer and networking technology is changing very rapidly, the growth in network traffic is immense, and hardware and circuit costs are relatively less expensive than they used to be. Therefore, use of the traditional network design approach is decreasing.

Building-Block Approach to Network Design The building-block approach attempts to build the network using a series of simple predefined building components, resulting in a simpler design process and a more easily managed network built with a smaller range of components. The basic process involves three steps that are performed repeatedly. Needs analysis involves developing a logical network design that includes the geographic scope of the network and a categorization of current and future network needs of the various network segments, users, and applications as either typical or high traffic. The next step, technology design, results in a set of one or more physical network designs. Network design and simulation tools can play an important role in selecting the technology that typical and high-volume users, applications, and network segments will use. The final step, cost assessment, gathers cost information for the network, usually through an RFP that specifies what equipment, software, and services are desired and asks vendors to provide their best prices. One of the keys to gaining acceptance by senior management of the network design lies in speaking management's language (cost, network growth, and reliability), not the language of the technology (Ethernet, ATM, and DSL).

Designing for Performance Network management software is critical to the design of reliable, high-performance networks. Device management software provides statistics about device utilizations and issues alerts when problems occur. System management software provides the same information, but also provides analysis and diagnosis to help the network manager make better decisions. Small networks often use device management software, while larger, more complex networks often use system management software. SNMP is a common standard for network management software and the managed devices that support it. Load balancing devices shift network traffic among servers in a server farm to

ensure that no one server is overloaded with traffic. Content caching and content delivery are commonly used to reduce network traffic.

KEY TERMS

access layer

Akamai

agent

alarm

alarm storm

application management software

bandwidth limiter

bandwidth shaper

baseline

building-block process

capacity management

capacity planning

circuit loading

cluster

Common Management Interface Protocol (CMIP)

content caching

content delivery

content delivery provider

content engine

core layer

cost assessment

desirable requirements

device management software
distribution layer
geographic scope
green IT
latency
load balancing switch
logical network design
managed device
managed network
management information base (MIB)
mandatory requirements
needs analysis
network management software
physical network design
policy-based management remote monitoring (RMON)
request for proposal (RFP)
RMON probe
root cause analysis
server farm
server virtualization
service-level agreement (SLA)
Simple Network Management Protocol (SNMP)
simulation
system management software
technology design

traditional network design process

traffic analysis

turnpike effect

virtual server

wire speed

wish-list requirements

QUESTIONS

1. What are the keys to designing a successful data communications network?
2. How does the traditional approach to network design differ from the building-block approach?
3. Describe the three major steps in current network design.
4. What is the most important principle in designing networks?
5. Why is it important to analyze needs in terms of both application systems and users?
6. Describe the key parts of the technology design step.
7. How can a network design tool help in network design?
8. On what should the design plan be based?
9. What is an RFP and why do companies use them?
10. What are the key parts of an RFP?
11. What are some major problems that can cause network designs to fail?
12. What is a network baseline and when is it established?
13. What issues are important to consider in explaining a network design to senior management?
14. What is the turnpike effect and why is it important in network design?
15. How can you design networks to improve performance?
16. How does a managed network differ from an unmanaged network?
17. Compare and contrast device management software, system management software, and application management software.

18. What are SNMP and RMON?
19. What is a traffic analysis and when is it useful?
20. What is a service level agreement?
21. How do device latency and memory affect performance?
22. How does a load balancing switch work?
23. How does content caching differ from content delivery?
24. Why do you think some organizations were slow to adopt a building-block approach to network design?
25. For what types of networks are network design tools most important? Why?
26. How important is Green IT? Why?

EXERCISES

11-1. What factors might cause peak loads in a network? How can a network designer determine if they are important, and how are they taken into account when designing a data communications network?

11-2. Collect information about two network design tools and compare and contrast what they can and cannot do.

11-3. Investigate the latest versions of SNMP and RMON and describe the functions that have been added in the latest version of the standard.

11-4. Investigate and report on the purpose, relative advantages, and relative disadvantages of two network management software tools (e.g., Open-View, Tivoli).

11-5. Explore the network management software demo from Tivoli (www-306.IBM.com/software/tivoli/library/demos/twa-demo.html).

MINI-CASES

I. Computer Dynamics

Computer Dynamics is a microcomputer software development company that has a 300-computer network. The company is located in three adjacent

five-story buildings in an office park, with about 100 computers in each building. Each building is approximately 90 feet long by 50 feet wide. They are set about 100 feet apart. The current network is poorly design for its current needs and must be completely replaced. Describe the network you would recommend and how it would be configured with the goal of building a new network that will support the company's needs for the next 3 years with few additional investments. Figure 11.16 provides a list of equipment and costs you can use to build your network. You will need to make some assumptions, so be sure to document your assumptions and explain why you have designed the network in this way.

II. Drop and Forge

Drop and Forge is a small manufacturing firm with a 60-computer network. The company has one very large manufacturing plant with an adjacent office building. The office building houses 50 computers, with an additional 10 computers in the plant. The current network is old and needs to be completely replaced. Describe the network you would recommend and how it would be configured. The goal is to build a new network that will support the company's needs for the next 3 years with few additional investments. Figure 11.16 provides a list of equipment and costs you can use to build your network. You will need to make some assumptions, so be sure to document your assumptions and explain why you have designed the network in this way.

III. Mary's Manufacturing

Mary's Manufacturing is a small manufacturing company that has a network with eight LANs (each with about 20 computers on them using switched 100Base-T) connected via 100Base-F over fiber-optic cable into a core switch (i.e., a collapsed BN). The switch is connected to the company's ISP over a fractional T1 circuit. Most computers are used for order processing and standard office applications, but some are used to control the manufacturing equipment in the plant. The current network is working fine

and there have been no major problems, but Mary is wondering whether she should invest in network management software. It will cost about \$5,000 to replace the current hardware with SNMP capable hardware. Mary can buy SNMP device management software for \$2,000. Should Mary install SNMP? Why?

IV. AdviceNet

AdviceNet is a consulting firm with offices in Toronto, New York, Los Angeles, Dallas, and Atlanta. The firm currently uses the Internet to transmit data, but its needs are growing and it is concerned over the security of the Internet. The firm wants to establish its own private WAN. Consultants in all offices are frustrated at the current 56-Kbps modems they use for Internet access, so the firm believes that it needs faster data transmission capabilities. The firm has no records of data transmission, but it believes that the New York and Toronto offices send and receive the most data. The firm is growing by 20 percent per year and expects to open offices in Vancouver and Chicago within the next 1 or 2 years. Describe two alternatives for the network and explain what choice you would make under what assumptions.

V. Accurate Accounting

Accurate Accounting is a regional accounting firm that has several local offices throughout the state. The company is constructing a new office building for use as its main headquarters. The building is about 70 feet by 50 feet, with two floors. There are a total of 40 offices, with a total of 45 desktop computers. Describe the network you would recommend and how it would be configured. Figure 11.16 provides a list of equipment and costs you can use to build your network. You will need to make some assumptions, so be sure to document your assumptions and explain why you have designed the network in this way.

VI. Salt Lake City Olympics

Reread Management Focus 11.4. Do you think the Salt Lake City Olympic network was a good design? How might you have improved it? How might you have reduced costs?

VII. Donald's Distributing

Donald's Distributing is a regional trucking firm that is constructing a new office building (their only office). The building is about 140 feet by 90 feet. The network has 80 desktop computers and two servers. Describe the network you would recommend and how it would be configured. Figure 11.16 provides a list of equipment and costs you can use to build your network. You will need to make some assumptions, so be sure to document your assumptions and explain why you have designed the network in this way.

Cable (Including Installation)	Price (\$)	
UTP Cat 5 (100Base-T)	50	
UTP Cat 5e (1000Base-T)	55	
STP Cat 5 (100Base-T)	60	
Fiber 1GbE	100	
UTP Cat 5e Patch Cables (short distances)	2	
Fiber 1GbE Patch Cables (short distances)	10	
Layer-2 Switches	Price without SNMP (\$)	Price with SNMP (\$)
Ethernet 10/100Base-T 8 port	30	300
Ethernet 10/100Base-T 16 port	40	400
Ethernet 10/100Base-T 24 port	50	500
Ethernet 10/100/1000Base-T 4 port	60	350
Ethernet 10/100/1000Base-T 8 port	70	400
Ethernet 10/100/1000Base-T 16 port	90	450
Ethernet 10/100/1000Base-T 24 port	110	500
Ethernet 10/100/1000Base-T 48 port	200	700
Ethernet 1000Base-F 4 port	400	700
Ethernet 1000Base-F 8 port	500	800
Ethernet 1000Base-F 16 port	700	900
Ethernet 10/100/1000Base-T 8 port Plus one 1000Base-F port	200	400
Ethernet 10/100/1000Base-T 16 port Plus one 1000Base-F port	250	500
Ethernet 10/100/1000Base-T 24 port Plus one 1000Base-F port	300	600
Wireless	Price without SNMP (\$)	Price with SNMP (\$)
802.11n wireless access point	60	250
802.11n wireless NIC	40	
Routers	Price without SNMP (\$)	Price with SNMP (\$)
Ethernet 10/100/1000 Base-T 2 port	100	300
Ethernet 10/100/1000 Base-T 4 port	120	400
Ethernet 10/100/1000 Base-T 8 port	150	500
Ethernet 1000Base-F 2 port	500	800
Ethernet 1000Base-F 4 port	800	1100
Ethernet 10/100/1000 Base-T 8 port Plus one 1000Base-F port	600	800
Add Firewall to any of the above	50	100
Add NAT Firewall to any of the above	75	150

WAN	Price without SNMP (\$)	Price with SNMP (\$)
DSL Modem with 1 DSL port and 1 Ethernet 10/100/1000 Base-T port	70	200
Cable Modem with 1 cable port and 1 Ethernet 10/100/1000 Base-T port	70	200
T1 CSU with 1 T1 port (also supports FT1) and 1 Ethernet 10/100/1000 Base-T port	350	500
T3 CSU with 1 T3 port and 1 Ethernet 10/100/1000 Base-T port	700	1000
Frame relay CSU with 1 frame port and 1 Ethernet 10/100/1000 Base-T port	350	500
Traffic Management	Price without SNMP (\$)	Price with SNMP (\$)
Bandwidth shaper with 2 Ethernet 10/100/1000 Base-T ports	500	800
Cache engine with 2 Ethernet 10/100/1000 Base-T ports	650	650
Security	Price without SNMP (\$)	Price with SNMP (\$)
Server Backup System	1000	n/a
DDOS System	5000	5000
IPS System	5000	5000
One time password System	3000 plus 10 per user	3000 plus 10 per user
Software	Price (\$)	
SNMP Network Management Software	2500	
Desktop Management Software	1000 plus 25 per computer	
Anti-virus Software	25 per computer	

FIGURE 11.16 Network equipment price list

CASE STUDY

NEXT-DAY AIR SERVICE

See the Web site

HANDS-ON ACTIVITY 11A

NETWORK DESIGN SOFTWARE

There are many different network design software tools. Some are simple drawing tools; others offer powerful network simulation modeling capabilities. One powerful tool that provides a free demo version that can be downloaded is SmartDraw.

The first step is to download and install the Smart-Draw software. The software is available at www.smartdraw.com.

SmartDraw comes with a variety of network icons and templates that can be used to quickly build network diagrams. Figure 11.17 shows the main drawing screen in SmartDraw and a network diagram.

DELIVERABLE

1. Select a network and draw it.

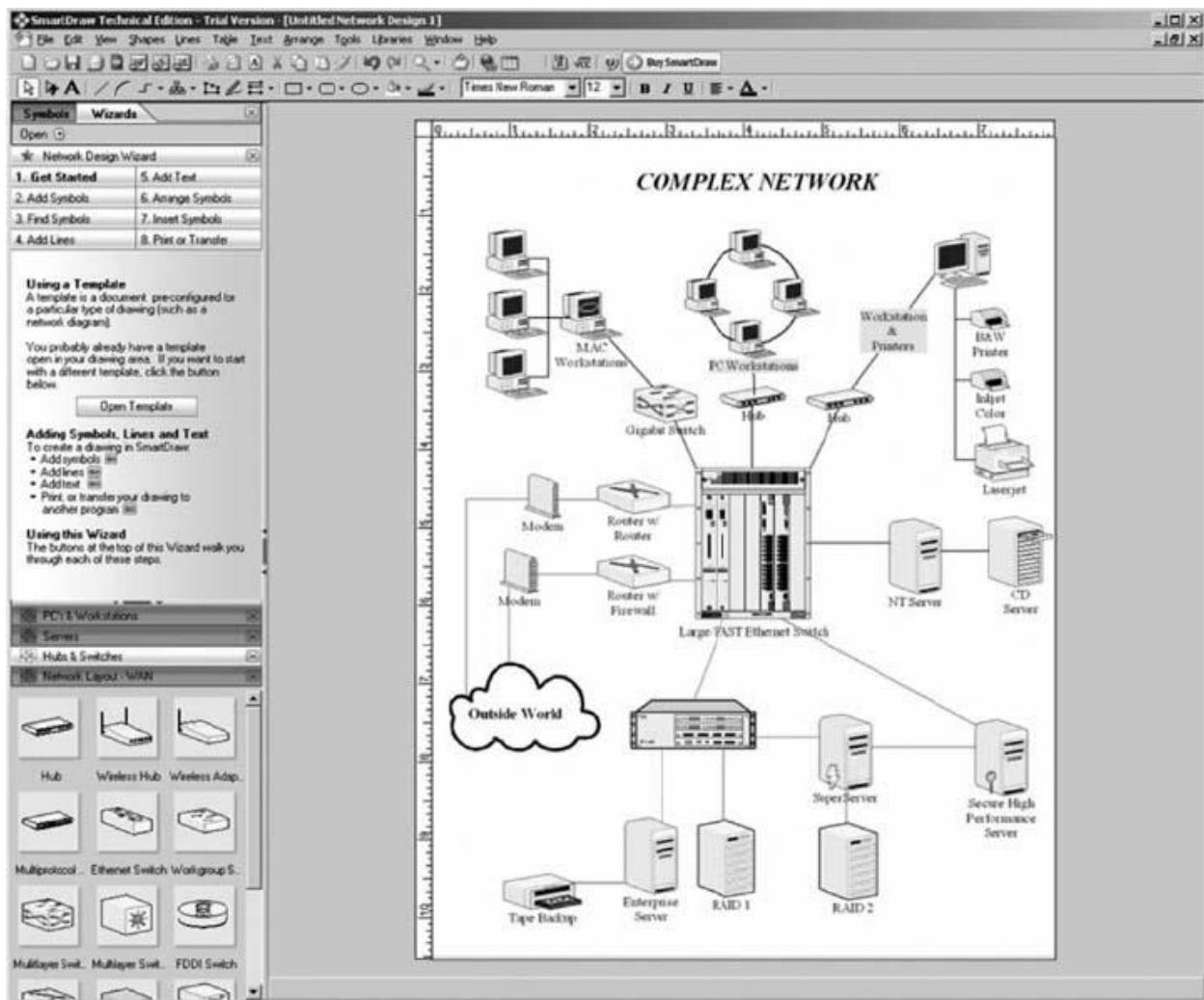


FIGURE 11.17 SmartDraw software

HANDS-ON ACTIVITY 11B

MONITORING AT&T'S WAN

AT&T permits you to monitor their Global IP network. Go to ipnetwork.bgtmo.ip.att.net/pws and click on Look at your world wide network.

You'll see a screen like that in [Figure 11.18](#) which shows the average delay ("latency") of all the circuits at each of the major PoPs in their global IP network. You can select a city and see the round-trip delay (from the city to the other city and back again). [Figure 11.18](#) shows the delays to and from Indianapolis. All are highlighted in green, which means the delays are

below the desired maximum. They range from a low of 13 ms to St. Louis to a high of 60 ms to San Diego.

This also displays the percent of packets that have been lost in transit (either due to errors or overloading of circuits). All circuits are below the target maximum of 0.1 percent.

The tabs across the top of the screen (e.g., Network Delay, Network Loss, Averages) show summary data across the entire network.

DELIVERABLES

1. What is the current latency and packet loss between Dallas and Austin?
2. What is the current latency and packet loss between Phoenix and New York?

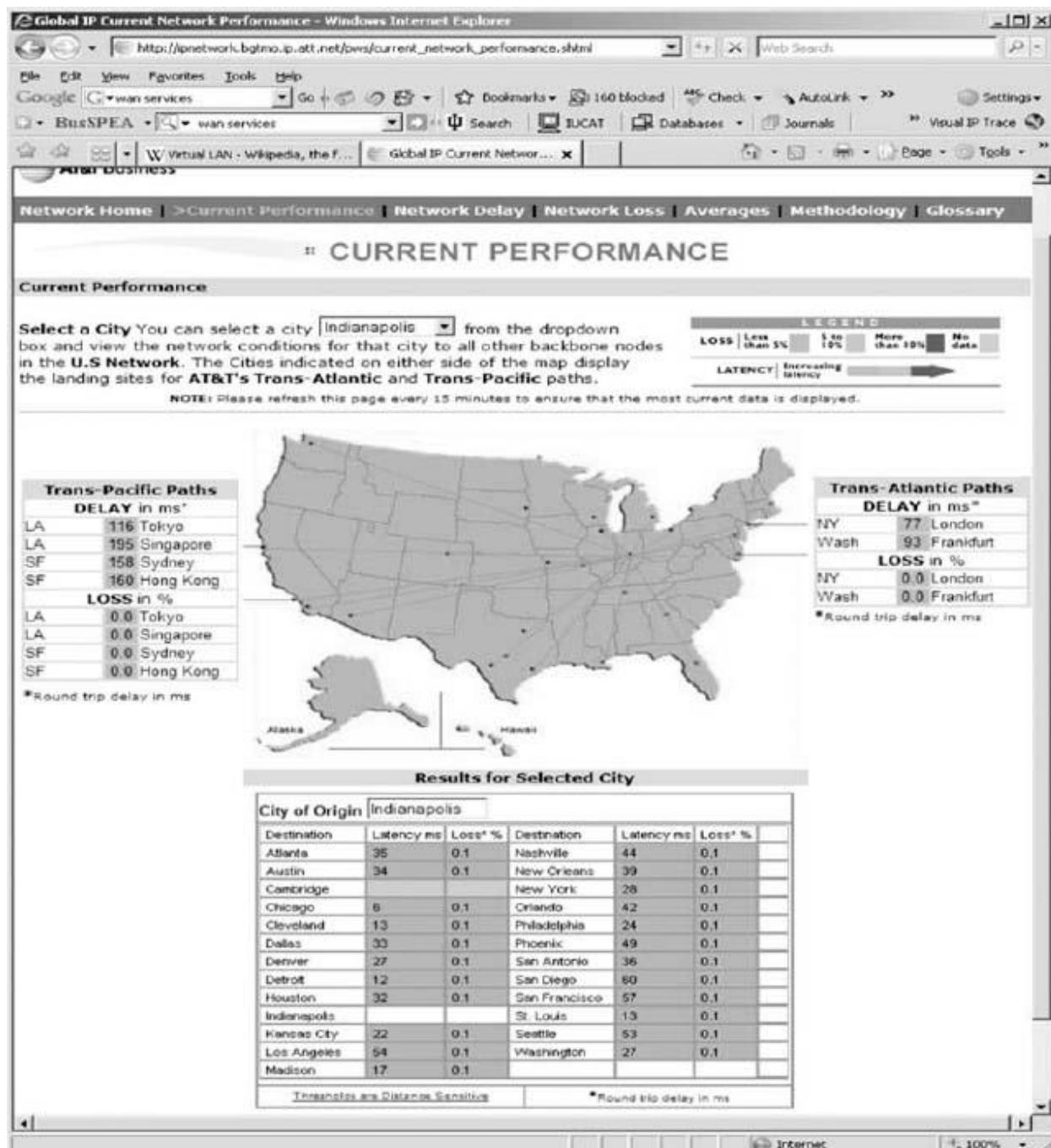


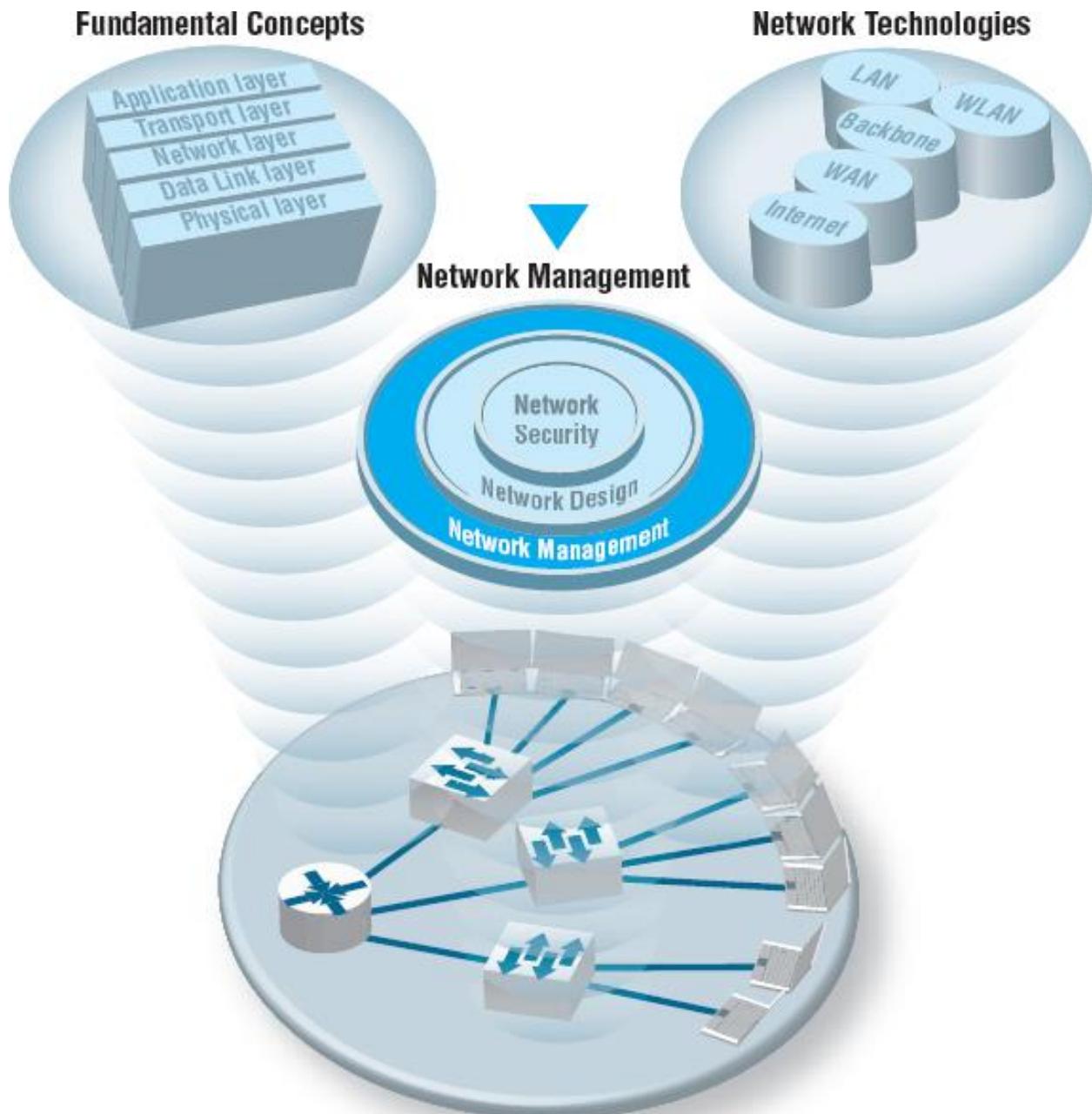
FIGURE 11.18 AT&T's global/IP network

¹ It is important to understand that these three layers refer to geographic parts of the network, not the five conceptual layers in the network model, such as the application layer, transport layer, and so on.

² Akamai (pronounced *AH-kuh-my*) is Hawaiian for intelligent, clever, and “cool.” See www.akamai.com.

CHAPTER 12

NETWORK MANAGEMENT



The Three Faces of Networking

NETWORK MANAGERS perform two key tasks: (1) designing new networks and network upgrades and (2) managing the day-to-day operation of existing networks. This chapter examines day-to-day network

management, discussing the things that must be done to ensure that the network functions properly. We discuss the network management organization and the basic functions that a network manager must perform to operate a successful network.

OBJECTIVES ▼

- Understand what is required to manage the day-to-day operation of networks
- Be familiar with the network management organization
- Understand configuration management
- Understand performance and fault management
- Be familiar with end user support
- Be familiar with cost management

CHAPTER OUTLINE ▼

12.1 INTRODUCTION

12.2 ORGANIZING THE NETWORK MANAGEMENT FUNCTION

12.2.1 The Shift to LANs and the Internet

12.2.2 Integrating LANs, WANs, and the Internet

12.2.3 Integrating Voice and Data Communications

12.3 CONFIGURATION MANAGEMENT

12.3.1 Configuring the Network and Client Computers

12.3.2 Documenting the Configuration

12.4 PERFORMANCE AND FAULT MANAGEMENT

12.4.1 Network Monitoring

12.4.2 Failure Control Function

12.4.3 Performance and Failure Statistics

12.4.4 Improving Performance

12.5 END USER SUPPORT

12.5.1 Resolving Problems

12.5.2 Providing End User Training

12.6 COST MANAGEMENT

12.6.1 Sources of Costs

12.6.2 Reducing Costs

12.7 IMPLICATIONS FOR MANAGEMENT

12.1 INTRODUCTION

Network management is the process of operating, monitoring, and controlling the network to ensure it works as intended and provides value to its users. The primary objective of the data communications function is to move application-layer data from one location to another in a timely fashion and to provide the resources that allow this transfer to occur. This transfer of information may take place within a single department, between departments in an organization, or with entities outside the organization across private networks or the Internet.

Without a well-planned, well-designed network and without a well-organized network management staff, operating the network becomes extremely difficult. Unfortunately, many network managers spend most of their time **firefighting**—dealing with breakdowns and immediate problems. If managers do not spend enough time on planning and organizing the network and networking staff, which are needed to predict and prevent problems, they are destined to be reactive rather than proactive in solving problems.

In this chapter, we examine the network management function. We begin by examining the job of the network manager and how the network management function can be organized within companies. We then break down the activities that network managers perform into four basic functions: configuration management (knowing what hardware and software are where), performance and fault management (making sure the network operates as desired), end user support (assisting end users), and cost management (minimizing the cost of providing network services). In practice, it is difficult to separate the network manager's job into these four neat categories, but these are useful ways to help understand what a network manager does.

12.2 ORGANIZING THE NETWORK MANAGEMENT FUNCTION

Communication and networking functions present special organizational problems because they are both centralized and decentralized. The developers, gatherers, and users of data are typically decentralized. The need for communications and networking affects every business function, so the management of voice and data communications has traditionally been highly centralized. Networks and mainframe servers were “owned” and operated by centralized IT departments that were used to controlling every aspect of the IT and communication environment.

12.2.1 THE SHIFT TO LANS AND THE INTERNET

Since the late 1980s, this picture has changed dramatically. There has been an explosion in the use of microcomputer-based networks. In fact, more than 90 percent of most organizations' total computer processing power (measured in millions of instructions per seconds) now resides on microcomputer-based LANs. Since the early 1990s, the number of computers attached to LANs has grown dramatically. Today, the host mainframe computer provides less than 10 percent of the organization's total computing power whereas the number of Internet-based servers (e.g., Web servers, mail servers) has grown dramatically.

Although the management of host-based mainframe networks will always be important, the future of network management lies in the successful management of multiple clients and servers communicating over LANs, BNs, and the Internet. Many LANs and Web servers were initially designed and implemented by individual departments as separate networks and applications, whose goals were to best meet the needs of their individual owners, not to integrate with other networks and applications.

Because each LAN was developed by a different department within the organization, not all LANs used the same architecture (e.g., shared 100Base-T versus switched 10Base-T, routed backbone versus switched backbone). The more types of network technology used, the more complex network management becomes.

12.2.2 INTEGRATING LANS, WANS, AND THE INTERNET

The key to integrating LANs, WANs, and the Internet into one overall organization network is for both LAN/Web and WAN managers to recognize that they no longer have the power they once had. No longer can network managers make independent decisions without considering their impacts on other parts of the organization's network. There must be a single overall communications and networking goal that best meets the needs of the entire organization. This will require some network managers to compromise on policies that are not in the best interests of their own departments or networks.

The central data communication network organization should have a written charter that defines its purpose, operational philosophy, and long-range goals. These goals must conform both to the parent organization's information-processing goals and to its own departmental goals. Along with its long-term policies, the organization must develop individual procedures with which to implement the policies. Individual departments and LAN/Web managers must be free to implement their own policies and procedures that guide the day-to-day tasks of network staff.

12.1 WHAT DO NETWORK MANAGERS DO?

MANAGEMENT FOCUS

If you were to become a network manager, some of your responsibilities and tasks would be to

- Manage the day-to-day operations of the network.
- Provide support to network users.
- Ensure the network is operating reliably.
- Evaluate and acquire network hardware, software, and services.
- Manage the network technical staff.
- Manage the network budget, with emphasis on controlling costs.

- Develop a strategic (long-term) networking and voice communications plan to meet the organization's policies and goals.
- Keep abreast of the latest technological developments in computers, data communications devices, network software, and the Internet.
- Keep abreast of the latest technological developments in telephone technologies and metropolitan area and local area network services.
- Assist senior management in understanding the business implications of network decisions and the role of the network in business operations.

12.2 FIVE KEY MANAGEMENT TASKS

MANAGEMENT FOCUS

PLANNING ACTIVITIES REQUIRE

- Forecasting
- Establishing objectives
- Scheduling
- Budgeting
- Allocating resources
- Developing policies

ORGANIZING ACTIVITIES REQUIRE

- Developing organizational structure
- Delegating
- Establishing relationships
- Establishing procedures
- Integrating the smaller organization with the larger organization

DIRECTING ACTIVITIES REQUIRE

- Initiating activities
- Decision making
- Communicating
- Motivating

CONTROLLING ACTIVITIES REQUIRE

- Establishing performance standards
- Measuring performance
- Evaluating performance
- Correcting performance

STAFFING ACTIVITIES REQUIRE

- Interviewing people
- Selecting people
- Developing People

12.2.3 INTEGRATING VOICE AND DATA COMMUNICATIONS

Another major organizational challenge is the integration of the voice communication function with the data communication function.

Traditionally, voice communications were handled by a manager in the facilities department who supervised the telephone switchboard systems and also coordinated the installation and maintenance of the organization's

voice telephone networks. By contrast, data communications traditionally were handled by the IT department because the staff installed their own communication circuits as the need arose, rather than coordinating with the voice communications staff.

This separation of voice and data worked well over the years, but today changing communication technologies are causing enormous pressures to combine these functions. These pressures are magnified by the high cost of maintaining separate facilities, the low efficiency and productivity of the organization's employees because there are two separate network functions, and the potential political problems within an organization when neither manager wants to relinquish his or her functional duties or job position. A key factor in voice/data integration might turn out to be the elimination of one key management position and the merging of two staffs. There is no perfect solution to this problem because it must be handled in a way unique to each organization. Depending on the business environment and specific communication needs, some organizations may want to combine these functions whereas others may find it better to keep them separate. We can state unequivocally that an organization that avoids studying this situation might be promoting inefficient communication systems, lower employee productivity, and increased operating costs for its separate voice and data networks.

12.3 NETWORK MANAGER JOB REQUIREMENTS

MANAGEMENT FOCUS

Being a network manager is not easy. We reviewed dozens of job posting for the key responsibilities, skills, and education desired by employers. Those responsibilities listed below were commonly mentioned.

RESPONSIBILITIES:

- Determine network needs and architect solutions to address business requirements.

- Procure and manage vendor relations with providers of equipment and services.
- Deploy new network components and related network systems and services, including the creation of test plans and procedures, documentation of the operation, maintenance and administration of any new systems or services, and training.
- Develop, document, and enforce standards, procedures, and processes for the operation and maintenance of the network and related systems.
- Manage the efficiency of operations of the current network infrastructure, including analyzing network performance and making configuration adjustments as necessary.
- Administer the network servers and the network-printing environment.
- Ensure network security including the development of applicable security, server and desktop standards, and monitoring processes to ensure that mission critical processes are operational.
- Manage direct reports and contractors. This includes task assignments, performance monitoring, and regular feedback. Hire, train, evaluate, and terminate staff and contractors under the direction of company policies and processes.
- Assist business in the definition of new product/service offerings and the capabilities and features of the systems in order to deliver those products and services to our customers.

SKILLS REQUIRED:

- Strong, up-to-date technology skills in a variety of technologies
- LAN/WAN networking experience working with routers and switches
- Experience with Internet access solutions, including firewalls and VPN
- Network architecture design and implementation experience
- Information security experience

- Personnel management experience
- Project management experience
- Experience working in a team environment
- Ability to work well in an unstructured environment
- Excellent problem-solving and analytical skills
- Effective written and oral communication skills

EDUCATION:

- Bachelor's degree in an information technology field
- Security Certification
- Microsoft MCSE Certification preferred
- Cisco CCNA Certification preferred

In communications, we are moving from an era in which the computer system is the dominant IT function to one in which communications networks are the dominant IT function. In some organizations, the total cost of both voice and data communications will equal or exceed the total cost of the computer systems.

12.3 CONFIGURATION MANAGEMENT

Configuration management means managing the network's hardware and software configuration, and documenting it, and ensuring it is updated as the configuration changes.

12.3.1 CONFIGURING THE NETWORK AND CLIENT COMPUTERS

One of the most common configuration activities is adding and deleting user accounts. When new users are added to the network, they are usually categorized as being a member of some group of users (e.g., faculty,

students, accounting department, personnel department). Each user group has its own access privileges, which define what file servers, directories, and files they can access and provide a standard log-in script. The log-in script specifies what commands are to be run when the user first logs in (e.g., setting default directories, connecting to public disks, running menu programs).

Another common activity is updating the software on the client computers attached to the network. Every time a new application system is developed or updated (or, for that matter, when a new version is released), each client computer in the organization must be updated. Traditionally, this has meant that someone from the networking staff has had to go to each client computer and manually install the software, either from diskettes/CDs or by downloading over the network. For a small organization, this is time consuming but not a major problem. For a large organization with hundreds or thousands of client computers (possibly with a mixture of Windows and Apples), this can be a nightmare.

Desktop management sometimes called *electronic software delivery* or *automated software delivery*, is one solution to the configuration problem. ESD enables network managers to install software on client computers over the network without physically touching each client computer. Most desktop management packages provide application-layer software for the network server and all client computers. The server software communicates directly with the desktop management software on the clients and can be instructed to download and install certain application packages on each client at some predefined time (e.g., at midnight on a Saturday or as requested by the user. Microsoft and many antivirus software vendors use this approach to deliver updates and patches to their software).

Desktop management greatly reduces the cost of configuration management over the long term because it eliminates the need to update each and every client computer manually. It also automatically produces and maintains accurate documentation of all software installed on each client computer and enables network managers to produce a variety of useful reports. However, desktop management increases costs in the short

term because it costs money (typically \$50 per client computer) and requires network staff to install it manually on each client computer. Desktop Management Interface (DMI) is the emerging standard for desktop management.

12.3.2 DOCUMENTING THE CONFIGURATION

Configuration documentation includes information about network hardware, network software, user and application profiles, and **network documentation**. The most basic information about network hardware is a set of network configuration diagrams that document the number, type, and placement of network circuits (whether organization owned or leased from a common carrier), network servers, network devices (e.g., hubs, routers), and client computers. For most organizations, this is a large set of diagrams: one for each LAN, BN, and WAN. Figure 12.1 shows a diagram of network devices in one office location.

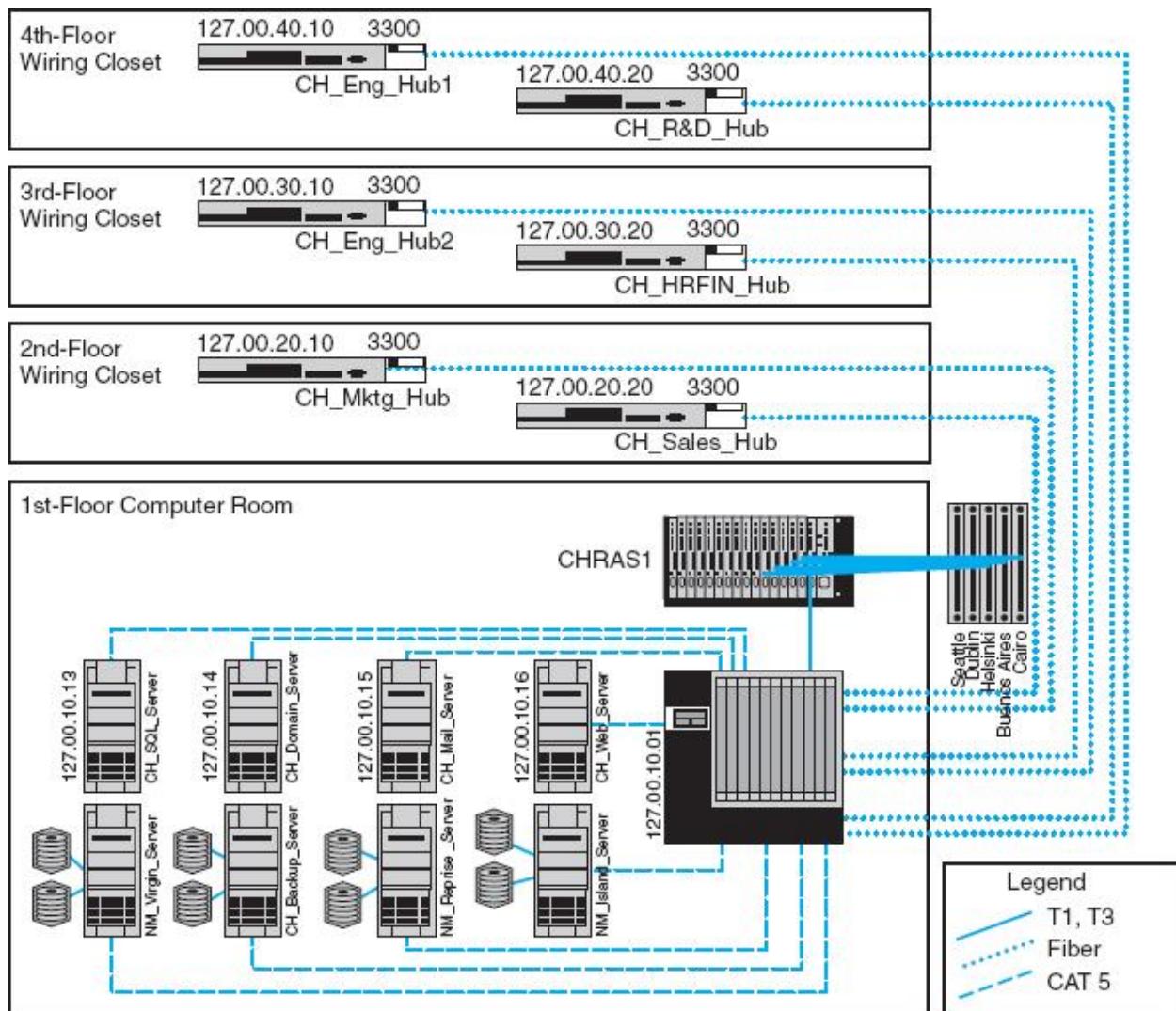


FIGURE 12.1 Network configuration diagram

Source: netViz

These diagrams must be supplemented by documentation on each individual network component (e.g., circuit, hub, server). Documentation should include the type of device, serial number, vendor, date of purchase, warranty information, repair history, telephone number for repairs, and any additional information or comments the network manager wishes to add. For example, it would be useful to include contact names and telephone numbers for the individual network managers responsible for each separate LAN within the network, and common carrier telephone contact information. (Whenever possible, establish a national account with the common carrier rather than dealing with individual common carriers in separate states and areas.)

A similar approach can be used for network software. This includes the network operating system and any special-purpose network software. For example, it is important to record which network operating system with which version or release date is installed on each network server. The same is true of application software. As discussed in Chapter 6 on LANs, sharing software on networks can greatly reduce costs although it is important to ensure that the organization is not violating any software license rules.

Software documentation can also help in negotiating site licenses for software. Many users buy software on a copy-by-copy basis, paying the retail price for each copy. It may be cheaper to negotiate the payment of one large fee for an unlimited use license for widely used software packages instead of paying on a per-copy basis.

The third type of documentation is the user and application profiles, which should be automatically provided by the network operating system or additional vendor or third-party software agreements. These should enable the network manager to easily identify the files and directories to which each user has access and each user's access rights (e.g., read-only, edit, delete). Equally important is the ability to access this information in the "opposite" direction; that is, to be able to select a file or directory and obtain a list of all authorized users and their access rights.

In addition, other documentation must be routinely developed and updated pertaining to the network. This includes network hardware and software manuals, application software manuals, standards manuals, operations manuals for network staff, vendor contracts and agreements, and licenses for software. The documentation should include details about performance and fault management (e.g., preventive maintenance guidelines and schedules, disaster recovery plan, and diagnostic techniques), end user support (e.g., applications software manuals, vendor support telephone numbers), and cost management (e.g., annual budgets, repair costs for each device). The documentation should also include any legal requirements to comply with local or federal laws, control, or regulatory bodies.

Maintaining documentation is usually a major issue for most organizations. Have you written programs? How well did you document them? Many technicians hate documentation because it is not “fun” and doesn't provide immediate value the same way that solving problems does. Therefore, it is often overlooked so when someone leaves the organization, the knowledge of the network leaves with them.

12.4 PERFORMANCE AND FAULT MANAGEMENT

Performance management means ensuring the network is operating as efficiently as possible whereas **fault management** means preventing, detecting, and correcting faults in the network circuits, hardware, and software (e.g., a broken device or improperly installed software). Fault management and performance management are closely related because any faults in the network reduce performance. Both require **network monitoring**, which means keeping track of the operation of network circuits and devices to ensure they are functioning properly and to determine how heavily they are used.

12.4.1 NETWORK MONITORING

Most large organizations and many smaller ones use *network management software* to **monitor** and control their networks. One function provided by these systems is to collect operational statistics from the network devices. For small networks, network monitoring is often done by one person, aided by a few simple tools (discussed later in this chapter). These tools collect information and send messages to the network manager's computer.

A Day in the Life: Network Policy Manager

All large organizations have formal policies for the use of their networks (e.g., wireless LAN access, password, server space). Most large organizations have a special policy group devoted to the creation of network policies, many of which are devoted to network security. The job of the policy officer is to steer the policy through the policy making process and ensure that all policies are in the best interests of the organization as a

whole. Although policies are focused inside the organization, policies are influenced by events both inside and outside the organization. The policy manager spends a significant amount of time working with outside organizations such as the U.S. Department of Homeland Security, CIO and security officer groups, and industry security consortiums. The goal is to make sure all policies (especially security policies) are up-to-date and provide a good balance between costs and benefits.

A typical policy begins with networking staff writing a summary containing the key points of the proposed policy. The policy manager takes the summary and uses it to develop a policy that fits the structure required for organizational policies (e.g., date, rationale, scope, responsible individuals, and procedures). This policy manager works with the originating staff to produce an initial draft of the proposed policy. Once everyone in the originating department and the policy office are satisfied with the policy, it is provided to an advisory committee of network users and network managers for discussion. Their suggestions are then incorporated in the policy or an explanation is provided is to why the suggestions will not be incorporated in the policy.

After several iterations, a policy becomes a draft policy and is posted for comment from all users within the organization. Comments are solicited from interested individuals and the policy may be revised. Once the draft is finalized, the policy is then presented to senior management for approval. Once approved, the policy is formally published, and the organization charged with implementing the policy begins to use it to guide their operations.

With thanks to Mark Bruhn

12.4 NETWORK MANAGEMENT SALARIES

MANAGEMENT FOCUS

Network management is not easy, but it doesn't pay too badly. Here are some typical jobs and their respective annual salaries.

Network Vice President \$150,00

Network Manager 90,000

Telecom Manager 77,000

LAN Administrator 70,000

WAN Administrator 75,000

Network Designer 80,000

Network Technician 60,000

Technical Support Staff 50,000

Trainer 50,000

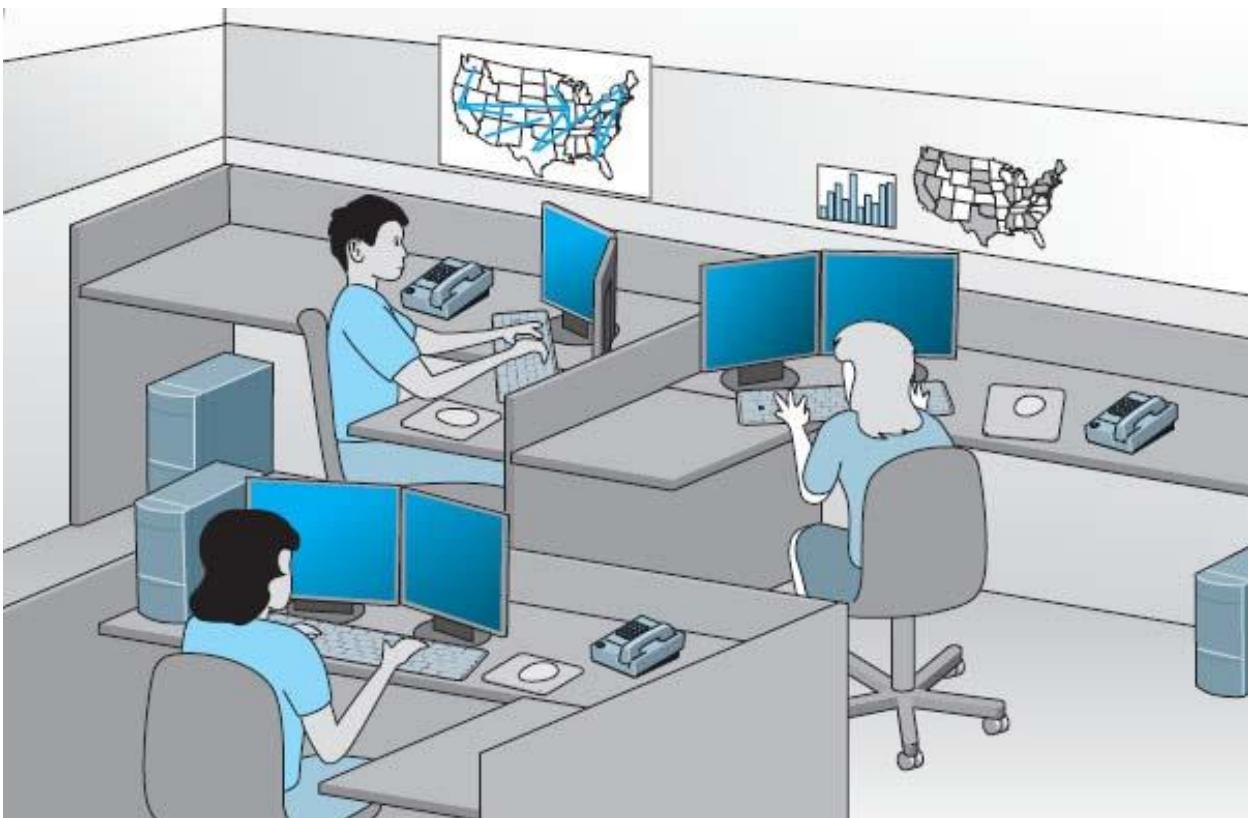


FIGURE 12.2 A network operations center

In large networks, network monitoring becomes more important. Large networks that support organizations operating 24 hours a day are often mission critical, which means a network problem can have serious business consequences. For example, consider the impact of a network failure for a common carrier such as AT&T or for the air traffic control system. These networks often have a dedicated **network operations center (NOC)** that is responsible for monitoring and fixing problems. Such centers are staffed by a set of skilled network technicians that use sophisticated network management software. When a problem occurs, the software immediately detects the problems and sends an alarm to the NOC. Staff members in the NOC diagnose the problem and can sometimes fix it from the NOC (e.g., restarting a failed device). Other times, when a device or circuit fails, they must change routing tables to route traffic away from the device and inform the common carrier or dispatch a technician to fix or replace it.

Figure 12.2 depicts an NOC similar to one at Indiana University. The NOC at Indiana University is staffed 24 hours a day, 7 days a week to monitor

the university's networks. The NOC also has responsibility for managing portions of several very high-speed networks including the Abilene Network of Internet2 (see Management Focus Box 12.5).

The parameters monitored by a network management system fall into two distinct categories: physical network statistics and logical network information. Gathering statistics on the **physical network parameters** includes monitoring the operation of the network's modems, multiplexers, circuits linking the various hardware devices, and any other network devices. Monitoring the physical network consists of keeping track of circuits that may be down and tracing malfunctioning devices. **Logical network parameters** include performance measurement systems that keep track of user response times, the volume of traffic on a specific circuit, the destination of data routed across various networks, and any other indicators showing the level of service provided by the network.

Some types of management software operate passively, collecting the information and reporting it back to the central NOC. Others are active, in that they routinely send test messages to the servers or application being monitored (e.g., an HTTP Web page request) and record the response times. One common type of monitoring approach is the **network weather map**, which displays the usage of all major circuits in the network in real time.¹

Performance tracking is important because it enables the network manager to be proactive and respond to performance problems before users begin to complain. Poor network reporting leads to an organization that is overburdened with current problems and lacks time to address future needs. Management requires adequate reports if it is to address future needs.

12.4.2 FAILURE CONTROL FUNCTION

Failure control requires developing a central control philosophy for problem reporting, whether the problems are first identified by the NOC or by users calling in to the NOC or a help desk. Whether problem reporting is done by the NOC or the **help desk**, the organization should maintain a central telephone number for network users to call when any problem occurs in the

network. As a central troubleshooting function, only this group or its designee should have the authority to call hardware or software vendors or common carriers.

Many years ago, before the importance (and cost) of network management was widely recognized, most networks ignored the importance of fault management. Network devices were “dumb” in that they did only what they were designed to do (e.g., routing packets) but did not provide any network management information.

For example, suppose a network interface card fails and begins to transmit garbage messages randomly. Network performance immediately begins to deteriorate because these random messages destroy the messages transmitted by other computers, which need to be retransmitted. Users notice a delay in response time and complain to the network support group, which begins to search for the cause. Even if the network support group suspects a failing network card (which is unlikely unless such an event has occurred before), locating the faulty card is very difficult and time consuming.

Most network managers today are installing *managed devices* that perform their functions (e.g., routing, switching) and also record data on the messages they process (see [Chapter 12](#)). These data can be sent to the network manager's computer when the device receives a special control message requesting the data, or it can send an *alarm* message to the network manager's computer if the device detects a critical situation. In this way, network faults and performance problems can be detected and reported by the devices themselves before they become serious. In the case of the failing network card, a managed device could record the increased number of retransmissions required to successfully transmit messages and inform the network management software of the problem. A managed hub or switch might even be able to detect the faulty transmissions from the failing network card, disable the incoming circuit so that the card could not send any more messages, and issue an alarm to the network manager. In either case, finding and fixing the fault is much simpler, requiring minutes, not hours.

12.5 INTERNET2 WEATHER MAP

MANAGEMENT FOCUS

The Abilene network is an Internet2 high-performance backbone that connects regional gigapops to provide high-speed network services to over 220 Internet2 university, corporate, and affiliate member institutions in all 50 states, the District of Columbia, and Puerto Rico. The current network is primarily an OC-192c (10 Gbps) backbone employing optical transport technology and advanced high-performance routers.

The network is monitored 24 hours a day, seven days a week from the network operations center (NOC) located on the campus of Indiana University in Indianapolis. The NOC oversees problem, configuration, and change management; network security; performance and policy monitoring; reporting; quality assurance; scheduling; and documentation. The center provides a structured environment that effectively coordinates operational activities with all participants and vendors related to the function of the network.

The NOC uses multiple network management software running across several platforms. Figure 12.3 shows one of the tools used by the NOC that is available to the general public: the Internet2 Weather Map. Each of the major circuits connecting the major Abilene gigapops is shown on the map. Each link has two parts, showing the utilization of the circuits to and from each pair of gigapops. The links are color-coded to quickly show the utilization of the link. Figure 12.3 is not in color so it is difficult to read, but if you visit the Abilene Web site (the URL is listed below), you can see that circuits with very low utilization are different shades of blue, which turn to green and then yellow and orange as utilization increases to 10 percent of capacity. Once utilization climbs above 30 percent, the link is shown in deeper shades of red and then purple. If you look back at the photo in Figure 12.2 you'll see the weather map displayed on the large screen in the NOC.

The link from the Chicago gigapop to the New York City gigapop, for example, indicates that over the last few minutes, an average of 546 Mbps has been transmitted, giving a 10 percent utilization. The link from New

York City to Chicago shows that over the last few minutes, an average of 6.2 Gbps has been transmitted, giving a 70 percent utilization.

If you look carefully at the utilization rates and percentages, you will see that not all circuits in the Abilene network were 10 Gbps when this weather map was done. Currently, the plan is to upgrade most circuits to 100G.

SOURCE: abilene.internet2.edu.

Numerous software packages are available for recording fault information. The reports they produce are known as **trouble tickets**. The software packages assist the help desk personnel so they can type the trouble report immediately into a computerized failure analysis program. They also automatically produce various statistical reports to track how many failures have occurred for each piece of hardware, circuit, or software package. Automated trouble tickets are better than paper because they allow management personnel to gather problem and vendor statistics. There are four main reasons for trouble tickets: problem tracking, problem statistics, problem-solving methodology, and management reports.

Problem tracking allows the network manager to determine who is responsible for correcting any outstanding problems. This is important because some problems often are forgotten in the rush of a very hectic day. In addition, anyone might request information on the status of a problem. The network manager can determine whether the problem-solving mechanism is meeting predetermined schedules. Finally, the manager can be assured that all problems are being addressed. Problem tracking also can assist in problem resolution. Are problems being resolved in a timely manner? Are overdue problems being flagged? Are all resources and information available for problem solving?

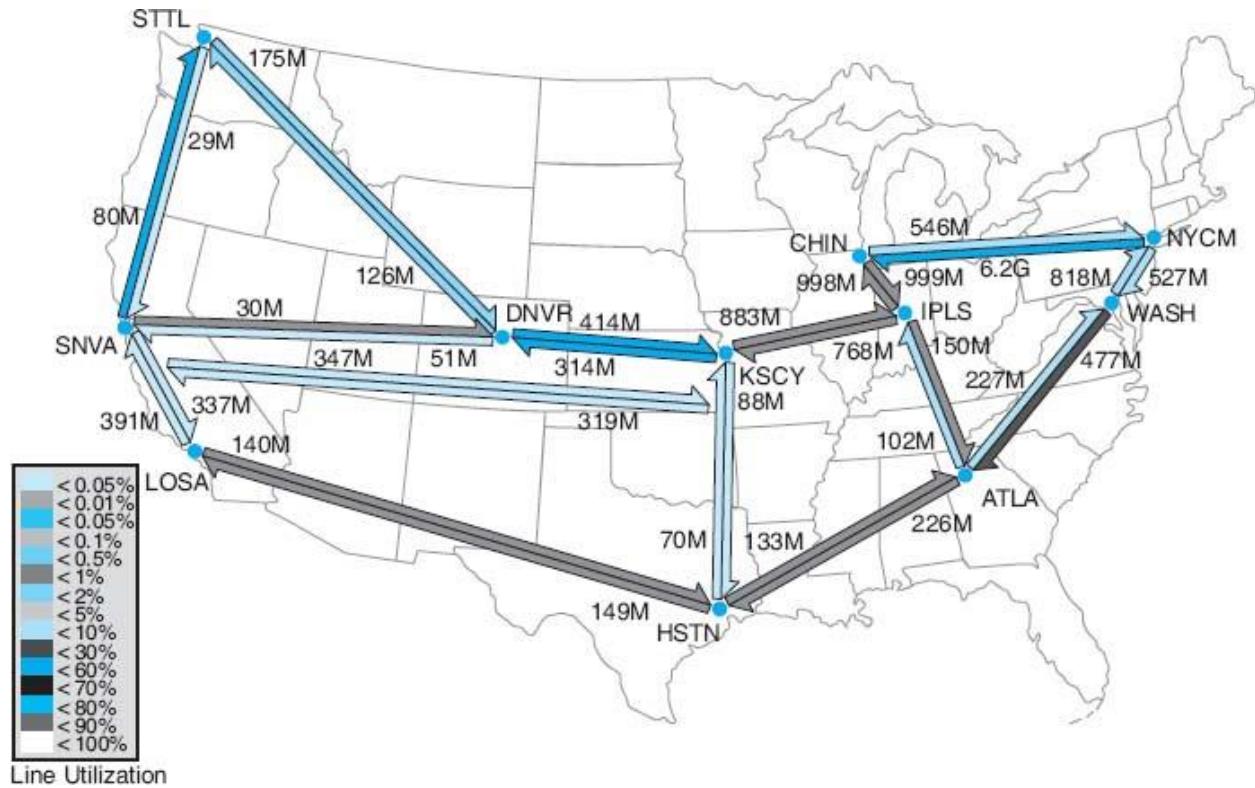


FIGURE 12.3 Internet2 Weather Map

Problem statistics are important because they are a control device for the network managers as well as for vendors. With this information, a manager can see how well the network is meeting the needs of end users. These statistics also can be used to determine whether vendors are meeting their contractual maintenance commitments. Finally, they help to determine whether problem-solving objectives are being met.

Problem prioritizing helps ensure that critical problems get priority over less important ones. For example, a network support staff member should not work on a problem on one client computer if an entire circuit with dozens of computers is waiting for help. Moreover, a manager must know whether problem-resolution objectives are being met. For example, how long is it taking to resolve critical problems?

Management reports are required to determine network availability, product and vendor reliability (mean time between failures), and vendor responsiveness. Without them, a manager has nothing more than a “best guess” estimate for the effectiveness of either the network’s technicians or the vendor’s technicians. Regardless of whether this information is typed

immediately into an automated trouble ticket package or recorded manually in a bound notebook-style trouble log, the objectives are the same.

The purposes of the trouble log are to record problems that must be corrected and to keep track of statistics associated with these problems.

For example, the log might reveal that there were 37 calls for software problems (3 for one package, 4 for another package, and 30 for a third software package), 26 calls for cable modem problems evenly distributed among two vendors, 49 calls for client computers, and 2 calls to the common carrier that provides the network circuits. These data are valuable when the design and analysis group begins redesigning the network to meet future requirements.

12.1 TECHNICAL REPORTS

TECHNICAL FOCUS

Technical reports that are helpful to network managers are those that provide summary information, as well as details that enable the managers to improve the network. Technical details include:

- Circuit use
- Usage rate of critical hardware such as host computers, front-end processors, and servers
- File activity rates for database systems
- Usage by various categories of client computers
- Response time analysis per circuit or per computer
- Voice versus data usage per circuit
- Queue-length descriptions, whether in the host computer, in the front-end processor, or at remote sites
- Distribution of traffic by time of day, location, and type of application software
- Failure rates for circuits, hardware, and software
- Details of any network faults

12.4.3 PERFORMANCE AND FAILURE STATISTICS

There are many different types of failure and recovery statistics that can be collected. The most obvious performance statistics are those discussed above: how many packets are being moved on what circuits and what the response time is. Failure statistics also tell an important story.

One important failure statistic is **availability**, the percentage of time the network is available to users. It is calculated as the number of hours per month the network is available divided by the total number of hours per month (i.e., 24 hours per day \times 30 days per month = 720 hours). The **downtime** includes times when the network is unavailable because of faults and routine maintenance and network upgrades. Most network managers strive for 99 to 99.5 percent availability, with downtime scheduled after normal working hours.

The **mean time between failures (MTBF)** is the number of hours or days of continuous operation before a component fails. Obviously, devices with higher MTBF are more reliable.

When faults occur, and devices or circuits go down, the **mean time to repair (MTTR)** is the average number of minutes or hours until the failed device or circuit is operational again. The MTTR is composed of these separate elements:

$$MTTR_{Repair} = MTT_{Diagnose} + MTT_{Respond} + MTT_{Fix}$$

The **mean time to diagnose (MTTD)** is the average number of minutes until the root cause of the failure is correctly diagnosed. This is an indicator of the efficiency of problem management personnel in the NOC or help desk who receive the problem report.

12.2 ELEMENTS OF A TROUBLE REPORT

TECHNICAL FOCUS

When a problem is reported, the trouble log staff members should record the following:

- Time and date of the report
- Name and telephone number of the person who reported the problem
- The time and date of the problem (and the time and date of the call)
- Location of the problem
- The nature of the problem
- When the problem was identified
- Why and how the problem happened

The **mean time to respond (MTTR)** is the average number of minutes or hours until service personnel arrive at the problem location to begin work on the problem. This is a valuable statistic because it indicates how quickly vendors and internal groups respond to emergencies. Compilation of these figures over time can lead to a change of vendors or internal management policies or, at the minimum, can exert pressure on vendors who do not respond to problems promptly.

Finally, after the vendor or internal support group arrives on the premises, the last statistic is the **mean time to fix (MTTF)**. This figure tells how quickly the staff is able to correct the problem after they arrive. A very long time to fix in comparison with the time of other vendors may indicate faulty equipment design, inadequately trained customer service technicians, or even the fact that inexperienced personnel are repeatedly sent to fix problems.

For example, suppose your Internet connection at home stops working. You call your ISP, and they fix it over the phone in 15 minutes. In this case, the MTTR is 15 minutes, and it is hard to separate the different parts (MTTD, MTTR, and MTTF). Suppose you call your ISP and spend 60 minutes on the phone with them, and they can't fix it over the phone; instead, the technician arrives the next day (18 hours later) and spends one hour fixing the problem. In this case $MTTR = 1\text{ hour} + 18\text{ hours} + 1\text{ hour} = 20\text{ hours}$.

The MTBF can be influenced by the original selection of vendor-supplied equipment. The MTTD relates directly to the ability of network personnel to isolate and diagnose failures and can often be improved by training. The

MTTR (respond) can be influenced by showing vendors or internal groups how good or bad their response times have been in the past. The MTTF can be affected by the technical expertise of internal or vendor staff and the availability of spare parts onsite.

Another set of statistics that should be gathered are those collected daily by the network operations group, which uses network management software. These statistics record the normal operation of the network, such as the number of errors (retransmissions) per communication circuit.

Statistics also should be collected on the daily volume of transmissions (characters per hour) for each communication circuit, each computer, or whatever is appropriate for the network. It is important to closely monitor usage rates, the percentage of the theoretical capacity that is being used. These data can identify computers/devices or communication circuits that have higher-than-average error or usage rates, and they may be used for predicting future growth patterns and failures. A device or circuit that is approaching maximum usage obviously needs to be upgraded.

12.3 MANAGEMENT REPORTS

TECHNICAL FOCUS

Management-oriented reports that are helpful to network managers and their supervisors provide summary information for overall evaluation and for network planning and design. Details include:

- Graphs of daily/weekly/monthly usage, number of errors, or whatever is appropriate to the network
- Network availability (**uptime**) for yesterday, the last 5 days, the last month, or any other specific period
- Percentage of hours per week the network is unavailable because of network maintenance and repair
- Fault diagnosis

- Whether most response times are less than or equal to 3 seconds for online real-time traffic
- Whether management reports are timely and contain the most up-to-date statistics
- Peak volume statistics as well as average volume statistics per circuit
- Comparison of activity between today and a similar previous period

Such predictions can be accomplished by establishing simple **quality control charts** similar to those used in manufacturing. Programs use an upper control limit and a lower control limit with regard to the number of blocks in error per day or per week. Notice how Figure 12.4 identifies when the common carrier moved a circuit from one microwave channel to another (circuit B), how a deteriorating circuit can be located and fixed before it goes through the upper control limit (circuit A) and causes problems for the users, or how a temporary high rate of errors (circuit C) can be encountered when installing new hardware and software.

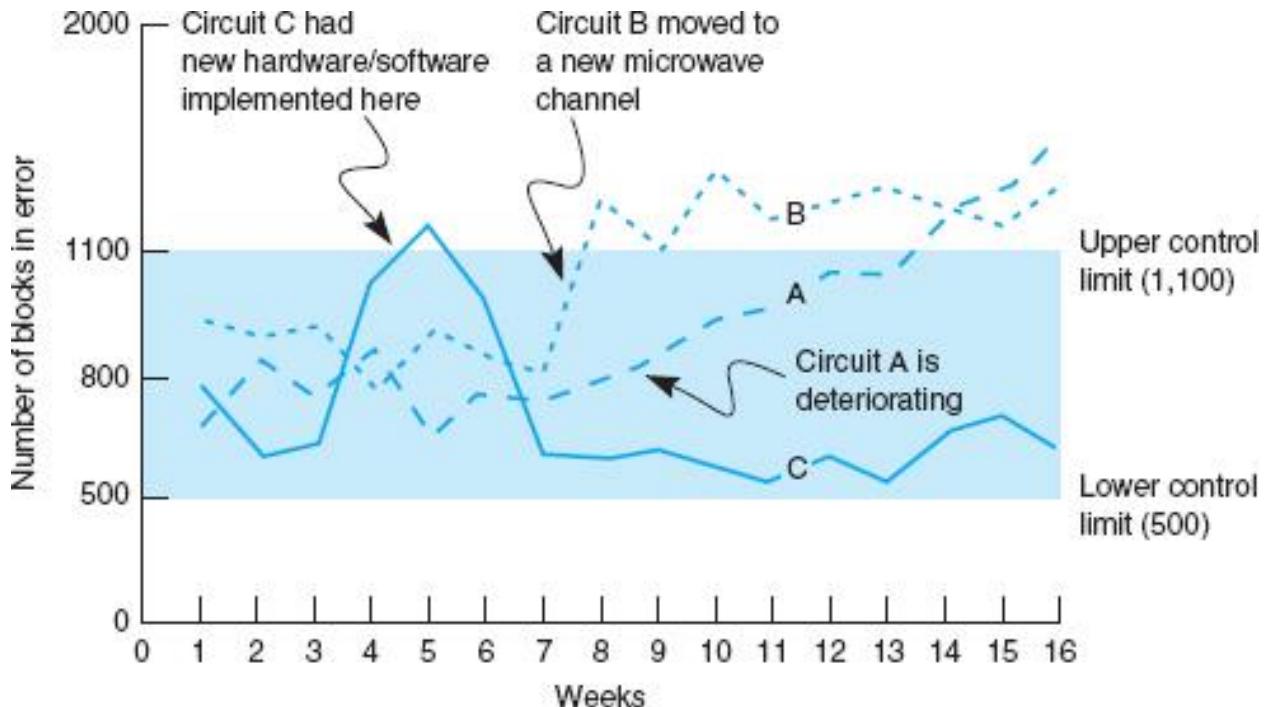


FIGURE 12.4 Quality control chart for circuits

12.4.4 IMPROVING PERFORMANCE

The chapters on LANs, BNs, and WANs discussed several specific actions that could be taken to improve network performance for each of those types of networks. There are also several general activities to improve performance that cut across the different types of networks.

Policy-Based Management A new approach to managing performance is policy-based management. With *policy-based management*, the network manager uses special software to set priority policies for network traffic that take effect when the network becomes busy. For example, the network manager might say that order processing and videoconferencing get the highest priority (order processing because it is the lifeblood of the company and videoconferencing because poor response time will have the greatest impact on it). The policy management software would then configure the network devices using the QoS capabilities in TCP/IP and/or ATM to give these applications the highest priority when the devices become busy.

Service-Level Agreements More organizations establish **service-level agreements (SLAs)** with their common carriers and Internet service providers. An SLA specifies the exact type of performance and fault conditions that the organization will accept. For example, the SLA might state that network availability must be 99 percent or higher and that the MTBF for T1 circuits must be 120 days or more. In many cases, SLA includes maximum allowable response times. The SLA also states what compensation the service provider must provide if it fails to meet the SLA. Some organizations are also starting to use an SLA internally to define relationships between the networking group and its organizational “customers.”

12.4 INSIDE A SERVICE-LEVEL AGREEMENT

TECHNICAL FOCUS

There are many elements to a solid service-level agreement (SLA) with a common carrier. Some of the important ones include

- Network availability, measured over a month as the percentage of time the network is available (e.g., [total hours—hours unavailable]/total hours) should be at least 99.5 percent
- Average round-trip permanent virtual circuit (PVC) delay, measured over a month as the number of seconds it takes a message to travel over the PVC from sender to receiver, should be less than 110 milliseconds, although some carriers will offer discounted services for SLA guarantees of 300 milliseconds or less
- PVC throughput, measured over a month as the number of outbound packets sent over a PVC divided by the inbound packets received at the destination (not counting packets over the committed information rate, which are discard eligible), should be above 99 percent—ideally, 99.99 percent
- Mean time to respond, measured as a monthly average of the time from inception of trouble ticket until repair personnel are on site, should be 4 hours or less
- Mean time to fix, measured as a monthly average of the time from the arrival of repair personnel on-site until the problem is repaired, should be 4 hours or less

SOURCE: “Carrier Service-Level Agreements,” International Engineering Consortium Tutorial, www.iec.org, February 2001.

12.5 END USER SUPPORT

Providing **end user support** means solving whatever problems users encounter while using the network. There are three main functions within end user support: resolving network faults, resolving user problems, and training. We have already discussed how to resolve network faults, and now we focus on resolution of user problems and end user training.

12.5.1 RESOLVING PROBLEMS

Problems with user equipment (as distinct from network equipment) usually stem from three major sources. The first is a failed hardware device. These are usually the easiest to fix. A network technician simply fixes the device or installs a new part.

The second type of problem is a lack of user knowledge. These problems can usually be solved by discussing the situation with the user and taking that person through the process step by step. This is the next easiest type of problem to solve and can often be done by email or over the telephone, although not all users are easy to work with. Problematic users are sometimes called ID ten-T errors, written ID10T.

The third type of problem is one with the software, software settings, or an incompatibility between the software and network software and hardware. In this case, there may be a bug in the software or the software may not function properly on a certain combination of hardware and software.

Solving these problems may be difficult because they require expertise with the specific software package in use and sometimes require software upgrades from the vendor.

Resolving either type of software problem begins with a request for assistance from the help desk. Requests for assistance are usually handled in the same manner as network faults. A trouble log is maintained to document all incoming requests and the manner in which they are resolved. The staff member receiving the request attempts to resolve the problem in the best manner possible. Staff members should be provided with a set of standard procedures or scripts for soliciting information from the user about problems. In large organizations, this process may be supported by special software.

There are often several levels to the problem-resolution process. The first level is the most basic. All staff members working at the help desk should be able to resolve most of these. Most organizations strive to resolve between 75 and 85 percent of requests at this first level in less than an hour. If the request cannot be resolved, it is escalated to the second level of problem resolution. Escalation is a normal part of the process and not something that is “bad.” Staff members who handle second-level support

have specialized skills in certain problem areas or with certain types of software and hardware. In most cases, problems are resolved at this level. Some large organizations also have a third level of resolution in which specialists spend many hours developing and testing various solutions to the problem, often in conjunction with staff members from the vendors of network software and hardware.

12.5.2 PROVIDING END USER TRAINING

End user training is an ongoing responsibility of the network manager. Training is a key part in the implementation of new networks or network components. It is also important to have an ongoing training program because employees may change job functions and new employees require training to use the organization's networks.

Training usually is conducted through in-class, one-on-one instruction, and online self-paced courses. In-class training should focus on the 20 percent of the network functions that the user will use 80 percent of the time instead of attempting to cover all network functions. By getting in-depth instruction on the fundamentals, users become confident about what they need to do. The training should also explain how to locate additional information from online support, documentation, or the help desk.

12.6 COST MANAGEMENT

One of the most challenging areas of network management over the past few years has been **cost management**. Data traffic has been growing much more rapidly than has the network management budget, which has forced network managers to provide greater network capacity at an ever lower cost per megabyte ([Figure 12.5](#)). In this section, we examine the major sources of costs and discuss several ways to reduce them.

12.6.1 SOURCES OF COSTS

The cost of operating a network in a large organization can be very expensive. [Figure 12.6](#) shows a recent cost analysis to operate the network for one year at Indiana University, a large Big Ten research university serving 36,000 students and 4,000 faculty and staff. This analysis includes

the costs of operating the network infrastructure and standard applications such as email and the Web, but does not include the costs of other applications such as course management software, registration, student services, accounting, and so on. Indiana University has a federal IT governance structure, which means that the different colleges and schools on campus also have budgets to hire staff and buy equipment for their faculty and staff. The budget in this figure omits these amounts, so the real costs are probably 50 percent higher than those shown. Nonetheless, this presents a snapshot of the costs of running a large network.

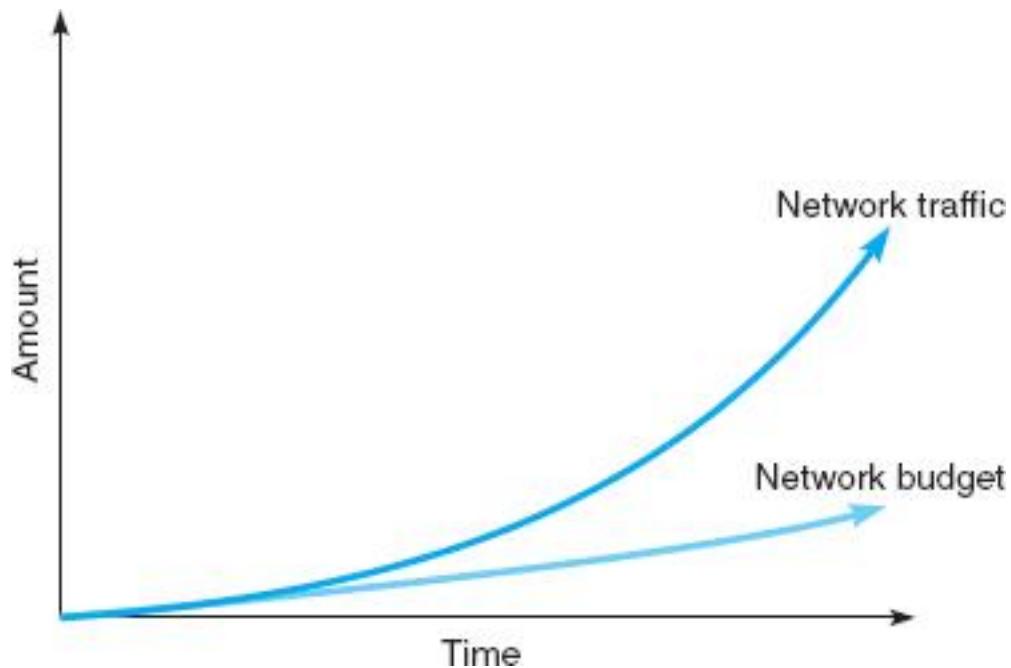


FIGURE 12.5 Network traffic versus network management budgets

Network Operations		\$14,871,000
Account Administration	275,000	
Authentication Services	257,000	
Directory Services Infrastructure (incl DHCP, DNS)	746,000	
E-mail and Messaging	1,434,000	
Mainframe and Cluster Operations	633,000	
Mass Data Storage	1,424,000	
Policy Management	75,000	
Printing	201,000	
Security Administration	1,270,000	
WAN Operations	7,410,000	
Web Services	1,146,000	
End User Support		\$6,544,000
Departmental Technology Support	553,000	
Instructional Technology Support	856,000	
Student Residence Halls Support	279,000	
Student Technology Centers Support	1,288,000	
Support Center (Help Desk)	2,741,000	
Training and Education	827,000	
Client Hardware		\$3,901,000
Classroom Technology Equipment and Supplies	844,000	
Student Residence Halls Equipment and Supplies	601,000	
Student Technology Centers Equipment and Supplies	2,456,000	
Application Software		\$3,729,000
Software Site Licenses	2,540,000	
Student Residence Halls Software	146,000	
Student Technology Centers Software	1,043,000	
Total		\$29,045,000

FIGURE 12.6 Annual networking costs at Indiana University

The largest area of costs in network operations is the \$7.4 million spent on WAN circuits. Indiana University operates many high-speed networks (including Internet2) so these costs are higher than might be expected. This figure also shows the large costs of email, Web services, data storage, and security. The cost of end user support is the next largest cost item. This includes training as well as answering users' questions and fixing their problems. The remaining costs are purchasing new and replacement hardware and software. But, once again, remember that this does not include the hardware and software purchased by individual colleges and schools for their faculty and staff which does not come from the central IT budget.

The **total cost of ownership (TCO)** is a measure of how much it costs per year to keep one computer operating. TCO includes the actual direct cost of repair parts, software upgrades, and support staff members to maintain the network, install software, administer the network (e.g., create user IDs, back up user data), provide training and technical support, and upgrade hardware and software. It also includes the indirect cost of time “wasted” by the user when problems occur, when the network is down, or when the user is attempting to learn new software.

Several studies over the past few years by Gartner Group, Inc, a leading industry research firm, suggest that the TCO of a computer is astoundingly high. Most studies suggest that the TCO for typical Windows computers on a network is about \$7,000 *per computer per year*. In other words, it costs almost five times as much *each year* to operate a computer than it does to purchase it in the first place. Other studies by firms such as IBM and *Information Week*, an industry magazine, have produced TCO estimates of between \$5,000 and \$10,000 per year, suggesting that the Gartner Group's estimates are reasonable.

Although TCO has been accepted by many organizations, other firms argue against the practice of including indirect in the calculation. For example, using a technique that includes indirect, the TCO of a coffee machine is more than \$50,000 per year—not counting the cost of the coffee or supplies. The assumption that getting coffee “wastes” 12 minutes per day times 5 days per week yields 1 hour per week, or about 50 hours per year, of wasted time. If you assume the coffeepot serves 20 employees who have an average cost of \$50 per hour (not an unusually high number), you have a loss of \$50,000 per year.

Some organizations, therefore, prefer to focus on costing methods that examine only the direct costs of operating the computers, omitting softer indirect costs such as “wasted” time. Such measures, often called **network cost of ownership (NCO)** or *real TCO*, have found that NCO ranges between \$1,500 and \$3,500 *per computer per year*. The typical network management group for a 100-user network would therefore have an annual budget of about \$150,000 to \$350,000. The most expensive item is personnel (network managers and technicians), which typically accounts

for 50 to 70 percent of total costs. The second most expensive cost item is WAN circuits, followed by hardware upgrades and replacement parts. Calculating TCO for universities can be difficult. Do we calculate TCO for the number of computers or the number of users. Figure 12.6 shows an annual cost of \$29 million. If we use the number of users, the TCO is about \$725 (\$29 million divided by 40,000 users). If we use the number of computers, TCO is \$4,800 (\$29 million divided by about 6,000 computers owned by the university).

There is one very important message from this pattern of costs. Because the largest cost item is personnel time, the primary focus of cost management lies in designing networks and developing policies to reduce personnel time, not to reduce hardware cost. Over the long term, it makes more sense to buy more expensive equipment if it can reduce the cost of network management.

Figure 12.7 shows the average breakdown of personnel costs by function. The largest time cost (where staff members spend most of their time) is systems management, which includes configuration, fault, and performance management tasks that focus on the network as a whole. The second largest item is end user support.

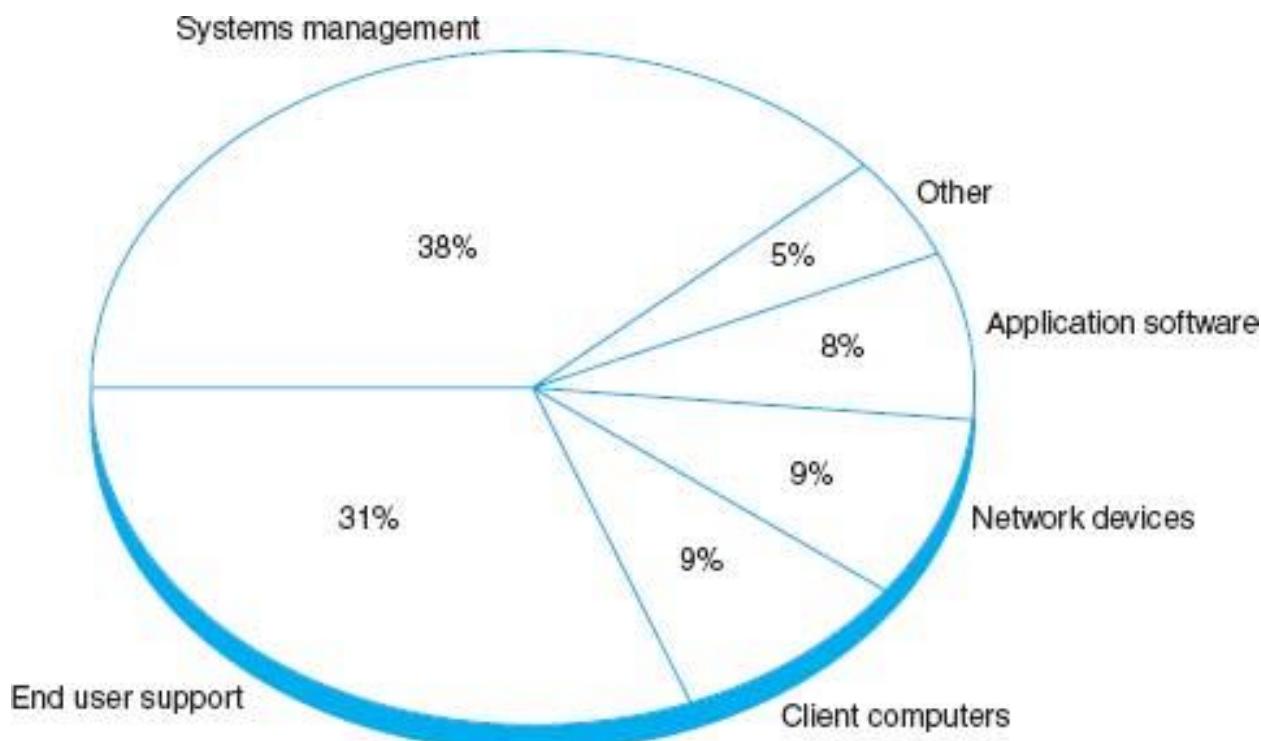


FIGURE 12.7 Network management personnel costs

Network managers usually find it difficult to manage their budgets because networks grow so rapidly. They often find themselves having to defend ever-increasing requests for more equipment and staff. To counter these escalating costs, many large organizations have adopted **charge-back policies** for users of WANs and mainframe-based networks. (A charge-back policy attempts to allocate the costs associated with the network to specific users.) These users must “pay” for their network usage by transferring part of their budget allocations to the network group. Such policies are seldom used in LANs, making one more potential cultural difference between network management styles.

12.6.2 REDUCING COSTS

Given the huge amounts in TCO or even the substantial amounts spent in NCO, there is considerable pressure on network managers to reduce costs. Figure 12.8 summarizes five steps to reduce network costs.

The first and most important step is to develop standards for client computers, servers, and network devices (i.e., switches, routers). These standards define one configuration (or a small set of configurations) that are permitted for all computers and devices. Standardizing hardware and software makes it easier to diagnose and fix problems. Also, there are fewer software packages for the network support staff members to learn. The downside, of course, is that rigid adherence to standards reduces innovation.

Five Steps to Reduce Network Costs

- Develop standard hardware and software configurations for client computers and servers.
- Automate as much of the network management function as possible by deploying a solid set of network management tools.
- Reduce the costs of installing new hardware and software by working with vendors.
- Centralize help desks.
- Move to thin-client architectures.

FIGURE 12.8 Reducing network costs

12.6 TOTAL COST OF OWNERSHIP IN MINNESOTA

MANAGEMENT FOCUS

Total Cost of Ownership (TCO) has come to the classroom. As part of a national TCO initiative, several school districts, including one in Minnesota, recently conducted a TCO analysis. The school district was a system of eight schools (one high school, one middle school, and six elementary schools) serving 4,100 students in kindergarten through grade 12. All schools are connected via a frame relay WAN to the district head office.

Costs were assessed in two major groups: direct costs and indirect costs. The direct costs included the costs of hardware (replacement client computers, servers, networks, and printers and supplies), software, internal network staff, and external consultants. The indirect costs included staff training and development. “Wasted time” was not included in the TCO analysis.

The district examined its most recent annual budget and allocated its spending into these categories. The district calculated that it spent about \$1.2 million per year to support its 1,200 client computers, providing a TCO of about \$1,004 per client computer per year. Figure 12.9 provides a summary of the costs by category.

A TCO of \$1,004 is below average, indicating a well-managed network. The district had implemented several network management best practices, such as using a standardized set of software, using new standardized hardware, and providing professional development to teachers to reduce support costs. One other major contributing factor was the extremely low salaries paid to the IT technical staff (less than \$25,000 per year) because of the district's rural location. Had the district been located in a more urban area, IT staff costs would double, bringing TCO closer to the lower end of the national average.

SOURCE: “Minnesota District Case Study,” Taking TCO to the Classroom, k12tco.gartner.com, 2004.

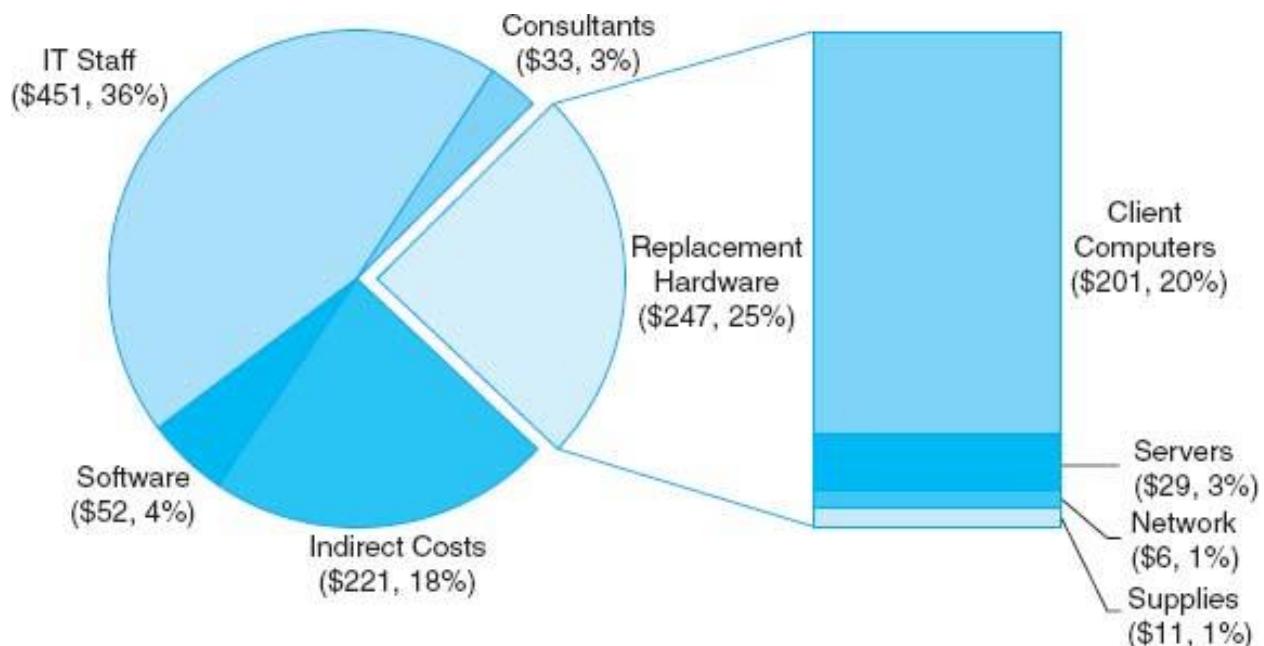


FIGURE 12.9 Total Cost of Ownership (per client computer per year) for a Minnesota school district

The second most important step is automate as much of the network management process as possible. Desktop management can significantly reduce the cost to upgrade when new software is released. It also enables faster installation of new computers and faster recovery when software needs to be reinstalled and helps enforce the standards policies. Dynamic address assignment (e.g., DHCP; see [Chapter 5](#)) can reduce time spent on managing TCP/IP addresses. The use of network management software to identify and diagnose problems can significantly reduce time spent in performance and fault management. Likewise, help desk software can cut the cost of the end support function.

A third step is to do everything possible to reduce the time spent installing new hardware and software. The cost of a network technician's spending half a day to install and configure new computers is often \$300 to \$500. Desktop management is an important step to reducing costs, but careful purchasing can also go a long way. The installation of standard hardware and software (e.g., Microsoft Office) by the hardware vendor can significantly reduce costs. Likewise, careful monitoring of hardware failures can quickly identify vendors of less reliable equipment who should be avoided in the next purchasing cycle.

Traditionally, help desks have been decentralized into user departments. The result is a proliferation of help desks and support staff members, many of whom tend to be generalists rather than specialists in one area. Many organizations have found that centralizing help desks enables them to reduce the number of generalists and provide more specialists in key technology areas. This results in faster resolution of difficult problems. Centralization also makes it easier to identify common problems occurring in different parts of the organization and take actions to reduce them. Finally, many network experts argue that moving to thin-client architectures, just Web browsers on the client (see [Chapter 2](#)), can significantly reduce costs. Although this can reduce the cost to buy software, the real saving lies in the support costs. Because they are restricted to a narrow set of functions and generally do not need software installations, thin-client architectures become much easier to manage. TCO and NCO drop by 20 to 40 percent. Most organizations anticipate using thin-client architectures selectively, in areas where applications are well defined and can easily be restricted.

12.7 IMPLICATIONS FOR MANAGEMENT

Network management is one of the more challenging functions because it requires a good understanding of networking technologies, an ability to work with end users and management, and an understanding of the key elements driving networking costs. Normally no one notices it until something goes wrong.

As demand for network capacity increases, the costs associated with network management have typically increased in most organizations. Justifying these increased costs to senior management can be challenging because senior management often do not see greatly increasing amounts of network traffic—all they see are increasing costs. The ability to explain the business value of networks in terms understandable to senior management is an important skill.

As networks become larger and more complex, network management will increase in complexity. New technologies for managing networks will be developed, as vendors attempt to increase the intelligence of networks and

their ability to “self-heal.” These new technologies will provide significantly more reliable networks, but will also be more expensive and will require new skills on the part of network designers, network managers, and network technicians. Keeping a trained network staff will become increasingly difficult because once staff acquire experience with the new management tools, they will be lured away by other firms offering higher salaries—which, we suppose, is not a bad thing if you’re one of the network staff.

SUMMARY

Integrating LANs, WANs, and the Internet Today, the critical issue is the integration of all organizational networks. The keys to integrating LANs, WANs, and the Web into one overall organization network are for WAN managers to recognize that LAN/Web managers can make independent decisions and for LAN/Web managers to realize that they need to work within organizational standards.

Integrating Voice and Data Communications Another major challenge is combining voice communications with data and image communications. This separation of voice and data worked well for years, but changing communication technologies are generating enormous pressures to combine them. A key factor in voice/data integration might turn out to be the elimination of one key management position and the merging of two staffs into one.

Configuration Management Configuration management means managing the network's hardware and software configuration, documenting it, and ensuring the documentation is updated as the configuration changes. The most common configuration management activity is adding and deleting user accounts. The most basic documentation about network hardware is a set of network configuration diagrams, supplemented by documentation on each individual network component. A similar approach can be used for network software. Desktop management plays a key role in simplifying configuration management by automating and documenting the network configurations. User and application profiles should be automatically provided by the network and desktop management software. There are a

variety of other documentation that must be routinely developed and updated, including users' manuals and organizational policies.

Performance and Fault Management Performance management means ensuring the network is operating as efficiently as possible. Fault management means preventing, detecting, and correcting any faults in the network circuits, hardware, and software. The two are closely related because any faults in the network reduce performance and because both require network monitoring. Today, most networks use a combination of smart devices to monitor the network and issue alarms and a help desk to respond to user problems. Problem tracking allows the network manager to determine problem ownership or who is responsible for correcting any outstanding problems. Problem statistics are important because they are a control device for the network operators as well as for vendors.

Providing End User Support Providing end user support means solving whatever network problems users encounter. Support consists of resolving network faults, resolving software problems, and training. Software problems often stem from lack of user knowledge, fundamental problems with the software, or an incompatibility between the software and the network's software and hardware. There are often several levels to problem resolution. End user training is an ongoing responsibility of the network manager. Training usually has two parts: in-class instruction and the documentation and training manuals that the user keeps for reference.

Cost Management As the demand for network services grows, so does its cost. The TCO for typical networked computers is about \$10,000 per year per computer, far more than the initial purchase price. The network management cost (omitting "wasted" time) is between \$1,500 and \$3,500 per year per computer. The largest single cost item is staff salaries. The best way to control rapidly increasing network costs is to reduce the amount of time taken to perform management functions, often by automating as many routine ones as possible.

KEY TERMS

availability

charge-back policy
configuration management
cost management
desktop management
downtime
end user support
fault management
firefighting
help desk
logical network parameters
mean time between failures (MTBF)
mean time to diagnose (MTTD)
mean time to fix (MTTF)
mean time to repair (MTTR)
mean time to respond (MTTR)
monitor
network cost of ownership (NCO)
network documentation
network management
network monitoring
network operations center (NOC)
network weather map
performance management
physical network parameters
problem statistics

problem tracking

quality control chart

service-level agreement (SLA)

total cost of ownership (TCO)

trouble ticket

uptime

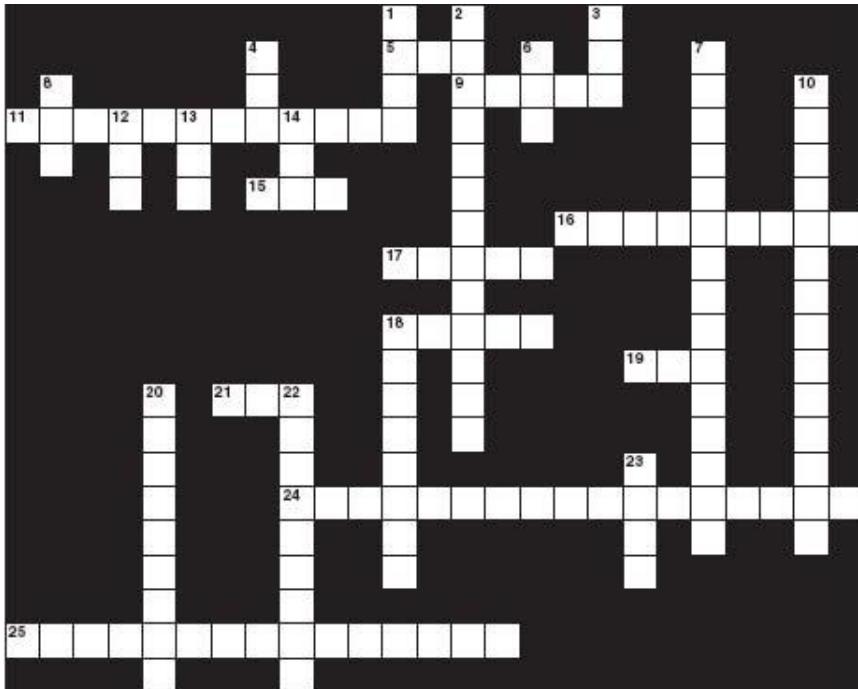
QUESTIONS

1. What are some differences between LAN and WAN management?
2. What is firefighting?
3. Why is combining voice and data a major organizational challenge?
4. Describe what configuration management encompasses.
5. People tend to think of software when documentation is mentioned.
What is documentation in a network situation?
6. What is desktop management and why is it important?
7. What is performance and fault management?
8. What does a help desk do?
9. What do trouble tickets report?
10. Several important statistics related to network uptime and downtime are discussed in this chapter. What are they and why are they important?
11. What is an SLA?
12. How is network availability calculated?
13. What is problem escalation?
14. What are the primary functions of end user support?
15. What is TCO?
16. Why is the TCO so high?
17. How can network costs be reduced?
18. What do network management software systems do and why are they important?

19. How does network cost of ownership differ from total cost of ownership? Which is the most useful measure of network costs from the point of view of the network manager? Why?
20. Many organizations do not have a formal trouble reporting system. Why do you think this is the case?

EXERCISES

- 12-1.** What factors might cause peak loads in a network? How can a network manager determine if they are important and how are they taken into account when designing a data communications network?
- 12-2.** Today's network managers face a number of demanding problems. Investigate and discuss three major issues.
- 12-3.** Research the networking budget in your organization and discuss the major cost areas. Discuss several ways of reducing costs over the long term.
- 12-4.** Explore the Internet2 weather map at abilene.internet2.edu.
- 12-5.** Do the puzzle on the next page.



Across

- 5. A measure of cost effectiveness that includes direct and indirect costs
- 9. The first step in network design is to examine user _____
- 11. A device that sends requests to different servers in a cluster
- 15. A measure of cost effectiveness that focuses only on direct costs
- 16. This form of encryption has two keys
- 17. One of the most common security threats
- 18. This fixes a security hole
- 19. A device that prevents power loss
- 21. The document asking vendors to bid on a proposal
- 24. A non-technical way to get someone's password
- 25. Storing your content on other people's servers

Down

- 1. The average time it takes to fix a broken device
- 2. Documenting the network is part of _____ management
- 3. A system to prevent intrusion
- 4. A contract with a common carrier always has this
- 6. A strong encryption standard
- 7. This device limits the amount of network capacity available to a user
- 8. Denial of service
- 10. Storing other people's Web content on your network
- 12. Obsolete encryption standard
- 13. The highest level of security is to check something you _____
- 14. Staff working in this organization monitor the network
- 18. Using email to trick users into revealing their password
- 20. This form of encryption has one key
- 22. The largest single part of a networking budget is the cost of _____
- 23. A network management standard

MINI-CASES

I. City School District, Part 1

City School District is a large, urban school district that operates 27 schools serving 22,000 students from kindergarten through grade 12. All schools are networked into a regional WAN that connects the schools to the district central office and each other. The district has a total of 5,300 client computers. The table below shows the annual costs. Calculate the real TCO (without wasted time).

Budget Item	Annual Cost
IT Staff Salaries	\$7,038,400
Consultants	1,340,900
Software	657,200
Staff training	545,900
Client computers	2,236,600
Servers	355,100
Network	63,600
Supplies and parts	2,114,700

II. City School District, Part 2

Read and complete Mini-case I above. Examine the TCO by category. Do you think that this TCO indicates a well-run network? What suggestions would you have?

III. Central Textiles

Central Textiles is a clothing manufacturer that operates 16 plants throughout the southern United States and in Latin America. The Information Systems Department, which reports to the vice president of finance, operates the central mainframe and LAN at the headquarters building in Spartanburg, South Carolina, and the WAN that connects all the plants. The LANs in each plant are managed by a separate IT group at each plant that reports to the plant manager (the plant managers report to the vice president of manufacturing). The telephone communications system and long-distance agreements are managed by a telecommunications department in the headquarters that reports to the vice president of finance. The CEO of Central Textiles has come to you asking about whether this is the best arrangement, or whether it would make more sense to integrate the three functions under one new department. Outline the pros and cons of both alternatives.

IV. Internet2

Reread Management Focus 12.5. If the weather map shown in Figure 12.3 is a typical traffic pattern for Internet2, how would you suggest that they improve performance?

CASE STUDY

NEXT-DAY AIR SERVICE

See the Web site.

HANDS-ON ACTIVITY 12A

NETWORK MONITORING

One of the key tasks of network management is monitoring the network to make sure everything is running well. There are many effective network monitoring tools available and several have demonstrations you can view on the Web. One of my favorites is solarwinds.net. They have a live demonstration of their network management software available at npm.solarwinds.net.

Once you arrive at their page you can select which part of their network to examine. [Figure 12.10](#) shows the U.S. portion of the network. It shows a map of the network with circuits and locations color coded to show their status (green for good, yellow for some problems, and red for major problems), although the colors are hard to see in the figure. You can click on a circuit, a city, or a link on the bottom of the page to obtain more information about that part of the network.

The Tulsa Office shows green on the map, with a small red box next to it in the more detailed listing below the map. This indicates that the network is operating well, but that there is minor trouble with some part of the network that is not having a major impact.

[Figure 12.11](#) shows what happened when I clicked on the Tulsa Office. We now see the details of the network in Tulsa. It has a set of switches and routers, all of which are green, except the Amsterdam Lab Router (GWC198) which is shown in bright red (although it's hard to see the real colors from this figure). The table below the network map also says that the router is down, again in bright red letters, in addition to a red bullet in front of the line.

You can click on any device in the picture or in the table to obtain more information about it. [Figure 12.12](#) shows the status of the Gateway Router which connects the Tulsa Office to the 12vBNS network at the top of the display. At first glance, you can see the four “dashboard gauges” that show that response time is good at below 150 milliseconds, that there is no noticeable packet loss, that the CPU load is good at less than 30 percent, and that memory usage is hitting the high level at almost 75 percent. Memory usage is not yet a problem, but it's probably time to plan for a memory upgrade before the device begins to have problems from running out of memory.

The two graphs in this figure show data over the past 12 hours for comparison. The first graph shows a few spikes in response time in the morning (a Monday morning) as people returning from the weekend begin reading email, but nothing that would be a problem. Likewise, between 2 a.m. and 5 a.m., something happened to cause some packet loss but it was not substantial (major thunderstorms swept through Tulsa overnight, so they may have been to blame). The second graph shows that the CPU load was fairly constant over the last 12 hours, always below 30 percent.

The rest of the display shows additional information about the device, such as what it is (a Cisco 1601 router), what version of the operating system it is running (12.0(8)), its IP address (65.113.77.57), and when it was last booted (2:33 a.m., March 2, 2006).

DELIVERABLES

1. What is the general status of the Boston location right now?
2. Are there any problems in the Boston location? If so, describe them.
3. Pick one of the devices in Boston. How has response changed over the past 24 hours?

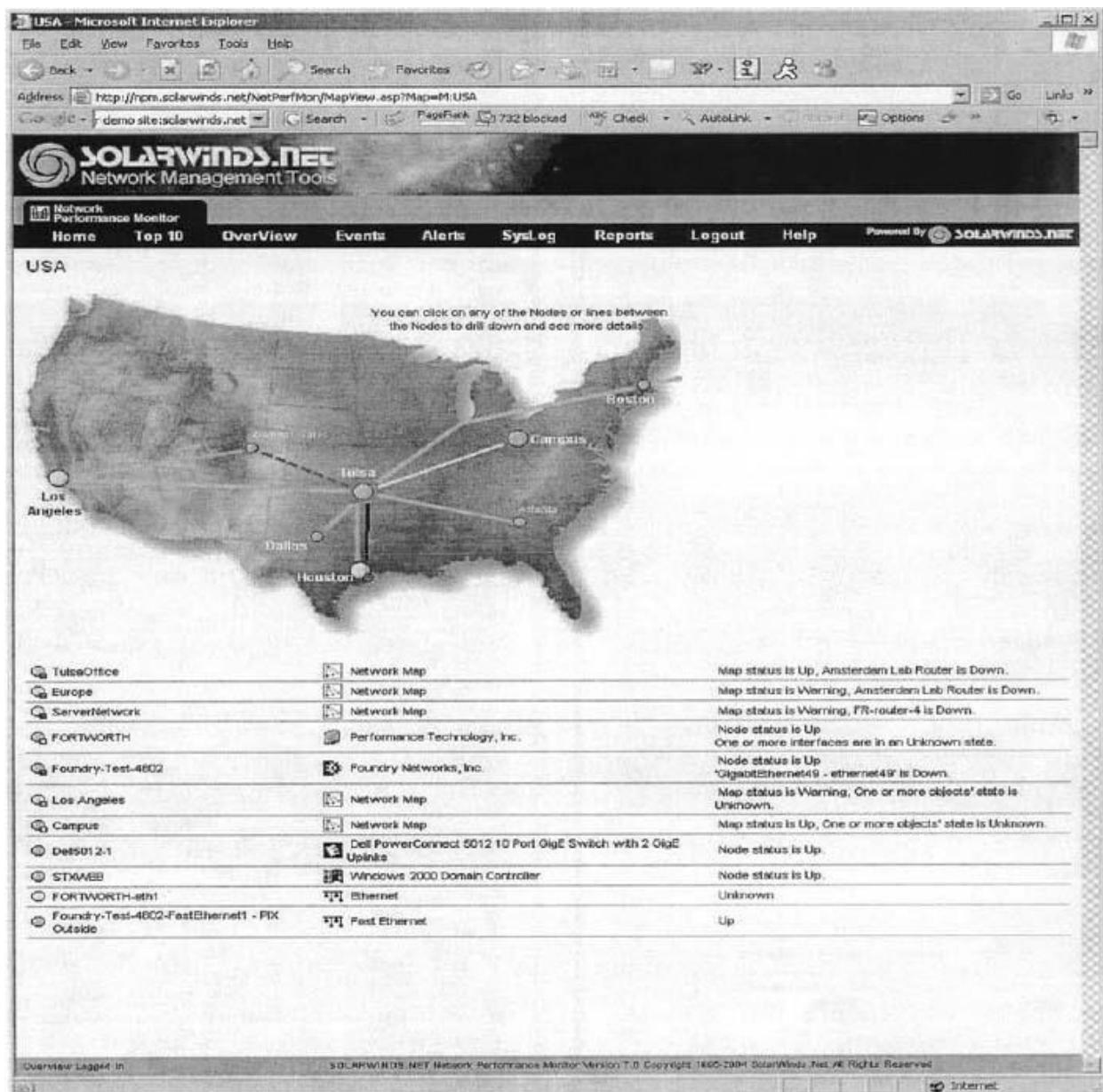


FIGURE 12.10 Solarwinds.net network monitoring software

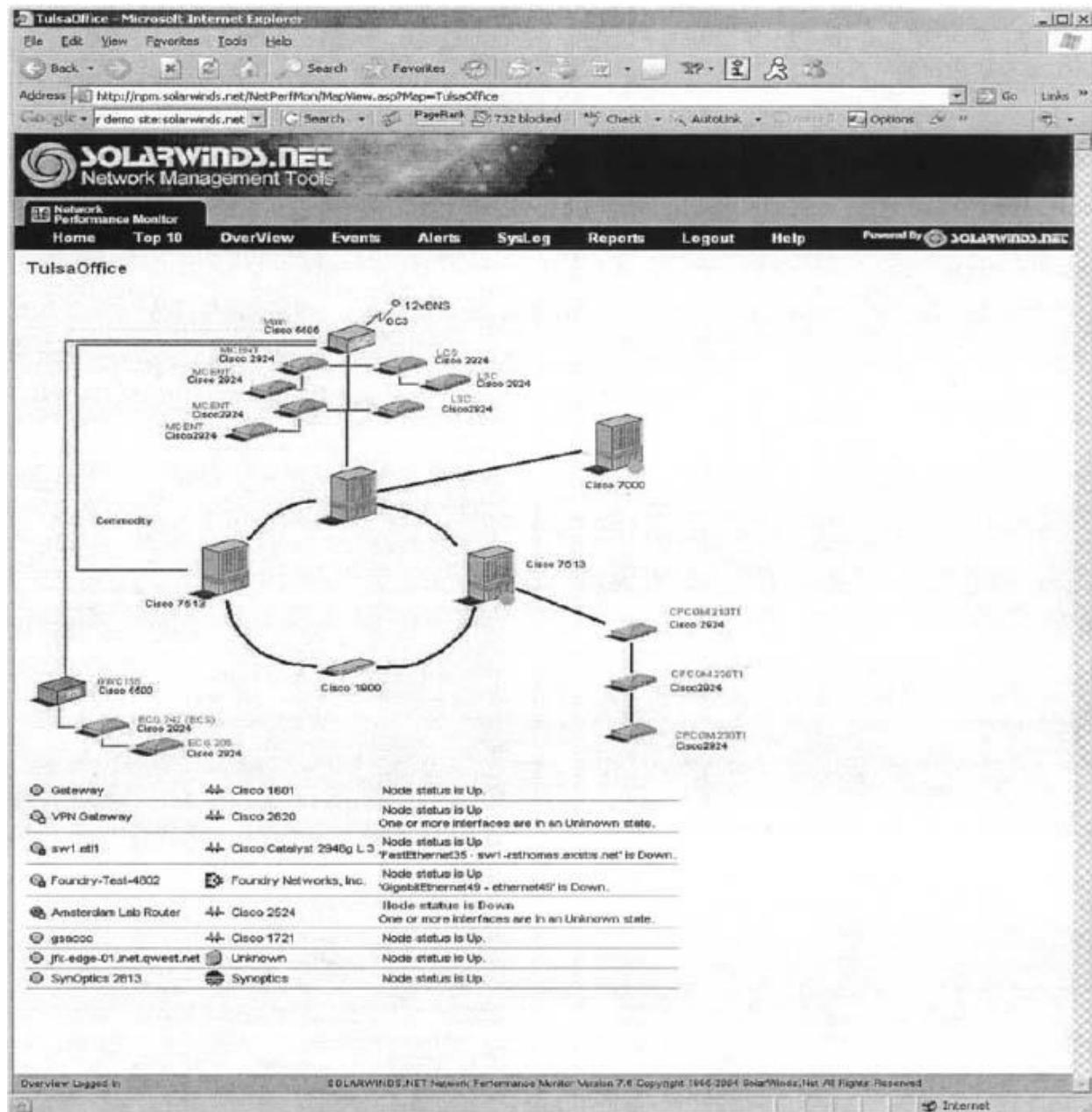


FIGURE 12.11 Status of the Tulsa office

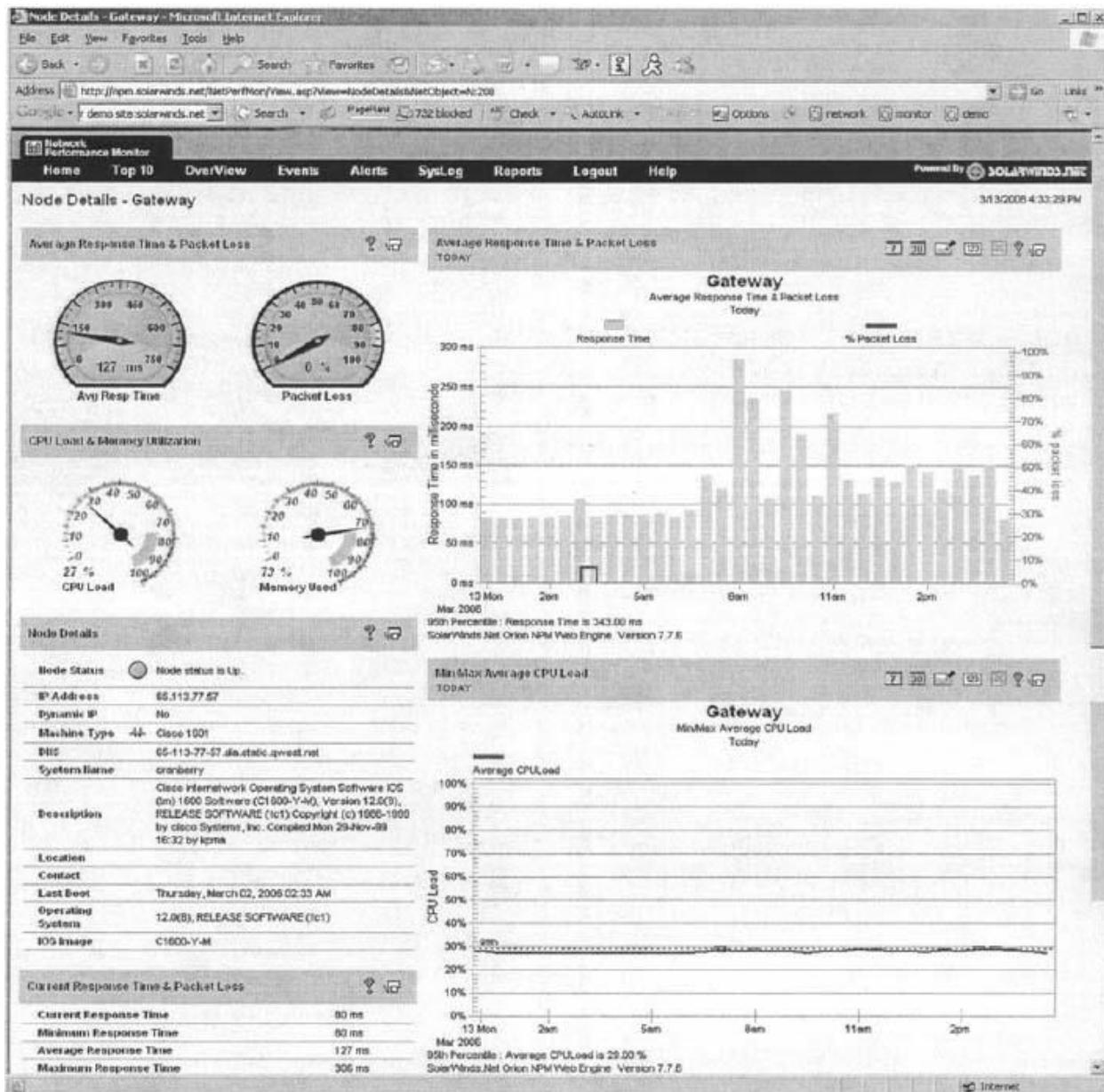


FIGURE 12.12 Information about the Gateway router

¹ One example of network weather maps for the Internet that provides a simple overview is www.InternetTrafficReport.com.

PART FIVE

APPENDICES

APPENDIX A

CONNECTOR CABLES

When a message leaves a computer and begins to move onto the network, the first component it encounters is the *connector cable* between the computer and the circuit. When people discuss connector cables, the focus is on the standards (such as RS232 or RS449).

A.1 RS232 (DB-25)/RS449 (DB-9)

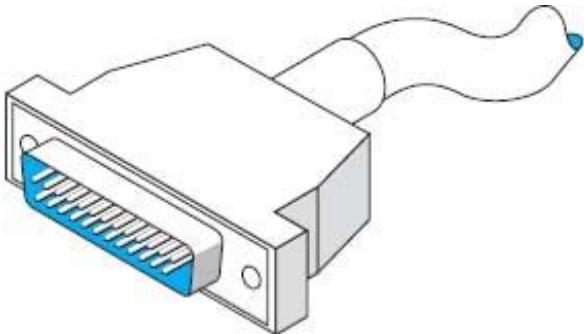
When people talk about connector cables, they frequently refer to them as a *RS232*, *DB-25*, *RS449*, or *DB-9*. This is because each connector cable is based on a specified standard. Calling the connector by its standard designation allows everyone to know precisely which connector is being discussed.

The RS232 standard is the most frequently mentioned. It was first issued in 1962, and its third revision, RS232C, was issued in 1969. The RS232D standard was issued in 1987 to expand on RS232C. The RS232D standard is also known as the EIA-232-D.

The RS232 connector cable is the standard interface for connecting *data terminal equipment (DTE)* to *data circuit terminating equipment (DCE)*. The newer RS232D is specified as having 25 wires and using the DB-25 connector plug like the one used on computers. If this connector cable is attached to a computer, people may refer to it simply as DB-25; if it is not attached to a computer, they may refer to it as the RS232 interface.

DTE comprises the data source, the data sink, or both. In reality, it is any piece of equipment at which a data communications path begins or ends, such as a terminal. DCE provides all the functions required to establish, maintain, and terminate a connection. This includes signal conversion and coding between the DTE and the common carrier's circuit, including the modem. A modem is DCE.

Figure A.1 shows a picture of the RS232D interface plug and describes each of its 25 protruding pins. It is the standard connector cable (25 wires/pins) that passes control signals and data between the terminal (DTE) and the modem (DCE). This standard has been supplied by the Electronic Industries Association (EIA). Outside the United States, this RS232D connector cable is known as the V.24 and V.28. The V.24 and V.28 standards have been accepted by the international standards group known as the ITU-T. These standards provide a common description of what the signal coming out of and going into the serial port of a computer or terminal looks like electrically. Specifically, RS232 provides for a signal changing from a nominal +12 volts to a nominal -12 volts. The standard also defines the cables and connectors used to link data communications devices. This is the cable that connects an external modem to your computer.



Pin	Circuit Name
1	Shield
2	Transmitted data
3	Received data
4	Request to send
5	Clear to send
6	DCE ready
7	Signal ground
8	Received line signal detector
9	(Reserved for testing)
10	(Reserved for testing)
11	(Unassigned)
12	Secondary received line signal detector/data signal rate select (DCE source)
13	Secondary clear to send
14	Secondary transmitted data
15	Transmitter signal element timing (DCE source)
16	Secondary received data
17	Receiver signal element timing (DCE source)
18	Local loopback
19	Secondary request to send
20	DTE ready
21	Remote loopbacks/signal quality detector
22	Ring indicator
23	Data signal rate select (DTE/DCE source)
24	Transmitter signal element timing (DTE source)
25	Text mode

FIGURE A.1 RS232 cable specifications. DCE = data circuit terminating equipment; DTE = data terminal equipment

The RS232 has a maximum 50-foot cable length, but it can be increased to 100 feet or more by means of a special low-capacitance, extended-distance cable. This is not advised, however, because some vendors may

not honor maintenance agreements if the cable is lengthened beyond the 50-foot standard.

In illustration, we present the cable distances for Texas Instruments' products. The cable length of the RS232 varies according to the speed at which you transmit. For Texas Instruments, the connector cable length can be up to 914 meters (1 meter = 1.1 yards) when transmitting at 1,200 bps, 549 meters when transmitting at 2,400 bps, 244 meters when transmitting at 4,800 bps, and 122 meters when transmitting at 9,600 bps. When end users operate equipment at maximum distances, it is important to remember that they must meet the restrictions on all types of equipment used, including the electrical environment, cable construction, and cable wiring. This means that when you want to operate at a maximum cable distance, you must contact the computer and/or modem vendors to obtain their maximum cable distance before you proceed.

The RS449 standard has been adopted as U.S. Federal Standard 1031. The RS449 is shown in [Figure A.2](#). A 4,000-foot cable length can be used, there are 37 pins instead of 25 (useful for digital transmission), and various other circuit functions have been added, such as diagnostic circuits and digital circuits. In addition, secondary channel circuits (reverse channel) have been put into a separate 9-pin connector known as a DB-9. The serial port on your microcomputer may be either a DB-9 or a DB-25.

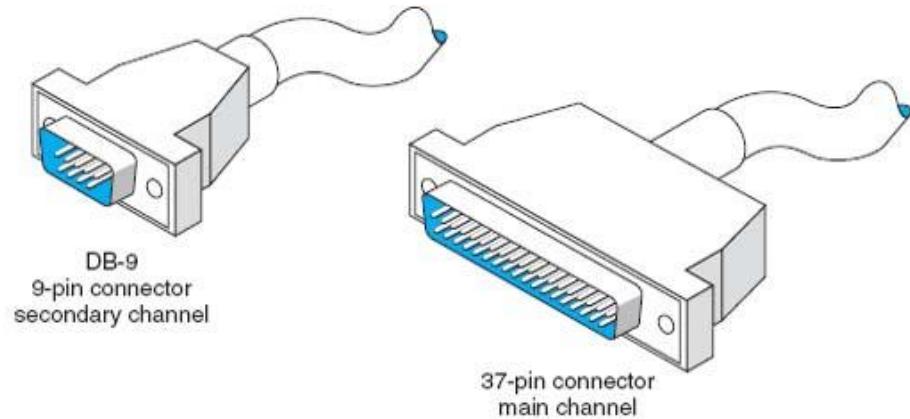
For some of the new features, look at pin 32 (Select standby). With this pin, the terminal can instruct the modem to use an alternate standby network such as changing from a private leased line to a public packet network, either for backup or simply to access another database not normally used. In other words, a terminal can be connected to two different networks, and the operator can enter a keyboard command to switch the connection from one network to another. With regard to loopback pins 10 and 14, the terminal can allow basic tests without special test equipment or the manual exchanging of equipment or cables.

With microcomputers, the RS232 and RS449 also are referred to as D-type connectors. As stated above, the RS232 may be called a DB-25, and the 9-pin RS449 may be called a DB-9. Look at [Figure A.3](#) to see the computer pin configurations for these two connectors.

There are also X.20 and X.21 interface cables. The X.20 interface is for asynchronous communications, and the X.21 is for synchronous communications. Each is based on only 15 pins (wires) connecting the DTE and the DCE; the presence of fewer pins requires an increased intelligence in both the DTE and the DCE. X.20 and X.21 are international standards intended to provide an interface with the X.25 packet switching networks discussed elsewhere in this book.

Another option that may become available in the near future is a fiber-optic cable in place of the standard RS232 electrical cables. Currently, by using fiber-optic cable, we can locate a computer 1,000 meters (3,280 feet) from a server. With a 1,000-meter fiber-optic cable, these products can communicate at speeds ranging from 19,200 bps to twice that speed. Therefore, you get not only greater distance (1,000 meters) but also greater speed. This may be another example in which fiber optics eventually will replace electronics.

The *high-speed serial interface (HSSI)* is beginning to appear in new products. HSSI defines the physical and electrical interface between the DTE and the DCE equipment. It was developed by Cisco Systems of Menlo Park, California, and T3plus of Santa Clara, California. They have submitted it to the American National Standards Institute, which also formalized the EIA-232 and V.35 standards. HSSI allows data transfers over the connector cable at 52 million bps, whereas RS-449 cannot handle more than 10 million bps. HSSI is a 50-pin connector using shielded twisted-pair cabling.

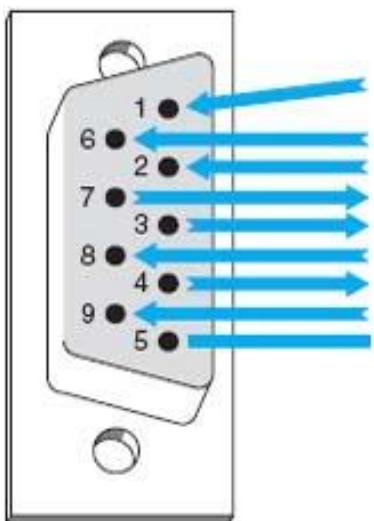
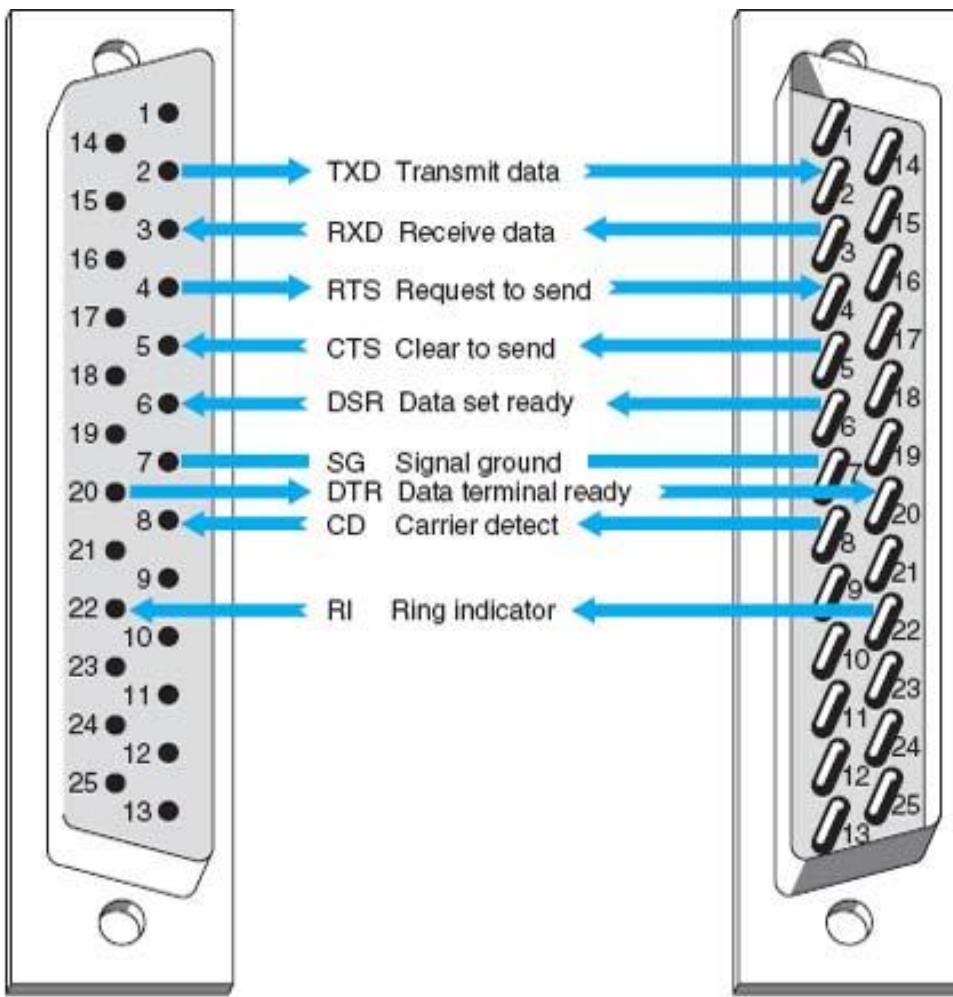


37-Pin Connector				9-Pin Connector	
Pin	First Segment Assignment Function	Pin	Second Segment Assignment Function	Pin	Function
1	Shield	20	Receive common	1	Shield
2	Signaling rate indicator	21	(Unassigned)	2	Secondary receiver
3	(Unassigned)	22	Send data ready	3	Secondary send data
4	Send data	23	Send timing	4	Secondary receive data
5	Send timing	24	Receive data	5	Signal ground
6	Receive data	25	Request to send	6	Receive common
7	Request to send	26	Receive timing	7	Secondary request to send
8	Receive timing	27	Clear to send	8	Secondary clear to send
9	Clear to send	28	Terminal in service	9	Send common
10	Local loopback	29	Data mode		
11	Data mode	30	Terminal ready		
12	Terminal ready	31	Receiver ready		
13	Receiver ready	32	Select standby		
14	Remote loopback	33	Signal quality		
15	Incoming call	34	New signal		
16	Select frequency/signaling rate selector	35	Terminal timing		
17	Terminal timing	36	Standby indicator		
18	Test mode	37	Send common		
19	Signal ground				

FIGURE A.2 RS449 cable specifications

A.2 NULL MODEM CABLE CONNECTIONS

Null modem cables allow transmission between two computers that are next to each other (6 to 8 feet apart) without using a modem. If you discover that the diskette from your computer will not fit into another one, that transmitting over telephone lines is impossible, or that you cannot transmit data easily from one computer to another for any reason, then it is time to get a null modem cable.



CD Carrier detect (used by a modem to indicate the presence of a carrier signal)
 DSR Data set ready
 RXD Receive data
 RTS Request to send
 XD Transmit data
 CTS Clear to send
 DTR Data terminal ready
 RI Ring indicator
 SG Signal ground

FIGURE A.3 Pin configurations

First, bring the two computers close together. Next, obtain a null modem cable (more on the pin connections shortly). The cable runs from the serial communication port on the first computer to the serial communication port on the second one. The cable is called a *null* modem cable because it eliminates the need for a modem. You can either build a null modem cable or buy one from any computer store. Null modem connector blocks are available to connect between two cables you already own.

To transfer data between two computers, just hook the null modem cable between them and call up one of the computers by using the communication software you normally use. To do so, put one computer in answer mode and use the other one to call it, but skip the step of dialing the telephone number. After the receiving computer has answered that it is ready, the data can be sent, just as you would on a normal long-distance dial-up connection. Basically, a null modem cable switches pins 2 and 3 (Transmit and Receive) of the RS232 connector plug.

A.3 DATA SIGNALING/SYNCHRONIZATION

Let us look at *data signaling* or *synchronization* as it occurs on a RS232 connector cable. Figure A.4 shows the 13 most frequently used pins of the 25-pin RS232 connector cable. A computer is on the left side of the figure and a modem is on the right.

Do you ever wonder what happens when you press the “send” key to transmit synchronous data? When a synchronous block of data is sent, the computer and the modem raise and lower electrical signals (plus and minus polarity) between themselves over the RS232 connector. This is usually a nominal +12 or -12 volts. For example, a modem with a RS232 interface might indicate that it is on and ready to operate by raising the signal on pin 6, *Data set ready*. (*Data set* is an older term for a modem.) When a call comes in, the modem shows the computer that the telephone line is ringing by raising a signal on pin 22, the *Ring indicator*. Raising a signal means putting +12 volts on the wire or pin. The computer may then tell the modem

to answer the call by raising a signal on pin 20, *Data terminal ready*. After the modems connect, the modem may indicate the connection status to the computer by raising a signal on pin 8, *Carrier detect*. At the end of the session, the microcomputer may tell the modem to drop the telephone call (release the circuit) by lowering the signal on pin 20, *Data terminal ready*. The *Request to send* and *Clear to send* signals go over pins 4 and 5, respectively, which are used in half-duplex modems to manage control of the communication channel. Incidentally, some of these basic procedures may vary slightly from one manufacturer to another.

Computer DTE side *Name and pin number* *Modem DCE side*

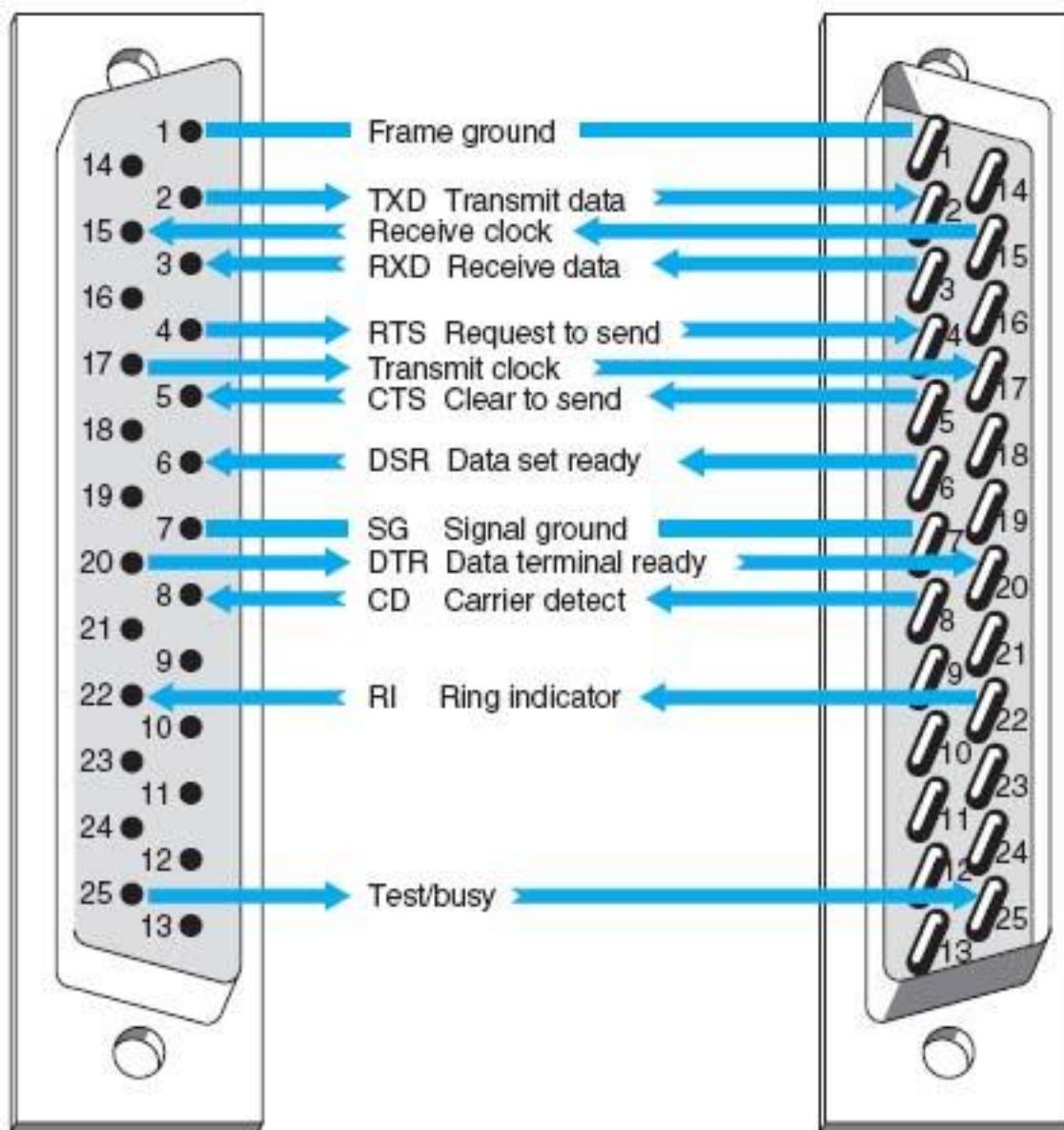


FIGURE A.4 Data signaling with RS232 cables. DCE 1-1-data circuit terminating equipment: DTE 1-1-data terminal equipment

Follow the pins and signal direction arrows in [Figure A.4](#) as we discuss an example that handles the flow of a block of synchronous data. When the computer operator presses the “send” key to transmit a block of data, pin 4, *Request to send*, transmits the signal from the computer to the modem. This informs the modem that a block of data is ready to be sent. The modem then sends a *Clear to send* signal back to the computer by using pin 5, thus telling the computer that it can send a synchronous block of data.

The computer now outpulses a serial stream of bits that contain two 8-bit SYN characters in front of the message block. A SYN character is 0110100 (decimal 22 in ASCII code). This bit stream passes over the connector cable to the modem using pin 2, *Transmit data*. The modem then modulates this data block to convert it from the digital signal (plus and minus polarity) to an analog signal (discussed in the next section). From the modem, the data go out onto the local loop circuit between your business premises and the telephone company central office. From there, it goes to the long-distance IXC and the receiving end's telephone company central office. Then it moves to the local loop, into the modem, across the connector cable, and into the server at the other end of the circuit.

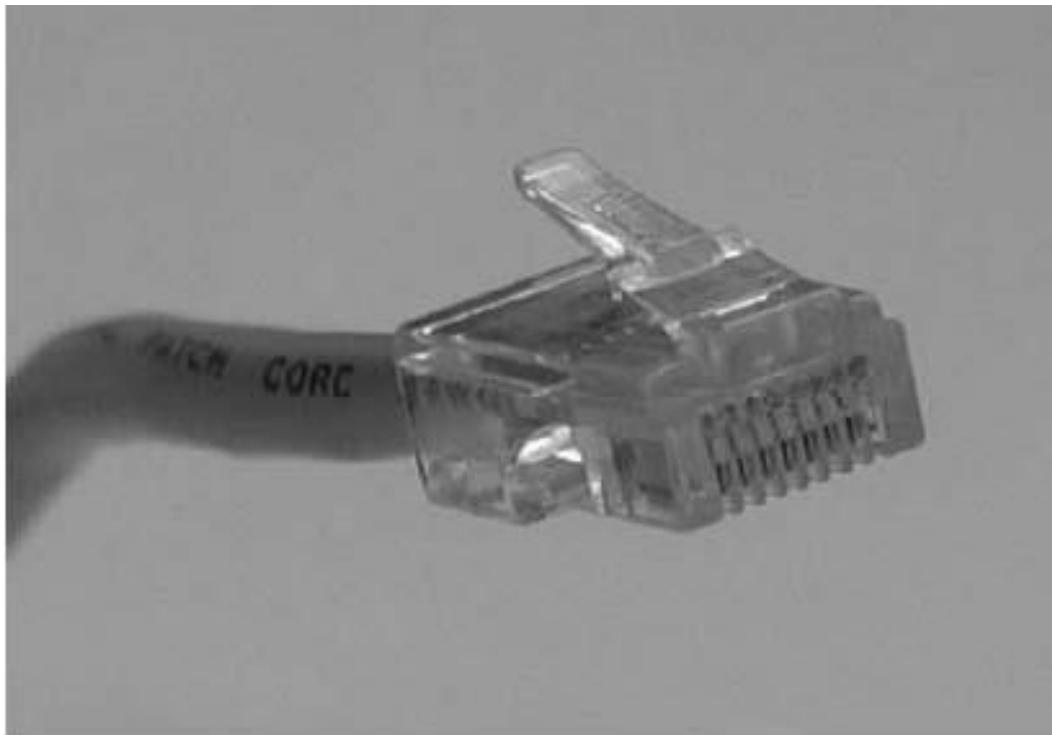
This process is repeated for each synchronous message block in half-duplex transmission. The data signaling that takes place between the computer and the modem involves the *Request to send*, *Clear to send*, and *Transmit datapins*. Accurate timing between blocks of data is critical in data signaling and synchronization. If this timing is lost, the entire block of data is destroyed and must be retransmitted.

A.4 ETHERNET AND RJ-45

A.4.1 10BASE-T

Ethernet 10Base-T is most often wired with cat 5 cable, which has four pairs of wire in each cable, but only two pairs are used so that cat 3 cable can still be used if desired. One pair of two wires is used to transmit from the computer to the hub (or switch), while the other pair of two wires is

used to receive data from the hub (or switch). Both wires in each pair transmit the same signal but with opposite polarity; the transmit + wire uses positive charges while the transmit—uses negative charges. This redundancy helps reduce errors and also reduces interference between the wires in the pair. Thus, 10Base-T is capable of full-duplex transmission at the hardware level, but it usually is only implemented as half-duplex.



Pin number	Color (EIA/TIA 568B standard)	Name
1	White with orange stripe	Transmit +
2	Orange with white stripe or solid orange	Transmit -
3	White with green stripe	Receive +
4	Blue with white stripe or solid blue	Not used
5	White with blue stripe	Not used
6	Green with white stripe or solid green	Receive -
7	White with brown stripe or solid brown	Not used
8	Brown with white stripe or solid brown	Not used

FIGURE A.5 Pins used by 10Base-T and 100Base-T at the computer end

Figure A.5 shows the way in which cat 5 cables are wired. The cable is wired into an RJ-45 connector,¹ which is an 8-pin connector used to plug into NICs, hubs, and switches. Pins 1 and 2 are the wires used to transmit

from the computer's NIC while pins 3 and 6 are used to receive transmissions at the computer's NIC. The pins on the hub or switch are reversed; that is, pins 1 and 2 deliver the computer's NIC's transmissions, so they are the receive pins at the hub or switch, while 3 and 6 are the receive pins at the hub or switch. Any time you want to directly connect two computer NICs or two hubs/switches, you must use a crossover cable, which connects pins 1 and 2 at one end to pins 3 and 6 at the other (and vice versa).

In order to successfully send and receive messages, both the sender and receiver have to agree how bits will be transmitted over the specific wires in the cable. They must understand both how fast the data will be sent and what electrical voltages will be used to represent a binary 1 and a binary 0. 10Base-T transmits at a rate of 10 Mbps, or 10 million bits per second. This means that the computers divide each second into 10 million time periods in which they can send data. Each time period (100nanoseconds [i.e., 100 billionths of a second]) contains one bit, either binary 1 or a binary 0. Thus each wire in the cat 3 or cat 5 cable must be capable of carrying a signal that changes 10 million times per second; we call this a *signaling rate* of 10 million Hertz, or 10 MHz.

One of the challenges in transmitting this fast is making sure that the clock at the receiver is synchronized with the clock at the sender so they can both understand when one of these 100-nanosecond time periods starts and stops. This is done by using *Manchester encoding*, a special type of signaling in which the signal is changed from high voltage (2 volts) to low voltage (0 volts) or vice versa in the middle of the signal. A change from low to high is used to represent a 1, while the opposite (a change from high to low) is used to represent a 0. Thus, in the exact middle of each time period, the signal voltage changes. This “heartbeat” synchronizes the clocks.

A.4.2 100BASE-T

Ethernet 100Base-T also transmits data over cat 5 cables. It uses exactly the same wiring and connector pin configurations as 10Base-T so that the wiring for the two types of LANs is identical.

100Base-T does not use Manchester encoding. 100Base-T uses *4B5B coding*, in which the data are sent in groups of 5 bits, the first 4 of which are data and the last one is used for clock synchronizing purposes and to minimize interference. The fifth bit is chosen to ensure than no more than 4 out of the 5 bits have the same value. Because of the high speed at which the data is being transmitted, a long series of all ones or all zeros would result in a long transmission of positive or negative voltage, which has a greater chance of causing interference to other wires than an alternating positive and negative pattern of voltages. Also, without regular changes in signal as is done in Manchester encoding, it becomes increasingly difficult to ensure that the clocks on the sender and receiver are synchronized. Adding this extra fifth bit every 4 bits of data ensures no long single-level transmissions are sent and ensures a transition for clock synchronizing. In order to achieve a data rate of 100 Mbps when using 4B5B, the sender and receiver have to operate at 125 MHz, because only 4 out of every 5 bits transmitted contain data. 100Base-T uses a technique called *Multi-Level Transmission–3 Level* (MLT-3) to transmit the 4B5B codes through the cable. With MLT-3, three levels of voltage are defined, +1 volts, 0 volts, and -1 volts. MLT-3 is based on changes in voltages like Manchester encoding, but in a different way. To send a binary zero, MLT-3 simply maintains the same voltage as used in the previous time slot. To transmit a binary 0, the voltage is changed to an adjacent level (e.g., from -1 to 0 or 0 to +1).

A.4.3 1 GBE

The version of 1 GbE that runs over twisted-pair cables is called 1000Base-T and runs over one cat 5 cable by using parallel transmission. That is, it uses each of the four pairs of wires in the cat 5 cable as a separate half-duplex circuit with a transmit and receive wire pair. We now have four parallel circuits running through one cable, so in each clock tick we can send four signals at a time through the cable. 100Base-T Ethernet uses a

4B5B coding scheme in which the set of 5 bits (4 data, one overhead) were transmitted at 125 MHz (i.e., 125 million times per second), giving a speed of 100 Mbps. 125 MHz is the fastest data rate at which the wires in cat 5 can reliably transmit for any reasonable distance. However, 125 MHz times 4 bits per signal equals only 500 Mbps. In order to get 1000 Mbps, we have to do something more creative.

Until now, we talked about transmitting one bit in each time interval by using a higher voltage and a lower voltage (e.g., see Manchester encoding). Gigabit Ethernet uses the same 125 MHz clock speed as 100Base-T Ethernet, but sends 2 bits in each time interval using *Pulse Amplitude Modulation–5* (PAM-5). With PAM-5, five different voltage levels are defined, ranging from +1 volts to -1 volts. Four of these voltage levels are used to send data. One voltage is defined to be the 2-bit pattern 00, another is defined to be 01, another 10, and another 11. The fifth voltage level is used for the fifth control bit. So, in each time period, the sender sends one electrical pulse at one of the five defined voltages, which represents a certain pattern of 2 bits, rather than just 1 bit as with Manchester encoding. Two bits per time interval times 125 time intervals per second times four separate circuit pairs in each cat 5 cable equals 1000 Mbps.

Because we are now sending 2 bits per signal using five different voltage levels rather than just two voltage levels as with Manchester encoding or 4B5B, the signal is more susceptible to noise or interference. This is because it is more difficult for the NIC to distinguish among differences in five voltage levels rather than two voltage levels because the differences between levels are smaller. It takes a much smaller amount of noise to trick the NIC into thinking a signal sent at one voltage level is actually a different level. For this reason, most organizations use cat 5e cable for 100Base-T; cat 5e is a version of cat 5 cable specially modified to reduce errors when

used in 1000Base-T installations. Cat 6 cable has also been proposed, which has a capacity of 250 MHz. The maximum length of cat 5/5e/6 cable for 1000Base-T is 100 meters from the computer to the hub or switch.

A.5 UNIVERSAL SERIAL BUS

Universal Serial Bus (USB) is another commonly used data transfer standard. Older USB devices will support serial data transfer at either 1.5 Mbps or 12 Mbps. Devices that conform to the USB 2.0 standard will support both these older speeds, plus 480 Mbps, which is sometimes called *Hi-Speed USB*.

USB cables have a host end and a device end, each of which have different styles of connectors ([Figure A.6](#)). Inside the cable, there are four wires. One is a ground wire and one (VBUS) is used to send a +5 volt power signal to the USB device. The two D wires are used to transmit the data in two separate serial data streams using a nonreturn to zero technique. The D+ wire sends the data with a positive charge while the D- wire sends the identical data with an offsetting negative charge to reduce interference and error.

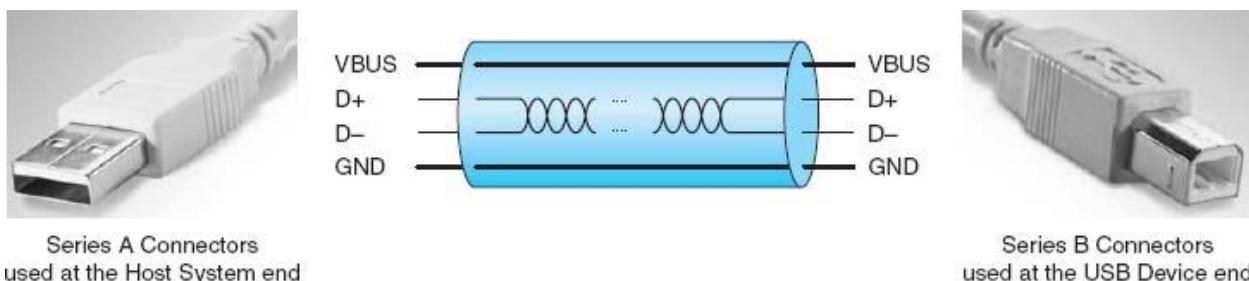


FIGURE A.6 USB cables

A.6 FIREWIRE

Firewire, a competitor to USB, was originally developed by Apple computer in the early 1990s and was standardized as IEEE 1394a-2000. Like USB, it is a serial bus connector. Firewire is also called i.Link.

Modern 1394a-2000 Firewire devices will support serial data transfer at 400 Mbps. Firewire cables have either a 4-pin or 6-pin configuration with a variety of different types of connectors. Inside the cable there are six wires ([Figure A.7](#)). Two are used to send 8–40 volts of power to the Firewire

device. The other wires are two pairs of two wires used to transmit the data in two separate serial data streams using a nonreturn to zero technique. Within each pair, the D+ wire sends the data with a positive charge while the D- wire sends the identical data with an offsetting negative charge to reduce interference and error.

Because there are two pairs of wires, Firewire could be configured to transmit in parallel, but it is not. Instead, one pair of wires is used to send data and the other pair is used to continuously send clocking signals to minimize the chance of error.

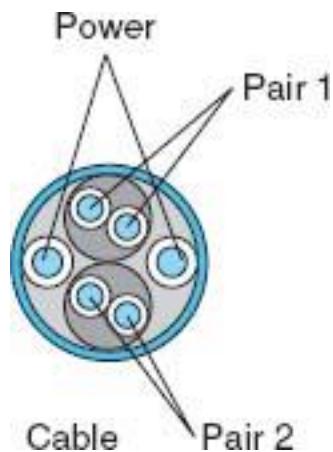


FIGURE A.7 Firewire cables

¹To be very precise, it is not an RJ-45 connector, but rather a version of the RJ-45 designed for network use. The RJ-45 is designed for telephone use, which tolerates higher interference. Just about everyone calls it an RJ-45 connector, but if you ever buy a “real” RJ-45 connector designed for telephone use and try to build a LAN cable yourself to save a few dollars, it won’t work.

APPENDIX B

SPANNING TREE PROTOCOL

Redundancy is an important element of good network design (see [Chapter 12](#)). Redundant circuits and devices mean that the network can continue to operate even if one circuit or device fails. For example, if a device has a 99.99 percent reliability, there is a 0.01 percent chance of failing. This means on average that the device will fail for about one hour per year. With two devices, the reliability increases to 99.9999 percent, or less than one minute of expected downtime per year.

Figure B.1 shows a common redundant network design. Two LAN segments (LAN 1 and LAN 2) are connected to two separate switches (A and B), that are in turn connected to two separate routers (X and Y) connected to the corporate WAN. Each switch has 4 ports; port 1 on switch A connects to LAN 1, port 2 connects to LAN 2, port 3 connects to router X, and port 4 connects to router Y. In this way, both LAN 1 and LAN 2 can continue to operate and send messages to and from each other and the WAN if any one circuit or device fails. For example, if switch A fails, all traffic into LAN 1 can still flow through switch B. Likewise, if router X fails, if the circuit from switch A to router X fails, or if port 3 on switch A fails, then traffic can flow through switch A to router Y and then into the WAN.

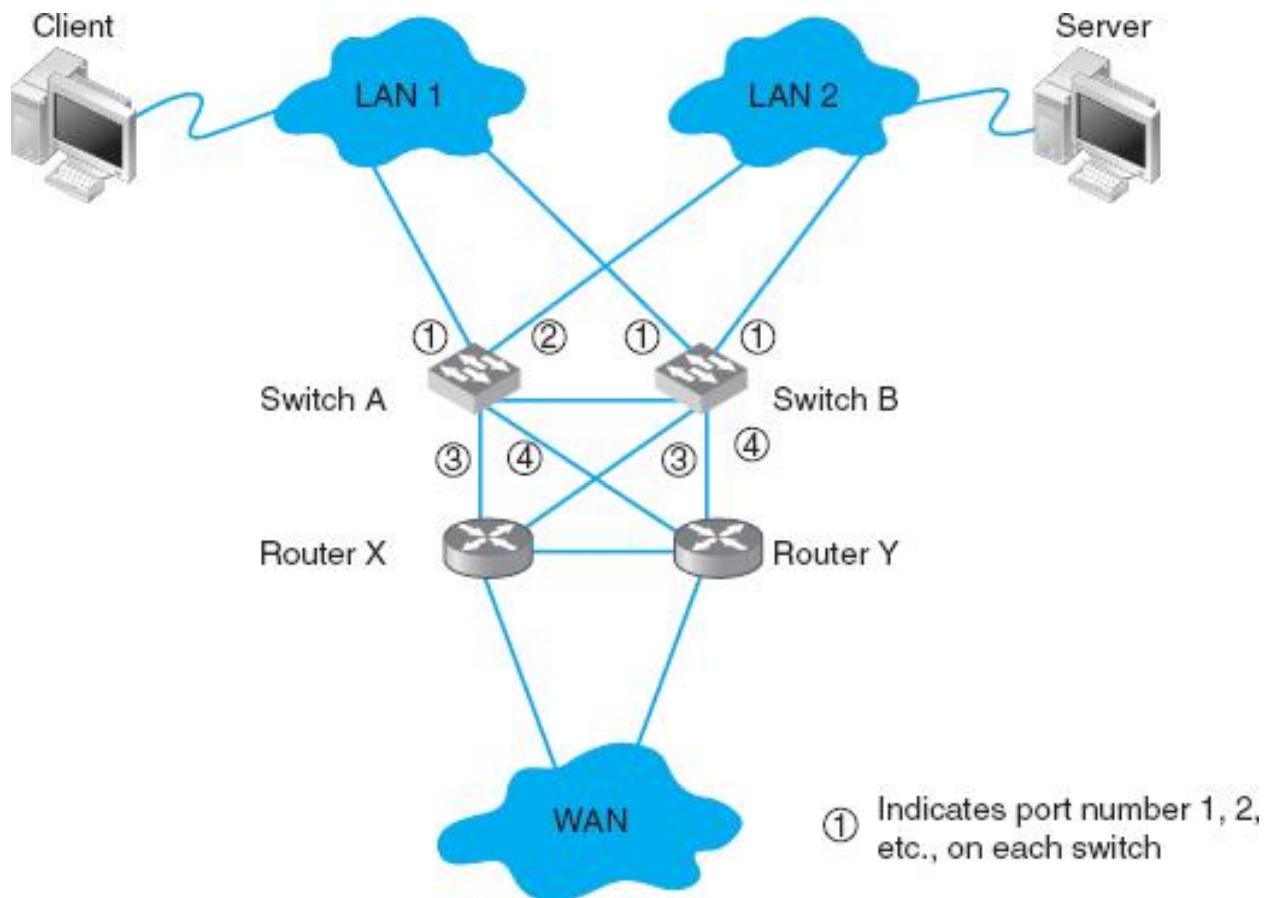


FIGURE B.1 Network design with redundant circuits and devices. LAN = local area network; WAN = wide area network

The challenge with redundant designs is to prevent broadcast storms. Remember that when switches are first turned on, they act like bridges, sending all messages in all directions, until they learn which device can be

reached through which port (see [Chapter 6](#)). This means, for example, when the network in [Figure B.1](#) is first turned on, neither switch A nor switch B will know where any device is. Assume that the client computer wants to send a message to the server. The message will enter LAN 1 from the client computer and be sent to switch A via the circuit connected to switch A's port 1. Switch A will learn that the client is on port 1. It won't know where the server is, so it will forward the packet on all remaining ports (2, 3, and 4). Router X on port 3 and router Y on port 4 will read the Ethernet address and ignore the message because it is not addressed to them. Eventually, the message will reach the server on LAN 2 via the message sent on port 2. The server will receive the message and send a response message to the client. The response message will hit switch A on port 2 (switch A will learn that the server is on port 2) and it will forward the response message to the client via port 1.

So far, so good. Now the problems start. Switch B is also on LAN 1, so it too will receive the very first message sent by the client, and will do exactly the same thing as switch A: it will learn that the client is on its port 1, and forward the message on its ports 2, 3, and 4. Once again, routers X and Y will ignore the message because it is not addressed to them (although the duplicate message has used up some of their processing capacity needlessly). When the message is sent to LAN 2 via port 2, the server sees it and starts to process it; we now have a duplicate message being processed twice.

But it gets worse. Switch A is also on LAN 2, so it receives all messages sent on LAN 2. When switch B sends the message from the client to the server into LAN 2, switch A also receives it, this time on its port 2. It now learns that the client is on port 2 (not port 1 as it originally thought; it assumes the computer has moved and updates its forwarding table), and promptly forwards the message a second time to the server on all remaining ports (1, 3, and 4). Routers X and Y see the message a third time and ignore it, but because switch B is also on LAN 1, it picks up the message again, thinks it is a new message, and again transmits the message on all other ports, which, of course, means that switch A gets the message again and forwards it again, and therefore switch B gets it again and forwards it, and so on, in a never-ending cycle. The same thing

happens with the response message from the server to the client, and in fact, with all messages. They circulate forever through the circular loops in the redundant network, until the network collapses under the storm.¹

The solution is to have switches configured with these redundant *physical* loops, but to create a way for the switches to recognize these physical loops and block them so that we create a different *logical* topology that does not have a loop. The method used to create this logical topology is called the *spanning tree protocol* and has been standardized as IEEE 802.1D.

With the spanning tree protocol, one switch is designated the *root node* or *root switch*. The cost to reach every computer, switch, or other device on the network from the root switch is calculated based on the “cost” of the intervening circuits (a 10 GbE circuit costs 2, 1 GbE costs 4, 100Base-T costs 19, and 10Base-T costs 100). The switches calculate the cost from the root switch to every device by sending information on the circuits they have to the switches around them using a special control message called a *Bridge Protocol Data Unit (BPDU)*.² Switches send BPDUs every 2 seconds so that the network can quickly learn the logical topology and adjust to changes (e.g., if a circuit fails).

Once the switches determine the cost to reach other devices, they select one port as the *designated port* for each device and block all the other ports so that all messages to any one device use only the designated port. For example, in [Figure B.1](#), switch A can reach the client via port 1 through one circuit. If all the circuits in the figure are 100Base-T, then the cost from switch A to the client via port 1 is 19. Switch A can also reach the client via port 2 through three circuits at a cost of 57 (to LAN 2, to switch B, to LAN 1). Ports 3 and 4 do not reach the client. Port 1 has the lowest cost, so it becomes the designated port for the client, and ports 2, 3, and 4 are marked as blocked for all traffic to the client (a blocked port is also called a *discarding port*). Likewise, switch A's port 2 is the designated port for traffic to the server (and ports 1, 3, and 4 are blocked for traffic to the server).

A switch only listens, learns, and forwards packets it receives on a designated port. In some cases, the network will change or a circuit may go down, meaning that the switch needs to be able to move from blocking a

port to marking it as the designated port. If a circuit or device goes down, a switch can recognize it from the changes in the BPDUs it receives from the other switches in the network (or from the failure to receive BPDUs on that port). When a switch realizes that a designated port no longer reaches the target destination (or the cost has suddenly increased), then it recalculates the costs and designates a new port.

One challenge is to determine how fast a switch should alter its designated port. If the time is set too short, then loops may develop and the network becomes unstable. If time is too long, then the network takes too long to respond to problems and users experience delays. In the original version of the spanning tree standard (IEEE 802.1D), switches were set to take 50 seconds to change designated ports. Because networks are more reliable today and they are less likely to lose BPDUs unless a circuit goes down, the newer version of spanning tree standard (IEEE 802.1 w) waits only 15 seconds.

When a switch first starts up, it does not know the cost to any devices, to what devices it is connected, which ports should be designated and blocked, or which switch is the root switch. It must learn all of these. The switch starts by presuming that it is the root switch and sending out BPDUs on all ports. These BPDUs identify the switch and start by assuming a cost of 32,768 to reach other devices (i.e., that the distance is very far). If there are no other switches, then it remains the root switch (although because there are no other switches, there is no redundancy and spanning tree is not needed).

If there are other switches in the network, then the switch starts receiving BPDUs from the switches around it and starts updating its cost table. Gradually the artificially high costs are replaced by actual ones and the switch is able to build an accurate forwarding table and determine whether or not it is the root node.

¹You may recall that an IP packet has a maximum hop count (also called time to live) to prevent this endless looping (see [Chapter 5](#)). Switches operate at the data link layer and therefore do not read the IP packet; the maximum hop count won't prevent looping at this layer.

²The spanning tree protocol was originally developed to be used by bridges and other layer-2 devices. Today, bridges are almost obsolete, so you are more likely to see spanning tree in a switched environment, but the terminology still reflects the origin with bridges.

APPENDIX C

IP TELEPHONY

IP Telephony refers to the use of Internet protocols to provide voice, video, and data in one integrated service over LANs, BNs, MANs, and WANs.

When most people talk about IP Telephony, they mean *Voice over IP (VoIP)*. *Voice over ATM (VoATM)* and *Voice over Frame Relay (VoFR)* are less common, and, as the names suggests, are close cousins to VoIP. VoIP provides three key benefits compared to traditional voice telephone services. First, it minimizes the need for extra wiring in new buildings (there is one cable for both voice and data, not two). Second, it provides easy movement of telephones and the ability of phone numbers to move with the individual (the number is installed in the telephone, much like an IP address, so anywhere the phone is connected or the phone number programmed, the phone will connect, even if it is halfway around the world). Finally, VoIP is generally cheaper to operate because it requires less network capacity to transmit the same voice telephone call over an increasingly digital telephone network.

VoIP requires a VoIP *Private Branch Exchange (PBX)*, which connects the organization's internal telephone network into the *public switched telephone network (PSTN)*. The PBX can also be connected into the organization's WAN and be configured to route calls through the WAN to other organization locations (or even over the Internet), thereby bypassing any long-distance charges in the PSTN (although the call does use up network capacity on the organization's WAN or Internet connection).

The VoIP PBX can be considered a gateway that connects the internal IP telephones to the PSTN.¹ When the IP telephone user lifts the receiver off the hook to place a call, the IP telephone sends a message to the PBX, which responds by sending a dial tone. Once the number has been dialed, the IP telephone then sends a message to the PBX with the telephone number, and the PBX connects the telephone into the PSTN or over the organization's WAN to the VoIP PBX at the other location.

VoIP often uses H.323 at the application layer (see [Chapter 2](#)), although *Session Initiation Protocol (SIP)* is also common. *Media Gateway Control*

Protocol (MGCP) and *Skinny Call Control Protocol (SCCP)* are other competing application layer protocols although they offer fewer features than H.323 and SIP. All four protocols (H.323, SIP, MGCP, and SCCP) operate at the application layer and contain all the functions needed to start and end telephone calls, as well as to transmit the call data. MGCP and SCCP require the PBX to act as a server and communicate with other MGCP and SCCP devices only through the PBX server; H.323 and SIP can both communicate with other H.323 and SIP clients without needing to go through the PBX (except for telephone number resolution, which is a process much like using a DNS to resolve an application layer name into an IP address [see [Chapter 5](#)]). SIP is a newer and more efficient protocol than H.323, and was developed using HTTP as its core, which means that it is simpler to debug and can be easily integrated into Web-based applications and SMTP e-mail applications.

In order to use VoIP, a device such as an IP telephone must support H.323, SIP, MGCP, or SCCP, and also contain a *CODEC* to convert the incoming analog voice signal into a digital bit stream (see [Chapter 3](#)). The CODEC is also used at the receiving end to convert the digital data back into the analog voice data. The most commonly used digital voice protocols are 64 Kbps PCM, 32 Kbps ADPCM (see [Chapter 3](#)), and more recent variants on them, such as 8 Kbps G.729 (also called CELP) or 6.3 Kbps G.723 (also called MPMLQ). As might be expected from their lower bandwidth requirements, sound quality can become an issue.

A technique called *Mean Opinion Score (MOS)* has been developed by ITU-T to subjectively rate the voice quality of different CODEC standards. A MOS of 5 is the theoretical maximum (meaning excellent) while a 1 is the lowest score (very poor quality). A 4 is generally regarded as an acceptable level of quality, with barely perceptible levels of quantizing error. PCM has a MOS of 4.1; ADPCM, 3.85; G.729, 3.92; and G.723 (at 6.3 Kbps), 3.9.

Once the CODEC has produced the digital data, the data is surrounded by an application layer packet. H.323 often uses *RTP* (see [Chapter 5](#)) for transmission through an IP-based network. The RTP packet in turn is surrounded by UDP, IP, and data link layer packets (e.g., Ethernet, frame relay) for transmission through the network. Voice data packets tend to be

very small, and thus the packets added at layers 5, 4, 3, and 2 can add considerable overhead to the transmission. A new version of RTP called *Compressed Real Time Protocol* (CRTP) has been developed that enables the set of RTP, UDP, and IP packets to be compressed to 2 bytes, thus significantly reducing the overhead.

Voice Activity Detection (VAD) is another way of reducing the network capacity required to send VoIP calls. With VAD, the end VoIP device monitors the analog voice signal and if the signal drops below a certain amplitude, then the device assumes that no one is speaking and stops sending packets. Since most conversations are silent at least half the time, this can significantly reduce the bandwidth required. VAD must be done carefully to avoid clipping the speech (cutting off the beginning and end). The other problem with VAD is that because no data packets are transmitted, the line is completely silent. We are so used to experiencing background noise from interference on traditional analog telephone calls that silence is usually interpreted as meaning the call has been disconnected. Therefore, several vendors have begun to add in background *comfort noise* (sometimes called pink noise) when no data packets are flowing. The VAD device at the sender's location initially sends some ambient background noise packets, which are recognized by the receiving device. After a few seconds, the VAD sending device begins operating normally and no longer sends background noise packets when speech ends. When the receiver detects the slowdown in packets, it repeatedly reproduces the ambient background noise packets to fill the "dead air" so that the receiver does not think the call has been disconnected.

As a result of VAD, the network capacity requirements for VoIP on Ethernet networks ranges from about 8 Kbps using G.729 and CRTP to 45 Kbps using PCM with RTP. On ATM networks, it ranges from about 6 Kbps using G.723 and CRTP to 53 Kbps using PCM.

One of the key issues in VoIP is ensuring that the network has sufficient capacity to send the VoIP packets. While users will accept a few second delays in Web traffic or e-mail, most people cannot tolerate delays in voice conversations over about 250 milliseconds (a quarter of a second).

Therefore, VoIP is only practical in networks that enable *Quality of Service* (QoS) routing at the IP layer (see [Chapter 5](#)) and ideally matching QoS at the data link layer. Most organizations that deploy VoIP, therefore, use IP with QoS and also have policy-based VLANs at the data link layer (see [Chapter 8](#)).

¹Another type of VoIP PBX uses regular telephones and regular analog circuits inside the organization, and the PBX does all the conversion between the analog telephone and the digital network. This is an older, temporary approach that is quickly disappearing.

APPENDIX D

CELLULAR TECHNOLOGIES

Cellular technology is becoming increasingly popular. Its most common use is to provide *cellular telephoneservices*, but the cellular network is also being used more and more often by data communication devices such as pagers, personal digital assistants (PDAs), and handheld computers.

Cellular technology is a form of high frequency radio in which antennas are spaced strategically throughout a service area. The service area is divided into many cells, each with its own antenna. This arrangement generally provides subscribers with reliable mobile telephone service of a quality almost that of a hardwired telephone system. Users (voice or data transmission) dial or login to the system, and their voices or data are transmitted directly from their telephone to one of these antennas. In this way, the cellular system replaces the hardwired local loop. Each phone service provider uses a different part of the radio frequency spectrum, which is why cell phones designed for one provider's network often won't work on another provider's network.

This network of cell antennas is an intelligent system. For example, as you drive your car through the service area, you move away from one antenna and closer to another. As the signal weakens at the first antenna, the system automatically begins picking up your signal at the second antenna. Transmission is switched automatically to the closest antenna without communication being lost.

The older technology used for cell phones is digital (not analog; see [Chapter 3](#)), and is sometimes called *2G wireless* because it is the second-generation mobile phone service (old analog cell phones were the first generation). A 2G phone has a built-in CODEC that converts the analog voice data into digital signals for transmission. These phones enable limited data transfer, often only 19.2 Kbps, because the cell phone network was designed primarily for phone calls, not data transmission.

There are three incompatible standards for cell phone technology that are commonly used around the world. *Code Division Multiple Access (CDMA)* is a spread spectrum technology that works by digitizing multiple conversations, attaching a code known only to the sender and receiver and then dicing the signals into bits for transmission and reassembling them at the receiving device. *Time Division Multiple Access (TDMA)* allows multiple users to share the same voice channel by having each conversation transmitted alternately over short lengths of time (statistically time division multiplexing). *Global System for Mobile Communication (GSM)* is a TDMA-like digital system that transmits digital voice data in bursts during brief time slots allocated to multiple subscribers sharing a radio channel. GSM is the standard in most of the world, except for the United States and Canada, which still use a mix of CDMA, TDMA, and GSM.

The current technology for mobile wireless is *3G wireless*, so called because it is the third generation of public wireless networks. 3G wireless is still under development with no clear winners at this point. Several industry groups are racing to provide high-speed digital telephone and wireless Internet services. Most “high-speed” cell technologies currently deployed are called 2.5G because they serve as a stepping stone to 3G. The adoption of 3G was relatively slow because mobile operators had to build new networks as 3G uses different frequencies than its predecessor 2G. The data transfer offered by 3G can be up to 2-3 Mbps, although this can drop down to approximately 300 Kbps when in motion.

Two sets of technologies are leading in the 3G race. The first is *Enhanced Data GSM Environment (EDGE)*, a 2.5G step along the path to *Wideband Code Division Multiple Access (WCDMA)* as the 3G standard. As the name suggests, EDGE is an enhancement of the current GSM and provides a

data rate of 384 Kbps (it is sometimes called GSM384). WCDMA provides 2.3 Mbps. For more information, see www.umts-forum.org.

The second technology group sponsors *CDMA2000* (2.5G) and *CDMA2000 1X* (3G). As the names suggest, CDMA2000 and CDMA2000 1x are extensions to CDMA that provide 153 Kbps and 2.4 Mbps, respectively. For more information, see www.cdg.org.

Meanwhile, other vendors are beginning to talk about *4G wireless* services—that is, the next generation after 3G—because 2–3 Mbps data rates are not as powerful as current wireless LAN technologies such as 802.11 (see [Chapter 7](#)). Some vendors have begun to call for universal public 802.11 access as a 4G option, with 802.11 hot spots being deployed in major urban areas. In other words, your cell phone would have both the 2.5G or 3G antenna, plus an 802.11 antenna to enable faster data transfer in areas covered by 802.11. While the standard version of 802.11 has a very short range, new emerging versions of 802.11 designed for outdoor use have ranges of 20 miles or more.

Stay tuned because this battle is just starting.

APPENDIX E

TCP/IP GAME

E.1 INTRODUCTION

The purpose of this game is to help you better understand how messages are transmitted in TCP/IP-based computer networks. Players are organized into five-person teams that represent different computers in the network. Each person in the team assumes the role of one layer of software or hardware on that computer (e.g., data link layer) and works with the others to send messages through the network.

E.1.1 GENERAL RULES

1. This is a team game. The class will be broken into a set of five-member teams, with each team being one computer in the communications network. Each person in the team will role-play one

layer in the computer, either the application layer, the transport layer, the network layer, the data link layer, or the physical layer.

2. Messages will be created by the application layer and passed to the transport layer. The transport layer will break the message into several smaller messages if necessary and pass them to the network layer. The network layer will address and route the message and pass the message to the data link layer. The data link layer will format the message and perform error control (which will involve sending ACKs and NAKs) and pass the message to the physical layer for transmission. The physical layer will transmit the message to the physical layer of the destination computer. Messages are sent using the forms in Figure E.1. Be sure to make lots of copies of the forms before the game starts.
3. Each layer will have a set of instructions to follow to ensure the messages are sent and received properly. Follow them carefully. These instructions explain what you are to write on the message forms. Never write anything on the message form in an area used by another layer.
4. At some point, someone will make a mistake. If you receive a message that contains an error, hand it back to the person who gave it to you and explain the error to that person.
5. And remember, the game is meant to be fun, too!

SMTP	From	To	Message	
				⋮

TCP	Sequence Number of	User Data

IP	Final Destination	Next Node	User Data

Ethernet	Source	Destination	Control	Message #	Error	User Data

FIGURE E.1 Forms for the TCP/IP game

E.2 APPLICATION LAYER

E.2.1 ACTIVITIES

1. Send messages to other computers
2. Respond to messages from other computers

E.2.2 TOOLS NEEDED

- Several blank SMTP forms
- List of messages
- Network map ([Figure E.2](#) shows an example; the instructor will draw one for your class)
- A blank piece of paper

E.2.3 SENDING OUTGOING MESSAGES

To send a message, you must:

1. Find a blank SMTP packet.
2. Write the *IP address* of your computer in the **From** box.
3. Use the network map to select a computer as the destination for this message. Write the *IP address* of the destination computer in the **To** box. Don't send all your messages to one computer; we want to even out the messages. Try to send a few messages to computers close to you and a few to computers far away.
4. Write the message you wish to send in the **Message** box. To make the message simple to understand, please use a hyphen (-) to indicate spaces between words. Select a message from the list of messages (see below). Try to have at least one hyphen in the message (this is to help the data link layer do error control) or add one at the end or at the

start if you must.

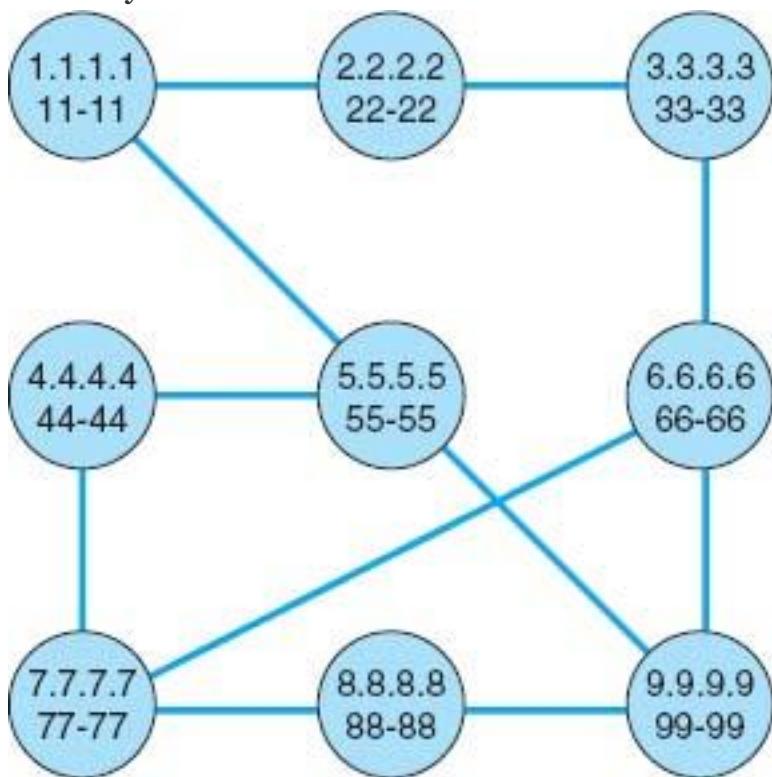


FIGURE E.2 Sample network map

5. Write the message and the name of the computer to which you send the message on the blank piece of paper. This will help you understand the responses you get to your messages.
6. Pass the message to the transport layer.

E.2.4 RESPONDING TO INCOMING MESSAGES

Eventually, you will receive an incoming message from the transport layer that was sent to you by some other computer asking you a question. To respond to the message, you will send a message that answers the question. Follow the same steps above to send a message, but in step 4, write your answer in the **Message** box. For example, if the message you received asked what your favorite color was, you might write *red* or *blue* in the **Message** box.

E.2.5 LIST OF MESSAGES

Here are a list of messages you can send. Remember to use a hyphen instead of a space to separate the words. Rather than writing the entire message, you can omit the words *What is your*.

- What is your favorite color?
- What is your birthday?
- What is your phone number?
- What are your favorite holidays?
- What is your favorite car?

E.3 TRANSPORT LAYER

E.3.1 ACTIVITIES

1. Accept outgoing SMTP messages from the application layer, packetize them, and pass them to the network layer.
2. Accept incoming messages from the network layer and, if they are made up of several packets, assemble the entire SMTP message before passing it to the application layer.

E.3.2 TOOLS NEEDED

- TCP forms
- Tape

E.3.3 ACCEPTING OUTGOING MESSAGES FROM THE APPLICATION LAYER

Every few minutes, the application layer will hand you an outgoing message to transmit. To transmit them, you must:

1. Break the SMTP message into smaller packets. Tear the SMTP packet into two parts at the dotted line. If there is writing on both parts, then you must send each part as a separate message. If the second half of the SMTP packet has no writing on it, throw it away and ignore it.
2. Find one or two blank TCP packets.
3. Fill in the **Sequence Number** box. If there is only one part of the SMTP packet, write “1 of 1” in the **Sequence Number** box. If there are two parts of the SMTP packet, write “1 of 2” on the first TCP packet and “2 of 2” on the second TCP packet.
4. Tape the SMTP packet(s) to the TCP packet(s) over the **User Data** space. (The packet(s) will be too big to fit, but don't worry about it.)
5. Pass the TCP + SMTP packet(s) to the network layer.

E.3.4 ACCEPTING INCOMING MESSAGES FROM THE NETWORK LAYER

Every few minutes, the network layer will hand you an incoming message. To process it, you must:

- **If the message is complete (that is, if the Sequence Number box says “1 of 1”):**
 1. Take the TCP packet off of the SMTP packet and throw away the TCP packet.
 2. Pass the SMTP packet to the application layer.
- **If the message is not complete (that is, if the Sequence Number box says “1 of 2”):**
 1. Wait for the second part of the message to arrive.
 2. Take the TCP packets off of both SMTP packets and throw away the TCP packets.
 3. Tape the two parts of the SMTP packet back together.
 4. Pass the SMTP packet to the application layer.

E.4 NETWORK LAYER

E.4.1 ACTIVITIES

1. Accept messages from the transport layer, route them, and pass them to the data link layer.
2. Accept messages from the data link layer and, if they are addressed to you, pass them to the transport layer; if they are not addressed to you, route them and pass them back to the data link layer.

E.4.2 TOOLS NEEDED

- IP forms
- Tape
- Network map

E.4.3 ACCEPTING OUTGOING MESSAGES FROM THE TRANSPORT LAYER

Every few minutes, the transport layer will hand you an outgoing message to transmit. To transmit them, you must:

1. Find a blank IP packet.
2. Address the message by copying the IP address from the **To** box of the SMTP packet into the **Final Destination** box of the IP packet.
3. Route the message by finding the next computer in the network map to which the message should be sent and writing its Ethernet address in the **Next Node** box. If your computer is directly connected to the final destination computer, the next node is the same as the final destination. If your computer is not directly connected to the destination, you must select the best route that the message should follow and specify one of the computers to which you are connected.

4. Tape the TCP + SMTP packet to the IP packet over the **User Data** space. (It will be too big to fit, but don't worry about it.)
5. Pass the IP + TCP + SMTP packet to the data link layer.

E.4.4 ACCEPTING INCOMING MESSAGES FROM THE DATA LINK LAYER

Every few minutes, the data link layer will hand you a message to process. You must:

- **If the message is addressed to you (that is, if the Final Destination box in the IP packet lists your IP address):**
 1. Remove the IP packet from the SMTP + TCP packet and throw the IP packet away.
 2. Pass the SMTP + TCP packet to the transport layer.
- **If the message is not addressed to you (that is, if the Final Destination box in the IP packet lists someone else's IP address):**
 1. Scratch out or erase the address in the **Next Node** box.
 2. Route the message by finding the next computer in the network map to which the message should be sent and writing its data link layer address in the **Next Node** box. If your computer is directly connected to the destination computer, the next node is the same as the final destination. If your computer is not directly connected to the destination, you must select the best route that the message should follow and specify one of the computers to which you are connected.
 3. Pass the message to the data link layer.

E.5 DATA LINK LAYER

E.5.1 ACTIVITIES

1. Accept outgoing messages from the network layer, format them, add error-control information, and pass them to the physical layer.
2. Accept incoming messages from the physical layer. If they are data messages and contain no errors, send an ACK and pass them to the network layer. If they are data messages with an error, send an NAK. If they are an ACK, destroy the message they acknowledge. If they are an NAK, retransmit the original message.

E.5.2 TOOLS NEEDED

- Ethernet forms
- Tape
- Network map
- Some blank pieces of paper. You will discover that you are receiving and storing many different types of messages. To help you organize those messages, we suggest that before you begin, you use three blank pieces of paper to create three message storage piles:
 - Label one pile **Messages from the Network Layer**.
 - Label the second pile **Messages from the Physical Layer**.
 - Label the third pile **Messages Transmitted**.

E.5.3 ACCEPTING OUTGOING MESSAGES FROM THE NETWORK LAYER

Every few minutes, the network layer will hand you a message to transmit. If you receive more messages from the network layer than you can process right away, put them in the **Messages from the Network Layer** pile until you can process them. For each message, you must:

1. Find a blank Ethernet packet.
2. Format the message for the physical layer by writing your Ethernet address in the **Source** box. Copy the Ethernet address from the **Next Node** box in the IP packet into the **Destination** box. Write an asterisk (*) in the **Control** box.
3. Number the message. Write a two-digit number in the **Message Number** box. This should be *01* for the first message you send, *02* for the second, and so on. Use the blank piece of paper to help you remember what numbers you have used.
4. Add error-control information. Most error control is very sophisticated, but in this game, we'll use something very simple. Count the number of hyphens in the user data (the SMTP packet, the TCP packet, and the IP packet [but not the Ethernet packet]) and write this number in the **Error** box on the Ethernet packet.
5. Tape the SMTP + TCP + IP packet to the Ethernet packet over the **User Data** space. (It will be too big to fit, but don't worry about it.)
6. Pass the message to the physical layer. In a few moments, the physical layer will return the packet to you. *Save it in the Messages Transmitted pile!*

E.5.4 ACCEPTING INCOMING MESSAGES FROM THE PHYSICAL LAYER

Every few minutes, the physical layer will hand you a message to process. If you receive more messages than you can process right away, put them in the **Messages from the Physical Layer** pile. These messages will either be data messages, ACKs, or NAKs. Each is processed differently.

- **If the Control box contains an asterisk (*), this is a data message. Do the following:**
 1. Perform error checking. Count the number of hyphens in the user data (the SMTP packet, the TCP packet, and the IP packet [but not the Ethernet packet]). If this number is the same as the

number in the **Error** box, no errors have occurred. If they are different, an error has occurred.

2. If no errors have occurred, you must send an ACK to the sender and send the incoming message to the next layer:
 1. Find a blank Ethernet packet.
 2. Write your Ethernet address in the **Source** box. Write the Ethernet address contained in the **Source** box of the incoming message in the **Destination** box of your message. (This ACK message is going to the sender of the original message.) Write *ACK* in the **Control** box. Write the two-digit number contained in the **Message Number** box of the incoming message in the **Message Number** box.
 3. Pass the outgoing ACK message to the physical layer.
 4. Remove the Ethernet packet from the incoming message and throw the Ethernet packet away.
 5. Pass the incoming SMTP + TCP + IP packet to the network layer.
3. If an error has occurred, you must send an NAK to the sender and discard the incoming message:
 1. Find a blank Ethernet packet.
 2. Write your Ethernet address in the **Source** box. Write the Ethernet address contained in the **Source** box of the incoming message in the **Destination** box of your message. (This NAK message is going to the sender of the original message.) Write *NAK* in the **Control** box. Write the two-digit number contained in the **Message Number** box of the incoming message in the **Message Number** box.
 3. Pass the outgoing NAK message to the physical layer.
 4. Throw away the incoming message containing the error.
4. **If the Control box contains an ACK, this is an ACK message. Do the following:**

1. Find the original message you sent, in the **Messages Transmitted** pile, that has the same message number as the ACK.
 2. Destroy the original message and the ACK.
- **If the Control box contains an NAK, this is an NAK message. Do the following:**
 1. Find the original message you sent, in the **Messages Transmitted** pile, that has the same message number as the NAK.
 2. Give the original message to the physical layer to transmit again. In a few moments, the physical layer will return the packet to you. *Save it* in the **Messages Transmitted** pile.
 3. Destroy the NAK.

E.6 PHYSICAL LAYER

E.6.1 ACTIVITIES

1. Accept messages from the data link layer and pass them to the physical layer of the computer to which they are to go, possibly introducing a transmission error.
2. Accept messages from the physical layer of other computers and pass them to the data link layer.

E.6.2 TOOLS NEEDED

- Ethernet forms
- IP forms
- TCP forms
- SMTP forms

- Network map
- Transmission forms
- Two coins

E.6.3 ACCEPTING MESSAGES FROM THE DATA LINK LAYER

Every few minutes, the data link layer will hand you a message to transmit. These messages will either be data messages or control messages (ACKs or NAKs). Each is processed differently.

- **If the Control box contains an asterisk (*), this is a data message. Do the following:**
 1. Determine if there will be an error in transmission by tossing two coins; if they are both heads, you will introduce an error.
 2. Copy the entire contents of the message packet onto new forms; that is, copy the SMTP packet to a new SMTP packet, the TCP packet to a new TCP packet, the IP packet to a new IP packet, and the Ethernet packet to a new Ethernet packet. If you are to introduce an error, omit all the data in the **SMTP Message** box. Be sure to tape the packets together in the right order.
 3. Pass the copied SMTP + TCP + IP + Ethernet packet to the physical layer of the computer whose address is listed in the **Destination** box.
 4. Pass the original SMTP + TCP + IP + Ethernet packet back to the data link layer and make sure that that person understands that you are giving back the message that he/she just gave you to transmit.
- **If the Control box contains an ACK or an NAK, this is a control message. Do the following:**
 1. Simply pass the Ethernet packet to the physical layer of the computer whose address is listed in the **Destination** box. Things are complicated enough without ACKs and NAKs getting destroyed.

E.6.4 ACCEPTING MESSAGES FROM THE PHYSICAL LAYER OF ANOTHER COMPUTER

Every few minutes, the physical layer of another computer will hand you a message. Simply hand the message to the data link layer.

E.7 NOTE TO INSTRUCTORS

E.7.1 BACKGROUND

This game helps students *really* understand what the various layers actually do and how they must work together to send a message. Reading about it is one thing; having to perform a simple version of the function is something else altogether. Experiential learning can be an extremely powerful tool. I have noticed a distinct improvement in students' understanding of this material since I have begun using the game.

The game is an extremely simplified version of what happens in a real TCP/IP network. Nonetheless, it can be complicated. Students have to work together and sometimes make mistakes. Ideally, students will recognize mistakes themselves and will help one another learn.

Participation is key to the learning objectives. It's also key to making a somewhat dry conceptual set of issues more real—and more fun.

When I teach the course, I usually use this game after I complete **Chapter 5, The Network and Transport Layers**. At this point students will have learned everything they need to know to run the game, and it will reinforce the material.

E.8 PREPARING TO TEACH THE GAME

This game contains all the materials you will need to run the game, except a set of coins and paper (which you can rely on students to have), enough tape for each group (bring several rolls), and a network map (which you draw on the board just before the game starts). You will also have to make copies of the four types of packets. It takes an average of three SMTP, TCP, and IP forms and four Ethernet forms for each message, so you will need a lot of them. I usually plan on the class sending about 10–15

messages per team; for a 40-person class, this means you will need 250–350 SMTP, TCP, and IP forms and 350–500 Ethernet forms.

I have found from experience that it takes the students a little while to catch on to the game. Be sure to tell the students to read the game before they come to class.

E.9 TEACHING THE GAME

It usually takes 20 minutes before the game gets going. The first step is to organize the class into five-person teams. Each team represents one computer in the network. If there are more than five people in a team, have two people play the data link layer; if there are less than five, then combine the application, transport, and/or network layers.

Draw the network map on the board. The map will have a circle to represent each team (i.e., computer). Try to draw the circles to represent the actual physical placement of the teams within the classroom. Inside each circle, write:

- The IP address (e.g., 1.1.1.1). Arbitrarily choose a number for each team but keep it short and easy to remember.
- The Ethernet address (e.g., 11-11). Arbitrarily choose a number for each team but keep it short and easy to remember. It helps if it matches the IP address in some way. Be sure to have at least one hyphen in the address to help reinforce the error-control concepts.

Next, connect the computers (i.e., teams) by drawing lines (i.e., circuits) between the circles. Don't draw in all possible circuits, because you want some teams to have to route messages through other teams to reach their final destination. Likewise, don't put too few circuits, or else all messages will take a long time to send.

Do a simple example. Walk through the sending of one message on the board and have the students follow by replicating each step you do for one of their own messages. Once the message has reached the physical layer on the next computer, I turn the students loose and let them play. I usually

walk around the classroom answering questions and listening in on discussions as the game progresses.

Because each layer performs a unique function, it is useful to have each student play each layer if time permits. I try to have students rotate layers after 15 minutes. I keep the game going so that the students playing one layer need to explain to the person taking over their layer what is going on and how to play. The easiest way to rotate is downward; that is, the person playing the application layer moves to the transport layer, and so on.

E.9.1 DISCUSSION QUESTIONS

After each person has had the opportunity to play several layers, it is useful to ask what the students have learned. This gives you the opportunity to reinforce the concepts the game was designed to teach. Some possible discussion questions are:

1. Why are standards important?
2. How could you improve network performance by changing the topology?
3. What layer is the busiest? How could you improve network performance by changing the protocol at this layer?

APPENDIX F

WINDOWS SERVER

Windows server is one of the most popular operating systems for servers. The server operating system enables you to share resources such as files, applications, and printers with other computers. In this section, we will explain how to set up Windows Server to share files.

F.1 MANAGING USER ACCOUNTS

Every user who wants to use the server must have an account that specifies what they can and cannot access. There are two types of accounts. A *local account* is an account that is managed on just one

computer. A *domain account* is an account that is managed by *Active Directory* and can provide access rights to many different computers through a single login. For this activity, we will assume you are working with local accounts, although the processes for managing domain accounts is almost identical to the process for managing local accounts.

The administrator account is the account that controls the server. The administrator has the rights to add users, change their rights, and control who can do what on the server. In order to manage user accounts, you must login as the administrator. We will assume that you have already logged in as the administrator for the rest of this activity.

Each user account belongs to a *group*. For example, we might create groups by function with one group for sales, one group for accounting, one for production, and so on. We might also create groups by region so that we have one group for Los Angeles, one group for Toronto, one group for New York, and so on. Groups can be organized in a hierarchy so that we can start by defining groups by region, and then add the functional groups below the region so that we have Los Angeles staff, Los Angeles sales staff, Los Angeles accounting staff, and so on.

We can set individual access rights user by user. We can also set access rights by group so that all members of the same group receive the rights for the group. Groups make it simpler to manage user accounts because we do not need to enter information for every user, just every group.

F.1.1 CREATING USERS

To create a local user, click Start, Administrative Tools, Computer Management. This will show you the list of objects on the server, including folders, users, and groups. Figure F.1 shows the display after clicking on Local Users and Groups and then Users. This shows all currently defined users, which are those that were created automatically by Windows.¹

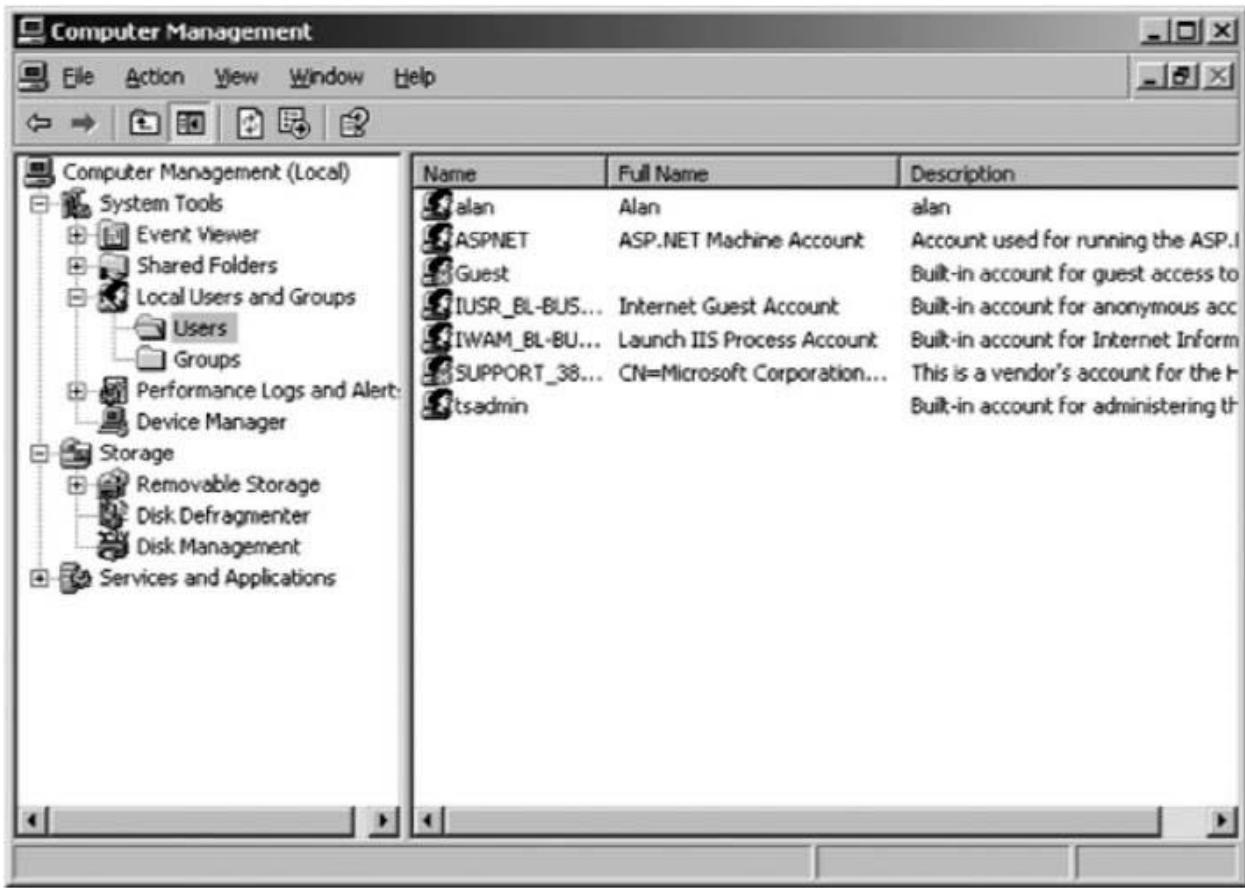


FIGURE F.1 List of users

To create a user, right click on the Users and then choose New User. You can then enter the information about the user such as the user name (i.e., userid) he or she will use to login as well as his or her full name and description (see [Figure F.2](#)). You also enter the password associated with the account, as well as the policies associated with the password. You can, for example, require the user to change the password when he or she next logs in, or prevent the user from changing the password. Click Create to add the user.

F.1.2 SETTING USER PROPERTIES

There are dozens of properties you can set for each user. After you have created the user, the user name will appear in the list shown in [Figure F.1](#). Right click on the user name and then click Properties. You can record additional information about the user, define what groups the user belongs

to (more on that in a moment), and even restrict what hours the account can be used (See [Figure F.3](#)).



FIGURE F.2 Creating a user

F.1.3 CREATING GROUPS

Before you create groups, you should have a plan. Prepare a list of groups you would like to create and determine the hierarchy of the groups you want to implement.

To create a group, click Start, Administrative Tools, Computer Management, and then click on Groups. This will show you the list of currently defined groups which are those automatically defined by Windows (see Figure F.4).

Right click on Groups and then choose New Group. You can then enter the information about the group, including its name. This is very similar to creating a new user.

F.1.4 ADDING USERS TO GROUPS

To add users to a group, click Start, Administrative Tools, Computer Management, and click on Users. This will show you the list of currently defined users as in Figure F.1.



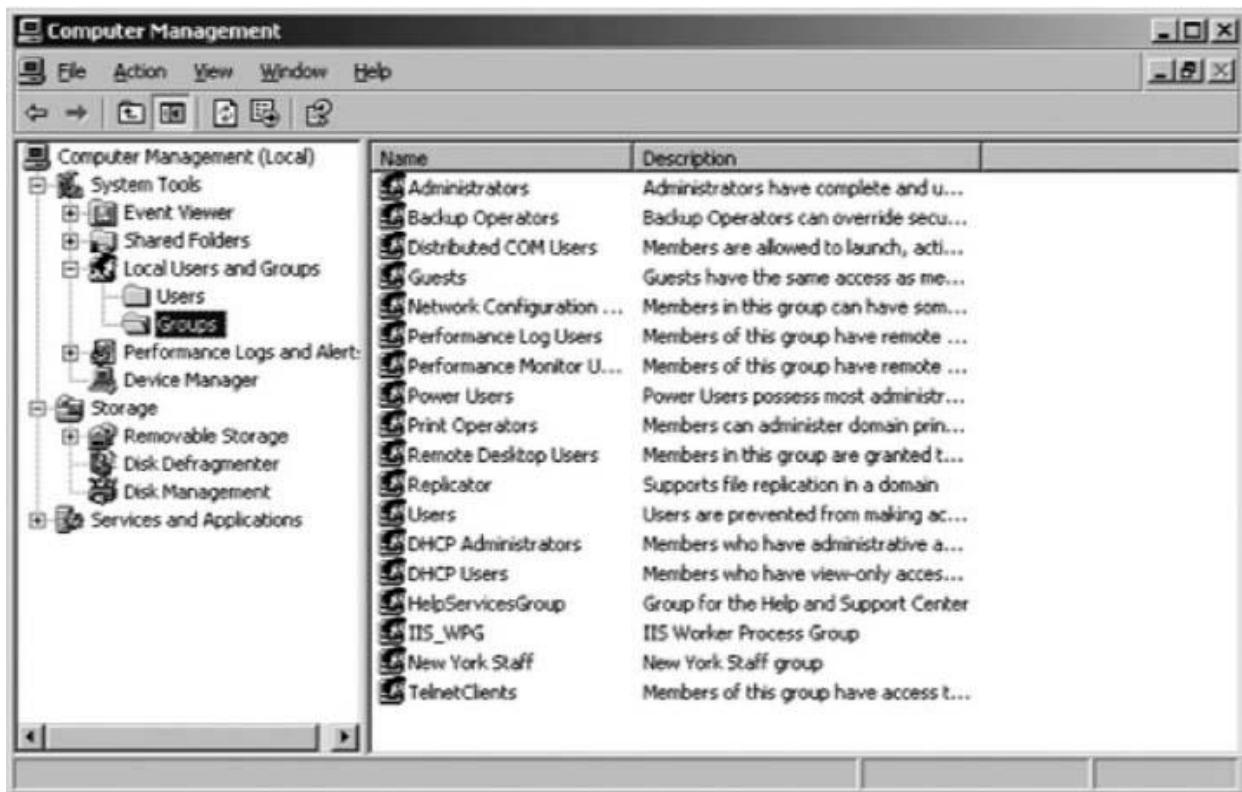
FIGURE F.3 Managing user properties

Right click on the user name you want to add into the group. Then select the Properties.

Click on the Member Of tab (See [Figure F.5](#)). Click Add and select the name of the group into which you want to add the user. Then click OK.

F.2 MANAGING FILE SHARING

Any resource on the server can be shared with one or more users. Each resource (e.g., file, printer) has an *access control list* (ACL) that defines which user(s) and/or which group(s) have access to the resource and what they can do with it—in other words, their *permissions*. For example, some users might have permission only to read files in a shared directory, others might have permission only to add new files to the directory, while others might have permission to change or delete existing files. [Figure F.6](#) lists the basic permissions you can set. There are also more advanced *special permissions* that can be set as well.



The screenshot shows the Windows Computer Management console window titled "Computer Management (Local)". The left pane displays a tree view of management tools, including System Tools, Storage, and Services and Applications. The "Local Users and Groups" node under System Tools is expanded, showing "Users" and "Groups". The right pane is a table listing various user groups with their descriptions:

Name	Description
Administrators	Administrators have complete and u...
Backup Operators	Backup Operators can override secur...
Distributed COM Users	Members are allowed to launch, acti...
Guests	Guests have the same access as me...
Network Configuration ...	Members in this group can have som...
Performance Log Users	Members of this group have remote ...
Performance Monitor U...	Members of this group have remote ...
Power Users	Power Users possess most administr...
Print Operators	Members can administer domain prin...
Remote Desktop Users	Members in this group are granted t...
Replicator	Supports file replication in a domain
Users	Users are prevented from making ac...
DHCP Administrators	Members who have administrative a...
DHCP Users	Members who have view-only acces...
HelpServicesGroup	Group for the Help and Support Center
IIS_WPG	IIS Worker Process Group
New York Staff	New York Staff group
TelnetClients	Members of this group have access t...

FIGURE F.4 User groups

Permissions can be assigned to folders or to files. If you assign a permission to a folder, all the files and subfolders it contains receive the same permissions unless you specifically change the permissions of the files and subfolders. Likewise, if you grant a permission to a group, all users in the group and all subgroups receive the same permissions.

F.2.1 CREATING A SHARED FOLDER

To create a shared folder, you must first create the folder exactly as you would in Windows on your desktop computer. Open Windows Explorer (click Start, Programs, Accessories, Windows Explorer). Click on the folder in which to place the shared folder and click File, New, Folder. Then type the name of the folder.

There are two steps in permitting users to access the shared folder. First, you must enable sharing for the folder and then define the security ACL. This is rather cumbersome, but this is how Windows requires you to do it.



FIGURE F.5 Adding users to groups

F.2.2 ENABLING SHARING

In Windows Explorer right click on the folder and Select Properties. Then click the Sharing tab (see [Figure F.7](#)). Click the radio button to Share this folder. Then type the name that the folder will be known as to users.

Next, click Permissions. This will show you the list of users who can access this folder (see [Figure F.8](#)). By default, Windows permits the group named Everyone to access all shared folders. The Everyone group is exactly what it sounds like—every user name on the server. Typically, network managers start by removing the Everyone group and adding in only those users or groups who should have access to the folder. Click the Remove button to remove the Everyone group.

Click Add to grant permission to access this folder to a user (see [Figure F.9](#)). In the window, type the name of the group or user with whom you want to share the folder and click Check Names. Then click OK.

Permission	When Applied to a File	When Applied to a Folder
List Folder Contents	This applies only to folders.	Permits the user to view the folder contents, but to do nothing else.
Read	Permits the user to read the file.	Permits the user to view the folder contents and to read every file in the folder.
Read and Execute	Permits the user to read a file and execute it, if it is a program.	Permits the user to view the folder contents and read or execute any file it contains.
Write	Permits the user to change the contents of a file or its attributes.	Permits the user to add new files and subfolders to the folder, but not to change any existing files in the folder.
Modify	Permits the user to change the contents of a file.	Permits the user to add new files and subfolders to the folder, and to change or delete any existing files and their attributes in the folder.
Full Control	Permits the user to do anything to the file.	Permits the user to do anything to the folder.

FIGURE F.6 File and folder permissions

Once the user name is found, you can then define the type of access to permit (see [Figure F.10](#)). In this figure, you can see that we've granted access to the group called New York Staff. The types of access are fewer than those shown in [Figure F.6](#), but there will be more options shortly. Then click OK.

At this point, the folder is now available to be shared to those users or groups to whom you have granted permission. However, they still cannot access the folder. You must define the security access list first.

F.2.3 DEFINING SECURITY

In Windows Explorer, right click on the folder and Select Properties and then click the Security tab (see [Figure F.11](#)). This will display all users and groups who have security access to the folder. You will see that New York Staff does not appear in this list. Even though they were granted sharing permission, this does not grant security permission. Click Add and enter the New York Staff group as a permitted group.

You can then grant the types of permissions this group has (see [Figure F.12](#)). This is the same list of options as described in [Figure F.6](#).



FIGURE F.7 Enabling sharing

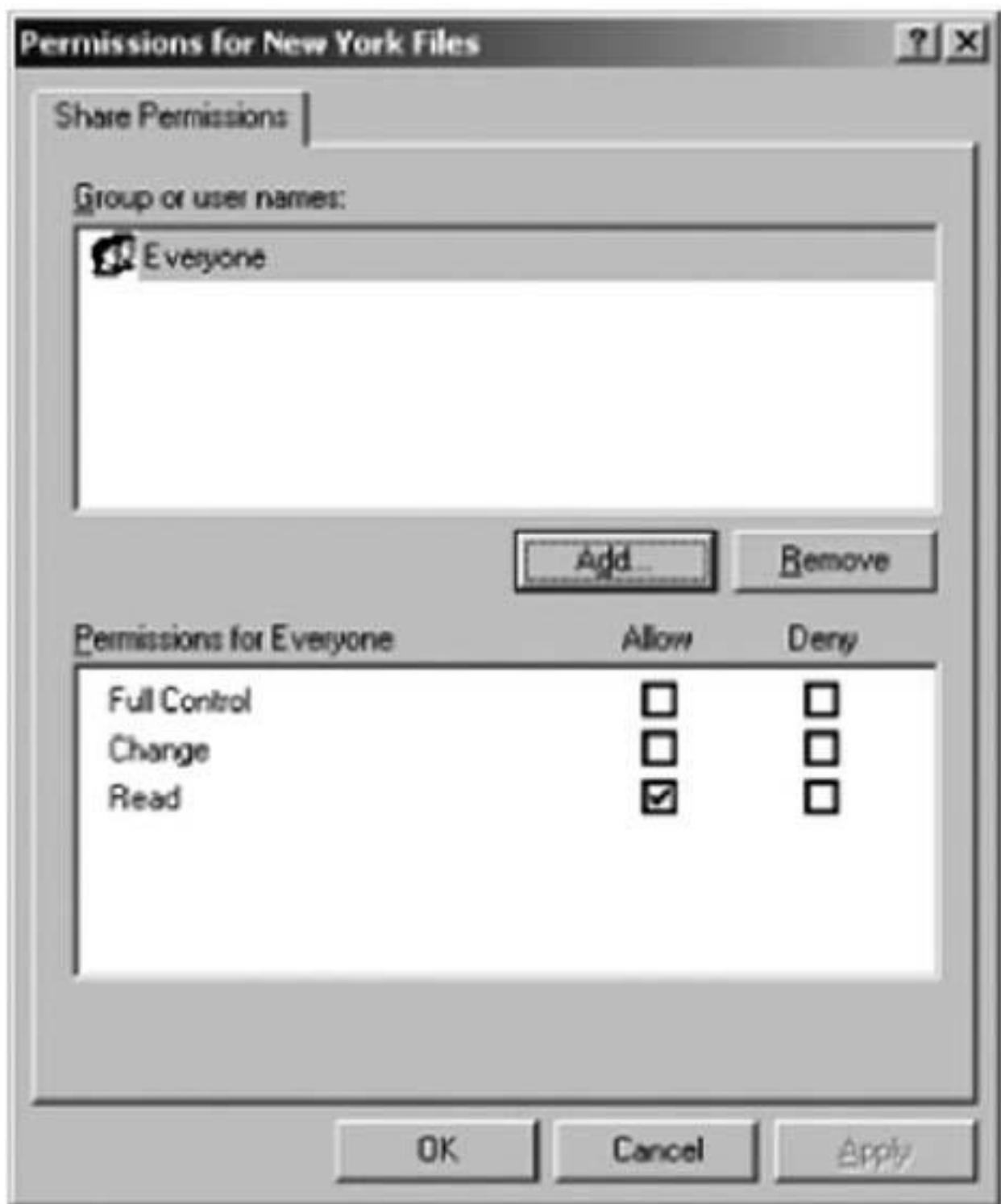


FIGURE F.8 Viewing sharing permissions



FIGURE F.9 Selecting groups for sharing permissions

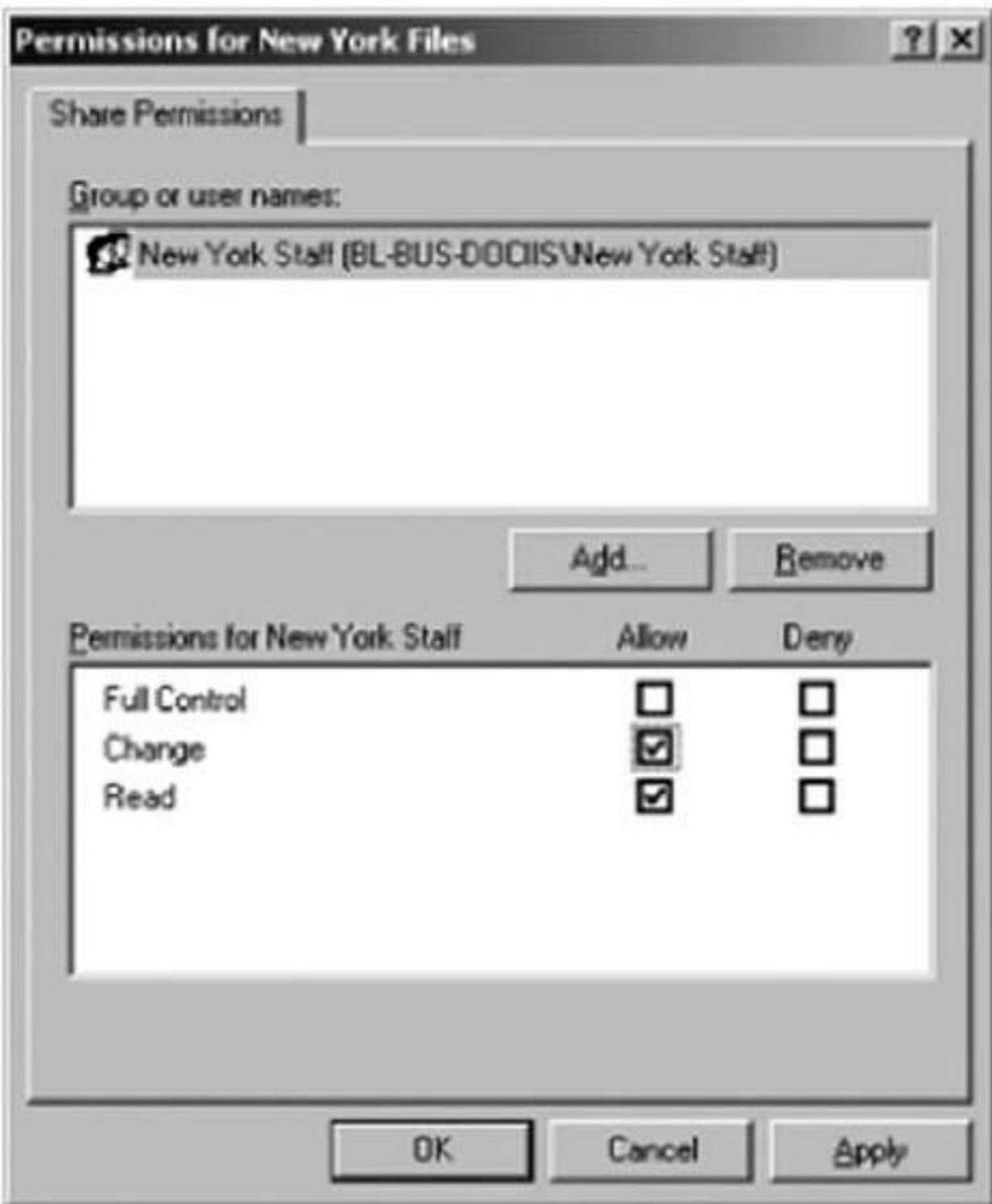


FIGURE F.10 Setting sharing permissions



FIGURE F.11 Viewing security permissions



FIGURE F.12 Granting security permissions

¹To create a domain account using Active Directory, click Start, Administrative Tools, Active Directory Users, and Computers. The screen in [Figure F.1](#) would display the domains rather than users, which you could then click on to see the users and groups.

GLOSSARY

A

Abilene network: The Abilene network is the part of Internet2 that is run by Indiana University.

access layer: The access layer is the part of a network that connects clients or servers to the rest of the network. It is often a LAN.

access point (AP): The part of the wireless LAN that connects the LAN to other networks.

ACK: See **acknowledgment (ACK)**.

acknowledgment (ACK): A character indicating a positive acknowledgment that a message has been received correctly.

ACM: Association for Computing Machinery. The ACM is an association of computer professionals.

acronym: A word formed from the initial letters or groups of letters of words in a phrase. An example is the word *laser*, which means *l*ight *a*mplification by *s*timulated *e*mission of *r*adiation.

address: A coded representation of the destination of data or of its originating source. For example, multiple computers on one communication circuit must each have a unique data link layer address.

address resolution: The process of determining the lower-layer address from a higher-layer address. For example, IP address resolution means determining the IP address from the application-layer address, whereas data link layer address resolution means determining the data link layer address from an IP address.

Address Resolution Protocol (ARP): The network-layer protocol standard for data link layer address resolution requests.

ADSL: See **asymmetric DSL (ADSL)**.

Advanced Encryption Standard (AES): A new single-key encryption standard authorized by NIST that replaces DES. It uses the Rijndael

(pronounced “rain doll”) algorithm and has key sizes of 128, 192, and 256 bits. NIST estimates that using the most advanced computers and techniques available today, it will require about 150 trillion years to crack AES by brute force.

Advanced Research and Development Network Operations

Center (ARDNOC): The agency funded by the Canadian government to develop new Internet2 technologies and protocols.

AES: *See Advanced Encryption Standard (AES).*

American National Standards Institute (ANSI): The principal standards-setting body in the United States. ANSI is a nonprofit, nongovernmental organization supported by more than 1,000 trade organizations, professional societies, and companies. It belongs to the ITU-T CCITT and the ISO.

American Standard Code for Information Interchange: *See ASCII.*

amplifier: A device used to boost the strength of a signal. Amplifiers are spaced at intervals throughout the length of a communication circuit to increase the distance a signal can travel. *See also repeater.*

amplitude modulation: *See modulation, amplitude.*

analog: Pertaining to representation by means of continuously variable quantity, such as varying frequencies. Physical quantities such as temperature are continuous variable, and therefore are “analog.”

analog signal: A signal in the form of a continuously varying quantity such as amplitude, which reflects variations in the loudness of the human voice.

analog transmission: Transmission of a continuously variable signal as opposed to a discrete on/off signal. The traditional way of transmitting a telephone or voice signal is analog.

ANI: *See automatic number identification (ANI).*

anonymous FTP: *See File Transfer Protocol (FTP).*

ANSI: *See American National Standards Institute (ANSI).*

AP: *See access point (AP).*

API: Application Program Interface. API is the way IBM links incompatible equipment for computer-to-mainframe links. API allows applications on

computers and mainframes to speak directly to each other at the application software level, even though the equipment is from different vendors.

Apple Talk: A set of communication protocols that defines networking for Apple computers. Rarely used today.

application service provider (ASP): An application service develops an application system (e.g., an airline reservation system, a payroll system) and companies purchase the service, without ever installing the software on their own computers. They simply use the service the same way you might use a Web hosting service to publish your own Web pages rather than attempting to purchase and operate your own Web server.

ARDNOC: *See Advanced Research and Development Network Operations Center (ARDNOC).*

ARP: *See Address Resolution Protocol (ARP).*

ARPANET: One of the early packet-switching networks. ARPANET was developed by the U.S. Department of Defense Advanced Research Projects Agency. It was the predecessor of the Internet.

ARQ: Automatic Repeat reQuest. A system employing an error-detecting code so conceived that any error initiates a repetition of the transmission of the incorrectly received message.

ASCII: American Standard Code for Information Interchange. Pronounced “ask-e.” An eight-level code for data transfer adopted by the ANSI to achieve compatibility among data devices.

asymmetric DSL (ADSL): A data link layer technology that provides high-speed (“broadband”) communication over traditional telephone lines. A DSL modem is used to provide three channels: a traditional voice channel, an upstream channel for communicating from the client to the ISP (often at speeds of 64 to 640 Kbps), and a downstream channel for communicating from the ISP to the client (often at speeds of 640 Kbps to 6 Mbps).

asynchronous transfer mode (ATM): A communication switch that handles interface speeds ranging from 25 million to 622 million bps. It multiplexes data streams onto the same BN by using cell relay techniques.

ATM switches can handle multimedia traffic, such as data, graphics, voice, and video.

asynchronous transmission: Transmission in which each information character is individually synchronized, usually by start and stop bits. The gap between each character is not a fixed length. *Compare with synchronous transmission.*

ATM: *See asynchronous transfer mode (ATM).* In banking, an automated teller machine.

attenuation: As a signal travels through a circuit, it gradually attenuates, or loses power. Expressed in decibels, attenuation is the difference between the transmitted and received power caused by loss of signal strength through the equipment, communication circuits, or other devices.

authentication: A security method of guaranteeing that a message is genuine, that it has arrived unaltered, and that it comes from the source indicated.

automatic number identification (ANI): The process whereby a long-distance common carrier provides its customers with a visual display of an incoming caller's telephone number.

Automatic Repeat reQuest: *See ARQ.*

B

backbone network (BN): A large network to which many networks within an organization are connected. It usually is a network that interconnects all networks on a single site, but it can be larger if it connects all the organization's terminals, computers, mainframes, LANs, and other communication equipment.

bandwidth: The difference between the highest and lowest frequencies in a band. For example, a voice-grade circuit has a 4,000-Hz bandwidth. In common usage, *bandwidth* refers to circuit capacity; when people say they need more bandwidth, they need a higher transmission speed.

basic rate interface (BRI): In ISDN, two 64,000-bps B circuits for data transmission and one 16,000-bps D circuit for signaling (2 B+D). Also called *basic rate access*. *See also primary rate interface (PRI).*

baud: Unit of signaling speed. Now obsolete and replaced by the term *symbol rate*. The speed in baud is the number of signal elements per second. If each signal represents only 1 bit, *baud* is the same as *bits per second (bps)*. When each signal contains more than 1 bit, *baud* does not equal *bps*.

BCC: See **block check character (BCC)**.

BER (bit-error rate): The number of bits received in error divided by the total number of bits received. An indicator of circuit quality.

BERT (bit-error rate testing): Testing a data line with a pattern of bits that are compared before and after the transmission to detect errors.

BGP: See **Border Gateway Protocol (BGP)**.

binary: A number system using only the two symbols 0 and 1 that is especially well adapted to computer usage because 0 and 1 can be represented as “on” and “off,” respectively, or as negative charges and positive charges, respectively. The binary digits appear in strings of 0’s and 1’s.

bipolar transmission: A method of digital transmission in which binary 0 is sent as a negative pulse and binary 1 is sent as a positive pulse.

bit: 1. An abbreviation of the term *binary digit*. 2. A single pulse in a group of pulses. 3. A unit of information capacity.

bit-error rate (BER): See **BER**.

bit-error rate testing (BERT): See **BERT**.

bit rate: The rate at which bits are transmitted over a communication path, normally expressed in bits per second (bps). The bit rate should not be confused with the data signaling rate (*baud*), which measures the rate of signal changes being transmitted. *See also bps*.

bit stream: A continuous series of bits being transmitted on a transmission line.

bits per second (bps): See **bps**.

BKER: Block-error rate. The number of blocks received in error divided by the total number of blocks received.

BKERT: Block-error rate testing. Testing a data link with groups of information arranged into transmission blocks for error checking.

block: Sets of contiguous bits or bytes that make up a message, frame, or packet.

block check character (BCC): The character(s) at the end of a binary synchronous communications (BSC) message used to check for errors.

block-error rate (BKER): *See BKER.*

block-error rate testing (BKERT): *See BKERT.*

Bluetooth: A standard for short-distance wireless communication.

BN: *See backbone network (BN).*

BOC: *See RBOC.*

BONDING (Bandwidth on Demand Interoperability)

Networking Group: An inverse multiplexing proposal for combining several 56-Kbps or 64-Kbps circuits into one higher-speed circuit.

Border Gateway Protocol (BGP): A network-layer standard protocol used to exchange route information between routers using dynamic decentralized routing. Used only between different TCP/IP autonomous systems (i.e., major sections of the Internet).

bps: Bits per second. The basic unit of data communication rate measurement. Usually refers to rate of information bits transmitted.

Contrast with baud and bit rate.

BRI: See basic rate interface (BRI)

bridge: A device that connects two similar networks using the same data link and network protocols. *Compare with gateway and router.*

broadband circuit: An analog communication circuit.

broadband communications: Originally, the term referred to analog communications, but it has become corrupted in common usage so that it now usually means high-speed communications networks, typically Internet access technologies with access speeds of 1 Mbps or higher.

broadband Ethernet: The 10Broad36 version of Ethernet IEEE 802.3, meaning that it transmits at 10 millions bps in broadband with a maximum distance of 3,600 meters.

broadcast routing: *See decentralized routing.*

brute-force attack: A way of breaking an encrypted message by trying all possible values of the key.

buffer: A device used for the temporary storage of data, primarily to compensate for differences in data flow rates (for example, between a terminal and its transmission circuit) but also as a security measure to allow retransmission of data if an error is detected during transmission.

burst error: A series of consecutive errors in data transmission. Refers to the phenomenon on communication circuits in which errors are highly prone to occurring in groups or clusters.

bus: A transmission path or circuit. Typically an electrical connection with one or more conductors in which all attached devices receive all transmissions at the same time.

byte: A small group of data bits that is handled as a unit. In most cases, it is an 8-bit byte and it is known as a *character*.

C

CA*net: The Canadian network that forms part of Internet2.

carrier: An analog signal at some fixed amplitude and frequency that then is combined with an information-bearing signal to produce an intelligent output signal suitable for transmission of meaningful information. *Also called carrier wave or carrier frequency.* **carrier frequency:** The basic frequency or pulse repetition rate of a signal bearing no intelligence until it is modulated by another signal that does impart intelligence.

Carrier Sense Multiple Access: *See CSMA/CA and CSMA/CD.*

CCITT: *See Consultative Committee on International Telegraph and Telephone (CCITT).* Now obsolete and renamed **International Telecommunications Union—Telecommunications (ITU-T)**.

CD: 1. Collision detection in the CSMA (Carrier Sense Multiple Access) protocol for LANs. 2. Carrier detect occurs when a modem detects a carrier signal to be received.

central office: The switching and control facility set up by the local telephone company (common carrier) where the subscriber's local loop terminates. Central offices handle calls within a specified geographic area, which is identified by the first three digits of the telephone number. *Also called an end office or exchange office.*

Central processing unit (CPU): *See CPU.*

CENTREX: A widespread telephone company switching service that uses dedicated central office switching equipment. CENTREX CPE is where the user site also has customer premises equipment (CPE).

CERT: See **Computer Emergency Response Team (CERT)**.

certificate authority (CA): A CA is a trusted organization that can vouch for the authenticity of the person or organization using authentication (e.g., VeriSign). A person wanting to use a CA registers with the CA and must provide some proof of identify. CA issues a digital certificate that is the requestor's public key encrypted using the CA's private key as proof of identity that can be attached to the user's e-mail or Web transactions.

channel: 1. A path for transmission of electromagnetic signals. *Synonym for line or link. Compare with circuit.* 2. A data communications path. Circuits may be divided into subcircuits.

character: A member of a set of elements used for the organization, control, or representation of data. Characters may be letters, digits, punctuation marks, or other symbols. *Also called a byte.*

cheapnet: See **thin Ethernet**. **checking, echo:** A method of checking the accuracy of transmitted data in which the received data are returned to the sending end for comparison with the original data.

checking, parity: See **parity check**.

checking, polynomial: See **polynomial checking**.

circuit: The path over which the voice, data, or image transmission travels. Circuits can be twisted-wire pairs, coaxial cables, fiber-optic cables, microwave transmissions, and so forth. *Compare with channel, line, and link.*

circuit switching: A method of communications whereby an electrical connection between calling and called stations is established on demand for exclusive use of the circuit until the connection is terminated.

cladding: A layer of material (usually glass) that surrounds the glass core of an optical fiber. Prevents loss of signal by reflecting light back into the core.

client: The input–output hardware device at the user's end of a communication circuit. There are three major categories of clients: computers, terminals, and special-purpose terminals.

cluster controller: A device that controls the input–output operations of the cluster of devices (computers, terminals, printers, and so forth) attached to it. Also called a *terminal controller*. For example, the 3274 Control Unit is a cluster controller that directs all communications between the host computer and remote devices attached to it.

CMIP: See **Common Management Interface Protocol (CMIP)**.

coaxial cable: An insulated wire that runs through the middle of a cable. A second braided wire surrounds the insulation of the inner wire like a sheath. Used on LANs for transmitting messages between devices.

code: A transformation or representation of information in a different form according to some set of preestablished conventions. *See also ASCII and EBCDIC.*

code conversion: A hardware box or software that converts from one code to another, such as from ASCII to EBCDIC.

codec: A codec translates analog voice data into digital data for transmission over computer networks. Two codecs are needed—one at the sender's end and one at the receiver's end.

collapsed backbone network: In a collapsed BN, the set of routers in a typical BN is replaced by one switch and a set of circuits to each LAN. The collapsed backbone has more cable but fewer devices. There is no backbone cable. The “backbone” exists only in the switch.

collision: When two computers or devices transmit at the same time on a shared multipoint circuit, their signals collide and destroy each other.

common carrier: An organization in the business of providing regulated telephone, telegraph, telex, and data communications services, such as AT&T, MCI, Bell-South, and NYNEX. This term is applied most often to U.S. and Canadian commercial organizations, but sometimes it is used to refer to telecommunication entities, such as government-operated suppliers of communication services in other countries. *See also PTT.*

Common Management Interface Protocol (CMIP): CMIP is a network management system that monitors and tracks network usage and other parameters for user workstations and other nodes. It is similar to SNMP, but it is more complete and is better in many ways.

communication services: A group of transmission facilities that is available for lease or purchase.

comparison risk ranking: The process by which the members of a Delphi team reach a consensus on which network threats have the highest risk. It produces a ranked list from high risk to low risk.

component: One of the specific pieces of a network, system, or application. When these components are assembled, they become the network, system, or application. Components are the individual parts of the network that we want to safeguard or restrict by using controls.

compression: *See data compression. Computer Emergency*

Response Team (CERT): The job of CERT, located at Carnegie Mellon University, is to respond to computer security problems on the Internet, raise awareness of computer security issues, and prevent security breaches. It was established by the U.S. Department of Defense in 1988 after a virus shut down almost 10 percent of the computers on the Internet. Many organizations are starting their own computer emergency response teams, so the term is beginning to refer to any response team, not just the one at Carnegie Mellon University.

concentrator: A device that multiplexes several low-speed communication circuits onto a single high-speed trunk. A remote data concentrator (RDC) is similar in function to a multiplexer but differs because the host computer software usually must be rewritten to accommodate the RDC. RDCs differ from statistical multiplexes because the total capacity of the high-speed outgoing circuit, in characters per second, is equal to the total capacity of the incoming low-speed circuits. On the other hand, output capacity of a statistical multiplexer (stat mux) is less than the total capacity of the incoming circuits.

conditioning: A technique of applying electronic filtering elements to a communication line to improve the capability of that line so it can support higher data transmission rates. *See also equalization.*

configuration: The actual or practical layout of a network that takes into account its software, hardware, and cabling. Configurations may be multidrop, point-to-point, LANs, and the like. By contrast, a topology is the

geometric layout (ring, bus, star) of the configuration. Topologies are the building blocks of configurations. *Compare with topology.*

connectionless routing: Connectionless routing means each packet is treated separately and makes its own way through the network. It is possible that different packets will take different routes through the network depending on the type of routing used and the amount of traffic.

connection-oriented routing: Connection-oriented routing sets up a virtual circuit (one that appears to use point-to-point circuit switching) between the sender and receiver. The network layer makes one routing decision when the connection is established, and all packets follow the same route. All packets in the same message arrive at the destination in the same order in which they were sent.

Consultative Committee on International Telegraph and Telephone (CCITT): An international organization that sets worldwide communication standards. Its new name is **International Telecommunications Union—Telecommunications (ITU-T).**

content caching: Storing content from other Web sites on your network to reduce traffic on your Internet connection. A content engine regularly stores incoming static content such as banners and graphics files so that future requests for those items can be processed internally.

content delivery: Storing content for your Web sites on the content delivery provider's servers spread around the Internet to reduce traffic on your Internet connection. The content delivery provider's servers contain the static content on your pages such as banners and graphics files. Software on your Web server locates the nearest content delivery server to the user (based on his or her IP address) and changes the references on your Web pages to draw the static content from that server. Content delivery was pioneered by Akamai, which is one of the leading content delivery services on the Internet.

contention: A method by which devices on the same shared multipoint circuit compete for time on the circuit.

control: A mechanism to ensure that the threats to a network are mitigated. There are two levels of controls: system-level controls and application-level controls.

control character: A character whose occurrence in a particular context specifies some network operation or function.

control spreadsheet: A two-dimensional matrix showing the relationship between the controls in a network, the threats that are being mitigated, and the components that are being protected. The controls listed in each cell represent the specific control enacted to reduce or eliminate the exposure.

core layer: The core layer is the central part of a network that provides access to the distribution layer. It is often a very fast BN that runs through the center of a campus or office complex.

COS: Corporation for Open Systems. An organization of computer and communications equipment vendors and users formed to accelerate the introduction of products based on the seven-layer OSI model. Its primary interest is the application layer (layer 7) of the OSI model and the X.400 email standard.

CPE: See **customer premises equipment (CPE)**.

CPU: Central processing unit.

CRC: Cyclical redundancy check. An error-checking control technique using a specific binary prime divisor that results in a unique remainder. It usually is a 16- to 32-bit character.

CSMA/CA: Carrier Sense Multiple Access (CSMA) with Collision Avoidance (CA). This protocol is similar to the Carrier Sense Multiple Access (CSMA) with Collision Detection (CD) protocol. Whereas CSMA/CD sends a data packet and then reports back if it collides with another packet, CSMA/CA sends a small preliminary packet to determine whether the network is busy. If there is a collision, it is with the small packet rather than with the entire message. CA is thought to be more efficient because it reduces the time required to recover from collisions.

CSMA/CD: Carrier Sense Multiple Access (CSMA) with Collision Detection (CD). A system used in contention networks. The network interface unit listens for the presence of a carrier before attempting to send and detects the presence of a collision by monitoring for a distorted pulse.

customer premises equipment (CPE): Equipment that provides the interface between the customer's CENTREX system and the telephone

network. It physically resides at the customer's site rather than the telephone company's end office. *CPE* generally refers to voice telephone equipment instead of data transmission equipment.

cut-through switching: A type of switching in which messages are forwarded as they arrive, almost on a bit-by-bit basis.

cyclical redundancy check (CRC): *See CRC.*

D

data: 1. Specific individual facts or a list of such items. 2. Facts from which conclusions can be drawn.

data circuit terminating equipment (DCE): *See DCE.*

data compression: The technique that provides for the transmission of fewer data bits without the loss of information. The receiving location expands the received data bits into the original bit sequence.

Data Encryption Standard (DES): *See DES.*

Data over Cable System Interface Specification (DOCSIS): A de facto data link layer standard for transmitting data via a cable modem using Ethernet-like protocols.

Data-over-Voice (DOV): When data and voice share the same transmission medium. Data transmissions are superimposed over the voice transmission.

data terminal equipment (DTE): *See DTE.*

datagram: A connectionless service in packet-switched networks. Each packet has a destination and sequence number and may follow a different route through the network. Different routes may deliver packets at different speeds, so data packets often arrive out of sequence. The sequence number tells the network how to reassemble the packets into a continuous message.

dB: *See decibel (dB).*

DCE: Data circuit terminating equipment. The equipment (usually the modem) installed at the user's site that provides all the functions required to establish, maintain, and terminate a connection, including the signal conversion and coding between the data terminal equipment (DTE) and the common carrier's line.

DDoS attack: *See distributed denial-of-service (DDoS) attack.*

decentralized routing: With decentralized routing, all computers in the network make their own routing decisions. There are three major types of decentralized routing. With static routing, the routing table is developed by the network manager and remains unchanged until the network manager updates it. With dynamic routing, the goal is to improve network performance by routing messages over the fastest possible route; an initial routing table is developed by the network manager but is continuously updated to reflect changing network conditions, such as message traffic. With broadcast routing, the message is sent to all computers, but it is processed only by the computer to which it is addressed.

decibel (dB): A tenth of a bel. A unit for measuring relative strength of a signal parameter such as power and voltage. The number of decibels is ten times the logarithm (base 10) of the ratio of the power of two signals, or ratio of the power of one signal to a reference level. The reference level always must be indicated, such as 1 milliwatt for power ratio.

dedicated circuit: A leased communication circuit that goes from your site to some other location. It is a clear, unbroken communication path that is yours to use 24 hours per day, 7 days per week. Also called a *private circuit* or **leased circuit**.

delay distortion: A distortion on communication lines that is caused because some frequencies travel more slowly than others in a given transmission medium and therefore arrive at the destination at slightly different times. Delay distortion is measured in microseconds of delay relative to the delay at 1,700 Hz. This type of distortion does not affect voice, but it can have a serious effect on data transmissions.

delay equalizer: A corrective device for making the phase delay or envelope delay of a circuit substantially constant over a desired frequency range. *See also equalizer.*

Delphi group: A small group of experts (three to nine people) who meet to develop a consensus when it may be impossible or too expensive to collect more accurate data. For example, a Delphi group of communication experts might assemble to reach a consensus on the various threats to a communication network, the potential dollar losses for each occurrence of each threat, and the estimated frequency of occurrence for each threat.

denial of service (DoS) attack: A DoS attempts to disrupt the network by flooding the network with messages so that the network cannot process messages from normal users.

DES: Data Encryption Standard. Developed by IBM and the U.S. National Institute of Standards, this widely used single-key encryption algorithm uses a 64-bit key.

desktop videoconferencing: With desktop videoconferencing, small cameras are installed on top of each user's computer so that participants can hold meetings from their offices.

DHCP: *See Dynamic Host Control Protocol (DHCP).*

digital signal: A discrete or discontinuous signal whose various states are discrete intervals apart, such as +15 volts and -15 volts.

digital subscriber line (DSL): A data link layer technology that provides high-speed ("broadband") communication over traditional telephone lines. A DSL modem is used to provide three channels: a traditional voice channel, an upstream channel for communicating from the client to the ISP (often at speeds of 64 to 640 Kbps), and a downstream channel for communicating from the ISP to the client (often at speeds of 640 Kbps to 6 Mbps).

distortion: The unwanted modification or change of signals from their true form by some characteristic of the communication line or equipment being used for transmission—for example, delay distortion and amplitude distortion.

distortion types: 1. *Bias:* A type of distortion resulting when the intervals of modulation do not all have exactly their normal durations. 2.

Characteristic: Distortion caused by transient disturbances that are present in the transmission circuit because of modulation. 3. *Delay:* Distortion occurring when the envelope delay of a circuit is not consistent over the frequency range required for transmission. 4. *End:* Distortion of start-stop signals. The shifting of the end of all marking pulses from their proper positions in relation to the beginning of the start pulse. 5. *Jitter:* A type of distortion that results in the intermittent shortening or lengthening of the signals. This distortion is entirely random in nature and can be

caused by hits on the line.

6. Harmonic: The resultant process of harmonic frequencies (due to nonlinear characteristics of a transmission circuit) in the response when a sinusoidal stimulus is applied.

distributed denial of service (DDoS) attack: With a DDoS attack, a hacker breaks into and takes control of many computers on the Internet (often several hundred to several thousand) and uses them to launch the DoS attack from thousands of computers at the same time.

distribution layer: The distribution layer is the part of a network that connects the access layer to other access layers and to the core layer. It is often a BN in a building.

DNS: See **Domain Name Service (DNS)**.

DOCSIS: See **Data over Cable System Interface Specification (DOCSIS)**.

Domain Name Service (DNS): A server that provides a directory used to supply IP addresses for application-layer addresses—that is, a server that performs IP address resolution.

DoS attack: See **denial of service (DoS) attack**.

download: The process of loading software and data into the nodes of a network from the central node. Downloading usually refers to the movement of data from a host mainframe computer to a remote terminal or computer.

DPSK: Differential phase shift keying. See **modulation, phase**.

DSL: See **digital subscriber line (DSL)**.

DTE: Data terminal equipment. Any piece of equipment at which a communication path begins or ends, such as a terminal.

duplexing: An alternative to the process of mirroring, which occurs when a database server mirrors or backs up the database with each transaction. In mirroring, the server writes on two different hard disks through two different disk controllers. Duplexing is more redundant and therefore even safer than mirroring, because the database is written to two different hard disks on two different disk circuits. *Compare with mirroring.*

Dynamic Host Control Protocol (DHCP): A network-layer protocol standard used to supply TCP/IP address information using dynamic address assignment.

dynamic routing: *See decentralized routing.*

E

EBCDIC: Extended Binary Coded Decimal Interchange Code. A standard code consisting of a set of 8-bit characters used for information representation and interchange among data processing and communication systems. Very common in IBM equipment.

echo cancellation: Used in higher-speed modems to isolate and filter out (cancel) echoes when half-duplex transmissions use stop and wait ARQ (Automatic Repeat reQuest) protocols. Needed especially for satellite links.

echo checking: *See checking, echo.*

echo suppressor: A device for use in a two-way telephone circuit (especially circuits over 900 miles long) to attenuate echo currents in one direction caused by telephone currents in the other direction. This is done by sending an appropriate disabling tone to the circuit.

ECMA: *See European Computer Manufacturers Association (ECMA).*

EDI: *See Electronic Data Interchange (EDI).*

EIA: *See Electronic Industries Association (EIA).*

Electronic Data Interchange (EDI): Electronic Data Interchange for Administration, Commerce, and Transport. Standardizes the electronic interchange of business documents for both ASCII and graphics. Endorsed by the ISO. Defines major components of the ANSI X.12 EDI standard.

Electronic Industries Association (EIA): Composed of electronic manufacturers in the United States. Recommends standards for electrical and functional characteristics of interface equipment. Belongs to ANSI. Known for the RS232 interface connector cable standard.

electronic mail (email): A networking application that allows users to send and receive mail electronically.

electronic software distribution (ESD): ESD enables network managers to install software on client computers over the network without physically touching each client computer. ESD client software is installed on each client and enables an ESD server to download and install certain

application packages on each client at some predefined time (e.g., at midnight on a Saturday).

email: *See electronic mail (email).*

emulate: Computer vendors provide software and hardware emulators that accept hardware and software from other vendors and enable them to run on their hardware or software.

encapsulation: A technique in which a frame from one network is placed within the data field of the frame in another network for transmission on the second network. For example, it enables a message initiated on a coaxial cable-based Ethernet LAN to be transmitted over an ATM fiber-optic-based network and then placed onto another Ethernet LAN at the other end.

encryption: The technique of modifying a known bit stream on a transmission circuit so that to an unauthorized observer, it appears to be a random sequence of bits.

end office: The telephone company switching office for the interconnection of calls. *See also central office.*

envelope delay distortion: A derivative of the circuit phase shift with respect to the frequency. This distortion affects the time it takes for different frequencies to propagate the length of a communication circuit so that two signals arrive at different times.

equalization: The process of reducing frequency and phase distortion of a circuit by introducing time differences to compensate for the difference in attenuation or time delay at the various frequencies in the transmission band.

equalizer: Any combination (usually adjustable) of coils, capacitors, or resistors inserted in the transmission circuit or amplifier to improve its frequency response.

error control: An arrangement that detects the presence of errors. In some networks, refinements are added that correct the detected errors, either by operations on the received data or by retransmission from the source.

ESD: *See electronic software distribution (ESD).*

Ethernet: A LAN developed by the Xerox Corporation. It uses coaxial cable or twisted-pair wires to connect the stations. It was standardized as IEEE 802.3.

European Computer Manufacturers Association (ECMA): Recommends standards for computer components manufactured or used in Europe. Belongs to the International Organization for Standardization (ISO).

exchange office: *See central office.*

exposure: The calculated or estimated loss resulting from the occurrence of a threat, as in “The exposure from theft could be \$42,000 this year.” It can be either tangible and therefore measurable in dollars or intangible and therefore not directly measurable in dollars. *See also comparison risk ranking.*

Extended Binary Coded Decimal Interchange Code (EBCDIC): *See EBCDIC.*

extranet: Using the Internet to provide access to information intended for a selected set of users, not the public at large. Usually done by requiring a password to access a selected set of Web sites.

F

FCC: *See Federal Communications Commission (FCC).*

FCS: *See frame check sequence (FCS).*

FDDI: *See fiber distributed data interface (FDDI).*

FDM: Frequency division multiplexing. *See multiplexer.*

feasibility study: A study undertaken to determine the possibility or probability of improving the existing system within a reasonable cost. Determines what the problem is and what its causes are and makes recommendations for solving the problem.

FEC: *See forward error correction (FEC).*

Federal Communications Commission (FCC): A board of seven commissioners appointed by the U.S. president under the Communication Act of 1934, having the power to regulate all interstate and foreign electrical communication systems originating in the United States.

FEП: *See front-end processor (FEP).*

fiber distributed data interface (FDDI): A token ring-like LAN technology that permits transmission speeds of 100 million bps using fiber-optic cables (ANSI standard X3T9.5).

fiber-optic cable: A transmission medium that uses glass or plastic cable instead of copper wires.

fiber optics: A transmission technology in which modulated visible lightwave signals containing information are sent down hair-thin plastic or glass fibers and demodulated back into electrical signals at the other end by a special light-sensitive receiver.

File Transfer Protocol (FTP): FTP enables users to send and receive files over the Internet. There are two types of FTP sites: closed (which require users to have an account and a password) and anonymous (which permit anyone to use them).

firewall: A router, gateway, or special-purpose computer that filters packets flowing into and out of a network. No access to the organization's networks is permitted except through the firewall. Two commonly used types of firewalls are packet level and application level.

firmware: A set of software instructions set permanently or semipermanently into read-only memory (ROM).

flow control: The capability of the network nodes to manage buffering schemes that allow devices of different data transmission speeds to communicate with each other.

forward error correction (FEC): A technique that identifies errors at the received station and automatically corrects those errors without retransmitting the message.

fractional T1 (FT1): A portion of a T1 circuit. A full T1 allows transmission at 1,544,000 bps. A fractional T1 circuit allows transmission at lower speeds of 384,000, 512,000, or 768,000 bps. *See also T carrier.*

fragment free switching: A type of switching that is a cross between store and cut through. Messages are stored until the header has been checked for errors and then the message is forwarded without checking for errors in the rest.

frame: Generally, a group of data bits having bits at each end to indicate the beginning and end of the frame. Frames also contain source addresses, destination addresses, frame type identifiers, and a data message.

frame check sequence (FCS): Used for error checking. FCS uses a 16-bit field with cyclical redundancy checking for error detection with retransmission.

frame relay: A type of packet-switching technology that transmits data faster than the X.25 standard. The key difference is that unlike X.25 networks, frame relay does not perform error correction at each computer in the network. Instead, it simply discards any messages with errors. It is up to the application software at the source and destination to perform error correction and to control for lost messages.

frequency: The rate at which a current alternates, measured in Hertz, kilohertz, megahertz, and so forth. Other units of measure are cycles, kilocycles, or megacycles; *hertz* and *cycles per second* are synonymous.

frequency division multiplexing (FDM): *See multiplexer.*

frequency modulation: *See modulation, frequency.*

frequency shift keying (FSK): *See FSK.*

front-end processor (FEP): An auxiliary processor that is placed between a computer's CPU and the transmission facilities. This device normally handles housekeeping functions like circuit management and code translation, which otherwise would interfere with efficient operation of the CPU.

FSK: Frequency shift keying. A modulation technique whereby 0 and 1 are represented by a different frequency and the amplitude does not vary.

FTP: *See File Transfer Protocol (FTP).*

full duplex: The capability of transmission in both directions at one time. *Contrast with half-duplex and simplex.*

G

gateway: A device that connects two dissimilar networks. Allows networks of different vendors to communicate by translating one vendor's protocol into another. *See also bridge, router, and brouter.*

Gaussian noise: *See noise, Gaussian.*

Gbps: Gigabit per second; 1 Gbps is equal to 1 billion bps.

GHz: Gigahertz; 1 GHz is equal to 1 billion cycles per second in a frequency.

gigabyte: One billion bytes.

G.Lite: One de facto standard form of ADSL.

guardband: A small bandwidth of frequency that separates two voice-grade circuits. Also, the frequencies between subcircuits in FDM systems that guard against subcircuit interference.

H

hacker: A person who sleuths for passwords to gain illegal access to important computer files. Hackers may rummage through corporate trash cans looking for carelessly discarded printouts.

half-duplex: A circuit that permits transmission of a signal in two directions but not at the same time. *Contrast with full duplex and simplex.*

Hamming code: A forward error correction (FEC) technique named for its inventor.

handshaking: Exchange of predetermined signals when a connection is established between two data set devices. This is used to establish the circuit and message path.

HDLC: See **high-level data link control (HDLC)**.

Hertz (Hz): Same as cycles per second; for example, 3,000 Hz is 3,000 cycles per second.

high-level data link control (HDLC): A bit-oriented protocol in which control of data links is specified by series of bits rather than by control characters (bytes).

home page: A home page is the main starting point or page for a World Wide Web entry.

host computer: The computer that lies at the center of the network. It generally performs the basic centralized data processing functions for which the network was designed. The host used to be where the network communication control functions took place, but today these functions tend

to take place in the front-end processor or further out in the network. Also called a *central computer*.

hotline: A service that provides direct connection between customers in various cities using a dedicated circuit.

HTML: Web text files or pages use a structural language called HTML (Hypertext Markup Language) to store their information. HTML enables the author to define different type styles and sizes for the text, titles, and headings, and a variety of other formatting information. HTML also permits the author to define links to other pages that may be stored on the same Web server or on any Web server anywhere on the Internet.

hub: Network hubs act as junction boxes, permitting new computers to be connected to the network as easily as plugging a power cord into an electrical socket, and provide an easy way to connect network cables. Hubs also act as repeaters or amplifiers. Hubs are sometimes also called *concentrators*, *multistation access units*, or *transceivers*.

Hypertext Markup Language (HTML): See **HTML**.

Hz: See **Hertz (Hz)**.

I

IAB: See **Internet Architecture Board (IAB)**.

IANA: See **Internet Assigned Numbers Authority (IANA)**.

ICMP: See **Internet Control Message Protocol (ICMP)**.

idle character: A transmitted character indicating “no information” that does not manifest itself as part of a message at the destination point.

IDS: See **intrusion detection system (IDS)**.

IEEE: See **Institute of Electrical and Electronics Engineers (IEEE)**.

IESG: Internet Engineering Steering Group.

IETF: Internet Engineering Task Force.

IMAP: See **Internet Mail Access Protocol (IMAP)**.

impulse noise: See **noise, impulse**.

in-band signaling: The transmission signaling information at some frequency or frequencies that lie within a carrier circuit normally used for information transmission.

Institute of Electrical and Electronics Engineers (IEEE): A professional organization for engineers in the United States. Issues standards and belongs to the ANSI and the ISO. IEEE has defined numerous standards for networks; see [Chapters 6–9](#).

integrated services digital network (ISDN): *See ISDN.*

interexchange circuit (IXC): A circuit or circuit between end offices (central offices).

interLATA: Circuits that cross from one LATA (local access and transport area) into another.

intermodulation distortion: An analog line impairment whereby two frequencies create a third erroneous frequency, which in turn distorts the data signal representation.

International Organization for Standardization (ISO): *See ISO.*

International Telecommunications Union—Telecommunications (ITU-T): An international organization that sets worldwide communication standards. Its old name was **Consultative Committee on International Telegraph and Telephone (CCITT)**.

Internet: The information superhighway. The network of networks that spans the world, linking more than 20 million users.

Internet Architecture Board (IAB): IAB provides strategic architectural oversight (e.g., top-level domain names, use of international character sets) that can be passed on as guidance to the IESG or turned into published statements or simply passed directly to the relevant IETF working group. The IAB does not produce polished technical proposals but rather tries to stimulate action by the IESG or the IETF that will lead to proposals that meet general consensus. The IAB appoints the IETF chair and all IESG members.

Internet Assigned Numbers Authority (IANA): IANA governs the assignment of IP numbers.

Internet Control Message Protocol (ICMP): A simple network layer protocol standard intended to exchange limited routing information

between routers. Most commonly known as a ping, after the DOS and UNIX command.

Internet Engineering Steering Group (IESG): The IESG is responsible for technical management of IETF activities and the Internet standards process. It administers the process according to the rules and procedures and is directly responsible for the actions associated with entry into and movement along the Internet “standards track,” including final approval of specifications as Internet standards. Each IETF working group is chaired by a member of the IESG.

Internet Engineering Task Force (IETF): IETF is a large, open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. IETF operates through a series of working groups, which are organized by topic (e.g., routing, transport, security). The requests for comment (RFCs) that form the basis for Internet standards are developed by the IETF and its working groups.

Internet Mail Access Protocol (IMAP): An application-layer protocol standard that covers communication between an email client and an email server.

Internet Research Task Force (IRTF): IRTF operates much like the IETF, through small research groups focused on specific issues. Although IETF working groups focus on current issues, IRTF research groups work on long-term issues related to Internet protocols, applications, architecture, and technology. The IRTF chair is appointed by the IAB.

Internet Service Provider (ISP): ISPs offer connections to the Internet. Some access providers charge a flat monthly fee for unlimited access (much like the telephone company), whereas others charge per hour of use (much like a long-distance telephone call).

Internet Society (ISOC): ISOC is the closest the Internet has to an owner. ISOC is an open-membership professional society with more than 175 organizational and 8,000 individual members in over 100 countries and includes corporations, government agencies, and foundations that have created the Internet and its technologies.

internetworking: Connecting several networks together so workstations can address messages to the workstations on each of the other networks.

Internet2: There are many different organizations currently working on the next generation of the Internet, including the Abilene network, vBNS, and CA*net. Although each is working in a slightly different fashion, they join together with each other and parts of the regular Internet at gigapops (gigabit points of presence).

interoperability: The interconnection of dissimilar networks in a manner that allows them to operate as though they were similar.

IntraLATA: Circuits that are totally within one LATA (local access transport area).

intranet: Using Internet protocols on a network internal to an organization so that information is accessible using a browser, for example, but only by employees, not the public at large. Usually done by requiring a password to access a selected set of Web sites and protecting the site by a firewall so no outsiders can access it.

intrusion detection system (IDS): An IDS monitors a network segment, a server, or an application on the server for signs of unauthorized access and issues an alarm when an intrusion is detected. A misuse detection IDS compares monitored activities with signatures of known attacks, whereas an anomaly detection IDS compares monitored activities with the “normal” set of activities.

inverse multiplexer: Hardware that takes one high-speed transmission and divides it among several transmission circuits.

IPX/SPX: Internetwork packet exchange/sequenced packet exchange (IPX/SPX), based on a routing protocol developed by Xerox in the 1970s, is the primary network protocol used by Novell NetWare. About 40 percent of all installed LANs use it.

IRTF: See **Internet Research Task Force (IRTF)**.

ISDN: Integrated services digital network. A hierarchy of digital switching and transmission systems. The ISDN provides voice, data, and image in a unified manner. It is synchronized so all digital elements speak the same “language” at the same speed. *See also basic rate interface (BRI) and primary rate interface (PRI).*

ISO: International Organization for Standardization, in Geneva, Switzerland. The initials *ISO* stand for its French name. This international standards-making body is best known in data communications for developing the internationally recognized seven-layer network model called the Open Systems Interconnection (OSI) Reference model. *See also OSI model.*

ISOC: *See Internet Society (ISOC).*

ISP: *See Internet Service Provider (ISP).*

ITU-T: *See International Telecommunications Union—Telecommunications (ITU-T).*

IXC: *See interexchange circuit (IXC).*

J

jack: The physical connecting device at the interface that mates with a compatible receptacle—a plug.

jumper: 1. A small connector that fits over a set of pins on a computer circuit card. 2. A patch cable or wire used to establish a circuit for testing or diagnostics.

K

K: A standard quantity measurement of computer storage. A K is defined loosely as 1,000 bytes. In fact, it is 1,024 bytes, which is the equivalent of 2^{10} .

Kbps: Kilobits per second. A data rate equal to 10^3 bps (1,000 bps).

Kermit: A very popular asynchronous file transfer protocol named after Kermit the Frog. The Kermit protocol was developed by Columbia University, which released it as a free software communications package. Various versions of Kermit can be found on public bulletin board systems for downloading to a computer.

key management: The process of controlling the secret keys used in encryption.

KHz: Kilohertz; 1 KHz is equal to 1,000 cycles per second in a frequency.

kilobits per second (Kbps): *See Kbps.*

kilometer: A metric measurement equal to 0.621 mile or 3,280.8 feet.

L

LAN: See **local area network (LAN)**.

laser: Light amplification by stimulated emission of radiation. A device that transmits an extremely narrow and coherent beam of electromagnetic energy in the visible light spectrum. (*Coherent* means that the separate waves are in phase with one another rather than jumbled as in normal light.)

LATA: Local access transport area. One of approximately 200 local telephone service areas in the United States roughly paralleling major metropolitan areas. The LATA subdivisions were established as a result of the AT&T/Bell divestiture to distinguish local from long-distance service. Circuits with both end points within the LATA (intraLATAs) generally are the sole responsibility of the local telephone company. Circuits that cross outside the LATA (interLATAs) are passed on to an interexchange carrier like AT&T, MCI, or US Sprint.

latency: The delay between when the first bits of a message arrive at a device and when it begins transmitting them.

leased circuit: A leased communication circuit that goes from your site to some other location. It is a clear, unbroken communication path that is yours to use 24 hours per day, 7 days per week. Also called *private circuit* or **dedicated circuit**.

line: A circuit, channel, or link. It carries the data communication signals. An early telephone technology term that may imply a physical connection, such as with a copper wire. Compare with **channel**, **circuit**, and **link**.

link: An unbroken circuit path between two points. Sometimes called a **line**, **channel**, or **circuit**.

LLC: The logical link control, or LLC, sublayer is just an interface between the MAC sublayer and software in layer 3 (the network layer) that enables the software and hardware in the MAC sublayer to be separated from the logical functions in the LLC sublayer. By separating the LLC sublayer from the MAC sublayer, it is simpler to change the MAC hardware and software without affecting the software in layer 3. The most commonly used LLC protocol is IEEE 802.2.

local access transport area (LATA): See **LATA**.

local area network (LAN): A network that is located in a small geographic area, such as an office, a building, a complex of buildings, or a campus, and whose communication technology provides a high-bandwidth, low-cost medium to which many nodes can be connected. These networks typically do not use common carrier circuits, and their circuits do not cross public thoroughfares or property owned by others. LANs are not regulated by the FCC or state public utilities commissions.

local exchange carrier: The local telephone company, such as one of the seven regional Bell operating companies (RBOCs).

local loop: The part of a communication circuit between the subscriber's equipment and the equipment in the local central office.

log: 1. A record of everything pertinent to a system function. 2. A collection of messages that provides a history of message traffic.

logical link control (LLC): *See LLC.*

longitudinal redundancy check (LRC): A system of error control based on the formation of a block check following preset rules. The check formation rule is applied in the same manner to each character. In a simple case, the LRC is created by forming a parity check on each bit position of all characters in the block. (That is, the first bit of the LRC character creates odd parity among the 1-bit positions of the characters in the block.)

LRC: *See longitudinal redundancy check (LRC).*

M

M: Mega. The designation for 1 million, as in 3 megabits per second (3 Mbit/s).

MAC: *See media access control (MAC).*

MAN: *See metropolitan area network (MAN).*

management information base (MIB): The extent of information that can be retrieved from a user computer when using the Simple Network Management Protocol (SNMP) for network management. MIBs are sets of attributes and definitions that pertain to specific network devices.

Manchester encoding: The digital transmission technique used in the physical layer of Ethernet LANs. *See Chapter 3.*

Mbps: A data rate equal to 10^6 bps. Sometimes called *megabits per second* (1,000,000 bps).

mean times: See **MTBF**, **MTTD**, **MTTF**, and **MTTR**.

media access control (MAC): A data link layer protocol that defines how packets are transmitted on a local area network. *See also CSMA/CD, token bus, and token ring.*

medium: The matter or substance that carries the voice or data transmission. For example, the medium can be copper (wires), glass (fiber-optic cables), or air (microwave or satellite).

megabit: One million bits.

megabyte: One million bytes.

mesh network: A network topology in which there are direct point-to-point connections among the computers.

message: A communication of information from a source to one or more destinations. A message usually is composed of three parts: (1) a heading, containing a suitable indicator of the beginning of the message together with some of the following information: source, destination, date, time, routing; (2) a body containing the information to be communicated; (3) an ending containing a suitable indicator of the end of the message.

message switching: An operation in which the entire message being transmitted is switched to the other location without regard to whether the circuits actually are interconnected at the time of your call. This usually involves a message store and forward facility.

meter: A metric measurement equal to 39.37 inches.

metropolitan area network (MAN): A network that usually covers a citywide area. Because MANs use LAN and fiber-optic technologies, transmission speeds can vary between 2 million and 100 million bps.

MHz: Megahertz; 1 MHz is equal to 1 million cycles per second in a frequency.

MIB: *See management information base (MIB).*

MIME: *See Multipurpose Internet Mail Extension (MIME).*

MIPS: One million instructions per second. Used to describe a computer's processing power.

mirroring: A process in which the database server automatically backs up the disk during each database transaction. During this process, the computer writes on two different hard disks on the same disk circuit every time the hard disk is updated. This creates two mirror images of the database data. Disk mirroring can be accomplished only when the database server contains two physical disk drives, because the records or data structures are written to both disks simultaneously. Should a problem develop with one disk, the second disk is available instantly with identical information on it. *Compare with duplexing.*

mnemonic: A group of characters used to assist the human memory. A mnemonic frequently is an acronym.

modem: A contraction of the words **mo**dulator-**dem**odulator. A modem is a device for performing necessary signal transformation between terminal devices and communication circuits. Modems are used in pairs, one at either end of the communication circuit.

modulation, amplitude: The form of modulation in which the amplitude of the carrier is varied in accordance with the instantaneous value of the modulating signal.

modulation, frequency: A form of modulation in which the frequency of the carrier is varied in accordance with the instantaneous value of the modulating signal.

modulation, phase: A form of modulation in which the phase of the carrier is varied in accordance with the instantaneous value of the modulating signal. Phase modulation has two related techniques. Phase shift keying (PSK) uses a 180° change in phase to indicate a change in the binary value (0 or 1), Differential phase shift keying (DPSK) uses a 180° change in phase every time a bit is transmitted; otherwise, the phase remains the same.

modulation, pulse code: See **pulse code modulation (PCM).**

MTBF: mean time between failures. The statistic developed by vendors to show the reliability of their equipment. It can be an actual calculated figure that generally is more accurate, or it can be a practical (theoretical) figure.

MTTD: Mean time to diagnose. The time it takes the network testing and problem management staff to diagnose a network problem.

MTTF: Mean time to fix. The time it takes vendors to remedy a network problem once they arrive on the premises.

MTTR: 1. Mean time to repair—the combination of mean time to diagnose, mean time to respond, and mean time to fix, indicating the entire length of time it takes to fix a fault in equipment. 2. Mean time to respond—the time it takes the vendor to respond when a network problem is reported.

multidrop (multipoint): A line or circuit interconnecting several stations/nodes in a sequential fashion.

multiplexer: A device that combines data traffic from several low-speed communication circuits onto a single high-speed circuit. The two popular types of multiplexing are FDM (frequency division multiplexing) and TDM (time division multiplexing). In FDM, the voice-grade link is divided into subcircuits, each covering a different frequency range in such a manner that each subcircuit can be employed as though it were an individual circuit. In TDM, separate time segments are assigned to each terminal. During these time segments, data may be sent without conflicting with data sent from another terminal.

multiplexing (MUX): The subdivision of a transmission circuit into two or more separate circuits. This can be achieved by splitting the frequency range of the circuit into narrow frequency bands (frequency division multiplexing) or by assigning a given circuit successively to several different users at different times (time division multiplexing).

Multipurpose Internet Mail Extension (MIME): An application-layer standard protocol that enables SMTP mail messages to transfer nontext characters such as graphics and software. The sending email client translates the nontext characters into something that resembles text using MIME codes and attaches it to the message. The receiving email client translates the MIME codes back into the original graphic or software file.

MUX: *See multiplexing (MUX).*

N

NAK: *See negative acknowledgment (NAK).* **nanosecond:** One billionth ($1/1,000,000,000$) of a second or 10^{-9} .

NAP: *See network access point (NAP).*

NAT: See **network address translation (NAT)**.

National Institute of Standards and Technology (NIST): Formerly the National Bureau of Standards. The agency of the U.S. government responsible for developing information processing standards for the federal government.

NCO: See **network cost of ownership (NCO)**.

negative acknowledgment (NAK): The return signal that reports an error in the message received. The opposite of **acknowledgment (ACK)**.

network: 1. A series of points connected by communication circuits. 2. The switched telephone network is the network of telephone lines normally used for dialed telephone calls. 3. A private network is a network of communication circuits confined to the use of one customer.

network access point (NAP): An “intersection” on the Internet where many national and regional ISPs connect to exchange data.

network address translation (NAT): The process of translating between one set of private IP addresses inside a network and a set of public IP addresses outside the network for use on the Internet. NAT is transparent in that no computer notices that it is being done.

network cost of ownership (NCO): NCO is a measure of how much it costs per year to keep one computer operating. NCO includes the cost of support staff to attach it to the network, install software, administer the network (e.g., create user IDs, back up user data), provide training and technical support, and upgrade hardware and software. NCO is often \$1,500 to \$3,500 per computer per year. *Compare with total cost of ownership (TCO).*

network interface card (NIC): An NIC allows the computer to be physically connected to the network cable; the NIC provides the physical-layer connection from the computer to the network.

network operating system (NOS): The NOS is the software that controls the network. The NOS provides the data link and the network layers and must interact with the application software and the computer's own operating system. Every NOS provides two sets of software: one that runs on the network server(s) and one that runs on the network client(s).

network operations center (NOC): Any centralized network management control site.

network profile: Every LAN computer has a profile that outlines what resources it has available to other computers in the network and what resources it can use elsewhere in the network.

network service: An application available on a network—for example, file storage.

NIC: *See network interface card (NIC).*

NIST: *See National Institute of Standards and Technology (NIST).*

NOC: *See network operations center (NOC).*

node: In a description of a network, the point at which the links join input–output devices. It could be a computer or a special-purpose device such as a router.

noise: The unwanted change in waveform that occurs between two points in a transmission circuit.

noise, amplitude: A sudden change in the level of power with differing effects, depending on the type of modulation used by the modem.

noise, cross-talk: Noise resulting from the interchange of signals on two adjacent circuits; manifests itself when it is possible to hear other people's telephone conversations.

noise, echo: The “hollow” or echoing characteristic that is heard on voice-grade lines with improper echo suppression.

noise, Gaussian: Noise that is characterized statistically by a Gaussian, or random, distribution.

noise, impulse: Noise caused by individual impulses on the circuit.

noise, intermodulation: Noise that occurs when signals from two independent lines intermodulate. A new signal forms and falls into a frequency band differing from those of both inputs. The new signal may fall into a frequency band reserved for another signal.

NOS: *See network operating system (NOS).*

NRZ: Nonreturn to zero. A binary encoding and transmission scheme in which 1's and 0's are represented by opposite and alternating high and low

voltages, and in which there is no return to a reference (zero) voltage between encoded bits.

NRZI: Nonreturn to zero inverted. A binary encoding scheme that inverts the signal on a 1 and leaves the signal unchanged for a 0, and in which a change in the voltage state signals a 1-bit value and the absence of a change denotes a 0-bit value.

null character: A control character that can be inserted into or withdrawn from a sequence of characters without altering the message.

null modem cable: A 6- to 8-foot RS232 cable that makes the two computers connected at each end of the cable think they are talking through modems.

O

office, central or end: The common carrier's switching office closest to the subscriber.

100Base-T: An Ethernet LAN standard that runs at 100 million bps and uses unshielded twisted-pair wires.

1000Base-T: An Ethernet LAN standard that runs at 1 billion bps and uses unshielded twisted-pair wires.

Open Shortest Path First (OSPF): A network-layer standard protocol used to exchange route information between routers using dynamic decentralized routing.

Open Systems Interconnection (OSI) Reference model: See **OSI model**.

optical fibers: Hair-thin strands of very pure glass (sometimes plastic) over which light waves travel. They are used as a medium over which information is transmitted.

OSI model: The seven-layer Open Systems Interconnection (OSI) Reference model developed by the ISO subcommittee. The OSI model serves as a logical framework of protocols for computer-to-computer communications. Its purpose is to facilitate the interconnection of networks.

OSPF: See **Open Shortest Path First (OSPF)**.

out-of-band signaling: A method of signaling that uses a frequency that is within the passband of the transmission facility but outside of a carrier circuit normally used for data transmission.

overhead: Computer time used to keep track of or run the system, as compared with computer time used to process data.

overlay network: A network (usually a WLAN) used to supplement a primary network (usually a wired LAN).

P

packet: A group of binary digits, including data and control signals, that is switched as a composite whole. The data, control signals, and error-control information are arranged in a specific format. A packet often is a 128-character block of data.

packet assembly/disassembly (PAD): *See PAD.*

Packet Layer Protocol (PLP): *See PLP.* **packet switching:** Process whereby messages are broken into finite-size packets that always are accepted by the network. The message packets are forwarded to the other party over a multitude of different circuit paths. At the other end of the circuit, the packets are reassembled into the message, which is then passed on to the receiving terminal.

packet switching network (PSN): A network designed to carry data in the form of packets. The packet and its format are internal to that network. The external interfaces may handle data in different formats, and format conversion may be done by the user's computer.

PAD: Packet assembly/disassembly. Equipment providing packet assembly and disassembly between asynchronous transmission and the packet-switching network.

PAM: *See pulse amplitude modulation (PAM).*

parallel: Describes the way the internal transfer of binary data takes place within a computer. It may be transmitted as a parallel word, but it is converted to a serial or bit-by-bit data stream for transmission.

parity bit: A binary bit appended to an array of bits to make the number of 1 bits always be odd or even for an individual character. For example, odd parity may require three 1 bits and even parity may require four 1 bits.

parity check: Addition of noninformation bits to a message to detect any changes in the original bit structure from the time it leaves the sending device to the time it is received.

Pbps: Petabits per second. A data rate equal to 1 quadrillion bits per second (1,000,000,000,000,000).

PBX: private branch exchange. Telephone switch located at a customer's site that primarily establishes voice communications over tie lines or circuits as well as between individual users and the switched telephone network. Typically also provides switching within a customer site and usually offers numerous other enhanced features, such as least-cost routing and call detail recording.

PCM: *See pulse code modulation (PCM).*

PDN: *See public data network (PDN).*

PDU: Protocol Data Unit.

peer: A dictionary definition of *peer* is “a person who is equal to another in abilities.” A peer-to-peer network, therefore, is one in which each computer node has equal abilities. In communications, a peer is a node or station that is on the same protocol layer as another.

peer-to-peer communications: 1. Communication between two or more processes or programs by which both ends of the session exchange data with equal privilege. 2. Communication between two or more network nodes in which either side can initiate sessions because no primary–secondary relationship exists.

peer-to-peer LAN: A network in which a computer can serve as both a server and a user. Every computer has access to all the network's resources on an equal basis.

permanent virtual circuit (PVC): A virtual circuit that resembles a leased line because it can be dedicated to a single user. Its connections are controlled by software.

phase modulation: *See modulation, phase.* **pirate:** A person who obtains the latest software programs without paying for them. A skilled software pirate is able to break the protection scheme that is designed to prevent copying.

PKI: See **public key infrastructure (PKI)**.

plain old telephone network (POTS): The nickname for the public switched telephone network. Often used when referring to dial-up Internet access using a modem.

PLP: Packet Layer Protocol (PLP) is the routing protocol that performs the network layer functions (e.g., routing and addressing) in X.25 networks.

point of presence (POP): The physical access location of an ISP or voice or data communications carrier.

point-to-point: Denoting a circuit or line that has only two terminals. A link. An example is a single computer connected to a mainframe.

polling: Any procedure that sequentially queries several terminals in a network.

polling, hub: A type of sequential polling in which the polling device contacts a terminal, that terminal contacts the next terminal, and so on, until all the terminals have been contacted.

polling, roll call: Polling accomplished from a prespecified list in a fixed sequence, with polling restarted when the list is completed.

polynomial checking: A checking method using polynomial functions to test for errors in data in transmission. Also called **cyclical redundancy check (CRC)**.

POP: See **Post Office Protocol (POP)** and **point-of-presence (POP)**.

port: One of the circuit connection points on a front-end processor or local intelligent controller.

Post Office Protocol (POP): An application-layer standard used to communicate between the client and the email server.

POTS: See **plain old telephone network (POTS)**.

PPP: PPP (multilink Point-to-Point Protocol) is an inverse multiplexing protocol for combining circuits of different speeds (e.g., a 64,000-bps circuit with a 14,400-bps circuit), with data allocated to each circuit based on speed and need. PPP enables the user to change the circuits allocated to the PPP multiplexed circuit in mid-transmission so that the PPP circuit can increase or decrease the capacity. PPP is the successor to SLIP.

primary rate interface (PRI): In ISDN, twenty-three 64,000 bits per second D circuits for data and one 64,000 bits per second B circuit for signaling (23 B+D). See also **basic rate interface (BRI)**.

private branch exchange (PBX): *See PBX.* **propagation delay:** The time necessary for a signal to travel from one point on the circuit to another, such as from a satellite dish up to a satellite or from Los Angeles to New York.

protocol: A formal set of conventions governing the format and control of inputs and outputs between two communicating devices. This includes the rules by which these two devices communicate as well as handshaking and line discipline.

protocol stack: The set of software required to process a set of protocols.

PSK: Phase shift keying; *see modulation, phase.*

PSN: *See packet switching network (PSN).*

PTT: Postal, telephone, and telegraph. These are the common carriers owned by governments; the government is the sole or monopoly supplier of communication facilities.

public data network (PDN): A network established and operated for the specific purpose of providing data transmission services to the public. It can be a public packet-switched network or a circuit-switched network. Public data networks normally offer value-added services for resource sharing at reduced costs and with high reliability. These time-sharing networks are available to anyone with a modem.

public key encryption: Public key encryption uses two keys. The public key is used to encrypt the message and a second, very different private key is used to decrypt the message. Even though the sender knows both the contents of the outgoing message and the public encryption key, once it is encrypted, the message cannot be decrypted without the private key. Public key encryption is one of the most secure encryption techniques available.

public key infrastructure (PKI): The PKI is the process of using public key encryption on the Internet. PKI begins with a certificate authority (CA), which is a trusted organization that can vouch for the authenticity of the person or organization using authentication (e.g., VeriSign). The CA issues a digital certificate that is the requestor's public key encrypted using the

CA's private key as proof of identity. This certificate is then attached to the user's email or Web transactions. The receiver then verifies the certificate by decrypting it with the CA's public key—and must also contact the CA to ensure that the user's certificate has not been revoked by the CA.

pulse amplitude modulation (PAM): Amplitude modulation of a pulse carrier. PAM is used to translate analog voice data into a series of binary digits before they are transmitted.

pulse code modulation (PCM): Representation of a speech signal by sampling at a regular rate and converting each sample to a binary number. In PCM, the information signals are sampled at regular intervals and a series of pulses in coded form are transmitted, representing the amplitude of the information signal at that time.

Q

QAM: Quadrature amplitude modulation. A sophisticated modulation technique that uses variations in signal amplitude, which allows data-encoded symbols to be represented as any of 16 states to send 4 bits on each signal.

Quality of Service (QoS): The ability of devices to give different priorities to different types of messages so that some messages (e.g., voice telephone data) are transmitted faster than other messages (e.g., email).

quantizing error: The difference between the PAM signal and the original voice signal. The original signal has a smooth flow, but the PAM signal has jagged "steps."

R

RBOC: Regional Bell operating company. One of the seven companies created after divestiture of the old Bell system to provide local communications. Includes Ameritech, Bell Atlantic, BellSouth, NYNEX, Pacific Telesis, Southwestern Bell, and US West.

reclocking time: *See turnaround time.* **redundancy:** The portion of the total information contained in a message that can be eliminated without loss of essential information.

regional Bell operating company (RBOC): *See RBOC.*

reliability: A characteristic of the equipment, software, or network that relates to the integrity of the system against failure. Reliability usually is measured in terms of mean time between failures (MTBF), the statistical measure of the interval between successive failures of the hardware or software under consideration.

repeater: A device used to boost the strength of a signal. Repeaters are spaced at intervals throughout the length of a communication circuit.

request for comment (RFC): A proposed standard for the Internet on which anyone in the world is invited to comment.

request for proposal (RFP): A request for proposal is used to solicit bids from vendors for new network hardware, software, and services. RFPs specify what equipment, software, and services are desired and ask vendors to provide their best prices.

response time: The time the system takes to react to a given input; the time interval from when the user presses the last key to the terminal's typing the first letter of the reply. Response time includes (1) transmission time to the computer; (2) processing time at the computer, including access time to obtain any file records needed to answer the inquiry; and (3) transmission time back to the terminal.

retrain time: *See turnaround time.*

RFC: *See request for comment (RFC).*

RFP: *See request for proposal (RFP).*

ring: 1. The hot wire in a telephone circuit. 2. An audible sound used for signaling the recipient of an incoming telephone call. 3. A LAN topology having a logical geometric arrangement in the shape of a ring.

RIP: *See Routing Information Protocol (RIP).*

risk: The level or amount of exposure to an item when compared with other items. It is a hazard or chance of loss. Risk is the degree of difference, as in, "What level of risk does one threat have when compared to the other threats?"

risk assessment: The process by which one identifies threats, uses a methodology to determine the tangible or intangible exposures, and develops a sequenced list of the threats from the one having the highest risk to the one having the lowest risk. The list may be in a sequence based on

tangible dollar losses or on intangible criteria such as public embarrassment, likelihood of occurrence, most dangerous, most critical to the organization, and greatest delay. Also called *risk ranking* or *risk analysis*.

RMON: Remote monitoring. The definitions of what is stored and therefore retrievable from a remote user computer when using the Simple Network Management Protocol (SNMP). It is referred to as the RMON MIB (management information base). *See also management information base (MIB) and Simple Network Management Protocol (SNMP).*

router: A device that connects two similar networks having the same network protocol. It also chooses the best route between two networks when there are multiple paths between them. *Compare with bridge, brouter, and gateway.*

Routing Information Protocol (RIP): A network-layer standard protocol used to exchange route information between routers using dynamic decentralized routing.

RS232: A technical specification published by the Electronic Industries Association that specifies the mechanical and electrical characteristics of the interface for connecting data terminal equipment (DTE) and data circuit terminating equipment (DCE). It defines interface circuit functions and their corresponding connector pin assignments.

RS449: An Electronic Industries Association standard for data terminal equipment (DTE) and data circuit terminating equipment (DCE) connection that specifies interface requirements for expanded transmission speeds (up to 2 million bps), longer cable lengths, and 10 additional functions.

S

SDLC: *See synchronous data link control (SDLC).*

serial: 1. Transmitting bits one at a time and in sequence. 2. The sequential or consecutive occurrence of two or more related activities in a single device or circuit.

server: A computer that provides a particular service to the client computers on the network. In larger LANs, the server is dedicated to being

a server. In a peer-to-peer LANs, the server may be both a server and a client computer. There may be file, database, network, access, modem, facsimile, printer, and gateway servers.

server farm: A LAN segment containing many servers.

service-level agreement (SLA): Specifies the exact type of performance and fault conditions that the organization will accept and what compensation the service provider must provide if it fails to meet the SLA. For example, the SLA might state that network availability must be 99 percent or higher and that the MTBF for T1 circuits must be 120 days or more.

Service Set Identifier (SSID): A simple, easily broken approach to WLAN security.

session: A logical connection between two terminals. This is the part of the message transmission when the two parties are exchanging messages. It takes place after the communication circuit has been set up and is functioning.

signal: A signal is something that is sent over a communication circuit. It might be a control signal used by the network to control itself.

signal-to-noise ratio: The ratio, expressed in dB, of the usable signal to the noise signal present.

Simple Mail Transfer Protocol (SMTP): An application-layer protocol standard used to transfer email messages across the Internet.

Simple Network Management Protocol (SNMP): An application-layer protocol standard used in network management for monitoring and configuring network devices. *See also management information base (MIB) and RMON.*

simplex: A circuit capable of transmission in one direction only. *Contrast with full duplex and half-duplex.*

single cable: A one-cable system in broadband LANs in which a portion of the bandwidth is allocated for “send” signals and a portion for “receive” signals, with a guardband in between to provide isolation from interference.

SLIP: Serial Line Internet Protocol (SLIP) is a proposed standard for inverse multiplexing. It has been surpassed by PPP.

SMTP: *See Simple Mail Transfer Protocol (SMTP).*

SNA: See **systems network architecture (SNA)**.

SNMP: See **Simple Network Management Protocol (SNMP)**.

SONET: See **synchronous optical network (SONET)**.

spanning tree protocol: A data link layer protocol used to prevent broadcast storm in networks that have redundant links providing multiple paths between LAN segments.

spike: A sudden increase of electrical power on a communication circuit. *Spike* is a term used in the communication industry. *Contrast with surge*.

spread spectrum: The U.S. military developed spread spectrum through-the-air radio transmission technology primarily to overcome the problem of intentional interference by hostile jamming and secondarily for security. A spread spectrum signal is created by modulating the original transmitted radio frequency (RF) signal with a spreading code that causes “hopping” of the frequency from one frequency to another. By contrast, conventional AM and FM radio uses only one frequency to transmit its signal.

start bit: A bit that precedes the group of bits representing a character. Used to signal the arrival of the character in asynchronous transmission.

static routing: See **decentralized routing**.

statistical multiplexer: Stat mux or STDM. A time division multiplexer (TDM) that dynamically allocates communication circuit time to each of the various attached terminals, according to whether a terminal is active or inactive at a particular moment. Buffering and queuing functions also are included. *See also concentrator*.

stop bit: A bit that follows the group of bits representing a character. Used to signal the end of a character in asynchronous transmission.

store and forward switching: A switching technique that accepts messages, stores them, and then forwards them to the next location after ensuring they contain no errors as addressed in the message header.

STX: A control character used in ASCII and EBCDIC data communications to mean start of text.

surge: A sudden increase in voltage on a 120-volt electrical power line. A term used in the electric utilities industry. *Contrast with spike*.

switch: Switches connect more than two LAN segments that use the same data link and network protocol. They may connect the same or different

types of cable. Switches typically provide ports for 4, 8, 16, or 32 separate LAN segments, and most enable all ports to be in use simultaneously, so they are faster than bridges.

switched circuit: A dial-up circuit in which the communication path is established by dialing. If the entire circuit path is unavailable, there is a busy signal, which prevents completion of the circuit connection.

Switched Multimegabit Data Service (SMDS): See **SMDS**.

switched network: Any network that has switches used for directing messages from the sender to the ultimate recipient.

switched network, circuit switched: A switched network in which switching is accomplished by disconnecting and reconnecting lines in different configurations to set up a continuous pathway between the sender and the recipient. *See also circuit switching.*

switched network, store and forward: A switched network in which the store-and-forward principle is used to handle transmission between senders and recipients. *See also store and forward switching.*

switching: Identifying and connecting independent transmission links to form a continuous path from one location to another.

symbol rate: The speed in baud is the number of symbols per second. If each signal represents only one bit, *symbol rate* is the same as *bits per second*. When each signal contains more than one bit, *symbol rate* does not equal *bits per second*.

synchronization character (SYN): An 8-bit control character that is sent at the beginning of a message block to establish synchronization (timing) between the sender and the receiver. Term used for the characters preceding an Ethernet packet. Term used for a TCP open connection request.

synchronous data link control (SDLC): A protocol for managing synchronous, code-transparent, serial bit-by-bit information transfer over a link connection. Transmission exchanges may be full-duplex or half-duplex and over switched or nonswitched links. The configurations of the link connection may be point-to-point, multipoint, or loop. SDLC is the protocol used in IBM's systems network architecture.

synchronous optical network (SONET): The National Exchange Carriers Association standard for optical transmission at gigabits-per-second speeds. For example, digital signals transmit on T1 circuits at 1,544,000 bps and on T3 circuits at 44,376,000 bps. The slowest SONET OC-1 optical transmission rate of 51,840,000 bps is slightly faster than the T3 rate.

synchronous transmission: Form of transmission in which data is sent as a fixed-length block or frame. *Compare with asynchronous transmission.*

systems network architecture (SNA): The name of IBM's conceptual framework that defines the data communication interaction between computer systems or terminals.

T

T carrier: A hierarchy of digital circuits designed to carry speech and other signals in digital form. Designated T1 (1.544 Mbps), T2 (6.313 Mbps), T3 (44.736 Mbps), and T4 (274.176 Mbps).

tariff: The formal schedule of rates and regulations pertaining to the communication services, equipment, and facilities that constitute the contract between the user and the common carrier. Tariffs are filed with the appropriate regulatory agency (FCC or state public utilities commission) for approval and published when approved.

TASI: Time-assisted speech interpolation. The process of interleaving two or more voice calls on the same telephone circuit simultaneously.

Tbps: Terabits per second. A data rate equal to 1 trillion bits per second (1,000,000,000,000).

TCM: Trellis-coded modulation (TCM) is a modulation technique related to QAM that combines phase modulation and amplitude modulation. There are several different forms of TCM that transmit 5, 6, 7, or 8 bits per signal, respectively.

TCP/IP: Transmission Control Protocol/Internet Protocol is probably the oldest networking standard, developed for ARPANET, and now used on the Internet. One of the most commonly used network protocols.

TDM: *See multiplexer.*

telecommunications: A term encompassing voice, data, and image transmissions that are sent over some medium in the form of coded signals.

telecommuting: Telecommuting employees perform some or all of their work at home instead of going to the office each day.

teleconferencing: With teleconferencing, people from diverse geographic locations can “attend” a business meeting in both voice and picture format. In fact, even documents can be shown and copied at any of the remote locations.

telephony: A generic term to describe voice communications. Pronounced “te-LEF-o-nee,” not “te-le-FO-nee.”

Telnet: Telnet enables users on one computer to log in to other computers on the Internet.

10Base-T: An Ethernet LAN standard (IEEE 802.3) that runs at 10 million bps and uses unshielded twisted-pair wires.

10Base2: An Ethernet LAN standard that runs at 10 million bps, uses baseband transmission techniques, and allows 200 meters maximum cable length.

10Base5: An Ethernet LAN standard that runs at 10 million bps, uses baseband transmission techniques, and allows 500 meters maximum cable length.

10Broad36: An Ethernet LAN standard that runs at 10 million bps, uses broadband transmission techniques, and allows 3,600 meters maximum cable length.

thick Ethernet: Refers to the original Ethernet specification that uses thick coaxial cable that is both grounded and shielded. The many layers of shielding are of polyvinyl and aluminum, which make the cable wider in diameter than other Ethernet cables. The heavy shielding also makes the cable more expensive and less flexible; therefore, it is impractical for many installations.

thin Ethernet: Refers to the 10Base2 baseband Ethernet, meaning the version that transmits at 10 million bps in baseband at 200 meters maximum. It uses thin coaxial cable. Also called **cheapnet**.

threat: A potentially adverse occurrence or unwanted event that could be injurious to the network, the computing environment, the organization, or

a business application. Threats are acts or events the organization wants to prevent from taking place, such as lost data, theft, disasters, virus infections, errors, illegal access, and unauthorized disclosure. In other words, threats are events no one wants to occur.

3DES: *See triple DES (3DES).*

throughput: The total amount of useful information that is processed or communicated during a specific time period.

Time-assisted speech interpolation (TASI): *See TASI.*

Time division multiplexing (TDM): *See multiplexer.*

token: The special sequence of characters used to gain access to a token ring or token-bus network to transmit a packet.

token bus: A LAN with a bus topology that uses a token-passing approach to network access. In a token-bus LAN, the next logical node or station is not necessarily the next physical node because it uses preassigned priority algorithms. Message requests are not handled in consecutive order by stations. *Contrast with*

token ring. token passing: A method of allocating network access wherein a terminal can send a message only after it has acquired the network's electronic token.

token ring: A LAN with a ring topology that uses a token-passing approach to network access. In a token ring LAN, the next logical station also is the next physical station because the token passes from node to node. *Contrast with token bus.*

topology: The basic physical or geometric arrangement of the network—for example, a ring, star, or bus layout. The topology is the network's logical arrangement, but it is influenced by the physical connections of its links and nodes. This is in contrast to its configuration, which is the actual or practical layout, including software and hardware constraints. Topologies are the building blocks of a network configuration. *Compare with configuration.*

total cost of ownership (TCO): A measure of how much it costs per year to keep one computer operating. TCO includes the cost of support staff to attach it to the network, install software, administer the network (e.g., create user IDs, back up user data), provide training and technical support,

and upgrade hardware and software, along with the cost of “wasted time” when the network is down. TCO is often \$10,000 per computer per year. ***Compare to network cost of ownership (NCO).***

transceiver: A device that transmits and/or receives data to or from computers on an Ethernet LAN. Also a hub.

transmission rate of information bits (TRIB): *See TRIB.*

tree: A network arrangement in which the stations hang off a common “branch,” or data bus, like leaves on the branch of a tree.

TRIB: Transmission rate of information bits. A TRIB is the network's throughput. It is the effective rate of data transfer over a communication circuit per unit of time. Usually expressed in bits per second.

triple DES (3DES): 3DES is a symmetric encryption technique that involves using DES three times, usually with three different keys, to produce the encrypted text, which produces a stronger level of security than DES, because it has a total of 168 bits as the key (i.e., 3×56 bits).

trunk: A voice communication circuit between switching devices or end offices.

turnaround time: The time required to reverse the direction of transmission from send to receive or vice versa on a half-duplex circuit.

twisted pair: A pair of wires used in standard telephone wiring. They are twisted to reduce interference caused by the other twisted pairs in the same cable bundle. Twisted-pair wires go from homes and offices to the telephone company end office.

U

UDP: *See User Datagram Protocol (UDP).*

uniform resource locator (URL): *See URL.*

uninterruptible power supply (UPS): Provides backup electrical power if the normal electrical power fails or if the voltage drops to unacceptably low levels.

unipolar transmission: A form of digital transmission in which the voltage changes between 0 volts to represent a binary 0 and some positive value (e.g., +15 volts) to represent a binary 1. *See also bipolar transmission.*

unshielded twisted-pair (UTP) wires: The type of wiring used in 10Base-T Ethernet networks. Same as **twisted pair**.

upload: The process of loading software and data from the nodes of a network (terminals or computers), over the network media, and to the host mainframe computer.

UPS: See **uninterruptible power supply (UPS)**.

URL: To use a browser to access a Web server, you must enter the server's addresses or URL (uniform resource locator). All Web addresses begin with seven characters: http://.

USASCII: See **ASCII**.

User Datagram Protocol (UDP): A connectionless transport layer protocol standard used by TCP to send short messages such as DNS requests.

user profile: The user profile specifies what data and network resources a user can access, and the type of access (read-only, write, create, delete, etc.).

UTP: See **unshielded twisted-pair (UTP) wires**.

V

V.nn: The V. nn series of ITU-T standards relating to the connection of digital equipment to the analog telephone network. Primarily concerned with the modem interface. See [Chapter 3](#) for definitions.

value-added network (VAN): A corporation that sells services of a value-added network. Such a network is built using the communication offerings of traditional common carriers, connected to computers that permit new types of telecommunication tariffs to be offered. The network may be a packet switching or message switching network.

VBNS: See **very-high-performance backbone network service (vBNS)**.

VDSL: See **very-high-data-rate digital subscriber line (VDSL)**.

VDT: Video display terminal.

vertical redundancy check (VRC): See **parity check**.

very-high-performance backbone network service (vBNS): One part of Internet2 run by MCI World-Com.

video teleconferencing: Video teleconferencing provides real-time transmission of video and audio signals to enable people in two or more locations to have a meeting.

virtual: Conceptual or appearing to be, rather than actually being.

virtual circuit: A temporary transmission circuit in which sequential data packets are routed between two points. It is created by the software in such a way that users think they have a dedicated point-to-point leased circuit.

virtual private network (VPN): A hybrid network that includes both public and private facilities. The user leases a bundle of circuits and configures the VPN on an as-needed basis so that some traffic travels on the private leased network and some travels on the common carrier's public network.

virus: Viruses are executable programs that copy themselves onto other computers. Most viruses attach themselves to other programs or to special parts on disks, and as those files execute or are accessed, the virus spreads. Viruses cause unwanted events—some are harmless (such as nuisance messages) and others are serious (such as the destruction of data). Some viruses change their appearances as they spread, making detection more difficult.

voice-grade circuit: A term that applies to circuits suitable for transmission of speech, digital or analog data, or facsimile, generally with a frequency range of about 300 to 3,300 Hz contained within a 4,000-Hz circuit.

VPN: *See virtual private network (VPN).*

VRC: Vertical redundancy check. Same as **parity check**.

W

WAN: *See wide area network (WAN).*

WAP: *See Wireless Application Protocol (WAP).*

warchalk: marking (usually using chalk on pavement) the location and information for unsecured WLANs.

wardriving: The act of finding unsecured WLAN access points (usually by driving around).

weather map: A network map showing real-time utilization on each circuit.

Web: See **World Wide Web**.

Web browser: A software package on the client computer that enables a user to access a Web server.

Web crawler: A Web crawler searches through all the Web servers it knows to find information about a particular topic.

Web server: A Web server stores information in a series of text files called pages. These text files or pages use a structured language called HTML (Hypertext Markup Language) to store their information.

wide area network (WAN): A network spanning a large geographical area. Its nodes can span city, state, or national boundaries. WANs typically use circuits provided by common carriers. *Contrast with backbone network (BN), local area network (LAN), and metropolitan area network (MAN)*.

Wi-Fi: The trademarked name for 802.11b.

Wi-Fi Protected Access (WPA): A technique for providing security in WLANs.

Wired Equivalent Privacy (WEP): A technique for providing security in WLANs that is not very effective.

Wireless Application Protocol (WAP): A de facto standard set of protocols for connecting wireless devices to the Web. WAP provides a variety of protocols at the application, transport, and network layers to enable devices with a very small display screen to display standard Web information.

wire speed: Operating at the same speed as the incoming circuit; having extremely low latency.

wiring closet: A central point at which all the circuits in a system begin or end, to allow cross-connection.

World Wide Web: The Web provides a graphical user interface and enables the display of rich graphical images, pictures, full-motion video, and sound clips.

X

X.nn: The X. nn series of ITU-T standards relating to transmission over public data networks.

X.400: An OSI standard that defines how messages are to be encoded for the transmission of email and graphics between dissimilar computers and terminals. X.400 defines what is in an electronic address and what the electronic envelope should look like. Approved by the CCITT.

X.500: An OSI standard that defines where to find the address to put on the electronic envelope of a X.400 transmission. X.500 is the directory of names and addresses similar to the yellow pages of a telephone directory.

Xmodem: Xmodem is an asynchronous file transmission protocol that takes the data being transmitted and divides it into blocks. Each block has a start of header (SOH) character, a 1-byte block number, 128 bytes of data, and a 1-byte checksum for error checking.

Y

Ymodem: Ymodem is an asynchronous file transmission protocol. The primary benefit of the Ymodem protocol is CRC-16 error checking.

Z

Zmodem: Zmodem is a newer asynchronous file transmission protocol written to overcome some of the problems in older protocols. It uses CRC-32 with continuous ARQ and dynamically adjusts its packet size according to communication circuit conditions to increase efficiency. It usually is the preferred protocol of most bulletin board systems.

INDEX

A

Abilene network, 326, 329, 334, 458, 460

Acceptance stage, of standardization process, 23

Access BN layer, 243

Access cards, 383–84

Access control list (ACL), [173](#), [364–65](#), [518–19](#)
Access layer, [414](#)
of backbone network, [9](#), [12–14](#), [25](#), [126](#), [239–62](#), [346](#), [359](#)
of network, [245](#), [250](#), [259](#), [356](#), [414–16](#), [421](#)
Access points (AP), [201–03](#), [219–20](#), [226](#), [232](#), [241](#), [248](#), [255](#), [318](#), [326](#),
[362–63](#)
Access request technique, [121](#)
Access VPN, [287–89](#)
Account, [397](#), [468](#)
Acknowledgment (ACK), [128](#)
negative, [128](#)
Active Directory Service (ADS), [206](#)
Adaptive differential pulse code modulation (ADPCM), [108](#), [498](#)
Address field, [133–35](#), [151](#), [215](#)
Address resolution, [162–65](#), [193](#)
data link layer, [16–19](#), [21](#), [25](#), [30](#), [120](#), [126–27](#), [131–32](#), [135](#), [157–65](#), [178–79](#), [502–12](#)
server name resolution, [162–64](#)
Address Resolution Protocol (ARP), [165](#)
Addressing, [157–65](#)
address resolution, [162–65](#)
data link layer address resolution, [164](#)
domain name service (DNS), [163](#)
server name resolution, [162](#)
application layer address, [157](#)
assigning addresses, [158–62](#)
classless addressing, [159](#)
data link layer address, [158](#)
dynamic addressing, [161–62](#)
internet addresses, [159](#)
network layer address, [157](#)
subnet mask, [161](#)

subnets, [160–61](#)
types of, [158](#)

Advanced Encryption Standard (AES), [217](#), [377](#)

Advanced Research and Development Network Operations Center (ARDNOC), [326](#)

Adware, [374](#)

Agent, [427](#)

Akamai, [434–35](#)
Ticketmaster and, [434](#)

Alarm, [424–25](#)
message, [424](#)
storm, [425](#)

Algorithms, [374–76](#)

Alternating current (AC), [97](#)

[Amazon.com](#), [349](#)

American National Standards Institute (ANSI), [23](#)

American Telephone and Telegraph Company (AT&T), [6](#), [295](#), [312](#), [341](#), [356](#)
global/IP network, [470](#)

Amperes (amps), [97](#)

Amplifiers, [125](#)

Amplitude, [100](#)

Amplitude modulation (AM), [101](#)

Amplitude shift keying (ASK), [101](#)

Analog circuit, [77](#)

Analog data, [78](#)
translating to digital, [105–06](#)

Analog transmission of digital data, [100–04](#)
amplitude modulation (AM), [101](#)
bit rate versus baud rate versus symbol rate, [103](#)
frequency modulation (FM), [101–02](#)
modems transmitting data, [104](#)
data compression, [104](#)

modulation, [101–04](#)
 basic modulation, [101](#)
 phase modulation (PM), [102–03](#)
 multiple bits, sending, [102](#)
 quadrature amplitude modulation (QAM), [103](#)
Anomaly detection, [387](#)
Antennas
 directional, [205](#)
 omnidirectional, [204](#)
Antivirus software, [352](#)
AOL Instant Messenger, [60](#)
Apple Mac Operating System, [59](#), [206](#)
Application architectures, [40–64](#)
 client-based, [40](#), [42–43](#)
 client-server, [40](#), [43–46](#), [56–57](#)
 factors in choosing, [47–49](#)
 host-based, [40](#), [41–42](#)
 peer-to-peer, [40](#), [46–47](#)
Application layer, [39–65](#), [504–05](#)
 address, [157](#)
 application logic, [40](#)
 architectures, [40–49](#)
 client-based architectures, [40](#), [42–43](#)
 clients, [41](#)
 client-server architectures, [40](#), [43–46](#)
 cluster, [41](#)
 data access logic, [40](#)
 data storage, [40](#)
 dumb terminals, [41](#)
 functions, [40](#)
 host-based architectures, [40–42](#)
 internet model, [19](#)

mainframe, [41](#)
message transmission using, [19](#)
network computer, [41](#)
OSI model, [18](#)
peer-to-peer architectures, [40](#), [46–47](#)
personal computer, [41](#)
presentation logic, [40](#)
servers, [41](#)
structured query language (SQL), [40](#)
terminal, [41](#)
transaction terminal, [41](#)
virtual server, [41](#)
Application logic, [40](#), [46](#)
Application management software, [426](#)
Application service providers (ASPs), [28](#)
Application systems, [46](#), [410](#), [414](#)
Application-based VLANs, [428](#)
Application-level firewall, [365–66](#)
Architectures, choosing, [47–49](#)
ARPANET, [9](#), [59](#), [150](#)
ASCII. *See* United States of America Standard Code for Information Interchange (USASCII)
Assets, network, [345](#)
Assigning addresses, [158–62](#)
Association, [213](#)
 associating with AP, [214](#)
Asymmetric digital subscriber line (ADSL), [319](#)
 G.Lite, [87](#)
Asymmetric encryption, [375](#)
Asynchronous transfer mode (ATM), [282–3](#)
Asynchronous transmission, [132–33](#)
AT&T. *See* American Telephone and Telegraph Company (AT&T)

Attenuation, [124](#)
Audit, software, [199](#)
Australia, networking in, [85](#)
Authentication, [378–381](#). *See also* User authentication
 authentication server, [385](#)
 central authentication, [385](#)
Automated teller machine (ATM) network, [383](#)
Automatic number identification (ANI), [273](#)
Automatic Repeat reQuest (ARQ), [128](#)
 continuous ARQ, [128](#)
 stop-and-wait ARQ, [128](#)
Autonomous systems, [168–69](#), [314](#)
Auxiliary port, [172](#)
Availability, [294](#), [342](#), [462](#)

B

Back Orifice Trojan horse, [373–75](#), [391](#)
Backbone networks (BNs), [12–15](#), [239–67](#). *See also* Switched backbones
 architecture layers, [243–44](#)
 access layer, [243](#)
 core layer, [244](#)
 distribution layer, [244](#)
 architectures, [243–58](#)
 campus network, [239](#)
 components, [240–43](#)
 enterprise network, [240](#)
 gateways, [242–43](#)
 improving performance, [260–61](#)
 circuit capacity, [260–61](#)
 computer and device performance, [260](#)
 routers, [240–42](#)
 switches, [240](#)

Backup, [358–59](#)
Bain, Alexander, [5](#)
Bandwidth, [104](#)
 limiters, [432](#)
Baseline, [414–15](#)
Basic access service. *See* Basic rate interface (BRI)
Basic rate interface (BRI), [273](#)
Batch processing, [8](#)
Baud rate, [103](#)
Beacon frame, [214](#)
Bell Canada, [270](#)
Bell, Alexander Graham, [5–6](#)
BellSouth, [7](#), [270](#), [284](#), [315](#)
Biometrics, [384](#)
Bipolar signaling, [98](#)
Bit rate, [103](#)
BITNET network, [9](#)
Bits per second (bps), [15](#), [104](#)
 Gbps, [27](#)
 Kbps, [15](#)
 Mbps, [27](#)
 Pbps, [27](#)
Bluetooth, [226](#)
 media access control, [120](#), [202](#)
 topology, [208–11](#)
Body, of SMTP packet, [57](#)
BONDING (Bandwidth on Demand Interoperability Networking Group)
standard, [86](#)
Border Gateway Protocol (BGP), [168–69](#), [314](#)
Border router, [169](#)
Bottleneck, [223](#)
Bridge Protocol Data Unit (BPDU), [495](#)

Broadband communication, [27](#)
Broadband ISDN (B-ISDN), [272–73](#)
Broadband technologies, [318](#), [328](#)
Broadcast message, [164](#), [171](#)
Browser, web, [49](#)
Brute-force attacks, [376](#)
Building-block network design process, [411–13](#)
 cost assessment, [412](#), [421–24](#)
 needs analysis, [412–18](#). *See also individual entry*
 technology design, [412](#), [418–21](#). *See also individual entry*
Burst error, [123](#)
Bus topology, [208](#), [228](#)
Business continuity, [342](#), [351–61](#)
 denial-of-service protection, [352–56](#)
 device failure protection, [356–57](#)
 disaster protection, [357–61](#)
 intrusion prevention, [361–90](#)
 intrusion prevention systems, [387–88](#)
 intrusion recovery, [388–90](#)
 server and client protection, [369–74](#)
 social engineering prevention, [385–87](#)
 theft protection, [356](#)
 virus protection, [351–52](#)
Byte, [96](#)

C

CA*net, [9](#), [10](#), [326](#)
Cable modem termination system (CMTS), [321](#)
Cable modems, [104](#), [320–22](#)
 architecture, [320–22](#)
 types of, [322](#)
Cables, [12](#)

Cat 5, [88](#)
coaxial, [89](#)
connector, [482–92](#)
fiber-optic, [89–91](#)
looking inside, [114–16](#)
managing network, [205](#)
moving, [125](#)
network, [202](#)
patch, [116](#), [247](#)
plan for, [205](#)
problems with, [204](#)
twisted-pair, [88–89](#), [484](#)
Cabling, [205](#), [219](#)
Cache engine. *See* Content engine
Campus network, [239](#)
Canadian Radio-Television and Telecommunications Commission (CRTC),
[270](#)
Capacity management, [432](#)
Capacity planning, [419](#), [428](#)
Career opportunities, [5](#)
Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), [213–14](#)
 contention-based CSMA/CD approach, [213](#)
Carrier Sense Multiple Access with Collision Detection (CSMA/CD), [211](#),
[213](#)
Carrier wave, [101](#)
Carterfone court decision, [6](#)
Casual intruders, [361](#)
Cat 5 cable, [114–15](#)
 Cat 5e patch cable, [116–17](#)
Cat5, [114–16](#)
 pin connection for, [115](#), [486](#)

CDMA2000, [501](#)
Cellular technologies, [500–01](#)
Cellular telephone, [7](#), [500](#)
Central authentication, [385](#)
Central distribution facility (CDF), [246](#)
Centralized routing, [167](#)
Certificate, [385](#)
Certificate authority (CA), [381](#)
Chambers, John, [4](#)
Channel service unit (CSU), [273](#)
Channels, [82](#), [202](#), [221](#)
Character, in coding, [95](#)
Charge-back policies, [470](#)
Chassis switch, [249](#)
Checksum technique, [127](#)
Ciphertext, [375](#)
Circuit loading, [419](#), [428](#)
Circuits, [7](#), [13](#), [78–87](#)
 analog, [78](#)
 capacity of, [104](#)
 configuration, [79–80](#)
 data flow, [80–81](#)
 dedicated, [79](#)
 designing, [445–46](#)
 digital, [78](#)
 DSL transmission of data, [87](#)
 logical, [78](#)
 multiplexing, [81–87](#)
 multipoint, [80](#)
 network, [428–30](#)
 permanent virtual, [282](#)
 physical, [78](#)

point-to-point, [79–80](#)
shared, [80](#)
simplex, [80–81](#)
switched virtual, [282](#)
virtual, [281](#)

Circuit-switched networks, [271–73](#)
basic architecture, [271–72](#)
integrated services digital network (ISDN), [272–73](#)
plain old telephone service (POTS), [272](#)

Circuit-switched services, [271](#)

Cisco telepresence, [62, 64](#)

Classes of service, [156](#)

Classless addressing, [159](#)

Clear to transmit (CTS), [215](#)

Client-based architectures, [40, 42–43](#)

Clients, [12](#)
client-based architectures, [40, 42–43](#)
protection, [369–74](#)

Client-server architectures, [40, 43–47](#)
n-tier, [45–46](#)
thick-client approach, [46](#)
thin-client approach, [46](#)
three-tier, [44](#)
two-tier, [44](#)

Client-server computing, [8](#)

Closed source software, [372](#)

Closed source software, open source *versus*, [372](#)

Cloud architecture, [271](#)

Cloud computing, [47–48, 271–72](#)
Gmail, [48](#)
green computing, [48](#)
server virtualization, [48](#)

Clusters, [41](#), [431](#)
Coaxial cable, [89](#)
Code Division Multiple Access (CDMA), [500](#)
Codecs, [78](#)
Coding, [95–96](#)
Coding scheme, [95–97](#)
 byte, [96](#)
 character, [95](#)
Collapsed backbones, [421](#)
Collision, [211](#)
 collision detection (CD), [211](#)
Comfort noise, [498](#)
Committed information rate (CIR), [282](#)
Common carriers, [7](#), [270](#)
Common Management Interface Protocol (CMIP), [427](#)
Common Messaging Calls (CMC), [54](#)
Common Object Request Broker Architecture (CORBA), [44](#)
Communication media, [88–95](#)
 coaxial cable, [89](#)
 fiber-optic cable, [89–91](#)
 guided media, [88](#)
 media selection, [94–95](#)
 guided media, [94](#)
 network type, [94](#)
 radiated media, [94](#)
 twisted-pair cable, [88–89](#)
 wireless media, [88](#)
Communication services, [88](#)
Communications
 during Desert Shield/Desert Storm, [10](#)
 history of, in North America, [5–7](#)
Compressed Real Time Protocol (CRTP), [498](#)

Computer Emergency Response Team (CERT), [340](#)
Computer forensics, [389](#)
Confidentiality, [342](#)
Configuration, circuit, [79–80](#)
Configuration management, [454–56](#)
 desktop management, [454](#)
 documenting, [454–56](#)
 network and client computers, configuring, [454](#)
Connectionless messaging, [155–56](#)
Connection-oriented messaging, [155–56](#)
Connector cables, [482–93](#)
 data signaling/synchronization, [487–88](#)
 Ethernet and RJ45, [488–92](#)
 firewire, [492](#)
 null modem cable connections, [485–87](#)
 RS232 cable standard, [482–85](#)
 universal serial bus, [491–92](#)
Console port, [172](#)
Content caching, [433–34](#)
 at Olympic Games, [436](#)
Content delivery, [434–36](#)
 provider, [435](#)
Content engine, [433](#)
Contention, [119, 121](#)
Contention-based CSMA/CD approach, [213](#)
Continuous ARQ, [128–29](#)
Continuous data protection (CDP), [359](#)
Control
 documenting, [349–50](#)
 identifying, [349–50](#)
Control field, [133–35](#)
Control signals, [80](#)

Control spreadsheet, [345–49](#)
 assets, [346–47](#)
 threats, [347–49](#)

Controlled access, [121–22](#), [215](#)

Controls, network, [342–73](#)
 basic principles of secure network, [341–45](#)
 control spreadsheet, [345–49](#)
 corrective, [344–45](#)
 detective, [343–44](#)
 identification and documentation of, [349–50](#)
 preventive, [343](#)

Convergence, [27](#)
 in Maryland, [28](#)

Copyright law, [53](#)

Core BN layer, [244](#)

Core layer, [244](#), [414](#)
 of backbone network, [244](#)
 of network, [244](#)

Corrective controls, [344](#)

Corrupted data, [123](#)

Cost assessment
 in building-block network design process, [412](#), [421–24](#)
 circuit costs, [421](#)
 deliverables, [423–24](#)
 request for proposal (RFP), [422](#)
 selling proposal to management, [422–23](#)

Cost management, [467–72](#)
 application software, [468](#)
 charge-back policies, [470](#)
 client hardware, [468](#)
 end user support, [468](#)
 network cost of ownership (NCO), [469](#)

network operations, [468](#)
reducing costs, [470–72](#)
 by automation, [472](#)
 by centralizing help desks, [472](#)
 by developing standards, [470–71](#)
 by reducing installation cost, [472](#)
 thin-client architectures, [472](#)
sources of costs, [467–70](#)
total cost of ownership (TCO), [469](#)

Costs

media selection and, [94–95](#)
networking, [472](#)
reducing, [470–72](#)
sources, [467–70](#)

Crackers, [362](#)

Credit card data theft, [340](#)
Cross-talk, [124](#)
Cryptography, [374](#)
Customer premises equipment (CPE), [87, 318](#)
Cut through switching, [210](#)
Cyclical redundancy check (CRC), [127–28](#)

D

Data
 corrupted, [123](#)
 credit card theft, [340](#)
 destruction of, [342](#)
 disruptions in, [342](#)
 efficiency of, [126](#)
 integration with voice and video, [27–28](#)
 lost, [123](#)
Data access logic, [40](#)

Data between the terminal (DTE), [482](#)
Data circuit terminating equipment (DCE), [482](#)
Data communications, [2–30](#)
 future trends in, [26–27](#)
 integration with voice, [27–28](#)
Data communications networks, [11–15](#)
Data compression, [104](#)
Data Encryption Standard (DES), [377](#)
 Triple, [377](#)
Data flow, [80–81](#)
 full-duplex transmission, [81](#)
 half-duplex transmission, [80–81](#)
 simplex transmission, [80–81](#)
 turnaround time, [81](#)
Data flow diagram (DFD), [208](#)
Data flow, in circuits, [80–81](#)
Data link layer, [119–45](#), [508–10](#)
 address, [158](#)
 address resolution, [164](#)
 internet model, [18](#)
 logical link control (LLC) sublayer, [120](#)
 media access control (MAC) sublayer, [120–22](#). *See also individual entry*
 message transmission using, [21](#)
 OSI model, [16](#)
Data link protocols, [131–36](#)
 asynchronous transmission, [132–33](#)
 point-to-point protocol (PPP), [135–36](#)
 synchronous transmission, [133–36](#)
Data over Cable Service Interface Specification (DOCSIS), [320](#)
Data rate, [104](#)
Data service unit (DSU), [273](#)
Data set, [487](#)

ready, [487](#)
Data signaling/synchronization, [487–88](#)
 carrier detect, [488](#)
 data terminal ready, [488](#)
 request to send and clear to send signals, [488](#)
 transmit data pins, [488](#)
Data storage, [40](#)
Data synchronization, [487–88](#)
Data terminal equipment (DTE), [482](#)
Data terminal ready, [488](#)
Data transmission
 DSL and, [87](#)
 full-duplex, [81](#)
 half-duplex, [80](#)
 simplex, [80–81](#)
Database servers, [47, 199, 207](#)
Datagram, [281](#)
DDoS agent, [352](#)
DDoS handler, [352](#)
De facto standards, [22–23](#)
De jure standards, [22–23](#)
 acceptance stage, [23](#)
 identification of choices stage, [23](#)
 specification stage, [23](#)
Decryption, [374](#)
Dedicated circuits, [79](#)
Dedicated-circuit networks, [273–79](#)
 basic architecture, [273–78](#)
 distributed star architecture, [274](#)
 dedicated-circuit services, [278](#)
 mesh architecture, [276](#)
 ring architecture, [274](#)

star architecture, [275](#)
T carrier services, [278–79](#)
Dedicated-circuit services, [269](#)
Dedicated-server LANs, [199–200](#)
Dedicated server networks, [199–200](#)
Deep Space Communications Centers (DSCCs), [85](#)
Deliverables
 cost assessment, [423–24](#)
 needs analysis and, [417–18](#)
 technology design, [420–21](#)
Delphi team, [350](#)
Demilitarized zone (DMZ), [366](#)
Denial-of-service attack (DoS), [352](#)
 inside, [355](#)
Denial-of-service (DoS) attack, [352–55](#)
 DDoS agent, [352](#)
 DDoS handler, [352](#)
 distributed, [353](#)
Denial-of-service protection, [352–55](#)
Dense WDM (DWDM), [85](#)
Design, network, [408–39](#)
Designated port, [495](#)
Designated router, [169](#)
Desirable requirements, [417](#)
Desktop management, [391, 454](#)
Desktop videoconferencing, [61–62](#)
Destination box, [508](#)
Destination port address, [153](#)
Destruction, of data, [342](#)
Detection
 anomaly, [387](#)
 error, [126](#)

misuse, [387](#)

Detective controls, [343](#)

Device failure protection, [356–57](#)

Device management software, [424](#)

Device memory, [430–31](#)

Device performance, improving, [260](#)

Devices, managed, [424](#), [459](#)

Digital circuit, [78](#)

Digital data, [78](#)

- analog transmission, [100–01](#)
- digital transmission of, [98–99](#)
- translating from analog, [105–06](#)

Digital signatures, [378](#)

Digital subscriber line (DSL), [87](#), [318–20](#)

- access multiplexer, [319](#)
- architecture, [318–19](#)
- asymmetric, [319](#)
- asymmetric DSL (ADSL), [319](#)
- data transmission, [318](#)
- modem, [318](#)
- types of, [319–20](#)

Digital transmission, [98–99](#)

Digital transmission of analog data, [105–08](#)

- adaptive differential pulse code modulation (ADPCM), [108](#)
- voice data transmission
 - by instant messenger, [108](#)
 - by telephones, [106–08](#)

voice over internet protocol (VoIP), [108](#)

Digital transmission of digital data, [95–100](#)

- coding scheme, [95–97](#)
- double current signaling, [98](#)
- ethernet transmitting data, [99–100](#)

Manchester encoding, [100](#)
polarity, [97](#)
transmission modes, [97–98](#)
Unicode, [96](#)

Direct current (DC), [97](#)

Directional antennas, [205](#)

Directory service, [206](#)

Disaster protection, [357–61](#)
 avoiding disaster, [357](#)
 backup controls, [358](#)
 business continuity plan, [358](#)
 continuous data protection
 (CDP), [359](#)
 disaster recovery, [358](#)
 disaster recovery drill, [360](#)
 disaster recovery outsourcing, [360](#)
 disaster recovery plan, [358–59](#)
 online backup, [360](#)
 recovery controls, [358](#)

Disaster recovery, [358–60](#)
 drill, [360](#)
 example of, [358](#)
 outsourcing, [360–61](#)

Disaster recovery plan, [358](#)
 elements of, [359](#)

Disasters, [342](#)

Discard eligible (DE), [282](#)

Discarding port, [495](#)

Disk mirroring, [357](#)

Disruptions, [342](#)

Distance vector dynamic routing, [167](#)

Distortion, [123](#)

harmonic, [125](#)
Distributed Computing Environment (DCE), [44](#)
Distributed computing model, [46](#)
Distributed coordination function (DCF), [214](#)
Distributed denial-of-service attack (DDoS), [352](#)
 agent, [352](#)
 distributed, [352](#)
 handler, [352](#)
Distributed star architecture, [274](#)
Distribution BN layer, [244](#)
Distribution hub, [321](#)
Distribution layer, [244](#)
 of backbone network, [243–44](#)
 of network, [243](#)
Distribution list, [53](#)
Documentation, network, [454–56](#)
Domain account, [513](#)
Domain controllers, [206](#)
Domain Name Server (DNS), [163](#)
 cache, [191–93](#)
 recursion attacks, [355](#)
Domain names, [11](#), [159](#)
 registering, [325](#)
Double current signaling, [98](#)
Downtime, [462](#)
DSL access multiplexer (DSLAM), [319](#)
Dumb terminals, [41](#)
Dynamic addressing, [161–62](#)
Dynamic Host Configuration Protocol (DHCP), [156](#), [161](#)
Dynamic routing, [167–68](#)
 distance vector, [167](#)
 link state, [167](#)

E

Eavesdropping, [368](#)

Echoes, [124](#)

Edison, Thomas, [5](#), [22](#)

Efficiency, of data, [126](#)

802.11a Wi-Fi, [213](#), [216](#)

802.11b Wi-Fi, [216](#)

802.11g Wi-Fi, [216](#)

802.11i Wi-Fi, [217](#)

802.11n Wi-Fi, [216](#)

802.11n wireless LANs, [30](#)

Electrical current, [97](#)

Electronic mail (email), [53](#)–[58](#)

 distribution list, [53](#)

 Internet Message Access Protocol (IMAP), [54](#)

 mail transfer agent, [54](#)

 mail user agent, [54](#)

 Post Office Protocol (POP), [54](#)

 three-tier thin client-server architecture, [56](#)

 two-tier email architecture, [54](#)

 web-based email, [56](#)

 working, [54](#)–[57](#)

Electronic software distribution (ESD), [454](#)

Electronics Industries Association (EIA), [482](#)

Encapsulating Security Payload (ESP), [289](#), [382](#)

Encapsulation, [21](#)

Encoding

 Lempel-Ziv, [104](#)

 Manchester, [100](#), [490](#)

Encryption, [374](#)–[82](#)

 asymmetric encryption, [375](#)

authentication, [378–81](#)
brute-force attacks, [376](#)
digital signatures, [378](#)
encryption software, [381–382](#)
key management, [376](#)
single key encryption, [375–77](#)
 algorithm, [375](#)
 key, [375](#)
symmetric encryption, [375](#)
triple DES (3DES), [377](#)
End user support, [466–67](#)
 problem resolution, [466](#)
 training for, [467](#)
Energy Sciences Network, [291](#)
Enhanced Data GSM Environment (EDGE), [501](#)
Enhanced Interior Gateway Routing Protocol (EIGRP), [169](#)
Enterprise network, [240](#)
Entity relation diagram (ERD), [208](#)
Entrapment techniques, [389](#)
Error box, [508](#)
Error control, [123–31](#)
 burst error, [123](#)
 corrupted data, [123](#)
 error detection, [126–28](#)
 error prevention, [125–6](#)
 lost data, [123](#)
 sources of errors, [123–25](#)
Error correction via retransmission, [128–30](#)
Error detection, [126–28](#)
 checksum technique, [127](#)
 cyclical redundancy check, [127–28](#)
 parity checking, [126–27](#)

Error prevention

 moving cables, [125](#)

 shielding, [125](#)

Error rates, [123](#)

 media selection and, [95](#)

Errors

 burst, [123](#)

 human, [123](#)

 minimizing, [124](#)

 network, [123](#)

 sources of, [123–25](#)

Ethernet, [134–35](#). *See also* Wired Ethernet; Wireless Ethernet

 1 GbE, [212](#)

 100Base-T, [212](#)

 10Base-T, [212](#)

 data transmission by, [99–100](#)

 error control in, [224](#)

 gigabit, [15](#), [213](#)

 in home, [352](#)

 Manchester encoding, [100](#)

 media access control, [211–12](#)

 RJ45 and, [488–91](#)

 services, [284–85](#)

 shared, [208](#)

 switched, [219](#)

 topology, [208](#), [213](#)

 traditional, [208](#), [214](#)

 types of, [212](#)

European Particle Physics Laboratory (CERN), [49](#)

Even parity, [127](#)

Extensible Authentication Protocol (EAP), [217](#)

Exterior routing protocols, [168](#)

Extranet VPN, [287](#)

Extranets, [15](#)

F

Failure control function, [459–62](#)

Failure statistics, [462–64](#)

Fake antivirus, [370](#)

Fast packet services, [286](#)

Fat-client approach. *See* Thick-client approach

Fault management, [456–66](#)

- failure control function, [459–62](#)

- network monitoring, [456–59](#)

- performance and failure statistics, [462–64](#)

Fault-tolerant servers, [357](#)

Fax services, [6](#)

Federal Communications Commission (FCC), [6, 270](#)

Fiber channel, [207](#)

Fiber to the home (FTTH), [27, 322–23](#)

- architecture, [322](#)

- types, [322](#)

Fiber-optic cable, [89–91, 201](#)

- microwave transmission, [92–93](#)

- radio, [91](#)

- satellite transmission, [93–94](#)

- single-mode, [90](#)

Fiber-to-the-home (FTTH), [329](#)

Fields

- address, [133](#)

- control, [133, 134](#)

- frame check sequence, [134](#)

- message, [134](#)

File servers, [12, 200](#)

File sharing, managing, [518–24](#)
 creating shared folder, [519–20](#)
 defining security, [521–24](#)
 enabling sharing, [520–21](#)

File Transfer Protocol (FTP), [39](#)

Final Destination, [507](#)

Finger of Death attacks, [355](#)

Firefighting, [450](#)

Firewalls, [362–69](#)
 application-level firewall, [365](#)
 architecture, [366](#)
 packet-level firewall, [364](#)

Firewire, [492](#)

Firewire cables, [492](#)

First router (R1), [165](#)

Fixed wireless, [323–24](#)

Flag, [133](#)

Flow control, [129](#)

Formal language, [19](#)

Formal standards, [22](#)

40 GbE, [212](#)

Forward error correction, [130–31](#)

Forward Ethernet switching, [211](#)

Forwarding equivalence classes (FEC), [259](#)

Forwarding table, [210](#)

4G wireless services, [501](#)

Four-way handshake, [156](#)

Fractional T1 circuit (FT1), [278](#)

Fragment-free Ethernet switching, [211](#)

Fragment-free switching, [211](#)

Frame check sequence field, [134](#)

Frame relay, [283–86](#)

in California, [311](#)
Frames, [132](#), [138](#)
Free speech, Internet and, [53](#)
Frequency, [100](#)
Frequency division multiplexing (FDM), [82](#)–[84](#), [87](#)
Frequency modulation (FM), [101](#)
Frequency shift keying (FSK), [101](#)
Full-duplex transmission, [81](#)
Full-mesh architecture, [276](#)
Future trends, [26](#)–[29](#)
pervasive networking, [26](#)–[27](#)

G

G.Lite ADSL, [87](#)
Gartner Group, Inc., [469](#)
Gateways, [181](#), [242](#)–[43](#)
building TCP/IP, [243](#)
VPN, [286](#)–[92](#)
Gaussian noise. *See* White noise
Gbps, [27](#)
Geographic scope, of network, [414](#)–[15](#)
Geosynchronous satellites, [93](#)
Gigabit Ethernet, [295](#), [491](#)
Gigabits per second, [15](#)
Gigapops, [325](#)
Pacific/Northwest, [326](#)
Global System for Mobile Communication (GSM), [500](#)
Gmail, [48](#)
Go-Back-N ARQ, [128](#)
Green computing, [48](#)
Green IT, [436](#)–[37](#)
Ground communication network at NASA, [85](#)

Guardbands, [82–83](#)
Guided media, [88–95](#)
 coaxial cable, [89](#)
 fiber-optic cable, [88–91](#)
 twisted-pair cable, [88–89](#)

H

H.320 standard, [62](#)
H.323 standard, [62](#)
Hackers, [362](#)
Half-duplex transmission, [80–81](#)
Hamming code, [130](#)
Hardware
 improving performance, [225–26](#)
 layers, [19](#)
 life spans of, [411](#)
Header, of SMTP packet, [57](#)
Health Insurance Portability and Accountability Act (HIPAA), [340](#)
Help desk, [459](#)
Hertz (Hz), [98](#)
Hidden node problem, [214](#)
Hierarchical backbones, [250](#)
High-level data link control (HDLC), [134](#)
High-speed serial interface (HSSI), [484](#)
Hi-Speed USB, [491](#)
Honey pot, [389](#)
Hops, [167, 286](#)
Host computer, [40](#)
Host-based IPS, [387](#)
Hotmail, [56](#)
HTTP request, [50](#)
 example of, [51](#)

- inside, [50–51](#)
- HTTP response, [50](#)
 - example of, [52](#)
 - inside, [51–53](#)
- HTTP Viewer, [68](#)
- Hub polling, [122](#)
- Hub-based Ethernet, [208](#)
- Hubs, [203–05](#)
- Human errors, [123](#)
- Hurricane Katrina, recovering from, [358](#)
- Hybrid fiber coax (HFC), [320](#)
- Hypertext Markup Language (HTML), [53](#)
- Hypertext networks, [49](#)
- Hypertext Transfer Protocol (HTTP), [50](#)
 - HTTP request, [50–51](#)
 - request body, [51](#)
 - request header, [51](#)
 - request line, [50](#)
 - HTTP response, [50–53](#)
 - response body, [51](#)
 - response header, [51](#)

I

- ICANN (Internet Corporation for Assigned Names and Numbers), [159](#)
- ICMP attacks, [355](#)
- Identification of choices stage, of standardization process, [23](#)
- Idle signal, [132](#)
- IEEE 802.11a standard, [216](#)
- IEEE 802.15 standard, [242](#)
- IEEE 802.1D standard, [494](#)
- IEEE 802.1q standard, [254](#)
- IEEE 802.1w standard, [495](#)

IEEE 802.3ac standard, [134](#)
Impulse noise, [124](#)
 source of, [124](#)
Incoming messages accepting, [506–09](#)
Information bits, [136](#)
Information frame, [134](#)
Information lag, [4](#)
Information services, new, [28–29](#)
Information sharing, [198](#)
 Information sharing through LANs, [198](#)
Information systems, history of, [7–9](#)
 1950s, [8](#)
 1970s, [8](#)
 1980s, [8](#)
Information utilities, [29](#)
Information warfare, [362, 392](#)
Instant messaging (IM), [60–61](#)
Instant messenger, [108](#)
Institute of Electrical and Electronics Engineers (IEEE), standard-making process and, [23](#)
Integrated services digital network (ISDN), [272](#)
 basic rate interface, [273](#)
 narrowband, [272](#)
 primary rate interface, [273](#)
Integration of voice, video, and data, [27–28](#)
Integrity, [342](#)
Interchange carriers (IXC), [6, 270](#)
Interface, routing, [165](#)
Interior Gateway Routing Protocol (IGRP), [171](#)
Interior routing protocols, [168](#)
Intermediate System to Intermediate System (IS-IS), [169–70](#)
Intermodulation noise, [125](#)

International Organization for Standardization (ISO), [16](#)
standard-making process and, [23](#)

International Telecommunications Union-Telecommunications Group (ITU-T), standard-making process and, [23](#)

Internet, [311–64](#)
applications used on, [40](#)
basic architecture, [312–14](#)
connecting to ISP, [314–16](#)
contemporary, [342–43](#)
domain names, [11](#)
free speech and, [53](#)
functioning of, [338–43](#)
governance, [324–25](#)
history of, [9–11](#)
integration of, [474–75](#)

Internet access technologies, [317–23](#)
cable modems, [320–22](#)
DSL, [318–20](#)

Internet addresses, [159](#)
classes, [159](#)

Internet Architecture Board (IAB), [324](#)

Internet Control Message Protocol (ICMP), [168–69](#)

Internet Corporation for Assigned Names and Numbers (ICANN), [159, 325](#)

Internet domain names, [11](#)

Internet Engineering Steering Group (IESG), [324, 325](#)

Internet Engineering Task Force (IETF), [24, 324](#)
management focus on, [24](#)
standard-making process and, [24](#)

Internet Exchange Points (IXPs), [314](#)

Internet Explorer, [12, 17, 49, 51, 145, 154](#)

Internet Group Management Protocol (IGMP), [172](#)

Internet Key Exchange (IKE), [381](#)

Internet Message Access Protocol (IMAP), 54–57

Internet model, 18–19

- application layer, 19

- data link layer, 18

- hardware layers, 19

- internetwork layer, 19

- network layer, 18

- physical layer, 18

- transport layer, 18

Internet Protocol (IP), 151–52

- spoofing, 365

Internet Research Task Force (IRTF), 324, 325

Internet Service Provider (ISP), 4, 286, 289, 311–36

- basic architecture, 313

- cable modems, 322

- fiber to the home (FTTH), 322–23

- internet today, 316–17

- national ISPs/tier 1 ISPs, 314

- optical unit network (ONU), 322

Internet Society (ISOC), 324

Internet video, at Reuters, 29

Internet2, weather map, 460, 461

Internetwork layer, 19

Internetwork Operating Systems (IOS), Cisco, 173

Interstate Commerce Commission (ICC), 6

Intranet VPN, 287

Intranets, 15

Intrusion, 342

- recovery, 388–90

Intrusion prevention, 361–88

- perimeter security and firewalls, 362–69

- security policy, 362

Intrusion prevention systems (IPS), 387–88

anomaly detection, 387

casual intruders, 361

crackers, 362

hackers, 362

host-based IPS, 387

management console, 387

misuse detection, 387

network-based IPS, 387

Intrusion recovery, 388–90

Inverse multiplexing (IMUX), 85–86

IP Security Protocol (IPSec), 381

IP spoofing, 365

IP telephony, 497–99

IP version 4 (IPv4), 151

IPS management console, 387

IPS sensor, 387

IPSec, 287, 381

IPSec transport mode, 382

IPSec tunnel mode, 382

ISO8859, 96

J

Jet Propulsion Laboratory (JPL), 85

K

Kbps, 15

Kerberos, 385–86

Kerckhoffs, Auguste, 372

Key, 375, 452

management, 376

private, 378

public, [378](#)
Knoppix, [369](#)

L

L2TP, [286](#)
Label Switched Routers (LSRs), [259](#)
LAN metering software, [198](#)
Latency, [210](#), [294](#), [430](#)
Layer address
 application, [157](#)
 data link, [158](#)
 network, [157](#)
Layer-2 switches, [210](#), [240](#)
Layer-2 tunneling protocol (L2TP), [286](#)
Layer-2 VPN, [286](#)
 tunneling protocol, [286](#)
Layer-3 switches, [243](#)
Layer-3 VPN, [286](#)
Layers, [18](#)–[22](#). *See also* Message transmission using layers pros and cons of using, [21](#)
Lempel-Ziv encoding, [104](#)
Lightweight directory services (LDAP), [207](#)
Line noise, [123](#)
Line splitter, [318](#)
Link Access Protocol for Modems (LAP-M), [128](#)
Link Access Protocol-Balanced (LAP-B), [134](#)
Link state dynamic routing, [167](#)
Linux, [30](#), [49](#), [59](#), [132](#), [199](#), [206](#), [371](#), [432](#)
Load balancing, [431](#)–[2](#)
 at Bryam Healthcare, [435](#)
 server, [431](#)
 switch, [431](#)

Local account, 513

Local area networks (LANs), 12–15, 198–237. *See also* Wired LANs; Wireless LANs

components, 201–13

dedicated-server, 199–200

design practice, 218–23

file servers, 200

improving LAN performance, 223–27

circuit capacity, 226

reducing network demand, 226–27

server performance, 224–26

LAN metering software, 198

peer-to-peer LANs, 199–200

print servers, 200

usage reasons, 198–99

information sharing, 198

resource sharing, 198

Local exchange carriers (LEC), 6, 270

Local loop, 107, 318

Logical circuit, 78

Logical link control (LLC) sublayer, 120

Logical network design, 414

Logical network parameters, 458–59

Logical topology, 208

Long-distance telephone, 6

Lost data, 123

Low earth orbit (LEO) satellites, 93

M

MAC address filtering, 217

Macintosh, 49

Mail transfer agent, 54

Mail user agent, 54

Main distribution facility (MDF), 246, 344
network diagram, 248

Mainframe, 41

Managed devices, 424, 459

Managed networks, 424–54
policy-based management, 427–28
software, 424–26
standards, 426–27

Management console, IPS, 387

Management implications, application layer, 63–64

Management information base (MIB), 427

Management reports, 461, 464

Management, implications for, 29–30
backbone networks and, 261
data transmission and, 109
Internet and, 328
local area networks and, 227
MANs and WANs, 261
network design and, 427–38
network management and, 472–73
network security and, 391–92
networking environment and, 29–30
networks and, 63
protocol and, 139
TCP/IP and, 182
WLAN and, 227

Management, network, 449–73

Manager
network, 59, 450
network policy, 407
network security, 391

Manchester encoding, [100](#), [490](#)
Mandatory requirements, [417](#)
Master, [217](#)
Maximum allowable rate (MAR), [282](#)
Mbps, [27](#)
MCI, [6](#)
Mean Opinion Score (MOS), [498](#)
Mean time between failures (MTBF), [462](#)
Mean time to diagnose (MTTD), [462](#)
Mean time to fix (MTTF), [463](#)
Mean time to repair (MTTR), [462](#)
Mean time to respond (MTTR), [463](#)
Media access control (MAC), [120–21](#), [211–12](#)
 Bluetooth and, [226](#)
 contention, [121](#)
 controlled access, [121–22](#)
 distributed coordination function, [214](#)
 Ethernet and, [211–12](#)
 point coordination function, [214–15](#)
 relative performance, [122](#)
 sublayer, [120](#)
 switched Ethernet and, [219](#)
 Wi-Fi and, [213–18](#)
 WiMAX and, [323](#)
Media communication, [88–95](#)
 guided, [88](#)
 selection, [94–95](#)
 wireless, [88](#)
Media Gateway Control Protocol (MGCP), [497](#)
Media selection
 cost and, [95](#)
 error rates and, [95](#)

network types, 94
transmission distance and, 95
transmission speeds and, 95

Memory, device, 430

Mesh architecture, 274, 276
full-mesh architecture, 276
partial-mesh architecture, 276

Message box, 505

Message field, 134

Message Number box, 508

Message transmission using layers, 19–22, 149
application layer, 19
common standards, 24–25
data link layer, 21
network layer, 20
physical layer, 21
protocol, 19
transport layer, 20

Messages from the Network Layer, 508

Messages from the Physical Layer pile, 509

Messaging
connectionless, 156
connection-oriented, 155–56

Metcalfe, Bob, 134

Metropolitan area exchange (MAE), 313

Metropolitan area networks (MAN), 12–15
best practice design, 318–20
of Cisco Systems Inc., 290
improving performance, 294–97
relationship to other networks, 14

Microcomputer, explosion in, 450

Microsoft Outlook, 57

Microsoft Windows Server, [199](#)
Microwave tower, [92](#)
Microwave transmission, [92–93](#)
Middleware, [44](#)
Middleware problem, [44](#)
Mini-cases
 ABC Warehouse, [232](#)
 Accurate Accounting, [67](#), [442](#)
 AdviceNet, [442](#)
 Amalgamated Stores, [113](#)
 Asia Importers, [34](#)
 Atlas Advertising, [33](#)
 Belmont State Bank, [395](#)
 Big E. Bank, [32–34](#)
 Boyle Transportation, [114](#)
 CareGroup, [300](#)
 Cathy's Collectibles, [332](#)
 Central Textiles, [476](#)
 Central University, [185](#)
 CISCO Systems Inc., [301](#)
 City School District, [476](#)
 Classic Catalog Company, [396](#)
 Computer Dynamics, [441](#)
 Connectus, [185](#)
 Consolidated Supplies, [33](#)
 Cookies Are Us, [300](#), [332](#)
 Deals-R-Us Brokers, [66–7](#)
 Drop and Forge, [441](#)
 Energy Sciences Network, [301](#)
 Ethernet, designing, [230](#)
 Eureka!, [113](#), [231](#)
 fire departments, [301](#)

Fred's Donuts, [185](#)
General Hospital, [255](#)
General Stores, [187](#)
Global Consultants, [33](#)
Hospitality Hotel, [262](#)
Household Wireless, [231](#)
Internet2, [476](#)
Ling Galleries, [67](#)
Mary's Manufacturing, [442](#)
Mega Investments, [34](#)
MegaCorp, [300](#)
Metro Motel, [232](#)
NASA's Ground Network, [114](#)
Old Army, [187](#)
Organic Foods, [332](#)
Pat's Engineering Works, [263](#)
Pat's Petunias, [230–31](#)
personal security, [396](#)
Sally's Shoes, [231](#)
Salt Lake City Olympics, [442](#)
South West State University, [231](#)
Speedy Package, [114](#)
Sunrise Consultancy, [300](#)
Surfing Sam, [332](#)
SURFnet, [301](#)
Tom's Home Automation, [231](#)
Ubiquitous Offices, [232](#)
Western Bank, [395](#)
Western Trucking, [264](#)
Mission-critical application, [347](#)
Misuse detection, [387](#)
Mobile wireless, [323](#)

Modems, [78](#), [104](#)
cable, [320–22](#)
data transmission by, [104](#)
defined, [105](#)
DSL, [318](#)

Modulation, [100–03](#)
adaptive differential pulse code, [108](#)
amplitude, [101](#)
basic, [101–02](#)
bit rate *versus* baud rate *versus* symbol rate, [103](#)
frequency, [101](#)
phase, [102](#)
pulse amplitude, [107](#), [491](#)
pulse code, [107](#)
quadrature amplitude, [103](#)
sending multiples bits simultaneously, [102–03](#)

Modules, [249](#)

Monitoring, network, [456–59](#)

Monopoly, [7](#)

Morse, Samuel, [5](#)

Mosaic browser, [49](#)

MoSucker Trojan horse, [373](#)

MPEG-2 standard, [63](#)

Multicast message, [171](#)

Multicasting, [171–72](#)
broadcast message, [171](#)
unicast message, [171](#)

Multi-Level Transmission-3 Level (MLT-3), [490](#)

Multimode fiber-optic systems, [89](#)

Multiplexing, [81–87](#)
BONDING (Bandwidth on Demand Interoperability Networking Group),
[86–87](#)

frequency division multiplexing (FDM), 82–83
inverse multiplexing (IMUX), 85–86
statistical time division multiplexing (STDM), 83–84
time division multiplexing (TDM), 83
wavelength division multiplexing (WDM), 84–85
Multipoint circuit, 80
Multiprotocol label switching (MPLS), 259, 282, 285–86
Multiprotocol routers, 259
Multipurpose Internet Mail Extension (MIME), attachments in, 58
Multiswitch VLAN, 254

N

Name servers, 163
Nanoseconds, 490
Narrowband ISDN, 272
NASA, ground communication, network of, 85
National Center for Supercomputing Applications (NCSA), 49
National Science Foundation, 9
Needs analysis
 in building-block network design process, 412–18
 access layer, 414
 application systems, 415–16
 categorizing needs, 417
 core layer, 414
 deliverables, 417–18
 desirable requirements, 417
 distribution layer, 415
 geographic scope, 414–15
 mandatory requirements, 417
 network users, 416
 wish-list requirements, 417
Negative acknowledgment (NAK), 128

Net neutrality, [10](#)
NetEqualizer, [432](#)
Network
 cables, [12](#)
 circuit, [12](#)
 file server, [12](#)
 future trends, [26–29](#)
 models, [15–22](#)
 peer-to-peer networks, [12](#)
 print server, [12](#)
 router, [12](#)
 standards, [22–25](#)
 switch, [12](#)
 types of, [12–15](#)
 web server, [12](#)
Network access points (NAP), [312](#)
 inside Chicago, [316](#)
Network address translation (NAT), [365–66](#)
Network cables, [203](#)
 standards, [202](#)
Network circuits, [201–03](#), [428–30](#)
 service-level agreement (SLA), [430](#)
 traffic analysis, [428–29](#)
Network computer, [41](#)
Network cost of ownership (NCO), [469](#)
Network demand, reducing, [226–27](#), [285–86](#), [296–97](#)
Network design, [408–47](#)
 building-block network design process, [411–13](#)
 cyclical nature of network design, [413](#)
 for performance, [424–27](#)
 alarm storm, [425](#)
 application management software, [426](#)

capacity management, [432](#)
device management software, [424–25](#)
device memory, [430–31](#)
load balancing, [431–32](#)
managed networks, [424–28](#)
management software, [424](#)
minimizing network traffic, [432–36](#)
network circuits, [428–30](#)
network devices, [430–32](#)
network management standards, [426](#)
policy-based management, [427](#)
root cause analysis, [425](#)
system management software, [425](#)
virtual server, [431–32](#)
traditional process, [410–11](#)

Network devices, [430–36](#)
capacity management, [432](#)
content caching, [433–34](#)
content delivery, [434–36](#)
latency of, [430](#)
load balancing, [431–32](#)
memory, [430–31](#)
minimizing traffic, [432–33](#)

Network documentation, [454](#)

Network interface cards (NIC), [201](#)

Network interface port, [172](#)

Network layer, [148–94, 506–07](#)
address, [157](#)
internet model, [18](#)
message transmission using, [20–21](#)
OSI model, [17](#)

Network management, [449–80](#). *See also* Configuration management

failure control function, [459–62](#)
firefighting, [450](#)
improving performance, [465–66](#)
integrating LANs, WANs, and Internet, [451–52](#)
internet2 weather map, [460–61](#)
logical network parameters, [458](#)
manager job requirements, [453](#)
organizing, [450–53](#)
performance and failure statistics, [462–64](#)
physical network parameters, [458](#)
policy-based management, [465](#)
problem statistics, [461](#)
shift to Internet, [450–51](#)
shift to LANs, [450–51](#)
software, [427](#)
standards, [426](#)
voice and data communications, integrating, [452–53](#)
weather map, [459](#)

Network models, [15–22](#)
 Internet model, [18–19](#)
 message transmission using layers, [19–22](#)
 Open Systems Interconnection Reference (OSI) model, [16–18](#)

Network monitoring software, [478](#)

Network operating systems (NOS), [206–07](#)
 client software, [206–07](#)
 network profiles, [207](#)
 server software, [206](#)

Network operations center (NOC), [458, 460](#)

Network policy manager, [457](#)

Network profiles, [207](#)

Network security, [338–407](#). *See also* Encryption; Intrusion prevention; Risk assessment

device failure protection, [356–57](#)
disaster protection, [357–61](#)
ensuring business continuity, [351–61](#). *See also* Business continuity evaluating, [350–51](#)
firewalls, [362–69](#)
need for, [341–42](#)
network controls, [342–45](#)
operating systems, [371](#)
perimeter security, [362–69](#)
phishing, [387](#)
physical security, [356](#)
redundancy, [356](#)
security policy, [362](#)
security threats, types of, [342](#)
 availability, [342](#)
 business continuity, [342](#)
 confidentiality, [342](#)
 destruction of data, [342](#)
 disasters, [342](#)
 disruptions, [342](#)
 integrity, [342](#)
 intrusion, [342](#)
server and client protection, [369–74](#)
theft protection, [356](#)
Network segmentation, [226](#)
Network servers, [206](#)
Network standards, [22–26](#)
 common, [24–26](#)
 standards-making process, [22–24](#)
Network support technician, [136](#)
Network terminator (NT-1 or NT-2), [272](#)
Network traffic, minimizing, [432–36](#)

content caching, 433
content delivery, 434
content delivery provider, 435
content engine, 433
green IT, 436–37
Network users, 416
Network weather map, 459
Network-attached storage (NAS) devices, 207
Network-based IPS, 387
Networking, 8
 car, 419
 costs, 472
 expertise, demand for, 5
 passive optical, 322
 pervasive, 26–27
Networks/Networking, 8–9
 access layer, 414
 backbone, 12
 campus, 239
 circuit-switched, 271–73
 components of, 12
 core layer, 244
 dedicated server, 199–200
 dedicated-circuit, 273–78
 distribution layer, 414
 efficiency, 136
 enterprise, 240
 errors, 123
 geographic scope of, 414–15
 ground communication, 85
 hypertext, 49
 local area networks, 12

managed, [424–28](#)
metropolitan area networks, [12](#)
monitoring, [456–59](#)
overlay, [219](#)
packet-switched, [279–86](#)
peer-to-peer, [12](#), [200](#)
secure, [342](#)
types of, [12–15](#), [94](#)
users, [416](#)
wide area networks, [15](#)
New information services, [28–9](#)
Next Generation Internet (NGI), [326](#), [328](#)
Next Node, [507–08](#)
Noise
 impulse, [124](#)
 intermodulation, [125](#)
 white, [123](#)
North America
 communications in, [5–7](#)
 cellular telephone networks, [7](#)
 fax services, [6](#)
 history, [5–7](#)
 long-distance telephone, [6](#)
 picturefone service, [6](#)
 Telstar I satellite, [6](#)
 transatlantic voice connections, [6](#)
 transcontinental telephone service, [6](#)
NSFNET, [9](#), [10](#)
N-tier architecture, [45–46](#)
Null modem cable connections, [485–87](#)
pin configurations, [486](#)

O

Odd parity, [127](#)
Omnidirectional antennas, [204](#)
 1 GbE, [212](#), [495](#)
 1000Base-T, [212](#), [226](#), [249](#), [490](#)
 100Base-T, [212](#), [218](#), [490](#)
1 GbE, [490–91](#)
One-time passwords, [384](#)
1000Base-T standard, [212](#), [490](#)
100Base-T standard, [212](#), [490](#)
Online backup services, [360](#)
Open Database Connectivity (ODBC), [44](#)
Open Shortest Path First (OSPF), [169](#)
Open source software, closed, source versus, [372](#)
Open Systems Interconnection Reference (OSI) model, [16–18](#)
 application layer, [18](#)
 data link layer, [16](#)
 network layer, [17](#)
 physical layer, [16](#)
 presentation layer, [17](#)
 session layer, [17](#)
 transport layer, [17](#)
Operating systems, security, [371](#)
Operating systems, server and, client protection and, [369–74](#)
Optical unit network (ONU), [322](#)
Optical-electrical (OE) converter, [321](#)
Optix Pro Trojan horse, [373](#)
Ordered chaos, [211](#)
Outgoing messages, accepting, [506](#)
Outsourcing, disaster recovery, [360–61](#)
Overhead bits, [136](#)

Overlay networks, [219](#)

Oversampling, [105](#)

P

Packet assembly/disassembly device (PAD), [280](#)

Packet service, [284](#)

unreliable, [283](#)

Packet-level firewall, [364–65](#)

Packet-switched networks, [279–86](#)

asynchronous transfer mode, [282–83](#)

basic architecture, [280–81](#)

Ethernet services, [284–85](#)

frame relay, [283–84](#)

X.25, [484](#)

Parallel transmission, [97](#)

Parity bit, [126](#)

Parity check, [126–27](#)

Parity checking, [126](#)

even parity, [127](#)

odd parity, [127](#)

Partial-mesh architecture, [276](#)

Pass phrases, [383](#)

Passive optical networking, [322](#)

Passive scanning, [214](#)

Passphrases, [383](#)

Passwords, [383](#)

cracking, [383](#)

one-time, [384](#)

Patch, [369](#)

Patch cables, [247](#)

Pbps, [27](#)

Peering, [314](#)

Peer-to-peer (P2P) architectures, [40](#), [46–47](#)
advantages, [47](#)
scalability, [47](#)

Peer-to-peer LANs, [199–200](#)

Peer-to-peer networks, [12](#), [200](#)

Performance

designing for network, [424–63](#)
managed networks and, [424–28](#)
network circuits and, [428–30](#)
network devices and, [430–32](#)

Performance and failure statistics, [462–64](#)

Performance improvement, in satellite communications, [94](#)

Performance management, [456–66](#)
failure control function, [459–62](#)
improving performance, [465–66](#)
network monitoring, [456–59](#)
performance and failure statistics, [462–64](#)

Performance statistics, [462–64](#)

Perimeter security and firewalls, [362–69](#)
application-level firewall, [365](#)
firewall architecture, [366–68](#)
network address translation firewalls, [365–66](#)
packet-level firewalls, [391–92](#)
physical security, [367–68](#)

Perl, [56](#)

Permanent virtual circuits (PVC), [282](#)

Permissions, [518](#)

Personal computer, [41](#)

Personal digital assistants (PDA), [41](#), [500](#)

Pervasive networking, [26–27](#)

Phase, [100](#)

Phase hits, [107](#)

Phase modulation (PM), [102–03](#)
Phase shift keying (PSK), [102](#)
Phishing, [387](#)
 attack, [401](#)
Physical carrier sense method, [214](#)
Physical circuit, [78](#)
Physical layer, [77–117](#), [510–11](#). *See also* Circuits
 internet model, [18](#)
 message transmission using, [21](#)
 OSI model, [16](#)
Physical network
 design, [415](#)
 parameters, [458](#)
Physical security, [356](#), [367–69](#)
 data security and, [369](#)
Physical topology, [208](#)
Piconet, [243](#)
Picturefone service, [6](#)
Pin configurations, [486](#)
PING, [188–90](#)
Piracy, software, [199](#)
Plain old telephone service (POTS), [100](#), [272](#)
Plaintext, [374](#)
Podcasting, [181](#)
Point coordination function (PCF), [214–15](#), [323](#)
Point-to-point circuit, [79](#)
Point-to-point protocol (PPP), [135–36](#)
Points of presence (POP), [282](#), [314](#)
Polarity, [97](#)
Policy-based management, [427–28](#), [465](#)
Polling, [121](#)
 hub, [122](#)

roll-call, [121](#)
Port, [203–204](#)
 designated, [495](#)
Port address, [153](#)
 destination, [153](#)
 source, [153](#)
Post Office Protocol (POP), [54](#)
POTS (plain old telephone service), [100](#)
Power over Ethernet (POE), [204](#)
Preamble, [134](#)
Presentation layer, OSI model, [17](#)
Presentation logic, [40](#)
Pretty Good Privacy (PGP), [381](#)
Preventive controls, [343](#)
Primary access service. *See* Primary rate interface (PRI)
Primary rate interface (PRI), [273](#)
Print servers, [12](#), [200](#)
Private Branch Exchange (PBX), [497](#)
Private key, [378](#)
Private line services, [273](#)
Probe frame, [214](#)
Problem prioritizing, [461](#)
Problem statistics, [461](#)
Problem tracking, [460](#)
Propagation delay, [93](#)
Proposals, selling to management, [472–73](#)
Protocol, [19](#), [22](#), [50](#)
 data link, [131–6](#)
 exterior routing, [168](#)
 interior routing, [168](#)
 point-to-point, [135–36](#)
 routing, [168–71](#)

spanning tree, 493–96
stack, 22
Protocol Data Unit (PDU), 19, 20, 120, 149
Public key, 378
 encryption, 378
Public key infrastructure (PKI), 378, 380
Public switched telephone network (PSTN), 271, 497
Public utilities commission (PUC), 270
Public Wi-Fi, 198, 213
Pulse Amplitude Modulation (PAM), 106–07
Pulse Amplitude Modulation–5 (PAM-5), 491
Pulse code modulation (PCM), 107
PuTTY package, 59

Q

Quadrature amplitude modulation (QAM), 103
Quality control charts, 464
Quality of Service (QoS), 156–57, 499
Quantizing error, 105

R

Rack of equipment, 246
Radiated media, 94
Radio frequencies, 91–93
Radio Frequency Identification (RFID) chip, 60
Radio transmission, 91–93
Raindrop attenuation, satellite transmission and, 93
RC4, 377
RC4 encryption algorithm, 377
Real-Time Streaming Protocol (RTSP), 157
Real-Time Transport Protocol (RTP), 157
Recovery controls, 358

Redundancy, 356
Redundant array of independent disks (RAID), 226, 357
Regional Bell operating companies (RBOCs), 6
Regional ISP, 313
Relative performance, 122
Reliable packet service, 283
Remote monitoring (RMON), 427
probes, 427
Remote-access server (RAS), 314
Repeaters, 125
Replication, 163
Request body, 51
Request for Comment (RFC), 24
Request for proposal (RFP), 422
Request header, 51
Request line, 50
Request to transmit (RTS), 215
Requests for comment (RFC), 324
Requirements, network
desirable, 417
mandatory, 417
wish-list, 417
Resolution
address, 162–65. *See also* Addressing
server name, 162–65
Resolving problems, 466–67
Resource Reservation Protocol (RSVP), 157
Resource sharing through LANs, 198
Response body, 52
Response header, 52
Response status, 52
Retrain time. *See* Turnaround time

Retransmission, error correction via, [128–30](#)
Return to zero (RZ), [98](#)
Reuters, Internet video at, [29](#)
Rich Site Summary (RSS), [181](#)
Ring architecture, [274–75](#)
Ring indicator, [487](#)
Risk assessment, [345–51](#)
 assets, [346–47](#)
 control spreadsheet, developing, [345–49](#)
 identifying and documenting control, [349–50](#)
 threat, [347–48](#)
RJ–45, [488–91](#)
Roaming, [247](#)
Roll-call polling, [121](#)
Root cause analysis, [425](#)
Root node, [495](#)
Root switch, [495](#)
Rootkits, [373, 375](#)
Routed backbones, [249–52](#)
 design, [250](#)
 hierarchical backbones, [250](#)
 subnetted backbones, [250](#)
Routers, [12, 240–42](#)
 anatomy of, [172–73](#)
 auxiliary port, [172](#)
 border, [169](#)
 console port, [172](#)
 designated, [169](#)
 functions, [172](#)
 label switched, [259](#)
 multiprotocol, [259](#)
 network interface port, [172](#)

Routing, [165–73](#)
 centralized routing, [167](#)
 distance vector dynamic routing, [167](#)
 dynamic routing, [167](#)
 first router (R1), [165](#)
 interface, [165](#)
 link state dynamic routing, [167](#)
 multicasting, [171–72](#)
 protocols, [168–71](#)
 autonomous system, [168](#)
 Border Gateway Protocol (BGP), [168–69](#)
 Enhanced Interior Gateway
 Routing Protocol (EIGRP), [169](#)
 exterior routing protocols, [168](#)
 interior routing protocols, [168](#)
 Intermediate System to
 Intermediate System (IS-IS), [169](#)
 Internet Control Message Protocol (ICMP), [168–69](#)
 Open Shortest Path First (OSPF), [169–70](#)
 Routing Information Protocol (RIP), [158](#), [168](#), [170](#)
 static routing, [167](#)
 types, [167–68](#)

RS232 (DB-25)/RS449 (DB-9), [482–85](#)

RS232 cable standard, [482–85](#)

RS449 cable specifications, [482–85](#)

S

Sarbanes-Oxley Act (SOX), [340](#)

Satellite transmission, [93–94](#)

 geosynchronous, [93](#)

 improvement of performance, [94](#)

 raindrop attenuation and, [93](#)

Satellite, 93–94
Scalability, 47
Scanning, 214
Script kiddies, 344
Secure network, principles of, 342
Secure shell (SSH) encryption, 59
Secure Sockets Layer (SSL), 381
Secure switch, 369
Security
 media selection and, 94
 network, 338–92
Security account manager (SAM), 383
Security holes, 362, 369
 exploiting, 371
Security policy, 390
 elements of, 391
Security, network. *See* Network security
Segment, 149
Segmenting, 154–55
Sequence number, 506
Serial transmission, 97
Server, 12, 41
 server farms, 199, 431
 server name resolution, 162
 server protection, 369–74
 server virtualization, 48–49, 431–32
 web, 50
Server and client protection, 369–74
 encryption, 374–82
 operating systems, 371–73
 security holes, 369–70
Trojan horses, 373–74

Server farm, [29](#), [199](#)
Server load balancing, [431](#)
Servers, [12](#)
 authentication, [385](#)
 clusters, [431](#)
 database, [207](#)
 farms, [199](#)
 fault-tolerant, [357](#)
 file, [12](#), [200](#)
 as honey pot, [389](#)
 improving performance, [224–26](#)
 print, [12](#), [200](#)
 remote-access, [314](#)
 software for, [206](#)
 technology design, [412](#), [418–21](#)
 terminology for, [159](#)
 virtual, [41](#), [431](#)
Web, [12](#)
Windows, [513–24](#)
 wireless telephony application, [350](#)
Service profile identifier (SPID), [273](#)
Service-level agreement (SLA), [430](#), [465](#)
Session Initiation Protocol (SIP), [497](#)
Session layer, OSI model, [17](#)
Session management, [155–57](#)
 connectionless messaging, [155](#)
 connection-oriented messaging, [155–56](#)
 four-way handshake, [156](#)
 Quality of Service (QoS), [156](#)
 three-way handshake, [155](#)
Shared circuit, [80](#)
Shared Ethernet, [208](#)

Shared folder, creating, [519](#)
Shielded twisted pair (STP), [201](#)
Shielding, [125](#)
Shields Up website, [402](#), [403](#), [405](#)
Signaling rate, [490](#)
Signal-to-noise ratio (SNR), [237](#)
Simple Mail Transfer Protocol (SMTP), [54–58](#)
 inside SMTP packet, [57–8](#)
 body, [57](#)
 header, [57](#)
 message ID, [58](#)
Simple Network Management Protocol (SNMP), [427](#)
Simplex circuit, [81](#)
Simplex transmission, [80](#)
Simulation, [420](#)
Single key encryption, [375–77](#)
Single-mode fiber-optic cable, [90](#)
Single-switch VLAN, [252](#)
Site survey, [220](#)
Skinny Call Control Protocol (SCCP), [497](#)
Slash notation, [159](#)
Sliding window, [129](#)
Small office, home office (SOHO), [204](#)
 environments, designing for, [222–23](#)
Smart card, [383](#)
SmartDraw, [469](#)
 system management, [452](#)
 VPN, [313](#), [315–316](#)
SmartDraw software, [445](#)
Sniffer program, [369](#)
Social engineering, [388](#)
Social engineering, preventing, [385–87](#)

Software, [225](#)
 Akamai, [435–36](#)
 antivirus, [352](#)
 application management, [426](#)
 audit, [199](#)
 client, [206–07](#)
 device management, [424](#)
 encryption, [381–82](#)
 improving performance, [218](#)
 network management, [424–26](#)
 network monitoring, [456](#)
 open versus closed source, [372](#)
 piracy, [199](#)
 server, [206](#)

Software Publishers Association (SPA), [199](#)

SOHO switch, [203](#)

Something you are approach, [383](#)

Something you have approach, [383](#)

Something you know approach, [383](#)

SONET services. *See* Synchronous optical network (SONET)

Sony's spyware, [375](#)

Sound wave, [100](#)

Source address, [134](#)

Source box, [508](#)

Source port address, [153](#)

Spanning tree protocol, [493–96](#)

Specification stage, of, standardization process, [23](#)

Sprint, [316–17](#)

Spyware, [374](#)
 at Sony, [375](#)

Standardization process, [23](#)
 acceptance stage, [23](#)

identification of choices stage, [23](#)
specification stage, [23](#)

Standard-making process
American National Standards Institute, [23](#)
Institute of Electrical and Electronics Engineers, [23](#)
International Organization for Standardization and, [23](#)
International
Telecommunications
Union-Telecommunications
Group, [23](#)
Internet Engineering Task Force, [24](#)

Standards, network, [22–25](#)
American National Standards Institute (ANSI), [23](#)
De facto standards, [22](#)
De jure standards, [22](#)
importance of, [22](#)
Institute of Electrical and Electronics Engineers (IEEE), [23](#)
International Organization for Standardization (ISO), [23](#)
protocols, [24](#)
Telecommunications Group (ITU-T), [23](#)

Star architecture, [275](#)

Start bit, [132](#)

Static routing, [167](#)

Statistical time division multiplexing (STDM), [83–84](#)

Stop bit, [132](#)

Stop-and-wait ARQ, [128](#), [214](#)

Storage area network (SAN), [207](#)

Store and forward switching, [211](#)

Store Ethernet switching, [211](#)

Structured query language (SQL), [40](#)

Subnets, [160–61](#)

Subnetted backbones, [250](#)

Supervisory frame, [134](#)
Switch, [12](#), [107](#)
Switch-based Ethernet, [208](#)
 cut-through switching, [210](#)
 forward switching, [211](#)
 fragment-free switching, [211](#)
 latency, [210](#)
 store switching, [211](#)
Switched backbones, [244–49](#)
 chassis switch, [249](#)
 main distribution facility (MDF), [246](#)
 modules, [249](#)
 network design, [245–46](#)
 patch cables, [247](#)
Switched Ethernet, [208–11](#)
 media access control, [211–12](#)
 performance benefits, [276](#)
 topology, [208–11](#)
Switched virtual circuits (SVCs), [282](#)
Switched-circuit services
 integrated services digital network, [272–73](#)
 plain old telephone service, [100](#), [272](#)
Switches, [203](#), [240](#), [431](#), [495](#)
 chassis, [249](#)
 layer-2, [240](#)
 layer-3, [243](#)
 load balancing, [431](#)
 root, [495](#)
Switching
 fragment-free, [211](#)
 store and forward, [211](#)
Symbol rate, [79](#), [103](#)

Symmetric encryption, [375](#)
Symmetric multiprocessing (SMP), [226](#)
Synchronization, [132](#)
Synchronization characters (SYN), [133](#)
Synchronous data link control (SDLC), [133–34](#)
Synchronous digital hierarchy (SDH), [279](#)
Synchronous optical network (SONET), [278–79](#)
Synchronous transmission, [133–36](#)
 Ethernet, [134–35](#)
 high-level data link control, [134](#)
 point-to-point protocol, [135–36](#)
 synchronous data link control, [133–34](#)
System management software, [425](#)

T

T carrier circuits, [278](#)
T carrier services, [278–79](#)
 fractional T1, [278](#)
 synchronous optical network (SONET), [279](#)
T1 circuit, [278](#)
T3 circuit, [278](#)
T1 circuit, [278](#)
 fractional, [278](#)
T2 circuit, [278](#)
T3 circuit, [278](#)
T4 circuit, [278](#)
Tagging, with RFID chip, [60](#)
Tbps, [27](#)
TCP/IP. *See* Transmission Control Protocol/Internet Protocol (TCP/IP)
TCP connection, [155](#)
TCP SYN floods, [355](#)
Technical reports, [462](#)

Technology design
in building-block network design process, [418–21](#)
 capacity planning, [419](#)
 circuit loading, [419](#)
 circuits, designing, [419–20](#)
 clients, designing, [418–19](#)
 design tools, [420](#)
 devices, designing [419–20](#)
 servers, designing, [418–19](#)
 turnpike effect, [419](#)

Telecommunications Act, [53](#)

Telecommunications Group (ITU-T), [23](#)

Telecommunications, [11](#)

Telephone
 relative capacities of, [26](#)
 transmission of voice data, [91](#)
 voice data transmission by, [106–08](#)

Telepresence, Cisco, [64](#)

Telnet, [59–60](#), [132](#), [398](#)

Telstar I satellite, [6](#)

10Base-T standard, [212](#), [488–90](#)

10 GbE, [212](#), [213](#)

10/100 Ethernet, [316](#)

10/100/1000 Ethernet, [212](#)

Terminal, [41](#)
 dumb, [41](#)
 transaction, [41](#)

Terminal adapter (TA), [272](#)

Theft, credit card data, [340](#)

Theft protection, [356](#)

Thick-client approach, [46](#)

Thin-client approach, [46](#)

Threats

- control spreadsheet, 345–49
- security, 342
- 3G wireless, 501
- Three-tier architecture, 44–45
- Three-tier thin client-server architectures, 56–57
- Three-way handshake, 155
- Throughput, 137–38
- Ticket-Granting Ticket (TGT), 386
- Tier 1 ISP, 312
- Tier 2 ISP, 313
- Tier 3 ISP, 315
- Time-based tokens, 384
- Time Division Multiple Access (TDMA), 500
- Time division multiplexing (TDM), 82, 83
- Token passing, 122
- Tokens, 384
 - time-based, 384
- Toolkits, network management, 438
- Topology, 208–11
 - bus, 208, 228
 - logical, 208
 - physical, 208
- Total cost of ownership (TCO), 469
- TracePlus Ethernet, 227–28
- TRACERT, 192, 194
- Traditional network design process, 410–11
- Traffic analysis, 354, 428–29
- Traffic anomaly analyzer, 354
- Traffic anomaly detector, 354
- Traffic filtering, 353
- Transaction terminal, 41

Transmission asynchronous, 132–33
laser/LED/fiber optic cable, 89
microwave, 92–93
satellite, 93–93
synchronous, 132–35

Transmission Control Protocol/Internet Protocol (TCP/IP), 148, 150–52
example, 174–81
 known addresses, different subnet, 177–78
 known addresses, same subnet, 174–77
 TCP connections, 179
 TCP/IP and network layers, 179–81
 unknown addresses, 178–79
network layer protocol, 150
TCP/IP game, 502–12
 general rules, 502–03
 transport layer protocol, 150

Transmission distance, media selection and, 95

Transmission efficiency, 136–39
 defined, 137

Transmission modes, 97–98
 digital transmission, 98–99
 bipolar signaling, 98
 unipolar signaling, 98
 parallel transmission, 97
 serial transmission, 97

Transmission rate of information bits (TRIB), 139
 calculation of, 139

Transmission speeds, media selection and, 95

Transmit data pins, 488

Transport layer, 148–94, 505–06
 functions, 152–57
 internet model, 18

linking to application layer, [153–54](#)
message transmission using, [20](#)
OSI model, [17](#)
segmenting, [154–55](#)
session management, [155–57](#)
Transport mode, in IPSec, [382](#)
Transport/network layer protocols, [150–52](#)
 Internet protocol, [151–52](#)
 transmission control protocol, [151](#)
Triple DES (3DES), [377](#)
Trojan horses, [373–74](#)
 Black Orifice, [402](#)
 at home, [376](#)
 MoSucker, [373](#)
 Optix Pro, [373](#)
Trouble report, elements of, [463](#)
Trouble tickets, [460](#)
Tunnel mode, in IPSec, [382](#)
Turnaround time, [81](#)
Turnpike effect, [419](#)
Twisted-pair cable, [88–89, 203](#)
Two-bit amplitude modulation, [103](#)
Two-tier architecture, [44–45, 49](#)
 World Wide Web as, [49](#)
Two-tier e-mail architecture, [54–56](#)

U

Unicast message, [171](#)
Unicode, [96](#)
Uniform resource locator (URL), [50](#)
Uninterruptable power supplies (UPS), [108, 357](#)
Unipolar signaling, [98](#)

United States of America Standard Code for Information Interchange (USASCII), [96](#)

Universal Serial Bus (USB), [491–92](#)

University Corporation for Advanced Internet Development (UCAID), [326](#)

UNIX, [49](#), [59](#)

- process table attacks, [355](#)
- Unreliable packet service, [283](#)
- Unshielded twisted-pair (UTP) wires, [201](#)
- User accounts, managing, [513–16](#)
 - active directory, [513](#)
 - creating users, [513–14](#)
 - domain account, [513](#)
 - group, [513](#)
 - local account, [513](#)
 - setting user properties, [515–16](#)
- User authentication, [382–85](#)
 - access cards, [383](#)
 - account, [382](#)
 - automated teller machine (ATM) network, [383](#)
 - one-time passwords, [384](#)
 - passphrases, [383](#)
 - passwords, [383](#)
 - smart card, [383](#)
 - time-based tokens, [384](#)
 - token, [384](#)
 - user profile, [382](#)
- User Data space, [506–07](#)
- User Datagram Protocol (UDP), [151](#), [156](#)
 - attacks, [355](#)
- User profile, [207](#), [382](#)

V.44 standard, [104](#), [110](#)

Video, integration with voice and data, [27–28](#)

Videoconferencing, [61–63](#)

desktop, [61–63](#)

H.320 standard, [62](#)

H.323 standard, [62](#)

MPEG-2 standard, [63](#)

webcasting, [63](#)

Virtual carrier sense method, [214](#)

Virtual circuit, [281](#)

Virtual LANs (VLANs), [252–58](#)

benefits of, [253](#)

design, [258–59](#)

multiswitch VLAN, [254](#)

single-switch VLAN, [252](#)

VLAN tag, [256](#)

VLAN trunks, [257](#)

working, [255](#)

Virtual private networks (VPNs), [286–92](#)

access VPN, [287](#)

basic architecture, [286–87](#)

extranet VPN, [287](#)

intranet VPN, [287](#)

layer-2 tunneling protocol (L2TP), [286](#)

layer-3 VPN, [286](#)

VPN gateway, [286](#)

VPN software, [286](#)

working, [288–92](#)

Virtual server, [41](#), [431–32](#)

Virus protection, [351–52](#)

Viruses, [351](#)

VLAN ID, [255–58](#)

VLAN tag, 134–35, 254–57
VLAN trunks, 257
Voice Activity Detection (VAD), 498
Voice communications
 integration with data, 452
 integration with video and data, 27–28
Voice data
 instant messenger transmission of, 108–09
 telephone transmission of, 318
Voice data transmission
 by instant messenger, 108
 by telephones, 106–08
Voice over ATM (VoATM), 497
Voice over Frame Relay (VoFR), 497
Voice over Internet Protocol (VoIP), 27, 108–09, 497
VoIP. *See* Voice Over Internet Protocol (VoIP)
Voltage, 97

W

Wal-Mart, 8
Warchalking, 216
Wardriving, 216
War-walking, 235
Watson, Tom, 5
Wavelength division multiplexing (WDM), 81–85, 322, 328
Weather map, Internet2, 334, 460
Weather map, network, 459
Web browser, 12, 44, 153, 302
Web packets, 63
Web server, 12, 51
 response from, 51
Web-based email, 56–57

Webcasting, [65](#)

Westinghouse, George, [22](#)

White noise, [123–24](#)

Wide area networks (WANs), [15](#), [268–309](#). *See also* Circuit-switched networks; Dedicated-circuit networks; Packet-switched networks
design, [292–94](#)

improving performance, [294–97](#)

circuit capacity, [295–96](#)

device performance, [294–95](#)

reducing network demand, [296–97](#)

Wideband Code Division Multiple Access (WCDMA), [501](#)

Wi-Fi, [213–22](#)

802.11a, [216](#)

802.11b, [216](#)

802.11g, [216](#)

802.11n, [216](#)

on cruise ships, [236](#)

interference, [220](#)

media access control, [120](#), [140](#)

mooching, [218](#)

public, [235](#)

topology, [245](#)

tourism and types of, [215–16](#)

Wi-Fi Protected Access (WPA), [217](#)

WiMAX (Worldwide Interoperability for Microwave Access), [323](#)

media access control, [323](#)

topology, [323](#)

types of, [323](#)

Windows, [22](#), [30](#), [49](#), [59](#), [96](#), [175](#), [200](#), [206](#), [371](#), [515](#)

Windows server, [199](#), [513–24](#)

managing file sharing, [518–24](#)

managing user accounts, [513–18](#)

Wire speed, [430](#)
Wired Equivalent Privacy (WEP), [216](#)
Wired Ethernet, [208–13](#), [219–20](#)
 error control in, [224](#)
 media access control, [211–12](#)
 shared Ethernet, [208](#)
 switch-based Ethernet, [208–09](#)
 topology, [208–11](#)
 bus topology, [208](#)
 frames, [208](#)
 hub-based Ethernet, [208–09](#)
 logical topology, [208](#)
 physical topology, [208](#)
Wired LANs, [201](#)
Wireless Application Environment (WAE), [350](#)
 banking and, [213](#)
Wireless Ethernet, [213–18](#), [220–22](#)
 802.11a, [216](#)
 802.11b, [216](#)
 802.11g, [216](#)
 802.11n, [216](#)
 associating with AP, [214](#)
 association, [213](#)
 controlled-access methods, [215](#)
 distributed coordination function (DCF), [214](#)
 frame layout, [215](#)
 hidden node problem, [214](#)
 MAC address filtering, [217](#)
 media access control, [213–15](#)
 point coordination function (PCF), [214](#)
 security, [216–18](#)
 site survey, [220](#)

topology, [213](#)
types of, [215–16](#)
virtual carrier sense method, [214](#)

Wireless LANs (WLANs), [33](#), [91](#), [144](#), [202–03](#), [221](#), [228–29](#), [235](#), [457](#), [501](#)
[802.11i](#), [217](#)
access points, [202–03](#)
best practice design, [218](#), [424](#)
Bluetooth, [226](#)
circuit capacity improvement, [260–61](#), [419](#)
components of, [198–213](#)
device performance improvement, [294–97](#)
improving performance, [224–27](#)
MAC address filtering, [217](#)
multistory design, [221](#)
network interface cards, [201](#), [227](#)
physical design, [420](#)
radio frequencies, [80](#), [213](#)
recommendations for, [261](#), [292](#)
reducing network demand, [226–27](#)
security, [217](#)
SSID, [237](#)
Wi-Fi, [198–228](#)
Wi-Fi Protected Access, [217](#)
WiMAX, [318](#), [323](#), [329](#)
Wired Equivalent Privacy, [216–17](#)

Wireless media, [88](#), [91–95](#)
radio transmission, [91](#)
microwave transmission, [93–94](#)
in Munich airport, [91](#)
satellite transmission, [93–94](#), [125](#), [130](#), [139](#)

Wireless networking, [10](#), [201](#)

Wireless telephony application (WTA) server, [350](#)

Wish-list requirements, [417](#)
Workgroup switch, [214](#)
World Wide Web, [49–53](#)
 functioning of, [49–50](#)
 Web browser, [49](#)
 Web server, [50](#)
Worldwide Interoperability for Microwave Access (WiMAX), [323](#)
Worm, [340](#), [352](#), [370](#), [393](#)
 Slammer, [399](#)

X

X.25 packet switching, [484](#)

Y

Yahoo, [34](#), [316](#), [319](#), [344](#), [431](#), [434–36](#)
[Yipes.com](#), [87](#), [284](#)

Z

Zero day attacks, [370](#)