Getting a Networking Job

FOR DUMMIES®

A Wiley Brand

Learn to:

- Find the right organization
- Write a resume that gets attention
- Answer difficult interview questions
- Identify required certifications

Get access to free online resources, including video, articles, and a sample resume

Peter H. Gregory
Bill Hughes

Getting
a Networking
Job

FOR
DUMMIES®
A Wiley Brand

by Peter H. Gregory and Bill Hughes

Getting a Networking Job For Dummies®

Published by: **John Wiley & Sons, Inc.,** 111 River Street, Hoboken, NJ 07030-5774, `www.wiley.com`

Copyright © 2015 by John Wiley & Sons, Inc., Hoboken, New Jersey

Media and software compilation copyright © 2015 by John Wiley & Sons, Inc. All rights reserved.

Published simultaneously in Canada

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at `http://www.wiley.com/go/permissions`.

Trademarks: Wiley, For Dummies, the Dummies Man logo, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

For general information on our other products and services, please contact our Customer Care Department within the U.S. at 877-762-2974, outside the U.S. at 317-572-3993, or fax 317-572-4002. For technical support, please visit `www.wiley.com/techsupport`.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at `http://booksupport.wiley.com`. For more information about Wiley products, visit `www.wiley.com`.

Contents at a Glance

Table of Contents

Part II: Having the Right Stuff 81

Chapter 5: Getting the Necessary Education and Training 83

Chapter 6: Becoming Certifiable 101

Introduction

∙ ∙

*T*he networking profession got its start decades ago, even before there were networks as we understand them today. From the 1960s through the 1980s, computer centers (as they were known then) had their support specialists who connected terminals and printers to mainframes through serial lines, and occasionally to modems, multiplexors, and other devices. These technicians were the plumbers of their day, and they're the plumbers today, indispensable in their skill in connecting systems and networks, facilitating the business use of computers. Networking today is a good deal more complicated than it was then, requiring more skills and knowledge.

About This Book

There are more than enough books on networking, but until now, there was no clear guide to getting into the profession. Delivered in the same rich tradition of the *Dummies* series, *Getting a Networking Job For Dummies* is that clear guide on planning your entry into networking, no matter where you are in your career today:

- ✔ **If you're a student or recent graduate,** you'll get real-life information on what it's like in the networking profession.

- ✔ **If you're already getting your start in networking,** you can chart your career path and decide what kind of an organization you may want to work in.

- ✔ **If you're in the networking job market,** you'll understand different types of networking jobs in different types of organizations.

- ✔ **If you need to hire a networking professional,** you'll find lots of information to help you focus on what kind of candidate you need and to better understand the people who are applying for your positions.

No matter why you're reading this book, you can use it as a networking career reference. *Getting a Networking Job For Dummies* is written by career IT professionals who have spent years in networking. You'll begin to understand what the networking profession is really like from professionals who have been doing it for years.

Foolish Assumptions

While writing this book, we've made some assumptions about you:

- ✔ **You are curious about technology and how things work.** Even if you're looking to get into the management aspect of networking, having a healthy appreciation for how technology supports an organization is important.

- ✔ **You enjoy helping others.** Anyone in a networking job is part of information technology, a service organization that supports the business and the people trying to get things done. With technology so important in business, networking professionals are on the front lines helping others get their jobs done every day.

- ✔ **You enjoy learning.** My first clue: You're reading this book! Being in networking — or any branch of information technology — demands continuous learning. Networking and technology itself change rapidly, and continuous learning is needed just to keep up!

- ✔ **You like Dr. Who and his problem-solving capabilities,** even if some of the scenarios he finds himself in are a little odd.

How are we doing so far? If all my assumptions are right, you may be networking material and ready to seriously consider a career in networking.

Icons Used in This Book

Throughout this book, you'll see icons in the left margin that call attention to information that's worth noting. No smiley faces winking at you or other cute little emoticons, but you'll definitely want to take note! Here's what to look for and what to expect.

This icon identifies general information and core concepts that are well worth committing to your nonvolatile memory, your gray matter, or your noggin' — along with anniversaries, birthdays, and other important stuff!

Thank you for reading; we hope you enjoy the book; please take care of your writers! Seriously, this icon includes helpful suggestions and tidbits of useful information that may save you some time and headaches.

Whatever I'm warning you about isn't *that* hazardous. These helpful alerts point out easily confused or difficult-to-understand terms and concepts.

Beyond the Book

In additional to the material in the print or ebook you're reading, this product comes with more online goodies:

- **Cheat sheet:** The cheat sheet offers tips on interviewing for a networking job, building your personal brand, and information on the major applications on the networks you build and support. You can find the cheat sheet at

  www.dummies.com/cheatsheet/gettinganetworkingjob

- **Web extras:** You'll find some great references that you can use, including a resume template, a sample resume, and a list of websites of value to networking professionals. Go to

  www.dummies.com/extras/gettinganetworkingjob

- **Updates:** If we have any updates to this book, you can find them at

  www.dummies.com/go/gettinganetworkingjobupdates

Where to Go from Here

If you're wondering what the networking profession is all about, go to Part I. If you want to dive into the education, training, and knowledge required in networking, start with Part II. If you're wondering what life is like in different types of organizations, Part III was written just for you. If you're ready to get out there in the networking job market, go right to Part IV. If you love lists, head for Part V.

And for those who want to take an even deeper dive into the knowledge expected of networking professionals, get a copy of *Networking For Dummies,* 10th Edition, by Doug Lowe.

Part I

So You Want to Be a Networking Professional

In this part . . .

- ✔ Understand what you'll be getting yourself into.
- ✔ Appreciate the scope of your responsibilities.
- ✔ Find out your day-to-day tasks.
- ✔ Anticipate changing trends.

Chapter 1

Working with Networks

In This Chapter

▶ Understanding the need for networking professionals

▶ Exploring the wide range of activities in networking jobs

▶ Predicting the future for networking jobs

*I*f you conduct an online search on the phrase *demand for networking jobs,* you'll find article after article citing networking jobs as one of the high-demand jobs. You've chosen a great time to learn more about this exciting and rapidly growing and changing field!

This chapter takes a closer look at the changes in business and technology that have given rise to the high demand for networking professionals. You will also discover why networking is such a great career field.

Why Are Networks Important?

Networks facilitate data communications in organizations, between organizations, and over the Internet itself. Without networks, computers are practically worthless. Then again, without computers, networks would not be needed. But let's not get caught up in circular arguments. Instead, let's look a little deeper into why networks are important.

Organizations of every kind, as well as a growing number of private citizens, rely on information systems to conduct their daily affairs more than ever before. We buy more and more products that are Internet connected, partly for convenience and partly for the cool factor. Before long, it will be easier to count the things that *aren't* connected to the Internet.

Computers and networks are inseparable

A networking professional who knows little about computers cannot be any more useful than a computer professional who knows little about networks. To be an expert in one requires skills and knowledge in the other.

Networks facilitate communications between computers. A networking professional must understand how computers communicate over networks to be able to set up and manage networks properly. And similarly, computer professionals must understand how networks work so that they can set up and manage computers in the right way. Computers and networks are like peanut butter and jelly, or drums and drumsticks, or . . . well, we think you get the idea.

You might have heard that data and information are the new currency. Although this statement might sound like a cliché, it's true for several reasons:

✔ Organizations can use software tools to examine electronic business records and gain valuable insights that help them find new opportunities. For instance, a grocery store can add items to its inventory based on sales trends.

✔ Organizations can use information systems to make business processes more efficient. For example, if an organization puts sales details in an information system, the customer service department could electronically access those records and be far more efficient.

✔ For banks and other financial institutions, data actually *is* money, or at least the closest representation of money. For instance, transferring funds or paying bills online is mostly about making a number bigger in one place and smaller in another.

This increased reliance on Internet-connected systems and devices makes our businesses more efficient and our lives easier. Networks — and the professionals who design, build, and maintain them — are essential.

Skills and Activities in Networking Jobs

You might be wondering what people do in a networking job. Well, networking tasks can vary widely from company to company, and from person to person within a company. If you asked twenty people what networking professionals do, you'd probably get twenty different answers. This section explores some of these activities.

In smaller organizations, a networking professional may do most or all of the activities discussed here. In larger organizations, the activities described in

this section may be assigned to different teams, so there would be less variety for individual networking professionals.

Managing network devices

Network devices such as switches and routers facilitate communications between computers in an organization and between organizations. A smaller organization may have just a single router that connects the internal network to the Internet via a DSL (digital subscriber line) or cable modem. A larger organization will have more routers, as well as switches, to connect various internal networks.

Setting up remote access

Remote access permits personnel to access an organization's internal systems from remote locations such as home or while traveling. Often, remote access is provided to an employee upon approval from management. Then networking personnel make the required configuration changes in the network equipment and the employee's workstation to facilitate remote access.

Networking personnel often help employees learn how to use and troubleshoot remote access. Connecting remotely sometimes requires a series of steps that don't always work, especially where Internet connectivity isn't great.

Maintaining user accounts

In many organizations, networking professionals must maintain user accounts. Generally, maintaining user accounts includes the following tasks: creating user accounts for new employees (as well as business partners and others authorized to access systems or networks), removing user accounts for departing personnel, and making changes in access rights as needed.

Often, a documented approval from management is required before a networking professional can make any additions, changes, or deletions.

Helping end users

In some organizations, networking professionals play (or support) the role of a help desk person who assists end users. Activities related to the help desk could range from operating system and program configuration on workstations to Internet and remote access connectivity.

In some organizations, front-line help desk people answer the phone and help with simple issues. In other organizations, network professionals and other IT workers help users directly.

Configuring firewalls

Firewalls are networking devices that play a role in keeping the bad guys (and gals) out of an organization's network. Some lucky networking professional's job is going to be designing, setting up, and managing those firewalls, including managing the complex rulesets that determine exactly which types of Internet traffic are allowed to pass through the firewall.

Monitoring antimalware consoles

Smaller organizations and home users run standalone copies of antivirus or antimalware on their individual workstations. In larger organizations as well, each system has antimalware (or antivirus) software, but they also have a central console where a (you guessed it) networking professional can view the state of antimalware across all the machines in the organization.

In addition to just monitoring, a networking professional can use the console to change the configuration of antimalware on individual systems as well as run malware scans on individual systems or all systems at once.

Issuing authentication tokens

Many organizations have gone beyond simple user IDs and passwords for authentication and are using token-based authentication. Depending on the organization, token-based authentication may be used for remote access, privileged access, or perhaps everyone.

Another form of strong authentication is where a code is sent to a user's mobile phone and the user must enter that number to log in to a system. Who's gonna set that up? A networking professional!

Setting up wireless networks

Everybody loves their Wi-Fi connections. In some organizations, Wi-Fi is the only way to communicate over networks. Many organizations provide guest Wi-Fi connections for visitors and customers.

Organizations that want Wi-Fi require networking professionals with skills to design a Wi-Fi network, which can be a challenge in a multistory building or a campus with multiple buildings.

Setting up Wi-Fi networks involves choosing good locations for radios, antennas, and controllers, and connecting these to the organization's data network and the Internet. Another issue is deciding how users will authenticate to the Wi-Fi network, which will require interconnections with domain controllers or LDAP (Lightweight Directory Access Protocol) servers.

Configuring communications with business partners

Not long ago, it was common for companies with frequent data communications to set up dedicated telecommunications circuits such as T-1 or DS-3 connections. Nowadays, MPLS (multiprotocol label switching) or over-the-Internet VPN connections are often used. Networking professionals design and set up these connections, in coordination with their counterparts in the business partner organization.

Connecting storage devices

Computers access storage area network (SAN) and network attached storage (NAS) devices to store and retrieve data. Sometimes this communications is on the general data network, but often it will be on a separate network dedicated to storage. Someone has to figure out how to access storage devices and how to hook them up. If you're a networking professional, that person is you!

Managing telecommunications services

No man or business is an island. In the networking world, organizations connect their internal networks to the outside world. Those connections require telecommunications services of some kind, including a digital subscriber line (DSL), cable, or T-1 connection. A networking professional is instrumental in determining how much information needs to flow to and from the outside world and how fast it needs to flow. Buying too much or too little bandwidth is inefficient.

Setting up VoIP phones and voicemail

Voice is just another form of data on a network. Networking professionals install and configure VoIP (voice over Internet protocol) phones for office workers. Incidentally, they often set up voicemail as well.

Pulling network cabling

Although wireless networks are popular and, in some cases, replace network wiring for individual users, network cabling is still needed. This cabling could be fiber-optic cabling for high-speed storage systems or for connecting floors in a campus or high-rise building, as well as copper network patch cords in data centers.

In some companies, networking personnel also build custom-length cables and install connectors on each end.

Installing network devices in data centers and closets

Networking professionals occasionally install network devices in equipment racks in data centers as well as in data closets. Some organizations have equipment in *co-lo (co-location)* facilities, which provide commercial data center space for companies that don't want to build their own data centers, so working on these components of the company network might require a drive across town or further.

Designing networks

Senior networking professionals spend some of their time doing design work. Many events and trends necessitate changes in the design of an organization's network, including the following:

- ✔ **Business growth:** More users and equipment on a network often results in increased network traffic, which will occasionally require upgrades in equipment or speeds.

- ✔ **New equipment:** The addition of new servers, storage systems, and appliances usually require minor changes in network architecture.

- ✔ **Emerging threats:** Firewalls are no longer enough; organizations are investing in other types of security equipment such as intrusion

prevention systems (IPS), web filters, and data leakage prevention (DLP) systems to improve the protection of systems and data.

✔ **New business partners:** The addition of new business partners can require changes in the network to facilitate direct communications to those partners.

✔ **New or upgraded business applications:** Upgrades or complete replacements to business applications may require changes in supporting networks.

✔ **Business office relocation:** Moving a company headquarters or even a branch office requires considerable planning to make sure that network communications will work properly in the new location and for personnel and systems in all locations.

Completing paperwork

We hate to be a spoiler: You don't get to have fun all day long with networking technologies. Proper management of devices, systems, user accounts, firewall rules, and so forth requires sound business processes and controls to ensure that everything is properly approved and recorded. Yes, you need to fill out the paperwork before the job is done — and often before it begins!

Fixing things

No person or network is perfect — things go wrong for many reasons. Networking professionals often must troubleshoot different kinds of communications problems that can crop up in an organization. Good troubleshooting skills are essential so that you can isolate the cause of a problem quickly and get it fixed.

Working with People

Sure, technology skills are important in networking jobs. In some ways you need to be able to think like networking equipment and computer software to understand how they work. Okay, we're stretching it a bit by suggesting that hardware and software "think." What we mean is that it takes someone special to understand how information technology works.

However, no matter how strong your networking skills and knowledge, you'll have a hard time finding a networking job if you lack people skills. A lot of people are attracted to high-tech and information technology, in part

because they are attracted to complex machinery but sometimes because they'd rather work with machinery than with people. They may be shy, or they may not be sociable, or they may prefer to work alone. Some IT workers earn a reputation for lacking people skills.

All of us can stand to improve our people skills. The best way? Practice! Be conscious of your interaction with your coworkers and others. Step out of your comfort zone and meet people. One of the best ways to rid yourself of nervousness is to ask others about themselves; this approach takes the pressure off you. When you show interest in others, you gain a reputation as a friendly and sociable person.

Depending on the activities in your networking job, you might be on the phone a lot or working with people all day long. Remember, IT is a business service function, so IT must exhibit great customer service. IT is a person-to-person activity that involves good communication at every level, as well as honesty, empathy, sincerity, and above all, patience.

Be sure to read Chapter 13, where you will learn how to develop your brand, meet people, and expand your network of business associates.

How Networking Fits in a High-Tech Career Path

Depending on your long-term career plans, networking may be your entire high-tech career or a stepping stone to a different position in high-tech. Plenty of people are in both camps, and a lot of career paths in high tech include networking.

Figure 1-1 depicts six typical job paths in an IT department. The topmost row in the figure shows four typical job titles in networking (network technician, network administrator, network engineer, and network architect). Larger organizations with a lot of networking professionals might have people in all these (or similar) job titles, which represent increasing skills, experience, and seniority in networking.

Each of the job groups in Figure 1-1 has its own range of job titles representing career growth.

Some professionals may use networking jobs as a path to positions in other IT disciplines, while others will stay in networking for most or all their career. Let's look at a couple of examples:

✔ John starts his IT career as a help desk technician, is promoted to help desk analyst, and then help desk specialist. Next, he moves into networking, first as a network technician and then as a network administrator. But John's passion is managing operating systems, and his next job is as a systems administrator, followed by a systems engineer, where he stays for many years.

✔ Jane starts her career as a project analyst and is promoted to project manager. But Jane wants to be involved in networking and gets a network technician position, followed by promotions to network administrator, network engineer, and finally to network architect after many years.

In the first example, John uses the help desk and networking jobs as stepping stones to systems engineering. Knowledge of networking is essential for the success of a systems engineer. In the second example, Jane acquires her basic IT skills in project management, and then moves into a more technical role in networking, which was where she wanted to be.
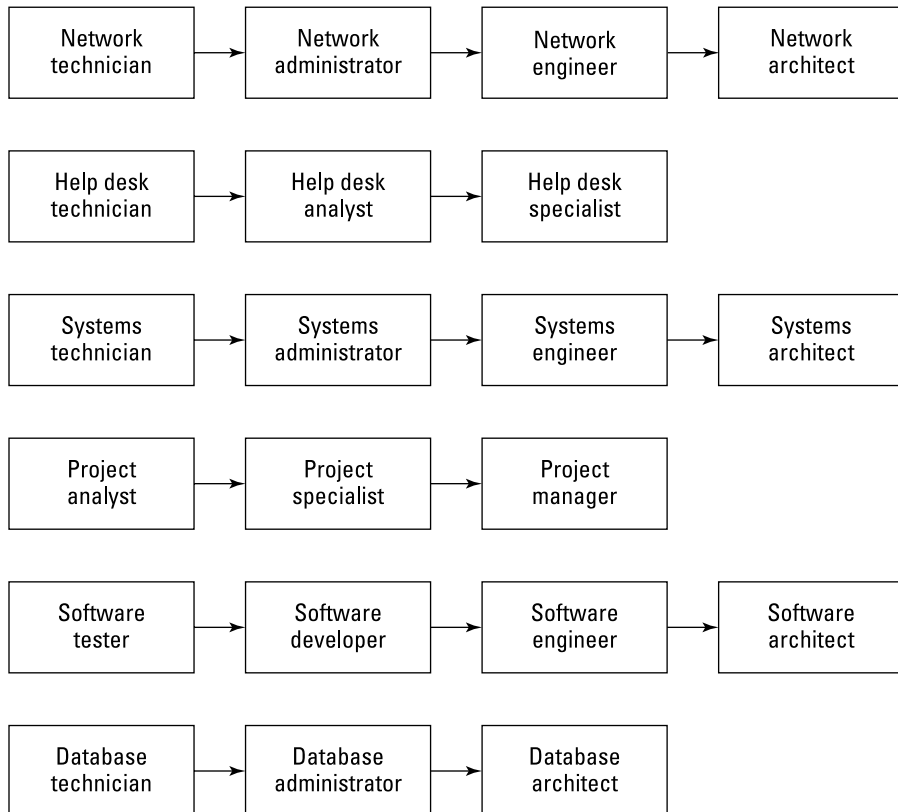
Figure 1-1:
IT job
families.

You can look at a networking job in two ways. One, a networking job can be a way to get into a different IT discipline such as systems engineering or software development. Two, a particular networking job is where you want to spend your entire career, or at least as far over the horizon as you can imagine.

The Future Is Bright for Networking Jobs

Every organization that uses computers and networks must employ people with networking skills and knowledge. With the pace of change in information technology and new uses for Internet-based services, even a one-person IT department must be knowledgeable about basic networking skills.

The United States has a big shortage of workers in STEM (science, technology, engineering, and mathematics) jobs, as indicated by the following numbers:

- ✔ According to IT Business Edge, network engineer is one of the top 10 most in-demand job titles (`www.itbusinessedge.com/slideshows/top-10-most-in-demand-it-job-titles-11.html`).

- ✔ According to the Conference Board, three job vacancies are advertised for every unemployed computer worker (`www.usnews.com/opinion/articles/2014/09/15/the-stem-worker-shortage-is-real`).

- ✔ According to Mashable, a network systems analyst/network engineer ranked third in the eight hottest tech jobs in 2014 (`http://mashable.com/2014/01/06/tech-jobs-2014/`).

We could keep going and cite more of these facts, but we think you get the idea.

A networking career is not a get-rich-quick career — far from it. But if you are motivated, possess an aptitude for working with technology, and have good people skills, you should enjoy more-or-less steady employment and a decent standard of living.

Many consider networking to be an entry-level field in IT. As we've mentioned, networking is a great way to start a career in IT, and many use networking as a stepping-stone into other IT fields such as software development or database administration. However, networking itself is a great career: highly skilled and experienced network engineers are among the highest paid positions in IT. To summarize: A networking career offers a full career path with great opportunity for advancement, from entry-level help-desk roles to senior management or director positions.

Chapter 2

Understanding Networking Roles

● ●

In This Chapter

▶ Understanding the responsibilities of networking in a company

▶ Exploring the array or networking jobs

▶ Stepping from a non-networking job to a networking one

● ●

*M*odern organizations depend on their computer systems to serve customers and reduce costs. The most susceptible part of any IT system is its computer network. Whatever your official title may be in the networking realm, your goal is to create and maintain a service that keeps the organization up and functioning.

This goal involves a number of responsibilities, each with its own job titles. This chapter describes the generally accepted usage for job titles. However, don't be surprised if your employer takes some poetic license and uses a slightly different title or job description.

Reviewing First Principles

The most basic reason for an organization to have a computer network is so that employees can collaborate; access relevant information stored on other computers, both local and remote; and engage with customers. The ideal network is so reliable that users can ignore it. Networking professionals get a lot of unwelcome attention the minute things do not function. The following are some reasons why networking professionals are needed:

✔ **Companies grow.** A company should have resources in place for new employees so that they can be productive fast. These resources may include a physical network connection, wireless network access and appropriate access to the IT system and various applications needed to perform the tasks assigned to the new user.

✔ **Companies shrink.** Companies fire or lay off employees. The company must freeze, or disable, the accounts of these employees to protect information assets of the company. Often the task of disabling access must be done without deleting the user files or work product so the access is only disabled.

Some salespeople feel a close tie with their customers, some doctors, with their patients, and some lawyers, with their clients. However, when they are let go, the law is clear that the employer owns the records associated with the customer or patient or client. State laws vary, but it is usually considered intellectual property theft for a former employee to take customer records.

✔ **Employees move.** An employer moves the office location of each employee on average once a year. A company that relies on wireless LAN connections may have less physical rewiring to do, but many companies still prefer good old wired connections.

✔ **WANs, in particular, are flaky.** The moment you want to connect outside your property line, you rely on someone else's network (unless you happen to be employed by a telecommunications carrier). Backhoes rip up cables, backup generators fail, lightning strikes, and more. This, in turn, can cause remote offices or data centers to go offline. You may have service level guarantees from these suppliers, but that is cold comfort when the network is down during your peak revenue day.

✔ **The security situation is evolving rapidly.** Information security and networking are intimately related, so security solutions require close collaboration between the two.

✔ **New apps are added.** IT regularly adds new and updated applications. Many of these have implications for networking.

✔ **Networking technology standards evolve.** Networking is high-tech after all. New equipment and services are coming to the market all the time.

✔ **Network elements needs to be watched.** Some routine tasks can be automated, such as backups and alarms. But ultimately, a human must make sure that everything is operating within normal limits and decide what to do when things go sideways.

✔ **End-users are impatient.** Individuals and department heads dislike waiting for the IT department to support their device or new application. They figure out a way to use their insecure personal device to connect to the corporate network or find an application that is available in the cloud. IT ends up either supporting their stopgap measure or gets roped into helping them with migration from the unofficial solution. The current acronym for users attaching to the network with their own computing resources is BYOD, or bring your own device. The definition is more commonly defined among networking professionals as bring your own disaster.

Performing Essential Tasks in Networking

Regardless of title and the size of the organization, the networking department performs certain tasks. They include the following:

- ✔ **Solve end-user problems:** End-users in your organization need a person to call when there are issues such as a problem with a password, a website, or remote access. In larger organizations, someone has to act as the clearinghouse for questions. Because most issues relate to the network, the networking department is the first line of support. Many organizations implement a ticketing system to track and close out inquiries.

- ✔ **Update configurations of servers and applications:** The networking department is responsible for ensuring that the equipment works as intended as well as adding, changing, and deleting end users (employees). (The abbreviation A/C/D stands for adds/changes/deletions.) The task of making adds, changes, or deletions applies to both LANs and WANs.

- ✔ **Install cabling and update hardware:** This task is where you get your hands dirty. Even if you have a wireless LAN, you will need to run cabling to the access points.

- ✔ **Conduct user training:** End-users need to know how to access the system as well as protect the intellectual property assets of the company. This effort can be done one at a time, in a classroom with multiple end-users, or by training the trainers.

- ✔ **Manage upgrades and patches:** It falls to the networking department to distribute software upgrades to all the equipment in the organization.

- ✔ **Monitor network performance:** Networks will experience outages and congestion. Multiple people use a given resource, and inevitably multiple people will want some of the resource at the same time. Momentary blips are to be expected, but wholesale failure of significant elements is unacceptable. Modern networking equipment and vendor solutions are available to offer insight into the nature of network performance problems before you get the first call.

- ✔ **Implement information security and backup policies:** Networking may or may not create the information security or backup policy, but they will be called to implement and enforce these policies.

- ✔ **Plan future requirements:** The IT environment is constantly changing. New employees are hired and others leave. Applications are added or upgraded. Business strategies change. Acquisitions and divestitures take place. Remote offices open and others are closed. Suppliers offer equipment that is faster, better, and cheaper. The network needs to keep up.

✔ **Work with third-party suppliers:** Some companies want to do as much in-house as possible, while others outsource as much as possible. Regardless of whether companies choose to do their own network planning and implementation or outsource it, they have to deal with service providers. This task is usually performed by the networking department.

✔ **Monitor and plan budgets:** If you have a budget, someone needs to monitor the performance relative to the budget as well as tell the powers that be what you will need in the future.

A given company may choose to have the networking department specialize and assign titles to clarify roles. In times of emergency, however, you can almost certainly count on an "all hands on deck" approach.

Navigating Networking Job Titles

The titles associated with networking are vexingly similar. However, we have to start somewhere. In this section, you explore the following titles and the skills typically associated with them:

✔ Service desk analyst

✔ Network administrator

✔ Network engineer

✔ Network architect

✔ Network manager

✔ Wireless network engineer

✔ Telecommunications manager or specialist

✔ Pre-sales engineer

Service desk analyst

A *service desk (or help desk) analyst* assists users who have problems with their computers, user accounts, or business applications. In some companies, this position is the equivalent of a help desk technician.

In many ways, service desk analysts have one of the most important positions because they are in contact with users in all levels of the organization. For many non-IT employees, service desk analysts are the only IT people they will ever contact.

A service desk person must be able to recognize several types of issues, including the following:

- ✔ Trouble with network connections
- ✔ Forgotten passwords
- ✔ Requests to install software
- ✔ Phishing messages
- ✔ Unsafe practices, such as sharing passwords or visiting malicious web sites

A service desk analyst is a good entry-level position for those with good customer service skills. You must know, for example, how to defuse irate people and help them overcome their frustration.

Network administrator

A *network administrator* often administers the following:

- ✔ User accounts
- ✔ File server access
- ✔ Remote access

Network administrators are on the front lines of access control, and effective access control practices reduce the likelihood of a number of security-related problems. A network administrator will find violations such as active user accounts for terminated personnel, granting excessive privileges, group accounts (a single user account shared and used by multiple users), and user accounts with nonexpiring or noncomplex passwords.

Much of this work is performed in front of a computer terminal, and communication with end-users is conducted through email. Communicating only through electronic means is one step removed from the front lines. Having empathy and the right personality are no less important to achieving user satisfaction than being accurate and performing duties on time.

Network engineer

The *network engineer* has more technical responsibilities than the network administrator role. Network engineers focus more on system upgrades, evaluating vendor products, and testing for security flaws.

The individual that holds this role should either have or be pursuing some of the education and certifications explored in Chapters 5 and 6, respectively.

Some companies use the title *network administrator* and *network engineer* interchangeably. The latter title sounds more serious, and the former has the connotation of a passive clerk. This role should be taken seriously, but the naming choice for this role is an HR decision taken by many companies.

Network architect

The title of *network architect* implies that the network engineer is focused on technical issues and free from administrative tasks. This role only makes sense in larger organizations where this kind of specialization is necessary.

Although no organization likes network downtime, some organizations face serious issues if the network is down for an extended period of time. The cost of a network outage on a financial trading floor, for example, can be measured in millions of dollars a minute. A network disruption to the military or to emergency first responders may be measured in lives lost.

Adding a wireless broadband connection through satellite or microwave to augment the landline solution is prudent. Ensuring that these wireless alternatives achieve the objective requires someone with more technical chops than a typical network administrator. That person is a well-trained network architect.

Network manager

The *network manager* is the boss of the department. This role often includes the administration of the following:

✔ Budget tracking and forecasting

✔ Personnel decisions

✔ Resource acquisition

The network manager does not need to be the most technical person, but it helps if he or she understands the department's importance to the business and has credibility in the rest of the organization to prioritize the needs of the department as business priorities evolve.

This role typically is involved in negotiations with third-party solution providers, both network services and hardware. It is enjoyable to be wined and dined by vendors, but this is a small part of the job. The network manager needs to

be able to walk the tightrope between pursuing new network technology for technology's sake versus achieving the business needs of the organization.

A network architect can make a company's network as close to invulnerable as unlimited funds would allow. No organization has unlimited funds, so trade-offs must be made. Ideally, budget decisions are not made arbitrarily by some faceless, nameless budgeting manager but are decided collaboratively. Ultimately, this job calls for an individual with good decision-making skills and the graciousness to take irate calls when the network fails from the very managers that just cut the budget and prevented the acquisition of the very tools that would have prevented the network from failing in the first place.

Wireless network engineer

A *wireless network engineer* uses his or her training and skills to complement the network design of cables and landlines with wireless technology. Wireless technology adds a new dimension to networks. Adding wireless offers the following features:

✔ Users can access the full resources of the organizations computer system when away from their desks, both in the office and when traveling.

✔ Fewer cables must be pulled during office moves.

✔ New applications that increase customer service and lower costs are possible, such as re-routing delivery trucks to respond to changing customer needs.

✔ Companies can increase productivity when management knows the goings-on of its mobile assets at all times.

At the same time wireless technology has several issues:

✔ Wireless is still more magical than a cable that anyone can touch and feel. As a result, some doubt the reliability of wireless in mission-critical applications.

✔ There is a sense that wireless is less secure because it is easier to snag a wireless connection from outside the doors of the company. An individual may understand intellectually that wireless security can be more secure than physical security with landlines. Emotionally, there is still a fear that wireless is less secure.

✔ Wireless signals propagate in strange ways. You may be able to get a wireless signal in a given location one day and not the next.

A wireless network engineer can design a system to ensure that the wireless part of the company's network is every bit as secure and reliable as the wireline network. A network engineer trained in wireline technology can do a respectable job in many companies. Additional training in wireless technology, however, can take the network to the next level by making it more convenient for users.

Telecommunications manager or specialist

A *telecommunications manager or specialist* has responsibility for planning for the voice usage of the network.

The traditional usage of a network refers strictly to the data network. However, unified communication (UC), which employs Voice over IP (VoIP) technology, allows voice and video communication to take place over the same network, and this convergence blurs the distinction between data, voice, and video technologies. Many companies find it more economical to have a single data network for all communication. This solution can also enables intracompany collaboration, among other benefits.

Combining voice, video, and data on a single network is not as simple as adding more capacity. For example, data communication requires perfect reception of the information no matter how long it takes. Digitized voice, on the other hand, can accept some loss but needs to get there on time and can then be enhanced to be recognizable. Video communication is somewhere in between.

A consideration of the different communications types (voice and data) has an effect on planning. Voice packets need to arrive on time but can take some loss. Data packets need to arrive perfectly and can tolerate some delays. Plus, the type of equipment used by employees is different. The result is a different title that refers to telecommunications instead of just network. Again, different companies have a different spin on the use of this title.

Pre-sales engineer

In companies that offer solution sales, the ideal is to have such a close working relationship with your customers that you provide network-engineering services on their behalf. The customer does not need to hire a well-trained network specialist.

To make the customer/vendor relationship work, the vendor must have competent network engineering staff. This situation involves the creation of a *pre-sales engineer*. This role is a good fit for individuals who like new

networking challenges and are willing to forgo the satisfaction of seeing the fruits or their labor and watching the network perform on an ongoing basis.

Getting Networking Experience Where You Are Now

Workers early in their careers have the following complaint:

> *I want to get this new job, but it requires experience. How can I get experience if I don't have this job?*

Sounds like a chicken-or-egg problem, right? Not necessarily. Most networking professionals didn't have a non-networking-related job one day and a networking job the next. Instead, they gained and built upon networking skills in their current IT job or in places where they volunteered.

The following are a number of examples of non-networking roles in IT organizations:

- ✔ Computer repair specialist
- ✔ Webmaster
- ✔ Software developer
- ✔ Database administrator
- ✔ Business analyst
- ✔ Information security analyst
- ✔ Project manager
- ✔ IT auditor

Even if you never want to perform these functions, it's good to know about them because you'll interact with people in these roles.

In this section, you explore these IT roles and discover how to build your networking knowledge and skills while in those roles.

Computer repair specialist

A *computer repair specialist* is the person who saves the day when an end-user's hard drive crashes or the laptop screen is cracked.

Webmaster

The webpage of the company is a critical part of how people outside the organization learn the vision of the organization and connect with the products and services offered. For each website, one person is identified on the Internet as the *webmaster,* and this individual has the responsibility for what is posted.

In practice, the web is a compromise of priorities among the different functions in an organization. The two greatest challenges in this role are: Everyone thinks they are an expert on what the web page should look like, and each department believes that their area should be more prominent on the home page.

Although most organizations chose to have their web page hosted by a professional service, the development of the site and the testing of the links typically reside in IT.

Software developer

A *software developer* (also referred to as programmer, software development engineer, or programmer-analyst) develops systems software, application software, tools and utilities, and system interfaces. Software development involves several activities, including the following:

- ✔ **Coding:** Developers use programming tools to develop application solutions to reduce cost and improve customer satisfaction. A great deal of time is spent enhancing existing systems. The glossary includes a list of typical corporate applications.
- ✔ **Testing:** Developers perform extensive functionality testing to ensure that their software is free of defects before it is distributed to the end-users.
- ✔ **Code reviews:** Developers should be checking each other's work, looking for flaws that could permit their software to be compromised by an attacker.

Database administrator

A *database administrator*, or *DBA*, is responsible for the care and feeding of databases that reside on servers as well as external storage systems. A large portion of the intellectual assets of a firm, including information on the depth

of key customer relationships and ways the companies performs its business, are found in these data. This data needs to be protected, but it also needs to be available for people to do their jobs. Making the data available to those who need it and keeping it away from the folks that don't are the responsibilities of the DBA.

A database management system is a sizeable piece of software in its own right, often with myriad configuration settings and its own user accounts and related settings. The database administrator must follow sound principles with regards to system hardening as well as user account management. Further, the DBA also controls access permissions to databases and their components.

Business analyst

Depending on the organization, a *business analyst* may be a jack-of-all-trades or focused on one set of activities. In this book, a business analyst is the former. Examples of business analyst activities include

- ✔ Running reports
- ✔ Analyzing the content of reports to assist other workers in their jobs
- ✔ Conducting research tasks and projects on internal business matters
- ✔ Organizing information into usable or readable form

A business analyst can also be thought of as a technical assistant.

Like other IT workers, a business analyst must be familiar with the concepts of safe computer usage and prudent handling of sensitive data, so that they don't unwittingly bring harm to the information by compromising sensitive data and systems.

All IT positions require security skills

Security is the responsibility of not just the security manager but also every IT worker in the organization. Every position in IT requires security skills and knowledge related to each particular position.

Information security analyst

An *information security analyst's* work can range across the entire spectrum of security management, security operations, and security administration. A security analyst may spend time conducting research — interpreting current events, new encryption algorithms, or many other things, and then figuring out how these external developments should shape the organization's short-term operations or long-term strategy.

Project manager

Have you seen those sleek racing rowboats, with the coxswain in back shouting, "Stroke! Stroke! Stroke!" to keep the rowers in sync? Similarly, *project managers* keep a project going in the same direction and at the right pace to ensure that it is completed correctly and on time.

Project managers, or PMs, keep projects running smoothly and ensure that all required resources are available as needed.

The status of networking in IT

Which IT area is the most important and where should you aspire to work? Database managers are highly valued. Information security professionals get a lot of resources and attention. Application developers are clever. IT bosses get schmoozed by vendors. Networking folks get dirty pulling cables, sometimes have to work late and during off hours, and get attention only when the vendor's network fails.

Many people start their career in IT in networking, and there is always the opportunity to either reduce costs or improve output in this area. What is best for you is explored in Chapter 17. Keep in mind that the prestige of any role is determined by the professionalism and integrity of the individual. Plus, it is always a good idea to improve you qualifications and try multiple roles in IT. Cross-experience makes you a better employee and allows you to smile politely when a newbie asserts that his or her department is the key to success in the IT department.

IT auditor

An *IT auditor* (also known as an IS auditor or a security auditor) determines the effectiveness of security controls, and communicates that level of effectiveness to others through written reports that describe controls, their intended function, and how well they carry out that function.

If you're picturing an auditor as someone with a checklist, you're right: Experienced auditors use checklists to make sure they don't forget any aspect of a control they are examining. However, they also have a deep understanding of the technologies and details involved in the controls they examine, and they understand that the true effectiveness of a control requires more than a checklist.

IT auditors must be independent and objective, so it is best if they are not members of the department they are auditing. Otherwise, it might appear that the auditor was being controlled by the department that he or she was auditing.

Chapter 3

Knowing Your Networking

· ·

In This Chapter

▶ Becoming familiar with key concepts in networking technologies

▶ Understanding the issues that concern networking professionals

▶ Making sure you know your priorities

▶ Adjusting to changing conditions

· ·

Chances are that you are knowledgeable about some aspects of networking, but are somewhat uncertain about others. Rather than make an assumption that you are a universal expert on all things networking, this chapter covers the most important technical elements of networking. Networking expertise is critical to your success in a networking job.

A great deal of time in this role is spent planning, budgeting, presenting, training, and generally collaborating with coworkers. We deftly avoid mentioning these administrative aspects of networking as of the end of this sentence.

Appreciating First Principles

Before we get started, a few things need to be said about the network in an organization. First we cover some basic concepts about the design goals of a network. Next we describe business objectives and how these affect network design.

Recognizing design goals for the network

There is no such thing as a one-size-fits-all network. Each organization has unique requirements:

 ✔ **Connection to legacy computer systems:** Unless you work at a startup launched just minutes ago, your organization has existing computer

systems for things such as email. Connecting your computers together (and to the Internet) involves a network.

✔ **Plans for future systems:** Organizations are dynamic and always evolving, including adding applications to increase customer service or reduce costs. New applications inevitably involve changes to the network.

✔ **The locations of offices:** Many organizations have remote offices that need connectivity to computer systems. Companies are regularly adding and reconfiguring remote offices.

✔ **Mobility needs of employees:** Companies have been issuing laptops to employees for years. Employees are now using tablets and smartphones, (their own or ones supplied by the company) to access company systems.

✔ **Throughput:** As IT offers new services, users need more capacity. The good news is that high-speed WAN service is getting cheaper (although it is still much more than LAN service).

✔ **Internet connectivity needs:** In addition to web hosting, many companies need to provide Internet connectivity for business use. It may or may not be company policy to allow the personal use of Internet during business hours.

✔ **Redundancy and resiliency:** The architects of the network need to decide which approach is the best fit for ensuring that business operations will continue when the inevitable failures happen on and around the network. A range of solutions keeps a network up and running. Choosing among redundancy options is typically limited by budget and also by the personnel involved in restoring a failing network when all heck breaks loose.

✔ **Level of security:** Just like redundancy and resiliency, you can pile on security until it becomes excessively costly and difficult to manage. The company needs to decide what level of security it wants to employ to achieve its overall business objectives.

Appreciating the business objectives of the network

It would be pure fantasy, and probably a bad idea, to think that a company would consider limiting its growth and business plans to meet the existing design of its computer network. The computer network, in all its capabilities and restrictions, needs to work around the business.

This concept of the network serving the business entails more than just coming in under budget during the current fiscal year and more than accepting budget cuts to achieve profitability during business planning. The entire computer networking team needs to be on board to provide remedies to the inevitable network glitches that occur.

Proper network management includes planning for server, LAN, WAN, and power outages; PC viruses and other malware; security breaches; and lightning strikes and other severe weather. The entire department needs to know what to fix first, second, and so on. Proper planning and operational management is not something that should be left to leadership skills implemented in real time.

Reviewing the OSI Model

It is an unwritten rule that every discussion of networking should include the 7-layer OSI (Open Systems Interconnection) model, depicted in Figure 3-1.
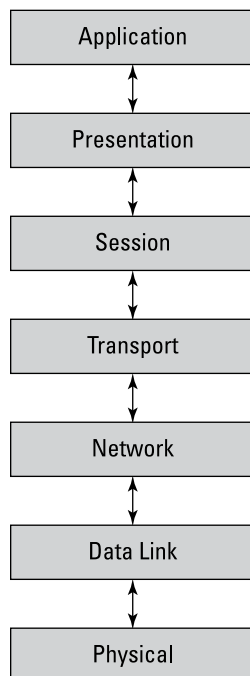
Figure 3-1:
The OSI
7-layer
networking
model.

Application

Presentation

Session

Transport

Network

Data Link

Physical

The OSI model breaks the network communications process into seven separate layers. From the top (the layer closest to the user) down, these layers are as follows:

- ✔ **Layer 7, Application:** The Application layer provides services to the software through which the user requests connectivity. This layer is about programs such as browsers, FTP clients, and mail clients.

- ✔ **Layer 6, Presentation:** The Presentation layer is concerned with data representation and code formatting.

- ✔ **Layer 5, Session:** The Session layer establishes, maintains, and manages the communication session between computers.

- ✔ **Layer 4, Transport:** The functions defined in the Transport layer take care of reliable transmission of data segments, as well as the disassembly and assembly of the data before and after transmission.

- ✔ **Layer 3, Network:** The Network layer is where routing takes place. As a result, this layer is perhaps the most important OSI layer for to know. We may even rename this book *OSI Model Level 3 Jobs For Dummies* (or not).

- ✔ **Layer 2, Data Link:** The Data Link layer is concerned with the mechanisms used to move data about the network, such as Ethernet, and deals with the ways in which data is reliably transmitted.

- ✔ **Layer 1, Physical:** The Physical layer defines the electrical and physical specifications for the networking media that carry the data bits across a network. Think of this layer as referring to copper, fiber optic, and wireless.

The 7-layer OSI model is imperfect. Many manufacturers develop products that touch on multiple layers. However, nothing beats this model for communicating a conceptual understanding of networks.

Exalting TCP/IP

Almost as pervasive as the OSI 7-layer model is the use of TCP/IP in networking equipment. It has become the universal solvent for all problems networking. Developed in the 1970s as a robust military communications network that had some self-healing properties and resilience, *TCP/IP* has formed the basis for virtually every home, business, and commercial network, as well as the global Internet itself.

TCP/IP is a packet-based technology in which messages are bundled into *packets* that are *routed* to their destinations. A single packet has a source address,

a destination address, a protocol number, and a payload (the contents of a message). Figure 3-2 shows how TCP/IP maps to the OSI 7-layer model.

OSI 7-Layer Model   TCP/IP Model

Application	↔	
Presentation	↔	Application
Session	↔	
Transport	↔	Transport
Network	↔	Internet
Data Link	↔	Network Access
Physical	↔	
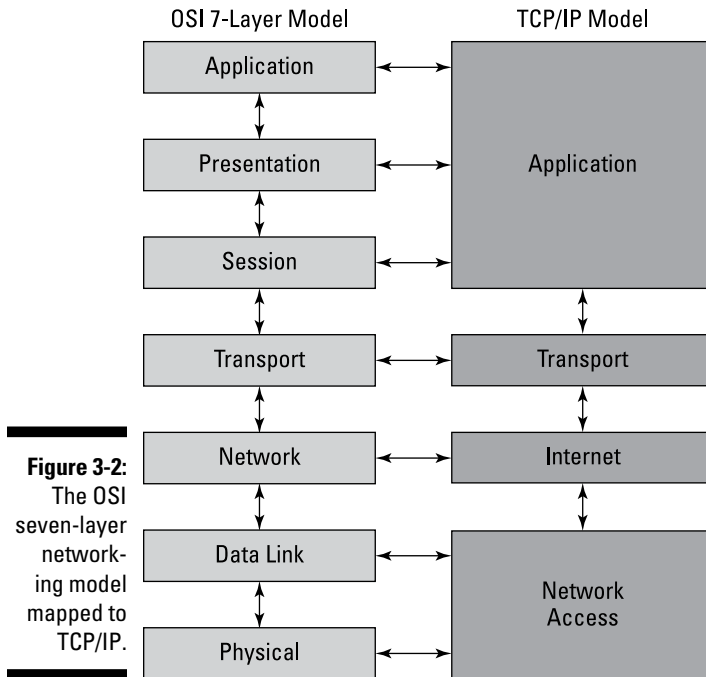
Figure 3-2: The OSI seven-layer networking model mapped to TCP/IP.

Staying Local with LANs

As long as you stay within your own property, you can network using LANs. As a rule, LAN technology is much cheaper and faster than WAN technology. An organization needs to use WAN technology when it must connect two LANs across some public right-of-way such as a street or a river.

The largest property under one fence in the United States is the Waggoner Ranch in northwest Texas. Ignoring propagation issues, the half million acres (about two-thirds the size of Rhode Island) could all be on one LAN. The instant they want to communicate with the bunkhouse in nearby Vernon, TX, however, they need to use WAN technology. That is just the way things work.

Using wired LANs

With some exceptions we discuss later in the chapter, pretty much every wired LAN is a variation of Ethernet. Four kinds of hardware elements are part of Ethernet data networking:

✔ **Network interface card (NIC):** This card goes into a PC, laptop, or smartphone.

✔ **Hub:** The hub connects Ethernet cables from multiple devices so that they can all communicate. This simple, unintelligent connection option is economical, particularly for a small office or a home network.

✔ **Switch:** An Ethernet switch combines a hub with a little bit of intelligence. Whereas the hub has each NIC card listen to each message and determine whether or not the packet is meant for it, an Ethernet switch will figure out which PC the message is for and not bother every NIC card with every message.

✔ **Router:** The term *router* applies to a range of equipment to manage an Ethernet LAN and interact with WANs. These devices range in complexity from routers in a small home office up to carrier-class devices that control the universe (or at least the digital part of the universe).

Some manufacturers incorporate a wireless LAN access point into a router. Other manufacturers don't. It is easy to be confused.

Ethernet technology has the lion's share of the installed base of LANs. The different flavors of Ethernet are based on cable and nominal speed, as shown in Table 3-1.

Table 3-1	Ethernet Speeds	
Ethernet Name	*Cable Connector*	*Nominal Speed*
Ethernet	10BASE-T	10 Mbit/s
Fast Ethernet	100BASE-TX	100 Mbit/s
Gigabit Ethernet	1000BASE-T	1 Gbit/s
10-gigabit Ethernet	10GBASE-X	10 Gbit/s
40-gigabit Ethernet	40GBASE-X	40 Gbit/s
100-Gggabit Ethernet	100GBASE-X	100 Gbit/s

Although Table 3-1 looks straightforward, there are several opportunities for confusion. First, some people refer to the 10Mb per second local area network as Ethernet. Others refer to the technology that includes all the options in the table as Ethernet. Both are correct, but the terminology can be confusing.

To distinguish among them, many people refer to the cable connector, such as 10BASE-T. However, the cable connector is also called RJ-45. On top of that, the cable can be called Cat-5 or Cat-6 cable. The best advice is to ask for clarification on the Ethernet speed only if it matters.

Another source of confusion is the speed of the Ethernet. There are two reasons why Ethernet speed issues can get confusing. A cool feature of this technology is that it will "dumb itself down" to accommodate the slowest technology. For example, your router and wiring may accommodate Gigabit Ethernet. However, if the NIC can work with only 10Mb per second, the technology will operate at the slower speed. The problem is that the technology will never tell you that it is operating below what it's capable of. You have to know to ask. The 10/100/1000 specification indicates that the equipment is happy to work at any of those speeds and will default to the highest possible.

Another side of Ethernet speed is that 10Mb per second is the nominal speed. TCP/IP is chatty. By *chatty,* we mean that the respective ends of the connection spend a fair amount of time making sure that the other end is ready to receive the transmission, that it received the transmission correctly, and that it has finished sending. These tasks are important to ensuring an accurate transmission, but they require bandwidth. You, as a user, get only a percentage of the nominal speed. This topic is described in the next section.

Using non-Ethernet LANs

Ethernet LANs are the most common type of LAN. The hardware is inexpensive and readily available. Plus, many people know how to support it.

There are many options for non-Ethernet LANs. They are typically used in special applications, such as when exceptional security is required.

Token-ring LANs, for example, were heavily promoted by IBM in the 1980s. Eventually, IBM gave up and accepted that Ethernet had the dominant market share. As the name implies, a token-ring LAN has all PCs on a logical ring. The PCs on a given LAN ring are in communication with the PC that is logically to its left and to its right. When it receives the token from the PC to its right, it looks to see if that token has a message that belongs to it. If it does, it takes that message and hands off the token to the PC on its left. If the token does not have a message for that PC, it passes the token along with the message to the next PC on the left. This process happens very fast.

This architecture feels more reliable compared to the Ethernet, where all the PCs essentially repeat until a message is acknowledged.

Another alternative to Ethernet is Fiber Distributed Data Interface (FDDI). This technology operates at a nominal rate of 100 Mbit/s. Whereas Ethernet uses copper wire, FDDI employs fiber-optic cabling. In addition, each PC is connected back to the central router in a star topology. These two features make FDDI more secure than Ethernet. (Note, however, that some Ethernet LANs use fiber-optic cable.)

Moving around with wireless LANs

The benefits of wireless LANs have been understood for quite a while. Running cable to offices through walls is annoying. Also, workers want to take their laptops and smartphones to meetings and still get emails and access to applications.

Wireless LANs did not gain popularity until the last decade or so. The first standard that caught on was 802.11, announced in 1997 by the Institute of Electrical and Electronics Engineers (IEEE) workgroup on wireless LANs.

The common term for 802.11 wireless LAN is Wi-Fi. This term is licensed by the Wi-Fi Alliance. The Wi-Fi Alliance picks up where the technical specifications leave off by providing a certification process to ensure that elements from competitive manufacturers work together.

This workgroup has since come out with new specifications that serve a wider area and add new frequency bands and, more importantly, higher data rates. The specifications and their nominal data rates are shown in Table 3-2.

Table 3-2		802.11 Specifications		
802.11 Protocol	*Year of Release*	*Nominal Data Rate (Mbit/s)*	*Indoor Range (ft)*	*Outdoor Range (ft)*
802.11	1997	2	66	330
802.11a	1999	54	115	390
802.11b	1999	11	115	460
802.11g	2003	54	125	460
802.11n	2009	72.2	230	820
802.11ac	2013	96.3	115	115

Note several things in this table. First, as with Ethernet, the elements in the system automatically adjust to the fastest protocol. You may put in an 802.11ac system, but if the laptop operates at only 802.11a, the protocol uses is 802.11a, which will limit the speed. Unless you check, you never know the speed at which a given laptop is connecting.

Also, the speed mentioned is at optimal conditions. Your mileage may vary — a lot. Wireless communications are fickle; one moment you may be crawling down the highway and the next you may be screaming down it.

The distance from the antenna is a big factor in the speed that a user will see. Table 3-2 shows the maximum distance at which the given protocol is designed to operate if there is a line of sight between the antenna and the device. This value is approximate and changes in real time. One solution for offering more complete coverage and avoiding dead spots is to put out multiple access points to serve a particular office space. Multiple access points work up to a point. It would take an entire *Dummies* book to cover all options and strategies for addressing coverage with wireless LANs.

Although wireless LAN coverage is important, security is more of an issue. Wireless LANs might seem like a security problem waiting to happen. However, a properly implemented wireless LAN can be more secure than some copper wire LANs. The key phrase in that last sentence is *properly implemented.*

A wireless LAN in an organization as well as in a home should be password-protected. Leaving a wireless LAN unprotected is an invitation for trouble. Some bad people make a habit out of walking around looking for unprotected LANs. They may just use some of your service when you want to use it. More likely, these will try to access your LAN and steal credit card and bank account numbers. Most systems allow you to enter a password once to access Wi-Fi. The password is then stored on your PC or smartphone for when you want to get on the LAN in the future.

Going Out with WANs

As mentioned in the section on LANs, the minute users step off the Waggoner Ranch onto route 183, they must connect to a WAN and not a LAN if they want to connect to the computers on the ranch. Historically, the easiest way to connect from here to there has been a dial-up circuit over telephone lines using a modem.

The first modem, the Bell 101, transmitted data at 110 bits per second. This speed was far superior to what a skilled Morse code operator could deliver

(20 bps) and was comparable to what a skilled typist could key in a Teletype machine (50 bps).

Even better, the pair of Bell 101 modems would also be on duty at all times, never needing a vacation or a break. For an investment of a few thousand dollars, you could avoid paying a human operator $2 per hour.

Modems added intelligence over the years, so that from the early 1960s to the late 1990s, they could eke out up to 56kbps from a single phone line. This is the greatest speed you can practically get from a single phone line, called a DS-0 in telephone lingo.

Speeds available on a DS-0 and below are called *narrowband*. Anything above DS-0 is *broadband*. These days, we think of narrowband as quaint. Broadband signals available from service carriers include DS-1, T-1, E-1, DSL, SONET, DOCSIS, MPLS, and dark fiber. (For details on these, see Chapter 3.) Older technologies you don't need to be too concerned with anymore (unless you're a technology history buff) include ISDN, ATM, Frame Relay, X.25, and PSTN.

Buying service from LECs and CLECs

Many data connection services are available from your local phone company. The "local phone company" refers to the company that used to have a monopoly in your particular area. Until the last few decades, some telecommunications companies were given exclusive rights to provide phone and other WAN services in a particular region, such as a city or a specified unincorporated area.

The deal, forced primarily by the Federal Communications Commission (FCC), was that local phone companies would provide local voice telephone service, and other companies would provide long-distance services. The local phone company in your area was called a local exchange company (LEC).

To make a long story short, the LECs wanted to get into providing long-distance voice service. The deal struck enabled existing LECs to offer long-distance services if they allowed other companies to provide local phone service. These were called competitive LECs (CLECs).

Some CLECs ran copper wires to provide service in areas with significant new construction. This practice was the exception rather than the rule. For the most part, CLECs carried high-capacity fiber-optic cable and would provide services to large building and corporate campuses.

Considering the cloud and managed service

An organization can buy individual links to connect the main office to a remote office. These can come from either a LEC or a CLEC. Another option is to buy networking services from a company that specializes in this area.

It is common practice to contract with an Internet service provider to provide Internet connectivity for organizational use and for web hosting. The extreme case of outsourcing network services involves relying upon the cloud. At this point, the only network access you need is a large pipe for Internet access. The cloud provider manages all server storage and security access. The use of cloud-based services is a viable strategy for startups.

Many LECs and CLECs offer managed networking services for their clients. Several IT companies, such as IBM, HP, and Level 3 Communications, provide this kind of service for organizations.

Accessing Wireless WANs

Unlike wired service, wireless WAN access is available from many sources. The largest providers these days are cellular carriers. In addition, you can get your own microwave connection, satellite service, or private radio.

Going beyond texting on a cellphone

Not too long ago, cellular carriers realized that you could send data over their cellular networks. A few pioneering souls back in the mid-1990s connected special modems to their cellphones. The cellular carriers found that these customers used three or four times as much airtime, never called for customer service, and did not switch their service to save a few pennies.

As a result, cellular carriers went on a competitive binge to offer faster service in more places. These new offerings were great because we all received faster service at a lower cost. However, all these new names and claims were confusing, with all kinds of acronyms and marketing hyperbole.

The different cellular companies would all claim that their network was the best and the fastest. They would claim that their network was 1G, or 2G, or 3G. They never explained that 1G meant first generation, 2G meant second generation, and so on.

They were also comparing apples and oranges. Sprint, Verizon, and US Cellular use a digital technology for voice called CDMA. AT&T and T-Mobile use a digital technology for voice call GSM. 2G technology on CDMA is different than the 2G technology on GSM.

Moreover, whether the user is stationary, moving (as in walking), or driving makes a significant difference in data throughput. This factor was conveniently left out of the advertising copy. The Radio Section of the International Telecommunications Union (ITU) says that 3G should be up to 7.2 Mbps. They also said that 4G should be 1Gbps when stationary and 100Mbps when moving.

However, ITU does not officially own the term 4G, plus other requirements are not met. The bottom line is that cellular carriers can call whatever they want 3G or 4G and get away with it.

What is more important is whether or not you are in coverage. The concept of coverage is easy to understand when dealing with voice service but less obvious when we are talking about data.

Ignore whatever *G* the carrier is telling you they have and pay attention to their coverage.

Cooking with a microwave connection

No, we aren't talking about cooking in the literal sense. We are talking about microwave communications. If you have to connect to buildings across the street, you may be surprised how economical and convenient it is to set up a point-to-point microwave system. As long as you have line-of-sight from point A to point B, many companies will put up microwave systems that are more economical over the long run than buying ongoing service from a LEC or CLEC.

Microwave is a telecommunications technology that has been used since World War II. Telecommunications companies have provided service between switching center offices for decades. About one third of the millions of miles of lines managed by LECs are provided by microwave.

Point-to-point microwave communication has several gotchas. First, you have to have line of sight from point A to point B. Next, you need access to the roof, which can be complicated if you are a renter, or you need to "shoot" through windows, which reduces your range. If these are not big issues, you should consider microwave as an alternative or a complement to service from the LEC.

Another option for microwave communication is WiMAX (Worldwide Interoperability for Microwave Access), which is a technology used by the Clearwire network.

WiMAX is a wireless telecom standard that provides data rates up to 40Mbps for mobile stations and 1Gbps for fixed stations. WiMAX was developed to be a wireless alternative to DSL and DOCSIS.

Clearwire offer service in 17 markets in the United States and is targeted to small businesses and fixed wireless applications.

Circling around satellite communications

Satellite communications seemed exotic at one time. These days, almost anyone can acquire television service from DirecTV or Dish Network and install his or her own satellite receiver.

The data-only equivalent satellite TV service is called VSAT, or Very Small Aperture Terminal. Depending on the service you acquire, you can get uploads and downloads in the narrowband or broadband range.

There are a few important considerations when considering VSAT service. First, VSAT terminals have a longer latency than ground-based systems. Regardless of the volume of data and the rate of speed on the network, it takes a few seconds to get everything flowing. This factor is not an issue for some applications and a showstopper for others. If you want to send and receive large files, the delay is not a problem. If you're doing lots of short transactions, the delays may drive users batty.

Another consideration is that VSATs are good at sending large files to a remote site, but are much more limited sending files from the remote site back up to the satellite. Again, slow upload speed is either a big problem or no problem depending on your circumstances.

VSAT excels in providing a backup to landlines. Landline service can fail, for example, when a backhoe rips up communications cables. A backhoe can't rip up communications between a satellite and the ground station antennae.

Chapter 4

Networking Concepts and Trends

. . . .

. . . .

*T*o successfully begin and navigate a career in networking, you need to understand a great deal about how various aspects of computing and networking technologies work. You don't need to understand everything in this chapter on day one, but the more you do know about the concepts behind the technologies, the easier it will be to learning more and do more as you increase your expertise and advance in networking.

Access Control

At its heart, access control is all about who (or what) is allowed to access something. In business, users are required to identify themselves — and prove their identity — before they can use workstations and applications. This section explains the concepts behind access control.

Basic concepts in access control

The basics of access control can be divided into two major categories:

✔ Authentication: the technology that facilitates access to systems, data, and workspaces

✔ Business processes used to manage access

Common terms in access control

access review	phishing
accumulation of privileges	rainbow table
authentication	replay attack
biometrics	salting
FTP, FTPS, and SFTP	session hijacking
hashing	single-factor authentication
key logger	social engineering
multifactor authentication	telnet
password	token
password quality	user ID
password recovery	watering hole attack

Authentication

Authentication is the process of asserting one's identity — including required proof such as a password, token, or biometric — to a system to access its resources. The identity takes the form of a *user ID,* which is a value assigned to a person or machine.

Single-factor authentication generally involves the presentation of a *user ID* and a *password*. This common form of authentication is more vulnerable to attack by adversaries due to its simplicity. The phrase "what you know" is associated with single-factor authentication because in this simplest form of authentication, the user has identified herself by presenting her user ID. The user then authenticates by stating something that she knows which is tied to her user ID (such as the current password).

A *password* is a secret word, phrase, or random characters used as a part of single-factor authentication. The quality of the password is an important factor that helps resist some forms of attack. Characteristics of password quality include length (how many characters), complexity (whether the password must contain lowercase letters, uppercase letters, numerals, and special characters), expiration (how much time may elapse before a user is required to select a new password), recovery (the process to follow when users forget their password), and reuse (whether previously used passwords may be used again).

What you know, have, and are

The concepts in single-factor and multifactor authentication are sometimes difficult to understand. Three phrases are often used to simplify these concepts:

✔ **What you know:** User ID and password authentication. The user ID and password are something that a user would know.

✔ **What you have:** Token or smart card authentication. The user must have the physical object (and use it properly) to log in.

✔ **What you are:** Biometric authentication. This refers to some physical aspect of a user, such as a fingerprint, retina scan, or even voiceprint.

Passwords are typically stored in hashed form. *Hashing* is an irreversible cryptographic function that creates a large number representing the password without exposing the password. The hash value then facilitates the confirmation of a correct password during the login process but prevents the extraction of passwords. Hashing is explained in more detail in the "Cryptography" section, later in the chapter.

Multifactor authentication generally involves the presentation of a user ID, a password, and a token or biometric. This type of authentication is generally stronger than single-factor authentication. A *token* is a hardware device (or sometimes a smartphone application) that is used in multifactor authentication and represents a far stronger form of authentication than single factor Multifactor authentication can also use some form of biometric, such as a fingerprint, a palm scan, an iris scan, or a voiceprint The phrase "what you are" is associated with biometric authentication because you're using a part of your body to authenticate your presented identification.

Access control processes

Getting access control technology right is a challenge, but it's not the biggest concern. The business processes supporting access controls are critical. If not implemented and managed correctly, the best access control technology is of little use — similar to owning a car with the best burglar alarm and then parking the car unlocked with the keys in the ignition switch.

Key processes in access control are collectively known as *identity access management* (IAM) and include the following:

✔ **Access provisioning:** The process of provisioning access for a user should follow a strict, documented process. Every request should be properly approved by one person or group and performed by a different person or group. Records for all steps must be retained.

✔ **Internal transfers:** Access management personnel need to be notified when an employee is transferred to another position to prevent an accumulation of privileges.

✔ **Employee termination:** Access management personnel need to be notified immediately when an employee leaves the organization, especially if the person is being terminated. All user accounts should be locked or removed and then double-checked.

✔ **Managing access controls for contractors, temps, and others:** All personnel with access to organization systems and applications should be managed using the same set of processes. When an organization does a substandard job of managing temporary workers, user accounts may exist for people who no longer work in the organization.

✔ **Password recovery:** Organizations need a solid process for users who forget their passwords. Otherwise, attackers may be able to use this process to take over an employee's user account.

✔ **Periodic access reviews:** Every aspect of access management must be periodically reviewed to ensure that each instance of access provisioning, termination, and transfers is performed correctly. Ineffective access control processes can result in active user accounts with excessive privileges and user accounts associated with terminated personnel.

Access control attacks and countermeasures

Adversaries who are attempting to access resources in a target system frequently attack access controls. Methods of attack include the following:

✔ **Replay attack:** An attacker intercepts an authentication, typically over a network, and replays the captured login credentials to try to gain unauthorized access to the target system. A replay attack can be successful even when some forms of token authentication are used, provided the attacker replays the captured login credentials soon after capturing them.

✔ **Stealing password hashes:** The attacker obtains the database of hashed passwords from a system. If the hashing method is weak, the attacker may be able to employ rainbow tables or other techniques to obtain account passwords. A *rainbow table* is a simple but very large lookup table containing all possible password hashes and their corresponding passwords. The technique known as *salting* (mixing in random numbers when storing the hash of a new password) prevents the use of rainbow tables.

✔ **Interception of passwords in transit:** An attacker may be able to intercept login credentials if they are transmitted "in the clear"

(unencrypted) over a network. Older but still-used protocols such as Telnet and FTP (File Transfer Protocol) employ the transmission of login credentials without encryption. This threat is eliminated if you discontinue Telnet and FTP in favor of ssh (Secure SHell), FTPS (File Transfer Protocol Secure), and SFTP (Secure File Transfer Protocol).

✔ **Session hijacking:** An attacker attempts to steal session cookies from a user's web session; if successful, the attacker will be able to hijack the user's session. The attacker may then be able to perform all functions that the user could perform. Session hijacking can be prevented with proper session management, including full session encryption and encryption of session cookies.

✔ **Key logger:** An adversary may be able to use one of several methods to get key logger malware installed on a user's system. If successful, the key logger will be able to intercept typed login credentials and transmit them to the adversary, who can use them later to access those same systems. Multifactor authentication and advanced malware prevention (AMP) tools can help thwart key loggers.

✔ **Social engineering:** Adversaries have a number of techniques available to trick users into providing their login credentials. Techniques include

- **Phishing:** The attacker sends an email that attempts to trick the user into clicking a link that takes the user to a *phishing site,* which is an imposter site used to request login credentials. If the user provides those credentials, the attacker can use them to access the real site.

- **Watering hole attack:** An attacker selects a website that he or she believes is frequented by targeted users. The attacker attacks the website and plants malware on the site that can, if successful, install a key logger or other malware on the victim's workstation.

Emerging issues in access control

Issues that keep networking professionals up at night include these:

✔ Key logging malware

✔ Stolen password hashes

✔ Users who select poor (easily guessed) passwords

✔ Users who reuse personal passwords on business sites

Telecommunications and Network Security

Networks are the lifeblood of every organization that utilizes computing in support of business processes. There's a lot to know about internal network technologies such as TCP/IP, Ethernet, and Wi-Fi. It's important that you also understand telecommunications technologies, including synchronous optical networks (SONET), multiprotocol label switching (MPLS), and wireless technologies such as WiMAX and LTE.

Understanding the security aspects of networking is vital as well. It's not just the security manager's job to protect networks — it's a networking professional job as well.

Basic concepts in telecommunications and network security

You need to understand the important concept of encapsulation because it is used throughout almost all network technologies. In *encapsulation,* messages of one protocol are placed in messages of another protocol. For example, SMTP (Simple Mail Transport Protocol) messages are placed in TCP (Transmission Control Protocol) datagrams, which are placed in IP (Internet Protocol) messages, which are placed in DS-1 frames, which are placed in OC-48 frames.

Here's an analogy. You write a message on a sheet of paper (SMTP message), place it in an envelope (TCP message), and place the envelope in a mailbox (IP message), where a mail truck (switch) picks it up and delivers it to a distribution center (router). There, the envelope (TCP message) is placed in a bin (IP message), which is driven to another distribution center (router). There, the bin (IP message) is placed in a larger bin (DS-1 frame) and driven to an airport (DACS), where the larger bin (DS-1 frame) is placed on an airplane (OC-48 frame) that flies through the air (optical fiber). At the other end of the flight, the process is reversed, and the recipient receives the note on the sheet of paper.

Network technologies

A plethora of network technologies exist; we discuss the important ones in this section.

Common terms in telecommunications and network security

ATM	IP address	routing table
CAT-6 cable	IPS	SONET
denial of service	ISDN	T-1
DLP	MAC address	TCP/IP
DMZ	MPLS	VoIP
DOCSIS	packet header	VPN
DS-1	payload	watering hole attack
E-1	POTS	WEP
encapsulation	PSTN	WiMAX
firewall	QoS	WPA
frame relay	router	WPA2

Wired telecom network technologies

Wired telecom networks connect homes, businesses, schools, and governments through technologies that use copper or fiber optic cabling to carry many types of signals. These signals include the following:

- **DS-1 (Digital Signal one), T-1, E-1:** *DS-1* is a family of multiplexed telecommunications technologies that have carried voice and data for decades in the United States and Europe. In the United States, *T-1,* which runs at 1.544Mbps, is the basic protocol. It's often multiplexed into 24 64Kbps voice channels for use by ordinary phone and fax lines, often known as *POTS (plain old telephone service).* In Europe, *E-1* is the basic protocol, at 2.048bps, or 32 voice channels. Speeds higher than DS-1 are available, such as DS-3 (44.736Mbps), DS-4 (274.176Mbps), and DS-5 (400.352Mbps).

- **SONET (Synchronous Optical Networking):** This new high-speed telecommunications backbone technology runs over fiber optic cables on land and in submarine cables. SONET runs at dizzying speeds, including OC-1 (48.960Mbps), OC-3 (150.336Mbps), OC-12 (601.344Mbps), OC-96 (4,810.752Mbps), and OC-192 (9,621.504Mbps).

- **DSL (Digital Subscriber Line):** This family of protocols is delivered to homes and businesses over the same pairs of copper wires as telephone service but at a higher frequency.

✔ **DOCSIS (Data Over Cable Service Interface Specification):** This family of technologies transports TCP/IP over cable television service to homes and businesses.

✔ **MPLS (MultiProtocol Label Switching):** This packet-switched technology transports a variety of protocols such as TCP/IP, Ethernet, ATM, and VoIP over long distances. MPLS includes Quality of Service (QoS) settings to ensure that protocols such as voice and streaming video are transported without annoying interruption even when networks are congested.

✔ **Dark fiber:** This option is not a technology but a telecommunications medium available to businesses. Businesses can connect their own telecom equipment to fiber optic cabling to connect their networks between buildings in a city or metropolitan area, using any protocol they want.

Older technologies you don't need to be too concerned with anymore (unless you're a technology history buff) include ISDN, ATM, frame relay, X.25, and PSTN.

Wireless telecom network technologies

Wireless telecom networks connect individuals, homes, and businesses through the use of several technologies, including the following:

✔ **GPRS (General Packet Radio Service):** This technology is encapsulated in the GSM (Global System for Mobile communications, originally *Groupe Spécial Mobile*) cellular protocol.

✔ **LTE (Long Term Evolution):** This wireless telecom standard provides voice and data service with speeds up to 300Mbps.

✔ **WiMAX (Worldwide Interoperability for Microwave Access):** A wireless telecom standard that provides data rates up to 40Mbps for mobile stations and 1Gbps for fixed stations, WiMAX was developed as a wireless alternative to DSL and DOCSIS.

Other notable technologies include CDPD, CDMA, and packet radio.

Wired consumer and business network technologies

Although many standards have been used for wired network technologies, the long-term trend has been a general migration to TCP/IP on Ethernet over copper cabling or fiber optic cabling. The dominant technologies follow:

✔ **CAT-6 (Category 6) cabling:** The darling of homes and businesses running wired networks over distances of up to 100 meters, CAT-6 cabling can run Ethernet speeds up to 10Gbps.

> ✔ **Fiber optics:** Businesses often run fiber optics in larger buildings to connect networks from floor to floor, as well as from building to building. Fiber-optic cabling is made of glass and transmits signals as visible light, as opposed to CAT-6 and other metallic cabling, which transmit data as electrical signals.

Has-been cabling used in the past include Thinnet, Thicknet, Cat-3, and Cat-5.

Wireless consumer and business network technologies

Wireless network technologies are wildly popular in a number of typical settings. The technologies in use are

> ✔ **Wi-Fi:** The IEEE 802.11 family of wireless protocols are widely used in small and large residences, businesses, retail stores, restaurants, government buildings, and even outdoors. A variety of security protocols are used on Wi-Fi, ranging from none (no encryption), *WEP* (Wired Equivalency Protocol, considered obsolete), *WPA* (Wireless Protected Access, which is just okay), and *WPA2* (preferred by anyone thinking about security). The range of Wi-Fi is about 20 meters indoors and farther outdoors.
>
> ✔ **Bluetooth:** This popular wireless protocol connects devices in close proximity. Wireless earsets and headsets were the first popular use of Bluetooth.
>
> ✔ **NFC (Near Field Communications):** This very short-range (6 cm) wireless protocol was developed for use in contactless payment systems.

Runner-ups include *iRDA* (the infrared point-to-point technology, which has all but disappeared) and *wireless USB* (up and coming, and possibly a force in the future).

Software-defined networking (SDN)

Software-defined networking is an emerging technology that is simplifying network architectures and helping to reduce costs. Instead of purchasing a lot of separate specialized network devices such as load balancers, web application firewalls, intrusion prevention systems, routers, and switches, organizations can purchase a few OpenFlow-enabled switches and a centralized controller, and then build a network fabric that exists virtually in the switch, performing all those functions in harmony instead separately.

As of this writing, 90 percent of IT workers (including a lot of senior-level people) don't understand SDN, so you should consider this a ground-floor opportunity. If you're fortunate enough to get some SDN training or work alongside someone who is doing SDN, stay with it as long as you can.

TCP/IP

Developed in the 1970s as a robust military communications network that had some self-healing properties and resilience, *TCP/IP* has formed the basis for virtually every home, business, and commercial network, as well as the global Internet itself.

TCP/IP is a packet-based technology in which messages are bundled into *packets* that are *routed* to their destinations. A single packet has a source address, a destination address, a protocol number, and payload (the contents of a message).

TCP/IP addressing

The source address and destination address follow a numbering convention, with a global authority that assigns addresses to organizations. In TCP/IP version 4, the form of an address is

```
xxx.xxx.xxx.xxx
```

where each *xxx (octet)* is commonly portrayed as a decimal value and can range from 1 through 255. In TCP/IP version 6, the form of an address is

```
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
```

where each *xxxx (hextet)* is a hexadecimal value that can range from 0000 through FFFF.

TCP/IP routing

In TCP/IP, routers process packets as they make their way from their source to their destination. Think of a router as a traffic cop in a street intersection who tells you which way to turn. A *router* examines a packet's destination address, consults its routing table, and then sends the packet in the correct direction to get it closer to its ultimate destination.

Routers exchange routing information so that each router has a better idea about which direction to send each packet. They exchange this information through several routing protocols, such as RIP, BGP, IGRP, OSPF, or IS-IS. These routing protocols each have best uses; some are used by Internet backbone routers, and others are better suited for routers inside a company. Some become obsolete as newer and better ones are developed.

TCP/IP protocols

TCP/IP has two basic protocols, on top of which nearly all the others are used through encapsulation (the nesting process explained earlier). These two basic protocols are

- ✔ **UDP:** Formally known as *User Datagram Protocol*, UDP is a simple connectionless protocol typically used to send a message in a single packet.

- ✔ **TCP (Transmission Control Protocol):** This connection-oriented protocol is usually intended for a longer conversation between systems. A TCP session is established by something called a three-way handshake, which works something like this:

```
Station A: Hello, I'm Station A and I'd like to talk
          to you, Station B.
Station B: Hello, I'm Station B and yes I'd like to
          talk to you, Station A.
Station A: Hello Station B, I'm happy we have agreed
          to talk to each other.
```

The TCP and UDP protocols contain hundreds of established protocol standards, a few of which are well known and frequently used, such as

- ✔ **HTTP (HyperText Transport Protocol):** Using port 80, transports user web traffic without encryption.

- ✔ **HTTPS (HyperText Transport Protocol Secure):** Using port 443, transports web traffic with encryption.

- ✔ **SMTP (Simple Mail Transport Protocol):** Using port 25, transports email without encryption.

- ✔ **DNS (Domain Name Service) protocol:** Using port 43 (on both TCP and UDP services), translates domain names such as *www.dummies.com* into IP addresses.

- ✔ **FTP (File Transfer Protocol):** Using ports 20 and 21, enables bulk file transfers without encryption.

- ✔ **SSH (Secure SHell) protocol:** Using port 22, provides administrative access to systems and network devices.

TIP

To understand concepts such as encapsulation, you should become familiar with the OSI Network Model.

Network security

Several network-centric security devices protect systems, networks, and information from intruders. We describe the more common types in this section.

Firewalls

Firewalls are inline devices placed between networks to control the traffic that is allowed to pass between those networks. Typically, an organization

places a firewall at its Internet boundary to prevent intruders from easily accessing the organization's internal networks.

A firewall uses a table of rules to determine whether or not a packet should be permitted. The rules are based on the packet's source address, destination address, and protocol number. Firewalls do not examine the contents of a message.

Firewalls are used to create a demilitarized zone (*DMZ*), which is half inside and half outside the networks in which organizations place Internet-facing systems such as web servers. This strategy helps protect the web server from the Internet and protects the organization in case an adversary compromises and takes over control of the web server. Figure 4-1 depicts a typical DMZ network.

Intrusion prevention system (IPS)

An *intrusion prevention system (IPS)* is an inline device that examines incoming and outgoing network traffic, looking for signs of intrusions and blocking such traffic when it detects an intrusion.

Unlike a firewall, an IPS examines the contents of network packets, not just their source and destination addresses. This approach is based on the principle that malicious traffic may be characterized by its contents, not merely its origin or destination.
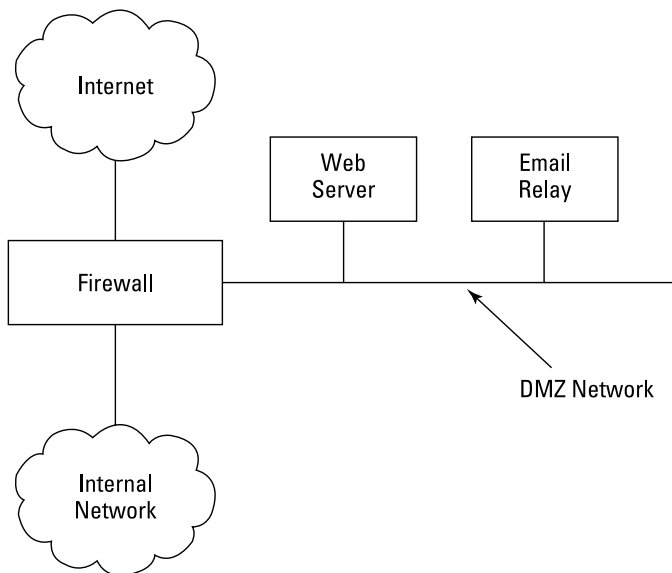

Figure 4-1:
Typical DMZ network architecture.

Like a firewall, an IPS is typically placed at or near Internet entrance and exit points, so that all Internet incoming and outgoing traffic, respectively, can be examined and any malicious traffic blocked.

Data loss prevention (DLP) system

A *data loss prevention (DLP) system* primarily examines outgoing traffic, looking for evidence of sensitive data being sent out of the organization inappropriately. A DLP system is configured to look for specific patterns in outgoing data and to send alerts or just block traffic meeting certain criteria.

Web-filtering system

A *web-filtering system* examines the websites that an organization's personnel are visiting. The web-filtering system logs all web access by personnel and can also be configured to block access to various categories of websites (for example, pornography, gambling, weapons, or social media sites) as well as specific sites. The purpose for web-filtering systems is generally twofold: to prevent access to sites that are clearly not work related and to protect the organization from accessing sites that may be hosting malware.

Virtual private network

A *virtual private network (VPN)* is a technique used to encapsulate network traffic flowing between two systems, between a system and a network, or between two networks. Typically, encryption is employed along with encapsulation so that the contents of the traffic cannot be read by anyone who intercepts the traffic.

VPNs are most commonly used for remote access, as well as to protect information flowing over the Internet between specific organizations.

Attacks and countermeasures

Intruders are incredibly efficient at finding ways to break into an organization's networks. They do so to steal valuable data that they can easily monetize. The techniques used and the defensive countermeasures include the following:

- ✔ **Phishing:** Adversaries compose realistic-looking emails to trick users into clicking links to *phishing sites,* which are malicious sites that will attempt to install malware on victims' workstations or steal login credentials. Countermeasures include spam filters, antimalware, intrusion prevention systems, and security awareness training.

✔ **Watering hole attack:** Adversaries find websites that they think an organization they're targeting might visit. They take over those websites and install malicious software that visitors will unknowingly install, leading to an intrusion. Countermeasures include web-filtering systems, antimalware, and intrusion prevention systems.

✔ **Denial of service attack:** Adversaries will attack a target system to incapacitate it, through either a high volume flood of data or malicious traffic designed to incapacitate the target system. Countermeasures include firewalls, intrusion prevention systems, and cloud-based denial-of-service defense services.

Emerging issues in telecommunications and network security

New developments that keep networking professionals on edge include the following:

✔ **The Internet of Things (IoT):** Many new devices are being connected to the Internet, and we all know that many of them do not have well-implemented security. The Internet of Things in the business environment includes accessing and controlling manufacturing equipment, tracking the performance and location of company trucks, tracking use of utilities, such as water and lighting, and medical monitors. The race is to implement the solution, and worry about security later.

✔ **BYOD (bring your own device):** Network interoperability and the proliferation of powerful consumer devices such as iPhone and Android mean that millions of workers are using their personal devices at work as work tools. Personally owned devices in a business network result in a wide range of issues, including malware control and data control.

✔ **IPv6:** The shortage of available IP addresses and other issues are compelling organizations to migrate to IPv6. Although iPv6 is more secure by design, few network and security professionals are as familiar with IPv6 as they are with IPv4. Implementing IPv6 can lead to security holes through improper configuration.

Cryptography

Cryptography is the art and science of hiding data in plain sight, and plays a key role in protecting data from onlookers and adversaries. In this section, you examine this mysterious craft and discover how it's used to protect sensitive data.

Cryptography terms

block cipher	encryption	plaintext
certificate authority (CA)	encryption algorithm	pseudorandom number generator
ciphertext	encryption key	public key cryptography
cryptanalysis	hashing	steganography
cryptosystem	key management	stream cipher
decryption key	key length	watermarking
digital certificate	message digest	
digital signature	nonrepudiation	

Although cryptography is often used as part of a complex system, it's often easier to think of cryptography in isolation, in the simple-use case of a message sent in plain sight from a sender to a receiver.

Basic concepts in cryptography

Encryption is the process of transforming plaintext into ciphertext through an encryption algorithm and an encryption key. *Decryption* is the process of transforming ciphertext back into plaintext, again with an encryption algorithm and the encryption key. In part, the strength of encryption is based on the *key length* (the number of characters that make up the encryption key) and the complexity of the encryption key.

An implementation of encryption and encryption keys is known as a *cryptosystem*. An attack on a cryptosystem is called *cryptanalysis*.

Most encryption algorithms employ a pseudorandom-number generator (PRNG), which is a technique for deriving a random number for use during encryption and decryption.

Types of encryption

The two basic ways to encrypt data are by block cipher and by stream cipher. Details follow:

✔ **Block cipher:** A *block cipher* encrypts and decrypts data in batches, or blocks. Block ciphers are prevalent on computers and on the Internet,

where they encrypt hard drives and thumb drives, and protect data in transit with SSL and TLS. Notable block ciphers are

- **Advanced Encryption Standard (AES):** Selected in 2001 by NIST (National Institute of Standards and Technology) to replace DES, AES is based on the Rijndael cipher and is in wide use today.

- **Data Encryption Standard (DES):** The leading official encryption standard in use from 1977 through the early 2000s. DES was considered obsolete mostly because of its short key lengths.

- **Triple DES (3DES):** Derived from DES, 3DES is essentially DES with a longer key length and, hence, more resistant to compromise than DES.

- **Blowfish:** Developed in 1993, Blowfish was developed as an alternative to DES, which was nearly twenty years old. Blowfish is unpatented and in the public domain.

- **Serpent:** Another public domain algorithm, Serpent was a finalist in the AES selection process.

✔ **Stream cipher:** A *stream cipher* encrypts a continuous stream of information such as a video feed or an audio conversation. The most common stream cipher is RC4.

Block ciphers are most often used to encrypt Internet-based streaming services. On the Internet, everything is transmitted in packets, which are individually encrypted using block ciphers.

Hashing, digital signatures, and digital certificates

Hashing is used to create a short fixed-length *message digest* from a file or block of data; this is something like a fingerprint: Message digests are unique and difficult to forge. Hashing is often used to verify the integrity of a file, or the originator of a file, or both. Common hashing algorithms include the following:

✔ **MD-5** is a formerly popular hashing algorithm developed in 1992. It is now considered too weak for reliable use and obsolete.

✔ **SHA-1** is another popular hashing algorithm that was determined in 2005 to be too weak for continued use. By 2010, U.S. government agencies were required to replace SHA-1 with SHA-2.

✔ **SHA-2** is a family of hashing algorithms: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256. These are all considered reliable for ongoing use.

A *digital signature* is a hashing operation carried out on a file. Depending on the implementation, the digital signature may be embedded in the file or separate. A digital signature is used to verify the originator of the file.

A *digital certificate* is an electronic document that consists of a personal or corporate identifier and a public encryption key, and is signed by a certificate authority (CA). The most common format for a digital certificate is X.509. The use of digital certificates and other tools such as strong authentication can lead to the failure for an individual to be able to plausibly deny involvement with a specific transaction or event. This process is known as *nonrepudiation*.

Encryption keys

The two main types of encryption keys in use today are

- ✔ **Symmetric key:** Both the sender and the receiver have the same encryption key.

- ✔ **Asymmetric key:** Also known as *public key cryptography,* utilizes a pair of encryption keys — a public key and a private key. A user who creates a keypair would make the public key available widely and protect the private key as vigorously as one would protect a symmetric key.

Private keys and symmetric keys must be jealously guarded from adversaries. Anyone who obtains a private or symmetric encryption key can decrypt any incoming encrypted message. The management and protection of encryption keys is known as *key management*.

Software programs often employ passwords to protect encryption keys. Hence, the strength of the cryptosystem is only as strong as the password protecting its keys.

Encryption alternatives

Two encryption alternatives provide some of the same features as a cryptosystem:

- ✔ **Steganography (stego):** A message is hidden in a larger file, such as an image file, a video, or sound file. Done properly, this technique can be as effective as encryption.

- ✔ **Watermarking:** A visible (or audible) imprint is added to a document, an image, a sound recording, or a video recording. Watermarking is a potentially powerful deterrent control because it indicates that some other party owns the object.

Emerging issues in cryptography

Encryption is not a magic sleeping pill. Instead, there are numerous worries ranging from new types of attacks to official government misbehavior. Let's take a look at what's keeping networking professionals awake at night.

- ✔ **Man-in-the-middle attacks:** Many attacks on cryptosystems involve a man-in-the-middle attack at the onset of a so-called secure communications session. Flaws in session initiation and key exchange can result in the attacker being able to easily read all encrypted communications between two endpoints.

- ✔ **Improper uses of cryptography:** Cryptography, like any tool, is useful when used properly. Used improperly, cryptography gives us a false sense of security. Two examples are failing to *salt* (mixing in random numbers when calculating the hash of a plaintext message) when hashing passwords and failing to adequately protect an encryption key.

- ✔ **Brute-force attacks:** Advances in distributed computing are making it easier for adversaries to build massive parallel computing machines to attack cryptosystems. A *brute-force attack* employs fast computers to guess every possible combination until the correct one is found. To stave off these attacks, key lengths are getting longer and longer. However, these longer key lengths require more computing power when performing legitimate encryption and decryption. It's a never-ending game of cat and mouse (in this case, we are the mouse).

- ✔ **Precompromised encryption algorithms:** In 2012–2013, revelations uncovered the plausibility that various government-spying organizations have been able to subvert the development or implementation or both of certain encryption algorithms and cryptosystems. The result is a serious crisis of trust in the cryptosystems used to protect sensitive information from adversaries.

- ✔ **Persistent use of compromised cryptosystems:** Encryption algorithms have a limited shelf life, after which some technique for compromising them is revealed.

Computing Architecture and Design

Every successful networking professional is familiar with the basics of computing architecture and design: how computers are architected internally, and the ways they are used, including virtualization and cloud computing. This is networking's bread and butter.

Common terms in computing architecture and design

bus	hypervisor	process
central processing unit (CPU)	infrastructure as a service	secondary storage
cloud computing	main storage	software as a service
dedicated public cloud	operating system (OS)	trusted platform module (TPM)
guest	platform as a service	virtualization
hybrid cloud	private cloud	

Basic concepts in computing architecture and design

Networking professionals must understand how computers are designed and how they function. This applies to computers used on-site and computers that are a part of cloud-based services.

Computer hardware architecture

Networking professionals need to understand how computer hardware functions, so that they can ensure that the hardware is properly managed and used. Modern computers are made up of the following components:

- ✔ **Central processing unit (CPU):** The component where computer instructions are executed and calculations performed.
- ✔ **Main storage:** The component where information is stored temporarily. Often known as RAM (random access memory), main storage is usually volatile and its contents lost if power is removed or the computer turned off.
- ✔ **Secondary storage:** The component — typically a hard drive or a solid-state drive (SSD) — where information is stored permanently. Information stored here is persistent even when the computer is switched off. Secondary storage is often organized into one or more *file systems*, which are schemes for the storage and retrieval of individual files.

✔ **Bus:** The component where data and instructions flow internally among the CPU, main storage, secondary storage, and externally through peripheral devices and communications adaptors. Popular bus architectures include SCSI (small computer systems interface) SATA (serial ATA), IEEE1394 (also known as FireWire), and USB (universal serial bus).

✔ **Firmware:** Software stored in persistent memory, generally used to store initial instructions that are executed when the computer is switched on.

✔ **Communications:** for Ethernet, Wi-Fi, or Bluetooth) and display adaptors (for computers with human interfaces). Most computers include one or more communication components — otherwise, how would you get problems into it and results out of it?

✔ **Security hardware:** Components for various security functions, such as a Trusted Platform Module (TPM), which is used to store and generate cryptographic keys, smart card readers, and fingerprint scanners. Some computers include specialized security hardware.

Computer operating system

A computer operating system (OS) consists of the set of programs that facilitate the operation of application programs and tools on computer hardware. The components of an OS include the kernel (the core software that communicates with the CPU, memory, and peripheral devices), device drivers (which facilitate the use of bus devices and peripheral devices), and tools (used by administrators to manage resources such as available disk space).

The main functions performed by an operating system are

✔ **Process management:** Processes are the individual programs that run on a computer. The OS starts and stops processes and makes sure they do not interfere with each other.

✔ **Resource management:** The OS allocates and manages the use of main storage, secondary storage, communications, and attached devices.

✔ **Access management:** The OS manages authentication as well as access to resources such as files and directories in secondary storage.

✔ **Event management:** The OS responds to events such as the insertion or removal of media and devices, keystrokes, or mouse movements.

✔ **Communications management:** The OS manages communications to ensure that incoming and outgoing communications are handled and routed properly.

An operating system can run directly on computer hardware or through a scheme called *virtualization,* in which many separate copies of operating systems can run simultaneously on a computer. In virtualization, the main

controlling program is called the *hypervisor*, and each running OS is called a *guest*. The hypervisor's jobs are to allocate computer hardware resources to each guest and to prevent guests from interfering with each other.

Virtualization permits an organization to make better use of its resources. Instead of running one operating system per server, multiple operating systems can run on each server, making better use of hardware investment and rack space.

With commercial virtualization tools, OS instances can be moved from one hardware platform to another (and even to one data center to another), and OS instances can be easily cloned to enable more running copies of a server if demand requires it.

Cloud services

The adoption of cloud services is in full swing despite the fact that many still don't understand how cloud services work. An organization using cloud computing has chosen to use computing or application resources that are owned by another organization and located away from the organization's premises.

The three common types of cloud services follow:

- ✔ **Infrastructure as a Service (IAAS):** Service providers enable customers to lease virtual machines, servers, storage, network functions, and so on. Examples include Amazon Web Services, Microsoft Azure, and Google Compute Engine (GCE).

- ✔ **Software as a Service (SAAS):** Service providers enable customers to use software applications managed by cloud service providers. Examples include Salesforce, Office365, and Cisco WebEx.

- ✔ **Platform as a Service (PAAS):** Service providers run application software with application programming interfaces (APIs) to which customers can connect their application. Examples include Engine Yard, Google App Engine, and Microsoft Azure Web Sites.

An organization can utilize cloud services in the following ways:

- ✔ **Public cloud:** An organization utilizes cloud services that are operated by and located at a cloud service provider's data center.

- ✔ **Private cloud:** An organization builds its own cloud computing infrastructure using hardware assets that it owns, and locates it in its own data center. An organization that builds a private cloud wants the logical capabilities of cloud computing but also wants to retain ownership and control of the hardware supporting it.

- ✔ **Hybrid cloud:** An organization utilizes a combination of public cloud services with its in-house resources. An organization that uses a hybrid cloud generally wants control of specific information or hardware assets.

- ✔ **Dedicated public cloud:** An organization utilizes public cloud services on hardware dedicated to that organization. An organization that uses dedicated public cloud wants the flexibility of cloud services but is unwilling to share infrastructure with other tenants.

Emerging issues in computing architecture and design

Issues that tend to keep networking professionals on their toes include:

- ✔ **Internet of Things (IoT):** We worry that insufficient work is put into developing sound security models and designs to prevent attacks in new Internet-connected products that.

- ✔ **Speed to market:** Many organizations, in attempts to get newly developed products to market more quickly, skip security designs, reviews, and controls, thereby leaving products open to attack.

- ✔ **Flawed access control:** Many organizations lack the skills to implement sound, effective access controls in their systems, resulting in unnecessary exposure of sensitive data.

IT Operations

IT operations is the heartbeat of organizations using computers and networks to support their key business processes. Many networking professionals begin their networking careers in IT operations; some spend their entire careers there.

The concepts in IT operations in this section follow the international standard called ITIL, or IT Infrastructure Library. To learn more about IT operations, get a copy of *ITIL For Dummies* by Peter Farenden.

Basic concepts in IT operations

Networking professionals spend their time working in one or more IT operations processes, which are summarized in this section.

Common terms in IT operations

antimalware	continuous monitoring	remote access
backup	data destruction	service desk
change management	help desk	vulnerability management
configuration management	incident management	

Change management

Change management is a basic IT operations process concerned with the management and control of changes made in IT systems. A proper change management process has formal steps of request, review, approval, execution, verification, and recordkeeping. The purpose of change control is the discussion of proposed changes before they take place, so that risks and other issues can surface.

All process and procedures, including those in incident management, vulnerability management, and change management, should be formally documented.

Configuration management

Configuration management is a basic IT operations process that is concerned with the management of configurations on servers, workstations, and network devices. Configuration management is closely related to change management. Whereas change management is involved with the process of performing the change, configuration management is involved with the preservation of present and prior configurations of each device and system.

Service desk

The *IT service (help) desk* is a central point of contact for users who require information or assistance. Users call or send a message asking for help with some matter concerning the use of a computer, network, program, or application.

In many organizations, IT service desk personnel are trained to assist with several common and easily remedied issues, such as forgotten passwords, simple support issues related to office productivity tools, accessing central resources such as file servers, and printing. When service desk personnel are unable to assist directly, they will refer the issue to a specialist who can offer more advanced assistance.

Most organizations utilize a ticketing system to track open issues, the time required to fix issues, and resources used. When used properly, a ticketing system can be a rich source of statistics related to the types of assistance that uses are requesting and the resources and time required to fix them.

Continuous monitoring

The velocity of harmful events has accelerated to a point where data review of incident logs is no longer an effective means of detecting unwanted behavior. Besides, the volume of available log data (gigabytes in the smallest organizations and terabytes in larger ones) is too great for humans to review.

Organizations must centralize their logging. All devices and systems should send their log data to a purpose-built central repository, called a security incident and event management (SIEM) system. But more than that, organizations need tools that not only detect serious security events but also alert key personnel and even remediate the incident in seconds instead of weeks or months as is often the case.

Backup

Hardware problems, software problems, and disasters of many kinds make organizations wish they had a backup copy of critical information. Most organizations routinely perform backups, where important data is copied to backup media or servers in some remote location.

Data destruction

When data is no longer needed, it must be effectively destroyed so that unauthorized parties can't recover it. Some companies pay little attention to this task, but others do a thorough job of data destruction. No, you won't get to smash obsolete printers out in a field, but you might get to operate some cool equipment to destroy unneeded data.

Antimalware

Antimalware, antivirus, and advanced malware protection (AMP) refer to tools designed to detect and block malware infections and malware activities.

Organizations often combat malware by having several layers of control in place (known as a *defense in depth*), including the following:

- ✔ **Workstation antimalware:** The front lines of the malware wars, every workstation (and even mobile devices) should have antimalware to block malware.

- ✔ **Server antimalware:** File servers and other systems used to store programs and files should have antimalware, just in case malware sneaks through a workstation.

✔ **Email server antimalware:** Email is a favored transportation route for malware, so blocking it at email servers is a good way to keep it from reaching workstations.

✔ **Intrusion prevention systems (IPS):** Malware commonly "calls home" upon installation to await further instructions. An IPS can detect and block such communications, which prevents malware from becoming active and harmful.

✔ **Spam filtering:** Because many attacks come in the form of phishing, spam filters can be effective at blocking most or all phishing messages.

✔ **Website filtering:** These appliances block access to websites based on category (generally not having to do with business operations) and block websites known to be compromised with malware.

The recent potency of malware is leading many organizations to enact more controls in the form of intrusion prevention systems, which block the command-and-control traffic associated with malware.

Remote access

Remote access is both the business process as well as the technology that facilitates an employee's ability to remotely access information systems that are not accessible from the Internet.

In the business process sense, many organizations permit only a subset of their workers to remotely access the internal environment. In the technical sense, remote access usually includes encryption of all communications, as well as two-factor authentication to make it harder for an attacker to gain access to internal systems.

The fact that many systems are opting to use cloud-based systems instead of internal systems makes some aspects of remote access obsolete. Or, to put it another way, cloud-based systems turn everyone into remote workers because their information systems are no longer located in their internal networks.

Incident management

Incident management is an IT operations process used to properly respond to operational and security incidents. Organizations should have written incident response plans along with training and testing to ensure that these plans are accurate and that personnel understand how to follow them. Written playbooks for common incidents should be developed.

Security incidents are just a special type of incident management, requiring a few additional considerations such as regulatory requirements and privacy laws.

The steps in a mature incident management process are

- ✔ Declaration
- ✔ Triage
- ✔ Investigation
- ✔ Analysis
- ✔ Containment
- ✔ Recovery or mitigation or both
- ✔ Debriefing

Not all security incidents require all these steps, but this framework ensures an orderly and coordinated response to reduce the scope and effect of an incident, as well as a debriefing and follow-up activities to reduce the likelihood or effect of a similar incident in the future.

Vulnerability management

Vulnerability management is an IT operations process concerned with the identification and mitigation of vulnerabilities in IT systems. An effective vulnerability management process includes procedures for identifying vulnerabilities, prioritizing them, and making changes (through change management) to eliminate vulnerabilities that could be used by an intruder to successfully attack the environment.

Other IT operations processes

Honorable mentions that we won't describe include the following:

- ✔ Capacity management
- ✔ Problem management
- ✔ Budget management
- ✔ Supplier management
- ✔ Service-level management

Emerging issues in IT operations

Yes, a lot of issues in the world of security operations keep security managers lying awake at night.

Advanced malware

Innovations in malware packaging have rendered antivirus and antimalware software virtually ineffective against advanced malware. Additional

layers of detection and prevention tools are needed to combat the threat. These tools have significant costs in terms of capital as well as manpower to maintain them.

The greatest fear is that malware creators will soon develop new ways of circumventing even advanced malware prevention (AMP) tools, thereby requiring even greater investment in effective defenses.

Bring your own device (BYOD)

With employees in so many organizations bringing personally owned devices to work for use in their daily job duties, organizations are finding it more difficult than ever to keep track of sensitive data and know when that data is leaving its control.

Physical and Environmental Security

Physical security is concerned with the protection of personnel at work locations, as well as information systems and related media and equipment. Supporting environmental controls and power protection are also a concern.

Although physical and environmental security systems are generally not a part of a networking professional's responsibility, being familiar with these systems will help you do your job better and keep you out of trouble!

Common terms in physical and environmental security

biometrics	guard	line conditioner	tailgating
digital video recorder (DVR)	guard dog	mantrap	uninterruptible power supply (UPS)
electric generator	heating, ventilation, and air conditioning (HVAC)	PIN pad	
exterior lighting		razor wire	video surveillance
fence	inert gas fire suppression	smoke detector	visitor log
fire extinguisher	key card	sprinkler system	wall

Basic concepts in physical and environmental security

This section discusses the most common concepts in security measures that are employed to protect personnel and equipment.

Site access security

Organizations should implement a level of site access security commensurate with the value of information and assets in the facility. The following types of controls contribute to the security of a work location, whether a facility is a data center or primarily used by employees:

- ✔ **Key cards:** Plastic cards with a magnetic strip, an RFID circuit, or an embedded processor and memory. Key cards are assigned to individual workers and are used to activate door locks to permit entry. With a key card system, a building can be divided into zones that restrict entry to specific areas or rooms as needed. Key card systems record successful and unsuccessful access attempts. Lost or stolen key cards can be deactivated in the system so that they will no longer function.

- ✔ **PIN pads:** Keypads with numbers or letters usually used with key cards. PIN pads reduce the risk associated with a lost or stolen key card: On a door controlled by a key card reader and a PIN pad, both the key card and knowledge of the PIN are required to unlock the door.

- ✔ **Biometric access controls:** Devices such as fingerprint readers, palm scanners, and iris scanners. These biometric access controls can be used as a more effective site access control than key cards and PIN pads alone because an intruder could steal a key card and obtain a PIN code.

- ✔ **Metal keys:** Still used for individual offices, but no longer recommended for rooms where several personnel need to routinely enter because there is no way to know which person entered a room.

- ✔ **Mantraps:** A set of two interlocked doors with a short passage between, to control movement of personnel through a door. A mantrap permits only one person at a time to pass, thereby preventing "tailgating," where one or more people can follow an authorized person into a room or building.

- ✔ **Guards:** Personnel with duties to protect facilities and personnel.

✔ **Guard dogs:** An effective deterrent that can assist in searches for persons and in apprehending intruders.

✔ **Visitor logs:** Written or electronic records of visitors to a building. Visitors can also be requested to present a government-issued identification to confirm their identity.

✔ **Fences and walls:** Deterrent and preventive measures to protect the perimeter of a facility or areas of particular interest. A fence or wall at least 8 feet high with strands of barbed wire or razor wire will keep out all but the most determined intruders.

✔ **Video surveillance:** Systems of cameras, monitors, and possibly recording equipment such as digital video recorders (DVRs) used to monitor key locations inside and outside a facility. A video system may include personnel who are observing in real-time, or it may be recording for later viewing when needed.

✔ **Exterior lighting:** Protects a facility by illuminating areas where an intruder would otherwise be able to work in darkness in an attempt to enter a facility.

✔ **Visible notices:** Posted signs and placards informing personnel of the presence of video surveillance, guards, guard dogs, and other controls. Visible notices can also inform visitors of the consequences of entering a facility.

Secure siting

Secure siting, also known as a *site survey*, is a process of searching for and analyzing a work site for nearby hazards and threats that could pose a risk to the security or safety of a work site and the personnel and equipment within.

Typical hazards that a site survey would identify include the following:

✔ **Transportation:** nearby airports, railroads, and highways

✔ **Hazardous substances:** nearby chemical facilities and petroleum pipelines

✔ **Behavioral:** nearby sites where mass gatherings, riots, and demonstrations could take place

✔ **Natural:** risk of flooding, landslide, avalanche, volcano, or lahar

Equipment protection

Measures need to be taken to protect equipment and personnel in work locations, including the following:

- ✓ **Theft protection:** Locking doors, video surveillance, and cable locks
- ✓ **Damage protection:** Earthquake bracing, and tip-over prevention
- ✓ **Fire protection:** Smoke detectors, heat detectors, sprinklers, inert gas suppression, and fire extinguishers
- ✓ **Cabling security:** Conduit or better siting to avoid exposure of communications or power cabling
- ✓ **Photography:** Notices and intervention to discourage photography in sensitive areas

Electric power

Information-processing equipment (computers, network devices, and so on) is highly sensitive to even slight fluctuations in electric power. The following specialized equipment ensures a continuous supply of clean electric power:

- ✓ **Line conditioner:** Absorbs noise present in utility power, such as spikes and surges.
- ✓ **Uninterruptible power system (UPS):** Equipped with backup batteries that can supply power to computing equipment from several minutes to an hour or more.
- ✓ **Electric generator:** Powered by gasoline, diesel fuel, natural gas, or propane and can generate electric power for hours, days, or more.

An electric generator and a UPS are typically used together to ensure continuous power. Because electric generators take several seconds to a minute or longer to activate, a UPS supplies power while the generator is starting up.

Many UPSs have built-in line conditioners, so standalone line conditioners are uncommon, except in environments where electric power is reliable but noisy.

Heating, ventilation, and air conditioning (HVAC)

People and information-processing equipment operate best within a narrow temperature and humidity range. (Humans are more tolerant of a wider range in temperature.)

Heating, ventilation, and air conditioning (HVAC) systems regulate temperature and humidity in buildings containing personnel, computers, or both. HVAC systems are especially important in data centers, which generate a considerable amount of waste heat that must be continuously moved away from computers to prevent overheating and premature failure.

Many newer data centers rely on circulation of outside ambient air (with particulate filtering) as opposed to refrigeration to provide cooling at a significantly lower cost.

Redundant controls

Many facilities incorporate redundant controls to ensure continuous availability of environmental needs. Redundancy allows for continuous protection in the event of equipment failure as well as routine maintenance. Examples of redundant controls follow:

- ✔ Utility power feeds
- ✔ UPSs
- ✔ Generators
- ✔ HVAC systems

Emerging issues in physical and environmental security

Issues in the physical and environmental security realm that keep security professionals awake at night include the following:

- ✔ **Use of cloud services:** Organizations that adopt cloud services give up a large measure of control and visibility into the physical controls protecting equipment that stores and processes their data. Some cloud service providers do not readily provide detailed information that some organizations may need for compliance purposes.

- ✔ **Increased equipment density and available environmental controls:** Newer servers and storage systems are constructed in smaller sizes, allowing for more servers and storage to be installed in a given area. Sometimes, however, data centers are unable to supply adequate power and cooling for this higher density equipment.

Regulations, Investigations, and Compliance

Because of their integral role in supporting business processes, information systems are in the crosshairs of laws and regulations. Computers are frequently involved in civil and criminal investigations, requiring forensic

procedures when collecting evidence from computers and other electronic devices. Some networking professionals will have the opportunity to work in these areas.

Basic concepts in regulations, investigations, and compliance

Even though networking professionals are not attorneys, it is helpful for them to understand the laws, regulations, and other legal requirements that drive compliance efforts in organizations. It's also helpful for networking professionals to understand how security investigations should be conducted. This is fun stuff!

Computer crime laws

Many countries have enacted computer crime laws that define trespass, theft, and privacy in the context of information systems. In the history of law, computers are still new, and the development of laws is ongoing and changing frequently.

This high frequency in changes of laws, regulations, and legal standards presents a challenge to information security and legal professionals as they strive to be compliant with these laws and also to recognize cybercrimes when they occur.

Industry regulations

Regulations on many topics have been enacted for various industries. In the information technology world, regulations such as HIPAA (Health Insurance Portability and Accountability Act) require the protection of healthcare-related information and GLBA (Gramm–Leach–Bliley Act) require protection of customer information in the financial services industry.

Common terms in regulations, investigations, and compliance

chain of custody	COSO	GLBA	ISO27002:2013
COBIT	forensics	HIPAA	

Managing compliance

Compliance is a matter of adhering to laws, regulations, contractual obligations, and policies. It takes a determined effort to know all compliance obligations in an organization, and more effort to achieve compliance. Many organizations develop or adopt a framework of controls to track compliance on an ongoing basis. Suitable frameworks include

- **COBIT (Control Objectives for Information and Related Technology):** Developed by ISACA, COBIT is a highly regarded framework for IT operations.

- **COSO (Committee of Sponsoring Organizations of the Treadway Commission):** Developed as a result of financial accounting scandals in the 1990s, COSO provides guidance for IT control frameworks for U.S. publicly traded companies.

- **ISO27002:2013:** The international standard for information security management, which establishes a process of controls development and management

Security investigations and forensics

Security investigations are an organization's response to isolated security incidents that have little direct effect on business operations. Still, the events requiring investigation can be important in other ways because they can have significant legal implications.

Any event that takes place in an organization in the context of computers where possible future legal action is involved may require an investigation with forensic rules of evidence in play. These rules include

- Evidence collection and preservation

- Evidence chain of custody

- Evidence collection recordkeeping

- Evidence examination recordkeeping

For an organization to prevail in any related legal proceedings, a trained individual with dedicated tools and hardware must carry out these forensic procedures.

Emerging issues in regulations, investigations, and compliance

Following are two issues keeping networking professionals on their toes:

- ✔ **Rapid onset of new laws and regulations:** New laws on computer operations, security and privacy are enacted and updated at a rate that makes it hard to keep up on their details, never mind figure out how to be compliant with them.

- ✔ **Jurisdictional issues:** Many new laws have greater jurisdictional reach than in the past. For example, privacy laws in many U.S. states have jurisdiction across state lines, and international privacy laws affect many organizations not located in countries that passed the laws. These jurisdictional issues are all about cross-border privacy, where each country passes laws requiring the protection of private data associated with its citizens, applicable regardless of the location of the organization that has the data. This issue has many corporate counsels on a steady diet of coffee and Rolaids.

Factoring Nontechnical IT Issues

A number of trends in business affect jobs in networking. These trends go beyond the technical aspects already covered and include

- ✔ Outsourcing
- ✔ Telecommuting

Outsourcing IT

It is human nature for a company to want to have formal possession and control of the assets on which the company relies. Historically, companies have wanted to own everything involved in the creation of their products and services. Some companies have taken this approach to the logical extreme and seek to own everything from mining the materials to owning the stores where the products are sold.

A more modern approach is to own the parts of the process where you have your best differentiation from the competition, either in lower price or better quality, and rely on suppliers to provide commodities or other undifferentiated parts of your solution. For example, the Ford Motor Company refined its own steel starting in 1917. In the 1960s, they thought better of this approach and sold their steelmaking assets to focus on the parts of car making that they could do better.

This approach can be applied to information technology, and by extension, networking. A given company could look at data connections as a commodity, then look at their computer network as a commodity, and then look at their data centers as a commodity. What the heck, they could look at everything in IT, including application development and systems integration, as a commodity.

Companies can change their approach as circumstances in their business evolve. One year they can choose to outsource. Another year, they may choose to bring a part of IT back in-house and discontinue working with outsourcing vendors.

No single strategy as to the right degree of in-house management versus outsourcing applies at all times. The best you can hope is that companies will be judicious in adjusting their outsourcing strategy. If the company is not judicious, the result will be more layoffs and rehiring between the company and the vendors.

Employees un-telecommuting

The last major trend under consideration is a company's policy about telecommuting. Many cities and regions have implemented incentives to companies to encourage telecommuting. Providing companies these incentives is less expensive than building more roads.

Many employees prefer doing their job while wearing their jammies. Plenty of organizations have embraced this approach because it allows them to operate in a smaller office space. But it puts a burden on the network to ensure proper security and adequate resources.

The shift towards telecommuting has not been without problems. Primary among them is a loss of camaraderie among employees, resulting in a loss of collaboration opportunities. This is particularly a problem in companies that produce creative products and services and in engineering-oriented companies.

As a result, some senior executives are reversing policies on telecommuting. Some employees must work in the office a certain number of days per week while other positions that were formerly done by telecommuters must be done in the office.

Re-accommodating employees who were once telecommuting and are now in the office is not the hardest challenge to address. It involves reinstallation of standard communication services. Some policies are as fickle as fashion — and networking is expected to turn instantly to adapt to these policy changes.

Part II
Having the Right Stuff
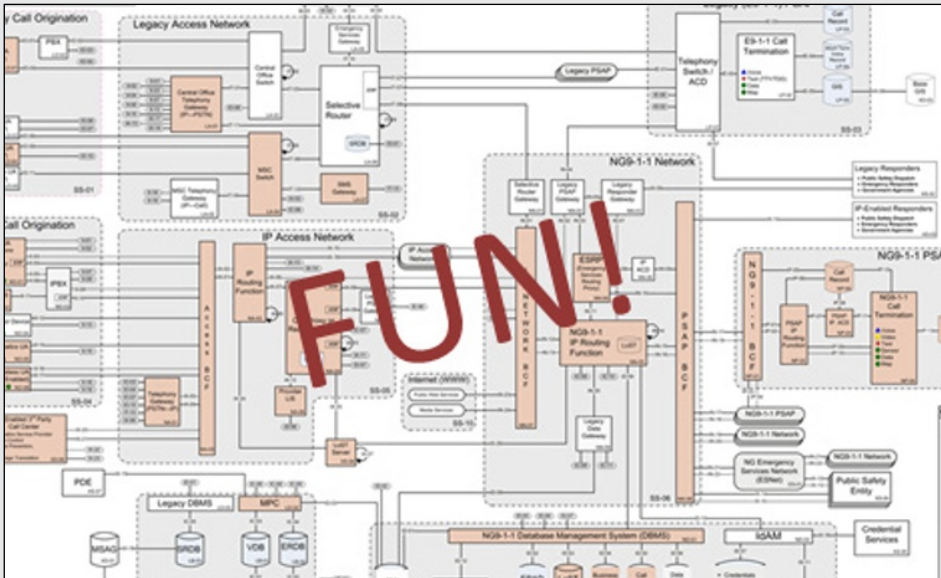
In this part . . .

- ✔ Know what you need to know.
- ✔ Prove your skills and knowledge.
- ✔ Understand the options for filling in the gaps.
- ✔ Keep current as technology evolves.

Chapter 5

Getting the Necessary Education and Training

*M*any learning opportunities are available for people who want to get into networking. The choices you make will depend on several factors, including the following:

- ✔ Work experience
- ✔ Prior education
- ✔ Age or stage in life
- ✔ Financial resources you have or can get
- ✔ Level of management or specialization you want to attain

TIP

A good educational foundation is essential for entry into the information technology profession, and a steady intake of continuing education is essential from then on.

The purpose of this chapter is to provide you with the options, so you can decide how to get from where you are now to where you want to be. Because the title of this book is "Getting a Networking Job For Dummies," not "Getting a Networking Job For Dummies Who Have an Associate's Degree from a Community College and Are Trying to Decide Their Major," we want to list all the options so you can decide what is right for you. In other words, this books examines a range of job scenarios which may or may not apply to your particular situation.

A good education in networking and the status associated with a particular mode of education are not necessarily related. You can get an excellent technical education from a correspondence school that advertises on late-night infomercials if you are motivated and the teachers know their information.

Off-the-Record Training

Abraham Lincoln went to school only until he was 10 years old. Then he read a lot of books. Now he's on the penny and the $5 bill. See what you can do if you are diligent?

If you can do the job, most employers will overlook how you got there. If self-paced, self-guided education is your style of learning, you have many options for learning about computer networking.

Studying with self-direction

Lots of books can teach you about networking. Because you have a natural affinity for Dummies books, here are a few examples from that series:

- *Networking For Dummies* by Doug Lowe
- *TCP/IP For Dummies* by Candace Leiden
- *Cisco Networking All-in-One For Dummies* by Edward Tetz

There are also Dummies books associated with attaining many important networking certifications. (For more on certifications, see Chapter 6.) It is wishful thinking to believe that you could pass a hands-on test purely by reading a book. At the same time, you can learn a great deal of practical knowledge simply by reading the books. A few examples of these Dummies books on passing networking certifications follow:

- *CCNA Certification All-In-One For Dummies* by Silviu Angelescu
- *CCENT Certification All-In-One for Dummies* by Glen E. Clark
- *CompTIA A+ Certification All-in-One For Dummies* by Glen E. Clarke and Edward Tetz
- *Network+ Certification For Dummies* by Ron Gilster

There are rumors that some other publishing companies offer technical books on networking. It is entirely possible, but they won't have a yellow cover or *Dummies* in the title.

On-the-job training

The guild method of learning a trade is the ancient process of a protégé following a mentor. It seems quaint in modern days, particularly when we're talking about high technology, but it is an effective and low-cost way to start in a new field. The first challenge is finding someone who would be willing to mentor you. The next challenge is finding a company that is willing to pay you while you're duplicating the job of another employee.

A lot of a mentor's job is spent on routine administrative tasks, as long as the network is running smoothly. If the network starts sliding sideways, it's best to step back and wait to ask questions at a more convenient time. Closely watching your mentor during a full network disruption is a golden opportunity to understand what goes on when managing networks and to learn how to make things work.

If you find yourself with a mentor, here are some suggestions on how to take full advantage of the situation:

- ✔ **Read networking books:** You could start with the ones mentioned previously. Next, build up your library with the books listed in Chapter 21.

- ✔ **Take vendor-specific training.** A significant portion of the training in networking is associated with certifications. Certifications, which are explored more in Chapter 6, may not be right for you at this point. Most manufacturers offer factory training on products for their customers. Equipment vendors provide this value-added service to make sure that their customers' employees are the first line of success.

- ✔ **Study emergency procedures.** Many companies have documented procedures for emergencies relating to the network and other critical functions. Find out where these are in case you ever need to find them in a hurry. Next, review them in detail and make sure that you understand what the steps mean. Finally, make sure all the information is current.

  One of those realities of business life is that manuals tend to become obsolete over time. You can make yourself useful and help avoid a problem by ensuring that the information is current. (Be sure to make a hardcopy. Wouldn't it be awkward if the only copy of what to do if the network fails were on the network?)

✔ **Pursue a certification.** Read Chapter 6 for information on the different certifications, and then ask your mentor for assistance. It helps you, and good mentors like refreshing their knowledge.

Viewing prerecorded college courses

The other end of the spectrum from shadowing a network expert is the new high-tech way of learning: taking online courses about networking topics. It seems consistent and logical to learn about data networking on a data network.

One scenario is to access online courses. These are regular college courses that include lectures, problem sets, notes, and tests. The lectures are recorded and available as videos. There are also a range of documents, including the syllabus, lecture notes, tests, and the final. These classes are usually recent, so the examples are timely.

The institutions of higher learning that participate are not off-brand colleges or diploma mills. How do MIT, Rensselaer Polytechnic Institute, and the University of Michigan sound to you?

✔ **MIT:** The site for MIT's Open Courseware is `http://ocw.mit.edu/index.htm`. You can shop around for other classes that interest you.

✔ **Rensselaer Polytechnic Institute (RPI):** RPI leaves participation to individual departments and professors. Prof. Shiv Kalyanaraman, for example, offers his lectures on computer communication at `http://www.ecse.rpi.edu/Homepages/koushik/shivkuma-teaching/video_index.html#ccn_foils`.

✔ **University of Michigan:** The site at the University of Michigan is called Open.Michigan and can be found at `http://open.umich.edu/`.

These institutions are just a sampling. You can find many other organizations that offer comparable courses on computer networking.

You can view and download the course material, but the intellectual property is not yours. Plus, you don't get any credit for taking the course. (You can still wear the school sweatshirt, put the little sticker in the back window of your car, and donate to the alumni organization).

You may be able to officially take a course online in pursuit of a certificate or a degree. This possibility is in the "Learning Networking through Higher Education" section, later in the chapter.

Let's say that you've been working with computers for a while now, but you want to start at the beginning to make sure that you have a solid understanding of the theoretical side of computers and networking.

You poke around the Internet and find that the Massachusetts Institute of Technology (MIT) offers its introductory computer science class online. Here's how to sign up to the MIT introductory course, Computer Science 101:

1. Go to `http://ocw.mit.edu/index.htm`.

A page like the one shown in Figure 5-1 appears. Note the prominent donation icons. It's almost like you are an MIT alumnus already!
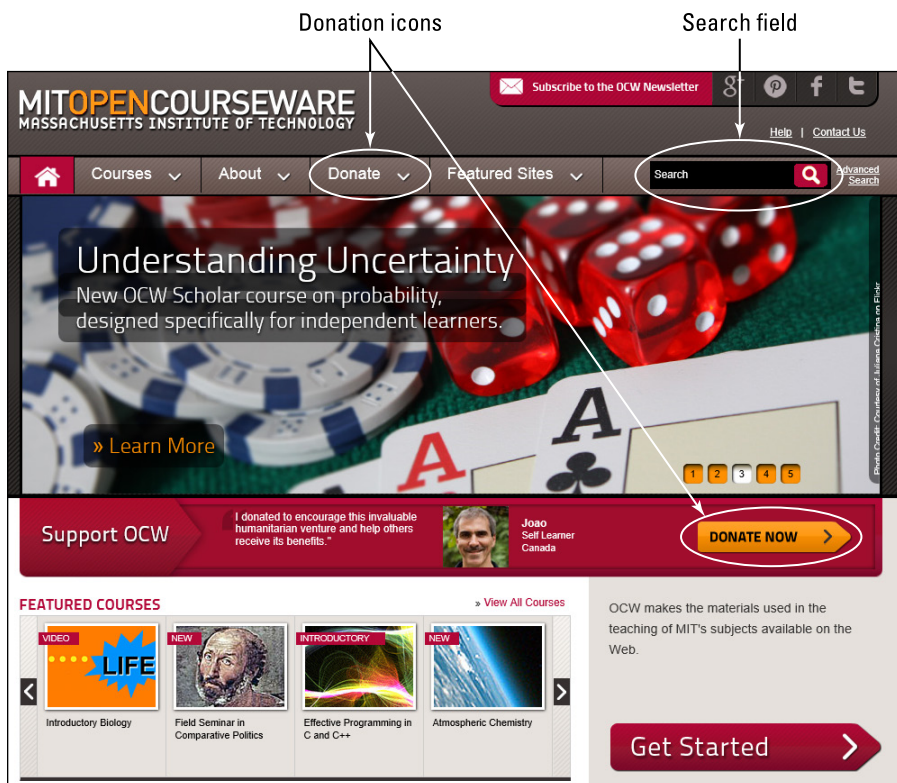
Figure 5-1:
The MIT Open Courseware home page.

   2. **In the search field, type** Introduction to Computer Science **and then press Enter.**

      The results screen shown in Figure 5-2 appears.

   3. **Click the 6.00 Introduction to Computer Science link.**

      The course description shown in Figure 5-3 appears.

      From this page, you can access the lecture videos, the assignments, the exams and tests, a course transcript, and links to obtain the textbook. You can also click the Download Course Material link to get the whole shebang at once.

   You can now view the lectures and read the material at your own pace. If you have questions, you can join a study group from this page. What could be easier?

Figure 5-3
CS 6.0
Introduction
to Computer
Science and
Programm-
ing home
page.

All course material   Individual course material elements

Learning through Higher Education

The most convenient time to decide on a career in computer networking is when you enter college. If you happen to be reading this book before you complete your college applications, consider yourself lucky. You may have been considering majoring in Art History without realizing that computer networking is your real calling.

Undergraduate and graduate degrees in management information systems, computer science, information technology, and similar subjects have been offered for decades. More recently, many colleges and universities are

offering degree programs in computer networking. Colleges and universities also offer continuing education programs in information technology and security.

Undergraduate programs

Universities around the world offer undergraduate degrees in information technology — too many to list in this book, and that's a good thing. You can probably find a university near you that offers a degree in information technology.

A number of majors have similar sounding names but a slightly different emphasis:

- ✔ **Bachelor of Computer Engineering:** Emphasis on the physical design of computing equipment
- ✔ **Bachelor of Science in Computer Science:** Emphasis on processing logic
- ✔ **Bachelor of Science in Management Information Systems:** Emphasis on computers in the enterprise

Note that there is significant overlap among these majors and all have a role in networking.

Hiring managers are typically eager to hire any of these titles if you're sincere about your interest of working in networking and for that particular company. Because the degrees mentioned are at the undergraduate level, most prospective employers want to make sure that you're skilled in technology but also have a variety of elective classes and extracurricular activities to ensure that you are a well-rounded individual.

Technical skills may be the focus in the interview, but employers are hesitant to hire individuals who are too narrow to thrive in the culture of their company. For more on this subject, see Chapter 17.

Your best long-term strategy should include the completion of an undergraduate degree in a technical field. The more college education you have, the more opportunities for jobs and career growth.

For your convenience, Table 5-1 lists the *US News and World Report* ranking of top computer programs. You may have noticed that tuition (shown for the 2014–2015 school year) is not cheap. In spite of the high cost, many of these schools turn away more than nine out of ten applicants.

Table 5-1	*US News and World Report* Ranking of Colleges		
Rank	*School*	*In-State Tuition and Fees*	*Out-of-State Tuition and Fees*
#1	Massachusetts Institute of Technology	$45,016	$45,016
#2	Stanford University	$44,757	$44,757
#3	Carnegie Mellon University	$48,786	$48,786
#4	University of California–Berkeley	$13,844	$25,064
#5	University of Illinois–Urbana-Champaign	$15,602	$30,288
#6	Georgia Institute of Technology	$11,394	$30,698
#7	University of Michigan–Ann Arbor	$13,977	$41,811
#8	University of Texas–Austin	$9,798	$34,722
#9	Cornell University	$47,286	$47,286
#10	California Institute of Technology	$43,362	$43,362

The value of a college degree

The advantage of a formal university education is that you have the opportunity to immerse yourself in information technology and really live and breathe it. Additionally, companies and the federal government are actively and heavily recruiting from university programs dealing with information technology. Internships are also available, and the major consulting companies are looking for individuals with some skill in the field.

The disadvantages? Getting a college degree is costly and time-consuming, and can be especially difficult if you're not in a position to go back to school full time. Thankfully, programs are available that accommodate those with a job and family life, but it's a considerable investment in time and resources regardless.

G.S., Seattle

Graduate degrees

Many universities offer graduate-level degrees in networking. A graduate degree will help you compete for advanced positions in companies. Many middle- and upper-management jobs in IT departments require an advanced degree.

Formal study at an online university

We talked about taking a class online previously. How about earning a certificate or a full degree at an online university? Not that long ago, there was a stigma attached to online universities. The idea of earning a useful degree from a website on the Internet instead of in a lecture hall was beyond the comprehension of many. This attitude is largely evaporating as more prestigious names in higher education offer online courses.

That said, here are the considerations that generate debate:

- **Nonprofit versus for-profit entity:** Is the website set up and run by a nonprofit entity or is the objective to make money?

- **Live recordings that are proctored versus just recorded:** Sometimes lectures are live, and the instructor conveys information as if in a video conference. Students can ask the instructor or a teaching assistant questions during the lesson. The second scenario is just a video and audio recording of a professor with no one to answer questions. You're on your own.

- **Degree versus certificate:** Many of these sites are accredited and degree- or certificate-granting institutions. Others give away education for the societal benefit. We explore the practice of giving away education on the Internet more in the next section on higher education. There are lots of good choices for getting a certificate or degree online.

Given this background on the kinds of online courses, there are three scenarios for online instruction:

- **Nonprofit online degree granting institutions:** Several established nonprofit schools have embraced online degrees. These are not free if you want the certificate or the official degree.

- **For-profit online degree-granting institutions:** A number of publicly traded companies offer accredited degrees.

✔ **MOOC-oriented organizations.** Bear with me on this one. Massively Open Online Courses, or MOOCs, challenge the business model of the education industry by offering classes on the Internet.

Following are some questions to ask to help you determine which scenario is best for you:

✔ **What is the tuition?** What does a class or classes cost me (regardless of the financial goals of the website)? Don't assume that a nonprofit charges less than a for-profit website. Tuition for these classes is anywhere from $0 (along with some guilt for being a freeloader) up to almost $50,000 for a top name university.

✔ **Does this method of instruction work for me?** Am I comfortable just hearing a lecture or do I learn only if I can ask questions along the way? Are online class discussions an important part of the learning process? As a rule, class discussions are more valuable for humanities classes.

✔ **Does the class, certificate, or degree move me toward my goal?** Do you want to learn some information or is attaining a goal such as a certificate or degree your main objective?

After you decide which scenario works for you, read on for information on the options.

Nonprofit online degree-granting institutions

A number of established colleges and universities offer degrees to students who may never travel to their ivy-covered buildings. Students can earn their degree and never set foot on the same continent as their alma mater. Some examples include the following:

✔ **University of Maryland:** UMUC (University of Maryland University College) offers a bachelor's degree in computer networks and security. Their website is `www.umuc.edu/academic-programs/bachelors-degrees/computer-networks-and-security-major.cfm`.

✔ **University of Illinois:** The site at the University of Illinois–Chicago offers a bachelors degree in computer science. The site is `www.usnews.com/education/online-education/computer-science-bachelors-degree?int=9fd708`.

✔ **Northwestern University:** Northwestern University offers several online masters degrees and certificates. The site for online learning is `http://sps.northwestern.edu/main/online-programs.php`.

This is just a sampling. Many other organizations offer comparable courses on computer science and computer engineering.

Keep the following in mind. First, these are full degrees. The diploma doesn't indicate that the degree was earned online. Also, acceptance into these programs is as competitive as nononline programs. You need the right credentials, test scores, and references to be accepted.

Finally, tuition is the same as if you were on campus. There is no discount associated with eliminating the wear and tear that you would have put on the university buildings. In fact, some universities charge a technology fee of about $100 per course to take it online. Online students are just as eligible as other students for financial aid.

Earning a degree or certificate from a for-profit school

The University of Phoenix is the largest and best-known for-profit online degree-granting institution. DeVry University and Capella University are two other companies that offer fully-accredited degrees when you complete the required courses.

Chances are you didn't know that the three schools mentioned are for-profit companies. They are respectively owned by Apollo Group (NASDAQ: APOL), DeVry Education Group (NYSE: DV), and Capella Education Company (NASDAQ: CPLA). For most of us, it doesn't matter because for-profit schools must be price competitive with the nonprofits. Your concern should be deciding which certificate or degree is best for you. Most people in networking pursue either computer science or computer engineering.

There are two important considerations for for-profit schools. First, most are taught by industry professionals, not academics. Instruction in networking benefits from both theoretical and practical knowledge. An instructor with years of experience addressing real-world networking issues can be as effective an instructor as an MIT computer science department head.

ANECDOTE

An education from a for-profit college

The rest of my family went to prestigious colleges and universities. I did not like the structure in high school, and the structure in college would not have been a good experience — for them or me.

My family cringed when I told them I was pursuing my degree from DeVry. However, I found that the instructors knew more about the real world. Since they worked with an industry, they were always eager to show how things really worked. My education propelled me to success.

I.P., Seattle

Another consideration is that acceptance into a program is more straightforward. For example, you simply need your high school diploma or GED and enough funds to pursue a bachelor's degree.

Some look down on schools with modest admission standards. Perhaps a more enlightened perspective is to look at the graduates of such programs as having taken the initiative to become successful.

A large percentage of students enrolled in these programs do not graduate, but there is no reason to hold this against students who do graduate. In fact, it should demonstrate that the students who graduate are motivated and would tend to make better employees.

A high dropout rate used to indicate a rigorous education. For example, the rate of dropout from the Navy Seal program is over 90 percent. According to a *New York Times* report, the dropout rate at the University of Phoenix online program is 95 percent. By comparison, only 6 percent of Cornell University–College of Engineering freshman don't graduate within five years.

Signing up with a MOOC-oriented accredited school

Still another option for an online degree is an organization that offers massively open online courses (MOOCs). For our purposes, we call these MOOC-oriented accredited schools.

These organizations offer lower tuition because of their large class size. They tend to be nonprofit and proud of it. Some can be somewhat antagonistic to traditional educational institutions, while others were founded by existing schools.

All incorporate lectures from well-respected institutions of higher education. Adding to the confusion is that many established schools have adopted the MOOC technology for online classes but have not adopted the MOOC business model.

The following are examples of MOOC-oriented accredited schools:

- **Coursera:** Coursera works with hundreds of universities to make their courses available online. Their certificate is called a specialization. The site is www.coursera.org.

- **Udacit:** This organization started as an extension of several universities but now offers courses that are more vocational. Visit www.udacity.com.

✔ **edX:** Harvard and MIT started this organization and have attracted a number of top-name universities. You can earn a certificate by taking a series of courses. Go to `www.edx.org`.

✔ **World Mentoring Academy:** This organization, which was founded independently of universities, states that you can earn a bachelor's degree for approximately $5000. You can find them at `www.worldmentoringacademy.com`.

Figure 5-4 shows a dashboard of a student working on a computer science degree from World Mentoring Academy.

These classes should look familiar to anyone who has pursued technical classes at another educational institution.

Adult education

Chances are, we did not catch you at that golden opportunity when you're deciding your major. You may have your undergraduate degree in textile design and fashion merchandising, but now you want a job other than re-folding sweaters at the J. Crew at the local mall.

Figure 5-4: Dashboard for a World Mentoring Academy computer science major.

Continuing education is the practice of continually obtaining training courses to expand one's knowledge and skills. In the computer networking profession, continuing education is essential to our success for several reasons:

- ✔ **Network technologies change.** What worked decades ago is obsolete today. We hope that your career in networking will last long enough for you to see great changes.

- ✔ **Humans forget information.** If you do not use your knowledge, you will forget it over time. This happens to the best of us.

- ✔ **Continuing ed builds contacts in the business.** Participating in continuing education often involves interacting with others in the networking community. Business networking is fun, helps us find solutions more quickly, and can help us find a job.

Many colleges and universities have certificate programs designed for working professionals who have their undergraduate degree. Often, these are evening or weekend programs, and many are offered online, which gives you a wider choice. Examples of these certificates include the following:

- ✔ Network+ Technologies Certificate or Advanced Networking certificate from the University of Phoenix

- ✔ Network and Communications Management certificate from DeVry University

- ✔ Computer Networking Post-Baccalaureate certificate from the University of Tennessee–Chattanooga

Check local educational institutions and online resources to see if they offer a certificate program that might interest you. There is a charge for tuition, but there are lots of ways to get funding; sometimes an employer will pay for this education or a union will pay for the continuing education of one of its members. Also, some religious organizations may be willing to help.

Pursuing a Nontraditional Education

There are a number of alternatives besides traditional educational venues for learning networking skills. We describe two in this section.

Military education

Today's military organizations still have their traditional weapons: guns, warships, submarines, fighter planes, and bombers. These large organizations also require a lot of information technology to support their warriors. They have an army (or boatload) of trained networking experts to keep the information flowing.

Military organizations train many of their personnel in different facets of networking. Most internal networks in military organizations use the same technologies as commercial networks, so most of the skills learned while in the military will translate directly into private sector or public sector jobs.

Examples of military training in information security follow:

- U.S. Army Signal Corp School offers training in Signal (Communications) Operations. The Network Switching Systems Operator-Maintainer (25F) is the closest to what we are talking here, but other job specializations use other, closely related transmission media, such as microwave.

- The U.S. Navy has the role of Information Systems Technician for enlisted personnel and Information Professional for officers. These roles can work on land or sea.

- U.S. Air Force trains enlisted personnel to become Cyber Transport Systems specialists.

- U.S. Marine Corp has the role of MOS 0651-Data Network Specialist. ("Oorah!")

Many people assume that the military is primarily made up of warriors, but a large number of enlisted personnel and officers are responsible for support functions. Besides getting to wear some nice uniforms, these individuals are paid to take classes and gain experience with modern telecommunications technology.

The military provides opportunities for personnel to earn college credits on most bases while on active duty.

For-profit training companies

The shortage of properly trained professionals in the computer networking field has attracted a number of organizations that now train people in computer technology, including computer networking. In general, these organizations do not confer degrees. Depending on your ambition and your ego, not getting a formal degree is either a no-go or no problem. What matters is the reputation of the organization and the information you receive.

Following are some of the leading training companies:

- ✔ Global Knowledge (`www.globalknowledge.com`)
- ✔ InfoSec Institute (`www.infosecinstitute.com`)
- ✔ NetCom Learning (`www.netcomlearning.com`)

The courses from these organizations tend to focus on helping students complete a certification in a technical area. For more on certifications, see Chapter 6.

Maintaining Your Networking Knowledge

While you're dutifully doing your job, those pesky computer scientists and engineers at the networking vendors are improving their products, making your skills obsolete. The updated version of the English proverb is "time and tide wait for no person." You'll need to pursue some continuing education if you want to remain effective in the networking space.

The tried-and-true method in the networking community is to pursue a certification. Chapter 6 describes the different kinds of certification, which range from simple to exclusive.

Some of the more basic certifications focus on knowledge that does not evolve quickly. These certifications, which are the exception, are a valid way to get started on the certification track.

REMEMBER

Most certifications recognize that technology changes, so you must retake the exam every few years to retain the ability to claim that you have a given certification.

Besides earning a certification, you can keep your knowledge fresh in a few other ways:

- ✔ **Retake a course for which you are certified.** By retaking the course, you will refresh your knowledge.

- ✔ **Pursue a related certification.** It can really help your perspective to learn other technologies. For example, studying network security will always help you in networking. Another option is to get certified in a product that is competitive to your specialization.

- ✔ **Become a trainer of networking technology.** There's nothing like the fear of being humiliated in public to force yourself to learn the newest information.

- ✔ **Attend vendor training.** Companies love to have customers take courses at their factory.

Chapter 6

Becoming Certifiable

. . . .

. . . .

*E*ducation and training are important, but a professional certification demonstrates your commitment and proves your proficiency. The top graduate from the best law school can't get paid for chasing an ambulance until he or she passes a bar exam. Likewise, a PhD from the top accounting school can't count a real bean for a paying customer until he or she passes the CPA exam.

There's nothing like a professional certification to change the focus during an interview from whether you can do a particular job to other concerns, such as softer skills or, even better, your salary requirements and start date.

Which certifications are best for you and your goals? There are dozens of professional certifications in networking and related skills. Pursuing the wrong one is a waste of your time. Pursuing them all is impractical and a waste of your time.

This chapter gives you some background on certifications and provides you with enough information to help you determine which certifications will be most beneficial to your career aspirations.

Planning for a Certification

When determining which certification to pursue first, consider the following factors,:

> ✔ **What is the "best" certification for you?** As mentioned, you have lots of choices. We present a good selection of options later in this chapter.

What constitutes "best" is a personal decision combining the respect that the industry has for a given certification and whether the certification covers an area that is consistent with your interests and ambitions.

✔ **Can you make the time commitment?** Every certification requires that you put aside a significant amount of time for studying and taking the test. Ask yourself whether you are in a situation to do this.

✔ **What is your studying style?** Popular certifications have study guides and preparation courses. Some people learn by reading, others by hearing, and still others by doing. Find a class that fits your learning style.

✔ **What is your test-taking style?** Some people struggle with answering multiple-choice questions. If that description fits you, a certification might be more frustration than it is worth. Be honest with yourself.

✔ **How much does it cost?** No certification is free, but you may be able to get someone else to pay for it. Many companies have a budget to pay for certifications pursued by employees. If the training is associated with a particular vendor, your employer may have earned credits from past sales with a vendor that will pay for training on the vendor's equipment. Otherwise, the training will be on your own dime, and it costs much more than a dime.

✔ **Are you prepared to keep your certification current?** Many certifications need to be renewed every two or three years. The sponsoring organizations of the certificates add new questions, delete obsolete questions, and change the answers as technology evolves. If you're not regularly using particular skills, you may need to refresh what you learned. Before you decide to pursue a certification, be aware that you are making a recurring commitment that often involves a least some cost for recertifiaction

WARNING! It is bad form to claim on a job application that you have a certification if it has expired. Most certificate-sponsoring organizations have a search capability that can be used to easily confirm your stated certification. Most companies consider falsifying this information to be a dismissible offense.

Deciding Which Certifications Are Right for You

So what is the right certification for you? In addition to the factors mentioned in the preceding section, you need to consider some important issues.

The two categories of certifications are vendor-specific certifications, which relate to the products made by a specific vendor, and non-vendor-specific certifications, which are created and maintained by independent organizations, typically nonprofits.

Vendor-specific certifications are marketable, but only to firms that use products from that vendor. A Cisco certification is valuable because many companies have at least some Cisco equipment.

Vendors such as Huawei and ZTE also have certification programs, but their customer installed base in the United States is relatively small. As a result, the value of their certification is less among U.S. companies.

In addition, a given vendor may have multiple certification types. For example, as of this writing, Cisco has 28 certification types, most of which relate to networking. (We describe Cisco certifications in the next section.)

Microsoft has seven certification types, but networking is only part of the curriculum. Having a Master-level certification is great, but a Microsoft Office Specialist-Master certification will not help you much in the networking field.

Non-vendor-specific certifications are a different kettle of fish. Non-vendor specific certifications tend to be more general and contain a wider set of study topics or body of knowledge. A vendor's certifications is limited to their products or services and how to apply them to specific network situations. Non-vendor certifications cover more material and focus on the control to be implemented or the business problem to be solved, including combinations of vendor solutions.

Although some vendor-specific information is part of non-vendor specific testing, the intent is to offer prospective customers assurance that the person who has passed the certification has at least a minimal set of skills. A number of non-vendor-specific certifications are explored later, in the section "Winning with a Third-Party Networking Certification."

So how do you decide which certification is best? In addition to the preceding considerations, also think about the following:

- ✔ **What does your boss want?** If you have a boss now, it never hurts to ask what he or she wants. Having support in pursuing a particular certification is essential if you want your boss to pay for the certification.

- ✔ **What certification do my peers or mentors have or respect?** Go ahead and ask them. They will be happy to share their experiences and opinions. Also talk to people who have gone through the certification process. They can warn you of any landmines, commiserate on the challenges, and let you know how this certification has helped in their career.

> ✔ **What certification sounds most interesting or fun?** The rest of the chapter explores a number of vendor-specific and non-vendor-specific certifications. We provide a good sample, but we don't list all available certifications. Spend a little time on the Internet and find out whether one captures your imagination.

Choosing a Vendor-Specific Networking Certification

Lots of organizations offer training to customers on how to more fully use their products. This approach makes business sense. Often these classes last a few days and help customers with configuration and maintenance. Upon completion, the company offers attendees something to resemble a diploma.

Earning a training diploma is good, but training is different from certification. One distinction is that a certification requires a test. In most vendor-specific training courses, the diploma primarily means that a warm body was present for the duration of the training. Whether the individual who was sneaking sips from his hip flask got anything from the information is between him and his boss (you know who you are).

Another distinction between a training diploma and a certification is that a certification is recognized in the industry as offering some level of value. With vendor-specific training, sometimes a third party creates the training program; completing the program won't help you get a job if the hiring manager has never heard of the company.

The issue of value is meant as a cautionary tale. Some shady companies offer discounted certification courses. If prospective employers have never heard of these companies, completing their courses won't help you in your job search, regardless of how much you learn or how sincere the marketing materials sound. Check first with those in the industry.

In this section, we describe well-known vendor-specific certifications that carry value.

Cisco certifications

Arguably the best-known certifications in the networking biz are from Cisco. As mentioned, Cisco offers 27 kinds of certification. One almost needs a certification to tell what the different Cisco certifications mean.

The first distinction among the Cisco certifications is the level:

- ✔ **Entry:** For individuals who are interested in getting started in networking
- ✔ **Associate:** The first level for people with a few years of experience in networking
- ✔ **Professional:** For people who want to impress the heck out of prospective bosses and in-laws
- ✔ **Expert:** For those who seek to impress professionals
- ✔ **Architect:** For those who are just showing off (but we're secretly jealous and want your autograph)

Entry level

The two certifications at the entry level are

- ✔ **Cisco Certified Entry Networking Technician (CCENT):** This certification covers the skills necessary for supporting small and medium-sized businesses.
- ✔ **Cisco Certified Technician (CCT):** A more hands-on certification for people who will perform physical installations and troubleshoot Cisco equipment in the field. Within this certification are specializations for technicians working in data centers, with switches and routers, and with telepresence equipment (used for voice and video).

Don't assume that these courses are simple because they include the word _entry_. These entry-level classes require several months of intense studying, lots of hands-on experience, and the successful completion of several rigorous tests.

Associate level

The Cisco Certified Network Associate (CCNA) certifications are the next step up from entry-level certifications. The associate level covers skills necessary to administer small or medium-sized networks with one of eight technology specializations:

- ✔ Routing and switching
- ✔ Data center
- ✔ Security
- ✔ Service provider
- ✔ Service provider operations
- ✔ Video

✔ Voice

✔ Wireless

The individual who earns one of these certifications would be, say, a Cisco Certified Network Associate (CCNA) Data Center or CCNA Routing and Switching.

Just to keep it a little confusing, another certification in the associate level is the Cisco Certified Design Associate (CCDA). This certification is suitable for network engineers and others who specify network environments.

Although *associate* sounds better than *entry,* it fails to capture the magnitude of the work involved. First, you need a few years of experience in the field. Then, to pass the exam, you need to devote six to nine months (depending on whether you have no or a minimal social life) to studying and taking classes. This timeframe is if you take a preparation class and spend many hours each day pursuing your goal. Your mileage may vary, but any of these certifications is a significant accomplishment and shows a commitment of 1000+ hours. Plan to retake this test every three years to keep your CCNA or CCDA certification valid.

Professional level

The professional level certification, Cisco Certified Network Professional (CCNP), covers the same specializations as the associate level with the exception of video technology. If you happen to specialize in video-networking technology, you may be happy to find out that the certification is only at the associate level.

The test is given in a series of steps, so you don't have to take all the tests at one time. Each test covers different technology areas (route, switch, and troubleshoot). Some people who have earned the professional-level certification say that they studied rigorously for nine months to a year.

The professional level has that same naming outlier for senior network design engineers, senior analysts, and principal systems engineers who design the networks. Rather than being consistent and, say, calling the certification for design professionals CCNP-Design, the certification at the professional level is called the Cisco Certified Design Professional (CCDP) certification.

Expert level

If the professional level isn't enough for you, you can get an expert-level certification. Most are called CCIE, for Cisco Certified Internetwork Expert,

followed by the specialization. There's one change to again make things interesting. The step above CCNP Voice is CCIE Collaboration.

The old CCIE Voice was retired as of Valentine's Day 2014. (I am not sure of the significance of this date.) The CCIE Collaboration terminology reflects the idea that businesses use internal voice communication along with data and video technology to collaborate.

Again, there is the same naming outlier, the Cisco Certified Design Expert (CCDE). It sure would be a lot simpler if they called this CCIE Design, but they did not ask me.

The CCIE variants and CCDE require another year of study and hands-on practice beyond the time spent on the CCNP/CCDP. This level is pretty darn elite: In the United States, there are about 5500 CCIEs of all types.

Architect level

Let's put it this way. More people have fallen out of planes at altitudes above 10,000 feet and survived (157) than have earned the Cisco Certified Architect (CCAr) certification. More professional baseball players have hit four home runs in a single game (16) then have earned the CCAr. You get the idea.

But if not, more people have walked on the moon (12) than have earned the Cisco Certified Architect (CCAr) certification. Ten folks have earned the CCAr certification. We hope you become one. It looks very good on your resume. When you make it, send us a postcard about your accomplishment.

Microsoft

Microsoft makes a lot of software, but they also have technical certifications, specifically Microsoft Office certifications and Microsoft Technology certifications. The Microsoft Office certifications are good but are not our focus in this book.

The following Microsoft Technology certifications include topics that are relevant to networking:

- **Microsoft Technology Associate (MTA):** Covers the basic skills IT of infrastructure, database, and application development

- **Microsoft Certified Solutions Associate (MCSA):** Goes deeper into a particular piece of Microsoft technology

- **Microsoft Certified Solutions Expert (MCSE):** Focuses on an application category

Microsoft Technology Associate (MTA)-IT Infrastructure

The Microsoft Technology Associate (MTA)-IT certification offers multiple tracks. Readers of this book will be most interested in the MTA IT infrastructure track, which has the following four tests:

- ✔ Windows Operating System Fundamentals
- ✔ Windows Server Administration Fundamentals
- ✔ Networking Fundamentals
- ✔ Security Fundamentals

This certification is an entry-level (no IT experience) kind of test that is a good way to get started in the certification world. There are no requirements to prepare for taking the test.

Microsoft Certified Solutions Associate (MCSA)

Microsoft Certified Solutions Associate (MCSA) is proudly listed as a prerequisite for becoming a Microsoft Certified Solutions Expert in much of the promotional literature. However, it looks pretty good as a certification by itself. The Solutions Associate specializes in configuring and maintaining one of the following systems:

- ✔ Windows Server 2012
- ✔ Windows Server 2008
- ✔ Windows 8
- ✔ Windows 7
- ✔ SQL Server 2012
- ✔ SQL Server 2008
- ✔ Office 365

These certifications do not expire but the products in which you get the MCSA may expire. An MCSA in the Windows NT operating system will not open many doors for you these days.

All MCSA certifications involve multiple tests. You can take the tests in any order. A general guideline is that you should be able to take all three tests in 90 days if you focus on them. Hands-on experience with the technology is essential.

Microsoft Certified Solutions Expert (MCSE)

Now you are talking. Microsoft Certified Solutions Expert (MCSE) is a widely recognized certification that will impress the folks you want to impress. The MCSE can cover any of the following areas:

> ✔ Server infrastructure
>
> ✔ Desktop infrastructure
>
> ✔ Private cloud
>
> ✔ Enterprise devices and apps
>
> ✔ Data platform
>
> ✔ Business intelligence
>
> ✔ Messaging
>
> ✔ Communication
>
> ✔ SharePoint

One of the good things about the MCSE is that you can go ahead and earn the MCSE and pick up the MCSA as you complete the first two or three tests.

The MCSE is the highest certification that Microsoft currently offers. They used to offer a Microsoft Certified Architect (MCA) certification but cancelled the program because there were only a few hundred MCAs.

Juniper Networks

Juniper Networks makes sure that Cisco doesn't have all the fun. Their product lineup offers high-speed switching for enterprises and Internet service providers (ISPs). Juniper Networks is frequently second or third in market share across their range of solutions, which is not shabby at all.

Describing the Juniper Networks Technical Certification Program (JNTCP) is not easy because they have 19 certifications. Understanding which one is right for you involves understanding Juniper's primary product lines, target markets, and sales channels. Buckle up and let's start breaking this down.

First, the four levels of certification, in order of increasing difficulty, are

> ✔ Juniper Network Certified Internet Associate (JNCIA)
>
> ✔ Juniper Network Certified Internet Specialist (JNCIS)
>
> ✔ Juniper Network Certified Internet Professional (JNCIP)
>
> ✔ Juniper Network Certified Internet Expert (JNCIE)

All Juniper networks certifications start with one of these four levels. For example, an associate-level certification in Junos (JNCIA-Junos), the operating system used by most Juniper Network products, is a prerequisite for most of the other certifications.

In addition, Juniper Networks sells to enterprises and service providers, primarily Internet service providers. There are important differences between private network belonging to an enterprise (ENT) and Internet service providers (SP). For example, most enterprises have slow periods when they can accept some downtime. ISPs must support traffic on an almost continuous basis. Also, ISPs need accurate information flow into the billing system but enterprises want to track usage.

One area that is similar for enterprises and service providers is the network's information security. The tools and strategies for ensuring information security are identical whether the customer is an enterprise or a service provider, so Juniper Networks has a single certification track for people responsible for information security.

Figure 6-1 is a matrix of ten of the certifications offered by Juniper Networks.
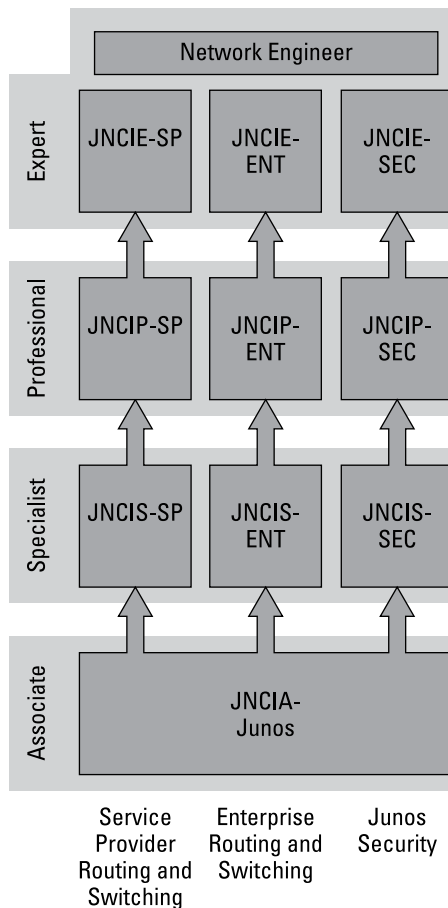
Figure 6-1:
Juniper
Networks
certifications for
network
engineers.

So far, so good. The next consideration is that Juniper Networks sells their solutions not only through a direct sales force to enterprises (ENTs) and service providers (SPs) but also through resellers. These resellers augment Juniper's direct sales force. Many of these resellers add value by offering network engineering services to their enterprise and service provider customers.

The network engineers employed by reseller organizations can earn the same certifications as everyone else at the associate and specialist levels. A source of confusion is that network engineers who work for these resellers are called support specialists, and it is easy to confuse this title with the level of Specialist used for the Juniper Network Certified Internet Specialist (JNCIS).

In other words, network engineers working for a reseller first earn their Juniper Network Certified Internet Associate for Junos (JNCIA-Junos) like everyone else. Next, they earn their Juniper Network Certified Internet Specialist-Enterprise (JNCIS-ENT) like everyone else.

Finally, these network engineers (also called service specialist) can pursue a certification strictly for resellers called Juniper Network Certified Service Professional-Enterprise (JNCSP-ENT) at the professional level. These service specialists can also earn JNCSP-SP to supporting ISPs and JNCSP-SP to become a professional on security issues.

That brings us to 13 certifications. The last several are related to specific product lines:

- ✔ **E-Series:** The E-Series routers are broadband edge routers.
- ✔ **Firewall/VPN:** Juniper makes a number of solutions for firewalls and to create VPNs.
- ✔ **Wireless LAN:** In 2010, Juniper acquired Trapeze Networks, a company that makes wireless LANs.
- ✔ **QFabric:** These products provide distributed connectivity for data centers.

The E-series has three levels of certification: associate (JNCIA-E), specialist (JNCIS-E), and professional (JNCIP-E). Do not confuse the *E* here with *ENT,* which refers to *enterprise.* And this brings us to 19 certifications for Juniper.

Palo Alto Networks

Palo Alto Networks specialize in firewalls and offer two certification programs based on their next-generation security products. (Yes, we know that this Dummies book focuses on networking and not information security, but you will help yourself by earning certifications in both.)

The Accredited Configuration Engineer (ACE) certification exam tests the candidate's knowledge of the core features and functions of the company's next-generation firewalls.

The Certified Network Security Engineer (CNSE) exam is a formal certification. Exam questions cover the following areas related to Palo Alto Networks firewalls:

- ✔ Administration and management
- ✔ Network architecture
- ✔ Security architecture
- ✔ Troubleshooting
- ✔ User identification
- ✔ Content identification
- ✔ Application identification

Check Point

Check Point Software Technologies, Ltd. offers the Check Point Certified Professional Program for network security. This is a product-focused certification based on the popular, but unimaginatively named Check Point Firewall-1. Certifications from Check Point include the following:

- ✔ **Check Point Certified Security Administrator (CCSA):** An entry-level certification for security administrators who have 6 to 12 months of work experience with Check Point security solutions. Candidates must pass an exam that covers the following topics:

  - Understanding Check Point technologies

  - Describing deployment platforms and security policies

  - Monitoring traffic and connections

  - Implementing network address translation (NAT)

  - Configuring user management and authentication

  - Using Check Point's SmartUpdate

  - Implementing identity awareness

  - Configuring virtual private network (VPN) tunnels

  - Resolving security administration issues

- ✔ **Check Point Certified Security Expert (CCSE):** Candidates must first earn the CCSA certification, and then take an additional exam that covers the same topics as the CCSA exam but at a more advanced level.

> ✔ **Check Point Certified Managed Security Expert (CCMSE):** For security administrators who manage large or virtualized network environments. The candidate must first earn the CCSE certification, and then pass an additional exam covering the following topics:
>
> - • Installing, configuring, and managing a multi-domain management (MDM) environment
>
> - • Understanding common deployment scenarios
>
> - • Understanding the traffic inspection process
>
> - • Configuring domain management server (DMS) high availability
>
> - • Configuring and implementing a global policy
>
> - • Applying common troubleshooting practices

Red Hat

The Red Hat Certificate of Expertise in Server Hardening is for security professionals with skills and experience in

> ✔ Configuring file systems and volumes for more restrictive security policies
>
> ✔ Implementing additional user account security and identity management
>
> ✔ Configuring enhanced, secure logging, and audit capabilities
>
> ✔ Identifying and performing appropriate package updates in response to Common Vulnerabilities and Exposure (CVE) and Red Hat Security Advisory (RHSA) reports

Other vendor-specific certifications

The Cisco and Microsoft certifications are the best known but are by no means the only certification programs with street cred. Following is a sampling of other vendors offering certification programs related to networking:

> ✔ Avaya
>
> ✔ Apple
>
> ✔ Hewlett-Packard
>
> ✔ LANDesk
>
> ✔ Novell
>
> ✔ SolarWinds

Winning with a Third-Party Networking Certification

A number of organizations that are not affiliated with a particular vendor are well respected in certifying the abilities of their graduates. Typically, these certifications originate at nonprofit organizations seeking to ensure quality standards among technical or support professionals. Because these certifications are not affiliated with a particular vendor, they are referred to as third-party certifications.

CompTIA

The best-known organization for providing networking technology certifications is CompTIA (Computing Technology Industry Association), a nonprofit trade association. The original motivation for creating their certifications was to provide a minimal level of expertise among the workforce so that customers could have some degree of confidence that the holder of the certification is competent.

CompTIA started in 1982 and was then called the Association of Better Computer Dealers (ABCD). Keep in mind that Microsoft DOS was released in 1981. PCs were new technology, and computer dealers found that any schlub could hang up a shingle and claim to be qualified to repair the PCs that were just coming out on the market.

These so-called repair technicians were not suited to repair anything as intelligent as an 8086 computer. To prevent the industry from getting a bad reputation among customers, the dealers banded together to create standards. The ABCD consortium was the origin of CompTIA's A+ certification for computer technicians.

The current A+ certification, which was updated in 2012, is comprised of two tests: CompTIA Essentials and CompTIA Practical Application.

The Essentials portion of the exam covers the basics of computer technology, networking, and security for hardware and operating systems. The Practical Application portion demonstrates the use of current operating systems.

CompTIA is probably best known for the A+ certification, but their other certifications are highly respected and valued. Some certifications are

difficult to categorize; we group them from the perspective of this book as follows:

- ✔ Network-related technology certifications
- ✔ Non-network technology certifications
- ✔ Technology skills certifications
- ✔ Strata certifications

Network-related technology certifications

Three certifications are relevant in one way or another to networking:

- ✔ **CompTIA Network+:** A well-respected, vendor-neutral certification for networking professionals. To earn this honor, expect to put in a lot of work for about nine months, with hands-on training.
- ✔ **CompTIA Security+:** A big benefit for those working in networking. Be ready for another nine months of classroom and hands-on training to get this one.
- ✔ **CompTIA Advanced Security Practitioner (CASP):** Intended for people who have been working in security for more than five years or in IT for more than 10 years.

Non-network-technology certifications from CompTIA

Although the following certifications are not specifically network-centric, there are elements of networking and operating systems technology in them that would have value to an aspiring network engineer:

- ✔ CompTIA Mobility+
- ✔ CompTIA Mobile App Security+
- ✔ CompTIA Server+
- ✔ CompTIA Cloud Essentials
- ✔ CompTIA Cloud+
- ✔ CompTIA CTP+ (Convergence Technology Professional)
- ✔ CompTIA Linux+ Powered by Linux Professional Institute
- ✔ CompTIA Storage+ Powered by Storage Networking Industry Association

Technology skill certifications

Technology skill certifications may be useful for someone focused on or seeking a career in networking (more on this later in this chapter). Note that each

of the following certifications involves a significant commitment of time and resources:

- **CompTIA CTT+:** This certification is for technical trainers. Technical trainers, as the name implies, demonstrate skills for teaching technical audiences.

- **CompTIA Project+:** Project management is an important skill, particularly in the IT environment. Project managers keep large-scale initiatives coordinated across a range of individuals, departments, and vendors. CompTIA provides a certification associated with learning these skills.

- **CompTIA PDI+:** This certification is associated with printing and document imaging. Although the paperless office was first discussed in the 1960s, US Census data shows that the use of printing continues to grow. The implication is that businesses need more PDI+ers.

- **CompTIA CDIA+:** Companies need advanced PDI+ers too. The certification above the CompTIA PDI+ certification is CompTIA CDIA+, which stands for Certified Document Imaging Architect.

- **CompTIA Social Media Security Professional:** This professional certification helps companies against hackers who enter networks through social media.

- **CompTIA Healthcare IT Technician:** Folks who work in the healthcare industry must comply with extra rules to ensure patient privacy and need to understand the industry's terminology. A prospective employer would know that a person with this certification has been exposed to all the relevant rules.

Strata certificates

CompTIA offers not only certifications but also certificates for particular areas of study. Earning a certification is more involved than earning a certificate, and therefore better. (Unfortunately, the names are similar.)

CompTIA certificates are prefaced with the *Strata* to distinguish them from certifications. They include the following:

- **Strata IT Fundamentals:** A more basic certification than A+.

- **Strata for Sales:** Ensures that the certificate holder has enough knowledge to talk to customers about their technical needs.

- **Strata Green IT:** This certificate teaches the many small changes that an IT organization can enact that will help the environment and minimally affect cost or performance.

Network Professional Association

Network Professional Association (NPA) is a nonprofit association for computer network professionals that offers the Certified Network Professional (CNP) Program. The primary goal of NPA is to raise the awareness of technical people working in networking as a profession by setting standards for ethics, training, and performance.

This approach is slightly different than the vendor-specific and the third-party certification programs in that no moral judgments are associated with the other certifications. They are purely technical.

The Network Processionals Association, on the other hand, may have issues with a CNP who designs a network to trade in blood diamonds and speed the burning of the Amazon rainforest while taking bribes from vendors and spying on its critics. Certainly, all the organizations mentioned in this chapter would have concerns, but the technical certifications are independent of any ethical judgments.

Planet3 Wireless

Planet3 Wireless is an organization that certifies wireless LAN professionals. Their certification focus on 802.11 wireless LANs. The certifications, in approximate order of easiest to hardest, include:

- ✔ **Certified Wireless Network Administrator (CWNA):** A basic course for individuals who will administer enterprise-class wireless LANs. CWNA is a prerequisite for the other certifications.

- ✔ **Certified Wireless Technology Specialist (CWTS):** A more in-depth certification than CWNA.

- ✔ **Certified Wireless Analysis Professional (CWAP):** Training on how to analyze, troubleshoot, and optimize an enterprise wireless LAN. Offered after you master the previous two certifications.

- ✔ **Certified Wireless Security Professional (CWSP):** The certification to keep pesky hackers from entering the corporate network.

- ✔ **Certified Wireless Network Expert (CWNE):** The top certification for 802.11 wireless LANs. It requires extensive experience operating wireless LANs in the corporate environment plus the previous four certifications and documented expertise.

- ✔ **Certified Wireless Network Trainer (CWNT):** If you are so smart, you should teach the class, but not before you earn this certification.

Earning a Vendor-Neutral Security Certification

Even though you may not be looking for a security job or even a security career, security is important in every IT job, especially networking! Chances are you'll be managing the security aspect of systems, devices, or users, and you'll be far more marketable if you have one or more security certifications.

International Information Systems Security Certification Consortium (ISC)²

Founded in 1988, (ISC)² (pronounced "I-S-C-squared") was formed to create a global information security certification program. In 1994, the CISSP certification was established, and it has since been recognized as one of the top security certifications in the profession. Some of the certifications offered by (ISC)² are described in this section.

Systems Security Certified Practitioner (SSCP)

Systems Security Certified Practitioner (SSCP) is the entry-level certification offered by (ISC)². Requiring as little as one year of professional experience, the SSCP certification is great for professionals who are working to establish their security careers.

Certified Information Systems Security Professional (CISSP)

Universally recognized as the greatest of all information security certifications, Certified Information Systems Security Professional (CISSP) covers a broad swath of subject matter in its Common Body of Knowledge (CBK):

- ✔ Access control
- ✔ Telecommunications and network security
- ✔ Information security governance and risk management
- ✔ Software development security
- ✔ Cryptography
- ✔ Security architecture and design
- ✔ Security operations
- ✔ Business continuity and disaster recovery planning

> ✔ Legal, regulations, investigations, and compliance
>
> ✔ Physical (environmental) security

The CISSP exam contains 250 multiple-choice questions and may take you up to six hours to complete.

Several CISSP concentrations are now available to CISSP holders who want to extend their certification into one of three important specialties:

> ✔ CISSP-ISSAP (Information Systems Security Architecture Professional)
>
> ✔ CISSP-ISSEP (Information Systems Security Engineering Professional)
>
> ✔ CISSP-ISSMP (Information Systems Security Management Professional)

You can learn more about the CISSP certification in *CISSP For Dummies,* 4th Edition, by Lawrence C. Miller and Peter Gregory.

Certified Software Security Lifecycle Professional (CSSLP)

The Certified Software Security Lifecycle Professional (CSSLP) certification recognizes expertise in the *security development life cycle,* which is the set of business processes and techniques that ensures the inclusion of security in every step of the software development process.

The range of subject matter in this certification includes

> ✔ Secure software concepts
>
> ✔ Security software requirements
>
> ✔ Secure software design
>
> ✔ Secure software implementation/coding
>
> ✔ Secure software testing
>
> ✔ Software acceptance
>
> ✔ Software deployment, operations, maintenance, and disposal
>
> ✔ Supply chain and software acquisition

Certified Cyber Forensics Professional (CCFP)

The Certified Cyber Forensics Professional (CCFP) certification is a recognition of skills and experience in the field of *computer forensics,* the science of conducting sound digital investigations that may be used in legal proceedings.

The range of subject matter in this certification includes

- ✔ Legal and ethical principles
- ✔ Investigations
- ✔ Forensic science
- ✔ Digital forensics
- ✔ Application forensics
- ✔ Hybrid and emerging technologies

Certified Authorization Professional (CAP)

The Certified Authorization Professional (CAP) certification recognizes skills and knowledge in the work of authorizing and maintaining information systems in the Risk Management Framework as defined in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*.

The range of subject matter in this certification includes

- ✔ Risk management framework (RMF)
- ✔ Categorization of information systems
- ✔ Selection of security controls
- ✔ Security control implementation
- ✔ Security control assessment
- ✔ Information system authorization
- ✔ Monitoring of security controls

Healthcare Information Security and Privacy Practitioner (HCISPP)

The Healthcare Information Security and Privacy Practitioner (HCISPP) certification recognizes expertise in the protection of personal health information. The range of subject matter in this certification includes

- ✔ Healthcare industry
- ✔ Regulatory environment
- ✔ Privacy and security in healthcare
- ✔ Information governance and risk management
- ✔ Information risk assessment
- ✔ Third-party risk management

(ISC)² also offers an *Associate of (ISC)²* Certification, for those who have passed CISSP, CSSLP, CAP, SSCP, CCFP, or HCISPP but do not yet have the required years of experience to be awarded the certificate.

ISACA

ISACA was formerly known as the Information Systems Audit and Control Association. They are now ISACA to show that they are known for more than just audits and controls. This nonprofit organization is dedicated to the development of frameworks, standards, guidance, education, and certifications for professionals in information systems audit and security management.

ISACA certification exams are conducted a limited number of times per year, at hundreds of locations around the world.

Certified Information Systems Auditor (CISA)

Enacted in 1978, the Certified Information Systems Auditor (CISA) certification is one of the most prestigious security certifications available in the industry. This certification covers the following subject matter:

- ✔ Information systems audit
- ✔ IT governance
- ✔ Systems and infrastructure life cycle
- ✔ IT service delivery and support
- ✔ Protection of information assets
- ✔ Business continuity and disaster recovery planning

The CISA certification is frequently required for IT audit professionals in positions focused on IT audit or IT audit management.

Certified Information Security Manager (CISM)

The Certified Information Security Manager (CISM) certification is recognition of the skills, knowledge, and experience of security managers. The CISM certification covers the following subject matter:

- ✔ Information security governance
- ✔ Information risk management and compliance
- ✔ Information security program development and management
- ✔ Information security incident management

Certified in the Governance of Enterprise IT (CGEIT)

Certified in the Governance of Enterprise IT (CGEIT) is a certification aligned more with IT management than IT security. The CGEIT certification covers the following domains:

- ✔ Framework for the governance of enterprise IT
- ✔ Strategic management
- ✔ Benefits realization
- ✔ Risk optimization
- ✔ Resource optimization

Certified in Risk and Information Systems Control (CRISC)

Certified in Risk and Information Systems Control (CRISC) is ISACA's newest security-related certification. With heavy emphasis in risk management and controls, CRISC complements CISA and CISM, and the three together provide comprehensive control over information security management and operations.

The CRISC certification covers the following domains:

- ✔ Risk identification
- ✔ Risk assessment
- ✔ Risk response and mitigation
- ✔ Risk and control monitoring and reporting

SANS Institute

Along with the (ISC)^2 Certified Information Systems Security Professional (CISSP) certification, discussed later in this chapter, Global Information Assurance Certification, or GIAC certifications are among the most widely known and respected security industry certifications today. The SANS (SysAdmin, Audit, Networking, and Security) Institute Global Information Assurance Certification (GIAC) program validates the skills and knowledge of security professionals, practitioners, and developers through nearly 30 certifications, which are grouped into the following categories:

- ✔ **Security administration:**
  - GIAC Security Essentials (GSEC)
  - GIAC Certified Incident Handler (GCIH)
  - GIAC Certified Intrusion Analyst (GCIA)

- GIAC Certified Penetration Tester (GPEN)
- GIAC Web Application Penetration Tester (GWAPT)
- GIAC Certified Perimeter Protection Analyst (GPPA)
- GIAC Certified Windows Security Administrator (GCWN)
- GIAC Information Security Fundamentals (GISF)
- GIAC Assessing and Auditing Wireless Networks (GAWN)
- GIAC Certified Enterprise Defender (GCED)
- GIAC Certified UNIX Security Administrator (GCUX)
- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
- GIAC Mobile Device Security Analyst (GMOB)
- GIAC Global Industrial Cyber Security Professional (GICSP)
- GIAC Critical Controls Certification (GCCC)

✔ **Forensics:**
- GIAC Certified Forensic Analyst (GCFA)
- GIAC Certified Forensics Examiner (GCFE)
- GIAC Reverse Engineering Malware (GREM)
- GIAC Network Forensic Analyst (GNFA)

✔ **Management:**
- GIAC Security Leadership Certification (GSLC)
- GIAC Information Security Professional (GISP)
- GIAC Certified Project Manager Certification (GCPM)

✔ **Audit:**
- GIAC Systems and Network Auditor (GSNA)

✔ **Software security:**
- GIAC Secure Software Programmer — .NET (GSSP-NET)
- GIAC Secure Software Programmer — Java (GSSP-JAVA)
- GIAC Certified Web Application Defender (GWEB)

✔ **Legal:**
- GIAC Law of Data Security & Investigations (GLEG)

✔ **Security expert:**
- GIAC Security Expert (GSE)

The GSE is the most prestigious certification in the GIAC family. To earn the GSE, you must successfully complete a 75-question, three-hour exam, followed by a two-day lab exam. Prerequisites include the GSEC, GCIH, and GCIA certifications.

Most GIAC certifications correspond to SANS Institute training courses. However, attending a SANS course is not required to earn GIAC certification. SANS GIAC recommends a minimum of 55 hours of study (in addition to any formal training courses) to prepare for a GIAC certification exam.

Earning Other Relevant Certifications

As if these certifications weren't enough, other certifications can help you professionally in the networking space. Some of these specializations include the following:

- **Technical training:** All of us have had at least one disappointing experience in receiving technical training. The trainer probably did not have a certificate in training techniques. If you want to become a technical trainer, seriously consider earning a certificate that demonstrates your capability in this area.

- **Project management:** If you're a Boy Scout who has earned his Eagle badge, you have run a project. The rest of us either figure out on-the-fly how to keep a complex project on track or take a course in project management. The best-known project management certification is the Project Management Institute's Project Management Professional (PMP).

- **IT quality auditing:** ISO 9001 is a business evaluation that measures the quality of management systems in general. An important IT component ensures that IT systems are consistent with quality programs throughout the organization. Many certification options are available for quality systems implementation and auditing.

Chapter 7

Making Your Own Way

*Y*ou walk to the beat of a different drummer. Perhaps college, vocational, or technical school is not for you, and those expensive training boot camps are out of reach. Fear not: You can find plenty of opportunities to gain skills and experience to parlay into a full-time networking job.

You bought this book because you're a self-starter. If you're going to dive in and learn networking with the hands-on techniques discussed in this chapter, you're a self-starter on steroids — the best kind! By their very nature, most technology workers are curious and driven to learn, and you shouldn't be surprised to discover that many networking professionals — even those well established in their careers — employ one or more approaches discussed in this chapter. For them, what they do in their day job is not enough. They want more — and they get more by using one of the means discussed here.

Put these ideas to work, and you'll be well on your way to becoming a hacker. We mean *hacker* in the traditional, positive sense: a hobbyist, a tinkerer, someone who wants to get inside the technology to learn how it works and make it better.

We cite several books in this chapter. Dozens of titles in the *Dummies* series can help smart people like you learn more about almost any networking technology.

Informal Education in Networking

With a desktop, laptop, or tablet computer and a decent Internet connection, the world is your oyster! Search your way to knowledge on just about any networking topic you want. Here are a few specific ideas:

- ✔ **Product websites:** Search on a networking topic (*firewall products,* for example) and visit the vendors' sites. View their product demos and download their whitepapers. You might be able to sign up for a webinar, in which experts describe and demonstrate products and how they are used for business.

- ✔ **Tech magazines and their websites:** Here you'll find articles on new and changing technologies as well as product evaluations and bake-offs. These articles are another great way to learn from the experts.

- ✔ **Vendor seminars:** Many vendors and integrators do live seminars that often include demos by technology experts. Sometimes existing customers attend to learn more, and you can learn from their experience.

- ✔ **Product evaluations:** Most vendors provide a way to let companies try out their products on-site. For software products, trying out products is usually as simple as downloading the product and obtaining an evaluation license key from a sales representative. For hardware products, the process is a little more complicated; your company will need to sign an agreement promising to purchase or return the equipment at the end of the evaluation period.

- ✔ **Networking club meetings:** Birds of a feather flock together, and this includes technologists and networking professionals. Find out where they meet and attend a few different meetings. Often they'll have speakers who will describe and demonstrate tools and techniques. You'll find helpful people who will answer your questions and help you learn more.

Chapter 21 lists ten networking books that will help to expand your knowledge.

One of our favorite sites for technical hobbyists is `www.hackaday.com`. This site publishes a rich variety of do-it-yourself computer and electronics projects.

Setting Up Your Own Lab

Hardware and software are becoming so inexpensive that many networking professionals have set up labs in their homes, under their desk at work, or online at Amazon Web Services (AWS) (`http://aws.amazon.com`) or

Microsoft Azure (`http://Azure.Microsoft.Com`). Depending on your own working and learning situation, you can use this setup to experiment with new ideas, as your primary source of learning, or to try out things that will get you in trouble if you did so on production systems!

Equipment

The equipment you'll want depends on what you want to learn. However, the following basic equipment is required for most anything you'll be doing:

✔ **Firewall:** Whatever you're doing, you will want to segregate it from your home or work network. But if you want to air gap your lab by isolating it from the Internet and work or home network, you'll need a firewall only if that's the subject you're learning.

✔ **Switch:** Chances are you'll be connecting things. A network switch is like duct tape.

✔ **Access point:** Unless all your tinkering will involve Ethernet, you'll want a wireless access point, particularly if you'll be using mobile devices. Consider *not* broadcasting your SSID.

✔ **Computers:** Whether you're tinkering with server or desktop operating systems, and whether you're virtualizing, you need at least one computer to run this stuff, right?

Figure 7-1 depicts a typical networking lab setup.

WARNING!

We'll say it again: A firewall is indispensable when experimenting with systems and networking technologies, and keeping your experiments separate from home or work networks.
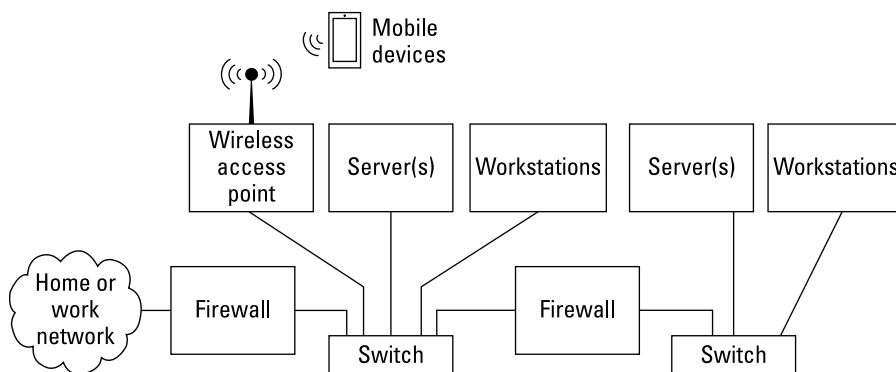
Figure 7-1: A typical networking lab setup.

WARNING!

You need to obtain permission to set up your own lab at work, even if it's firewalled or air-gapped (isolated).

Operating systems

A lab without operating systems is like a bicycle without wheels. Okay, corny metaphor aside, you'll need operating systems for storing data, scanning, sniffing, and just about everything else you'll want to do in your networking lab.

Windows

If the subject of your work involves Windows desktop or Windows servers, you'll need to purchase these licenses from Microsoft or an authorized reseller. Because so many organizations that you may want to work for use Microsoft products, including Active Directory, SharePoint, Exchange, and SQL Server, you'll need enough licenses to cover all the products that you install in your learning and testing network.

TIP

Microsoft offers free evaluation of many of its server products. Information is available at `www.microsoft.com/en-us/evalcenter/`. If you are a student with verifiable student credentials, you can get large discounts on Microsoft products at `www.microsoft.com/en-us/education/students/deals/default.aspx`.

Mac OSX

With so many Macs in use in organizations, you'll want to consider getting a Mac. You know you want one of those hipster machines.

TIP

If you can't or won't get a Mac, remember that OSX is Unix underneath. Depending on what you'll be doing in your lab, one of the free versions of Unix might work for you.

A copy of *MacBook For Dummies,* 5th Edition, by Mark L. Chambers or *Macs For Dummies,* 13th Edition, by Edward C. Baig will help you get started on Macs in your lab.

Linux

The quintessential hobbyists' operating system, Linux is powerful, versatile, and free! You can choose from many useful flavors, such as Ubuntu, Kali Linux, Centos, and Arch Linux.

Consider picking up a copy of *Linux For Dummies,* 9th Edition, by Richard Blum to learn more about Linux.

Linux is legendary for breathing new life into older hardware. Before discarding that laptop or desktop system because it suffers under newer releases of Windows, try loading Linux on it. You might be pleasantly surprised.

Virtualization

Packing one or more running operating systems into a single server, or even a desktop or laptop, is all the rage. Whether you want to learn more about virtualization or use virtualization to make the most of your lab budget, virtualization is a great way to build and manage your lab and to reduce the number of plug strips you need to buy.

Our favorite virtualization system is Oracle VirtualBox. It's free, and within it you can run various operating systems and even virtual network devices, all in your personal virtual networking lab inside your desktop or laptop system. You can obtain VirtualBox at `www.virtualbox.org`.

You can obtain virtual network appliances from several sources, such as

- **Endian Community firewall:** `www.endian.com/us/community/download/`
- **M0n0wall firewall:** `http://m0n0.ch/wall/downloads.php`

The book *Virtualization Essentials* (Sybex) will provide you a lot of information on using virtualization to its fullest in your lab.

Volunteering

Many nonprofit groups need to use computing technology for recordkeeping and other tasks. Typically, they have no employees who understand technology like you do, and chances are they would appreciate your help. You just might meet the IT manager of a local company who is also volunteering at the local nonprofit.

You might be able to help by setting up

- Computers and printers
- Internet connectivity
- Wireless networking, including guest access
- Corporate email

WARNING!

If you're asked to build a website for the organization, realize that you need a lot of security expertise to keep the site from being compromised.

Following are some organizations that might want your help:

- ✔ Smaller private schools
- ✔ Libraries
- ✔ Churches
- ✔ Retirement homes
- ✔ Service clubs

If you're just starting out in your networking career, consider being a networking volunteer's apprentice: Offer to help a networking professional who already helps out with computers and networks in a nonprofit organization. You'll be surprised at what you can learn. And someday, you might be that senior person who mentors an apprentice.

Working on the Side

The inside joke in the technology business is that every IT worker does consulting on the side. Well it's not a joke, but the truth. Except for employees who are overworked to the point that sleep is their only other interest, many IT workers help nonprofits or small businesses for a modest hourly rate. You can charge by the hour or by the job, or you can barter.

Providing your skill at a reduced rate is a great way to get work experience if you're just starting out. However, don't take on anything that is way beyond your understanding. Otherwise, you could make matters worse for the organization you're trying to help. Worst case: You could end up paying someone to fix your goof, and that would be an expensive way to learn from your mistakes.

WARNING!

If you work on the side, find answers to the following:

- ✔ Do you need to have a business license?
- ✔ Should you form a corporation or limited liability company (LLC)?
- ✔ Should you obtain liability insurance to cover your side work?
- ✔ Does your employer have any conditions regarding the side work?

On-the-Job Training

Many people advance in their careers by taking on additional responsibilities, tasks, skills, and knowledge. Most employers appreciate workers who want to continue learning and doing more. These are the same employees who also think up better ways of doing things, therefore saving the company money or helping it make its products or services better or less expensive to produce.

Most senior technologists appreciate requests for mentorship or offers of assistance from junior staffers. Perhaps it strokes their ego, but usually they'll recall when they were starting out and how they struggled to learn more about networking.

You can start by talking with your manager or with one or more senior staffers. Explain that you want to learn more about networking and that you are offering to help on your own time. Most IT departments are short staffed and will readily accept additional help from people with aspirations to grow their careers.

Make sure you are meeting all your present work obligations (on time and with the required quality) before asking for more responsibilities. Regardless of how well you do where you are volunteering or mentoring, failing to meet your present work obligations and responsibilities will derail your efforts to move in the direction you want with your career and current employer.

Finding a Job with the Right Organization
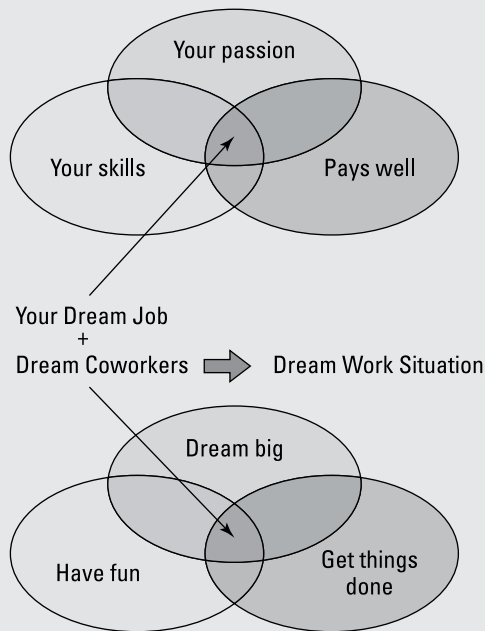
Your passion

Your skills

Pays well

Your Dream Job
+
Dream Coworkers ⟹ Dream Work Situation

Dream big

Have fun

Get things
done

In this part . . .

- ☛ Consider the range of employers.
- ☛ Think about your preferences.
- ☛ Evaluate risk and reward.
- ☛ Set your direction.

Chapter 8

Working for a Networking Solutions Provider

In This Chapter

▶ Pitching products and services as a pre-sales engineer

▶ Implementing your company's products

▶ Helping your customers with difficulties

*A*s an employee in a network solutions company, you'll have a role in the sales, support, implementation, or management of your company's products or services (or both). Most of these positions are "customer facing," meaning you'll be working with customers in person or by phone. You'll need above-average people skills because you'll be representing your company in front of customers and prospective customers, often with a sales executive but sometimes alone.

In this chapter, you find out about a variety of networking-related roles in network solutions provider organizations.

Working in Sales as a Pre-Sales Engineer

As a pre-sales engineer, you accompany sales executives on sales calls to clients and prospective clients, explaining the wondrous features of the hardware products, software products, consulting, and other services that your company provides. You'll be looked upon as the expert in the room who can take your salesperson's comments deeper with real-life examples about how your company made other clients successful.

This job, however, entails a lot more than just smiling, nodding, and tossing in an occasional tale or two:

- ✓ **Conducting product demos:** You might conduct a demonstration of your company's product or provide a depiction of its operation. You describe in technical terms what your product is doing and explain what the customers are viewing. In some cases, you set up a demo, also called a POC (proof of concept), in the customer's environment. When this is the case, you'll have limited time and possibly operational limitations. However, a POC will give an organization a good understanding on whether your product will actually work for them.

- ✓ **Designing solutions:** You design solutions that will work in your customers' environments. You select one or more products, create configurations or specifications related to sizing or other characteristics, and create documents or drawings to depict how your company's solution will work in the customer's network. The documents that you create may be part of a formal statement of work or proposal, which you might write on your own or with others in your company.

- ✓ **Creating price quotes:** You may be responsible for creating price quotes that your customer will use to make a purchasing decision. These price quotes include all hardware or software components necessary for the product to work correctly in the customer's environment. A quote might also include installation, integration, and training services. Often, you have to estimate the level of effort (LOE) and hourly consulting rate required for each of these.

- ✓ **Creating consulting proposals:** You may be creating consulting engagements for other networking experts to perform device or system health checks, compliance reviews, architecture reviews, or the development of new architecture. You may need to get information from your customer so that you can estimate the level of effort required for the consulting engagement. You might be the lucky person who gets to write the proposal and determine final pricing, although with most solutions providers, others will double-check your work and help you finalize all pricing.

- ✓ **Developing architectures:** You may work alongside experts in the customer's organization to develop an architecture — which could be a drawing, a technical specification, or both — that depicts your company's product in their environment. The plan to use your product in the customer's environment may necessitate changes to the customer's environment and additional equipment from other vendors.

For more information on the role of a networking consultant, see Chapter 12.

As a part of the sales organization, you'll probably have a sales quota, a commission, or other incentives such as *spiffs* (cash or non-cash rewards) to help your sales executive sell as much product or service as possible.

If you work with more than one sales executive, you'll have to decide who to help when two sales executives want you to attend a sales meeting at the same time in different locations. Even when everyone in a company can view their coworkers' appointment calendars, sometimes conflicts are unavoidable. Good negotiation skills are required so that you can artfully explain why you are attending one salesperson's meeting instead of another.

You'll also need to attend training sessions about your company's products (including new features and information on size, scope, and price). These sessions will add to your expertise and give your customers confidence that you really do know what you're talking about when you help them imagine success with your products.

If you work for a value-added reseller (VAR), you need to gain expertise in each of the products that your company sells. In larger companies, you might have to be familiar with products from *dozens* of different manufacturers!

Rolling Up Your Sleeves as an Implementation Engineer

As an implementation engineer, you install and configure your company's product in the customer's environment. Often, you visit the company's headquarters or other locations where the product will be installed or used. For a cloud-based product, you may still be on-site to work face to face with the customer's employees to get the product up and running correctly and perhaps provide informal training.

A job as an implementation engineer is great when things go well, but sometimes you will have unanticipated challenges, such as the following:

- **Functionality gap:** Sometimes salespeople are overzealous when pitching the product. When customers discover that the product does not in fact take out the garbage or create lattes, they may display their dissatisfaction and ask you to move heaven and earth to make it right.

- **Product DOA (dead on arrival):** It can be embarrassing when a product simply doesn't work! Your problem-solving skills will be put to the test as you plead with people in your organization to get replacement

hardware shipped to the customer as soon as possible. You'll need to make good use of your time (which may be billable), or leave and then return when the replacement product arrives.

✔ **Product undersized:** The product may be too small (not enough storage, or network throughput, for instance) and not work well in the customer's environment. Perhaps the sales engineer did not correctly size the product, or the customer was unaware of relevant environmental conditions.

✔ **Missing components:** The pre-sales engineer might not have included all necessary components for the product to work properly. You'll have to work with others in your organization to get replacement components shipped right away.

✔ **Licensing issues:** Sometimes there are difficulties activating a license that's required to get a product running. You'll need to know who to call to quickly get sticky license issues fixed.

✔ **Underqualified customer personnel:** Sometimes the customer's organization doesn't have a person with the necessary skills and knowledge to successfully operate the product after you've set it up. You'll need to tactfully bring up this situation without offending the customer. You need to inform your own management as well (and maybe they'll inform the customer and take the heat for you).

These situations will draw on your relationship and negotiation skills. You'll need to stay cool, help your customer separate emotion from fact, and keep your customer at ease and give him or her confidence in your ability to solve the problem. You are, after all, the expert in all things about your product and your organization — but make sure that you know who in your organization can help you in a crisis.

Helping Customers in Technical Support

As an expert in one or more of your company's products (or other companies' products if you work for a value-added reseller), you receive calls for assistance from a customer who is having some kind of difficulty.

Like an automobile mechanic whose customer complains vaguely about a rattle, your customer's call for help may include imprecise or ambiguous descriptions of a problem. Your skills as a kind, empathetic, expert listener and troubleshooter will guide you as you ask key questions to get to the root cause of the problem.

Customers are not often in a good mood when they're having difficulty with a system. What's more, they may be under pressure to get systems up and running again, and your product's problem may be standing in the way. You'll need to stay cool and collected, keeping the customer confident in your company's ability to stand behind them and solve their problem.

If you're in luck, your company will have good information to help you troubleshoot your customers' problems, with a knowledge base (KB) or other references to guide you. As you gain expertise, you may be contributing to the knowledge base, helping your colleagues and those who follow you. If your company doesn't have a good KB, you might struggle for a time in your support role until you gain more knowledge and expertise in the inner workings of the products you support for your customers.

Watching the Fort for a Managed Service Provider

A managed services provider (MSP) is an organization that provides services to customers who do not have the resources to perform these services on their own. An MSP will provide one or more of the following services to its customers:

- **Monitoring:** You use systems or network monitoring tools to observe the general health of a customer's critical systems or support the network infrastructure or both. When alarms (visual alerts indicating a malfunction or security issue) are displayed, you'll follow procedures specific to each type of problem. These procedures could also vary from customer to customer.

- **Systems management:** You manage network devices, servers, and storage infrastructure for multiple customers. You make configuration changes, upgrade device software, and watch the health of the infrastructure.

- **Incident response:** You monitor systems and networks for security incidents. When an incident is detected, you use tools to drill into affected systems to begin isolation, containment, and recovery operations. You participate in conference calls with affected clients to listen to their needs and inform them of your company's efforts.

A position in an MSP is a great place to start a networking career because you are exposed to enterprise tools and mature processes, and are surrounded by networking and security experts with a lot more experience than you.

"When it rains, it pours." This saying by a table salt manufacturer applies to the MSP business. Boredom can give way to frantic intensity when two or more customers have serious issues simultaneously. This type of job can be a bit like that of an airline pilot: interesting and challenging at takeoff and landing but boring in between. But in an MSP, as when flying an airplane, constant diligence is key.

Chapter 9

Working as an In-House Networking Professional

In This Chapter

▶ Understanding work in the private sector

▶ Comparing smaller and larger organizations

▶ Looking at networking jobs in various industry sectors

*M*ost networking professionals work as in-house experts, directly or indirectly contributing to the ongoing operation of their employer's systems and networks.

Networking jobs in private sector and nonprofit companies vary widely by industry, company size, and other factors. Some people prefer to be a one-man-band in a small company, responsible for all aspects of the systems and networks. Others prefer larger companies and to work as part of an information technology team or department. You must decide what you'll like best and where you can be successful.

Living Your Destiny

Probably the most distinguishing characteristic of being an in-house versus a consulting networking professional is that you're in the organization for the long haul. Consultants or contractors come in for a specific task or project and then leave, usually long before anyone realizes the consequences (good or bad) of their work. But as an in-house networking professional, you'll reap the fruits of your labor for years.

When you make a good decision, you'll enjoy the outcome and at times even bask in it. But when you make a poor decision, you'll be around to see the consequences and any discomfort that may result. However, you'll have the opportunity to improve both bad and good situations to make them even better.

Working in the Private Sector

Private individuals (or a group or people) own and run *private sector organizations.* A *private sector* company may also be publicly owned, meaning that all or part of its ownership is through publicly traded shares. And not to confuse you, but a *private company* is a private sector company that is privately owned, not owned through publicly traded shares.

The majority of jobs in the United States are in the private sector. In late 2014, there were 119 million non-farm jobs in private industry and 22 million jobs in government.

Industry regulations

People in many professions tend to work in one industry for much of their career, although they may change employers within an industry. Employers tend to select candidates for employment based on their past experience in the industry, which also tends to keep people in a particular industry sector.

Each sector in the networking field has its own regulations regarding the protection of information and information systems. Although information security professionals often take responsibility for translating regulations into company operations, networking professionals often do this task in smaller organizations that lack dedicated security staff. Familiarity with these regulations also tends to keep a networking professional tied to a specific industry sector. Table 9-1 provides a sample of industries and the regulations related to information security.

Many organizations are subject to multiple sets of regulations. For instance, a publicly traded healthcare organization that accepts payments by credit card would be subject to the Sarbanes-Oxley Act, Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), and U.S. state laws requiring public disclosure of breaches of personally identifiable information. As a result, the organization may have to enact a complex set of IT controls and endure multiple

external audits per year. These requirements, in part, drive demand for networking professionals: Companies need people who are familiar with these different security control frameworks and can implement them effectively and efficiently.

Table 9-1	Industry Sectors and Information Security Regulation
Industry	**Information Security Regulation**
Any public company	Sarbanes-Oxley
Financial sector	Gramm-Leach-Bliley Act (GLBA)
Public utility	North American Electric Reliability Corp (NERC); Federal Energy Regulatory Commission (FERC)
Healthcare	Health Insurance Portability and Accountability Act (HIPAA)
Pharmaceuticals	Food and Drug Administration (FDA)
Any company doing business with the public	Federal Trade Commission (FTC)
Any company accepting credit card payments	Payment Card Industry Data Security Standard (PCI-DSS)*
Any company using personally identifiable information (PII)	U.S. state laws requiring public disclosure of breaches of PII

*PCI-DSS is not a regulation but an industry standard with enforcement mechanisms that arguably make it as effective as government regulation

Comparing private versus public companies

A *public company* is one where all or part of its ownership is through publicly traded shares that are traded in an open market such as the New York Stock Exchange. Table 9-2 highlights key differences between private and public companies.

The only practical difference between working as a networking professional in a private company versus a public company (U.S. based) is that a public company must comply with the Sarbanes-Oxley Act and enact a framework of IT and business controls to protect the integrity of the company's financial accounting system and its financial reports. Networking professionals must document and follow policies and procedures. There is a greater emphasis on the security of systems and networks in a public company.

Table 9-2	Private versus Public Companies	
	Private Company	*Public Company*
Ownership	One or more private individuals	Public shareholders
Major decisions	Private; made by company management	Public; must be approved by shareholders
Financial disclosure	No public disclosure required	Public disclosure required
Reporting of material events	Not required	Required
Selection of board of directors	Private matter	Publicly disclosed; selected by shareholders

Supporting company goals and objectives

Networking professionals in the private sector (particularly those in management positions) must understand the mission, goals, and objectives of their company and then develop and enact networking strategies to support them. Otherwise, the networking and IT teams will be out of step with the rest of the organization.

To put it simply, a networking team must support and facilitate whatever business activities the organization wants to undertake. Networking should be involved all along the way, to understand new initiatives and to influence small and large outcomes so that those initiatives will be successful.

One Size Doesn't Fit All: Small and Large Businesses

For many professionals, including those in networking, considerable differences exist when working in small versus large organizations. Without considering an individual's preferences, the issue is not good versus bad but differences in the job based on company size.

Table 9-3 provides some general differences between small and large organizations. Remember that these are generalizations; every company is different.

Table 9-3	Small versus Large Organizations	
	Small Organization	*Large Organization*
Size of security team	Can be as small as one	Dozens or more
Variety of work	Higher	Lower
Process maturity	Lower	Higher
Human interaction	More face-to-face	Less face-to-face
Visibility to upper management	Higher	Lower

Chaos versus Calm: Growth, Mergers, and Acquisitions

They say that companies are either growing or dying. Although rewarding professional challenges exist in both types of companies, some characteristics of a company are worth a look.

On the surface, working for a company enjoying a high rate of growth looks like a lot of fun — and it can be. However, a rapidly expanding company experiences growing pains that you won't see in more stable, mature organizations:

✔ **Continuous process transformation:** In a growing organization, business processes are changed to accommodate new business features, offerings, teams, locations, clients — everything!

✔ **Outgrowing business systems:** An organization growing slowly will occasionally outgrow a system here and there. A rapidly growing company will make more frequent changes, many of which are disruptive.

✔ **Lots of additional staff:** A rapidly growing company can have many new people who are not yet familiar with the company's practices, making work chaotic. Processes, systems, and people's roles are changing, and inconsistencies, mistakes, and chaos can result.

Besides organic growth, some companies grow by gobbling up other companies. The result is nearly the same: People with different ways of doing things come together and try to figure out how to do things in the newly combined organization. Lots of decisions get made in the sloppy effort of joining companies in mergers and acquisitions.

In many companies that grow through acquisition, their internal IT systems are often a cobbled patchwork of systems and networks from each acquired company. Often these systems remain for years, with integration and consolidation proceeding slowly, if at all. This adds considerable complexity, which is another aspect of the excitement (or angst) that we get to look forward to each day.

Rapidly growing and changing companies are, by their nature, unstable and chaotic. You'll have to decide whether this kind of work environment is something you can live with.

Working in Global Enterprises

Global organizations have a unique set of challenges that companies in a single country aren't faced with. Sure, there are language, cultural, and geographic challenges that make company operations more interesting. But from the perspective of networking, the issues that we need to be aware of and manage include the following:

- ✔ **Data protection laws:** Many industrialized countries have enacted laws that detail measures that must be taken to protect certain types of data.

- ✔ **Data privacy laws:** Many countries have passed privacy laws that place various requirements on organizations doing business there. Some countries place stiff requirements on companies that transfer data about their citizens out of the country, and other countries do not permit companies to transfer private data out of their home country at all.

- ✔ **Employment laws:** Differences in employment law keep information security professionals up at night. For example, some countries do not permit companies to perform criminal background checks on employment candidates. In other countries, background checks are allowed but not effective. And in some countries, common security tools such as logging the websites that employees visit are not allowed.

A multinational company must deal with these different national and local laws, and often conduct its business operations differently in each country. A networking professional needs to understand that different technologies may be in use as well as differences in how they are managed.

Another important aspect of work in a multinational organization is the likelihood that some of your team members (including your boss and people who work for you) work and live in other countries. For some, the language and cultural differences are enriching experiences. For others, who prefer to work with people mainly face to face, this arrangement may not be a satisfying one.

Working for a Nonprofit Organization

In the legal sense, a *nonprofit* uses surplus revenues to further its goals rather than distributing them as profit or dividends to owners. When most people hear "nonprofit," they think of a charity or a foundation.

One typical characteristic of a nonprofit is its culture of frugality, because every dollar spent on anything other than its mission reduces the fulfillment of its mission. With a few exceptions, IT and networking professionals find work in nonprofits frustrating because they have fewer opportunities to gain experience with new technologies. They may also feel that their tenure in a nonprofit will hurt their long-term career outlook. Further, some nonprofits do not have the means to pay market-level salaries to their professionals, which can make it difficult for nonprofit organizations to find qualified talent.

Every cloud has its silver lining. Working in a nonprofit can be intensely rewarding and fulfilling because you are part of something important that is improving the world. For a networking professional, a nonprofit has another reward: Because the organization may not have the funds to buy the latest networking technologies, you'll learn how to do more with less, which is a skill valued not only in nonprofits but also throughout the private sector.

Chapter 10

Serving in the Public Sector
or Academia

Government agencies and educational institutions need experienced networking professionals as much as private industry does. Governments and educational institutions rely as much on information systems as the private industry, and they face the same challenges — primarily, building and managing networks and systems that adequately support key business processes.

Although the principles of networking are similar in any kind of organization, working in government and education is different from work in the private sector. Is it right for you? Only you can decide. In this chapter, you find information to help you make that decision.

Working for a Federal, State, or Local Agency

Agencies at all levels are in need of qualified networking professionals who have many of the same skills sought by the private sector. No matter where you work, your skills and knowledge of networking and information systems can be used to build and manage networks and systems that are vital to the ongoing operation of government agencies at all levels.

Public service

Working in any level of government is frequently referred to as *public service.* In a public sector job, you serve the public in a professional capacity, providing assistance to your agency in the quest to facilitate more efficient access to information and information systems.

Public service is an honorable career pursuit, but it is often considered a career that includes tradeoffs in the following four ways:

- ✔ **Compensation:** Generally, public service jobs pay 10 percent to 40 percent less than the private sector. However, you're less likely to work the long hours required in many private sector jobs. You might be home for dinner more often, but your dinner is more likely to be ground beef instead of filet mignon.

- ✔ **Skills and knowledge deficit:** In public service, you typically have less exposure to the latest in high-tech innovation. Over the long run, this deficit could put you at a slight disadvantage in the jobs market, where your skills would compare unfavorably against private sector candidates who have more experience with the latest tools and techniques.

- ✔ **Lower risk:** In a public sector job, you usually take smaller risks, and your job will be less likely to be affected by mergers, downsizing, and lay-offs. Put another way, you may have greater job security.

- ✔ **Benefits:** Public sector jobs often come with excellent benefits, more holidays and time off, good health benefits, and often a pension.

In the public sector, you're somewhat further away from the cutting edge, you will have a somewhat lower salary, but your level of risk and time commitment are lower as well. Is the public sector right for you? Only you can answer that. Let's look at more facts of public service in the rest of this section.

Transparency

Everything that goes on in all levels of the public sector is subject to public examination and scrutiny. The memos you write, the emails you send, and the contracts between your agency and outside companies are available to the public on request, with a few exceptions. (The privacy of citizens and public service employees is protected, and in some cases, sensitive information such as system security configurations are unavailable for reasons that I hope are obvious.)

Some professionals bristle at this level of transparency and consider it an invasion of their professional privacy. However, the rationale behind transparent government is a long-standing one in the United States: It is a protection against tyrannical rule. Transparency is just another aspect of public service that comes with the territory.

The glacial pace of change

Government has a long-standing reputation of making progress slowly. Sure, for the most part, government agencies may not have the latest high-tech gadgetry, but often our government agencies at least have the basics to get the job done. But the sometimes-slow pace of progress is not just about technology.

Government should be thought of as an institution with well-defined and deeply entrenched business practices, which sometimes lag behind the practices in private industry.

Leadership

Another big difference between public sector organizations and the private sector is that leadership changes are sometimes based on elections, rather than on a professional hiring process. Thus, executive leadership can change on a regular basis, and leaders are often chosen more for their political prowess or governing abilities than for their understanding, or even comprehension, of the world of information technology.

This same dynamic can raise challenges for nontechnical private sector organizations, but at least the leaders are usually selected and maintained for their expertise in the business of the enterprise. And in those cases, with the correct information from you and your peers, the private sector executive is more open or interested in understanding the risks presented by the use of technology.

In the public sector, leaders concentrate on their political priorities, so they often have no time or inclination to consider whether their computing and networking infrastructure is effective. Fortunately, department heads, at least in larger public sector organizations, often survive several terms of office. Therein lies the hope and possibility of creating and maintaining networks of lasting value and resilience.

Local versus federal

At state and local levels, you'll likely have less exposure to high tech innovations and experience. But as you go into the federal government and defense work level, you're likely to have more exposure to cutting edge technology.

With larger government institutions (especially those that protect information), you can get the benefits of scale. For example, monitoring and reporting of every system on a network may not be cost effective at smaller agencies but is routine at the Department of Defense level.

Tenure

In part, the pace of change in the public sector is a result of people remaining in their government jobs for decades, sometimes in the same job. People resist change, and if the same people stay in their jobs for years or decades, their way of doing things tends to stay the same. These practices lag behind the way things are accomplished in private industry. This practice drives some people a little crazy, but public service is not for everyone.

One reason why people tend to stay in public service jobs is the pension, a long-term benefit that has all but disappeared from the private sector. Whereas public sector pay is lower than the private sector, a public sector pension may be quite generous for those who spent their entire career in public service.

Regulations

Aside from the general theme of transparency described previously, government agencies are also subject to regulations requiring them to enact controls to protect information and information systems. The most noteworthy of these is the Federal Information Systems Management Act (FISMA) of 2002, which requires every U.S. federal agency to establish effective information security programs.

At a minimum, federal agencies are required to enact security programs based on two key documents:

> ✔ **FIPS 200:** Minimum Security Requirements for Federal Information and Information Systems
>
> ✔ **NIST 800-53:** Security and Privacy Controls for Federal Information Systems and Organizations

Agencies are required to develop a System Security Plan (SSP) for each information system, and undergo periodic certification and accreditation processes for each system to ensure that it meets applicable security requirements and standards. Networking professionals in government agencies are typically involved in these processes.

Working for a Military or Defense Contractor

U.S. federal agencies, including the Department of Defense, enlist the help of many outside organizations for the development of military and defense capabilities, including weaponry and other support of active military forces. They are also often used to provide staff augmentation to fill in understaffed roles; cyber-related roles are often filled with contractors due to the need for experienced and certified individuals. Although these organizations are considered to be in the private sector, they warrant a separate discussion because there are differences in how they operate.

Depending on the particular firm and its purpose, jobs in military and defense contracting companies can resemble government itself in terms of the rate of change, the longevity of the employees, and the potentially glacial pace of operation. On the other hand, many companies and their positions can be much more like the private sector, with a higher pace of work, more exposure to high-tech innovation, and profit sharing!

Employees in military and defense contractor firms usually undergo onerous background checks at the time of hire. For many people in positions of higher sensitivity, background checks may be periodically conducted throughout their employment.

ANECDOTE

Defense contractors are a public-private hybrid

By working for a defense contractor, you can get access to some of the benefits of working with large government organizations (and exposure to what they do) without having to work through government bureaucracy, and you get the benefits of working for the private sector (technically). At the same time, although you often get a comparably higher salary, you don't have the job security or necessarily the same hours.

I think government contracting is really in between private and public from a career and benefits perspective. A word of caution: Many of the larger government contracting firms work on a contract-by-contract basis, so while you're an employee of the contractor, after the contract with the government is over, you may not be guaranteed a job.

Brian Haller, Seattle

Going Back to School

Whether you consider working in K through 12 or in higher education, employment in education is public service work (unless you work for a private school).

For the most part, networking in education is a lot like networking in public service: things move slowly, and there may not be a lot of money in the budget to get the tools you think are needed to support the organization. Chances are, you'll be dealing with people deeply entrenched in their careers; many may be resistant to making the kinds of changes you think are warranted to ensure that networks and systems are more resilient and reliable.

Higher education suffers from a paradox in the closely related information security profession: Universities are generally thought of as open environments with little or no controls to restrict what students and faculty are permitted to do on campus networks. This practice sometimes contradicts security professionals' mission of protecting an environment through controls such as a firewall, an intrusion prevention system (IPS), and a data loss prevention (DLP) system. Often, however, this dichotomy plays out through the creation of a highly protected portion of a university's environment housing servers containing sensitive information. This practice of *network segmentation,* or the creation of various security zones, protects certain systems while relaxing security in other places. And guess who gets to design, implement, and manage that network segmentation? You guessed it: you.

Chapter 11

Living on the Edge with a Startup

*W*orking as a networking professional in a startup can be a life-changing experience. If you can tolerate the long hours, chaos, and uncertainty, working in a startup can be rewarding for a number of reasons. First, being part of something new carries a level of excitement (which is sometimes hard to distinguish from a feeling of terror). Also, you'll learn a lot in a startup that you won't learn elsewhere, primarily having to do with operating a small business.

Most startup businesses don't have a lot of money (although a few have more than they know what to do with), so networking professionals in these businesses have to find creative ways to implement technology without spending a lot of cash. Exactly how this is done will vary greatly based on the startup business's purpose and product, and many other factors too numerous to mention here.

Bottom line: Working with a start-up is risky and can be frustrating. It will certainly be demanding, but if things go well, it can be extremely rewarding.

If you look at any of the websites dedicated to startup companies that list open positions, such as angel.co (not angel.com), you'll rarely find a networking position — unless the company is building its own network infrastructure, in which case the design of its products or services are all about technology.

Doing More With Less

Startups are all about going lean and mean, focusing all resources on the product or service that the startup organization is creating. They won't have any profits to use for the purchase of new IT infrastructure. Instead, investors or owners fund the business and expect management to spend frugally, making the money last as long as possible.

At first blush, this might mean you'll be deprived of opportunities to get your hands on the latest networking technologies. We prefer to look at this situation in another way: You'll need to work smarter to eke out more value and functionality from the available infrastructure. You'll also be researching ways to get the functionality you need without breaking the bank. And you'll become skilled in integrating components to get what you need.

For every expensive product, there is almost always a free or open source version with a lot of the same basic functionality. Table 11-1 illustrates this with a few key pieces of technology.

When you have to piece together an infrastructure from open source and other alternative sources, you increase your skills and knowledge. Consider it a baptism by fire: The hard work putting this together will pay off many times over in the knowledge you gain.

Table 11-1	Commercial and Open Source Tools	
Component	*Commercial*	*Open Source/Free*
Operating system	Microsoft Windows	Linux
	Oracle Solaris	
Database management system	Microsoft SQL Server	MySQL
	Oracle	
Web server	Microsoft IIS Server	Apache
Firewall	Checkpoint	Vyatta
	Palo Alto Networks	iptables
Virtualization server	VMware	Oracle VirtualBox
Intrusion detection system	Tipping Point	Snort
	SourceFire	

Component	Commercial	Open Source/Free
File integrity monitoring	Tripwire	OSSEC
Host-based intrusion detection	Tripwire	OSSEC
	Verisys	
Centralized logging	Logrhythm	Splunk*
Directory	Microsoft Active Directory	OpenLDAP
SSL server	Microsoft SChannel	OpenSSL
	RSA BSAFE	
VPN server	Cisco	Untangle
	Juniper	OpenVPN
Antivirus software	Symantec	ClamAV
	Trend Micro	
	Sophos	

Splunk is free if daily log volumes are below 500 MB of data

Building Virtual Infrastructure in the Cloud

Most new high-tech startups are building their internal IT infrastructure entirely in the cloud. Buying services from cloud-based service providers is easier and far less costly than building physical file servers, email servers, and other corporate systems — and all the required power, cooling, and physical security.

On one hand, you might wonder about the loss of opportunity to get your hands on and configure a lot of network devices. However, in all but the smallest startups, you'll still probably have local infrastructure to set up for connecting laptops, desktops, tablets, and smartphones to the Internet.

Building virtual infrastructure is its own reward: Most organizations that need to build new systems give cloud-based infrastructure serious consideration. Some believe that cloud-based services are just the latest fad, but we believe that they're here to stay, even if they will undergo more changes in the future.

Building and managing cloud-based infrastructure through AWS or Azure, for example, is similar to using your own hardware. The only difference is that you won't be working with hardware. You'll still be configuring operating systems and dealing with capacity issues, security issues, patching, and integration with other systems, just like you would if the servers were in a data center in your building or across town.

The only thing you can't do with infrastructure in the cloud is walk into your data center and get your hands on it. You'll have to rely on your imagination — and Visio — to get a depiction of your network and systems architecture for your cloud-based environment.

Experiencing the Razor-Sharp Edge

If you're working for a high-tech startup, you might be involved in the design, implementation, and support of the infrastructure that is a part of the startup's product or service. If this is the case, you'll have some role in the architecture, design, implementation, or management (or all of these) of production infrastructure. Depending on the nature of the product or service, you might become involved in emerging technologies of some type and gain valuable experience that will add some punch to your resume.

If you aren't the architect of the startup's infrastructure, but are building or supporting that infrastructure, this role is still enviable for building skills. Even a junior role in a startup is great for your career, provided you are learning from others so that someday you can have a senior role in a future startup company.

Here are some of the advantages of working in a startup at some point in your career:

- ✔ **High velocity:** You'll learn how to build infrastructure in a hurry. You can use this skill anywhere.
- ✔ **High agility:** Startups often need to make changes quickly to accommodate growth as well as to support adjustments in the startup's product or service.
- ✔ **High energy:** Most startups have a high-energy, fast-moving culture in which everyone works together to do great things.
- ✔ **Prestige:** If the startup is successful, just being a part of it can be a plus on your resume.

Startups in existing companies

You don't necessarily have to join a startup company to be in a startup company. What we mean is that many larger organizations may organize semi-autonomous business units, or skunk works (the name given to Lockheed Martin's advanced development program; the term is widely used in business today) to develop new products or services for the larger organization. We've both been involved in these types of startups. In some ways, skunk works represent the best of both worlds: You get the agility, energy, and chaos of a startup but with the benefits of a big company.

Working in a startup is not all fun and games. However, some aspects of working in a startup company are viewed as disadvantages by some but opportunities by others. For example:

✔ **Long hours:** There are few hands to do the work of many, so you may be working longer hours than in other organizations. You'll need to manage your work-life balance so that you don't burn out or become embittered.

✔ **Small budgets:** Some startups have small IT budgets, and others have large IT budgets. It's safe to say that small budgets are a possibility but not a certainty.

✔ **Low process maturity:** Most startups, at least in their earliest stages, do not have formal IT lifecycle management processes such as change management, configuration management, incident management, and capacity management. Organizations lacking these processes will find it more difficult to properly manage their technology. If you're familiar with these processes and are in a position of leadership, you may be able to slowly introduce these processes.

In a startup organization, everyone needs to have a healthy dose of initiative. In other words, you need to have an instinct for identifying and exploiting opportunities for improving the business, in a setting devoid of organization.

Finding Startup Jobs

Startup companies usually do not have a formal recruiting person or process or a human resources department. Often, no one is available to post an open position on a job service such as Monster.com or Indeed.com. So you might be wondering how you can find startup company jobs.

Startup companies often hire people they already know. If you know people involved in a startup company, or know people who have recently gone to work for a startup company, contact them and express your desire to join them. Remember, though, that they will probably be extremely busy, so it may be a bit challenging to get their attention.

The following sites specialize in listing startup company jobs:

✔ **AngelList:** `https://angel.co` (not angel.com)

✔ **StartUpHire:** `www.startuphire.com`

✔ **VentureLoop:** `www.ventureloop.com`

If you're fortunate enough to get the attention of a startup company and are interviewed, don't expect a lot of formality or organization. Remember that startup companies are operating on a shoestring, and the interview might consist of a meeting with one or two people in a coffee shop or a restaurant. You should still expect to get a formal offer letter, and you shouldn't give notice at your old job until you're confident that you have a job at the startup company.

Is A Startup Right For You?

If you've been reading this chapter from the beginning, you may be getting the idea that a startup organization is quite different from other types of organizations. Honestly ask yourself the following questions to see whether a startup organization is right for you:

✔ **Do you have a built-in instinct for identifying opportunities for improvement and exploiting those opportunities?** In a startup, there often isn't someone to tell you what to do; you need to just *know* what to do and how to do it.

✔ **Can you thrive without much corporate structure?** The startup may have few or no corporate policies, no employee handbook, and no organization chart. It's often just you and some other people trying to build something new and cool.

✔ **Can you work long hours, and occasionally *very* long hours?** In a startup, you do what you have to do to get things done. Often this means working long hours building networks and systems, and more long hours supporting them and working out the kinks.

✔ **Can you work independently with little direction from your immediate boss?** Your boss might just be another peer, or he or she might have

a different responsibility and not really understand how you do what you do. For example, you might be a network architect and work for the VP of engineering in a software startup; your boss's area of expertise is software development and he or she doesn't understand infrastructure.

✔ **Have you worked in other organizations with structure and formally established processes?** Familiarity with business processes and how technology supports business are key skills to take into a startup. As the startup grows, those individuals who understand business processes will be the ones who take the company to the next level. Being a part of that metamorphosis can help you advance upward.

✔ **Do you enjoy working with cutting-edge technology with little or no reference material and no one to contact for help?** If you're working with cutting-edge technology in a startup, you might be the first company doing what you're doing, with no one else available to help.

✔ **Do you enjoy the challenge of working with less-than-the-latest technology and learning how to make do with it?** Many startups operate on a shoestring, and you'll need to know how to stretch those budget dollars.

If you answered "yes" to most or all these questions, work in a startup might be right for you. And if you want to work in a startup but don't have the knowledge and skills yet, do some career planning and figure out what skills or knowledge you need. If you have the initiative to make improvements to your career, you may have what it takes to work in a startup business someday.

Chapter 12

Life as a Consultant

*N*etworking consultants have an opportunity to help not just a single employer but also many organizations during their professional career. Working as a consultant is different from working in an organization, where you have responsibilities only to your employer and its internal operations. As a consultant, you won't be putting down roots in a single company (other than the consulting firm itself); instead, you'll be moving from place to place.

Consulting is fast-paced and highly rewarding but also unpredictable and stressful. If you're considering a position as a consultant, check out the pros and cons in this chapter.

Is Consulting Right for You?

In the 1960s, the original *Mission Impossible* TV series always started with a taped message to Mr. Phelps, who was given a life-and-death, world-peace-at-stake assignment in some remote corner of the world. Against all odds, Phelps and his team would overcome seemingly insurmountable obstacles and prevail.

Consulting is a lot like *Mission Impossible* missions. From one consulting gig to the next, you never know what kind of work, people, or company you'll encounter. Some assignments will be boring, others highly challenging, and others rewarding — for a variety of reasons.

ANECDOTE

Consulting requires social skills

One of the things that you always come up against when working as a consultant is the desire for absolutes. "If I buy this firewall/anti-virus/new device, I'll be 100 percent secure, right?" Or worse, "I thought that if I bought that firewall/antivirus/new device, I'd be 100 percent secure, right?" Of course, there's no such thing

as 100 percent in security. Being any kind of IT consultant is only 20 percent tech and 80 percent social skills. So if you're not prepared to (or just don't want to) respond to questions like these, take a different job path.

Marc Gordon, Seattle

Consulting is fundamentally different from many other jobs. Take a look at the following questions. Are you okay with a job where you

- ✔ May travel from 25 to 75 percent of the time, away from home for days or even weeks at a time?
- ✔ Work with different people from day to day or week to week?
- ✔ Won't know what city you'll be in a week or a month from now?
- ✔ Are expected to be a seasoned expert but won't know what expertise you'll have to call on a day, week, or month from now?
- ✔ Help build something but will not be around to see how successful it could become?
- ✔ Sometimes work for people whom you'll meet only by phone?
- ✔ Aren't around long enough to form deep relationships with the people you work alongside?

If you answered "yes" to most or all of these questions, consulting may be right for you. In the rest of this chapter, you find out more about working in a consulting organization or as an independent consultant.

Consulting workload

Consulting is hard work — very hard work — for a variety of reasons. Let's take a closer look at the four major factors that will always try to take you down in a consulting job:

- ✔ **Intellectual fatigue:** As a consultant, you're expected to be professionally superior to the client organization with which you'll be working. You are expected to have expertise and wisdom that surpasses that of the employees in your client's organization.

- ✔ **Performance fatigue:** Because you're in front of clients, you have to be on your A-game all the time. Your clients expect a professional polish from a high-priced consultant; whenever you speak, all eyes and ears will be focused on you. You might feel as though you're on stage all day, every day.

- ✔ **Physical fatigue:** You'll probably travel a lot, living out of your suitcase, eating in restaurants, and working evenings. You might not take the time for physical exercise while on business travel or working long hours.

- ✔ **Multitasking fatigue:** Often you won't be able to concentrate only on the project right in front of you. You may be drafting implementation reports for clients you met recently, and reading documents from a client you'll be working with next week or next month.

Appearance and approach

As a consultant, you are often "the face" of the consulting firm (or yourself, if you're an independent consultant), to whom the client is paying big bucks for their expertise. You should *always* behave, dress, and communicate in a bit more professional manner than the client employees (without seeming arrogant).

Even when working for a consulting firm, you have some responsibility for sales; your day-to-day actions, customer service, and exhibited expertise will help your consulting firm maintain their reputation with the client and your success and professionalism will be shared with other companies and clients. You must always be mindful of keeping your eyes and ears open for possibilities of add-on work or new business avenues with a client as well. These additional responsibilities go along with being a consultant.

ANECDOTE

Confidence as a consultant

You have to come into the room confident that you know what you are talking about and ready to listen to the customer and their concerns. You must roll with the material you have to work with and understand that what people are willing and not willing to do as well as their level of expertise are different.

Since you are not a member of the staff or the team you are working with, the trust level is different and you have to spend a lot of time justifying why you need to see what you need to see. Then you have to develop architectures, implement networks, or troubleshoot networks in a way that aligns with a business you may not know a lot about. You also have to understand that you will be spending a lot of time educating people about networking, technology, and other information related to the industry.

Bruce Lobree, Seattle

Working for a Consulting Firm

Working in a consulting firm can be a lot like working in a traveling circus. Some colleagues will stay the same but the scenery changes as you move from town to town (or client to client).

A job in a consulting firm will probably allow you to spend most of your time assisting other organizations with various aspects of their networking management or operations. Chances are, marketing people and sales people are selling the services that you and your consulting colleagues fulfill with your company's clients.

In many ways, work in a consulting firm can be similar to being an in-house networking expert. You'll be working with colleagues in the organization, which will give you a sense of normalcy (although you'll rarely see your colleagues if you work for a regional or national company). Plus, you'll have company benefits such as a retirement plan (a 401K in the United States), medical insurance, and paid holidays and vacation. In other words, you will still belong to an organization of your own, while you may spend most of your time inside client organizations and working with their employees.

In any job, you have to do what you're told. But in a lot of consulting jobs, you also have to go where you're sent. As a consultant, you'll be incented to work on billable projects to bring in the money that ultimately ends up in your paycheck (a portion of it, anyway). You want to avoid being on the "bench" (being paid while in between projects) as much as possible.

Consulting firm processes

Many consulting firms have established processes and procedures for a lot of operational activities. These processes and procedures drive consistency and can help the consulting firm increase its business without falling into chaos. Here are some examples:

- ✔ **Time accounting:** An established method for tracking billable hours by client and by project, so that each client can be invoiced accurately for all services rendered.

- ✔ **Expense accounting:** An established method for capturing billable and nonbillable expenses, such as travel costs, meals, and supplies.

- ✔ **Engagement management:** Standard procedures for starting, executing, and completing projects. For example:

    - *Pre-sales:* In some consulting firms, consultants participate in pre-sales activities with new clients, so that clients can meet the consultant and ask questions about the proposed engagement.

- *Project kickoff:* This procedure involves a conference call or an in-person meeting, as well as an exchange of documents and client contact information.

- *Project status reports*: The consultant writes these, although he or she may need to follow a company template and format.

- *Written deliverables:* Most consulting engagements include one or more written deliverables. You'll probably have a template and examples to follow so that new written reports are consistent with previous ones.

- *Project wrap-up:* This process includes the delivery of written reports, as well as a closing meeting.

- *Post project:* Includes a final accounting of all billable hours and expenses. Some consulting firms may do a project debrief to discuss what went well, what needed improvement, and how future projects can be performed better.

The consultant or other people or departments may perform many of these tasks. No one method is correct, but you may find some of the differences important.

Subject matter variety

In a smaller consulting firm, you'll be a networking generalist and may have a variety of consulting engagements. Depending on your areas of expertise, you could be chosen for many different consulting gigs, such as

- ✔ **Procedure development:** You interview key stakeholders in a client organization and develop the organization's networking procedures.

- ✔ **Network architecture review:** You examine (and in some cases, discover) an organization's network architecture, and make recommendations for improvements.

- ✔ **Selection of new networking technologies:** You develop recommendations for new networking technologies, such as routers, switches, netflow, and network management. You may even conduct a bake-off of competing products to help decide which one works best for a particular client and then implement the selected product.

In a larger consulting firm (and in some smaller ones), you may be specializing in one functional area, and most or all of your consulting engagements will be focused on a particular subject matter or activity. For example, if you were in a network infrastructure group, you would be working with routers and switches; in a network management group, you would be one of the experts on network management tools.

Consulting is itinerant work

Unless you get a long-term consulting gig, you won't be in one workplace for more than a few days or weeks. It can be difficult to forge long-term relationships with people in your client organizations, because you'll be moving on at just the point when you are getting to know and enjoy working with them.

When you are working as a consultant, you won't put down roots, in terms of hanging your hat in one organization. Instead, you're an expert, working on a particular task or project, and then you're out. You won't be around to see the fruits of your labor — at least not the long-term positive effects of your contribution. As a consultant, you have to simply be okay with that. But the other side of that coin is that you'll be able to help a lot of organizations, something you'd have little opportunity to do if you were working for a typical employer.

Peter H. Gregory, Seattle

Working in pre-sales

In many organizations, consultants will support the sales organization in the activity known as pre-sales. You might take part in sales calls to prospective clients. You're along for the ride so that you, the networking expert, can describe your approach to their particular problems. Seeing (or hearing) you in person also gives the client more confidence in the consulting firm and in you.

Pre-sales is essential to winning future business, but as a consultant you will face pressure to maximize billable hours (and complete tasks and projects on time for your clients). Often the hours spent on pre-sales must be made up by working extra hours in the early morning or evening to keep client projects on schedule.

Going It Alone as an Independent Consultant

In the movie *Star Wars,* the character Han Solo is the semi-romantic portrayal of an independent consultant. He is his own boss, he chooses what jobs to take, and he's in control of his destiny. You also get the impression that it's a lonely job, with only his sidekick Chewbacca as company.

As an independent networking consultant, you decide which companies you'll work with. Consulting is the ultimate in independence and the ultimate in risk, like climbing a mountain with no one to belay you if you fall.

Independent consulting is a lifestyle. It's difficult to master, and few are up to it. However, if you're independent consulting material, the rewards can be great. As an independent consultant, it's just you and your clients: You have no coworkers and none of the encumbrances of working in a company with others.

Independent consultants have to do a lot of things on their own:

- ✔ **Marketing and sales:** These tasks require a different set of skills and can take considerable time. Sales is a very difficult job and typically requires a lot of energy and urgency, along with a fearless and outgoing personality.

- ✔ **Legal:** You need to manage your contracts or have outside legal counsel from time to time. You'll want to develop template documents for nondisclosure agreements, statements of work, and a master services agreement.

- ✔ **Accounting:** Unless you're an expert with small business accounting and taxes, you'll probably want to find an accountant to keep your books and complete your tax filings.

- ✔ **Earned time and benefits:** As an independent consultant, you'll appreciate the concept of a paid vacation, holidays, and sick days. As an independent consultant, you still need time off, but you're not billing hours while you're not working for a client. You also have to pay for all other benefits, including medical insurance, life insurance, and health club discounts.

- ✔ **No colleagues:** Without colleagues to talk with, independent consultants must look to the professional community for like-minded security professionals with whom they are willing to share ideas, struggles, and joys. Put another way: If you need help on a project, you have to find that help on your own.

The prospect of independent consulting is an intense, rewarding challenge to some, and terrifying to others. It's definitely not for everyone.

Nothing happens until a sale is made. If you can't sell, or hate to do so, you're unlikely to find much success as an independent consultant.

The Good, the Bad, and the Ugly of Consulting

Table 12-1 provides a comparison of working in a consulting firm, as an independent consultant, and in a regular organization (which could be a public company, a private company, an institute of higher learning, or the government).

Table 12-1	Consulting Work versus Internal Work		
	Consulting Firm	*Independent Consultant*	*Internal Company*
Marketing and sales	Provided by consulting firm	Provided by independent consultant	N/A
Legal support	Provided by consulting firm	Paid by independent consultant	Provided by employer
Benefits	Paid by consulting firm	Paid by independent consultant	Paid by employer
Support	Coworkers at consulting firm	Must find trusted associates	Coworkers at employer
Job variety	You can help several companies	You can help several companies	You can help only your employer
Billing rate	You receive a small fraction	You receive all but must pay for overhead	N/A
Long-term relationships	Only within the consulting firm	Hard to come by	Definitely

Part IV
Getting Hired!
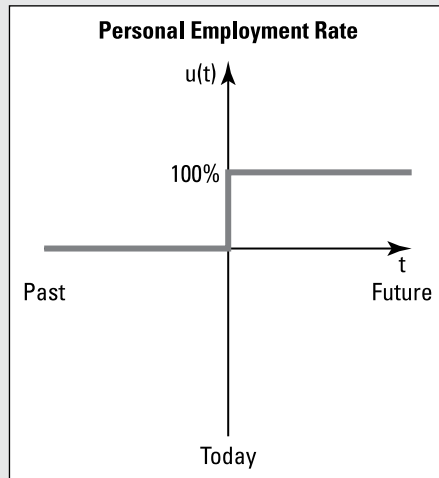
Personal Employment Rate

u(t)

100%

t

Past

Future

Today

In this part . . .

- ✓ Express what you want.
- ✓ Write a resume that highlights your abilities.
- ✓ Customize your cover letter to land an interview.
- ✓ Ace your interview.
- ✓ Attain professional success.

Chapter 13

Branding Yourself for Your Dream Career

*T*he Internet is your marketing machine, and the world is your audience. It's no longer enough to build a resume and upload it to job search sites such as Monster.com. In today's job search marketplace, you also need to tap into business and social networking sites that give you the opportunity to market yourself, to create the *brand of you*.

People are the key to advancing your career — you can't do it on your own. Meeting your peers at industry events will help you understand how other networking professionals overcome obstacles and discover their recipes for career success. Reaching a broader audience through online professional networking on sites such as LinkedIn and Twitter will help you establish more professional connections. Expressing your opinion through your blog, as well as through articles and e-books, will help you establish yourself as a networking professional worthy of a serious look from recruiters and your next employer.

In this chapter, you discover how to build your brand through one-on-one networking and by building a personal brand that will set you apart from others. The topic of branding requires a book unto itself, so check out *Branding For Dummies*, 2nd Edition by Bill Chiaravalle and Barbara Findlay Schenck, which includes a chapter devoted to personal and one-person business brands. Plus, follow the advice in this chapter as you build your professional reputation in networking.

Many great resources are available for establishing and building a network of networking professionals. The most important resource is *you*. Building your network involves connecting one-on-one with people, not in using tools to create cool online personas (although those are important as well). Your number one objective is to establish yourself as an interesting professional with unique talents who understands the value in working with other technology professionals.

Meeting People

Building your network begins with meeting other professionals and getting to know them. You can meet people in many ways, such as the following:

- **Inside your company:** If you work in a larger organization with an established networking team, reach out to them and explain that you want to learn more about their careers. If you tell them that you're interested in a networking career, chances are good that someone will be happy to discuss their career with you.

- **Technology industry associations:** There are a lot of industry associations, and many of them organize local events in midsized and larger cities around the world. Some of these associations are

  - **Association for Computing Machinery (ACM):** Located at `www.acm.org`.

  - **Institute of Electrical and Electronic Engineers (IEEE):** Located at `www.ieee.org`.

  - **Linux Foundation.** Dedicated to all things about Linux. Located at `www.linuxfoundation.org`.

  - **SANS (SysAdmin, Audit, Networking, and Security) Institute:** Networking and systems administration. Located at `www.sans.org`.

  - **USENIX:** Unix-centric organization. Located at `www.usenix.org`.

- **Computing and networking conferences:** Conferences are a great way to meet people, including other attendees as well as exhibitors and speakers. Many industry associations just listed also host networking conferences. A few others follow:

  - **CeBIT (Centrum für Büroautomation, Informationstechnologie und Telekommunikation).** Claims to be the world's largest computer expo, held in Hanover, Germany. Information at `cebit.de`.

  - **CES (Consumer Electronics Show).** Internationally popular electronics and computing exposition, held annually in Las Vegas. Information at `cesweb.org`.

- **Gartner IT Expo:** Held annually in the United States, Europe, and Asia. Information at `www.gartner.com/events`.

- **Interop**. Annual conferences in New York and Las Vegas. Information at `www.interop.com`.

- **ITEXPO.** Annual trade shows in Miami and Las Vegas. Information at `itexpo.tmcnet.com`.

- **LinuxCon.** Conferences on Linux in North America, Europe, and Japan. Information at `events.linuxfoundation.org`.

- Macworld/iWorld. Annual conference dedicated to the Apple Macintosh system. Information at `www.macworldiworld.com`.

✔ **Sponsored vendor events:** In medium-sized and larger cities, companies that produce networking products and services also hold vendor events, where they discuss related topics and demonstrate their products. These events are often held in hotel meeting spaces and community centers. To learn about these events, get your name on the vendor's mailing list.

✔ **Service clubs:** Organizations such as Rotary, Kiwanis, Lions, and Optimists focus on service to communities and are a good place to meet other professionals.

Even if you don't know anyone else who will be attending, you'll have an opportunity to meet other people. If you're not the outgoing type, you'll need to pretend to be. Besides, no one else will know whether you're introverted if you pretend for a while that you're an extrovert.

In most cases, it's not good form to introduce yourself and then immediately start talking about yourself, particularly if you tell them you're looking for a job. Instead, it's better to ask people to tell you something about themselves; people will remember you in a much better light if you ask and listen rather than talk their ears off.

If the subject comes back around and someone asks, "So, what do you do?" you can describe current and past positions, and that you are looking to get into networking. You might explain a little about what you're doing to get into the profession, and then ask the other person's opinion on your approach. You might get some good pointers and maybe even offers to introduce you to others at the event.

Develop an elevator pitch — what you would say about yourself to someone while riding an elevator between floors. You have about 1 to 2 minutes to quickly give an overview of what you do as well as your interest in becoming (or your experience as) a networking professional.

Networking with other networkers

Networking (the people-meeting-people type, we mean) is critical. If you're an introvert and don't always feel social, which is a category I fit into, networking is a good opportunity to overcome those feelings. Knowing people in security will help alleviate that "unknown entity" risk that potential employers face and will land you interviews for which you'd otherwise be overlooked. For me and many others I know, networking was the key to landing our first job in the field or a subsequent one. Beyond that, I've found that the community freely gives advice and help with networking problems.

Glen Sorensen, Seattle

If you're currently employed, bring plenty of business cards. If you're between jobs, or if your employer doesn't provide business cards, get some quality ones printed. (Many sites offer free business cards, but you might consider upgrading to a better cardstock or appearance.) In this day of electronic everything, business cards may seem a little old-fashioned, but a lot of people still use them. Business cards are a great way to capture names and contact information easily, so that you can follow-up with relevant and interesting professionals in the future.

The two most important reasons for meeting people? Companies prefer to hire people they know, and networking professionals are usually willing to discuss challenges with others they know.

Business Networking with LinkedIn

Launched in 2003, LinkedIn touts itself as the "world's largest professional network." With over 200 million users, LinkedIn is a great resource for establishing one's own brand as well as finding other like-minded people. LinkedIn is located at www.linkedin.com.

LinkedIn is your most important tool to establish your brand and a professional network, to be recognized as a thought leader in your area of expertise, and to seek opportunities or advance your career. If you want to learn a lot more about LinkedIn, pick up a copy of *LinkedIn For Dummies,* 3rd Edition by Joel Elad.

To use LinkedIn, sign up for a free account and build a profile that resembles a resume. You establish connections with people you know (or want to know)

for business networking. You can join special interest groups where private discussions take place, and you can search for jobs in any industry and location. You can search for people you might know in the "people you may know" feature. You can also search for people by name, location, or company in the freeform search, where you can conduct keyword searches to find people in specific interest areas such as network security.

LinkedIn is feature-rich: You can express and describe your professional background in many ways. Many consider a LinkedIn profile to be a living resume, which you can update and improve at any time.

In the remainder of this section, various features of LinkedIn are described.

Photo

You can upload a photo of yourself if you want, and most users do. I recommend that you use a recent, high-quality photo. Using a much older photo may capture the beauty of youth, but people who meet you in person may wonder if you are disingenuous. Also, it's best to have a head shot taken by a professional. Wear professional clothing and keep the colors conservative.

Avoid the following mistakes, which can make your first impression less than professional:

- ✔ **Cropped group photo:** A photo that's obviously cropped makes people wonder if you have any good photos of yourself.
- ✔ **Party photo:** Is that the first visual impression you want to make?
- ✔ **Look-at-my-cool-vacation photo**: Yes, the Eiffel Tower and the Statue of Liberty are cool, but leave those for your *personal* Facebook page.
- ✔ **Selfie:** Almost without exception, selfies are not kind to one's looks, especially if the camera is too close. Your nose looks huge!
- ✔ **Company logo:** I'm happy that you are enthused about your company, but others want to know what you look like.

You can change your photo any time. If you have a good photo now, use it. Upload a better one later.

LinkedIn also has a background image feature that enables you to upload a landscape-oriented background. It's appropriate to select something business oriented, or just about anything else that is tasteful and reflects well on you personally.

Headline

The LinkedIn headline is the phrase that appears directly below your name on your profile page. Ideas for your headline include title and company (such as *Systems Engineer at Newco*), mission (for instance, *Systems engineer in oil and gas industry*), and multiple activities (for example, *Systems engineer, ISSA board member, and instructor*).

The headline is short, just one or two lines. To those viewing your LinkedIn page, the headline serves as your personal brand statement. Most career coaches advise you to use your headline to define the unique talent and value you deliver.

Below the headline in a smaller type size is the area where you live. Next is a categorization, which you can select to tie into you or your company. For instance, if you're a networking professional in the retail industry, you could select Computer Networking or Retail.

TIP When writing your LinkedIn profile, be sure to use keywords that others are likely to use when seeking someone like you so you'll show up in their searches. Many recruiters and headhunters use premium LinkedIn accounts to search for candidates.

Background

The section of your profile directly below your photo is where you present your background and experience by completing each of the following sections:

- **Summary:** Write a few paragraphs about yourself. It's best to think about this like a summary near the top of a resume. Don't make it too long, or people might not read it all the way through.

- **Experience:** List each job you've had, and you can provide several details about your position, primarily in the freeform text field. For each position, you can specify a title, company, location, and description of your responsibilities and accomplishments.

- **Projects:** Describe any projects you have undertaken at each job. You can specify which other persons (they must be LinkedIn users) participated in the project.

- **Organizations:** List any organizations that you currently belong to or did in the past. If you've been out of college for less than five years, you can list campus organizations here if you want.

- **Volunteer Experience & Causes:** List the organizations where you volunteer your time, money, or other resources. You're seen as a better person if you put others' needs ahead of your own.

- ✔ **Skills:** List individual business and technical skills, separate from your individual jobs.

- ✔ **Certifications:** List each industry certification, including the year earned, when it expires (if it does), when you last held it (if it's not current), and a description of the certification if it's not a common one.

- ✔ **Education:** List your education, including courses, degrees, and significant training courses. My own rule of thumb is that you don't need to list your high school education if you're older than 25 years of age.

- ✔ **Additional Info:** List any outside interests, personal details, and how you can be contacted.

- ✔ **Honors and Awards:** List any honors and awards here.

TIP

Like a functional resume, you can change the order of appearance of the various sections in your LinkedIn profile by simply dragging them up or down.

Connections

Any connections you have will appear in your profile. These are other people you know and have agreed to connect with. When you're connected with someone, you can see more details in their profile, their contact information, and any connections you may have in common. If the connection permits, you can view all of the other person's connections (and they yours). LinkedIn does permit you to conceal your connections from others.

WARNING!

The connection feature is intended to be used with *people you know*. Before requesting a connection from someone you don't know, understand that the person can refuse to connect with you and state that he or she doesn't know you. If you decide to pursue a connection with someone you don't know, be sure to include a personal note in the connection request that includes the reason you want to connect. If you get several such rejections, LinkedIn will temporarily suspend your ability to request connections from other users.

Recommendations

LinkedIn provides a means for users to write a recommendation for one of their connections. A recommendation is just that — a description of how you know the person and why the person is a good professional. For example: "Over the past 7 years, I have had the pleasure of working with Emily on the university certification program. I have found her to be hard working, punctual, and a lot of fun to work with."

When you write a recommendation for another person, that person has the choice of whether to include the recommendation in his or her profile. If you didn't have nice things to say about the person, chances are he or she will not approve it. Also, if you got any facts wrong or just said anything that the recipient doesn't care for, he or she can reject it and request that you change it.

Recommendations can function like prewritten references and improve your professional image.

Updates

LinkedIn has a feature where you can write a message, upload an image, or put in a link to an article. You can do a lot of things with updates:

- ✔ Cite an industry article and include your opinion.
- ✔ Post a significant update about yourself.
- ✔ Cite a blog entry you've recently written.

The updates feature of LinkedIn helps you inform your connections about important professional events and issues. However, the feature is also misused — or at least some would say so. For instance, uploading an image of some clever saying ("Managers tell you what to do, Leaders show you how to do it.") borders on being noise, and uploading a photo of your cat would be considered inappropriate by most. Fortunately, LinkedIn gives you the ability to suppress updates from people who are too chatty about unimportant things. In other words, keep your updates professional and business related!

Groups

LinkedIn provides for the creation of *groups*, which are communities of LinkedIn members, where they can discuss matters on almost any topic. Groups can be moderated, which means that a group owner or coordinator (one or more of its members) can selectively approve or reject individual postings. Membership can be set to automatically approve or be subject to manual approval.

Groups are a great way to find people that are in your field or work for companies that you're interested in. When you join a group, you have a legitimate opening to connect directly with other group members. Also, many recruiters utilize groups to find qualified candidates. Recruiters will also make career-related posts that might help you identify employment trends in your field.

The contents of LinkedIn groups can be kept private, so that only its members can view its proceedings. A LinkedIn group can be made public, which means that non-LinkedIn members can join the group, and the contents of the group's discussions will be searchable by Internet search engines such as Google and Yahoo.

Jobs

Many professional recruiters and headhunters use LinkedIn to search for employment candidates. One sign of an effective LinkedIn profile is a periodic contact from a recruiter who asks you if you have any interest in positions he or she is trying to fill. Recruiters find you through keywords in your profile.

Recruiters can purchase a premium subscription to LinkedIn that affords them additional privileges, such as the ability to send messages to LinkedIn users with whom they are not connected.

Using LinkedIn successfully

LinkedIn can be a powerful tool to expand your professional network. You'll be seen as a good LinkedIn citizen if you follow these pointers:

- ✔ Keep your summary fairly short and include keywords that describe what you do and are likely to be used by others searching for people with your talents.

- ✔ Describe each employment position with the same level of detail as a resume.

- ✔ Use a high-quality professional photo.

- ✔ Request connections only from people you know, or you might lose the ability to request new connections.

- ✔ Accept connection requests only from people you know (fraudsters use LinkedIn to trick users into providing information to them).

- ✔ List your education and professional certifications.

Because your LinkedIn profile is so much like a resume, you'll want to read Chapter 12. Many of the tips in that chapter will apply to your usage of LinkedIn.

LinkedIn is my living resume

I've been using LinkedIn for ten years. I realized its value as a public, living resume. My efforts have paid off through numerous opportunities that otherwise would not have materialized.

My LinkedIn profile is bigger than my resume, and includes projects, publications, and over 60 recommendations from coworkers I have worked with over the past thirty years. The richness of my LinkedIn profile has resulted in a steady stream of contacts from recruiters over several years.

Peter H. Gregory, Seattle

Networking through Facebook

Facebook is one of the world's great social networking wonders. From a professional sense, some aspects of Facebook should be left to nonprofessional uses only, while other features can work to your advantage as you develop your personal brand. Facebook can be found at `www.facebook.com`.

Facebook profile and timeline

A Facebook *profile* is used to describe yourself in many ways: where you live, where you work, where you went to school, and much more. A Facebook *timeline* (once called the Facebook wall) is the place where you type updates of various kinds and where you can see your posts, friends' posts to you, and any posts or photos in which you're *tagged,* or mentioned with a link to your Facebook profile.

You are strongly recommended to keep your Facebook profile private, so that only your friends can see any of your content. Prospective employers search for candidates' Facebook pages to get an idea of their character. Because of the way that some Facebook features work, it's best to keep your Facebook profile concealed from all but those to whom you've accepted as Facebook friends.

Although Facebook is more of a *social* networking site, recruiters or companies often use it to learn about prospective or current employees. It's okay to have personal and fun info on Facebook, but treat it as if you know that a potential employer will look at it — err on the side of being conservative. Do not put anything on an online networking source that you wouldn't be comfortable having your employer see or read.

Facebook groups

Although there are many other more suitable places than Facebook for like-minded professionals to gather and discuss issues, millions of Facebook users connect with colleagues and professionals in their category through Facebook and Facebook groups.

Avoid mixing your personal and professional posts by taking a few key steps. First, from your Facebook page, click Friends in the left column. From the page that appears, click Create List to create a group of people with whom you can share information and stay in touch in one place.

Next, search for or create a group by clicking Create a Group or Find New Groups under the Groups listing in the left column of Facebook. From there, it's a matter of participating by checking updates and sharing posts with others in the group.

WARNING!

If the topic of a Facebook group includes confidential information, or if the members of a group should not be publicly known, you should set up the Facebook group as a secret group.

Facebook company pages

Facebook profiles are generally for personal use, and Facebook pages are for businesses and brands. You must have a Facebook profile before you can create a Facebook page for your business. Pages are public (unlike profiles) and discoverable through Facebook and browser searches. In addition, Facebook page posts are free but only a minor percentage of them will show up in the news feeds of your page followers. The rest get filtered as a result of Facebook's algorithms unless you develop high levels of interaction with your posts or pay to post the information as a promoted post.

REMEMBER

Facebook business pages and fan pages are one and the same.

Tweeting with Twitter

The microblogging sensation Twitter is another great way to build your brand. Twitter's function is simple: You build a profile, you follow other Twitter users, and others follow you, if they find what you have to say interesting and valuable. When a user you follow posts something (called a *tweet*), it appears in your timeline, along with posts from everyone else they follow. In your timeline, you view the posts made by everyone you follow, and your followers view your posts as well.

You can also send and receive direct messages with people you follow who also follow you.

Posts and direct messages are limited to 140 characters. You'd be wise to keep your posts even shorter because you want to encourage others to retweet or repost your tweets, and they'll need up to 20 characters to add their own message to yours.

To date, over 250 million users are on Twitter.

Setting up your Twitter profile

To set up a Twitter profile, you select a username and password, upload a photo, and provide a brief description of yourself, which is limited to 160 characters, slightly longer than the 140-character tweet limit. You can also have a background photo that will be visible when someone views your profile.

Tweeting

When you have something to say, you *tweet* it: you post an update, maximum of 140 characters including spaces. Everyone following you will see it in his or her timeline. You can include URLs, which Twitter automatically shortens to take less of your 140-character count, and you can include photos and video (a big draw on Twitter) as well. For all you need to know, check out Getting Started with Twitter in Twitter's help center.

Presenting yourself in 140 characters is difficult, but Twitter users do just that. However, for professional purposes, many tweets also include a URL to an article, which could be your blog post or an article of general interest to other networking professionals.

Using Twitter successfully

Twitter can be a great way to expand your professional network. You'll be successful with Twitter if you follow these pointers:

- ✔ Don't become the town crier by retweeting lots of stories put out by news media outlets such as CNN or AP.
- ✔ Add value to information rather than just rebroadcasting (retweeting) it.

✔ Maintain separate professional and personal Twitter accounts if you want to use Twitter for nonprofessional networking. Followers are visible to everyone, so consider not following your personal Twitter account from your professional one, and vice versa.

✔ Consider using TweetDeck to schedule Tweets at key times of the day or week. Information is available at `www.tweetdeck.twitter.com`.

Starting a Blog

Everyone has an opinion. A blog is a great way to express yours, particularly when something you have to say takes more than 140 characters. All kidding aside, writing a blog can be a great way to publicly express your opinion and solicit feedback. Blogging about networking can be a way of distinguishing yourself from other employment candidates. However, thousands of networking professionals have blog sites, so you may want to consider a blog as table stakes in our profession.

In case you're the last person living under a rock, a *blog* is a simple website that functions like a journal, with journal entries (short articles) that focus on a single point of view or interest area, with the most recent articles appearing first. A blog can also have pages for static content, such as a page for the blog site owner's biography.

Setting up a blog

Setting up a blog is easy. Go to one of several popular (and free) blogging sites, click the Start a New Blog link, and answer a few questions. First, though, consider the following:

✔ **Name and URL:** You can name your blog after your name or choose a keyword (or combination of keywords). You can also register your own domain name and associate it with your blog for a more professional feel. For example, on the WordPress service, you could be jim-smith.wordpress.com, or with your own domain name you could be `www.jimsmith.com`, which would redirect to your WordPress site.

✔ **Internet searchable:** You'll probably want your blog articles to be searchable so that people can find your blog's articles. Be sure to use keywords in your headlines, section titles, post content, and summary snippet — or in the first 160 characters of your post, because that's what search engines display if you don't provide a snippet. Again, keywords are critical! Find opportunities to insert your keywords into your blogs.

✔ **Statistics:** If you want to know how many visitors read your blog and what keyword searches lead them to you, use a blog that provides these types of statistics.

It's best if you keep your blog simple, so that you can maintain it easily. A few weeks or months after that "new blog smell" wears off, you may not be inclined to do much with it. If you keep the blog simple, it won't require much work to maintain it.

A couple of good books on the topic of blogging are *Blogging For Dummies,* 5th Edition by Amy Lupold Bair and Susannah Gardner and *WordPress For Dummies,* 6th Edition by Lisa Sabin-Wilson.

Blog services

Several excellent free blog sites are available. Check out the following:

✔ Blogger, `www.blogger.com`

✔ SquareSpace, `www.squarespace.com`

✔ TypePad, `www.typepad.com`

✔ WordPress, `www.wordpress.com`

All these sites make it easy to set up a blog. Many blog services offer free and paid versions.

Several high-quality (and often free) blog software packages are available that you can acquire and install on a server. However, information security issues today make keeping your site secure a time-consuming proposition. Why not let a free service take care of all this for you?

Networking blogs

If you're not sure how you want to set up your blog, you might want to check out the following blogs for networking professionals:

✔ Ethereal Mind, `www.etherealmind.com`

✔ Ethan Banks on Networking, `www.ethancbanks.com`

✔ wirednot, `wirednot.wordpress.com`

✔ Interop, `www.networkcomputing.com/interop.asp`

Besides seeing good examples, you may find them interesting and informative.

Using and maintaining your blog

After you've set up your blog, all you really need to do is write short or long articles with some regularity. You don't need to pen something as long as *War and Peace* every week, but you do need to write a blog entry at least once a month, preferably more frequently. Otherwise, your blog will take on a stale, abandoned look, which may be worse than not having one.

As you get accustomed to your blog, consider adding some other features, such as the following:

✔ **Subscribe:** This feature is a way for readers to subscribe to your blog, so that your blog site automatically emails new blog entries to them.

✔ **About:** The About page is a static page about you, which may include something about your education, work history, professional interests, and so on.

✔ **Tag cloud:** If you tag your blog entries, you get a tag cloud, which provides a nice visual depiction of the topics you write about the most. Figure 13-1 shows a tag cloud.

Figure 13-1: A tag cloud from a blog site.

Anti-Virus application security audit Blog breach career CISA ciso CISSP cloud data loss DRP Encryption Environment Humor identity theft incidents Interviews Law Enforcement my books News Off-Topic On writing Opinion pandemic passwords phishing Privacy professional ethics Quotes and Excerpts responsibility Risks spam threats Tips TJX tools Vista Wireless XP

✔ **Publications:** If you've written articles, books, or e-books, you might create a static page to list them or perhaps create a static page for each individual publication.

✔ **Guest posts:** Invite others to submit posts to your blog, and offer to guest blog on their blogs as well. Reciprocal links can develop traffic and readership for all blogs involved.

It's best to keep your blog fairly simple, so that it doesn't have a cluttered, chaotic look and is easier and less time consuming to maintain.

Writing Articles and E-Books

A great way to establish and expand your brand is to write articles for magazines (print or online) and e-books. Articles and e-books help to promote you as an expert in some facet of networking. They also provide you with valuable content you can feature in your Facebook, Twitter, and blog posts while establishing you as a thought leader in your field.

Writing for the reader

You don't need to invent something to write an article or an e-book; all you need is an opinion, a tip, or a story about something in business, information technology, or networking. Here are some ideas for an article or e-book:

✔ Your success story and how others can benefit

✔ A description of a problem or challenge

✔ An epiphany or some kind of new insight into a classic problem or situation

✔ A story of a networking failure

✔ Your idea on a new way to solve a classic problem in networking

✔ Your recipe for successfully completing something

When pondering the idea of an article or e-book, think about what benefit your readers will gain. These articles are not about you and how smart you are but about how your message can help others. When you're writing something for your readers, it's about them, not you.

Finding an outlet

If you've written a good article, consider submitting it to print or online magazines or websites for publication. Be sure that the content fits well with the established style and target audience. You might consider asking someone who writes a networking blog if you can submit an article as a guest author.

Or perhaps a publishing outlet will find you. The best way to get your article published is to publish it yourself on your blog. As long as the article uses good keywords so that it can be found in an Internet search, a few people might take notice and either post a link to refer readers to it or ask you if they can put a copy of your article on their website.

Chances are you will not be paid, and it's probably best not to even ask. Getting your article on someone else's website is free advertising for your brand, so don't bite the hand that feeds you.

Similarly, there are several outlets for publishing an e-book that are free or modestly priced. Two such outlets are

- ✔ Amazon Kindle, `kdp.amazon.com`
- ✔ Book Baby, `www.bookbaby.com`

If you pursue an e-publication, you can use it as a for-sale item on your website or blog, a gift to encourage blog subscriptions or event attendance, or a means for generating interest from potential clients or media outlets. You can also repurpose the content for use on your blog, on Facebook, or in tweets, always including a link where readers can obtain the complete e-book.

Publishing E-Books For Dummies is a great resource for publishing your own e-books.

You should refrain from writing tales about your workplace or your clients if you're in consulting, even if you change the names of companies and people. You need to avoid the perception that you're disclosing information about your employer or client that should be kept confidential.

Segregating Your Personal and Professional Lives

As you begin developing your professional reputation, you'll want to help others gain a clear and positive idea about who you are, your unique talents and value, and your career focus, work history, and professional interests. In other words, you'll want to rev up your personal branding efforts.

It's easy to buy into the false notion that you can have one brand for your personal life and one business brand for your professional life, but that's not the way personal brands work. Your brand is, quoting from *Branding For Dummies,* "whatever people believe about who you are and what you stand for, based on what they've personally experienced, what they've heard from others, or what they've seen online. Through personal branding . . . you help them see how you fit into their hierarchy of interests and needs. You enhance how they view you as an asset, a leader, and a star in your field. As a result, you improve how they react when they encounter you or your name and as they decide whether or not to involve you in their lives."

The Internet's long memory

The Internet has countless stories about companies who considered hiring someone until they found and read their public social networking content. Thousands of people have learned this bitter lesson, and you should not have to follow in their footsteps.

The best approach for preventing the potentially embarrassing consequences of social networking is to change your understanding of how the Internet works. Anytime you post something online through a social networking site or a blog, or as a comment on another site, you should consider that action permanent and irreversible. Even if you can later remove an article, a photo, or a comment, it may still be discoverable by someone at any time in the future.

Similarly, you should consider any and every communication, whether by email, chat, instant message, or photo, as public information and discoverable by others. For example, many recent scandals entailed famous people taking and sending private photographs to others, but that content was later revealed to the entire Internet, much to their embarrassment. Even online apps that promise to immediately delete text and images should not be considered safe.

Be clear about the reputation you want to develop and keep all communications — personal or professional — consistent with that brand image.

Because people are likely to either encounter you in both personal and professional situations or to come across online information that reveals both your personal and professional lives, it's important to keep your presentation in both arenas complementary and segregated. In the same way that you likely act and communicate differently in the rec room than in the conference room, you can act and communicate differently in personal and professional arenas. But you need to stand for the same values and traits in both places.

Your professional brand communications are intentionally accessible to the entire Internet — to anyone who cares to seek information you've published. But to the degree possible, your personal social networking should remain separate and restricted to your personal connections. The primary reasons for this follow:

- **Details of your personal life are not relevant to your professional audience.** Although it's nice that you (may) have a family, we don't need to see their Halloween costumes, school play photos, or that great sushi dinner you had last week. Save those for personal social networking.

- **Details of your personal life should not be accessible to the general public.** These details include photographs and names of family members, their schools or workplaces, and their friends.

On Facebook, for instance, you probably should be cautious about who you connect to, because you may be sharing intimate details of your life. But you might readily accept connection requests on LinkedIn from professional associates with whom you would not want to share details about your personal life, no matter how interesting.

If you're heavily into personal social networking on Facebook or similar sites, and if you want to use Facebook as a part of your professional brand, you should build a separate Facebook page and keep your professional information and connections restricted to that page. The same is true for Twitter, Pinterest, LinkedIn, your blog, and any other social networking site that you want to use for both personal and professional purposes.

You need to decide what degree of transparency you want in your public profile, for both your professional and personal social networking. Also consider your privacy and personal safety, as well as that of your family members and other significant people in your life.

A great way to see what others might discover about you online is to undertake several detailed searches on yourself. Examples of ways you might search include by

- Your full name
- Your email address
- Your residence address (try different combinations, such as 123 Elm St. and 123 Elm Street)
- Your date of birth together with your name (you'll need to try a lot of different combinations)
- Your social security number
- Your work address
- Your work email address
- Any other details that are uniquely you

Because most search engines personalize results based on your location and past searches, obtain an unbiased look at your online image by signing out of your Google account, if you have one, or going to the right edge of the Google screen, pulling down the menu, and clicking New Incognito Window to hide your location, IP, address, past search activity, and other identifiers. On Safari, Bing, or Internet Explorer, select Private Browsing. On Firefox, select New Private Window from the File menu. Then study the results, including the results for images linked to your name.

Before you begin your next big job search, it's a good idea to spend a few hours searching for yourself, because any prospective employer is likely to conduct online searches about you as well. When you know what can be discovered about you online, you can take steps to get content altered or removed (or change your social networking privacy settings so that a future employer won't find those beer-binging photos from college). At the very least, you can ramp up efforts to develop strong, well-linked positive content that will push unflattering or off-brand links further down the search results.

You can set up alert notifications with search services such as Google and Giga Alert to periodically email you regarding newly published pages with your specific keywords. These periodic searches can be a good way to discover new information that has been posted about you.

Working with Recruiters

Recruiters come in two flavors: Some are employees of a company looking to fill its own open positions, and others work for search firms that are looking to fill open positions for their corporate clients. In this section, we're looking primarily at the latter.

Think of a recruiter as your business agent, who will go to bat for you and pitch you as an ideal candidate for their corporate clients. In this regard, you need to make sure that your recruiter knows you, your knowledge and skills, and the kind of job you are looking for.

If possible, meet with your recruiter in person. That way, you can better understand the recruiter and he or she can better understand you. Explain your strengths, background, and the kind of job and company you are interested in. Give them confidence that you are a solid candidate with skills and professional integrity. When recruiters present you to one or more of their clients, they are putting their reputation on the line: If a recruiter's corporate client thinks you misrepresented yourself, the recruiter's relationship with that client could be in jeopardy.

A recruiter who is familiar with you and who believes you're a solid performer is more likely to think of you instead of other candidates and is more likely to propose you to more companies.

Chapter 14

Creating a Winning Resume

• •

In This Chapter

▶ Dissecting a typical resume

▶ Putting together the right type of resume for you

▶ Customizing resumes to target specific jobs

• •

A resume is usually the first thing that a typical employer will view about an employment candidate. Often, as few as ten seconds are spent scanning a resume before making an initial "keep or toss" decision, so it's vital that the appearance, structure, and words in your resume give it the best chance of landing in the "keep" list instead of in the trash.

The Basics of a Great Resume

Your resume is a written statement that describes your work experience, education, and short-term career goals. Your resume is your most important marketing tool. Often, recruiters and hiring managers form their first impression of you based on your resume.

Prospective employers are looking for skills, but they are focused on reading about your past accomplishments. How have you saved your employer money, improved security, solved serious issues, or improved efficiency? Tangible results are effective and capture a hiring manager's attention. You need to emphasize positive results in your work experience.

In this section, you look at the various elements of a great resume. The later section, "Different Types of Resumes," describes variations in a resume's arrangement.

Heading

The top of the first page of your resume is the heading, and it contains your name and contact information. If you have prominent certifications, they may appear here as well. Figure 14-1 contains a few sample headings.

John A. Smith, MCSE, A+
123 Elm St., Reno, NV 89509   johnasmith@gmail.com linkedin.com/jasmith

John A. Smith
MCSE, A+
123 Elm St., Reno, NV 89509 | johnasmith@gmail.com

Summary

Many resumes include a sentence or a short paragraph describing the candidate's mission or goals, or a statement about a desired position. Typically, this statement is about your experience and the position you want right now, not a position you want in the future. Your summary should tie directly into the position you are applying for and include a powerful statement regarding your experience, abilities, and meaningful accomplishments.

Example summary statements follow:

- ✔ Technology manager with eight years' experience seeking a software development or software QA position in online financial services.
- ✔ Systems and networking manager with experience managing successful infrastructure upgrades seeking a technology leadership position in a SaaS company. Part-time university instructor.

The second example emphasizes accomplishments in this case, successful infrastructure upgrades.

Employment history

The employment history section describes each job that you've had, along with relevant details. If you're writing a chronological resume, each job will include a summary of responsibilities and accomplishments, as shown in Figure 14-2.

> **Infrastructure Manager**
>
> Employer.com, Seattle, Washington, 1994-1999
>
> • Successful core network upgrades
>
> • Developed network device configuration standards, resulting in more efficient device administration and less unscheduled downtime
>
> • Implemented TACACS+ to simplify administrative access to network devices

If you're writing a functional resume, each entry will include the company, position, and timeframe; the details will appear elsewhere in the resume. Figure 14-3 depicts employment history entries in a functional resume.

Figure 14-3:
Sample
employ-
ment history
entry in a
functional
resume.

> **Infrastructure Manager**. Employer.com, Seattle, WA. 1994-1999
>
> **Operations Analyst**. Company.com, Bellevue, WA. 1990-1994

REMEMBER

Whether you are creating a chronological resume or a functional resume, make sure you list accomplishments and not merely responsibilities and skills.

For a description of chronological and functional resumes, see the "Different Types of Resumes" section, later in this chapter.

Education

The education section describes your formal education, such as the college, university, vocational school, or technical school you attended. Typically, this section is short and may appear before or after the employment history section.

If you have little higher education and work experience, you may need to include your high school education. However, professionals with a college degree probably don't need to list their high school. If you do not have a college degree, list certifications and professional training.

Figure 14-4 contains a sample education section for a professional with more than ten years' experience.

BS Computer Science. University of Washington, Seattle. GPA 3.25.

MS Information Management, University of Washington, Seattle. GPA 3.9

Training and certifications

Training and certifications may appear together in one section or separately. Or you might put training information in the education section. As you can see, no single right way to put this information together exists, as long as it is readable and accurate.

Someone with just a few training courses may want to list them individually. However, if you have 20–40 years of IT work experience, you'll likely have more training courses than can fit in several pages of text! In such a situation, a short narrative for training might appear as shown in Figure 14-5.

Training

Numerous courses in TCP/IP, network architecture, network routing, firewall configuration, systems administration, and database administration from organizations including SANS, Usenix, and Cisco.

Skills

People in a technology field learn a lot on the job, often without formal training, so be sure to include relevant skills on your resume. If you have a lot of skills in technology, you may want to group them in categories. Figure 14-6 includes a good example.

If you have too many skills to list, include relevant and up-to-date skills and discard the rest. For example, if you are applying for a Java developer job and your past experience includes Cobol and RPG, listing those skills may not be relevant. Look at what the company is seeking and highlight your related skills.

Skills

Programming Languages: C, C#, C++, Java, PHP, Ruby on Rails

Databases: MS-SQL, MySQL, Oracle 11i

Operating Systems: Windows 7/8, Ubuntu, RHEL

Networking: TCP/IP v4/v6, routing, Cisco firewalls, Tipping Point IPS

Figure 14-6:
Skills sum-
mary in a
resume.

TIP

If you have a lot of skills but are light on employment history, you might place your skills section before your employment history section, so that someone reviewing your resume will see your skills first.

Other sections

Depending on your background, you might want to include additional sections on your resume. Whether to include each depends on several factors, such as the following:

✔ **Company culture:** Your research needs to include the company's culture — how the company behaves in the community and what it values. Tie yourself into that culture somehow, so that you look like a good fit. For instance, if a company you're targeting emphasizes its volunteer work, include a volunteer work section in your resume.

✔ **Rounding out your profile:** If you believe that you need to emphasize that you are more than just a programming machine, you may want to include a section listing your outside interests and involvements.

Some of the sections you might include in your resume are described next.

Interests

Some professionals include an "interests" section to demonstrate that they are not all work and no play. Outside interests can show that you are gregarious, have varied interests, and have a life outside work. If you know that you have a connection to your hiring manager (or someone higher up in the company) through an outside interest, list it so that you become more familiar.

You could list interests in a short, bulleted list or in a few lines of text, such as "Interests include landscape photography, scuba diving, and RC airplanes."

Industry associations

You can list your industry association memberships, including any positions beyond that of a general member. Figure 14-7 shows a typical industry associations section.

Industry Associations

InfraGard, 1998-2015. Board Member, 2010-2013.

SANS, 2000-2015.

Volunteer work

Often, professionals like to include a short section on volunteer work. It's often not required, but it does demonstrate selflessness and a desire to help others. Employers usually appreciate someone who makes time for others, and volunteerism is a good indicator of someone who is comfortable in a variety of situations.

When filling in employment gaps, show that you kept busy.

References

Customarily, references are not included in a resume. In the past, including a general statement, such as "Professional and personal references available upon request," was common. Now this statement is unnecessary; an employer is going to ask for references whether or not you include this statement.

What I look for in a networking resume

Whenever I am reviewing resumes for networking positions in my organization, I look for the following things:

- ✔ Certifications: Which ones, and how long the candidates have had them (the longer, the better)
- ✔ Technology skills: Which technologies, including products and how they were used
- ✔ Soft skills: How the candidate worked with people in their companies to solve problems and finish projects

A really long list of certifications might indicate too much emphasis on technology skills at the expense of vital people skills. I'd rather see three or four certifications than ten or more.

Problem solving, working on project teams, and completing complex projects mean more to me than a long list of technology skills. I find that you can train someone on new technologies but not on people skills. Those with people skill deficits usually remain in that state throughout their careers.

Peter H. Gregory, Seattle

Resumes For Dummies, 6th Edition is a valuable resource if you want to read more on the topic of resumes and how they can help you find your dream job.

Formatting Your Resume

The format of your resume is as important as its content. If it's cluttered and hard to read, a resume for the best candidate will be discarded as quickly as a well-written resume for an unqualified candidate.

A well-formatted resume has the following characteristics:

- ✔ **Plenty of whitespace:** Text should not crowd the top, bottom, or side margins. There should be room between sections and paragraphs.

- ✔ **Absence of colors:** Keep everything in one color — black.

- ✔ **Single, readable font:** The entire resume should be in one easily read font such as Times Roman, Helvetica, or Arial, with the following exceptions: The heading with your name can be slightly larger and in a different font, and the limited use of boldface and underline is acceptable.

- ✔ **Visual simplicity:** A good resume is beautiful in its simple elegance. In a good resume, less is better.

- ✔ **No graphics:** So many of today's applicant tracking and application systems parse and populate data from your resume. Graphics will cause problems and cause fields to be populated inaccurately. Avoid cool graphics and complicated formatting techniques with your resume. Unless you're a graphic designer or a marketing campaign designer, hiring managers don't care about the graphics and may consider them distracting. Recruiters definitely don't like graphics, because they often must edit your resume, to, say, add a heading.

In short, a well-formatted resume is minimalist in its visual style.

Soft copy

When working with soft copy resumes that you're sending via email or uploading to an employer's website, a job search site, or a recruiter, it's best to send the resume in Word or PDF format. If you're working with an outside recruiter who will be presenting your resume to one or more employers, send your resume in Word format, with the document unlocked, because the recruiter might need to transform your resume into a particular format.

Although Acrobat's cool features include prohibiting printing or copying text from a document, it's better not to use these features in a resume you upload

or email. An employer's screening process might include the need to extract text from your resume, and you don't want to do anything to interfere with that. Best to send your resume as a plain, unprotected PDF.

In most cases, RTF (Rich Text Format) is acceptable format for your resume. Based on the rules of simplicity, your resume probably wouldn't need anything other than RTF in the first place.

Hard copy

For organizations that want hard copy resumes, print them on good quality white copier paper. Printing on colored paper (even the slightest off-white), textured paper such as linen, or paper with a lot of flecks can be harmful. (However, you might consider recycled paper if the company is committed to recycling.) Yes, in many ways you need to stand out, but using a brightly colored or textured resume is risky.

You might consider printing your resume double-sided, to give your potential employer the impression that you know how to be a good steward of resources.

Cleaning up metadata

Before you send a soft copy resume, you need to be sure it's free of metadata and other extraneous data that could cast you in a bad light. Check for the following:

- ✔ **Document properties:** Be sure that the document author and reviewers state your name or are blank. Check the description and also make sure that it contains your name or is blank.

- ✔ **Check for tracked changes:** If you have been using a Track Changes feature, be sure you have performed an "Accept All Changes" operation so that you are sending a completely clean resume free of any prior edits.

- ✔ **Hidden and deleted data:** When customizing resumes, you might mark some content as hidden. Sometimes, deleted content is still in the document. Make sure you have all that cleaned up. One technique is to start with a new, blank document and copy the text from a clean resume into the new empty document.

For more on hard copy resumes, see Chapter 13, which details the contents of a cover letter, and Chapter 14, which describes the interview process.

Tailoring Your Resume

You need to create a targeted resume for each position you seek. Word processing programs make this task fairly easy. However, be sure to develop a system to track each resume you send out.

Organizing your resumes

In this age of word processing programs, every resume should be customized for each particular job and company you're targeting. The method you use to create your customized versions is up to you. Some suggested techniques follow:

- **Super-sized resume (remove the parts you don't need):** Start with a master resume that includes lengthy descriptions of each job, education, and so on — perhaps even multiple separate descriptions. Make a copy of the resume, and then remove the parts you don't need. The result, those component parts that are just right for the position you are targeting.

- **Franken-resume (build from different parts):** From your collection of headings, summaries, employment positions, education, and more, pull together the pieces you want, in the order you want, to create that perfect, targeted resume.

- **Modify the last resume you used:** From the resume you most recently sent to another company, make all needed changes, so that your new resume is just right for the position you're targeting.

Content that you removed for a prior application may be relevant for a later one. Remember to restore content that you may need later.

Using keywords to grab attention

Innovations in automated job posting sites such as Monster.com and Indeed.com have resulted in companies getting hundreds, and sometimes thousands, of resumes for each advertised job. As a result, companies have invested in software that electronically evaluates resumes, based in part on the presence of certain keywords. Too few keywords, and your resume will be routed to the bit bucket.

But just including a lot of keywords in your resume is not enough. If your resume gets through the first layer of screening, someone will be reading your resume to see if you sound like a candidate worth a phone screen. At this point, not so much what you say but how you say it gets you to the next level. Remember, though, that you'll never get to that second level without the right keywords.

Whichever method you use is up to you. Perhaps you have a system different from these that works for you. As long as you can keep your records organized and know which resume you sent to which company (and still have copies of each), you should be all right.

You should also consider keeping a worksheet that lists the resumes you used for each job. You might create a little database that includes a lot of different details about each position you targeted, who you spoke with, which resume you sent and to whom, and so on.

Customizing resume content

Every prospective job is different from every other. Even two jobs with the same job title are different. Every company has its own style and way of doing things. These considerations should compel you to take the time to customize your resume for each job you apply for. Following are some pointers that will guide this work:

- ✔ **Match applicable skills and duties:** Read through the job description carefully, and make sure that each skill and knowledge required appears in your resume when applicable. In other words, if a job description requires Active Directory administration and you have that skill, make sure you include it in each job where you performed this task.

- ✔ **Emphasize company similarities:** Employers like to hire people who are familiar with their industry. If you have work experience in the right industries, make sure your resume includes this information.

- ✔ **Include required education:** If an education level is cited in the job description, and you have the proper education, make sure you include it clearly in your resume.

To make sure your resume stands out from others, you may want to read other position postings from the same company to get a broader view of the desired skills. Also, find out what you can about the company. Search for articles (good or bad) in local press and trade publications to get an even better idea of their recent history.

Plagiarizing

Although looking at other people's resumes is common, you should not borrow more than a phrase or two. Borrowing attractive styles and formats is okay. There is a tale of an employer who did an Internet search of a

sentence in an applicant's resume, and found that exact text (and more) on a sample resume found online. If you have someone else's resume (or a sample) and you like the way something was said, seriously consider rewording it.

Types of Resumes

Every professional has a unique work history, education, skills, and career path, with different strengths and weaknesses. Because of this, no single resume structure will ideally highlight everyone's strengths. For some, showing a progression of employment is ideal. For others, the best approach is to showcase skills and experience. In this section, you look at the two primary types of resumes and a type that's a combination of the two.

Chronological

A *chronological resume* lists work experience, typically in reverse chronological order (with the most recent position first). A chronological resume is the most common resume type because it's the easiest to build and maintain and because potential employers like to see a candidate's recent positions, responsibilities, and accomplishments first.

You'll want to use a chronological resume if you have continuous work experience and your most recent positions are relevant to the company and position you're targeting.

The typical order of sections in a chronological resume is

- ✔ Heading
- ✔ Summary

Finding and using good examples

A good way to figure out how to structure your own resume is to view many other resumes and borrow what you like from each. Because resumes typically don't contain overly sensitive information such as compensation, it's usually appropriate to ask others for a copy of their resume. As long as you have a reputation of being trustworthy, most other professionals will consider your resume request a compliment. As you progress in your career, you might consider returning the favor to those who ask you for a copy of yours.

✔ Employment history, including detailed descriptions of each position and notable accomplishments

✔ Education

✔ Accomplishments, skills, training, interests, associations, volunteer work, and so on

Functional

A *functional resume* highlights your skills and work experience as your resume's primary theme. You'll use this type of resume if your recent work history doesn't adequately show that you have recent, relevant work experience. For instance, if you're seeking a programming job but your last position was something different, a functional resume can emphasize your programming skills even if they aren't as current as you'd like.

Following are some reasons why you might want to use a functional resume include:

✔ A need to emphasize skills

✔ Little work experience

✔ Gaps in employment history

✔ Work in various industry sectors

✔ Employment history that doesn't show a steady progression of job titles or responsibilities

✔ Employment history with a long work history in one position

Following is the typical order of sections in a functional resume:

✔ Heading

✔ Summary

✔ Accomplishments and skills

✔ Education

✔ Training

✔ Employment history, listing only employers, positions, and dates, with no other details

✔ Interests, associations, volunteer work, and so on

Note that in a functional resume, like a chronological resume, you put your best material early in the resume. In a functional resume, you emphasize your accomplishments, skills, and experience, whereas in a chronological resume you emphasize your employment positions.

Combination

A *hybrid resume* is a combination of chronological and functional resumes. A hybrid resume depicts skills, education, and employment history, and these may appear in any sequence.

If you have a professional background that requires you to get creative with your resume structure, try different layouts and ask your peers and mentors for their opinion.

No one perfect resume format exists. The types of resumes discussed in this chapter should serve as a starting point for you to build the resume that perfectly and succinctly describes your skills and work experience.

What Not to Put in Your Resume

Although various countries have local practices on resume structure and content, in most locations you would never include certain items in a resume, such as the following:

- **Compensation:** You should keep records of your pay, but your resume is not the place to include this information.

✔ **Date of birth:** Because you already have your name and contact information, including your date of birth might be excessive. A potential employer will ask for your date of birth on an employment application form.

✔ **References:** Usually, you supply references in a separate document.

✔ **Opinion:** Your opinion of an employer, good or bad, is best left off a resume.

✔ **Work samples:** Including samples of your work could make your resume too long and might violate confidentiality agreements.

Examples of Winning Resumes

This section provides a complete chronological resume, shown in Figure 14-8, and a complete functional resume, shown in Figure 14-9. Both resumes describe the same fictitious individual whose background makes each type of resume ideal for that person.

The chronological resume shows a typical progression of work experience and accomplishments, whereas the functional resume portrays skills, accomplishments, and experience unrelated to the positions in which they occurred.

Padding your resume

It's a popular notion that everyone embellishes his or her resume to some extent. Yes, that statement probably contains some truth. Now and then we hear news stories about people padding their resumes and having to resign.

Your resume should be truthful. In the information technology business, the nature of our responsibilities and our codes of ethics require a high standard of professional integrity. We should not stretch the truth in our resume or in any other written statements about ourselves. Not even a little bit.

John A. Smith, MCSE, A+

123 Elm St., Reno, NV 89509 johnasmith@gmail.com linkedin.com/jasmith

SUMMARY

Networking manager with experience upgrading core network infrastructure, efficient management of network devices, seeking an infrastructure leadership position in a SaaS company. Part time university instructor and board member.

WORK EXPERIENCE

Networking Manager. Employer.com, Seattle, Washington, 2010-2015

- Successful core network upgrades

- Developed network device configuration standards, resulting in more efficient device administration and less unscheduled downtime

- Implemented TACACS+ to simplify administrative access to network devices

Operations Analyst. Company.com, Seattle, Washington, 2005-2009

- Updated operational procedures to improve recordkeeping, resulting in fewer outages and incidents

- Improved operational effectiveness three consecutive years

- President's Club Award, 2008 and 2009

Systems Administrator. Workplace.com, Bellevue, Washington, 2002-2005

- Responsible for management of production and test servers for company business applications, external websites, and internal services

- Incorporated hardening guidelines from Center for Internet Security, resulting in improved results in vulnerability scans

- Developed written procedures for the creation and management of virtual machines

- New Employee of the Year, 2002

Figure 14-8:
Chronological
resume
example.

EDUCATION

BS Computer Science, University of Washington, Seattle. GPA 3.25

MS Information Management, University of Washington, Seattle. GPA 3.9

TRAINING

Numerous courses in TCP/IP, network architecture, network routing, firewall configuration, systems administration, and database administration from organizations including SANS, Usenix, and Cisco.

SKILLS

Programming Languages: C, C#, C++, Java, PHP, Ruby on Rails

Databases: MS-SQL, MySQL, Oracle 11i

Operating Systems: Windows 7/8, Ubuntu, RHEL

Networking: TCP/IP v4/v6, routing, Cisco firewalls, Tipping Point IPS

INDUSTRY ASSOCIATIONS

InfraGard, 1998-2015. Board Member, 2010-2013.

Figure 14-8
(continued)

SANS, 2000-2015.

John A. Smith, MCSE, A+

123 Elm St., Reno, NV 89509   johnasmith@gmail.com   linkedin.com/jasmith

SUMMARY

Networking manager with experience upgrading core network infrastructure, efficient management of network devices, seeking an infrastructure leadership position in a SaaS company. Part time university instructor and board member.

EDUCATION

BS Computer Science, University of Washington, Seattle. GPA 3.25

MS Information Management, University of Washington, Seattle. GPA 3.9

AWARDS

- President's Club Award, 2008 and 2009

- New Employee of the Year, 2002

TRAINING

Figure 14-9:
Functional
resume
example.

Numerous courses in TCP/IP, network architecture, network routing, firewall configuration, systems administration, and database administration from organizations including SANS, Usenix, and Cisco.

SKILLS

Business: creation of procedural documentation, monthly executive reports, business process improvements

Networking: TCP/IP v4/v6, routing, Cisco firewalls, Tipping Point IPS, TACACS+, Active Directory

Operating Systems: Windows 7/8, Ubuntu, RHEL

Security: system and device hardening, security procedures development

Programming Languages: C, C#, C++, Java

Databases: MySQL

WORK EXPERIENCE

Networking Manager. Employer.com, Seattle, Washington, 2010-2015

Independent Consultant, Bellevue, Washington, 2008-2010

Operations Analyst. Company.com, Seattle, Washington, 2005-2008

Systems Administrator. Workplace.com, Bellevue, Washington, 2002-2005

Office Manager. City Realty, Kennewick, Washington, 1999-2002

System Administrator. Employer.com, Kennewick, Washington, 1996-1999

INDUSTRY ASSOCIATIONS

InfraGard, 1998-2015. Board Member, 2010-2013.

SANS, 2000-2015.

Figure 14-9
(continued)

Chapter 15

Getting Attention with Your Cover Letter

*Y*our cover letter is (probably) the first thing the hiring manager will see about you, so you want to make a good first impression.

A great deal of rumor, myth, and legend exists about what makes a good resume and how to construct one to maximize your success in getting a networking job. For some reason, the cover letter is often ignored in this process. Effective cover letters present the link between the job's requirements and your background and aspirations. Although a resume states what you have done, the cover letter cuts to the chase and addresses why you are the right person for the job.

The cover letter has the following logic: "Here is what you said you want. Here is what I have done. Here is how it relates. Here's my number, so call me, maybe." (Apologies to Carly Rae Jepsen.)

The goal is to get the cover letter and resume into the hands of the hiring manager. In a perfect world, your resume would tell the screener in HR, be it an internal or external recruiter or the applicant-tracking system, how good a fit you are. In the real world, the cover letter is your opportunity to spell it out for them.

Cover Letter Scenarios

At the highest conceptual level, your resume is fixed and you use the cover letter to express your interest and to explain why you should be considered. In reality, with digital resumes, you can customize, or at least tune, your resume for each job opportunity. However, it is generally more expedient and effective to use the cover letter to answer the questions of how and why you are a fit.

You would write a cover letter in response to the following four scenarios:

- ✔ **Response to a job posting:** You see a job description that interests you in the careers section of a company website or on a job board, such as monster.com or indeed.com.

- ✔ **Follow-up letter of introduction:** Let's say your friend has a friend who needs someone with your skills and asks to see your resume. When you respond to this request, you had better include a cover letter that at least reminds the reader why you've sent your resume. A resume without context is likely to end up in the bit bucket.

- ✔ **Letter to a recruiter:** Recruiters offer an invaluable service in connecting employers with prescreened candidates. The goal of this cover letter is to get you from the unscreened category to the prescreened category.

- ✔ **Generic application:** You can send your resume to a company to keep on file in case they have a need for someone like you.

The cover letter differs for each scenario. In general, you'll spend most of your time writing cover letters in response to job postings. However, follow-up letters of introduction are more effective. Figure 15-1 shows the source of new jobs of all types, not specifically networking jobs.
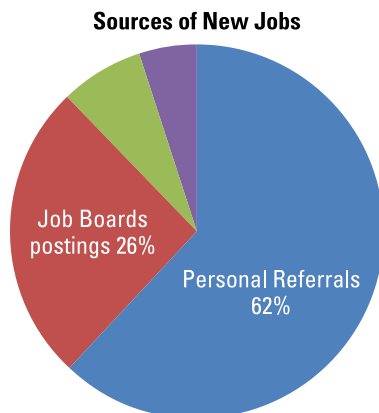
Sources of New Jobs

Figure 15-1: The sources of new jobs.

Job Boards postings 26%

Personal Referrals 62%

Source: U.S. Department of Labor

This figure implies that you should focus on personal networking to get a job in computer networking. However, responses to job postings are something you can work on while you wait to hear back from your contacts. The next sections explore ways to make your responses to job postings as effective as possible.

For more about creating and improving your brand, see Chapter 15. Find out how to create a winning resume in Chapter 14.

Essential Elements of the Cover Letter

Regardless of the scenario described in the preceding section, all cover letters have the following common elements:

- **Greeting:** Say "hello" in some manner.

- **Reason for the cover letter:** Before you start writing about how good a fit you are, give the reader some context. The reader of your cover letter doesn't necessarily know why he or she is reading it. Clarify who you are and the job you're seeking.

- **Logic of how you fit:** In this element, which is the body of the letter, you tie their needs to your skills and experience, point by point. Don't go down the list of every skill or experience stated in the job posting. Choose the two to four most critical requirements and focus a paragraph, maybe two, on those. You don't want a cover letter to be too long.

- **Call to action:** Now that you've laid out your logic, tell them what to do. Cover letters without a call to action, even one as minimal as asking for a return call, leave the reader feeling flat. The letter leaves the impression that you are interested only in talking about yourself.

- **Closing:** At this point, your goal is to get an interview. In the closing, sound excited and mention that you are looking forward to hearing from them.

The traditional cover letter

Readers of a certain age will recall a formal process associated with sending prospective employers a cover letter and resume. You'd take the draft of your resume to a printer, who would print your order of 250 to 500 copies (without typos, you hoped).

Next, you'd write your cover letter to respond to a particular job or one of the other scenarios described previously. If you were cool, your resume, cover letter, and envelope would use the same high rag content paper, preferably ecru. Off they would go in the mailbox to the intended recipient. A sample cover letter of this type is shown in Figure 15-2.

William D. Boyce
1325 Walnut Hill Ln
Ottawa, IL 89049

May 26, 2015

Mr. John Hireme
Initec Widgets
742 Evergreen Terrace
Arlen, TX 90120

Dear Mr. Hireme,

I have read your posting for the position of network analyst at Initec Widgets. Based upon your description, I have the skills and experience that you are seeking. I have seven years of network analyst experience at a number of leading firms.

I learned many of the basic skills of network management while at the Bre-X Mining Corporation. I later applied and refined my skills at the sub-prime mortgage unit of the Washington Mutual Bank of Seattle, as well as at Bernard L. Madoff Investment Securities, LLC in New York.

Your job description calls for a networking professional with extensive experience in delivering high-quality data communications with secure financial transactions. I am proud to say that my work has stood up to intense scrutiny and has not been found lacking.

I have attached my resume to more fully describe my background. I would like to explore your needs for this role at your convenience.

Sincerely,

William D. Boyce

William D. Boyce
Encl.: Resume for William D. Boyce

Figure 15-2:
A formal
cover letter.

Sending a traditional cover letter by post is now as outmoded as rotary phones and CRT monitors. Their use says that the user is stuck in the old ways.

Cover letters with applicant-tracking systems

These days, the vast majority of job posting ads are on the Internet. Applying to them involves creating an identity on the applicant-tracking system of the hiring company (or the recruiter). After you create a user name (often your email address) and establish a password, the system will typically import your resume to populate what it can.

It would be convenient if applicant-tracking system could perfectly populate all routine data fields from a resume. But often, it does not. You as the job seeker get to spend your time both uploading your resume and then copying much of the same information into the fields. Although there are some efforts to improve this process, it is still painfully tedious.

Errors in cover letters are unacceptable.

Many companies enable you to upload or copy-and-paste a cover letter. The image in Figure 15-3 is a typical example.

Figure 15-3:
A cover letter form in a typical applicant-tracking system.

The following sections offer helpful guidelines when writing a cover letter.

Greeting

A formal greeting is "Dear Sir or Madam" or "To whom it may concern." Some may find this type of greeting formal or stilted. With all due affection, get over it, unless you know that the company you're applying to would be put off with formality. A more casual option is "Greetings" or "Hello." You might be able to get away with "Hey there" if you're applying to a company stuck in 1960s counterculture. Otherwise, err on the side of formality.

Reason for the cover letter

The first sentences of the body of the cover letter give the reader some context as to why you're contacting them. Do not assume that the reason is readily apparent. Be helpful and tell the hiring manager which job you are seeking.

A formal start might look like this: "I have read your posting about the position of Network Analyst at Hughes Aircraft Company. Based on your job description for this role, I have the skills and experience that you are seeking."

Adding the job number in this introduction is always appreciated and sends a signal that you know what you are doing and are organized. Managers want to hire people who are more organized than they.

Again, don't worry if the introduction sounds formal. You can restructure it to fit your own voice, but don't delete any information.

In your cover letter, don't include phrases like "as you can see from my resume."

Logic of how you fit

Next, explain from the company's perspective why your skills and experience match what they need. These paragraphs need to be *short and compelling*, ideally highlighting the most relevant aspects of your background.

So how do you know what is compelling? You don't. The best you can do is make inferences from the job description, and hope you get it right.

In any case, you need to tie your background to their needs. For example, if one of the first bullets in the job description refers to experience in troubleshooting, by all means, talk about your experience in troubleshooting.

A typical paragraph may begin with "The job description emphasizes experience in troubleshooting of network issues. While a network analyst at Enron, I managed the trouble-ticketing system and provided ongoing reports to management on issues."

WARNING!

Unsuccessful cover letters share these characteristics:

- ✔ **Exclusive focus on what you have done:** Tie your experience to the requirements in the job description. For example, having a great education is not enough; you must state how your education applies to the job.

- ✔ **Hubris:** If you give the impression that you are the best candidate in the entire world, the recruiter will think your ego is far too large for the organization.

- ✔ **Poor grammar:** Errors in the cover letter are showstoppers for many companies. If in doubt, ask someone to read your cover letter before you click Submit. Automated spell checking and grammar checking are not enough to catch every error.

Recognize that you must have experiences that relate in some way to the job. If not, applying is a waste of your time.

TIP

Many of these fields have a spell checker. Do not rely on spell checkers. Write your cover letter using your computer's word processor and save it along with the job description in a file. In this way, you are more likely to catch typos, which can kill an opportunity, and you'll have a copy of your cover letter if you get the interview.

Call to action

When applying to a job through an applicant-tracking system, about the only thing you can write for your call to action is "I look forward to hearing from you about this opportunity." This one sentence communicates that you want something to happen and sends the message that you are a doer.

Closing

End your cover letter as you would if it were a hard copy. Write "Sincerely," or "Sincerely yours," and then put your name below it. Done.

When you have your letter prepared, copy and paste it into the cover letter box or upload it to the applicant-tracking system.

REMEMBER

Your cover letter (as well as your resume) will be digitally uploaded, and the applicant-tracking system will search it using keywords. It is critically important that a search on relevant keywords will show multiple hits for your cover letter and resume.

As mentioned, most companies allow you to enter a cover letter. Some notable exceptions are Microsoft, Amazon.com, and Verizon. These organizations believe that they can discern what they need strictly from your resume. This approach saves applicants time and encourages them to submit many applications, without much discernment as to whether there is a good fit.

Persistence

Paula Abdul, now a famous celebrity, got her start as a cheerleader for the Los Angeles Lakers, but she was not immediately selected for the squad. In an interview with Arsenio Hall, Miss Abdul confessed that she was cut. She reregistered, and tried out again. Again she was in a group that was cut, but she got in line with the group that was not. Then she was selected and started her career.

The message here is persistence. Do not give up on a position until they send you a letter stating that you are no longer under consideration. Until you get that letter, feel free to keep on trying for similar jobs at that company or the same job if the position posting is updated. The folks in HR and hiring managers might change their mind. Even if the job description stays the same, they may realize that they were too selective. You may just have the skills that they now realize they need.

Cover letters for referrals and recruiters

When you send a cover letter to a referral or a recruiter, compose it in an email message. However, the cover letter is not an email to an old friend. You should come across as a professional. The elements of the cover letter are the same, but the content is adjusted to suit the context.

Greeting

The good news is that you have the person's name. Use it. In an email message, it is okay to write "Dear Miles" or just "Miles." (Assuming the person's name is Miles. Otherwise, it would be awkward.) Email is a casual medium, so there is no need to write, say, "Mr. Raymond."

Reason for the cover letter

When you state the reason for the email, just lay it out there. "I was told by our mutual friend, Maya Randall, that you are seeking a security analyst and that you requested that I send my resume." Similarly, a recruiter will want to know why you are sending the email. "I understand that you recruit networking professionals for organizations in which I am interested" is sufficient.

Logic of how you fit

When you describe the logic of how your skills fit the requirements, be short and sweet. For example, "I have recently completed my Cisco Certified Network Professional Certification (CCNP) as Maya may have mentioned. I am now seeking the opportunity to use this certification at a firm such as

yours." For recruiters, you would write, "I have recently completed my Cisco Certified Network Professional Certification (CCNP). I understand that placing professionals such as myself is your area of expertise."

Call to action

Because you know the person's name and contact information, you have the opportunity to follow up. Your call to action should be polite and should give the person a chance to contact you. For example, you might write, "I have attached my resume to more fully describe my background. Please let me know if you have any questions. I will follow up with you in a week."

You need to be precise in your follow-ups. If you say you will follow up in a week, follow up in a week — not sooner, not later.

Closing

In the closing, write "Sincerely," on one line and your full name on the next. Some people omit the closing. This may be appropriate in correspondence with people you know, but it does not work here.

Generic replies to cover letters

When you get a response from a company that has reviewed your resume and cover letter but is not interested, they reassure you that they will keep your resume on file should another opportunity that better matches your background becomes available. It could happen. And the Cubs could win the World Series.

Although the chances that the employer will contact you in the future are slim, they are better than if you did nothing.

Your resume and cover letter will go into the applicant-tracking system and be available should the hiring manager need someone with your qualifications. This aspect of an applicant-tracking system works best when you have a unique skill.

Chapter 16

Bringing Your Resume to Life: The Interview

In This Chapter

▶ Knowing what employers look for during an interview

▶ Preparing to answer likely questions and impress interviewers

▶ Developing and selling your image

▶ Saying "thank you"

*T*he words on your resume and in your correspondence have taken you this far. The job interview is your opportunity to present your case on why you are the best candidate for the job.

Job interviews can be stressful. Regardless of whether you are introverted or extroverted, being on your A game for an extended period can take its toll. You can reduce your stress by being prepared.

The goal of this chapter is to give you the information you need to be as prepared as possible for an interview. You explore the purpose of the job interview, the types of interview questions you might face, and ways to appear as confident as possible. You also find out what *you* should get out of the interview so you can determine whether the job is right for you.

Knowing Why Interviews Are Important

First things first. You are not an interchangeable cog in a wheel. Similarly, the job responsibilities of a network analyst differ depending on whether you work at the National Security Agency, a local school district, a white shoe law firm, or a dot.com start-up. The technology is related, but the temperament of the users, the topology of the offices, the security requirements, and the corporate culture differ. All these factors contribute to the issue of whether a job is a good fit in terms of your technical competence and personality.

Your training, experiences, skills, flaws, ambitions, blind spots, strengths, and weaknesses define you. Your prospective employers also have training, experiences, skills, flaws, ambitions, blind spots, strengths, and weaknesses that define them. The interview is a chance to see whether the job and the company are a good fit for you and whether you are a good fit for them. Can we all just get along?

Preparing for the Interview

Preparation is critical for a successful interview. Sun Tzu, the author of the definitive book on military strategy and tactics, said, "Every battle is won before it's ever fought." The implication is that the side that is best prepared wins a battle.

Your goal is to get a job offer, so you must be as prepared as possible. You need to do a number of things to succeed: be prepared psychologically, know the prospective employer's environment, make a great first impression, and know what to say and what to ask.

Preparing yourself psychologically

The interview process is necessary but not natural. To be successful, it helps to put yourself in the right frame of mind:

- ✔ **Be on time.** Getting there right on time creates stress, which you do not need, so arrive five to ten minutes early. If you arrive more than 15 minutes early, just sit in your car or wait outside until you're within 15 minutes of your scheduled interview.

- ✔ **Allow them to take control.** If you are a take-charge kind of person, let that go. You are on their turf now, so do as you're told. Sit and go where they take you — with a smile on your face.

- ✔ **Turn off your phone.** Really. Do it. If it so much as vibrates, it can be interpreted as disrespectful to the interviewer. Do whatever you need to do to ensure that you give your interviewers your undivided attention.

- ✔ **Take notes.** Your memory is never as good as you think, in case you've forgotten. Bring a pad of paper. Ask your interviewers if it's okay to take notes. If it is, write their name and some highlights. This information will come in handy when you write thank-you notes. It may seem ironic to take notes on a pad of paper during an interview for a technology job, but using your computer, tablet, or smartphone instead would be distracting.

Investigating the corporate culture

Before the interview, investigate the company. Employers like to see inter-viewees who have done their homework and are serious about this opportu-nity. A lack of basic understanding of what the company does is a big red flag for many managers. Do not fall into the trap that computer networking is a support function so knowing the company's business is not that important. It is important to the management team who might want to hire you.

So how do you find out about the company? Following are your primary options:

- ✔ **Read the company's website.** Read the website thoroughly. Look at other jobs they are advertising. You can learn more about the organi-zation by reading its other open position descriptions. You can learn about the technologies in play, internal initiatives, and maybe a thing or two about new products or services they're working on. Become familiar with their solutions and their customers. Know their founders and their board members.

- ✔ **Find a contact at the target company via LinkedIn.** If you're not already on LinkedIn, put down this book right now and sign up. Come back to this page when you are finished and have linked with at least a few of your work friends. Not having a LinkedIn account when you are job hunt-ing is like not being on a social media site when you are an adolescent and want to have social contacts. For more on LinkedIn, see Chapter 13.

  After you have a stable of contacts, you can enter the name of the target company and see how well you are connected. When you find a contact inside your target company, ask them if you can meet or at least talk on the phone. I have never found a company where I learn more from the website than talking to an employee for five minutes.

- ✔ **Find a contact at the target company via alumni networks.** The same logic as described in the preceding point applies to using your alumni network. Talk to someone within the company. Only a stick-in-the-mud will ignore a request for a brief call.

- ✔ **Look up reviews on Glassdoor.com.** If you can't find a contact, look at company reviews on Glassdoor.com. After you log in, you can see how other employees rate your prospective employer. As long as you under-stand that this site tends to be over-represented with disgruntled former employees, you can find some interesting perspectives on what working at this firm is like.

- ✔ **Study the company financials.** If the target firm is publicly traded, check its profitability. If you have no idea what you are looking for, read some of the financial expert analyses of the firm. Your main concern

is to know whether this position is open because they are growing like gangbusters and need help, or they are a sinking ship and the staff is leaving in droves.

✔ **Poke around on the Internet.** A good ol' Internet search will uncover some interesting tidbits of information. Give it a try. You have nothing to lose!

Preparing for the first impression

Depending on the expert, it takes between one-tenth of a second and seven seconds for a person to develop a first impression. Regardless of whether this is fair or not, it is human nature.

Remember two facts. One, that impression may be positive, but it can't hurt to do everything possible to help your chances of success. In a moment, you learn about some ways to make a good impression (feel free to use these tips in other situations).

Two, you may never know what the interviewer is seeking. For example, in many cases, facial tattoos are problematic. However, if the person worked, say, at a call center, facial ink might be seen as a plus if the candidate was polite on the phone and otherwise technically competent. Why? Too many employees from call centers learn their skills and then leave to work in retail. There's nothing like a pentagram tattoo on the forehead to make for a loyal call center employee.

Be yourself. It does everyone a disservice if you pretend to be someone you are not. That said, you can be yourself and help your chances of creating a good first impression as follows:

✔ **Wear clothes that are one step nicer than is worn in the office.** So how do you know what they wear in the office? Unless you know that the interviewer wants you to dress business casual or even casual, you should wear a dark conservative suit, a white shirt (and for men, a tie). In most cases, it doesn't hurt to be overdressed, but being underdressed can be devastating.

✔ **Don't smell.** Don't smell either good *or* bad. You don't want to hit the interviewer with too much of your best perfume or cologne or the onions from your Big Mac. Good grooming is also essential.

✔ **Show good posture.** Good posture conveys confidence. Don't sit back in your seat. Sit toward the front edge of your chair with your back tall and straight.

✔ **Make eye contact and smile.** Making eye contact is important in the majority of North America businesses, and a smile conveys confidence.

> Work on these skills to avoid making the interviewer feel awkward. However, these gestures can be a significant challenge to someone from a different culture. Native Americans, Latin Americans, and Asians, for example, may consider it rude to look someone directly in the eyes, particularly when introduced to a person in a superior position. Know with whom you are interviewing.

The basic strategy is to make the interviewers feel at ease so that they can focus on your qualifications, not the spinach stuck in your teeth.

Most hiring managers are well trained in Equal Opportunity rules. If you are a member of a protected minority, do not make this an issue. Most companies actively want underrepresented minorities. Ideally, they want to give a person a chance, but some may only want to enhance their status with the bosses who are seeking to comply with nondiscrimination laws. Whatever the underlying cause, this requirement works best when you, the candidate, come across as competent in your area of expertise and not as a militant promoting minority rights. Just be a good team player.

If, in spite of training the interviewing managers received, you are openly discriminated against, immediately document the offence. Relay your experience of discrimination to the HR department. If you're certain that you've been asked an illegal question about your protected status, you probably don't want to work in the organization anyway.

Preparing to say what interviewers want to hear

Beyond all the preparation, ultimately the interview will determine whether you have the technical chops to perform the job and the personal skills to mesh with the company's culture. They want to find out if you are a better blend of technical skills and temperament than the other folks they are interviewing.

REMEMBER

It costs an organization a lot of time and effort to fire a person, so companies want to make sure that they are making the right decision when they bring you on in the first place.

Regardless of the interview style, you can improve your chances of getting an offer by doing the following:

✔ **Bring several hardcopies of your resume.** If your interviewer does not have a copy (or, more likely, did not have time to read your resume before interviewing you), you can offer a hardcopy. It is not a total waste of your time if the interviewer does not have a resume on which to take

notes, but it is close. A softcopy doesn't work as well in the interview environment.

- ✔ **Bring a hardcopy of the job description.** This copy is for your reference during the interview. It is bad form for you to have your laptop open during an interview.

- ✔ **Directly connect what is in the job description to the skills found on your resume.** Citing examples of work experience and training in comparison to the words in the job posting makes a powerful case. Before the interview, put together a cheat sheet with the words in the job description on your left and your qualification on the right. The conversation will flow better as you use your cheat sheet to link their requirements to your experience.

- ✔ **Answer in the positive.** If they ask if you have done something you have not done, respond with a related effort. For example, suppose they ask, "Have you designed a LAN for an office with 50 people?" If you haven't, you could say "No" and that would be factually correct — and you wouldn't get the job. Or you could respond, "I worked in an office with 25 people, but the design specification was to support up to 60 people and two smaller remote offices." This answer is factually correct *and* communicates that you are ready for the larger task. This advice takes some work, and you have to be on your toes to be a good spin-doctor.

- ✔ **Work your soft skills into the conversation.** Add unsolicited details about how you anticipated problems and took appropriate action to help your employer avoid or solve them. Employers want to hire employees who prevent problems. They will hire a lower skilled employee who gets along well with people and can keep the distractions down. You win if you bring these up first.

- ✔ **Discuss how you can add value to the company.** A common frustration managers have is that employees think narrowly about doing their job and don't think about how their job makes the company successful. Working in your past value contributions during the conversation will demonstrate an understanding of your job in the larger context.

Value is a key word in today's business world. You should always speak of your contributions in terms of value.

Following are some things that you should *not* do during an interview:

- ✔ **Speak negatively about previous or current employers.** You may work at the worst company in the world and for the worst boss in the universe. You may be desperate to get out of your current situation. Resist the temptation to say anything bad. This is an interview, not a therapy session. Do whatever it takes to stay positive. Talk about how you have grown and are now seeking greater challenges.

✔ **Reveal confidential information**. During the interview, never divulge
details about your current company that could be considered confiden-
tial. If they want to obtain the experience that their competitor has paid
for, let them make you an offer. Even after you are hired, it is poor form
to traffic in confidential information. Your new company may appreciate
it, but they will also know that you lack professional integrity.

✔ **Misrepresent your skills, work history, training, or education.** You will
be found out, and being found out is cause for immediate dismissal in all
50 states and the District of Columbia. If you get through the interview
process and are hired under false pretenses, you will get to keep your
paycheck during the two weeks in which they figure out the truth. You
will then need to spend the rest of your career explaining why you were
employed for such a short time. It's just not worth it.

✔ **Talk too long.** Perhaps you enjoy interviews. You may find it fun to
have the undivided attention of someone so you can talk about yourself.
Avoid this trap.

Preparing to hear what you want to hear

As mentioned, the interview process is an excellent time to find out if this
company is going to give you the fulfillment you are seeking. Assuming you
are meeting multiple managers and prospective coworkers, you have the
opportunity to find out if this company will give you the professional experi-
ence that moves you forward in life as well as the work/life balance that you
need at this point in your journey.

Chapter 19 offers ten questions you can ask to find out whether this company
will be a good fit for you. The assumption in these questions is that you know
what you want beyond a big fat paycheck.

Consulting firms and startups are known for being demanding on your sched-
ule. More established firms, particularly ones in stable industries, do have
their moments when all hands must be on deck, but these late-night scenar-
ios are few and far between. It is best to consider where you want trade-offs.

In addition, Part III discusses various types of organizations and their
demands on your work-life balance.

Types of Interviews and Tips for Each

In general, you won't know what kind of interview you are going to experi-
ence. Beyond the start time, perhaps the end time, and directions to the facil-
ity, you will typically have no idea if you are going to one long interview or a

series of short interviews. You won't know whether you are interviewing with one person at a time, or a panel of interviewers. You won't know if the focus will be on technical skills or other relevant characteristics. You will need to be prepared for any of these scenarios and roll with the punches as the day goes on. If you have a friendly contact on the inside, he or she may be able to provide you with insight.

The following are the most common forms of interviews you'll encounter.

Open-ended interview

An open-ended interview is the simplest and most common type of interview. The interviewer comes in and asks you to be taken through your work history. It is usually in your discretion whether you go from your earliest education to present day or the other way around. In either case, you should practice describing your professional journey. (We find it logical to start at the beginning.) Find a sympathetic friend or relative and practice before your first interview.

Be careful. If the interviewer asks for a summary of your job history, give them a brief summary. Let the interviewer ask for more details. Being long-winded on your first interview question is a fatal mistake!

The painful reality is that the interviewer may not have read your resume. Although this might seem discouraging, it is an opportunity because you can take the interviewer through your resume and highlight the technical and leadership areas that relate to the job description.

You can also let the interviewer see how you have grown professionally. By the end of the day, you may have repeated this story four or five times. Just remember that this is a new story for each person you meet. It is okay to enthusiastically emphasize the same points.

It will help to have some practice interviews. Few are smooth talkers the first time we talk about a subject, even if the subject is ourselves. Work with someone who does interview coaching professionally so you can get feedback. College and technical schools where you are an alumnus or have some affiliation often offer interview-coaching service. Your state's department of employment often offers interview-coaching service to unemployed citizens.

Technical interview

The technical interview format tests your technical skills. Usually, a technical professional gives you a test consisting of true/false questions, multiple

choice, open-answer questions, or hands-on problem solving. The questions help the company determine whether you can perform the tasks required in the position.

Technical interviews tend to go one of four ways. One, the interview is straightforward and you pass with no problem. Two, you are familiar with the questions but are a little rusty. Three, the questions are unfamiliar, and you come to realize that you don't have the skills that they are seeking. Four, the questions have nothing to with the job as described.

The first scenario, or course, is the ideal. The second scenario is under your control but only before interview day. If you have any indication that there will be a technical interview, brush up on your certifications. How deeply you dive into refreshing depends on your motivation and available time. The trade-off is that you have the chance to refresh your memory with manuals and other resources when you have the job. This is the challenge with technical interviews. As with so many other things in interviews, you can't anticipate every question in every challenge you face. Being as prepared as possible is your only approach.

What if you find yourself in the third situation, where the questions look legitimate but you don't have a clue where to start? This embarrassing situation will be made worse if you do not speak up to say that there must have been some misunderstanding about your qualifications. It takes courage to admit that you are not qualified, but your honesty may pay dividends later.

In the last situation, when you are asked questions that are not relevant for the job as described, perhaps the left hand in this company doesn't know what the right hand is asking. The only saving grace in the situation is that the hiring process probably involves nontechnical interviews. That would be your opportunity to clarify that you are eager to take a technical test more closely suited to the kind of work that you expect to be doing. It is risky, but the only thing you can do to save this opportunity.

Another more recent version of the technical interview involves white boarding a technical challenge. The interviewer might present a scenario and then draw something on the whiteboard. You are then asked to add details and explain your logic. Or the interviewer might verbally describe a problem and ask you to whiteboard the problem and its solution.

Chances are, the interviewer is describing a current or recent issue, or something memorable from the past. Remember, this is an interview, so you need to treat the problem as theoretical. It is not a good idea to ask whether this is an actual problem that the business is facing right now.

ANECDOTE

How deep is your knowledge?

I was interviewed for a consulting job in a small company. One of the company partners interviewed me and asked technical question after technical question. I couldn't answer many of them, and I politely told him so each time. I figured I was not going to get the job. But at the end of the interview, he said, "I knew you wouldn't be able to answer every question. I ask hard questions to see how people respond to difficult situations, and because I want to know just how deep your knowledge goes."

I was instantly relieved (and it probably showed), and I got the job!

Peter H. Gregory, Seattle

If you are venturing into uncharted territory, don't be afraid to say so, but keep talking through the problem and do the best you can. Unless the interviewer tells you, you might not know whether the topic you've been asked to discuss is part of your job or something more advanced that you would not be expected to work on right away.

Behavioral interview

A recent trend in interviewing circles is to make the interview process more meaningful than one where the candidate repeatedly reviews his or her resume for a series of interviewers. In behavioral interviews, HR asks each interviewer to ask candidates about how they handled a situation or two.

At least in theory, HR collects the notes from the interviewers and shares them with the team. You can tell that this is the kind of interview when you get asked a questions that starts "Describe a situation where you." For example, describe a situation where you

- ✔ Had a difficult coworker and how you handled it
- ✔ Encountered a technical obstacle and how you overcame it
- ✔ Set your sights too high
- ✔ Set your sights too low
- ✔ Were able to use persuasion to convince someone to see things your way
- ✔ Used good judgment and logic when solving a problem
- ✔ Had too many things to do and were required to prioritize your tasks

✔ Set a goal and were able to meet or exceed it

✔ Had to use your presentation skills to influence someone's opinion

✔ Had to go above and beyond the call of duty to get a job done

✔ Showed initiative and took the lead

✔ Used your fact-finding skills to solve a problem

✔ Anticipated potential problems and developed preventive measures

✔ Had to discipline or terminate an employee

You should have ready answers to these questions even if you do not have a behavioral interview. If you dig back through your experiences, you'll probably come up with good answers even if they do not relate to a work situation. Your answers will show that you are competent and can think on your own.

Panel interview

Panel interviews are arguably more efficient than single interviews because you don't have to repeat yourself multiple times covering the same background and qualifications. In this scenario, you walk into a room with a group of interviewers. Usually the more senior person will lead the questions, but everyone gets to ask questions and form their own impressions.

Many people find panel interviews to be more stressful than the other interview types. If you fit this description, it might help to consider that you need to be truly on for only one interview.

Confrontational interview

In a confrontational interview, the interviewer comes in angry and challenges every statement you make. The interviewer challenges you when you are right, when you are wrong, and when you voice an opinion. You may as well be a new recruit for the Marine Corps during your first week on Parris Island.

Thankfully, this kind of interview has gone out of vogue. Perhaps this interview technique weeds out candidates who would struggle under the stressful situation of working at the company. If you come across this kind of interview technique, take it with a grain of salt and try your best not to become flustered.

Videoconferencing interviews

Many companies now perform videoconferencing interviews, for a variety of reasons. With more of the workforce working out of their homes, some of the people who may be interviewing you may not live in the city where the company is located. Or perhaps you are interviewing for a national company with people scattered all over. You might also be interviewing for a job in a city where you are considering relocating.

If you are in a videoconferencing interview (for example, Skype with video), you need to be prepared:

✔ Find a quiet place free of distracting sights or sounds.

✔ Check what the interviewer will see behind you.

✔ Make sure your Internet connection is reliable and fast enough for high-quality video and audio.

✔ Check that the lighting on your face and background results in a good image.

✔ Test your technology with a friend to make sure your hardware and software work properly. Nothing is worse than experiencing technical problems during a video interview.

The rules for making a good first impression during in-person interviews apply also to videoconferencing interviews.

Your Turn to Ask Questions

In almost every interview, the interviewer will ask if you have any questions. Like other aspects of the interview, you need to prepare. Blurting out, "How do you like working here?" is not a good first response. This shallow question will almost always get a positive answer, whether the interviewer likes the job or not.

Before your interviews, write down some questions based on your research on the company or when reading other job descriptions or reviews from `Glassdoor.com`. Some examples follow:

✔ Ask whether the open position is new, or would you be replacing someone who left the company? (Don't pry too much on the reason your predecessor left.)

✔ Ask questions about management above the hiring manager.

✔ Ask about current or upcoming projects that you may be a part of.

✔ Ask a follow-up question on a topic discussed in this interview or a prior interview.

✔ Ask about recent events described in the company's press releases.

Chapter 19 contains more ideas for questions you can ask in your interview.

Focusing on the Goal

To get an interview, at least someone in the company has read your resume and perhaps done a phone screen. You have followed the guidelines, aced the technical questions, and assured them that you are cool (or at least cool enough for this role). Now you want to end the interview with a strong close.

If you were an interviewer and had two equally qualified candidates, would you hire a person who is eager for the job or one who seems indifferent? The clear answer is that the one with energy and enthusiasm has the advantage. Be that person!

Offering the following information shows that you are ready, without being too pushy:

✔ **Tell them when you could start.** Don't be shy about this. State it as a fact that you would need to give two weeks' notice. Tell them if you need longer because of a project you are completing. In practice, companies struggle to move fast anyway. You will come across as a person who is positive and has integrity.

✔ **Ask for their contact information.** You want the opportunity to follow up. Ask them if you may follow up if you haven't heard from them in a certain timeframe, depending on when they tell you that you can expect to hear something.

✔ **Mention any special circumstances.** Assuming that things are looking good, tell them now if you have a non-disclosure agreement (NDA) or a non-compete clause. These can usually be managed. Telling them now is better than after you have an offer and they need to rescind it.

Writing a Thank-You Letter

Thank-you letters are one of the easiest — and most overlooked — ways to stand out as a job candidate. Think about it. You've no doubt spent many hours creating your resume, writing cover letters, applying for jobs, and preparing for and going to interviews. What's another ten minutes of your time

to write a short note of gratitude? A thank-you note helps the interviewer remember who you are (which is helpful if the interviewer has talked to several candidates over an extended period of time) and could be the icing on the cake that gets you the job!

You thought you were buying "Getting a Networking Jobs For Dummies," not "Business Etiquette For Dummies." Actually, you bought both, because getting and keeping any job requires proper business etiquette. And writing a thank-you note is essential if you want to stand out as a candidate who is interested in working for the new organization.

In Chapter 15, we mention that you should ask each interviewer for a business card. If you followed our advice, you know the full name, title, email address, and snail-mail address of each interviewer.

If you don't have all this information, check the company's website to glean as much as you can. Then contact the HR department or the recruiter you worked with to provide the rest.

Within 24 hours of your interview, write a thank-you letter to each person. This effort says a lot about who you are, your enthusiasm for the position, and how you would conduct yourself when employed. If nothing else, it sets you apart from the other schlubs who interviewed for this position and did not write a thank-you note.

However, don't write a hastily penned, canned note in the parking lot immediately after your interview. Spend the time to write a professional, meaningful, and personalized letter of gratitude.

Handwritten thank-you notes are a nice touch, but if your penmanship isn't neat and legible, stick with a typed letter or an email.

Thank you notes should be brief — typically no more than two or three *short* paragraphs. As with all written correspondence, use a business letter format and proofread your letter for proper grammar and spelling.

You might start your note with "Thank you for taking the time to meet today. I enjoyed our discussion about the opportunity, particularly the part where we found that we both took our Basic Networking class from Dr. Skolnick! Now that I have met many people from your team, I am even more excited about working at the law firm of Dewey, Cheatham, and Howe."

In addition to expressing appreciation for your interviewer's time and consideration, each thank-you letter should include specific details from the interview and then highlight something in your background that was relevant. (This is another reason why you should take notes in your interviews.) These

people may have interviewed dozens of people, and it will help if you can stick out. For example:

- ✔ Emphasize specific qualifications or discussion points in which that particular interviewer seemed to show interest.

- ✔ If the interviewer asked you a question that you didn't answer as well as you would have liked, use the thank-you letter as an opportunity to refine your answer.

- ✔ If you forgot to mention something important during the interview that may help their decision, bring it up.

- ✔ Summarize the two or three most important points that you want them to remember about you.

Finally, close your thank-you letter by expressing your continued interest and enthusiasm for the company and the position.

Write a different thank-you note for every person you meet at your interview and address each note by name. Be sure to include the receptionist and any assistants you met at the start of your interview (believe it or not, these are often some of the most important — and overlooked — people in the decision process. Always treat them professionally and courteously).

Chapter 17

Becoming a Star Employee

- -

In This Chapter

▶ Settling in

▶ Making yourself irreplaceable

▶ Adjusting to changing conditions

- -

*A*ccording to one school of thought, all you need to do to keep a job is to show up to work on time, perform according to your job description, and do what you are told. We don't know whether this was ever true, but we do know it's not true today. This approach is also boring.

Ultimately, your job is to make your boss's job easier, or make your boss look good to his or her boss, or both. The best way to achieve this is to implement outstanding network solutions. Taking a more active role in the company can be fun!

These days, it is important to be seen as contributing to the overall success of the company. Failure to have a solid, or even stellar, reputation puts you at risk of being on the layoff list if the company decides to have a shake-up to get rid of dead wood or has to make some tough decisions for financial reasons.

Achieving that stellar reputation doesn't require that you work long hours every night as well as work weekends. You probably need to perform only a few actions differently. Some of these actions are relevant to the early days of your employment, and the rest are ongoing suggestions. This chapter documents as many of these actions as possible. We hope that most of these suggestions will seem like old news and a few will be novel and easy to apply.

On the other hand, if you prefer the old school of thought described earlier, be sure to keep this book handy and dog-ear Chapters 14 and 15. You may need them sooner than you imagine.

Onboarding and Orientation

Every new job has a honeymoon period. Be sure to take advantage of this period of time because it happens only once with every new job.

After your boss shows you your new cubicle and issues you your computer, you must discover what you need to be successful. Now is not the time to become bashful. Ask for what you need while upper management are still patting themselves on the back for landing you as a new employee. In this section, you discover some actions a new employee should take.

You will be drinking from the proverbial fire hose at the beginning of your tenure at your new job. You have a lot of information to understand, absorb, and categorize. Trying to take it all in once can be too much, so be sure to pace yourself.

Understanding the IT department

The IT department is your new home, so you should learn what goes on here: understand your narrow responsibilities as well as the priorities of the entire department. You should

✔ **Learn the installed technology:** You may say "duh" to this suggestion. because it seems obvious. But don't be surprised if you find many subtle differences between what you were led to believe during the interview process and reality. The managers with whom you interviewed may not really know what is going on in the network.

✔ **Map out current support systems:** Before you spend all your time understanding the technology, learn how it is applied in your firm. The general accounting system, for example may or may not be similar from company to company. The other major systems, such as the billing system, the CRM system, and the ERP system, are typically customized. Learn how and why they were customized.

✔ **Look at routine reports:** The IT department produces weekly, monthly, quarterly, and annual reports for most parts of the organization. See if you can get a list of these and review them. Whatever a company tracks is what is most important to them. The information in these reports is an important clue about the priorities of your new firm.

✔ **Understand major IT initiatives:** There are several good reasons for understanding active initiatives. First, you will probably be involved in at least some of these initiatives. Next, you can gain insight into where the company is heading. Executive management should understand

that IT is typically the long lead-time factor in implementing any new initiatives. This is a fact, not a criticism. An appreciation of these initiatives and their priorities will tell you where the company is heading.

Understanding the rest of your organization

In Chapters 15 and 16, you learned what your company looks like from the outside in. Now that you're an employee, you can look at the company from the inside in.

Sometimes people do not answer questions during the interview process because the answers are confidential. Other questions are so wrapped in spin that they are meaningless. Just as you answered everything positively, so did the interviewers. Now is the time to ask the difficult questions. Seek to learn the following:

- ✔ **Learn the organizational structure:** This task includes understanding both the formal hierarchy and the informal power structure. Information on the formal structure is probably stored digitally. You'll also want to talk to coworkers to find out how things get done.

- ✔ **Understand how to get things done:** Each company has a process for moving forward with projects and initiatives. It is important you understand how this is done.

- ✔ **Understand the company's priorities:** The HR department will say that a company's people are its most important asset. The sales department will say that its customers are the company's most important asset. The finance department will say that the investors are the most important. You need to know whose computer system gets priority when there is a network or computer system failure.

- ✔ **Get to know the support staff:** Make friends with everyone, particularly the people who do not seem to have influence over your job. Getting to know these people is not difficult. Everyone has a computer at home and horror stories about getting help. Giving someone a little free advice can pay dividends in this career (and your next).

Looking and becoming competent

You looked competent when you interviewed for the position, and you should keep this appearance while you are in the learning phase and are taking more than you are contributing. Take advantage of the life-work

balance after you're making a difference. Here are some ways to show that you are committed to this company:

✔ **Arrive on time:** Actually, arrive early.

✔ **Become familiar with the company's business:** We hope you've looked at recent financial information while you were interviewing. Now is your chance to really learn about how your company competes in the market-place. Ask about the company's competitors. Ask about the company's strategy. Find out which trade shows and conferences are most important. Subscribe to relevant trade magazines, e-zines, and blogs to keep current on what is happening in the industry.

✔ **Get training:** You might feel that it is too soon to ask for training. Untrue. Take the initiative and find technical classes that will make you more productive. Don't wait for your first annual review.

Moving Forward after the Honeymoon

You have to keep the momentum going after you have the basics down and have shown that you can contribute. The goal is to make yourself seem irreplaceable.

As mentioned in the introduction to this chapter, we hope that you do most of the following suggestions already. If not, you can learn to do them. These skills are in the following categories: professional skills you can learn and master regardless of your job title; technical skills that apply to this job; and personal attributes that are relevant outside your cubicle.

Developing professional skills

The following are skills and actions that apply directly to your job:

✔ **Expand your job description:** You should have been provided a job description, outlining the basic expectations of your role. Do everything in your job description, plus something more. Be part of the team planning the summer picnic. Even better, be on the team performing an in-depth system analysis of how orders flow through the organization. Engaging with other functional areas makes you look good, expands your contacts, and makes your boss look good. However, don't overcommit.

✔ **Get your responsibilities and the responsibilities of your department more organized:** When you start a new job, you may find that everything is disorganized. This is your opportunity to organize it. Even if

your house is a total mess and your car is a disaster, find it within yourself to improve the organization of what you are doing. If you find it well organized, make it better organized. Create the vision of what an exceptionally well-organized system looks like and present that to management.

✔ **Communicate frequently and succinctly:** Now that you have things better organized, continuously remind management about how things are changing. It is important to keep this communication brief. Take notes at staff meetings and track the progress of departmental initiatives.

✔ **Get on a team:** Join the teams that are working on new IT initiatives. Many people fear "death by meetings." There is no point fighting meetings. And if you embrace it, you will be a long way ahead in making yourself irreplaceable.

✔ **Invite others to be on your team:** President Harry S. Truman made the following quote famous: "It's amazing how much can be accomplished if no one cares who gets the credit." When you are tasked with running a meeting, be sure to take this bit of advice to heart.

✔ **Work on being reliable:** A wonderful compliment to someone in a networking role is to be told that you are reliable. Of course, the network should be reliable, but you can take steps to be reliable as well. Keep your smartphone charged and with you at all times. If a call comes when you're in a meeting, find a way to communicate with the caller that you will call as soon as there is a break, and then call back. Check and answer your email even when it is inconvenient or you are tired. Let people know when you are going to be unavailable on vacations and personal days.

✔ **Take direction from your boss:** Do the tasks you are asked, even if you believe you are moving in the wrong direction. Do it even if it undoes a lot of your good work. Do it with a big smile on your face. You should have pride in your work, but you can get in trouble if you fight too much. Tactfully tell the boss that his or her direction has trade-offs. This capability is sometimes called resiliency.

Enhancing your technical skills

Of course, you'll need to keep current on technology. Most companies have a budget to keep their technical employees up-to-date on evolving technology. Stay on top of trends in your area of expertise. Do not let the following list be an afterthought:

✔ **Engage in ongoing training:** Too many of us get to our annual review and then remember that one of our tasks was to take continuing training. Do not let that happen to you. Soon after you start your job, you should be looking for training programs and making plans to attend. In

networking, as in most IT jobs, on-going training is critical to having a successful career.

✔ **Join a users' group:** It is amazing what you can learn at a users' group meeting. Your technical peers have probably encountered the issues with which you are struggling. You can get these solved at the meeting, but more importantly, you can develop contacts at other companies to help you troubleshoot problems. Also, vendors will tell you what capabilities are coming in future releases, and you then become the conduit by which your company learns about new features. You get the credit instead of the vendor's salesman. Too bad for him or her. Good for you.

✔ **Work on tasks that matter most:** Everyone has a tendency to work on projects that are intellectually interesting or that are easy and give a sense of progress. It is better to be disciplined and focus on the projects that have the most affect on business success.

✔ **Anticipate problems and propose solutions while not in a crisis:** You cannot be too paranoid. You may or may not have responsibility for backing up the system, but your goal is to avoid unwanted attention from upper management. The only question is how much your company is willing to pay for resiliency and redundancy. Remember that matter how much you prepare, you can always do more. You will do yourself and your company a favor if you try to anticipate every negative situation and have a plan.

Acquiring positive personal attributes

You've learned about professional skills and technical skills that will enhance your success on the job. In this section, we cover some personal attributes that will make you more valuable at work:

✔ **Keep home at home and work at work:** One of the interview questions proposed in Chapter 18 has to do with balancing your work and personal life. Particularly in IT, this statement is usually more aspirational than reality. This job can involve late nights and long weekends. Also, the notion that we can compartmentalize and focus exclusively on work or on home is unrealistic. In spite of these realities, do yourself a favor and minimize the discussion of personal issues at work and looking for relief from work frustrations at home. When in doubt, choose to be discreet.

✔ **Volunteer in your community:** Almost anything you do to help other people will make you a better person, which is why many companies support their employees' volunteer efforts. Expanding your humanity makes you a more complete person, on and off the job.

✔ **Avoid gossip:** Involvement with others outside your direct job role provides cohesiveness in the organization. It keeps you informed about

events in other areas that relate to your job description. Knowing what is going on is important. In this process, you will also come across stories about other coworkers. Resist the temptation to share this information with others. Gossip is corrosive. Although it provides a momentary emotional charge, it ultimately weakens relationships. Don't let it go any further.

✔ **Maintain confidentiality:** A human trait is to share news, particularly bad news or news that will endear you to other people. Limit the people with whom you share your company's bad news as well as new and exciting innovations. Loose lips sink ships. This advice applies in war and in business.

As you work in an organization, you'll meet a variety of personality types. You'll meet workaholics, who have no balance in their life; sycophants, who seem to do nothing but feed the ego of their bosses; and narcissists, who take credit for all the work, whether or not they had any involvement. On the surface, companies seem to reward this kind of behavior. The apparent rewards are typically short term: workaholics burn out, sycophants get boring, and narcissists lose trust. The people who succeed over the long run are the ones who have a passion for their work and a passion outside their work.

Part V
The Part of Tens

In this part . . .

- ✔ Know what you'll be asked in an interview.
- ✔ Know what to ask in an interview.
- ✔ Pass on a regular job.
- ✔ Find out other books (besides this one) to have handy.

Chapter 18

Ten Great Answers for Your Interviewer

Some of your interviewers will be experienced and have developed a style to elicit the information they want to make a decision about you and this role. Others are newbies and base their questions on what they think they're supposed to ask. You'll want to be ready regardless of the interviewer's experience and skill.

This chapter presents the most common interview questions with an interpretation of what underlying information the interviewer is trying to gather. This English to interview-speak translation guide should help you prepare your answers. These prepared answers will be the most effective way to communicate your message — if you can deliver them in a way that sounds spontaneous.

In Chapter 16, we cover some of the types of interview you can expect to experience. Regardless of the interview type, keep in mind that you want to knit together a story that shows that you are qualified and a good personality fit. Having responses to the questions you will likely be asked will give you the tools necessary to knit that story into the job of your dreams.

Preparing for the Unprepared

Suppose that the HR department has scheduled an interview for two busy managers. They got the email with the job description and your resume yesterday. An alert pops up on their screen that the interview is in fifteen minutes. Just before you start the interview, they print out your resume and walk into the room.

The first thing one of them says as she starts looking at your resume for the first time is, "Tell me about yourself."

Do not be offended. Use their unpreparedness as an opportunity to spin your story by going through your resume. Practice this one and remember to have a coherent theme. Don't make the following blunders:

- ✔ **Don't cover your life story.** While you're talking, the interviewers are catching up as fast as they can. If you talk too long and go into too many details, you will lose them.

- ✔ **Don't read your resume.** The interviewer is looking for deeper information about what you learned, along with a little insight into why you moved to help discern how your background is relevant to this job.

Here are some things to do when answering this question:

- ✔ **Start by telling the interviewers what you want them to remember.** In other words, start by stating the conclusion you want them to remember at the end. For example, "I am a seasoned IT professional who has used my education to prevent problems in computer networks in every job I have had. I started at. . ."

- ✔ **Focus on the qualities they requested.** The job description describes what the interviewers want. Tell them you have these skills and show them where you have applied these skills in your resume.

Whacking Softball Question Number 2

The "Tell me about yourself" question is a softball question that you can take and suit to your needs. The only limitation is the time you have and your imagination. A similar softball question that gives you the opportunity to craft a clear and concise message typically comes at the end of the interview. It goes something like, "Why should we hire you?"

If you're unprepared, this direct question can seem confrontational. If you have your answer ready, however, you can bring to light clearly and concisely what you want them to remember. When they ask you this question, you have the opportunity to lay out one last time your unique combination of skills as well as let them know that you have researched the organization.

For example, the response "I am very skilled at managing the growth of networks, which would be of great help based on the industry forecasts and your company's expectations for growth." This reply shows in one fell swoop that you have a skill that they want and why it applies to them.

This question also gives you the opportunity to work in a situation that you want to mention. Essentially, think of this question as an "insert good story here" opportunity.

Responding to the Tried-and-True Standard

The classic interview question is "What are your strengths and weaknesses?" It is as unimaginative as it is common.

Answer with three traits that relate to the job description, and then expand upon them. For example, "My strengths are that I have completed valuable training; I have significant experience in this industry; and I have exceptional listening skills." Then provide examples that demonstrate your skills.

The biggest problem that some people have describing their strengths is the tendency to be modest or to imply that you were just part of a team. Under normal circumstances, this humility is a plus. In an interview, particularly when asked this question, it is a minus. Be direct and accurate, and don't be ashamed of taking credit for work done by a team.

Discussing your weaknesses requires more thought. Ideally, you want to come up with valid weaknesses that either have no relevance to this position or are really a positive. Some examples for a networking job follow:

- ✔ **I am self-critical.** The interviewer might think this answer means that you require less supervision. Being self-critical is a win for them.

- ✔ **I dislike speaking in front of crowds.** If the position involves some public speaking, you can modify this answer to "I do not like to speak impromptu in front of crowds." Chances are that you would never be expected to do so in this role and that the interviewer feels the same.

- ✔ **I dislike staffing trade shows.** This is probably not a problem for the position unless you would be working for a company whose business is offering network services. However, you would need to have had some experience with trade shows to credibly make this claim.

- ✔ **I don't have the temperament to write application code.** This answer is another case of a weakness that is not a problem in this role. It shows self-awareness, which is a strong positive.

Usually, you need to present only a single weakness. Have a second example ready just in case.

Outlining Soft Skills

Another common question is, "How do others view you?" This question gives you the opportunity to emphasize the soft skills that you bring to the job. Technical skills can be discerned by your education, training, and certifications. This question helps the interviewer anticipate your interactions with people in the company.

You should have a few soft skills that the company considers important, as detailed in the job description, such as *loyal, a leader,* and *dependable.* To find some of elements that would make you a star employee, check out Chapter 17.

Afterwards, write down what you said. If and when the company asks you for references, it will be helpful if you can ask your references to reiterate what you told the interviewer. References are only too happy to amplify a message that you want them to convey (assuming they are the right references!).

Explaining Your Motivation

Your interviewer may ask you the basic question, "Why do you want to work here?" This is not quite a softball question because your answer depends not so much on what you say as how you say it.

Put another way, the all-wrong answer is "I need a job." The interviewer wants to hear your enthusiasm and understand how much research you've invested in understanding the company. Answering this question is easier if you understand the organization's mission.

You want to connect your attributes to the company mission. The more specific you can be, the better. For example, "I have had success in building resilient and reliable networks that would allow this organization to achieve its stated goal of uninterrupted service for clients."

Determining Whether You Are Trouble

When asked, "Have you ever disagreed with your boss? If so, how did you handle it"? the dark, underlying meaning is "Are you a psychopath and do I need to fear for my safety if I hire you?"

The interviewer wants to hear about how respectful and resilient you are and that can you take direction. Sometimes, in spite of the emotional investment you have put into your work, you have to sacrifice your hard work and do something different.

Brittle people may quit on the spot if they have a disagreement with their boss. Marshmallows, those who don't have an opinion on anything, will simply follow along with whatever the boss says. Both approaches are undesirable in American businesses. Still other people nod politely, and prepare their resume so they can exit as quickly as possible.

The ideal answer from the point of view of the boss is that you respectfully expressed your concerns and then executed what the boss wanted with professionalism. Your answer to this line of questioning should reflect this ideal.

You should have at least one story where you had a difference of opinion with your boss and the boss learned you were right, with or without a positive outcome.

If you don't have one of these stories, you may be a marshmallow. There is a place in the world for marshmallows. Be upfront with your interviewers and tell them about your willingness to accept direction from management.

Predicting Your Future

Another favorite question is, "What are your goals?" This question may be phrased as, "Where do you see yourself in five years?" or "What do you see as your next job?"

What the interviewer wants to know is whether you have ambition, drive, and planning. Employers seek employees who are results oriented and know what they want.

These goals should not be self-serving. For example, "I want to earn enough money to buy a new Dodge Charger" does not inspire the interviewer to think about how well you fit in — even if the interviewer, too, would like a Dodge Charger.

You also don't want to make your goals too aggressive. Say something like "My first goal is to contribute to the success of the organization and company. I would certainly like the opportunity to grow technically and professionally with the company." If you have a specific position in mind as a goal, such as CIO, you might add something like, "and someday, I would even like to become a CIO-level executive." Employers typically don't want to hire people who come in the door looking too far past the job at hand.

Tie your career goals with the mission of the company. It also helps if you throw in a goal that is not a part of your professional life.

Not Looking like a Job Jumper

One concern companies have for technology employees is that they will come in, get all kinds of training, and then shop around for a job with a higher salary. This concern underlies the interview question, "Why do you want to leave your current job?"

You may be shopping around simply to get more money, but this should never be part of your answer. Make your answer pertain to personal and professional growth. Almost any other answer will send up a red flag.

If you indicate that you want more money, you play into the fear that you will become a serial job jumper. If you mention frustration with decision making, you come across as brittle. If you mention that your current employer has financial difficulties, you are sharing confidential information.

Talk about your aspirations to contribute to a company that is on a positive trajectory in an industry in which you have a sincere interest. Almost any other response is risky.

Describing Team Leadership Skills

We have all had the following experience. You're on a team and someone is not doing his or her share of the work. How you handle this situation is important. How you answer the questions, "Have you been on a team where someone was not pulling his or her weight? If so, what did you do about it?" is also important.

The ideal answer is that you focused on the task and worked with the team leader to make up the slack. Other scenarios are complicated. If you pulled aside and "worked" with the slacker, you might look like a bully or like you overstepped your role. You may have been unaware of the steps the team leader took with the slacker.

Another option is to say that you stepped up and organized the tasks and kept track of assignments and progress — with the consent of the team leader.

Note that this question typically asks if you are part of a team but not the team leader. If the question is asked with the assumption that you are the team leader, your response should be different. The team leader has responsibility for tracking objectives and sharing progress with management.

This tracking requires ongoing and consistent communication, which is a good habit to share with the interviewer.

Defusing the Financial Land Mine

The saying in price negotiations is that whoever mentions a price first loses. That is why interviewers often like to ask the question, "What are your salary requirements?"

This question is a good sign. If they weren't interested in you and were counting the minutes until you walked out the door, they would not ask this question. Instead, they like you enough to hear what you have to say and find out if you're in the salary range.

You can handle this question in a few ways. You could answer the question directly if you know where you stand. This approach works only if you have done your research and know the company's salary strategy.

A *salary strategy* is the general tendency of the firm to set salary ranges. Some firms like to pay a small premium above the going rate to keep employees. Others pay less, with the promise of an opportunity to get in the door and gain some experience. You can get a sense of the firm's approach on www.glassdoor.com.

Another approach is to tell them your current salary and that you are looking for an increase from 5 to 10 percent. An amount more than 10 percent will make you look greedy and unrealistic.

Note that you can pad your current income a little, but not too much. It is highly unlikely that the prospective employer could find your exact salary.

Finally, if you want to maximize your potential salary, avoid giving a number and indicate that you are open to a fair offer for the position with consideration for your experience and goals. Signal that the equation includes taking into consideration benefits and bonus opportunities. If pressed, you may try to say something like, "My last job was not indicative of a salary for this role." However, you have to be careful because you don't want to come across as disrespectful. A good compromise answer when pressed may be, "In my current role, I am making X. But considering the responsibilities in this role, I would like to be able to move forward with my compensation."

Every situation is different. You have to be prepared and be ready to think on your feet.

Chapter 19

Ten Great Questions to Ask Your Interviewer

· ·

· ·

Congratulations! You've just completed a grueling interview in which you answered some of the most probing and thought-provoking questions about yourself that anyone has ever asked. But your answer to one final, seemingly innocuous question could blow it all

Interviewer: "Do you have any questions for me?"

You: "Uh, no. I believe you've answered any questions. Thank you."

At best, this answer is a polite way to end the interview. At worst (and more likely), this answer may be construed as a cop out that demonstrates a lack of intellectual curiosity, preparation, and interest in the company or the job!

Always be prepared with a few questions to ask at the end of the interview. It's likely that the interviewer may have answered many of your questions

during the interview without you even having to ask them. And ideally, you've had several opportunities to ask questions and engage in meaningful dialogue during the interview. This chapter provides ten questions you might want ask.

> **TIP** You should always go into an interview with at least five or six questions written down. Be prepared to ask these questions during and at the end of the interview.

How Has Your Department Contributed to the Success of the Company?

You should include specific details about the company when you ask, "How has your department contributed to the success of the company?" Your goal is to show the interviewer that you researched the company. This question is also a great way to showcase your business acumen and demonstrate your understanding of what the company does. Far too many IT professionals get caught up in the cool technology and forget that IT supports the business — not the other way around (unless you happen to be applying for a job at an IT company)!

> **TIP** Everyone applying for the job will have some level of knowledge and experience in IT. Make yourself stand out as a candidate by demonstrating a keen understanding of the company's core business.

If the company is publicly traded, their annual 10-K Securities and Exchange Commission (SEC) shareholders report is available on the company's website. This report contains a wealth of information about who's who in the company, the overall strategic direction, and detailed financial data. Let the interviewer know that you've studied this report by asking questions that begin along the lines of "I see in your latest 10-K filing that the company's price-to-earnings ratio has increased to 28 times earnings over the past three quarters."

Getting information about private companies is more difficult because these companies tend to keep their financial performance data, well, private. However, you can still get a wealth of information from the company's website, press releases, and other sources. Both public and private companies love to tout their successes in the local media. Look for news interviews with company officers in local business journals and special interest stories such as a charitable cause the company supports, a recent community outreach project, a new diversity initiative, or a recent expansion or new client that the company is excited to talk or write about.

Complete your question by asking how the interviewer's department or team has contributed to that success. People usually enjoy talking about their accomplishments, so this question should lead to an engaging discussion and will also give you some insight on your potential new boss. Does the person speak with humility and downplay the team's contributions? Or does he or she burst with pride while offering specific examples and calling attention to key individuals on the team? After the interviewer answers this question, make it personal by explaining how you would help the team continue to succeed and contribute to the company's success.

Do your homework! If the company has had some recent struggles or setbacks, you don't want to ask about their recent success! In such cases, you may not want to ask this type of question at all.

What Are Some of the Biggest Challenges Your Department Is Facing?

To learn more about the company overall and some of the specific projects you may be working on if you get hired, ask "What are some of the biggest challenges your department is facing?" Your interviewer may not be comfortable giving you specifics, but you can still glean a lot of information from the answers you do get.

For example, your interviewer is unlikely to tell you "We're really short-handed since a lot of people have quit because of the long hours we work." But you might gain some helpful insight from an answer such as "We've had some turnover recently."

And it's unlikely that you'll hear, "Well, we've been behind the eight ball since that huge security breach last month, so we're scrambling to shore up the network infrastructure." But you might learn about a new initiative to build out a hybrid cloud infrastructure and that the executive team has concerns around security in the public cloud. There's your opportunity to talk about how your experience at your last company can help them address those challenges!

The answers to this question may also give you some idea of how urgently the company needs to fill the position and could strengthen your negotiating position when you get the job offer!

How Would You Describe the Company's Culture ?

Cultural fit is at least as important as your skills and experience. If your personality isn't in sync and your values aren't aligned with the company, you don't want the job. Period. You won't be happy, your new employer won't be happy, and you'll inevitably part ways on terms that leave neither of you happy.

Some people thrive in large organizations; others prefer a small company. Some people enjoy working in a loud, chaotic environment. Others prefer order and solitude. Some people need clear direction; others need autonomy. Understand who you are and what values are most important to you.

Listen carefully to your interviewer's answer to the question, "How would you describe the company's culture?" The answer will give you an idea of how happy people are working for the company. Does the interviewer describe the culture with passion and enthusiasm? Do you get specific examples? Does the interviewer explain how the culture affects him or her personally? Or does the person just recite the company's mission and values statement? It's hard to be passionate about a company's culture if the truth is that your interviewer can't stand his or her job and dreads coming to work every day. If that's the case, do you really want to work there?

Ask open-ended questions that enable follow-on questions and further discussion. After the interviewer answers your question, thank him or her and continue by explaining how you fit in or can contribute to the company based on the answer. For example, "Thank you for giving me that insight into your company's culture. Cultural fit is very important. XYZ company has a similar culture and when I worked there I believe I was an integral part of that culture because . . ."

What Do You Like About Working Here?

If you want to know what you might find rewarding about the job, ask "What do you like about working here?" You want to get answers at different levels, so that you can get several perspectives.

Next, you want to find out about the organization as a whole. Are people proud to be working there? The mood and the tone in the organization will affect you. Again, if people are unhappy, you'll hear this more in what they don't say than in what they do say.

If everyone is all smiles, you may have found the ideal organization where everyone is happy, or maybe they're putting happy dust in the coffee every morning. Somehow, you'll want to get to the bottom of everyone's bliss if it feels superficial.

Can You Describe How We Would Be Working Together?

Because a large part of your work satisfaction depends on your relationship with your boss, you need to ask, "Can you describe how we would be working together?"

There is no good or bad answer, because individual work habits drive how people work by themselves and with each other. However, you need to be able to determine whether you will find your manager's style compatible. You want the working relationship to be harmonious from day one.

There may be better ways to ask this question, such as:

- ✔ "What sort of daily, weekly, or monthly status reporting will you require of me?"
- ✔ "How much freedom will I have in the regular tasks that I'll be expected to perform?"

What Is the Makeup of the Team or Organization?

If someone hasn't already described the team's makeup, you might ask, "What is the makeup of the team or organization?" You are not looking for actual names, but instead you're trying to understand how the team or organization is structured.

You can ask about the position titles for others on the team, and to understand what their responsibilities are. Chances are you will be working closely with most of them, and that you'll be asked to fill in for some of them while they are out sick or on vacation. In fact, asking more about the entire team is another good line of questioning that will tell you more about team dynamics.

What Are the Key Traits of Your Most Successful Employees?

By asking, "What are the key traits of your most successful employees?" you're asking about the traits the interviewer is looking for in you.

Expend some effort interpreting the answers you get to this question. The interviewer might be telling you what is expected of everyone on the team and, if so, his or her answer might reflect a team dynamic or insight into the company's definition of success.

TIP

If you can, find out whether the company has published a set of guiding principles. If you're lucky, they'll be framed and hanging on the wall in the conference room where you're being interviewed. See whether or not interviewers describe traits straight from the guiding principles.

Interviewers might be telling you about the successful employees on the team and how they got that way. That may, or may not, mean that you need to have those same traits. But as team dynamics go, you might have different traits that could help the team be even more successful. Often, a diversity of skills makes a team more successful than a team in which everyone has the same strengths and weaknesses. Ask a follow-up question or two to see which is the case, such as, "What kind of skills would most enhance the performance of your team?"

How Would You Define Success During the First 90 Days?

The question "How would you define success during the first 90 days?" will tell you a lot about the level of maturity and organization in the team you're considering joining. If the team (or the hiring manager) is not well organized, they might not have a good answer for this question. They may be frantically working to put out fires with no time for even short-term planning; they just need another set of hands to pass buckets of water along the bucket brigade! If this is the case, think long and hard about whether this is the kind of position you want. Perhaps the company is looking to hire someone to replace one or more burnouts. Or maybe they want help to move the organization to the next level, which would be an extraordinary opportunity.

If you interview with a more organized team (or manager), they will be more likely to know what success looks like. And you'll have an idea of what will be expected of you in the first few months.

Honestly assess whether you are up to the job (or *almost* up to the job). Ask any follow-up questions, such as what resources will be available to you right away. Discuss tools that are available as well as the company's plans for future tools and technology.

Just as the company will put new hires on a 90-day probation, you should do the same with your employer. After 90 days, reassess whether this is the company you thought you were joining and whether they have met or exceeded your expectations.

Do You Have Any Concerns About Me That I Can Address Now?

You'll want to appear as the ideal, near-perfect candidate to your interviewers. But every employee has some imperfection, large or small. It takes a bit of courage to ask, "Do you have any concerns about me that I can address now?" The interviewer may answer with a gap in your skills or knowledge that is a shortcoming.

Do not despair and keep your good attitude. Consider the interviewer's point of view and tell him that you agree with his observation. If you can do so realistically, tell the interviewer what, if anything, you can do about the shortcoming. Every candidate has shortcomings, and the company may be willing to take you as-is.

What Is Your Next Step in the Selection Process?

"What is your next step in the selection process?" is a great question at the end of the interview. The answer helps clarify the next steps to expect, such as when and how you should follow up with the interviewer, whether or not there will be additional interviews (perhaps with human resources or other team members), and how long you should expect to wait before a hiring decision is made. Following are some variations of this question:

✔ "When should I expect to hear from you?"

✔ "When and how should I follow up with you?"

✔ "How soon do you expect to make a hiring decision?"

Be specific during your follow-up at the end of the interview. After asking, "When can I expect to hear from you?" follow up with "If I haven't heard from you by that date, may I follow up on [date]?"

After the interviewer answers this question, be sure to thank her for her answer and for taking the time to meet with you. Then restate the next steps so the interviewer knows that you understand her answer and knows what to expect from you. Finally, and most importantly, close with a crisp summary statement that asserts your enthusiasm for the position and the value you will bring to the table! If you are truly enthusiastic about the position and want the job, let the interviewer know. "I am excited about the opportunity to work at Dewey, Cheatham, and Howe and look forward to hearing from you soon."

The answer to this question may also provide insight into how well you did in the interview. For example, the interviewer may tell you she'd like to go ahead and schedule you to meet the rest of her team. A vague answer, such as "Well, we still have several other candidates to interview but we'll be in touch" might indicate some concerns or a lack of interest in you as a candidate.

Chapter 20

Ten Alternatives to a Regular Job

*M*aybe you've made your fortune and want to give back to society. Or perhaps you are a ne'er-do-well and live off the generosity of others. In either case or anything in between, let's say you want to use your networking skills for something other than a regular job. Hey, this is America. You are free to do what you want. This chapter lists a number of options, ten as a matter of fact, for working in networking while avoiding that troublesome regular paycheck.

Homing In on Your Home

A good place to start is where you hang your hat. Many homes have multiple PCs along with game consoles and smart televisions. And don't forget the smartphones that can connect to the Internet through Wi-Fi.

Many modern operating systems automatically whip up a network when they see each other sharing the same Wi-Fi. This is a start, but it barely constitutes a useful network. The locally connected PCs can't share files and back

up data. This is the computer equivalent of having a party where no one talks to each other and everyone is texting on their phone.

Companies have attempted to market home servers. For example, Microsoft produced Windows Home Server, but they later withdrew support for it. In lieu of a central server, any PC on the LAN can act in this role. The two main considerations when optimizing a network in the home are establishing file-sharing relationships with other devices, including PCs, game consoles, and smartphones, and ensuring adequate capacity on the LAN.

Regular old Ethernet is frequently the default speed of many home networks. It may be as simple as updating a router to get Fast Ethernet or Gigabit Ethernet in your home network. Simple changes such as this suddenly make sharing photo and video libraries on the home LAN convenient.

Becoming a Good Neighbor

Bringing a batch of cookies to the new neighbors is a great way to build community. It is also old school. Offering to help the new neighbors with their home network is a more modern way of making friends.

Admittedly, this type of neighborly gesture is a little unconventional. Also, the new people might be a bit concerned about your intentions. It would make most sense to stick with helping them with the hardware but sit with them and let them work up the software settings to connect. Be sure to steer clear of their passwords!

Consulting in Your Community

You have your house in order and, having helped your neighbors with their home networks, they now think you're a hero. The next step is to reread the section in Chapter 17 that talks about how important it is for you as a person to be involved in your community. The intent here is to get you out of the day-to-day rut about your job. At the same time, chances are that organizations in your community have computer networks. And computer networks are improved when people with different perspectives look at how they are put together.

Consider consulting with the person who runs the network at your place of worship, school, or social organization to understand the design and network goals. You can then offer advice and suggestions.

Engaging in Politics

Chances are, some political cause captures your imagination. Political efforts, both campaigns for individual office and ballot initiatives, often need to whip up a large network from scratch and then disassemble it after the election. This kind of opportunity is a great way to exercise some of your skills in a relatively forgiving environment.

Closing the Digital Divide

Here is yet another noble cause. This one, however, leverages your technical skills more than your networking knowledge. Organizations exist that accept obsolete computers, refurbish them, and then donate them to worthy individuals and causes. The PCs aren't up to snuff for you and me, but they can be a blessing to someone who has nothing.

This process also keeps electrical components out of the landfill. The US Environmental Protection Agency (EPA) estimates that only 15 to 20 percent of home PCs are properly disposed of. It is better to reuse than recycle.

If this suggestion resonates with you, you'll have to do a little bit of research. Some states mandate that electronic waste be recycled through official electronic recyclers. In states with less formal guidelines, many retailers take the initiative and offer their customers an opportunity to recycle their old technology. In other states, nothing stops you from dumping your toxic PC in the lake (which is a bad idea).

Use your favorite search engine and search the terms *PC, recycle, charity*. You may find Eagle Scout projects doing this kind of work, organizations that hold build-ins and are seeking volunteers with your skills, or organizations that have the components and tools and would let you and your technical buddies use recycled components to build new PCs.

Bartering Your Services

Enough with saving the world. Let's get back to thinking about numero uno for a moment. Your networking skills are valuable, but this does not always necessitate the exchange of cash.

Trade your services building and setting up a network for someone else's services. The direct approach is to trade hour for hour. It may be easier,

however, to trade task for task. For example, you will set up a network in your family lawyer's office if the lawyer will write your will. One issue is that an hour of networking time may or may not correspond in value to an hour of the other person's time. If you use, say, $100 per hour for networking services, you'll have a starting place for discussions.

The key to success when bartering is to be flexible in your negotiations.

Bartering for physical things is more complicated because often a discrete value is placed on a product while the value of a service is more arbitrary. The same principles of flexibility apply when negotiating for physical things.

Inspiring Others

After you have some experience, you have something valuable. You can sell your experience as a service. You can trade it for items of value. You can also teach others the lessons you have learned. As mentioned throughout this book, the demand for networking professionals is significant and growing. Other people can learn from your experiences.

Lots of people want to learn how to get more out of their network. You could put together a training program for small groups and teach them how to improve their home networks. You could become an instructor at a community college and teach networking. You could get your teaching certificate and teach technology in the public schools.

The only universal requirement when teaching networking is that you have to swear allegiance to the ISO 7-layer communications model. This model is an unwritten requirement (or rather, it was unwritten until I wrote it here).

Enabling Users Groups

You can find a range of users groups. At the lavish end are extravagant soi-rées at high-end resorts put on by manufacturers for their leading customers. The manufacturers roll out new products and collect user comments. A more modest example of a user group involves a few folks who get together over lunch at a local park and discuss tips and techniques that make their common technology work a little better.

The term *user group* can apply whenever a few people get together, in real life or online, to share experience of a common technology. It would be great to

be invited to the lavish type of user group, but these are typically reserved for paying or prospective customers.

Chances are, are other networking professionals could use your perspective and experience. These others could be local or regional. Often it is most convenient to start one of these user groups before or after another meeting that is associated. For example, people involved in police and fire dispatching often have meetings to discuss tips and techniques. This kind of collaboration helps ensure interagency cooperation. A part of these conferences involves the unique technology used by police and fire. Some of the technical users took it upon themselves to have a technology users group to figure out better ways to interoperate for large crises. This was not the initial role of the local convention, but it certainly was a good outcome.

Nothing says you have to be actively employed in a particular area to be a part of a users group. You just have to have an interest. Out of these formal and informal users groups, important information is shared and new products are developed.

Contributing to Open Source

The previous section talked about user groups associated with a particular technology. These groups are typically associated with particular hardware or software product, but may also be involved in a class of products or a type of application. Other efforts in the high-technology community involve the pursuit of a utopian environment where individuals contribute technical skills for the benefit of all. This model is generically called *open source* and is an extension of the free software movement.

Here is where you come in. If you like this idea, you can help. Your particular skill might focus on networking applications or utilities. Go to the Google Play Store and search for *network tools.* You'll find a long list of free applications that help network managers, ranked by users and rated by their effectiveness.

If you are so smart, which you are, and want to contribute, here is a convenient place to donate your skills. Your success is measured by the number of downloads and the rankings you receive. You perform this work in lieu of compensation, but this type of work can be rewarding if your application is popular.

Mentoring Up-and-Coming Networkers

Most of the alternatives proposed in this chapter focus on networking on the technical side. Another important side of networking is working with individuals. Successfully helping other people with their careers can offer you the greatest satisfaction.

After you have established your reputation, you're in a position to help other people develop theirs. The technology with which we work in networking is rapidly changing, and younger people need help in skills, connections, and insight that an older individual can provide.

You don't need to be an elder to be a mentor. You do need to have the maturity to recognize that personal relationships are the glue that help make things work better, from solving small problems to achieving world-changing results.

Chapter 21

Ten Networking Books for Your Professional Library

*T*he information in Chapter 7 is a good start for providing information on networking, but it will not solve every problem under every circumstance. In this chapter, we list ten good books that will provide lots of good information to get you through the day.

Knowing Your Way around a PC

The first book on the list, which is shown in Figure 21-1, is *CompTIA A+ Certification All-in-One For Dummies,* 3rd Edition by Glen Clarke and Edward Tetz.

"Come on," you say. "I'll be working with networks. I'll never get my fingernails dirty on the inside of a mere PC. I read Chapter 5, and know the CompTIA A+ Certification is for computer repair technicians. You can't fool me!"
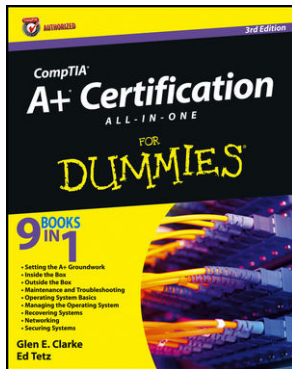
Figure 21-1:
Understand
PCs.

I'm sorry to be the one to tell you, but there is no company so big or so specialized that there will not be a time when you'll need to crack open a PC case during a critical upgrade or for some other failure. Having a book that incorporates the best practices for working with the PC is handy. Accept your fate and be prepared for when you are pressed into service in an emergency by becoming familiar with this book.

Building Your Network

Let's make sure that you have a comprehensive view of your network. What better way for a devoted *Dummies* reader than to read *Networking For Dummies,* 10th Edition by Doug Lowe? The cover is shown in Figure 21-2.
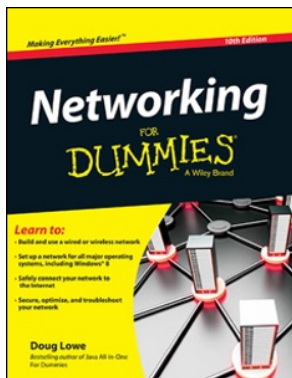
Figure 21-2:
Learn the
ins and outs
of building a
network.

We don't get a commission for *Dummies* books we reference. We do, however, want to make sure that you're successful in your job, and this book gives you an overall perspective of making a functioning and successful data network successful.

Visualizing the TCP/IP Protocol

Enough with the *Dummies* books for a while. They are great, and we know that you love the format, but other publishers have useful information too.

The next books in your library should be the *TCP/IP Illustrated* trilogy. The three titles are *TCP/IP Illustrated, Volume 1: The Protocols,* 2nd Edition by Kevin Fall and W. Richard Stevens; *TCP/IP Illustrated: The Implementation, Vol. 2* by Gary R. Wright and W. Richard Stevens; and *TCP/IP Illustrated, Vol. 3: TCP for Transactions, HTTP, NNTP, and the UNIX Domain Protocols* by W. Richard Stevens.

TCP/IP is so pervasive and important that you'll need to know it intimately to be effective in networking. This series will help you understand the TCIP/IP protocol at a fundamental level.

Getting Serious with Cisco Routing

The next book on your shelf should be *CCNA Routing and Switching Portable Command Guide,* 3rd Edition by Scott Empson. Now we're getting serious. The previous books have large print and lots of nice pictures. This book from Cisco serves as a reference for working with Cisco hardware.

You can't be expected to remember all the commands for Cisco routers. Use this book as a reference for finding what you need to get Cisco hardware to behave the way you want.

"Hold on," you say. "I can't simply pick up a book of commands and start programming a Cisco server." True, but you have to start somewhere. This book is a handy reference guide, not a replacement for proper training on Cisco hardware.

Remembering Juniper Networks

We recommend that you add the following title to your bookshelf: *Juniper Networks Reference Guide: JUNOS Routing, Configuration, and Architecture* by Thomas Thomas II (seriously, this is his name), Doris Pavlichek, Lawrence Dwyer III, Rajah Chowbay, Wayne Downing III, and James Sonderegger.

This reference guide for Juniper Networks routers has information about commands, configuration, and architecture. This book is valuable if you work in a Juniper Networks shop or a mixed environment. No system is an island, particularly on the Internet. If your network is having trouble with another organization, it is helpful to have some perspective when that other organization begins describing their troubleshooting.

Opening Up to Linux

The next book we recommend is *Linux Administration: A Beginner's Guide,* 6th Edition by Wale Soyinka. Chances are that you'll have at least some Linux equipment in your network. Certainly you'll connect to networks that have Linux equipment. You don't need to be an expert on day-to-day Linux administration, but when you start getting unexpected results, it is important to have a reference guide handy.

Closing Up Network Access with Security

Many things can go wrong on a network. Links can fail. Servers can fail. Backup systems can get lost. There's nothing like an intrusion to ruin your day.

The next book covers a topic that everyone involved with networks should be well versed in: security. Your job title might not include the word *security,* but you should be thinking about it in everything you do. We recommend *Computer Security: Principles and Practice,* 3rd Edition by William Stallings and Lawrie Brown.

Beating a Dead Horse

We may be beating a dead horse about the importance of security, but here is another book for your shelf: *CISSP Guide to Security Essentials,* 2nd Edition by Peter H. Gregory.

Nothing will impress the boss more than picking up this book, implementing its advice, and earning your CISSP certification from the International Information Systems Security Certification Consortium (ISC)[2].

Going Mobile

There are enough similarities with wireless and wireline services to lull us all into a false sense of serenity. The reality, however, is that wireless broadband brings a new dimension to network management and security, and you have to be on top of it.

Fundamentals of Wireless Communication by David Tse and Pramod Viswanath describes wireless LANs, Bluetooth-connected devices, in-vehicle devices, laptops, smartphones, and the Internet of Things (IoT), which involves every company asset that isn't nailed down.

Floating in the Cloud

Wireless technologies have a long and storied history of not performing as they are supposed to. Keep this book handy to help keep things working as they should.

Speaking of connecting to everything that isn't nailed down, the cloud resists being nailed down. Because of the cloud, inpatient department heads outside IT can implement data solutions without having to involve the IT department — until they need help, at which point it becomes your job to integrate sensitive infrastructure with the cloud network.

Taken to the logical extreme, the amorphous and ambiguous cloud allows entire companies to begin from scratch and implement enterprise-wide solutions. Starting from scratch can be a great opportunity, but the project then becomes your management nightmare.

The way to get ahead of the curve is to do your homework on cloud implementations by reading *Cloud Computing: Concepts, Technology & Architecture* by Thomas Erl, Ricardo Puttini, and Zaigham.

Cloud computing is evolving in the marketplace at a fast pace. Having an appreciation of the architecture is essential for keeping your current environment humming along.

Glossary

· ·

access point (AP): The radio transmitter/receiver for Wi-Fi systems. See Hot Spot.

acknowledgment (ACK): The occasional message sent from one device to another in a network to ensure that all elements are ready should a user request come in.

active hub: A networking device that amplifies signals on a LAN.

actual throughput: A measure of useful customer data bits delivered per unit of time. Affected by real-world conditions such as electromagnetic interference, overhead associated with routing information and error correction, and latency in switches and the network in general. See also *nominal throughput*.

alarm: A message notifying a network operator or administrator of some kind of problem. May also be called an *event* or a *trap*.

algorithm: The set of rules or procedures to follow in a specific circumstance.

American National Standards Institute (ANSI): A group that sets national standards within the United States.

applicant-tracking system: An information system used to accept, manage, and screen resumes and cover letters from employment candidates.

application development tools: Tools that enable application developers to manage revisions and collaborate with other developers.

application program (app): Software that is intended to achieve some useful purpose for the user.

architecture: The complete set of specifications, protocols, and topology of a particular network.

asynchronous transfer mode (ATM): A broadband transmission service with network speeds up to 2.2 GBPS.

attenuation: A loss in signal strength due to problems in the cable or interference.

availability: A condition in which computer services are available to users.

backup: The process of making copies of sensitive data.

benchmarking: A management process in which a company compares its capabilities to the best practices of others.

Bluetooth: A wireless protocol for data transmission using devices in close proximity.

bottleneck: In this context, the bottleneck is the primary factor in the design of a system that limits its overall throughput. See also *systems design*.

bring your own device (BYOD): Some organizations may allow employees to access company resources through mobile devices, such as laptops, smartphones, and tablets. This is in contrast to others that consider allowing access of personal devices to be a support challenge or a security threat.

broadband: A communications service that provides more bandwidth than a single voice line of 56 kb per second, also known as a DS0.

bus: The component in a computer where data and instructions flow between and among the CPU, main storage, and secondary storage, and externally through peripheral devices and communications adaptors.

business continuity planning (BCP): Activities that facilitate the capability of an organization to continue business operations using alternate facilities, equipment, or personnel in a disaster scenario.

business intelligence (BI): A suite of applications that enable marketing and business managers to examine sales and customer service data to discern important trends among customer behavior as well as financial objectives.

call center solutions: Customer support services such as a call distribution system to spread incoming calls among available call takers, access to the CRM system, and tools to track the performance of call takers, who are responding to voice calls, chats, and emails from existing and prospective customers.

capacity utilization: A measure of actual usage compared to total available resources. (Getting close to 100 percent capacity utilization is rarely a good thing in networking. See *congestion*.)

carrier: A company that provides telecommunications services or an electromagnetic wave of a single frequency used as a data-bearing signal.

CAT-5 cable: Copper cabling capable of transmitting Ethernet at speeds up to 100Mbps.

CAT-6 cable: Copper cabling capable of transmitting Ethernet at speeds up to 10Gbps.

central processing unit (CPU): The component in a computer where computer instructions are executed and calculations are performed.

certificate authority (CA): A trusted party that issues digital certificates to other parties after confirming their identity.

certification: The process of examining a system to determine its compliance to a set of requirements with the goal of demonstrating competence in a particular technology or skill.

change management: An IT operations process that is concerned with the management and control of changes made in IT systems.

circuit switching: A method of communication involving a dialed-up connection, typically used for temporary connections.

class of service (COS): The priority assigned to a user or an application to be used when multiple entities want to use the same resources.

client-server: An application architecture in which some of the application resides on a workstation (usually having to do with data display and data input), and some resides on a central server (usually having to do with data storage and retrieval).

cloud computing: The practice of utilizing remote resources for the processing or storage or both of information.

Code Division Multiple Access (CDMA): A protocol for cellular voice and data communications. In the United States, the cellular carriers Verizon, Sprint, and US Cellular use this technology on their respective wireless networks.

collaboration tools: Applications that simplify the interactions among employees. The core of many of these tools is document preparation, where the application tracks revision changes made by multiple contributors. This revision control system is supplemented with ad hoc workgroups and voice and videoconferencing in support of this effort.

Committee of Sponsoring Organizations of the Treadway Commission (COSO): An IT controls framework that is applied to financial systems.

common criteria (CC): A framework for the specification, implementation, and evaluation of a system against a set of security requirements.

competitive local exchange carrier (CLEC): Telecommunications carriers who put in equipment to allow them to compete with the established local phone company.

compiler: A program that converts a program in source code form into machine-readable form.

computer-aided design and drafting (CADD): Design engineers create product concepts in a digital format that can be tested and stored entirely on computer systems.

computer-aided engineering (CAE): Engineers can work with digital designs to perform prototype creation, destructive testing simulation, heat transfer, verification of electrical design, and other engineering tests that formerly needed to be done with physical samples.

computer-aided manufacturing (CAM): Modern manufacturing equipment and process control systems provide status information to a central site to allow for monitoring and control.

computer-integrated manufacturing (CIM): See *computer-aided manufacturing*.

configuration management (CM): Computers and network equipment on a network are regularly added, changed, or deleted. Configuration management tools keep track of what and who is on the network and what they are authorized to access.

congestion: Occurs when too many users want to send and receive more data than the network elements can handle.

connectionless: A semipermanent connection to a packet-switched network, such as the Internet, as opposed to a dial-up connection.

connectivity: The capability to establish some kind of connection to a circuit-switched or packet-switched network.

connector: The physical end of a cable used to make a connection to equipment that is logically residing on the network.

console: A computer and screen that presents a network administrator with the instantaneous performance of the elements on the network and the configuration management tools.

consulting: A business activity in which an expert party issues advice or guidance to another party.

contention: When multiple elements in a network want to use the same resource simultaneously. Networking equipment uses algorithms to manage contention.

continuous operations: Many networks have off-peak times when network managers can make configuration changes with no or minimal effect on users. If no suitable off-peak times are available, the network must operate in this mode.

Control Objectives for Information and Related Technology (COBIT): A control framework for business processes related to information technology (IT).

control: Any specific instance of a policy, standard, or key step in a business process or procedure that management has determined is essential for the proper operation and security of business processes and information systems.

convergence: A network that carriers digitized voice, computer data, and digitized video. Earlier network designs involved separate cabling for each kind of communication.

cookie: An identifier sent from a website and stored in a browser.

core router: An intelligent and reliable router used by telecommunication carriers to switch TCP/IP packets.

cover letter: A personalized letter sent to a prospective employer, containing a description of qualifications as they relate to the posted job description.

creative tools: Applications that produce videos and audio recordings, marketing documents, and other visuals. These run on general-purpose or specialized computers.

curriculum vitae (CV): A complete listing of employment positions, education, publications, and so forth. See also *resume*.

customer communications management (CCM): Applications that automate and control digital communications, such as emails and digital agreement, with different customers.

customer information management (CIM): Applications that track the buying history of specific customers.

customer relationship management (CRM): A class of applications that combine the information associated with customer communications management and customer information management to provide a single source of information about customers and prospective customers.

cutover test: A test of business continuity plans in which production systems are shut down or disconnected, and recovery systems are activated to manage live workload.

cyclical redundancy check (CRC): A technique to verify the accuracy of a data packet.

daisy chain: A LAN network topology in which computers and other elements are connected to each other in a series of rings.

dark fiber: Unused optical fiber that is available for voice or data communications.

dashboard: Similar to a car's dashboard, an image displaying the health of the network.

data center: The place where delicate computer hardware, including network equipment, database appliances, and application servers, are housed. The environment is secure and temperature controlled.

Data Over Cable Service Interface Specification (DOCSIS): A family of technologies used to transport TCP/IP over cable television service.

data retention: The process of defining minimum and maximum intervals for the retention of different types of information.

data warehouse: The logical repository of user information and application data.

database appliances: The hardware in which databases that make up the data warehouse are stored.

database management system (DBMS): A software program used to facilitate the storage and retrieval of information from a database.

database: A structured collection of information.

dedicated LAN: Some networks have one LAN for general purposes and another parallel LAN to serve a specific purpose or application. This second LAN is dedicated to that purpose for throughput or security reasons.

denial of service (DoS): An attack on a target system designed to incapacitate the system.

Department of Defense Information Assurance Certification and Accreditation (DIACAP): A process framework used to certify and accredit military systems.

digital certificate: An electronic document that consists of a personal or corporate identifier and a public encryption key and is signed by a certificate authority (CA).

digital signature: The result of a hashing operation carried out on a file that is used to verify the integrity of the file.

digital subscriber line (DSL): A family of protocols delivered over copper telephone network cabling to homes and businesses.

digital video recorder (DVR): A device that records images from one or more video surveillance cameras.

Director of Central Intelligence Directive (DCID 6/3): A framework used to certify and accredit systems in use by the Central Intelligence Agency (CIA).

disaster recovery planning (DRP): Activities that facilitate the salvage of facilities and equipment in a disaster.

disaster: An unexpected event that directly or indirectly disrupts ongoing business operations.

discretionary access control: A security model in which the owners of individual documents or folders manage access to information.

distributed antenna system (DAS): This solution provides coverage in areas that otherwise would have poor service by installing special antenna remotely from the main cell site.

distributed application: An application architecture consisting of several components residing on different systems.

distributed computing: When individual servers store and manipulate data, potentially at multiple locations. This approach is in contrast to centralized computing, in which all processing and data are in one location.

distributed denial of service (DDoS): A denial of service (DoS) attack originating from many points.

document management (DM): A single application that tracks all documents, sent externally and used internally, in a single repository. Such applications are used for archiving, but can also support collaboration among employees in in an organization.

DS-0: A telecommunications service with 64Kbps, which is the logical equivalent of a single phone line.

DS-1: A family of multiplexed telecommunications technologies that have carried voice and data for decades in the United States and are logically comprised of 24 DS-0 circuits for a total of 1.2 Mbps. Also called *T-1*.

E-1: The European version of a DS-1, E-1 is comprised of 30 DS-0 circuits for a total of 2 Mbps.

electric generator: A device powered by gasoline, diesel fuel, natural gas, or propane that can generate electric power for hours, days, or more.

electromagnetic interference (EMI): The major source of noise on a line. It can come from a variety of sources, such as improperly grounded equipment or frayed cables.

Electronic Protected Health Information (EPHI): Information related to the health and medical care of an individual.

enterprise class: Networking equipment built with the quality to operate in an enterprise. Consumer-class equipment is less reliable and less costly, and carrier-class equipment is more reliable and more costly.

enterprise network: A network set up for the private use of an organization to achieve the company's objectives by providing employees access to enterprise applications.

enterprise requirements planning (ERP): Applications that integrate materials requirement planning (MRP) with other organizational applications such as the general ledger.

enterprise unified communications infrastructure: The intent of unified communication is to integrate voice, email, and videoconferencing through employees' laptops and desktop computers.

Ethernet: A family of technologies for transmitting messages over a wired network.

expert system: A system to predict future events by accumulating knowledge of a particular subject in past events.

exterior lighting: Illumination of areas where an intruder would otherwise be able to work in darkness.

extranet: A web-based point of entry for users to gain access to a company's internal resources. The typical user is an employee in the field or a registered partner, such as a reseller or an agent.

Facebook: A social networking service with some business networking features.

fault management: Detects and tracks problems in a network to offer network administration insight for configuration management, performance tracking, and security.

Federal Communications Commission (FCC): The federal government agency that regulates electronic communications and the manufacture of communication equipment.

Federal Energy Regulatory Commission (FERC): The U.S. agency that regulates public utilities.

Federal Risk and Authorization Management Program (FEDRAMP): A framework for security assessments, authorization, and continuous monitoring for cloud-based security providers.

Federal Trade Commission (FTC): The U.S. agency that regulates all businesses that are engaged in interstate commerce or use interstate resources.

femtocell: A small cellular base station with a range of about 10 yards.

fence: A building structure used to prevent people from accessing an area.

fiber data distributed interface (FDDI): A specification for a 100 Mbps LAN implemented on fiber optic cabling.

fiber-optic cable: A cable that transmits information in light waves through pure glass strands.

File Transfer Protocol (FTP): A lowest-common-denominator protocol for the point-to-point transfer of text and binary files between IP-connected hosts.

file transfer: An application that sends files from a device on one network to a device on another network, typically with verification of its accuracy.

FIPS 200: A U.S. set of security requirements for federal information systems.

fire extinguisher: A portable device used to suppress a fire.

firewall: An inline device placed between networks to control the traffic that is allowed to pass between those networks.

firmware: Software stored in persistent memory on a computer, generally used to store initial instructions that are executed when the computer is switched on.

fixed-mobile convergence (FMC): These applications offer mobile employees the same types of services, such as email, phone, and videoconferencing, as employees who are at a fixed location.

fleet tracking: When a company monitors the status and performance of its mobile assets as well as tracks and monitors the maintenance of its fleet of vehicles.

forensics: The set of tools and procedures used to investigate an event and preserve evidence.

frame relay: A communications service that handles multiple packet connections between network-connected devices. Frame relay is faster and more efficient than X.25, its predecessor.

frame: An information packet plus all the preceding signals and succeeding signals necessary to convey it along the data link.

gateway: An element on the network that performs a protocol translation to connect different networks.

general ledger: A suite of applications that include budgeting tracking, order entry, payroll, accounts receivable, accounts payable, inventory tracking, financial reporting, inventory tracking, and tax reporting. All organizations have some custom variation of this application suite.

general office tools: Many office workers rely on office productivity tools, such as a word processor, a spreadsheet, email, a calendar, a contact database, presentation software, and a web browser. Office productivity tools may include a simple database application, a note-taking tool, and an imaging application. Many companies use Microsoft Office Suite, but may standardize on other specific applications for a variety of reasons.

governance: The set of activities performed by management to exert control over the organization.

grade of service: A measure of service quality from telecommunication carriers based on the probability that a connection will happen.

Gramm-Leach-Bliley Act (GLBA): A U.S. law that requires the protection of personal information in financial services organizations.

GSM: Cellular voice and data protocols used in cellular networks in most countries outside the United States and South Korea. AT&T Mobility and T-Mobile use this protocol in the United States.

guard dog: A trained canine used to protect facilities and personnel.

guard: A person with duties to protect facilities and personnel.

guideline: A statement that provides ideas on the implementation of policies and standards.

hacker: A hobbyist or an enthusiast who seeks to understand complex systems and make modifications to them.

hacktivist: A hacker-activist who attacks a system for political or ideological reasons.

hardware address: An address, fixed during manufacturing, identifying a network adapter such as a network interface card on an Ethernet.

headhunter: A colloquial reference to a recruiter.

Health Insurance Portability and Accountability Act (HIPAA): A U.S. law that defines requirements for the protection of health-related information.

heating, ventilation, and air conditioning (HVAC): Equipment that regulates temperature and humidity in buildings containing personnel, computers, or both.

hierarchical routing: Routing based on an addressing system that uses strict numbering schemes. For example, an IP routing algorithm uses IP addresses, which contain network numbers, subnet numbers, and host numbers.

high-performance computing: Exceptionally high-speed computational computers to perform research, such as meteorology, weapons design, and financial modeling.

hot spot: A Wi-Fi access point that is typically provided as a free service in a public area.

human resource management system (HRMS): A suite of applications supporting the human resources department. Modules typically include applicant tracking, recruiting, benefit selection, payroll (or an interface to payroll in the general ledger), and performance evaluation tracking.

implementation: The process of installing hardware, software, or a business process.

incident management: An IT process, a security operations process, or both used to properly respond to operational and security incidents.

incident response: Activities performed as a result of an incident.

inert gas fire suppression: A fire suppression system in which inert gas is discharged into an area to displace oxygen.

information flow: An access model in which information at specific levels of security are permitted to flow to specific systems or locations.

infrared communication: Communication by electromagnetic radiation just below visible light. The most common application of this technology is in remote controls for audiovisual systems.

infrastructure as a service (IaaS): An offering from a telecommunications carrier or a value-added network (VAN) to perform all voice, data, and video network services.

integrity: The concept in information security related to the protection of information and systems from unauthorized alteration.

internal audit: A process of self-examination of controls to determine their effectiveness.

Internet address: An address that identifies an element on the Internet with a number in the format of 172.16.254.1 for IP version 4. Also called *IP address*.

Internet Engineering Task Force (IETF): Corporate and academic volunteers who create and update Internet standards.

Internet of Things (IoT): Internet applications that remotely monitor and control intelligent devices, including home security systems, vehicles, home appliances, and medical-monitoring equipment.

Internet: The worldwide network of networks that exchanges email and data through an addressing and naming system using TCP/IP protocols.

interview: A discussion between an employer and an employment candidate, so that each can assess the other for suitability of employment.

intranet: A web page accessible with work-related applications and documents for use exclusively by employees.

intrusion prevention system (IPS): An inline device that examines incoming and outgoing network traffic, looking for signs of intrusions; when an intrusion is detected, it will block such traffic.

IP address: A unique identifier assigned to a node on a network.

ISO 27001: An international standard for the management of security in an organization.

ISO: Based in Switzerland, an international organization for standards, including networking standards.

ISP (Internet service provider): A telecommunications carrier that offers Internet connectivity.

job rotation: The practice of periodically moving personnel from role to role.

key card: A plastic card with a magnetic stripe, RFID, or smart card that is assigned to an individual worker, who uses it to activate door locks to permit entry into a room or a building.

key length: The length of an encryption key.

key logger: A hardware or software mechanism used to intercept keystrokes, especially login credentials.

key management: Procedures for the creation, use, protection, and disposal of encryption keys.

latency: The delay in sending or receiving data. (Latency reduces the response time of some high-speed communications).

layer: A set of functions defined by a network standards organization. For example, the OSI 7-Layer model is described by the ISO.

lighting a building: When a telecommunications company brings fiber-optic service to a building. This process typically involves a competitive phone company (CLEC), which can then compete with the established phone company.

line conditioner: A device that absorbs utility power noise, such as spikes and surges.

link: The logical connection between a sender and a receiver in a network.

LinkedIn: A business networking site used to establish business relationships.

local area network (LAN): A network that exists entirely in a single property.

login: A procedure in which a user establishes a connection on a network or an application. The procedure ensures proper security and accesses historical information about the user.

logout: A procedure in which a user ends a connection on a network or an application. See also *login.*

Long Term Evolution (LTE): A high-speed data technology used on both CDMA and GSM-based networks and commonly marketed as 4G.

loss: The amount of attenuation in a signal. Too much loss reduces throughput and causes either slow response times for data applications or poor quality sound or video.

Mac address: A standardized address for every element on a LAN used to create and update routing tables.

machine-to-machine communications (M2M): Intelligent equipment and remote sensors in which data is collected, analyzed, and managed by other machines without human intervention.

main storage: The component in a computer where information is stored temporarily.

mainframe: The heart of a centralized computing system where all applications are stored and through which all data is accessed and updated.

malicious software: Software designed to steal or alter data, steal login credentials, or permit a takeover of the target system for a malicious purpose.

malware: See *malicious software.*

managed network services: An offering from a telecommunications carrier or value-added network (VAN) to perform all network administration.

managed security service provider (MSSP): An organization that performs operational security tasks for one or more client organizations.

mandatory access control: A security model in which an access manager manages access to information.

mantrap: A set of two interlocked doors with a short passage between, to control movement of personnel through a door.

materials requirements planning (MRP): Applications in this class enable project managers to order necessary supplies timely and automatically.

maximum tolerable downtime (MTD): The theoretical period of time that a business process is incapacitated, after which the organization may fail to survive.

media access control (MAC): When an element on the network assumes control of the transmission media to send an information packet.

mesh: Network topology in which elements are organized to have multiple connections among network nodes to increase availability.

message switching: A switching technique that involves the transmission of messages from node to node through a network. The message is stored at each node until a forwarding path is available.

microwave: A point-to-point data transmission system employing electro-magnetic waves and licensed by the FCC in the United States. Enterprises and governments often use this system as an alternative to relying on a telecom-munications carrier.

mobile device management (MDM) services: An application used by com-panies to ensure proper security for mobile devices as well as ensuring that these devices have the correct provision of the mobile applications.

modem: A device that converts digital signals to analog for transmission over a circuit originally designed for voice communications, and then converts the analog signal to digital on the other side.

multifactor authentication: The presentation of a user ID with a token or a biometric.

multilayer switch: A switch that forwards packets based on MAC and network addresses.

multimode fiber: Whereas standard fiber-optic cable transmits data using white light, this solution sends more data down the same size cable by breaking white light into different frequencies (different colors).

multiplexing: A scheme that allows multiple signals to be transmitted simultaneously across a single physical channel.

multiprotocol label switching (MPLS): A packet-switched technology used to transport a variety of protocols, such as TCP/IP, Ethernet, ATM, and VoIP, over long distances.

narrowband: A communications service that provides bandwidth of 56 kb per second (DS 0) or less.

National Information Assurance Certification and Accreditation Process (NIACAP): A process framework used to certify and accredit U.S. national security systems.

near field communications (NFC): A protocol for wireless communications over short distances, up to 6cm.

need to know: The principle that people should have access to only the information (and systems) they need to perform their job.

network adapter: A network element that converts the electronic signals between a computer's network hardware and the transmission media.

network address: The logical address, rather than the physical address, of an element on a network.

network administrator: The person with the responsibility of managing the configuration and the performance of the elements of the network.

network analyzer: A hardware or software device offering various network troubleshooting features, including protocol-specific packet decodes, specific preprogrammed troubleshooting tests, packet filtering, and packet transmission.

network architecture: The design of a data network, including types of user interfaces employed, networking protocols, the physical topology, and the types of network cabling.

network bridge: A relatively basic element on a data network that connects two LANs.

network configuration and change management (NCCM) tools: The configuration management database along with applications tools that allow the administrator to track the effect of changes.

network fault monitoring tool: A tool that provides a clearer explanation of network problems to the administrator who is monitoring the system's health

network hub: A basic element on an Ethernet data network that connects a few PCs with NIC cards to a LAN.

network interface card (NIC): A card in a computer or other element on an Ethernet LAN that stores a logical IP address and physically connects with the LAN.

network management: The activities associated with providing, on an ongoing basis, the degree of quality needed by users, including resource planning, network design, user assistance, training, and troubleshooting network issues.

network operator: A person who routinely monitors and controls a network.

network performance monitoring tools: A tool that provides a clear analysis of system bottlenecks.

network redundancy: An approach whereby the failure of a single element in a network does not cause the failure of the entire network.

network resilience: The capability of a computer network to suffer failures but continue to operate in a diminished capacity.

network router: An element on an Ethernet data network that connects a few PCs with NIC cards to a LAN but is smarter and offers better throughput than a network hub.

network-attached storage (NAS): An architecture that allows database appliances to be stored remotely from servers.

network: A collection of computers and other intelligent devices that are controlled by equipment to provide the exchange of data.

NIST 800-53: A U.S. standard (Security and Privacy Controls for Federal Information Systems and Organizations) for the protection of information systems and supporting processes.

node: An element on the network that reads a protocol address and initiates a response to communication from other elements on the network that use the same networking protocols.

noise: Unwanted electrical or light signals on a network.

nominal throughput: The value of bits per second under optimal circumstances, which is typically quoted when comparing alternatives. See also *actual throughput*.

nondisclosure agreement: A legal agreement in which one or more parties agrees not to disclose the secrets of one or more other parties.

noninterference: An access model in which activities performed by persons at a higher level of security will not interfere with activities performed at lower levels of security.

nonprofit: A private organization that retains its surplus revenues to further its goals.

North American Electric Reliability Corp (NERC): The U.S. organization that creates standards for the protection of public utility control systems.

object oriented: A hierarchical system that consist of classes (software libraries), objects, methods, and a logical construction that includes encapsulation, inheritance, and polymorphism.

object: In access control, a system or data record that someone or something wants to access. See also *subject*.

offer letter: A formal written offer of employment, written by an employer and given to an employment candidate.

open source: Network tools or applications offered to users and companies at no charge. In many cases, the underlying code may be modified and improved by others under the premise that everyone will benefit.

operating system: A set of programs that facilitate the use of computer hardware, including storage, memory, and peripheral devices

OSI 7-Layer model: A method of describing the relationships between network protocols by grouping in layers. The layers logically define how the elements interact on data as it moves between the user and applications.

packet: A defined amount of data logically enclosed in a digital envelope with a digital address.

parallel test: A test of business continuity plans in which recovery systems are activated and process live data, but do so in isolation so as not to disturb production systems that are still running.

parity checking: A simple method to see whether any bits are missing from a packet by adding the bits and checking to see if there are too few or too many bits.

password quality: A measure of a password based on its complexity and resistance to attack.

password recovery: The process of assisting a user who has forgotten his or her password.

password: A secret word, phrase, or random characters used as part of authentication.

payload: The part of a transmission that is the customer information, not the overhead used for routing and error checking.

Payment Card Industry Data Security Standard (PCI-DSS): A standard for the protection of credit card data that is stored, processed, and transmitted.

phishing: A social engineering attack in which fraudulent messages are sent to targeted individuals to trick them into performing unauthorized actions.

picocell: A very small cellular transmitter/receiver. Its coverage is comparable to a Wi-Fi access point and greater than a femtocell.

PIN pad: A keypad with numbers or letters, generally used with key cards.

ping: A network diagnostic technique in which a network node asks another element to reply to verify a viable connection.

plain old telephone service (POTS): See *public-switched telephone network.*

plaintext: A message in its original, readable format (as opposed to ciphertext).

point-of-sale (POS): A custom-built device that supports all modes of payment, including cash, and results in more secure and efficient transactions.

policy: A formal statement that describes what actions and behaviors are required or forbidden in an organization.

polling: An approach used by some network protocols manage contention by allowing a device to send data only after it has been given permission by the controlling device. The controller will go around the network and asks, or polls, each device whether it has anything to send.

port: A distinct connection for PCs and intelligent devices on an Ethernet network hub, bridge, or router.

pre-sales: Activities between a vendor and a client organization where the vendor is exchanging information with the client.

privacy: The concept and practice of protecting a person's sensitive information.

private sector: The portion of an economy that consists of all organizations owned and operated by private individuals or groups.

procedure: Step-by-step instructions for carrying out a task.

process: A set of one or more procedures used to carry out a business activity.

project management tools: Tools that provide information to project managers on status and can help highlight potential problems before they become critical.

proof of concept (POC): The implementation of a system for a limited period of time to determine its long-term viability.

protocol stack: Defined by a vendor or a standards organization, a group of protocols that implement more than one layer of the OSI 7-Layer model.

protocol: A networking specification of the addresses and algorithms used to accomplish a specific network function.

pseudorandom number generator (PRNG): A technique for deriving a random number for use during encryption and decryption.

public sector: The portion of an economy that consists of all organizations owned and operated by governments.

public-switched telephone network (PSTN): The worldwide network of telephones, cabling, and switches to facilitate voice communications.

queuing theory: An academic discipline used in networking to scale the size of networks and provide enough bandwidth to keep user response times within an acceptable range.

quotation: A statement of cost for a particular product or service.

race condition: See *state attack*.

razor wire: A continuous mesh of metal strips with sharp edges along its length, placed at the top of a fence or wall to deter others from climbing over it.

recruiter: An individual who searches for employment candidates for one or more organizations.

reference: An individual who agrees to independently verify an employment candidate's background.

remote access: The process of facilitating an employee's ability to remotely access information systems that are not accessible from the Internet.

repeater: A device on the network that addresses attenuation by amplifying, or otherwise helping, a network signal without reading or interpreting it.

resignation: A written or verbal statement of intent to discontinue employment with an organization.

response time: The time from when a user initiates an action and the action displays its results. Response time is key factor of how users view the quality of a network.

resume: A document that summarizes skills, education, and employment history. See also *curriculum vitae (CV).*

ring topology: A LAN network topology in which computers and other elements are connected to each other and to a central switch.

risk assessment: An examination of risks present in specific systems, processes, suppliers, or perhaps the entire organization.

risk ledger: A listing of risks identified in a risk assessment or by other means.

risk management: Formal activities to identify and appropriately respond to risk.

risk treatment: The formal acceptance, mitigation, transfer, or avoidance of identified risks.

role-based access control (RBAC): An access model in which access is assigned to groups of users instead of individual users.

router: A device that forwards TCP/IP packets toward their destination.

routing table: Used by a router, a list of networks that permits the router to correctly route packets.

sales force automation (SFA): A class of applications designed for order entry, inventory checking, and collaboration tools as needed by a given sales force.

salting: The practice of inserting a set of characters into a hashing operation to thwart cryptanalysis.

Sarbanes-Oxley Act (SarBox): The U.S. law that requires publicly held organizations to enact business and IT controls to ensure the integrity of their financial systems and financial statements.

scalability: The capability of a network to operate properly when configured on a larger scale.

secondary storage: The computer component where information is stored permanently.

security awareness training: Formal training for employees regarding an organization's security policies and procedures.

segregation of duties: See *separation of duties*.

separation of duties: The practice of designing a critical task so that two or more people are required to complete it.

server: A computing device on a network that stores applications that are then shared by multiple users.

service-level agreement (SLA): A contractual commitment by a telecommunications carrier or VAN to provide a specified level of network availability or a specified rate of reimbursement.

session hijacking: An attack on a system in which an attacker intercepts session tokens and attempts to take over the session.

session: An ongoing connection between two computing devices on a network involving the sharing of resources and data.

shielded twisted pair (STP): Cabling with a layer of shielded insulation around twisted pair wires traditionally used for telephones. The shielded insulation is present to reduce electromagnetic interference, thereby improving the signal-to-noise ratio.

short: The inadvertent connection of two or more conductors that typically causes a failure.

side channel attack: A technique of observing a system's running states to make inferences about activities in the system.

signal-to-noise ratio: The ratio of the signal strength to the amount of undesired signal disturbances.

signal: Sending digital information by an electromagnetic wave that is modulated and demodulated in sequence to represents bits.

Simple Network Management Protocol (SNMP): The standard for management of networked devices.

simulation: A review of business-continuity-planning or disaster-recovery-planning procedures in which a realistic scenario is defined and exercised.

single point of failure: A component, system, or individual with no alternative resource.

smoke detector: A device that alerts personnel when smoke is detected. A smoke detector is considered an early warning device in the event of a fire.

social engineering: The practice of tricking individuals into performing unauthorized actions.

software as a service (SaaS): An arrangement for an outside company to provide a service provided over a network to another organization for an ongoing fee. This is in lieu of the outside company selling the application to the organization for a one-time fee and having the app reside on a server belonging to the organization.

software development life cycle (SDLC): The business process used to develop and maintain software programs.

Software Engineering Institute — Capability Maturity Model Integration (SEI-CMMI): A model for assessing the maturity of an organization's security practices.

source code: The human-readable form of a computer program.

spam: Unwanted email, generally sent from an unknown party.

specification: A document that defines an architecture or a protocol and the allowable implementations.

sprinkler system: A fire suppression system in which water is sprayed into an area.

standard: A formal statement that describes how a security policy will be carried out.

star topology: A LAN network topology in which computers and other elements are connected to a central switch.

state attack: A technique of exploiting a timing flaw in a system to gain access to a resource used by another process. Also known as a *race condition*.

statistical multiplexing: A technique to combine more information on a single physical connection by allocating small time slots to different users. Also known as *statistical time-division multiplexing* or *stat mux.*

steganography: A technique used to hide a message in a larger file such as an image file, a video, or a sound file.

stream cipher: An encryption algorithm used to encrypt or decrypt a stream of data, one character at a time.

structured cabling: Running cables or wires to the office space of employees and in operations in a tracked and managed way.

subject: In access control, a person or system that wants to access something. See also *object.*

subnet address: A portion of an IP address that specifies the number defining a portion of the TCP/IP network.

subnet mask: A representation of a computer's Internet address in which all bit positions corresponding to the user's network and subnetwork ID are 1s and the bit positions corresponding to the user's host ID are 0.

subnetwork: A portion of the LAN arbitrarily created by the network administrator to provide the user routing structure while shielding the subnetwork from the addressing scheme of the attached networks.

supervisory control and data acquisition (SCADA): An application to automatically control other machines.

Synchronous Optical Network (SONET): A family of protocols for carrying voice and data traffic over copper and fiber telecommunications networks.

systems design: A discipline in which a network architect specifies elements that have enough resources to meet the needs of the users but are as economical as possible.

Systems Security Engineering Capability Maturity Model (SSE-CMM): A model for evaluating an organization's capability to implement security in a system.

T-1: See *DS-1.*

tailgating: The practice of closely following an authorized person through a security door to gain unauthorized entry.

take-grant: An access model used to establish or disprove the safety of a given computer system.

telecommunications carrier: A company authorized by state or local governments or both to provide communication services across property lines. These companies can provide simple connections or may offer management services.

Telecommunications Industry Association (TIA): A standards setting organization in the United States for telecommunications technologies.

threat: The capability and the intent to carry out a harmful act.

throughput: The data rate measured in some factor of bits per second passing through a point in a network.

token: A hardware device used to facilitate authentication to a system.

topology: The physic arrangement of cables connecting computing devices in a network.

Transmission Control Protocol/Internet Protocol (TCP/IP): A family of data communications protocols for the transmission of data over networks.

Trojan horse: A program with a stated purpose as well as an unstated and malicious purpose.

trusted platform module (TPM): A hardware device used to store encryption keys.

TTY/TDD: Telecommunications device for the deaf. This telecommunications service allows individuals that are either death or are unable to speak to communicate with others over standard telephone lines.

Twitter: A microblogging site used to share information.

unified communications (UC): A combination of technologies in a single network backbone to provide an integrated solution for data, voice, and videoconferencing.

unified communications and collaboration (UCC): A combination of unified communication and collaboration tools with a single user interface.

uninterruptible power supply (UPS): A device equipped with backup batteries that can supply power to computing equipment for several minutes to an hour or more.

unshielded twisted pair (UTP): Inexpensive and readily available wiring in many office buildings.

user ID: A personal identifier issued to the user of a system.

users group: Organizations that use a common technology and gather to share information on troubleshooting and future needs. Companies typically support user groups as a way to gain insight into the ongoing needs of customers.

value-added network (VAN): An organization that buys basic connectivity from a telecommunications carrier and bundles other services to meet the needs of a segment of customers.

value-added reseller (VAR): A for-profit company that serves a customer segment by buying computers, networking equipment, and telecommunications services and bundling them to address a particular need.

very small aperture terminal (VSAT): A relatively low-cost data solution for communicating data to remote locations via satellite.

video surveillance: A system of one or more cameras plus monitors or recording equipment or both, used to monitor key locations inside or outside a facility.

virtual private network (VPN): A technique used to encapsulate network traffic flowing between two systems, between a system and a network, or between two networks.

virus: Malicious code that attaches itself to a file.

visitor log: A written or electronic record of visitors to a building.

voice over LTE (VoLTE): A technology that allows voice communication over the LTE data networks of wireless carriers.

vulnerability management: An IT operations process that is concerned with the identification and mitigation of vulnerabilities in IT systems.

walkthrough: A review of a process or procedure document in a group setting.

wall: A building structure used to prevent people from accessing an area.

WAN: Any network with connections extending beyond a property line. With a few exceptions, a telecommunication carrier is involved.

watermarking: A technique used to implant a visible (or audible) imprint on a document, an image, a sound recording, or a video recording.

web access filter: A device that examines the websites that users want to visit and then blocks or permits such access according to policy rules.

web application: An application consisting of a web browser on a user's workstation (or mobile device), a web server, and often an application server and a database management system.

Wi-Fi: A family of protocols for wireless communications over a distance up to 100 meters.

Wired Equivalency Protocol (WEP): An obsolete standard for encrypting data over Wi-Fi.

Wireless Protected Access (WPA): A standard for encrypting data over Wi-Fi.

Wireless Protected Access 2 (WPA2): A standard for encrypting data over Wi-Fi.

wiring closet: The location from which communication cables originate to allow users access to the network at their office space. The closet allows the network administrator to make changes closer to the users than the data center.

Worldwide Interoperability for Microwave Access (WiMAX): A wireless telecommunications standard for voice and data communications.

worm: Malicious software that can self-propagate.

Index

• *T* •

About the Authors

Peter H. Gregory, CISA, CISSP, CRISC, C|CISO, QSA, is the author of forty books on security and technology, including *Solaris Security* (Prentice Hall), *CISSP For Dummies* (Wiley), *IT Disaster Recovery Planning For Dummies* (Wiley), and *CISA Certified Information Systems Auditor All-In-One Study Guide* (McGraw-Hill/Osborne Media Group).

Peter is a 30-year career technologist and is currently Director of Strategic Services at Fishnet Security, a national information security professional services firm. He has had tactical and strategic security jobs in SAAS, retail, and large wireless telecommunications organizations. He has also held development and operations posts in casino management systems, banking, government, nonprofit organizations, and academia. He is the lead instructor and advisory board member for the University of Washington certificate program in information systems security and a graduate of the FBI Citizens' Academy. Peter can be found at `www.peterhgregory.com`.

Bill Hughes is an experienced marketing strategy executive with over two decades of experience in sales, strategic marketing, and business development roles at several leading corporations, including Microsoft, IBM, General Electric, Motorola, and Xerox. Recently, Bill has worked with Xerox to enhance their strategic marketing to mobile users. He has also lead initiatives to develop new products and solutions with several high technology organizations including Microsoft, Nextel, Motorola, SBC, and Tyco Electronics.

Bill has been a Professor of Marketing at the Kellogg School of Management of Northwestern where he taught business marketing to graduate MBA students. In his lectures, he presented his findings on the validity of the market research information used in financial analysis. Bill has also written articles on this subject for several wireless industry trade magazines as well as *USA Today* and *Forbes*. These articles were based on his research reports written for In-Stat, where he was a principal analyst covering the wireless industry, specializing in smartphones and business applications of wireless devices. His most popular studies include "The Symbian Foundation — A Battle Royal for the Ecosystem," "Wireless Data in the Enterprise: The Hockey Stick Arrives," and "Cellphone Trends in US Enterprises: A Small Step from Personal Wireless."

He graduated with honors with an MBA degree from the Kellogg School of Management at Northwestern University and earned a Bachelor of Science degree with Distinction from the College of Engineering at Cornell University, where he was elected to the Tau Beta Pi Engineering Honorary.

Dedications

To Rebekah, Shannon, and Nathan, and to the memory of my other children.

— Peter H. Gregory

To my son, Arlen, as he continues his education at Washington State University. Go Cougs, and continue to have fun, but not too much fun, at Phi Kappa Theta!

— Bill Hughes

Authors' Acknowledgments