PEARSON IT CYBERSECURITY CURRICULUM

THIRD EDITION

# NETWORK DEFENSE AND COUNTERMEASURES

## Principles and Practices

CHUCK EASTTOM

# Network Defense and Countermeasures

## Principles and Practices

### Third Edition

Chuck Easttom

Pearson

800 East 96th Street, Indianapolis, Indiana 46240 USA

## Network Defense and Countermeasures

ISBN-13: 978-0-7897-5996-2

ISBN-10: 0-7897-5996-9

Library of Congress Control Number: 2018933854

Printed in the United States of America

1 18

### Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose. All such documents and related graphics are provided “as is” without warranty of any kind. Microsoft and/ or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screenshots may be viewed in full within the software version specified.

Microsoft® and Windows® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. Screenshots and icons reprinted with permission from the Microsoft Corporation. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

### Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

### Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

**Editor-in-Chief**
Mark Taub

**Product Line Manager**
Brett Bartow

**Executive Editor**
Mary Beth Ray

**Development Editor**
Ellie C. Bru

**Managing Editor**
Sandra Schroeder

**Senior Project Editor**
Tonya Simpson

**Copy Editor**
Bill McManus

**Indexer**
Erika Millen

**Proofreader**
Abigail Manheim

**Technical Editors**
Akhil Behl
Steve Kalman

**Publishing Coordinator**
Vanessa Evans

**Cover Designer**
Chuti Prasertsith

**Compositor**
codemantra

# Contents at a Glance

# Table of Contents

## Chapter 2: Types of Attacks 40

**Chapter 3: Fundamentals of Firewalls** **76**

**Chapter 4: Firewall Practical Applications** **100**

# Preface

The hottest topic in the IT industry today is computer security. The news is replete with stories of hacking, viruses, and identity theft. The cornerstone of security is defending the organizational network. *Network Defense and Countermeasures: Principles and Practices* offers a comprehensive overview of network defense. It introduces students to network security threats and methods for defending the network. Three entire chapters are devoted to firewalls and intrusion-detection systems. There is also a chapter providing a basic introduction to encryption. Combining information on the threats to networks, the devices and technologies used to ensure security, as well as concepts such as encryption provides students with a solid, broad-based approach to network defense.

This book provides a blend of theoretical foundations and practical applications. Each chapter ends with multiple choice questions and exercises, and most chapters also have projects. Students who successfully complete this textbook, including the end of chapter material, should have a solid understanding of network security. Throughout the book the student is directed to additional resources that can augment the material presented in the chapter.

## Audience

This book is designed primarily as a textbook for students who have a basic understanding of how networks operate, including basic terminology, protocols, and devices. Students do not need to have an extensive math background or more than introductory computer courses.

## Overview of the Book

This book will walk you through the intricacies of defending your network against attacks. It begins with a brief introduction to the field of network security in Chapter 1, "Introduction to Network Security." Chapter 2, "Types of Attacks," explains the threats to a network—including denial of service attacks, buffer overflow attacks, and viruses.

Chapter 3, "Fundamentals of Firewalls," Chapter 4, "Firewall Practical Applications," Chapter 5, "Intrusion-Detection Systems," and Chapter 7, "Virtual Private Networks," give details on various security technologies including firewalls, intrusion-detection systems, and VPNs. These items are the core of any network's security, so a significant portion of this book is devoted to ensuring the reader fully understands both the concepts behind them and the practical applications. In every case, practical direction for selecting appropriate technology for a given network is included.

Chapter 6, "Encryption Fundamentals," provides a solid introduction to encryption. This topic is critical because ultimately computer systems are simply devices for storing, transmitting, and manipulating data. No matter how secure the network is, if the data it transmits is not secure then there is a significant danger.

Chapter 8, “Operating System Hardening,” teaches operating system hardening. Chapter 9, “Defending Against Virus Attacks,” and Chapter 10, “Defending Against Trojan Horses, Spyware, and Adware,” give the reader specific defense strategies and techniques to guard against the most common network dangers. Chapter 11, “Security Policies,” gives readers an introduction to security policies.

Chapter 12, “Assessing System Security,” teaches the reader how to do an assessment of a network’s security. This includes guidelines for examining policies as well as an overview of network assessment tools. Chapter 13, “Security Standards,” gives an overview of common security standards such as the *Orange Book* and the Common Criteria. This chapter also discusses various security models such as Bell-LaPadula. Chapter 14, “Physical Security and Disaster Recovery,” examines the often-overlooked topic of physical security as well as disaster recovery, which is a key part of network security.

Chapter 15, “Techniques Used by Attackers,” provides the tools necessary to “know your enemy,” by examining basic hacking techniques and tools as well as strategies for mitigating hacker attacks. Chapter 16, “Introduction to Forensics,” helps you understand basic forensics principles in order to properly prepare for investigation if you or your company become the victim of a computer crime. Chapter 17, “Cyber Terrorism,” discusses computer-based espionage and terrorism, two topics of growing concern for the computer security community but often overlooked in textbooks.

## About the Author

**Chuck Easttom** is a computer scientist, author, and inventor. He has authored 25 other books on programming, Web development, security, and Linux. He has also authored dozens of research papers on a wide range of computer science and cyber security topics. He is an inventor with 13 computer science patents. Chuck holds more than 40 different industry certifications. He also is a frequent presenter/speaker at computer and cyber security conferences such as Defcon, ISC2 Security Congress, Secure World, IEEE workshops, and more.

You can reach Chuck at his website (www.chuckeasttom.com) or by e-mail at chuck@chuckeasttom.com.

## Dedication

*This book is dedicated to all the people working in the computer security field, diligently working to make computer networks safer.*

## Acknowledgments

While only one name goes on the cover of this book, it is hardly the work of just one person. I would like to take this opportunity to thank a few of the people involved. First of all, the editing staff at Pearson worked extremely hard on this book. Without them this project would simply not be possible. I would also like to thank my wife, Teresa, for all her support while working on this book. She is always very supportive in all my endeavors, a one-woman support team!

## About the Technical Reviewers

**Akhil Behl**, CCIE No. 19564, is a passionate IT executive with key focus on cloud and security. He has more than 15 years of experience in the IT industry working in several leadership, advisory, consultancy, and business development profiles with various organizations. His technology and business specialization includes cloud, security, infrastructure, data center, and business communication technologies.

Akhil has authored multiple titles on security and business communication technologies. He has contributed as technical editor for a number of books on network and information security. He has published several research papers in national and international journals, including IEEE *Xplore*, and presented at various IEEE conferences, as well as other prominent ICT, security, and telecom events.

Akhil also holds CCSK, CHFI, PMP, ITIL, VCP, TOGAF, CEH, ISM, and several other industry certifications. He has bachelor's in technology degree and an MBA.

**Steve Kalman** is both an attorney and a professional security expert. He holds the following credentials from (ISC)2 for whom he worked as an authorized instructor: CISSP, CCFP-US, CSSLP, ISSMP, ISSAP, HCISPP, SSCP. Steve has been author or technical editor for more than 20 Pearson/Cisco Press books.

## We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

*Please note that we cannot help you with technical problems related to the topic of this book.*

When you write, please be sure to include this book’s title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification

ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

## Reader Services

Register your copy of *Network Defense and Countermeasures* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780789759962 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

# Chapter 1

# Introduction to Network Security

## Chapter Objectives

**After reading this chapter and completing the exercises, you will be able to do the following:**

- Identify the most common dangers to networks.
- Understand basic networking.
- Employ basic security terminology.
- Find the best approach to network security for your organization.
- Evaluate the legal issues that will affect your work as a network administrator.
- Use resources available for network security.

## Introduction

Finding a week without some major security breach in the news is difficult. University web servers hacked, government computers hacked, banks' data compromised, health information exposed—the list goes on. It also seems as if each year brings more focus to this issue. Finding anyone in any industrialized nation who had not heard of things such as websites being hacked and identities stolen would be difficult.

More venues for training also exist now. Many universities offer Information Assurance degrees from the bachelor's level up through the doctoral level. A plethora of industry certification training programs are available, including the CISSP, EC Council's CEH, Mile2 Security, SANS, and CompTIA's Security+. There are also now a number of universities offering degrees in cyber security, including distance learning degrees.

Despite this attention from the media and the opportunities to acquire security training, far too many computer professionals—including a surprising number of network administrators—do not have a clear understanding of the type of threats to which network systems are exposed, or which ones are most likely to actually occur. Mainstream media focuses attention on the most dramatic computer security breaches rather than giving an accurate picture of the most plausible threat scenarios.

This chapter looks at the threats posed to networks, defines basic security terminology, and lays the foundation for concepts covered in the chapters that follow. The steps required to ensure the integrity and security of your network are methodical and, for the most part, already outlined. By the time you complete this book, you will be able to identify the most common attacks, explain how they are perpetrated in order to prevent them, and understand how to secure your data transmissions.

# The Basics of a Network

Before diving into how to protect your network, exploring what networks are would probably be a good idea. For many readers this section will be a review, but for some it might be new material. Whether this is a review for you, or new information, having a thorough understanding of basic networking before attempting to study network security is critical. Also, be aware this is just a brief introduction to basic networking concepts. Many more details are not explored in this section.

A network is simply a way for machines/computers to communicate. At the physical level, it consists of all the machines you want to connect and the devices you use to connect them. Individual machines are connected either with a physical connection (a category 5 cable going into a network interface card, or NIC) or wirelessly. To connect multiple machines together, each machine must connect to a hub or switch, and then those hubs/switches must connect together. In larger networks, each subnetwork is connected to the others by a router. We look at many attacks in this book (including several in Chapter 2, “Types of Attacks”) that focus on the devices that connect machines together on a network (that is, routers, hubs, and switches). If you find this chapter is not enough, this resource might assist you: http://compnetworking.about.com/od/basicnetworkingconcepts/Networking_Basics_Key_Concepts_in_Computer_Networking.htm.

## Basic Network Structure

Some connection point(s) must exist between your network and the outside world. A barrier is set up between that network and the Internet, usually in the form of a firewall. Many attacks discussed in this book work to overcome the firewall and get into the network.

The real essence of networks is communication—allowing one machine to communicate with another. However, every avenue of communication is also an avenue of attack. The first step in understanding how to defend a network is having a detailed understanding of how computers communicate over a network.

The previously mentioned network interface cards, switches, routers, hubs, and firewalls are the fundamental physical pieces of a network. The way they are connected and the format they use for communication is the network architecture.

## Data Packets

After you have established a connection with the network (whether it is physical or wireless), you need to send data. The first part is to identify where you want to send it. We will start off discussing IP version 4 addresses; we will look at IPv6 a bit later in this chapter. All computers (as well as routers) have an IP address that is a series of four numbers between 0 and 255 and separated by periods, such as 192.0.0.5 (note that this is an IPv4 address). The second part is to format the data for transmission. All data is ultimately in binary form (1s and 0s). This binary data is put into packets, all less than about 65,000 bytes. The first few bytes are the header. That header tells where the packet is going, where it came from, and how many more packets are coming as part of this transmission. There is actually more than one header, but for now, we will just discuss the header as a single entity. Some attacks that we will study (IP spoofing, for example) try to change the header of packets to give false information. Other methods of attack simply try to intercept packets and read the content (thus compromising the data).

A packet can have multiple headers. In fact, most packets will have at least three headers. The IP header has information such as IP addresses for the source and destination, as well as what protocol the packet is. The TCP header has information such as port number. The Ethernet header has information such as the MAC address for the source and destination. If a packet is encrypted with Transport Layer Security (TLS), it will also have a TLS header.

## IP Addresses

The first major issue to understand is how to get packets to their proper destination. Even a small network has many computers that could potentially be the final destination of any packet sent. The Internet has millions of computers spread out across the globe. How do you ensure that a packet gets to its proper destination? The problem is not unlike addressing a letter and ensuring it gets to the correct destination. Let's begin by looking at IP version 4 addressing because it is the most common in use today, but this section also briefly discusses IP version 6.

An IP version 4 address is a series of four three-digit numbers separated by periods. (An example is 107.22.98.198.) Each of the three-digit numbers must be between 0 and 255. You can see that an address of 107.22.98.466 would not be a valid one. The reason for this rule is that these addresses are actually four binary numbers: The computer simply displays them to you in decimal format. Recall that 1 byte is 8 bits (1s and 0s), and an 8-bit binary number converted to decimal format will be between 0 and 255. The total of 32 bits means that approximately 4.2 billion possible IP version 4 addresses exist.

The IP address of a computer tells you a lot about that computer. The first byte (or the first decimal number) in an address tells you to what class of network that machine belongs. Table 1-1 summarizes the five network classes.

**TABLE 1-1** Network Classes

| Class | IP Range for the First Byte | Use |
|---|---|---|
| A | 0–126 | Extremely large networks. No Class A network IP addresses are left. All have been used. |
| B | 128–191 | Large corporate and government networks. All Class B IP addresses have been used. |
| C | 192–223 | The most common group of IP addresses. Your ISP probably has a Class C address. |
| D | 224–247 | These are reserved for multicasting (transmitting different data on the same channel). |
| E | 248–255 | Reserved for experimental use. |

These five classes of networks will become more important later in this book (or should you decide to study networking on a deeper level). Observe Table 1-1 carefully, and you probably will discover that the IP range of 127 was not listed. This omission is because that range is reserved for testing. The IP address of 127.0.0.1 designates the machine you are on, regardless of that machine's assigned IP address. This address is often referred to as the *loopback address*. That address will be used often in testing your machine and your NIC. We will examine its use a bit later in this chapter in the section on network utilities.

These particular classes are important as they tell you what part of the address represents the network and what part represents the node. For example, in a Class A address, the first octet represents the network, and the remaining three represent the node. In a Class B address, the first two octets represent the network, and the second two represent the node. And finally, in a Class C address, the first three octets represent the network, and the last represents the node.

There are also some very specific IP addresses and IP address ranges you should be aware of. The first, as previously mentioned, is 127.0.0.1, or the loopback address. It is another way of referring to the network interface card of the machine you are on.

Private IP addresses are another issue to be aware of. Certain ranges of IP addresses have been designated for use within networks. These cannot be used as public IP addresses but can be used for internal workstations and servers. Those IP addresses are

- 10.0.0.10 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

Sometimes people new to networking have some trouble understanding public and private IP addresses. A good analogy is an office building. Within a single office building, each office number must be unique. You can only have one 305. And within that building, if you discuss office 305 it is immediately clear what you are talking about. But there are other office buildings, many of which have their own office 305. You can think of private IP addresses as office numbers. They must be unique within their network, but there may be other networks with the same private IP.

Public IP addresses are more like traditional mailing addresses. Those must be unique worldwide. When communicating from office to office you can use the office number, but to get a letter to another building you have to use the complete mailing address. It is much the same with networking. You can communicate within your network using private IP addresses, but to communicate with any computer outside your network, you have to use public IP addresses.

One of the roles of a gateway router is to perform what is called network address translation (NAT). Using NAT, a router takes the private IP address on outgoing packets and replaces it with the public IP address of the gateway router so that the packet can be routed through the Internet.

We have already discussed IP version 4 network addresses; now let's turn our attention to subnetting. If you are already familiar with this topic, feel free to skip this section. For some reason this topic tends to give networking students a great deal of trouble. So we will begin with a conceptual understanding. *Subnetting* is simply chopping up a network into smaller portions. For example, if you have a network using the IP address 192.168.1.X (X being whatever the address is for the specific computer), then you have allocated 255 possible IP addresses. What if you want to divide that into two separate subnetworks? Subnetting is how you do that.

More technically, the subnet mask is a 32-bit number that is assigned to each host to divide the 32-bit binary IP address into network and node portions. You also cannot just put in any number you want. The first value of a subnet mask must be 255; the remaining three values can be 255, 254, 252, 248, 240, 224, or 128. Your computer will take your network IP address and the subnet mask and use a binary AND operation to combine them.

It may surprise you to know that you already have a subnet mask even if you have not been subnetting. If you have a Class C IP address, then your network subnet mask is 255.255.255.0. If you have a Class B IP address, then your subnet mask is 255.255.0.0. And finally, if it is Class A, your subnet mask is 255.0.0.0.

Now think about these numbers in relationship to binary numbers. The decimal value 255 converts to 11111111 in binary. So you are literally "masking" the portion of the network address that is used to define the network, and the remaining portion is used to define individual nodes. Now if you want fewer than 255 nodes in your subnet, then you need something like 255.255.255.240 for your subnet. If you convert 240 to binary, it is 11110000. That means the first three octets and the first 4 bits of the last octet define the network. The last 4 bits of the last octet define the node. That means you could have as many as 1111 (in binary) or 15 (in decimal) nodes on this subnetwork. This is the basic essence of subnetting.

Subnetting only allows you to use certain, limited subnets. Another approach is CIDR, or classless interdomain routing. Rather than define a subnet mask, you have the IP address followed by a slash and a number. That number can be any number between 0 and 32, which results in IP addresses like these:

192.168.1.10/24 (basically a Class C IP address)

192.168.1.10/31 (much like a Class C IP address with a subnet mask)

When you use this, rather than having classes with subnets, you have variable-length subnet masking (VLSM) that provides classless IP addresses. This is the most common way to define network IP addresses today.

You should not be concerned that new IP addresses are likely to run out soon. The IP version 6 standard is already available, and methods are in place already to extend the use of IPv4 addresses. The IP addresses come in two groups: public and private. The *public* IP addresses are for computers connected to the Internet. No two public IP addresses can be the same. However, a *private* IP address, such as one on a private company network, has to be unique only in that network. It does not matter if other computers in the world have the same IP address, because this computer is never connected to those other worldwide computers. Network administrators often use private IP addresses that begin with a 10, such as 10.102.230.17. The other private IP addresses are 172.16.0.0–172.31.255.255 and 192.168.0.0–192.168.255.255.

Also note that an ISP often will buy a pool of public IP addresses and assign them to you when you log on. So, an ISP might own 1,000 public IP addresses and have 10,000 customers. Because all 10,000 customers will not be online at the same time, the ISP simply assigns an IP address to a customer when he or she logs on, and the ISP un-assigns the IP address when the customer logs off.

IPv6 utilizes a 128-bit address (instead of 32) and utilizes a hex numbering method in order to avoid long addresses such as 132.64.34.26.64.156.143.57.1.3.7.44.122.111.201.5. The hex address format appears in the form of 3FFE:B00:800:2::C, for example. This gives you $2^{128}$ possible addresses (many trillions of addresses), so no chance exists of running out of IP addresses in the foreseeable future.

There is no subnetting in IPv6. Instead, it only uses CIDR. The network portion is indicated by a slash followed by the number of bits in the address that are assigned to the network portion, such as

/48

/64

There is a loopback address for IPv6, and it can be written as ::/128. Other differences between IPv4 and IPv6 are described here:

- Link/machine-local.
  - IPv6 version of IPv4's APIPA or Automatic Private IP Addressing. So if the machine is configured for dynamically assigned addresses and cannot communicate with a DHCP server, it assigns itself a generic IP address. DHCP, or Dynamic Host Configuration Protocol, is used to dynamically assign IP addresses within a network.

  - IPv6 link/machine-local IP addresses all start with fe80::. So if your computer has this address, that means it could not get to a DHCP server and therefore made up its own generic IP address.
- Site/network-local.
  - IPv6 version of IPv4 private address. In other words, these are real IP addresses, but they only work on this local network. They are not routable on the Internet.
  - All site/network-local IP addresses begin with FE and have C to F for the third hexadecimal digit: FEC, FED, FEE, or FEF.
- DHCPv6 uses the Managed Address Configuration Flag (M flag).
  - When set to 1, the device should use DHCPv6 to obtain a stateful IPv6 address.
- Other stateful configuration flag (O flag).
  - When set to 1, the device should use DHCPv6 to obtain other TCP/IP configuration settings. In other words, it should use the DHCP server to set things like the IP address of the gateway and DNS servers.

## Uniform Resource Locators

For most people, the main purpose for getting on the Internet is web pages (but there are other things such as e-mail and file downloading). If you had to remember IP addresses and type those in, then surfing the Net would be cumbersome at best. Fortunately, you don’t have to. You type in domain names that make sense to humans and those get translated into IP addresses. For example, you might type in www.chuckeasttom.com to go to my website. Your computer, or your ISP, must translate the name you typed in (called a *Uniform Resource Locator*, or URL) into an IP address. The DNS (Domain Name Service) protocol, which is introduced along with other protocols a bit later in Table 1-2, handles this translation process. So you are typing in a name that makes sense to humans, but your computer is using a corresponding IP address to connect. If that address is found, your browser sends a packet (using the HTTP protocol) to TCP port 80. If that target computer has software that listens and responds to such requests (like web-server software such as Apache or Microsoft Internet Information Services), then the target computer will respond to your browser’s request and communication will be established. This method is how web pages are viewed. If you have ever received an Error 404: File Not Found, what you’re seeing is that your browser received back a packet (from the web server) with error code 404, denoting that the web page you requested could not be found. The web server can send back a series of error messages to your web browser, indicating different situations.

E-mail works the same way as visiting websites. Your e-mail client will seek out the address of your e-mail server. Then your e-mail client will use either POP3 to retrieve your incoming e-mail, or SMTP to send your outgoing e-mail. Your e-mail server (probably at your ISP or your company) will then try to resolve the address you are sending to. If you send something to chuckeasttom@yahoo.com, your e-mail server will translate that e-mail address into an IP address for the e-mail server at yahoo.com, and then your server will send your e-mail there. Note that newer e-mail protocols are out there; however, POP3 is still the most commonly used.

IMAP is now widely used as well. Internet Message Access Protocol operates on port 143. The main advantage of IMAP over POP3 is it allows the client to download only the headers to the machine, and then the user can choose which messages to fully download. This is particularly useful for smart phones.

## MAC Addresses

*MAC addresses* are an interesting topic. (You might notice that MAC is also a sublayer of the data link layer of the OSI model.) A MAC address is a unique address for an NIC. Every NIC in the world has a unique address that is represented by a six-byte hexadecimal number. The Address Resolution Protocol (ARP) is used to convert IP addresses to MAC addresses. So, when you type in a web address, the DNS protocol is used to translate that into an IP address. The ARP protocol then translates that IP address into a specific MAC address of an individual NIC.

## Protocols

Different types of communications exist for different purposes. The different types of network communications are called *protocols*. A protocol is, essentially, an agreed-upon method of communications. In fact, this definition is exactly how the word *protocol* is used in standard, non-computer usage. Each protocol has a specific purpose and normally operates on a certain port (more on ports in a bit). Table 1-2 lists some of the most important protocols.

**TABLE 1-2** Logical Ports and Protocols

| Protocol | Purpose | Port |
|---|---|---|
| FTP (File Transfer Protocol) | For transferring files between computers. | 20 & 21 |
| SSH | Secure Shell. A secure/encrypted way to transfer files. | 22 |
| Telnet | Used to remotely log on to a system. You can then use a command prompt or shell to execute commands on that system. Popular with network administrators. | 23 |
| SMTP (Simple Mail Transfer Protocol) | Sends e-mail. | 25 |
| WhoIS | A command that queries a target IP address for information. | 43 |
| DNS (Domain Name Service) | Translates URLs into web addresses. | 53 |
| tFTP (Trivial File Transfer Protocol) | A quicker, but less reliable form of FTP. | 69 |
| HTTP (Hypertext Transfer Protocol) | Displays web pages. | 80 |