CHAPTER 1

Introduction

The turn of the century brings us into an era of exciting advancements in computer applications. New and innovative ways of integrating computer network technology into business, education, government, and even private homes have shifted focus from the underlying engineering that allows computer systems to talk to each other. And yet, when the systems don't talk to each other, the first thing people say is, "The network is having problems!" This book discusses methods for addressing those problems and explains how networks really work. Cisco and industry-standard troubleshooting methods for analyzing, diagnosing, and fixing problems are described in detail. The book also covers techniques for using protocol analyzers, such as the WildPackets EtherPeek and AiroPeek products, to recognize and isolate faulty network behavior.

Why We Wrote This Book

We wrote this book to provide technical people with technical information that they can apply to production environments and day-to-day network configuration, support, and troubleshooting. During the 1980s and 1990s, we worked with many experts in the computer industry, some very closely, some only in passing. It became clear who the experts were, because they all knew how networks really function. None of these people said "TCIP," and they all knew that a bridge operates at Layer 2 and a router at Layer 3. They also knew lots of other things.

Many people in the computer industry were not experts, however. They thought they understood many things, but they lacked certain fundamental knowledge. Lacking formal computer network education, and forced to use, implement, support, and maintain complex systems, they drew many erroneous conclusions and sometimes taught these to their peers.

This book focuses on many of the technology and engineering issues that are often misunderstood. In reading these pages you may encounter concepts that seem to contradict what others have told you. We have attempted to put down on paper some of the core information that is critical to successful troubleshooting and protocol analysis. This information is based on documents from renowned standards organizations such as the Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers (IEEE). Of more importance, the information is based on many years of analyzing real-world, diverse, and complex networks. This book has a unique protocol-level focus that is not found in most of the volumes of technical literature available today.

Guaranteed Not to Rust, Bust, or Collect Dust

Computer networks are like used cars, and, just as when you go to a used-car lot, you have to be careful not to get a lemon. The following can be said of both networks and used cars:

- They can be made to look good when you first examine them, but they sometimes have parts that are ready to fail when you need them most.
- An inexperienced technician can tinker with them and patch up the obvious problems, leading to the incorrect conclusion that the technician is an expert.
- Some problems have deceptive symptoms and only a true expert can discern the real causes.
- Even though the basic systems and technologies that make them work have not changed much over the years, they both incorporate whatever engineering schemes were popular at the time they were designed.

We were taught to pump the brakes if a car skids on an icy road, but this rule doesn’t apply when using anti-lock breaking. We were taught to turn into a skid, but this doesn’t apply when the car has front-wheel drive. Changes in automotive technology completely change the way we think about some of the fundamental aspects of driving.

We were taught that there are three Internet Protocol (IP) address classes (A, B, and C) that are used for unique host identification, but this doesn’t apply when classless addressing is implemented. We often hear that network utilization shouldn’t exceed 40 percent on Ethernet networks. However, this is no longer true on full-duplex Ethernet links. Changes in computer network technology change the way we think about fundamental methods of design and troubleshooting.

Whether you’re inspecting a used car or troubleshooting a computer network, you have to be on guard for hidden problems, advice from inexperienced helpers, confusing symptoms, and the fact that design evolution brings with it changes in terminology and function.

Audience and Scope

The audience for this book is network engineers, administrators, and technicians who manage Cisco and multivendor campus networks. A campus network is a network that spans buildings and consists of wired and wireless technologies that connect clients and servers. Although the word *campus* often refers to colleges or universities, and this book is perfectly matched to the needs of college network administrators, the book is not just for college network administrators but for any administrator who manages a campus network based on the following technologies:

- 10-, 100-, and 1000-Mbps Ethernet connectivity.
- 802.11 wireless communication.
- Switched connections between machines within a single network.
- Virtual Local Area Networks (VLANs) that segregate networks in a mesh topology.
- Routed connections between networks in a campus environment.
- Wide Area Network (WAN) connections between campus networks. (Although this book focuses on Local Area Networks [LANs], WAN information is also provided.)
- Upper-layer protocols from the Transmission Control Protocol (TCP)/Internet Protocol (IP), AppleTalk, Novell NetWare, and Windows networking protocol families.

This book isn't about figuring out if a cable is disconnected in a simple LAN; rather, it is about troubleshooting complex internetworks with tens, hundreds, or even thousands of users. This book is for network engineers who manage and configure internetworking devices. Although it doesn't cover workstation or server configuration, some of the information in this book will help desktop support personnel and server administrators also.

Finally, this book is also written for certification candidates, in particular, candidates for Cisco certifications and the vendor-neutral Network Analysis Expert (NAX) certification program sponsored by WildPackets Academy.

Cisco Certifications

In the Cisco arena, this book focuses on the Cisco Certified Network Professional (CCNP) and the Cisco Certified Internetwork Expert (CCIE) certifications.

The CCNP certification indicates advanced or journeyman knowledge of networks. Having the CCNP certification denotes to employers that you can install, configure, operate, and troubleshoot multiprotocol LAN, WAN, and dial-access services for organizations with networks from 100 to more than 500 nodes. To achieve CCNP status, you must pass five tests. This book focuses on the most advanced test, which is the Support Test. All the topics in Cisco's list of topics for the Support Test are covered.

This book is also for CCIE candidates. To achieve CCIE status, you must pass both a qualification written exam and a hands-on lab exam. This book will help you with the following CCIE Routing and Switching Qualification Exam topics:

- Cisco device operation
- General networking theory
- LAN addressing
- 10-, 100-, and 1000-Mbps Ethernet encapsulation, media access control, topologies, errors, and limitations
- Logical Link Control (LLC) 802.2
- Bridging and LAN switching
- TCP/IP
- IP routing protocols
- Desktop protocols including Novell NetWare and Windows networking
- Performance management
- WAN addressing, signaling, and framing

Because this book focuses on troubleshooting, it will also prepare you for the CCIE lab test. Now that Cisco has moved from a two-day lab test to a one-day lab test, applying efficient troubleshooting methods is even more important than it once was. The methods taught in this book will help you isolate and fix problems that appear in your lab network as you perform the difficult tasks required of the CCIE lab test-taker.

Please see www.cisco.com/warp/public/10/wwtraining for more information about Cisco certification programs.

The NAX Certification Program

The NAX certification program is an industry-standard, vendor-neutral program sponsored by the WildPackets Academy. Since 1990, WildPackets has been developing user-friendly and affordable tools for designing, maintaining, troubleshooting, and optimizing computer networks. WildPackets products include EtherPeek for Ethernet network analysis and AiroPeek for 802.11 wireless network analysis. Both of these products include NetSense real-time expert system technology for automated problem analysis. The TokenPeek analyzer addresses the needs of 802.5 Token Ring users.

To pass the NAX certification tests, a candidate can use WildPackets or other industry-recognized protocol analyzers. The candidate downloads an analyzer trace file and answers questions about real-world network problems. The exams test a candidate's understanding of protocols and ability to apply protocol analysis techniques to typical network problems. Achieving NAX certification involves three steps:

1. The Applied Analysis Technician (AATech) certification.
2. The Protocol Analyzer Specialist (PAS) certification.
3. The NAX certification.

These certifications require passing knowledge exams and practical skills exams. The knowledge exams require a candidate to demonstrate solid understanding of protocol analysis concepts and detailed knowledge of the Open System Interconnection (OSI) Reference Model and the protocols that operate at the various layers of the model. The practical skills tests require a candidate to demonstrate proficiency with a protocol analyzer. To achieve NAX certification, a candidate must also write a dissertation (white paper) on a topic selected from a list of topics approved by WildPackets Academy. This book will help with all of the knowledge exams in the NAX certification program as well as provide a solid foundation for the protocol-related aspects of many other industry certifications.

Please go to www.nax2000.com and download the Pre-Test Study Guide and Test-Taking Instructions document for complete details on the NAX certification program.

Organization

This book is organized in a bottom-up fashion. After an essential chapter on troubleshooting methods, the book works its way up the OSI Reference Model, starting with physical and data link layer concerns and ending with upper-layer concerns. The chapters are grouped as follows:

- Chapter 2 covers methods and tools for problem isolation, including Cisco and industry-standard troubleshooting procedures and protocol analysis with WildPackets or other analyzers. Chapter 2 also covers the OSI Reference Model and the Internet Control Message Protocol (ICMP).
- Chapters 3 and 4 explain how Ethernet and 802.11 wireless networks work and how to troubleshoot them when they don’t work. Chapter 3 also addresses 802.2 LLC.
- Chapters 5 and 6 remain at the data link layer and address the Spanning Tree Protocol, which is used on bridged and switched networks, and the configuration and troubleshooting of VLANs.
- Chapters 7 through 8 move up to the network layer and beyond, and cover IP addressing, IP routing protocols, a detailed analysis of TCP, and an overview of upper-layer TCP/IP protocols.
- Chapters 9 through 12 teach troubleshooting and protocol analysis for the most popular desktop protocols—Novell NetWare, AppleTalk, and Windows networking.

- Chapter 13 discusses WAN technology and troubleshooting from the perspective of the LAN-oriented network engineer.

Our Web Site

We have set up a Web site, which we hope you will visit often. The Web site will include updates as new information about troubleshooting becomes available. It also includes links to practice tests to help you study for certification exams, and suggestions for exercises you can try in a lab network to strengthen your troubleshooting skills. The address of the companion Web site is www.troubleshootingnetworks.com.